

Guía de Seguridad de las TIC

CCN-STIC 651B

Seguridad en Cortafuegos Cisco Firepower



Diciembre 2023



Catálogo de Publicaciones de la Administración General del Estado
<https://cpage.mpr.gob.es>

cpage.mpr.gob.es



CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL,
2.5.4.97=VATES-S2800155J, ou=CENTRO
CRYPTOLOGICO NACIONAL, o=CENTRO
CRYPTOLOGICO NACIONAL, c=ES
2024.01.29 13:41:06 +01'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2023

NIPO: 083-24-030-7

Fecha de Edición: diciembre de 2023

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

ÍNDICE

1. INTRODUCCIÓN	7
2. OBJETO.....	8
3. ALCANCE	9
4. SOBRE CISCO SYSTEMS	9
5. AMENAZAS DE SEGURIDAD – CISCO ATTACK CONTINUUM	10
6. ARQUITECTURA DE LOS EQUIPOS CISCO FIREPOWER	11
6.1 ARQUITECTURA DE LOS EQUIPOS ASA 5500-X E ISA 3000.....	15
6.2 ARQUITECTURA DE LOS EQUIPOS FIREPOWER 1000/2100	16
6.3 ARQUITECTURA DE LOS EQUIPOS FIREPOWER 4100/9300	17
6.4 MOTOR LINA	18
7. DISEÑOS Y POSICIONAMIENTO	19
7.1 CORTAFUEGOS PERIMETRAL	20
7.2 CORTAFUEGOS DE CENTRO DE DATOS (DATACENTER)	20
8. CONFIGURACIÓN INICIAL FIREPOWER FTD	21
8.1 CONFIGURACIÓN INICIAL ASA 5500-X/ISA 3000	21
8.2 CONFIGURACIÓN INICIAL FIREPOWER 1000/2100.....	24
8.3 CONFIGURACIÓN INICIAL FIREPOWER 4100/9300.....	28
8.4 CONFIGURACIÓN INICIAL FIREPOWER NGFW VIRTUAL (NGFWV).....	31
8.4.1 INSTALACIÓN Y CONFIGURACIÓN CON VMWARE VCENTER/VSPHERE	32
8.4.2 INSTALACIÓN Y CONFIGURACIÓN SIN VMWARE VCENTER/VSPHERE	36
9. MODOS DE FUNCIONAMIENTO DE CORTAFUEGOS FIREPOWER.....	39
9.1 MODO TRANSPARENTE	39
9.2 MODO RUTADO	41
10. FIREPOWER CHASSIS MANAGER - FXOS.....	42
10.1 MODO COMMON CRITERIA.....	43
10.2 SINCRONIZACIÓN DE HORA (NTP)	44
10.3 REGISTROS DE AUDITORÍA – AUDIT LOG.....	45
10.4 INSTALACIÓN DE CERTIFICADO HTTPS	47
10.5 GESTIÓN DE USUARIOS - RADIUS	50
10.6 COPIAS DE SEGURIDAD - BACKUP	52
10.7 CONFIGURACIÓN DE INTERFACES	54
10.8 INSTALACIÓN DE CORTAFUEGOS FTD	55
10.8.1 INSTALACIÓN INSTANCIA FTD NATIVE	57
10.8.2 INSTALACIÓN INSTANCIAS FTD CONTAINER	59
10.9 ACTUALIZACIÓN SISTEMA FXOS	62
11. BORRADO SEGURO DE FIREPOWER - DESMANTELAMIENTO	64
11.1 BORRADO SIMPLE EN FIREPOWER 1000/2100 (OPCIONAL)	64
11.2 FORMATEO Y BORRADO SEGURO ASA 5500-X/ISA 3000	65
11.3 FORMATEO Y BORRADO SEGURO FIREPOWER 1000/2100	65
11.4 BORRADO SEGURO FIREPOWER 4100/9300	67
12. REIMAGEN DEL SISTEMA.....	71
12.1 REIMAGEN DE EQUIPOS ASA 5500-X/ISA 3000	72

12.2 REIMAGEN DE EQUIPOS FIREPOWER 1000/2100	75
12.3 REIMAGEN DE EQUIPOS FIREPOWER 4100/9300	80
13. GESTOR FIREWALL MANAGEMENT CENTER (FMC)	86
13.1 EQUIPOS FÍSICOS FMC	86
13.1.1 CONFIGURACIÓN INICIAL	87
13.2 EQUIPOS VIRTUALES FMCV	88
13.2.1 INSTALACIÓN Y CONFIGURACIÓN INICIAL EN VMWARE	89
13.2.1.1 INSTALACIÓN Y CONFIGURACIÓN CON VCENTER/VSPHERE	89
13.2.1.2 INSTALACIÓN Y CONFIGURACIÓN SIN VCENTER/VSPHERE	93
13.2.2 INSTALACIÓN Y CONFIGURACIÓN INICIAL EN KVM	96
13.3 ALTA DISPONIBILIDAD FMC	97
13.4 MODO COMMON CRITERIA	103
13.5 SINCRONIZACIÓN DE HORA (NTP)	103
13.6 REGISTROS DE AUDITORÍA - AUDIT LOG	104
13.7 INSTALACIÓN DE CERTIFICADO HTTPS	106
13.8 CONFIGURACIÓN DE BANNER	108
13.9 GESTIÓN DE USUARIOS - RADIUS	109
13.10 LICENCIAMIENTO – SMART LICENSING	112
13.11 CONSIDERACIONES GENERALES: DEPLOY/TASKS/HEALTH	118
13.12 GESTIÓN DE DISPOSITIVOS	121
13.12.1 AÑADIR DISPOSITIVO	121
13.12.2 ELIMINAR DISPOSITIVO	124
13.12.3 GESTIÓN DE INTERFACES	125
13.12.3.1 ZONAS DE SEGURIDAD	125
13.12.3.2 ASIGNACIÓN DE DIRECCIONAMIENTO IP	125
13.12.3.3 ANTI-SPOOFING	127
13.12.3.4 ARP ESTÁTICO	127
13.12.3.5 CREACIÓN DE ETHERCHANNELS – ASA, ISA 3000 & FIREPOWER 2100/1000 128	
13.12.3.6 CREACIÓN DE SUBINTERFACES	130
13.12.3.7 CREACIÓN DE BRIDGE GROUP – FIREPOWER 4100/9300	131
13.12.4 ROUTING	132
13.12.5 VIRTUAL ROUTER (VRF)	135
13.12.6 DHCP RELAY	137
13.12.7 DHCP SERVER	139
13.13 CONFIGURACIÓN DE PLATAFORMA	140
13.13.1 MODO COMMON CRITERIA	141
13.13.2 SINCRONIZACIÓN DE HORA (NTP)	142
13.13.3 CONFIGURACIÓN DE BANNER	142
13.13.4 GESTIÓN DE USUARIOS – RADIUS	143
13.13.5 TIMEOUTS	145
13.13.6 RESOLUCIÓN DNS	145
13.13.7 SYSLOG	146
13.14 ALTA DISPONIBILIDAD	148
13.14.1 ALTA DISPONIBILIDAD ACTIVO/PASIVO – FAILOVER	148

13.14.2 ALTA DISPONIBILIDAD ACTIVO/ACTIVO – CLUSTER	152
13.15 POLÍTICA DE NAT	158
13.15.1 NAT DINÁMICO	159
13.15.2 NAT ESTÁTICO	163
13.15.3 NAT DE IDENTIDAD – IDENTITY NAT	165
13.16 POLÍTICA DE ACCESO – ACCESS CONTROL POLICY (ACP)	167
13.16.1 LOG DE CONEXIONES – SYSLOG	169
13.16.2 FILTRO DE APLICACIONES - AVC	170
13.16.3 FILTRO POR URL - URL FILTERING	172
13.16.4 FILTRO SECURITY INTELLIGENCE	174
13.17 DESCUBRIMIENTO EN RED – NETWORK DISCOVERY	178
13.18 POLÍTICA DE INTRUSIÓN – INTRUSION POLICY (NGIPS)	179
13.18.1 PREVENCIÓN DE PERDIDAS DE DATOS (DLP)	187
13.19 DESCUBRIMIENTO DE IDENTIDADES (IDENTITY POLICY)	189
13.20 PROTECCIÓN DE MALWARE (AMP)	201
13.21 INTERCEPCIÓN SSL – SSL POLICY	205
13.22 THREAT INTELLIGENCE DIRECTOR (TID)	211
13.23 RED PRIVADA VIRTUAL - VPN SITE TO SITE	214
13.24 RED PRIVADA VIRTUAL - VPN DE ACCESO REMOTO	219
13.25 COPIAS DE SEGURIDAD – BACKUP	227
13.26 INTERFAZ PROGRAMÁTICA REST API	232
13.27 ACTUALIZACIÓN DEL SISTEMA FMC	233
13.28 ACTUALIZACIÓN CORTAFUEGOS FTD	236
13.29 ACTUALIZACIÓN VULNERABILITY DATABASE (VDB)	239
13.30 ACTUALIZACIÓN SNORT RULE UPDATES (SRU)	240
13.31 ACTUALIZACIÓN DE GEOLOCALIZATION	241
14. GESTOR FIREPOWER DEVICE MANAGER (FDM)	242
14.1 ASISTENTE DE CONFIGURACIÓN	243
14.2 GESTIÓN DE INTERFACES	244
14.3 ZONAS DE SEGURIDAD	246
14.4 ROUTING	247
14.5 FILTRO DE GESTIÓN DE PLANO DE DATOS	247
14.6 DEPLOY/TASKS	248
14.7 POLÍTICA DE ACCESO – ACCESS CONTROL POLICY (ACP)	249
14.8 FILTRO DE APLICACIONES - AVC	250
14.9 LOG DE CONEXIONES – SYSLOG	250
14.10 POLÍTICA DE NAT	251
14.10.1 NAT DINÁMICO	252
14.10.2 NAT ESTÁTICO	252
14.11 CONSOLA CLI INTEGRADA	252
14.12 ALTA DISPONIBILIDAD ACTIVO/PASIVO – FAILOVER	253
14.13 ACTUALIZACIÓN SISTEMA FTD Y FDM	257
14.14 ACTUALIZACIÓN DE GEOLOCATION, RULE, VDB, SI	258
15. PROTECCIÓN DE DENEGACIÓN DE SERVICIO - DDOS	259
16. UTILIDAD DE MIGRACIÓN A FIREPOWER	265

17. ANEXO A. LISTA DE COMPROBACIÓN – CHECKLIST	273
18. ANEXO B. ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD	278

1. INTRODUCCIÓN

Los cortafuegos han sido tradicionalmente la primera y principal línea de defensa en las redes de comunicaciones. Su capacidad para filtrar tráfico, transformarlo, mediante traducciones y aleatorizaciones de secuencias, e inspeccionar su correcto cumplimiento con los protocolos, constituye una buena barrera defensiva.

Sin embargo, en los últimos años, las amenazas y los ataques se han vuelto más sofisticados, lo que ha requerido la mejora de los sistemas cortafuegos clásicos a cortafuegos de Nueva Generación (Next Generation Firewalls - NGFW).

No existe una definición formal o estandarizada sobre lo que un cortafuegos necesita para ser considerado de nueva generación (NGFW), pero se puede establecer que son cortafuegos que han evolucionado incorporando algunas nuevas funcionalidades de seguridad como inspección de aplicación DPI (Deep Packet Inspection - Inspección a fondo de los paquetes a nivel de aplicación, OSI capa 7), Anti-malware (anti-virus, anti-spyware, anti-spam), IPS (Sistema de Prevención anti Intrusiones), interceptación de tráfico cifrado (TLS/SSL), filtrado de sitios web por direcciones URL y categorías (URL filtering), gestión de identidades integrada (Windows User Agent), entre otras.

A lo largo de la historia, ha habido diversas generaciones de cortafuegos, siendo denominada la NGFW como la tercera generación.

Generación 1: Filtrado de paquetes (como una ACL unidireccional).

Generación 2: Filtrado de paquetes con seguimiento de estado (stateful firewall).

Generación 3: Filtrado en la capa de aplicación con características adicionales.

Cisco Systems ha estado durante muchísimos años a la vanguardia de los cortafuegos, con un producto sólido, eficaz y muy estable, los Cisco ASA.

Estos equipos se podían complementar con soluciones IDS/IPS y Anti-X añadidas, vía módulos y licencias.

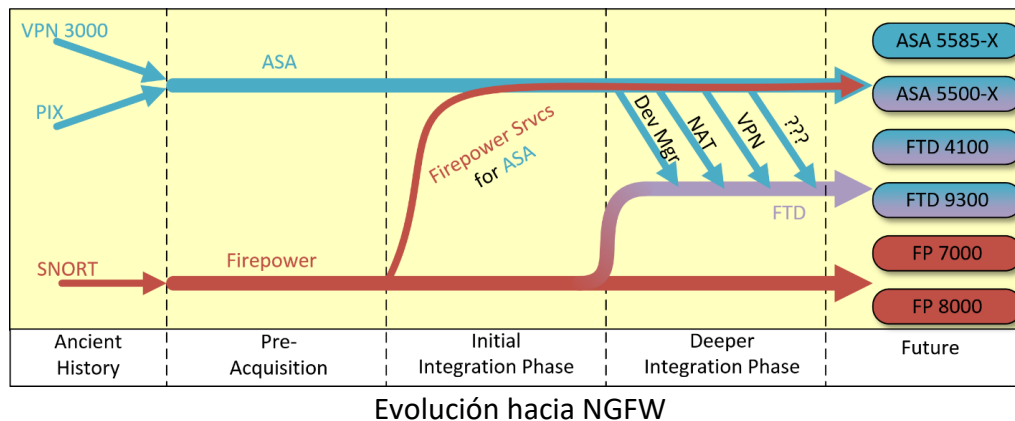
Sin embargo, lo que los firewalls de Nueva Generación proponen, es una integración de todas estas funcionalidades y no su funcionamiento por separado.

En el año 2013, Cisco Systems adquiere la compañía Sourcefire, lo que hace posible la integración de Cisco ASA con las funcionalidades avanzadas proveídas por Sourcefire, que tienen como máximo referente la herramienta Snort.

Tras la adquisición de Sourcefire, unida a la adquisición de ThreatGRID, se inicia un período de integración de tecnologías y la creación de Talos Intelligence como centro unificado de gestión de amenazas.

Talos es el equipo principal que aporta información sobre amenazas al ecosistema de Cisco Collective Security Intelligence (CSI). Cisco CSI se comparte a través de múltiples soluciones de seguridad y brinda protección y eficacia de seguridad líderes en la industria. Talos mantiene los conjuntos de reglas oficiales de Snort.org, ClamAV, SenderBase.org y SpamCop (<https://www.talosintelligence.com/>).

En el siguiente cronograma se puede observar visualmente la adaptación y evoluciones realizadas en el tiempo entre las diferentes soluciones de Cisco, desde PIX hasta ASA y, con la adquisición de Sourcefire, los nuevos equipos FTD (Firepower Thread Defense) como los cortafuegos de verdadera Nueva Generación de Cisco.



Los equipos FTD (Firepower) de Cisco son cortafuegos de Nueva Generación con las siguientes características resaltables:

- Seguimiento de estado de conexiones (Cortafuegos generación 2).
- Filtros de capa de aplicación (AVC - capa 7).
- Capacidad de Identificación de conexiones suministradas por terceros (usuarios de Windows – Windows User Agent).
- Sistema de Protección de Intrusiones (IPS) + Security Intelligence (filtros de reputación). Actualizados desde Talos.
- Anti-Malware Protección (AMP).
- Filtros de direcciones Web/URL (URL-Filtering).

2. OBJETO

Esta guía, dentro de las series CCN-STIC, tiene como objetivo servir como referencia en la configuración y administración correcta de los cortafuegos de Nueva Generación Cisco Firepower FTD.

El aspecto fundamental a cubrir en esta guía es la utilización y configuración de la solución completa de Firepower FTD de Cisco abordándolo desde el punto de vista de la seguridad.

Para cuestiones específicas de operación, configuración o instalaciones detalladas, deben referirse a las guías publicadas por Cisco Systems en su web.

3. ALCANCE

Esta instrucción es de aplicación para la instalación y gestión de los cortafuegos Firepower FTD del fabricante Cisco por parte de los administradores encargados de su gestión y de auditores de seguridad.

No obstante, aunque no puedan aplicarse directamente los ejemplos enumerados, sí que pueden seguirse sus directrices en otras tecnologías.

La aplicación de esta guía vendrá determinada por la correspondiente política de seguridad que corresponda (Política de Seguridad Nacional para Sistemas Clasificados, Esquema Nacional de Seguridad, etc...) y su correspondiente análisis de riesgos.

La información contenida en esta guía corresponde a la versión 7.0 de FTD.

4. SOBRE CISCO SYSTEMS

Cisco Systems fue fundada en diciembre de 1984 por Leonard Bosack y Sandy Lerner, dos científicos informáticos de la Universidad de Stanford. Fueron pioneros en el concepto de una red de área local (LAN) que se utiliza para conectar dispositivos geográficamente dispersos a través de un sistema de enrutador multiprotocolo. Cuando la compañía comenzó a cotizar en bolsa en 1990, Cisco tenía una capitalización de mercado de \$224 millones. Al final de la burbuja punto-com en el año 2000, Cisco tenía una capitalización de mercado de más de \$500 mil millones.

Cisco Systems, Inc. es un conglomerado de tecnología multinacional estadounidense con sede en San José, California, en el centro de Silicon Valley. Cisco desarrolla, fabrica y vende hardware de redes, equipos de telecomunicaciones y otros servicios y productos de alta tecnología. A través de sus numerosas subsidiarias adquiridas, como OpenDNS, WebEx, Jabber y Jasper, Cisco se especializa en mercados de tecnología específicos, como Internet of Things (IoT), seguridad de dominio y administración de energía.

Adquisiciones relevantes en materia de seguridad:

En octubre de 2013, Cisco adquiere la compañía de cyber-seguridad, Sourcefire.

En junio de 2014, Cisco anuncia la adquisición de ThreatGRID, compañía que provee de análisis dinámico de malware y tecnología de inteligencia ante amenazas.

En junio de 2015, Cisco adquiere OpenDNS, compañía privada conocida por proveer seguridad a través de la monitorización de consultas DNS.

En octubre de 2015, Cisco anuncia la adquisición de Lancope, compañía especializada en la detección de amenazas a través de análisis de actividad (Stealthwatch).

En junio de 2016, Cisco anuncia la adquisición de CloudLock, compañía de seguridad especializada por proveer servicios de seguridad para la nube.

5. AMENAZAS DE SEGURIDAD – CISCO ATTACK CONTINUUM

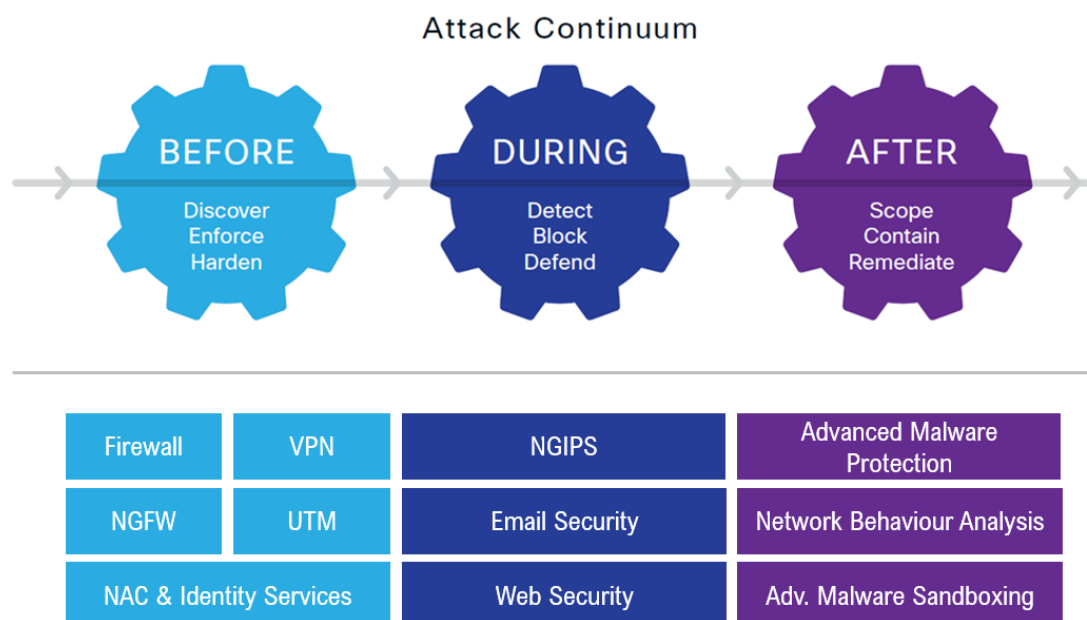
El panorama de amenazas de hoy no se parece en nada a lo que era hace una década. Los ataques simples han dado paso a ataques cibernéticos más sofisticados llevados a cabo por organizaciones especializadas en delitos informáticos y grupos financiados y patrocinados por diferentes países.

Con estas nuevas amenazas, Cisco sintió que era hora de un cambio de enfoque, y dado que en todo ataque cibernético existen pautas y fases. El modelo de Cisco Attack Continuum es el modelo de seguridad que respalda el portafolio de seguridad de Cisco y que vincula la operación de AMP, Umbrella y otros productos de seguridad.

Estos ataques avanzados de hoy en día se han vuelto muy difíciles de detectar, utilizan una gran cantidad de recursos para lanzar estos ataques de forma remota y tienden a permanecer presentes en una red comprometida durante largos períodos de tiempo. La industria ha calculado que la detección de estas amenazas lleva en promedio 100 días, lo que hace que los atacantes estén presentes en su red durante más de tres meses.

Los métodos de seguridad normales que se basan exclusivamente en mecanismos de detección y bloqueo, como firewalls y antivirus, ya no son suficientes para hacer frente a las amenazas en constante evolución de hoy en día.

Cisco Attack Continuum es un enfoque de seguridad centrado en amenazas que apunta a ofrecer Protección Avanzada contra Amenazas, Visibilidad Superior y Control Continuo, Antes, durante y después de un ataque.



La “fase previa” (BEFORE) de Attack Continuum busca impulsar las capacidades “Predictivas y Preventivas”. El objetivo aquí es proporcionar al personal de seguridad una visibilidad y conocimiento completos de lo que hay en la red. Al saber qué hay, se pueden desarrollar políticas de seguridad y configuraciones que fortalecerán las defensas y reducirán la superficie de ataque, haciendo que sea más difícil para los atacantes poner en peligro y comprometer la red.

La “fase durante” (DURING) se centra en las capacidades de “Prevención y Detección”. Aquí es donde debemos tomar conciencia del conocimiento adquirido en la fase BEFORE y actuar sobre ella, detectar el malware que está presente en sus entornos y tener los controles para bloquearlo. Aquí, no solo se busca depender de los métodos tradicionales de detección en un punto en el tiempo y bloqueo, sino que también se tiene en cuenta los patrones y comportamientos históricos, así como la inteligencia global de amenazas.

La “fase posterior” (AFTER) se centra en las capacidades de “Detective y Respuesta”. En el caso de que una amenaza atravesara el perímetro y evada la primera línea de las defensas de la red, aquí es donde necesita seguridad retrospectiva. El monitoreo continuo de los archivos, los procesos y la actividad de la red, permite comprender qué ha ocurrido en qué lugar, dar una mirada atrás en el tiempo para identificar indicaciones de compromiso y permitirle responder rápidamente y remediar cualquier problema descubierto.

Cisco cuenta con diferentes productos para gestionar este modelo:

Fase Before: Descubrir amenazas, aplicación y reforzamiento de políticas, y prevención en el perímetro. Utilizando los cortafuegos de última generación, NAC e Identity Services Engine.

Fase During: Detección, bloqueo y defensa contra ataques que ya han penetrado la red y están en curso. Usando sistema de prevención de intrusiones de Nueva Generación (NGFW-IPS) y seguridad en correo y web (ESA, WSA).

Fase After: Determinar el alcance de afectación, contención y remediación de un ataque para minimizar el daño, usando la Protección avanzada de malware (AMP, AMP Endpoint), la Threat Grid y el análisis del comportamiento de la red (StealthWatch).

6. ARQUITECTURA DE LOS EQUIPOS CISCO FIREPOWER

Los equipos que pueden correr imágenes Cisco Firepower FTD 7.0 actualmente son: Cisco ASA 5500-X (ASA 5508-X y ASA 5516-X), Cisco ISA 3000, Cisco Firepower 1000, Cisco Firepower 2100, Cisco Firepower 4100, Cisco Firepower 9300 y Firepower NGFW Virtual.

Todos estos equipos, excepto el Firepower NGFW Virtual, disponen de 2 opciones, ejecutar una imagen Cisco Firepower FTD o ejecutar una imagen Cisco ASA. Esta guía solo cubre la primera opción (imagen Cisco Firepower Threat Defense (FTD)).



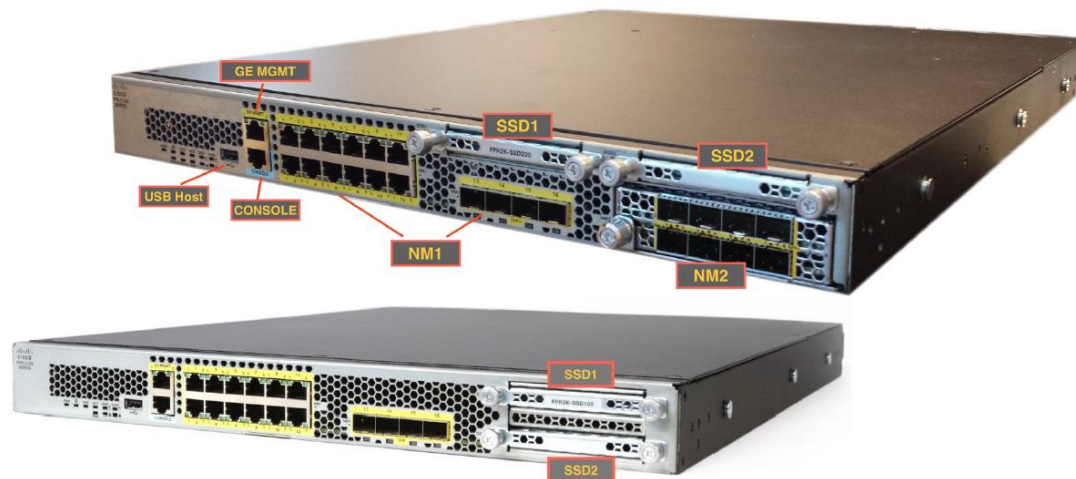
Cisco ASA 5516-X



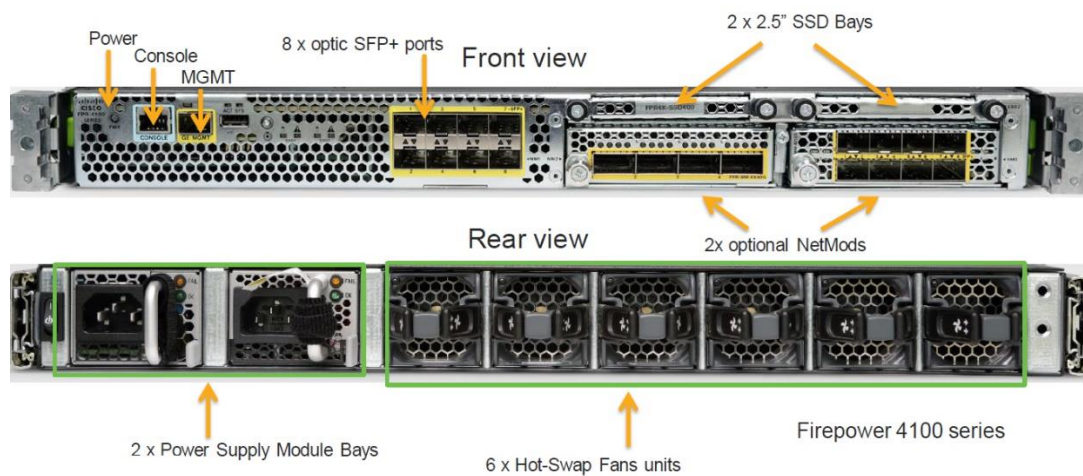
Cisco ISA 3000



Firepower 1000 Series (1010 – 1120/1140/1150)



Firepower 2100 Series (2110/2120 – 2130/2140)



Firepower 4100 Series



Firepower 9300 Series

Specification	4 vCPU	8 vCPU	12 vCPU
Throughput: FW + AVC (1024B)	3 Gbps	5.5 Gbps	10 Gbps
Throughput: FW + AVC + IPS (1024B)	3 Gbps	5.5 Gbps	10 Gbps
Throughput: FW + AVC (450B)	1.5 Gbps	3 Gbps	5 Gbps
Throughput: FW + AVC + IPS (450B)	1 Gbps	2 Gbps	3 Gbps

Firepower NGFW Virtual

Los equipos ASA 5508-X y 5516-X eran los antiguos modelos de firewall de gama baja hasta la introducción de la familia Firepower 1000. Estos equipos son adecuados para cortafuegos perimetrales sin muchos requerimientos de ancho de banda. Disponen de conexiones a 1G, incluyendo modelo con un switch, y el modelo superior dispone de algún interfaz de 10G en SFP+. El modelo 1010 es más pequeño que 1U, ideal para espacios pequeños, con opción de expansión a 1U enrackable. El resto son de 1U enrackables.

Los equipos Firepower 2100 son equipos de 1U adecuados para cortafuegos perimetrales o de centro de datos sin grandes requerimientos de un alto rendimiento. Vienen equipados con conexiones a 1G (2110/2120) y 1G/10G (2130/2140).

Los equipos Firepower 4100 son equipos de alto rendimiento en formato 1U, adecuados para su uso como cortafuegos de centro de datos. Equipados con conexiones a 1G y 10G, y módulos con posibilidad de conexiones a 40G. Su rendimiento puede mejorarse con la unión de varios de estos equipos en clúster.

Los equipos Firepower 9300 son chasis de hasta 3 equipos firewalls internos, cuyo rendimiento depende de los módulos instalados. Su rendimiento puede mejorarse utilizando tecnología clúster tanto interno como externo. O pueden usarse de manera separada.

Por último, los equipos Firepower NGFW Virtual son cortafuegos para instalar sobre hipervisores, ESXi, KVM o en imágenes de los principales proveedores de nube, AWS, Azure, Google, Oracle.

En esta guía vamos a tratar principalmente los equipos Firepower 2100 y 4100. Los equipos 1000 son de arquitectura similar a los 2100 y los equipos 4100 son arquitecturalmente similares a los 9300 disponiendo los 4100 de un único módulo (cortafuegos) en vez de la posibilidad de tres.

Por último, los equipos ISA 3000 están diseñados para ser resilientes en entornos industriales bajo condiciones más extremas en comparación al resto de modelos.

6.1 ARQUITECTURA DE LOS EQUIPOS ASA 5500-X e ISA 3000

Los equipos ASA tradicionales son capaces de correr tanto el software ASA como FTD. Estas imágenes se instalan sobre la ROMmon del sistema.

Estos hardware tienen su propia arquitectura donde, a diferencia de nuevo Firepower hardware no tienen la capa de FXOS.

Los equipos ISA (Industrial Security Appliances) 3000 tienen una arquitectura muy similar a los ASA pero reforzada para ser desplegados en entornos IoT/OT.

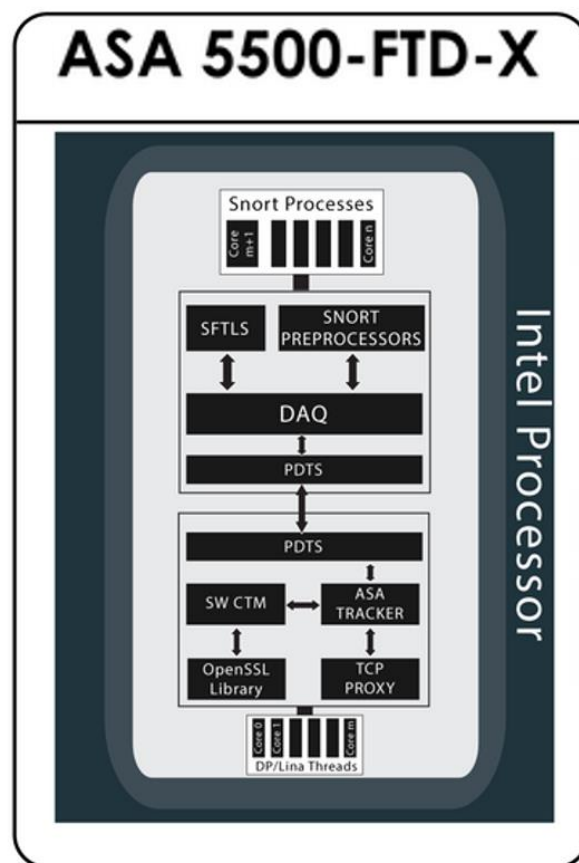


Diagrama de arquitectura ASA

6.2 ARQUITECTURA DE LOS EQUIPOS FIREPOWER 1000/2100

Los equipos Firepower, en general, están compuestos de la unión de tres tecnologías de Cisco.

El sistema de Fabric Interconnect (Nexus NXOS) provee de la conectividad de red.

Los servidores UCS (Unified Computing System) es el hardware servidor donde se instala y ejecuta el software del firewall.

La imagen FTD (Firepower Thread Defense) es el instalable que se ejecuta dentro del servidor y provee de las funcionalidades de cortafuegos de Nueva Generación. En esta imagen, por debajo corre una imagen de ASA modificada, junto a instancias Snort que proveen de las funcionalidades avanzadas de capa de aplicación AVC, IPS, AMP.

En Firepower 1000 y 2100 no existe el concepto de chasis, ya que son equipos integrados donde una única imagen gestiona todo el equipo.

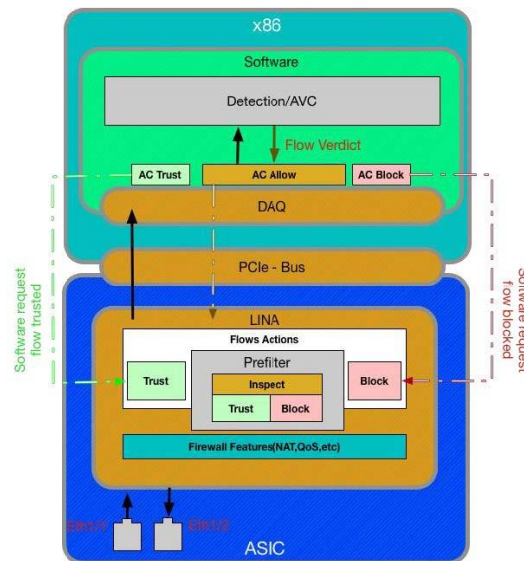


Diagrama de arquitectura Firepower 1000 y 2100

6.3 ARQUITECTURA DE LOS EQUIPOS FIREPOWER 4100/9300

Los equipos Firepower 4100 y 9300, en cambio, al ser una arquitectura heredada de FP 9300 presentan una gestión del chasis a través del sistema FXOS (Firepower eXtensible Operating System).

La parte de FXOS controla el chasis y las interfaces y se encarga de instalar la imagen de FTD y asignarle las interfaces. El sistema FXOS se actualiza y configura de manera independiente al FTD.

Es muy importante realizar las actualizaciones de FXOS además de las actualizaciones de FTD. En las notas de reléase debe verificarse que las versiones FXOS y FTD son compatibles entre sí.

La parte de FXOS controla el Fabric Interconnect.

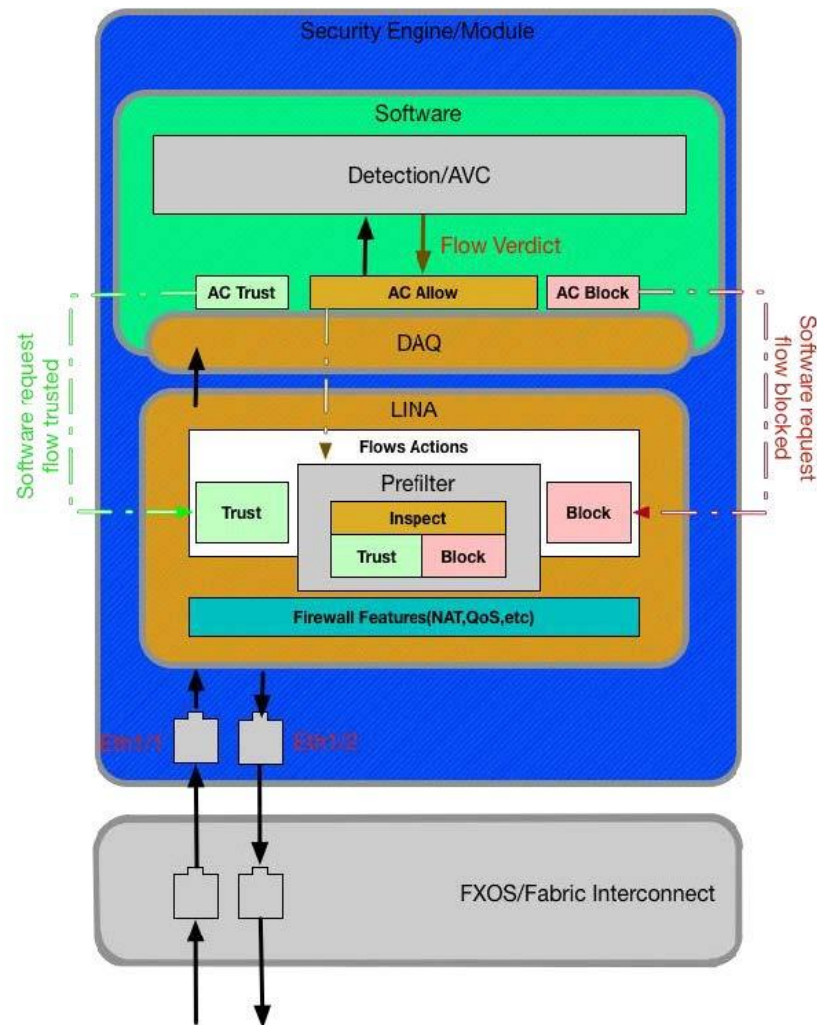


Diagrama de arquitectura Firepower 4100/9300

6.4 MOTOR LINA

El funcionamiento de los firewalls FTD está basado en el motor “Lina” (no es un acrónimo).

Este motor combina las funcionalidades de una imagen ASA como base para servicios adicionales proveídos por Snort.

A la imagen base ASA se puede acceder, mediante SSH/CLI, solo para consultas o solución de problemas, no se permite su configuración directa (“conf t”).

También es posible acceder al sistema Unix interno mediante el comando “expert”.

FTD Packet-Flow

```
graph LR; RX((RX)) --> Ingress[Ingress Interface]; Ingress --> Existing{Existing Conn}; Existing -- YES --> DAQ[DAQ]; Existing -- NO --> Egress[Egress Interface]; VPNDecrypt[VPN Decrypt] --> Egress; Egress --> PreFilter{Pre-Filter}; PreFilter --> L3L4ACL[L3/L4 ACL]; L3L4ACL --> DAQ; DAQ --> PDTS[PDTS]; PDTS --> Lina[Lina rule-id matched]; Lina --> DAQ; DAQ --> ALG[ALG checks]; ALG --> NAT[NAT]; NAT --> QoS[QoS, VPN Encrypt]; QoS --> L3L2[L3, L2 hops]; L3L2 --> TX((TX));
```

The diagram illustrates the FTD Packet-Flow process. It begins with an RX (Receive) interface, leading to an Ingress Interface. A decision is made on whether an Existing Conn (Connection) exists. If YES, the flow proceeds to the DAQ (Data Acquisition) block. If NO, it proceeds to the Egress Interface. A VPN Decrypt block feeds into the Egress Interface. The flow then passes through a Pre-Filter, followed by L3/L4 ACL (Access Control List). The DAQ block is also connected to the L3/L4 ACL. The DAQ block feeds into the PDTS (Packet Detection and Tracking System) block. The PDTS block feeds into the Lina (Lina rule-id matched) block. The Lina block feeds back into the DAQ block. The DAQ block feeds into the ALG (Application Layer Gateway) checks block. The ALG checks block feeds into the NAT (Network Address Translation) block. The NAT block feeds into the QoS (Quality of Service) and VPN Encrypt block. The QoS and VPN Encrypt block feeds into the L3, L2 hops block. The L3, L2 hops block feeds into the TX (Transmit) interface.

Data-Path / LINA

Nota Importante: mientras que es posible acceder y visualizar la configuración del sistema ASA/FTD básico, incluyendo lista de acceso (ACL), es el motor Lina el que decide si los paquetes son permitidos o denegados. Por lo tanto, no debe considerarse esta configuración, en lo relativo a “access-list”, como realista.

Dependiendo de la necesidad a cubrir se pueden establecer dos tipos de topologías o diseños principales a implementar con cortafuegos. Cortafuegos perimetrales o cortafuegos de centro de datos (DataCenter).

Centro Criptológico Nacional

7.1 CORTAFUEGOS PERIMETRAL

En este diseño lo que se requiere es que haya un cortafuegos “frontera” que delimite zonas de seguridad bien diferenciadas. Por ejemplo, entre diferentes organizaciones o unidades, o también publicaciones de servicios entre redes. En estos casos el cortafuegos se sitúa filtrando en los perímetros de esas zonas.

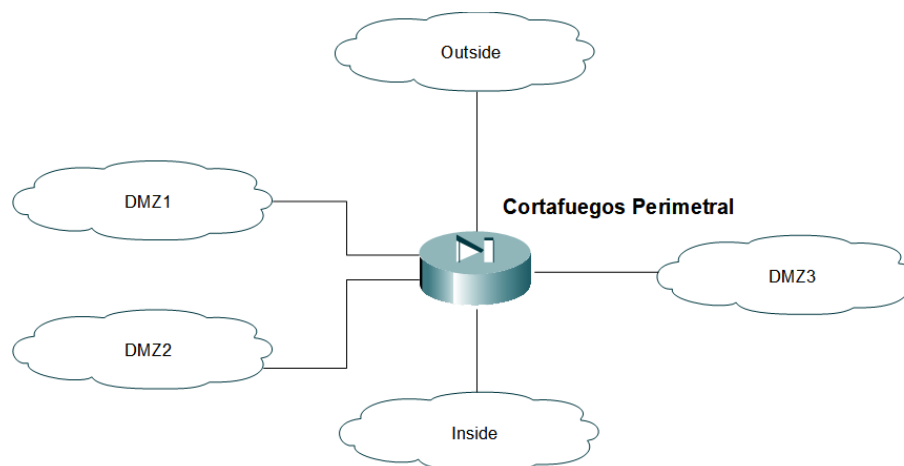


Diagrama de ejemplo de Cortafuegos Perimetral

Los equipos que Cisco posiciona para este tipo de diseños son:

- ASA 5500-X.
- Firepower 1000.
- Firepower 2100.

7.2 CORTAFUEGOS DE CENTRO DE DATOS (DATACENTER)

En este diseño no se pretende una separación o filtrado entre redes, lo que se pretende es ejercer control sobre la propia red y separar esta red en zonas de seguridad agrupando equipos con usos similares dentro de la misma zona, ejerciendo control y análisis sobre toda la red, además de filtrado.

Esta arquitectura de seguridad se basa en el principio de compartimentación de seguridad, donde en el caso de compromiso de una de las zonas de seguridad, el resto de las zonas no se vean afectadas.

Un ejemplo de beneficio de uso de esta arquitectura es un código dañino o virus que pueda tener éxito en un equipo de usuario y comprometerlo, donde esa amenaza no podría progresar libremente hacia los servidores u otras zonas.

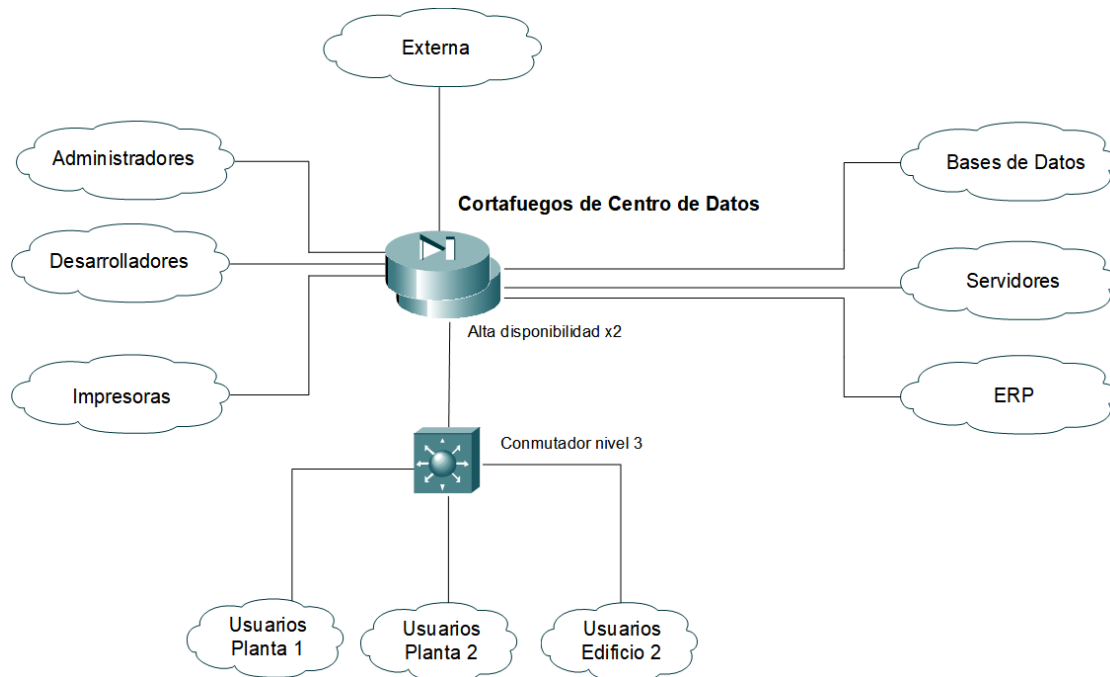


Diagrama de ejemplo de Cortafuegos de Centro de Datos (DataCenter)

Los equipos que Cisco posiciona para este diseño son:

- Firepower 4100.
- Firepower 9300.
- Firepower 2100, solo para redes pequeñas.

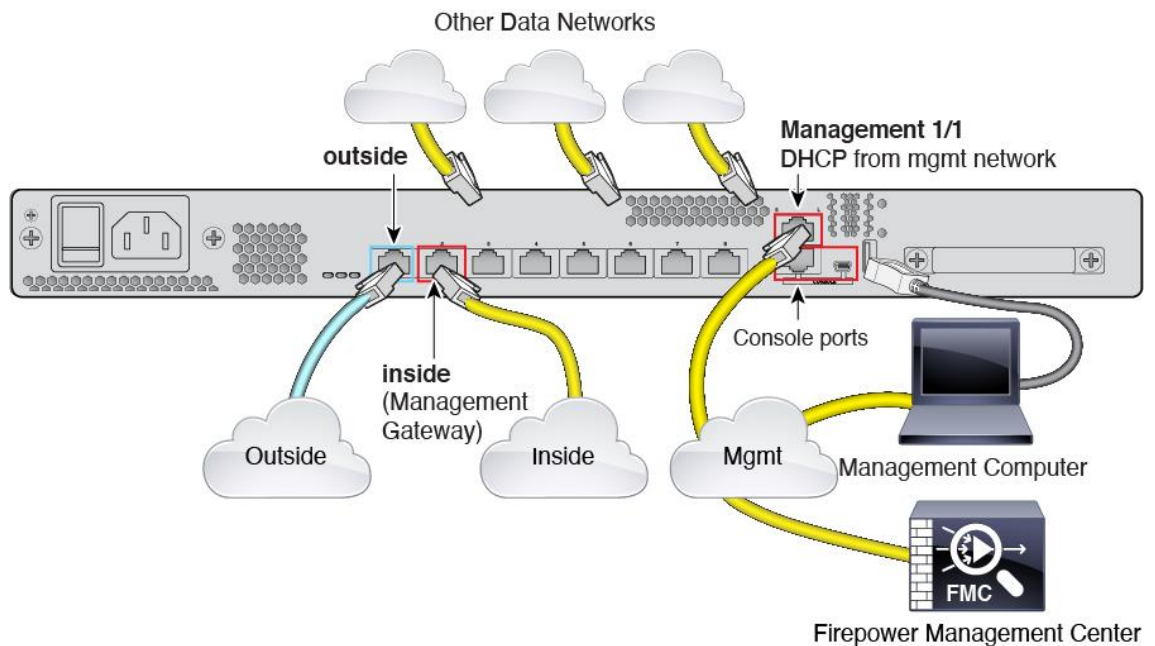
8. CONFIGURACIÓN INICIAL FIREPOWER FTD

Los cortafuegos Firepower disponen de gestión fuera de banda (Out of Band) mediante conexiones dedicadas.

Estas conexiones deben ser consideradas parte de la red de Gestión. Siempre que sea posible, deben configurarse en una zona de seguridad dedicada o, si no es posible, en una VLAN dentro de la red de Gestión.

8.1 CONFIGURACIÓN INICIAL ASA 5500-X/ISA 3000

Los ASA 5508/5516 tienen un puerto RJ-45 para la gestión que será el Management 1/1 y un puerto de consola. Para la configuración inicial, es recomendable utilizar este último:



Una vez encendido el equipo, a través del equipo conectado al puerto consola debemos ver en pantalla que se nos muestra el End User License Agreement (EULA) que deberemos aceptar antes de proceder con el resto de la configuración inicial:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress. Please stand by.
```

Una vez aceptado el EULA podemos proceder con la configuración de las credenciales del usuario administrador local “admin” y la configuración inicial. Esta configuración incluye:

- IP de interfaz de gestión Management 1/1.
- Default Gateway para la interfaz de gestión.
- Hostname.
- Servidores DNS.

- Modo de gestión del equipo (Local o FMC). Esta guía asume que el equipo será gestionado a través de una consola FMC.
- Modo del firewall (routed si va a tener interfaces con dirección IP o transparent en caso de ser un firewall que opera en L2).

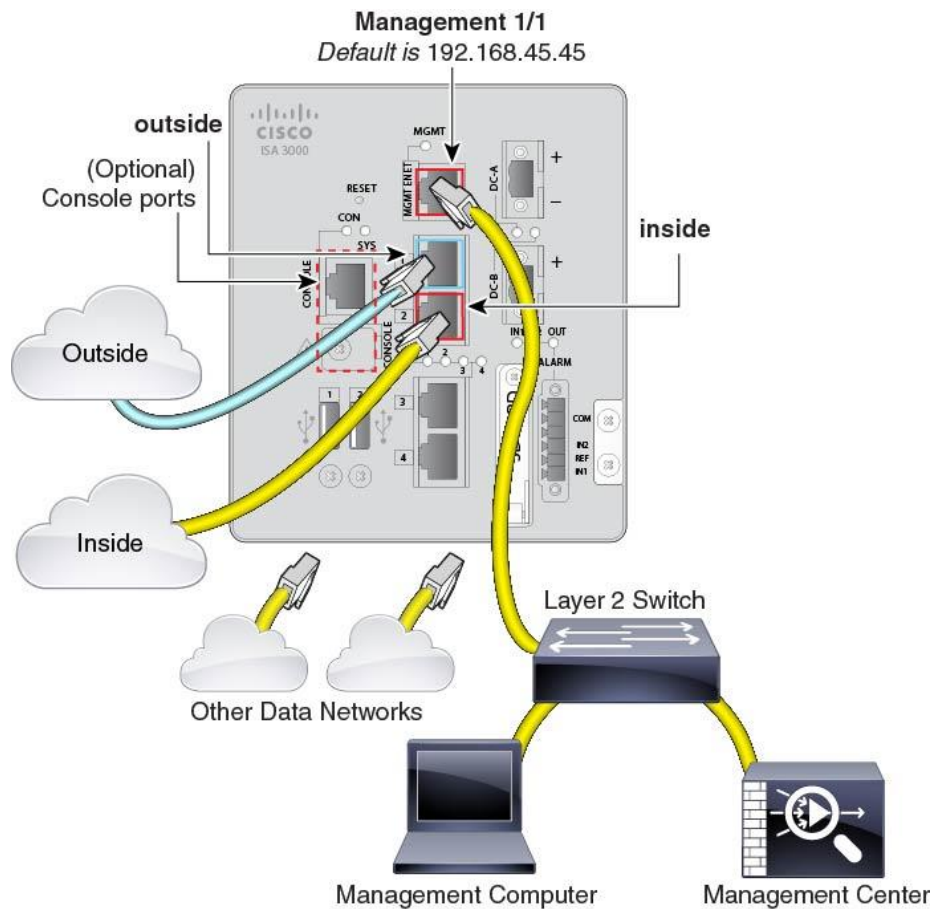
```
System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password: *****
Confirm new password: *****
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]:
10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]:
255.255.255.192
Enter the IPv4 default gateway for the management interface [data-
interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-
1.cisco.com
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to
reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...
```

Finalmente procederemos a configurar los detalles del FMC para la gestión del equipo desde el que se realizará el resto de la configuración del sistema:

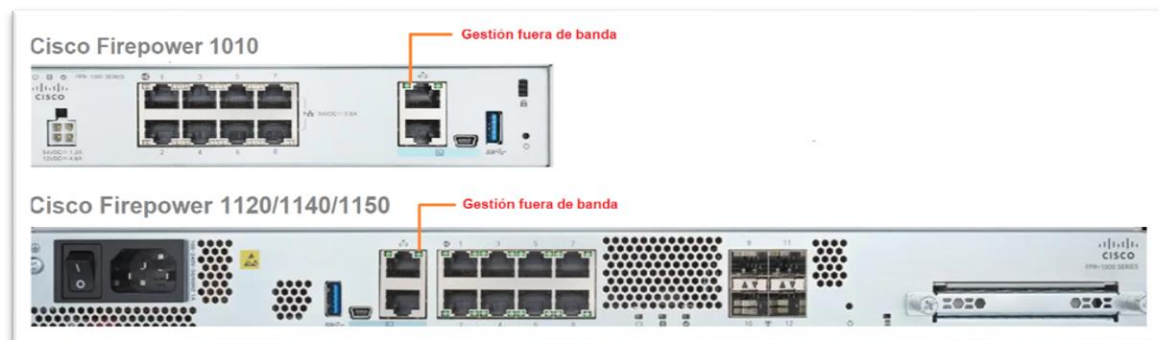
```
> configure manager add 10.10.20.20 clave
Manager successfully configured.
```

En el caso de los ISA 3000, la configuración es idéntica a la de los ASA 5500-X. Como referencia a continuación se encuentra el diagrama de puertos donde se muestra el puerto de consola y el de management 1/1:

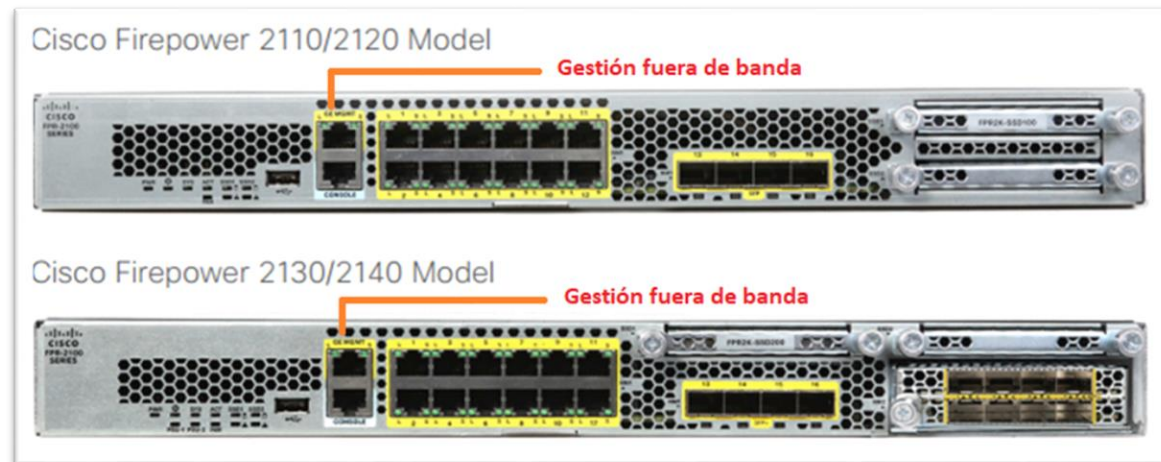


8.2 CONFIGURACIÓN INICIAL FIREPOWER 1000/2100

Tanto los equipos Firepower 1000 como 2100 son plataformas integradas con una sola imagen que incluye FTD+FXOS. Los equipos disponen de una conexión de red de gestión fuera de banda que puede manejar toda la plataforma.



Conexión de la gestión fuera de banda Firepower 1000



Conexión de la gestión fuera de banda Firepower 2100

Para la configuración inicial, se recomienda la conexión por consola RS232 9600bps, utilizando un cable de consola “Cisco” (rollover). En el encendido, el equipo realizará una serie de preguntas para configurarse. Tras la configuración se procederá a conectar el cable físicamente en el interfaz fuera de banda.

```
*****
Cisco System ROMMON, Version 1.0.06, RELEASE SOFTWARE
Copyright (c) 1994-2017 by Cisco Systems, Inc.
Compiled Wed 11/01/2017 18:38:59.66 by builder
*****

Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM_1/1 : Present
DIMM_2/1 : Absent

Platform FPR-2110 with 16384 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 38:90:a5:84:21:00

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.

Located '.boot_string' @ cluster 643911.

#
Attempt autoboot: "boot disk0:installables/switch/fxos-k8-fp2k-lfbff.2.2.1.49.SPA"
Located 'installables/switch/fxos-k8-fp2k-lfbff.2.2.1.49.SPA' @ cluster 15580.
.
...
.
Wind River Linux 6.0.0.29 firepower ttyS0

firepower login:
```

Las credenciales por defecto son:

- Usuario: admin

- Contraseña: Admin123

En los siguientes cuadros de texto, lo resaltado en negrita son las entradas de texto realizadas.

```
firepower login: admin
Password:
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2015, Cisco Systems, Inc. All rights reserved.
.
...
.
firepower#
```

El dispositivo arranca el sistema FXOS que, en estas plataformas, es parcialmente accesible.

Si es el primer arranque del sistema, hay que esperar a que la imagen FTD sea automáticamente instalada antes de poder iniciar el siguiente paso de la configuración inicial.

```
firepower#
Cisco FTD: CMD=-start, CSP-ID=cisco-ftd.6.2.1.341__ftd_001_JMX2131Y1Q1107B2H1, FLAG=""
Device type is FPR-2110. (77/A)
Cisco FTD starting ...
Registering to process manager ...
Cisco FTD started successfully.
Cisco FTD initializing ...
Updating /ngfw/etc/sf/arc.conf ...
Deleting previous CGroup Configuration ...
Initializing Threat Defense ...           [ OK ]
Starting system log daemon...             [ OK ]
.
...
.
Cisco FTD initialization finished successfully.
```

Una vez en este punto, desde la consola FXOS se realiza la conexión al FTD y se acepta el EULA.

Tras lo cual se preguntará por la nueva contraseña y los datos iniciales de direccionamiento IP, nombre de host y DNS.

```

firepower# connect ftd
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
END USER LICENSE AGREEMENT

IMPORTANT: PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY. IT IS VERY
IMPORTANT THAT YOU CHECK THAT YOU ARE PURCHASING CISCO SOFTWARE OR EQUIPMENT
.
...
.
Please enter 'YES' or press <ENTER> to AGREE to the EULA: yes

System initialization in progress. Please stand by.
You must change the password for 'admin' to continue.
Enter new password:
Confirm new password:
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]: y
Do you want to configure IPv6? (y/n) [n]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]: manual
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.1
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.0
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.254
Enter a fully qualified hostname for this system [firepower]: fp1.test.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]: 8.8.8.8
Enter a comma-separated list of search domains or 'none' []: test.com
If your networking information has changed, you will need to reconnect.
Setting DNS servers: 8.8.8.8
Setting DNS domains:test.com
Setting hostname as fp1.test.com
DCHP Server Disabled
Setting static IPv4: 10.10.10.1 netmask: 255.255.255.0 gateway: 10.10.10.254 on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 6 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]:

```

En este punto, se debe optar entre gestionar el equipo a través del gestor interno, Firepower Device Manager (FDM), o hacerlo a través de un gestor externo, Firepower Management Center (FMC).

En el caso de optar por usar el gestor interno (FDM), la configuración inicial terminará tras habilitarlo y se podrá conectar físicamente a la red de Gestión y acceder al gestor mediante HTTPS a la dirección IP configurada.

```

Manage the device locally? (yes/no) [yes]: yes
Configuring firewall mode to routed

Update policy deployment information
- add device configuration
Successfully performed firstboot initial configuration steps for Firepower Device Manager for Firepower Threat Defense.

>

```

En el siguiente paso se debe decidir si se quiere que el funcionamiento del cortafuegos sea en modo rutado o modo transparente y ya se podrá establecer la

conexión al gestor FMC. No se recomienda que el gestor esté separado remotamente ni que se le aplique NAT. La clave de registro debe coincidir con la que se configurará posteriormente en el FMC al añadir el dispositivo en el gestor.

```

Manage the device locally? (yes/no) [yes]: no
DCHP Server Disabled
Configure firewall mode? (routed/transparent) [routed]: routed
Configuring firewall mode ...

Update policy deployment information
- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
> configure manager add 10.10.10.20 clave
Manager successfully configured.

```

Please make note of reg_key as this will be required while adding Device in FMC.

>

8.3 CONFIGURACIÓN INICIAL FIREPOWER 4100/9300

Los equipos FP 4100 y 9300 presentan una plataforma con doble gestión.

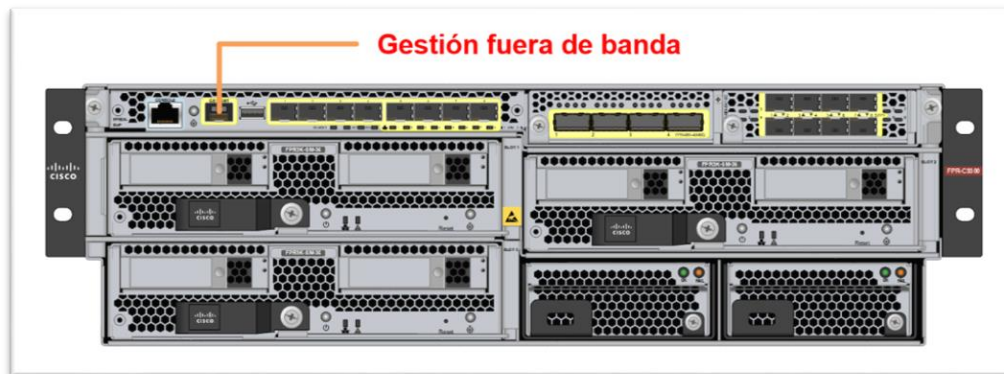
Por un lado, el sistema FXOS (Firepower eXtensible Operating System) gestiona el chasis, incluyendo las interfaces y la imagen o imágenes FTD/ASA que se desplegarán.

La configuración inicial, por tanto, inicializa solo el sistema FXOS.

Para la configuración inicial, se recomienda la conexión por consola RS232 9600bps, utilizando un cable de consola “Cisco” (rollover). En el encendido, el equipo realizará una serie de preguntas para configurarse. Tras la configuración se procederá a conectar el cable físicamente en el interfaz fuera de banda.



Conexión de la gestión fuera de banda Firepower 4100



Conexión de la gestión fuera de banda Firepower 9300

Se nos preguntará por la nueva contraseña, con recomendación de verificación de contraseña fuerte "strong password" y los datos iniciales de direccionamiento, nombre de host y DNS.

En esta configuración también se nos pregunta por los "IP block" para SSH y HTTPS. Estas son las direcciones IP autorizadas para gestionar el equipo, es decir, la del equipo o equipos de administración (administradores), no del gestor FMC. Se recomienda habilitar tanto SSH como HTTPS.

```
!! Rommon image verified successfully !!

Cisco System ROMMON, Version 1.0.10, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Mon 11/30/2015 15:23:18.60 by builder
Current image running: Boot ROM0
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR-4150-SUP with 8192 Mbytes of main memory
MAC Address: 38:90:a5:f2:34:cc

find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.4.61.131.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.4.61.131.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
Use SPACE to begin boot immediately.

Attempt autoboot: "boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.4.61.131.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.4.61.131.SPA"
!! Kickstart Image verified successfully !!
.
...
.
System is coming up ... Please wait ...
nohup: appending output to 'nohup.out'

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the FXOS Supervisor is performed through these steps.

Type Ctrl-C at any time for more options or to abort configuration
and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.

You have chosen to setup a new Security Appliance.
Continue? (yes/no): yes

Enforce strong password? (yes/no) [y]: y

Enter the password for "admin":
Confirm the password for "admin":
Enter the system name: fp4150-1
Supervisor Mgmt IP address : 10.10.10.1
Supervisor Mgmt IPv4 netmask : 255.255.255.0
IPv4 address of the default gateway : 10.10.10.254
Do you want to configure IP block for ssh access? (yes/no) [y]: y
SSH IP block address : 10.10.7.0
SSH IPv4 block netmask : 255.255.255.0
Do you want to configure IP block for https access? (yes/no) [y]: y
HTTPS IP block address : 10.10.7.0
HTTPS IPv4 block netmask : 255.255.255.0
Configure the DNS Server IP address? (yes/no) [n]: y
```

```
DNS IP address : 8.8.8.8
Configure the default domain name? (yes/no) [n]: y
Default domain name : test.com

Following configurations will be applied:

Switch Fabric=A
System Name=fp4150-1
Enforced Strong Password=no
Supervisor Mgmt IP Address=10.124.241.44
Supervisor Mgmt IP Netmask=255.255.255.0
Default Gateway=10.124.241.200
SSH Access Configured=yes
  SSH IP Address=10.124.241.0
  SSH IP Netmask=255.255.255.0
HTTPS Access Configured=yes
  HTTPS IP Address=10.124.241.0
  HTTPS IP Netmask=255.255.255.0
DNS Server=8.8.8.8
Domain Name=test.com

Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait... Configuration file - Ok
.....

Cisco FPR Series Security Appliance
fp4150-1 login:
```

Tras la configuración inicial del sistema FXOS, se debe proceder al login en FXOS y realizar la configuración e instalación de la imagen o imágenes FTD, según el diseño deseado.

8.4 CONFIGURACIÓN INICIAL FIREPOWER NGFW Virtual (NGFWv)

La opción de cortafuegos virtualizado Firepower permite su instalación en entornos ESXi (VMware) y KVM, así como en los entornos de nube de Microsoft Azure, Amazon AWS, Google GCP, Oracle OCI.

Dependiendo del despliegue y la infraestructura utilizada los rendimientos pueden variar. Consultar en la web de Cisco por las últimas versiones y su rendimiento aproximado dependiendo de la plataforma virtual/nube usada.

En esta guía vamos a cubrir la instalación en ESXi (VMware), sirviendo como base para el resto de plataformas.

Nota: los cortafuegos virtuales hacen reserva de toda su memoria en su instalación. Esto debe tenerse en cuenta en el correcto dimensionamiento del sistema de virtualización o nube.

8.4.1 INSTALACIÓN Y CONFIGURACIÓN CON VMWARE VCENTER/VSPHERE

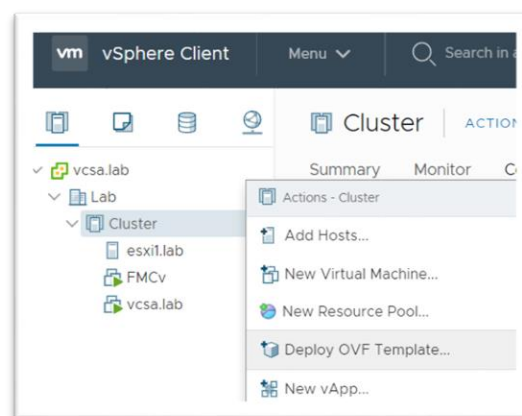
Con vSphere la instalación se hace utilizando el despliegue de OVF, que dispone de un asistente de configuración que realiza la configuración inicial a la vez que la instalación.

En este tipo de instalación se debe usar el fichero “VI”. Ejemplo: “Cisco_Firepower_Threat_Defense_Virtual-VI-7.0.0-94.ovf”.

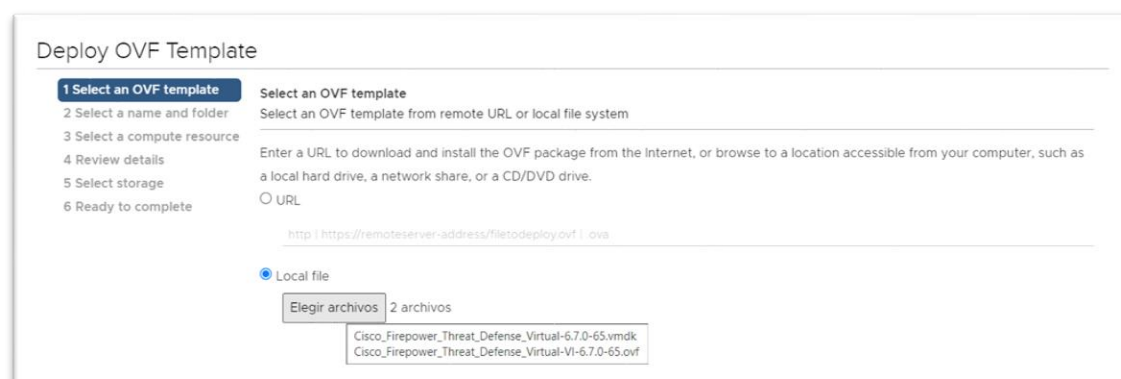
Dependiendo de la versión de VMWare usada los puntos o pantallas aquí expuestos pueden variar.

Se debe acceder al VCenter/VSphere y usar la opción “Deploy OVF template”.

Las imágenes a continuación usan como referencia la versión 6.7.0 pero el proceso sería idéntico para la imagen de la versión 7.0 mencionada más arriba.



Seleccionando ficheros locales, se deben seleccionar los 2 ficheros, tanto el .ovf como el .vmdk.



Seleccionar el Datacenter y asignar el nombre de la máquina virtual que recibirá el cortafuegos en el sistema. Luego el Cluster o Host donde debe ser ejecutada.

Deploy OVF Template

- ✓ 1 Select an OVF template
- 2 Select a name and folder**
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a name and folder
Specify a unique name and target location

Virtual machine name:

Select a location for the virtual machine.

- ▼ vcsa.lab
 - > Lab

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- 3 Select a compute resource**
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a compute resource
Select the destination compute resource for this operation

- ▼ Lab
 - > Cluster

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

Tras revisar los detalles se acepta también la licencia.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details**
- 5 License agreements
- 6 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Review details
Verify the template details.

⚠ The OVF package contains advanced configuration options, which might pose a security risk. Review the advanced configuration options below. Click next to accept the advanced configuration options.

Publisher	No certificate present
Product	Cisco FTDv
Version	6.7.0
Vendor	Cisco Systems, Inc.
Description	Cisco FTDv Cisco Systems, Inc. 170 West Tasman Dr San Jose, CA 95134 USA
Download size	1.1 GB
Size on disk	Less than 1 MB (thin provisioned) 48.5 GB (thick provisioned)
Extra configuration	numa.vcpu.preferHT = TRUE monitor_control.pseudo_perfctr = TRUE

El siguiente paso es importante, ya que se debe seleccionar cuál de los 3 tipos de cortafuegos virtual se desea instalar. Esto depende de los requisitos de rendimiento que se deseen.

Seleccionar el almacenamiento. Se recomienda el uso de Thick Provision para mejorar el rendimiento.

Name	Capacity	Provisioned	Free	Type	Cluster
datastore1	1.81 TB	573.31 GB	1.25 TB	VMFS 6	
Datastore2	1.82 TB	1.44 GB	1.82 TB	VMFS 6	

El cortafuegos virtual dispone de hasta 8 interfaces de red para datos y 1 para gestión fuera de banda.

Se deben seleccionar las redes (VLANs) donde se conectarán los interfaces, asignándoles los port-groups de VMware.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- 8 Select networks**
- 9 Customize template
- 10 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	Destination Network
GigabitEthernet0-0	VM Network
Management0-0	Vlan4010
GigabitEthernet0-1	VM Network
GigabitEthernet0-2	VM Network
GigabitEthernet0-3	VM Network
GigabitEthernet0-4	VM Network
GigabitEthernet0-5	VM Network
Diagnostic	VM Network
GigabitEthernet0-6	VM Network
GigabitEthernet0-7	VM Network

10 items

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

CANCEL BACK NEXT

En la última parte se muestra un formulario para rellenar los datos de inicio del cortafuegos, contraseña, hostname, direccionamiento IP, modo de funcionamiento del cortafuegos y registro con el gestor.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- ✓ 6 Configuration
- ✓ 7 Select storage
- ✓ 8 Select networks
- 9 Customize template**
- 10 Ready to complete

13. Management IPv6 Gateway Management IPv6 Gateway

3. Management 1 settings

Enable Local Manager Firewall mode will be changed to routed and local manager will be enabled.
No

4. Firewall Mode 1 settings

Firewall Mode Initial Firewall Mode
routed

5. Registration 3 settings

01. Manager Managing Firepower Management Center

02. Registration Key Registration Key

03. NAT ID NAT ID

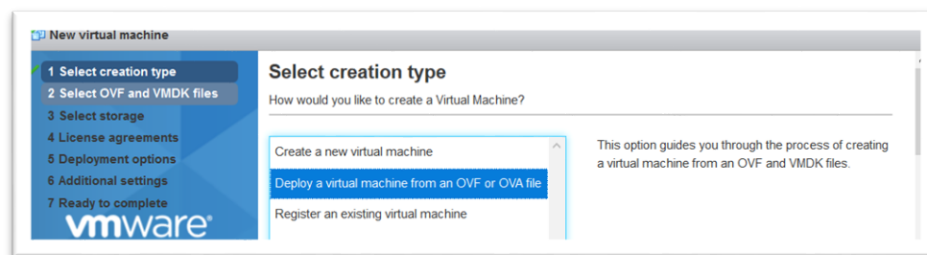
CANCEL BACK NEXT

Una vez instalada la máquina virtual, se puede arrancar y conectar directamente al gestor de los cortafuegos. Consultar el apartado específico de esta guía.

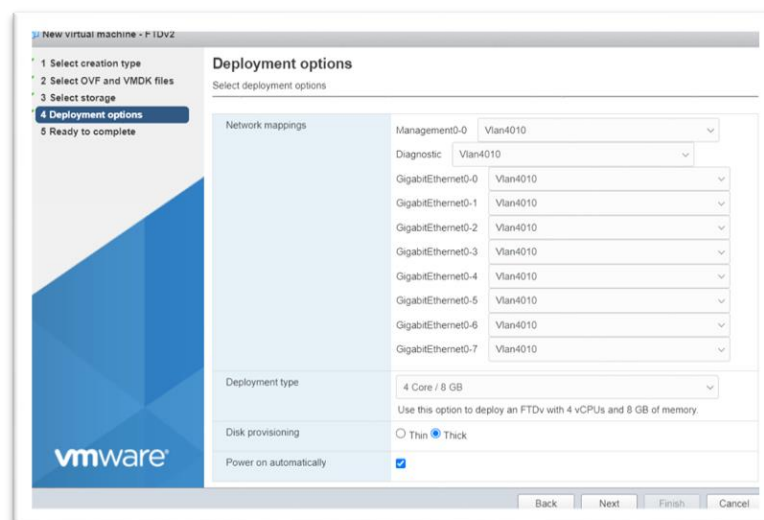
8.4.2 INSTALACIÓN Y CONFIGURACIÓN SIN VMWARE VCENTER/VSPHERE

Esta instalación se realiza en 2 pasos. El primero consiste en la creación de la máquina virtual a través del OVF con nombre “ESXi”. Ejemplo: “Cisco_Firepower_Threat_Defense_Virtual-ESXi-7.0.0-94.ovf”.

En la pantalla de selección de ficheros (Click to select files or drag/drop), se deben especificar los 2 ficheros, tanto el .ovf como el .vmdk.

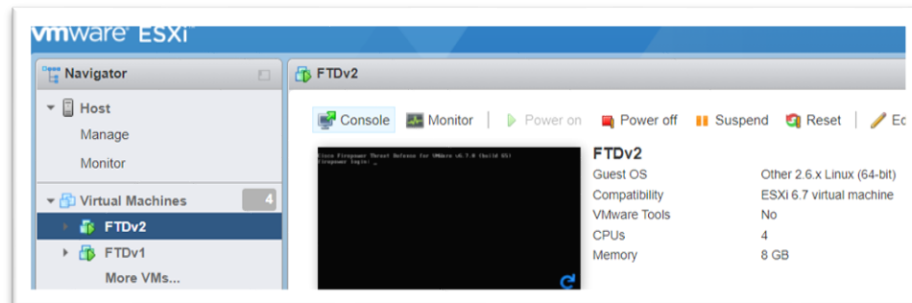


Se selecciona el almacenamiento y en la siguiente pantalla se asignan los interfaces de red a los port-groups del hipervisor, así como el tipo de cortafuegos a instalar, dependiendo de los requisitos de dimensionamiento deseados. Se recomienda utilizar Thick provisioning para mejorar el rendimiento.

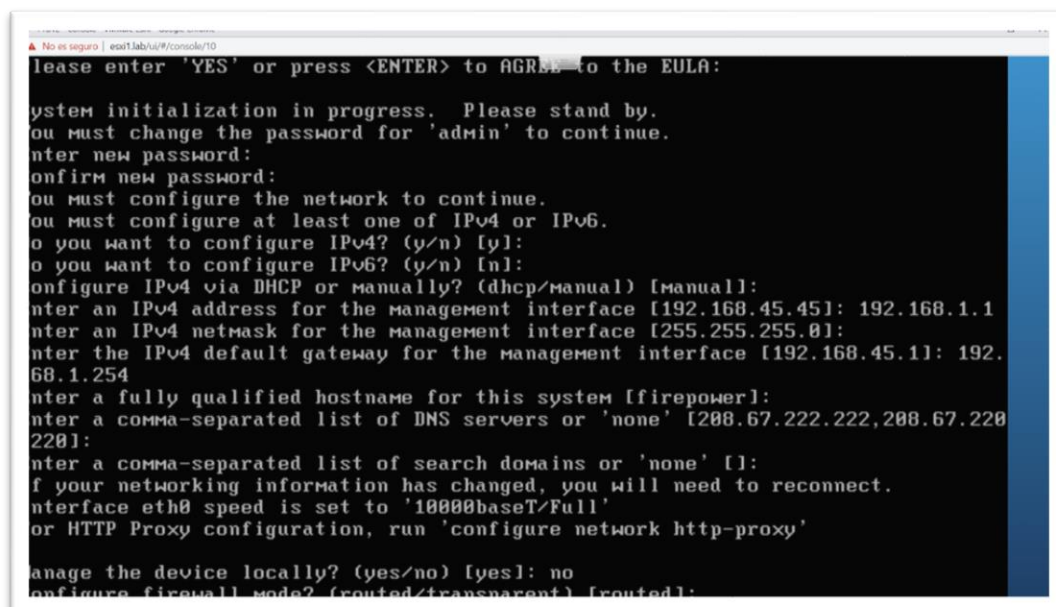
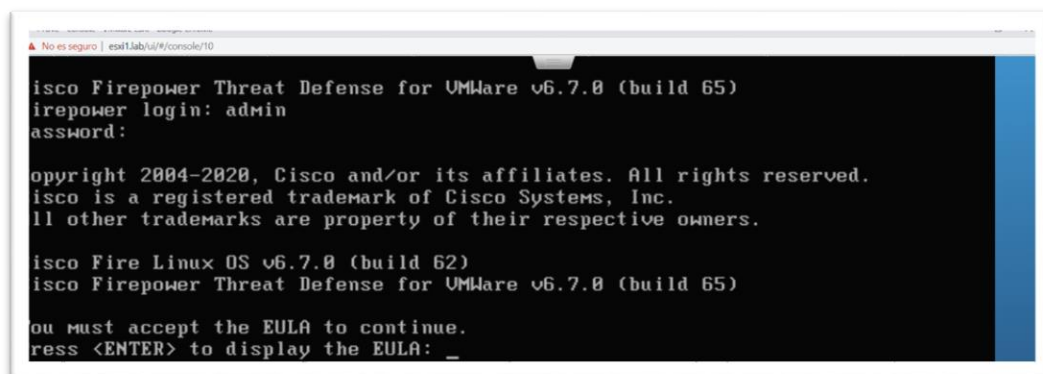


Una vez revisadas las opciones comenzará la instalación de la máquina virtual del cortafuegos. Esto concluye el primer paso de la instalación.

El segundo paso es la configuración del dispositivo. Para ello se accede a la consola de la máquina virtual.



El login es: admin y la contraseña: Admin123. Se debe aceptar la licencia (EULA) y luego configurar los parámetros de red y el modo y la gestión del cortafuegos.



```

Setting DNS servers: 8.8.8.8
Setting DNS domains:test.com
Setting hostname as fp1.test.com
DCHP Server Disabled
Setting static IPv4: 10.10.10.1 netmask: 255.255.255.0 gateway: 10.10.10.254 on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 6 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]:

```

En este punto, se debe optar entre gestionar el equipo a través del gestor interno, Firepower Device Manager (FDM), o hacerlo a través de un gestor externo, Firepower Management Center (FMC).

En el caso de optar por usar el gestor interno (FDM), la configuración inicial terminará tras habilitarlo. Se podrá acceder al gestor mediante HTTPS a la dirección IP configurada.

```

Manage the device locally? (yes/no) [yes]: yes
Configuring firewall mode to routed

Update policy deployment information
- add device configuration
Successfully performed firstboot initial configuration steps for Firepower Device Manager for Firepower Threat Defense.

>

```

En el caso de utilizar un gestor externo (FMC), se debe establecer la conexión al gestor FMC. No se recomienda que el gestor esté separado remotamente ni que se le aplique NAT. La clave de registro debe coincidir con la que se configurará posteriormente en el FMC al añadir el dispositivo en el gestor.

```

Manage the device locally? (yes/no) [yes]: no
DCHP Server Disabled
Configure firewall mode? (routed/transparent) [routed]: routed
Configuring firewall mode ...

Update policy deployment information
- add device configuration
- add network discovery
- add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required. In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration

```

```
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

Later, using the web interface on the Firepower Management Center, you must use the same registration key and, if necessary, the same NAT ID when you add this sensor to the Firepower Management Center.

```
> configure manager add 10.10.10.20 clave
```

Manager successfully configured.

Please make note of reg_key as this will be required while adding Device in FMC.

```
>
```

9. MODOS DE FUNCIONAMIENTO DE CORTAFUEGOS FIREPOWER

Existen 2 modos diferentes en que los cortafuegos Firepower FTD pueden operar, modo rutado y modo transparente. La recomendación es usar el modo rutado.

El modo de funcionamiento normalmente es seleccionado en el momento de la instalación inicial.

Si en algún momento posterior se requiere el cambio de modo de operación, es necesario des-registrar el equipo del gestor FMC, acceder por CLI (consola o SSH) y cambiar su modo, lo que borrará toda su configuración de producción, aunque no de gestión. Tras esto, se debe volver a registrar el cortafuegos en el gestor FMC.

```
configure firewall [routed|transparent]
```

Ejemplo:

```
> configure firewall transparent
```

This will destroy the current interface configurations, are you sure that you want to proceed? [y/N] **y**

The firewall mode was changed successfully.

Recordar volver a registrar en FMC:

```
'configure manager add [hostname | ip address ] [registration key ]'
```

9.1 MODO TRANSPARENTE

En este modo el cortafuegos no aparece como salto (hop) en la red y su funcionamiento está basado en reenvío de paquetes a nivel 2 OSI, mediante bridging.

Se crean “Bridge Groups” (BG) que agrupan interfaces que trabajan en el mismo rango de direccionamiento IP. Cada BG requiere una IP asignada del rango en un BVI (Bridge Virtual Interface). Cada BG requiere un BVI con dirección IP, pero esa dirección IP no hace routing/forwarding.

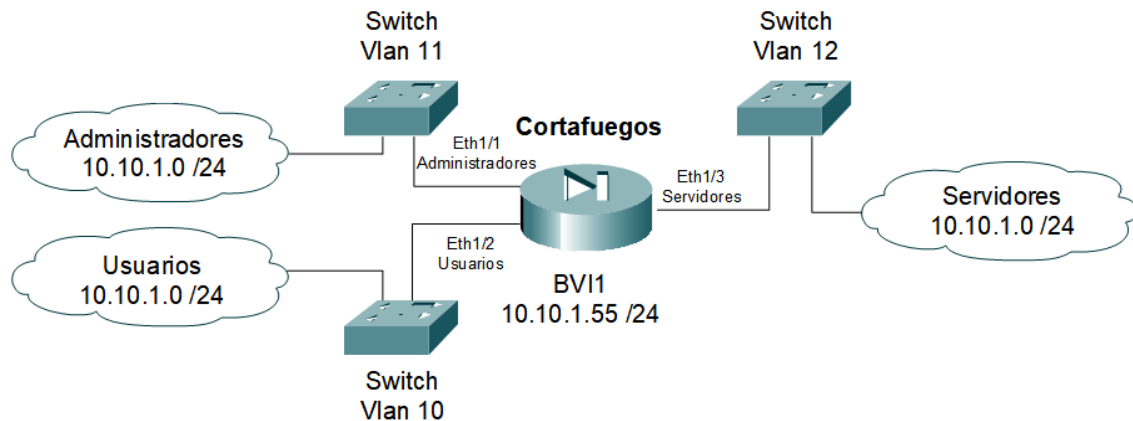


Diagrama de cortafuegos en modo transparente

Como se puede observar en el diagrama, las ventajas de este modo son:

- No es necesario realizar cambios de direcciones IP para la integración del cortafuegos. Especialmente importante en servidores.
- El cortafuegos se “esconde” y no es aparente en la red.
- Los protocolos de routing pueden formar adyacencias a través del cortafuegos sin problemas.
- El multicast puede atravesar el cortafuegos sin configuración adicional.
- Protocolos como HSRP, VRRP, GLBP pueden atravesar el cortafuegos.
- Tráfico no IP puede ser permitido (BPDUs, IPX, MPLS).

Las conexiones del cortafuegos con los diferentes segmentos de red, se pueden realizar mediante conmutadores físicamente distintos, o bien mediante el mismo conmutador utilizando diferentes VLAN.

El modo transparente tiene las siguientes características no soportadas:

- DHCP relay
Sin embargo, los paquetes DHCP “normales” Request, Offer, pueden atravesar el cortafuegos.
- VPN
No se pueden establecer VPN Lan-2-Lan ni de acceso remoto.
- QoS
La funcionalidad de Calidades de servicio no está disponible.
- Protocolos de routing (RIP, BGP, OSPF)
No pueden ser habilitados, sin embargo, los protocolos pueden atravesar el cortafuegos.
- Routing multicast
El cortafuegos no puede realizar routing, pero el protocolo puede atravesar el cortafuegos en el bridging.

- **Rutado**
No se pueden configurar interfaces adicionales de nivel 3, con IP, en este modo y enrutarlos.

9.2 MODO RUTADO

Este es el modo normal de funcionamiento y es el modo recomendado.

En este modo, el cortafuegos realiza el reenvío de paquetes a nivel 3 OSI, mediante tablas de rutado y la IP del cortafuegos, en la interfaz correspondiente, es la ruta que usan los equipos para comunicarse en la red.

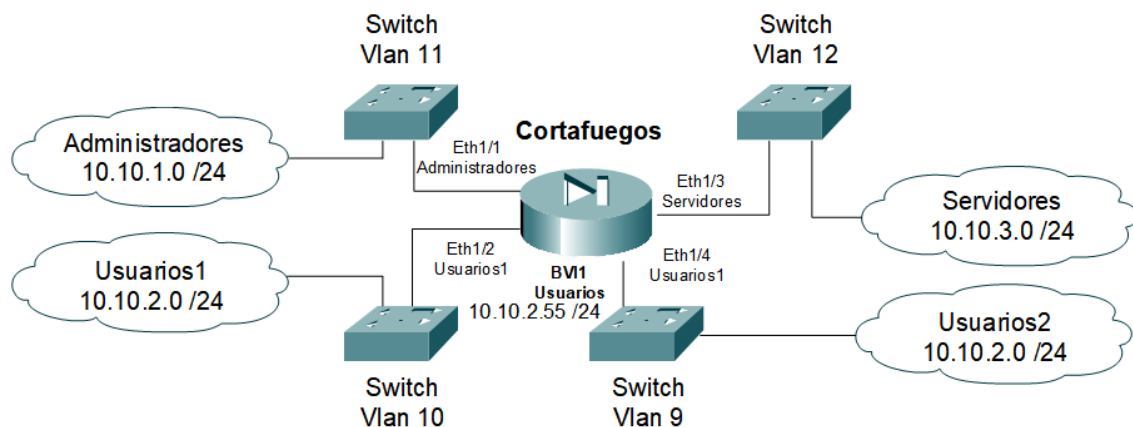


Diagrama de cortafuegos en modo rutado

Cada interfaz tiene su propio direccionamiento IP y el funcionamiento es muy similar al de un router.

En modo rutado todas las funciones están disponibles para las interfaces en modo rutado.

Pero, además, en equipos Firepower 4100 y 9300, en modo rutado, se pueden utilizar también BG que funcionan realizando bridging igual que en el modo transparente. En los equipos Firepower 1000/2100 no es posible utilizarlos.

Estos BG pueden funcionar en modo aislado, como en el modo transparente, o también realizando bridging y rutado concurrentemente, rutado a través de la IP del BVI, que se comunica con el resto de interfaces de rutado del equipo. Es posible seleccionar si el rutado en el BG está habilitado o no, mediante el Name, si se asigna Name el BVI entra en el rutado.

En el diagrama del modo rutado se visualiza un BG creado con BVI1 uniendo los 2 segmentos de la red de usuarios.

Las restricciones de estos BG son las mismas que en el modo transparente, con las siguientes restricciones añadidas:

- No se pueden utilizar Etherchannels (agregación de puertos) como miembros del BG.
- Los BG no están soportados en un clúster.

Las ventajas del modo rutado incluyen una mejor resolución de problemas al disponer de herramientas de depuración de nivel 3, mucho más amplias que las de nivel 2.

Por todo esto el modo rutado es el modo de funcionamiento recomendado.

10. FIREPOWER CHASSIS MANAGER - FXOS

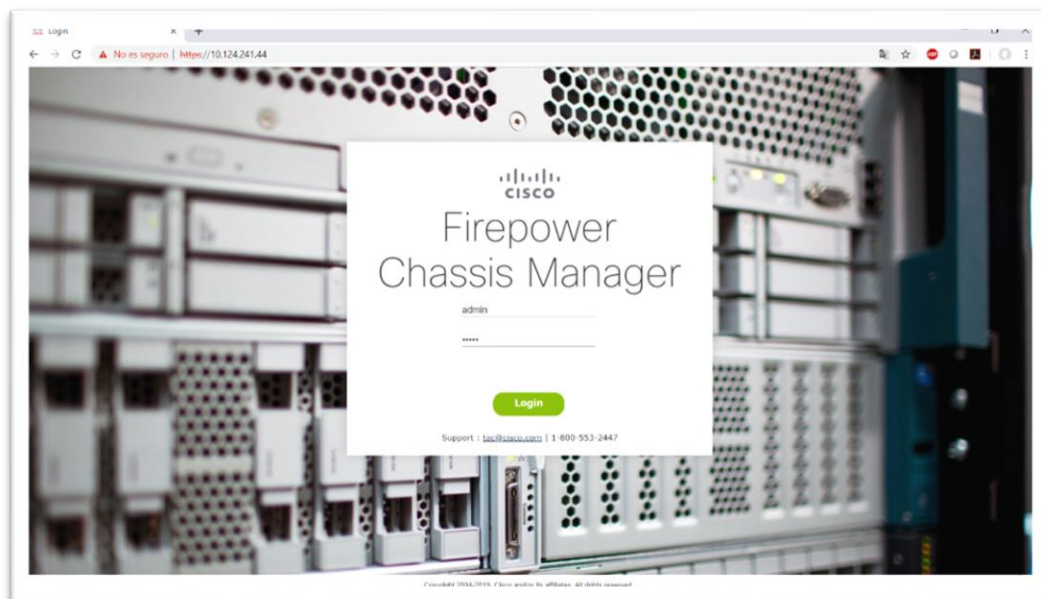
La gestión del chasis de los equipos Firepower 4100 y 9300 se realiza a través del Firepower Chassis Manager, también conocido como sistema FXOS.

La recomendación es utilizar el interfaz web de este sistema para la configuración, accediendo al CLI mediante SSH solo cuando sea necesario porque la funcionalidad requerida no se encuentra implementada en el web.

Las credenciales de autenticación son las introducidas en la configuración inicial del equipo Firepower.

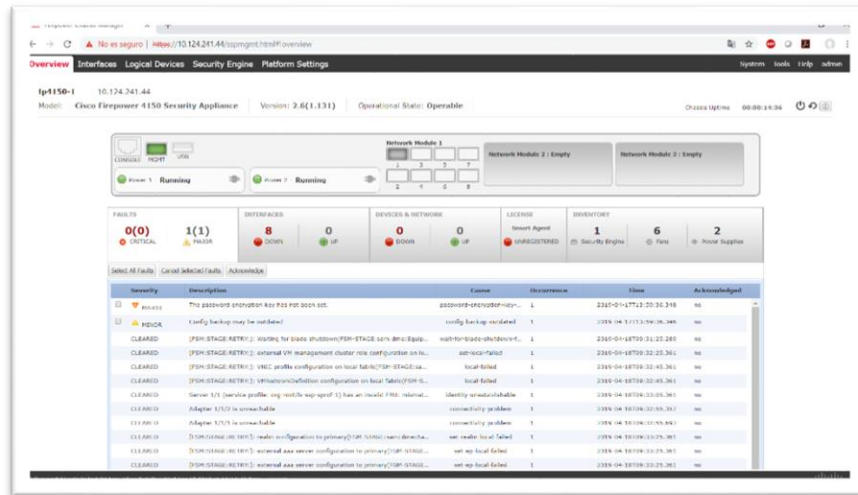
Cisco recomienda el uso del navegador Chrome para una óptima funcionalidad.

Dentro de este apartado vamos a indicar, principalmente, los puntos necesarios a configurar y revisar desde el punto de vista de la seguridad.



Pantalla de login del Firepower Chassis Manager (FXOS)

La pantalla inicial del FP Chassis Manager, Overview muestra el estado del equipo y las “Faults”, que son defectos detectados que deben ser atendidos. Los “Faults” en estado CLEARED significan que ya han sido resueltos y es común verlos en los rearranques del sistema. Los “Faults” INFO son de escasa relevancia.



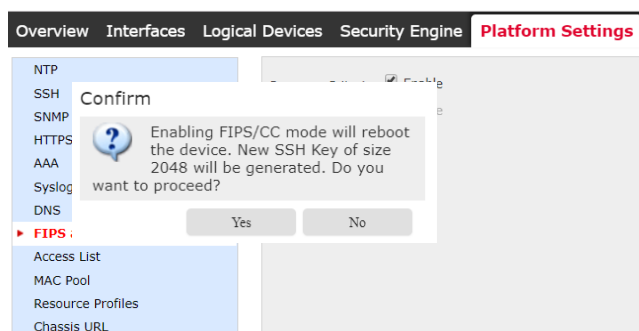
Pantalla de overview del Firepower Chassis Manager (FXOS)

10.1 MODO COMMON CRITERIA

Como paso inicial, se necesita activar el modo Common Criteria del Chassis Manager. Lo cual es fundamental para que la instalación cumpla con los requisitos de Common Criteria.

Nota: Sin este ajuste activado el equipo estará funcionando sin cumplir con Common Criteria. Debe activarse este modo.

Este ajuste modifica parámetros internos de cifrado, timeouts, longitud de claves y funcionamiento interno del dispositivo. Una vez activado se reiniciará el dispositivo.



10.2 SINCRONIZACIÓN DE HORA (NTP)

En un cortafuegos, es de vital importancia que la fecha y hora sea la correcta, tanto por cuestiones de funcionalidad como de visualización de conexiones en los logs, eventos ocurridos en un momento determinado, etc.

La sincronización se realiza a través de protocolo NTP (Network Time Protocol), desde la IP de gestión del FP Chassis Manager.

Primero se debe configurar correctamente la zona horaria (Time Zone) y posteriormente el servidor o servidores NTP a utilizar.

The screenshot shows the 'Platform Settings' tab with the 'Current Time' sub-tab selected. The 'Current Time' section displays the following information:

- Device Date: 04/18/2019
- Device Time: 10:01:26 AM
- Time Zone: Europe/Madrid (selected from a dropdown menu)
- NTP Status: Not configured

At the bottom of the window are 'Save' and 'Cancel' buttons.

The screenshot shows the 'Set Time Source' configuration window. It has two main sections:

- Set Time Manually:** Includes fields for Date (04/18/2019), Time (11:57 AM), and a 'Get System Time' button.
- Set Time Source:** Includes radio buttons for 'Set Time Manually' and 'Use NTP Server' (which is selected).

Below the 'Use NTP Server' option is a checkbox for 'NTP Server Authentication' with an 'Enable' label. To the right, there is an 'Add NTP Server' dialog box with fields for 'NTP Server *' (10.10.10.101), 'Authentication Key', and 'Authentication Value', along with 'Add' and 'Cancel' buttons.

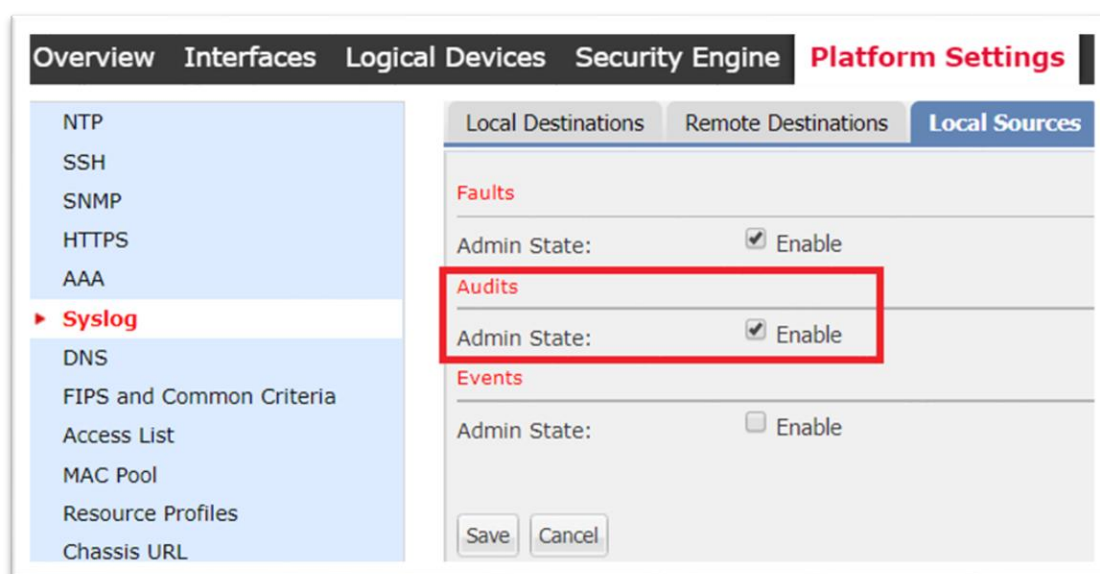
At the bottom of the main window is a table with columns 'NTP Server', 'Server Status', and 'Actions'. Below the table is a note: 'Use same settings on Firepower Management Center managing this application in case you are running a Firepower Threat Defense Device.' At the very bottom are 'Save' and 'Cancel' buttons.

10.3 REGISTROS DE AUDITORÍA – AUDIT LOG

Los registros, o logs, de auditoría, responden a las preguntas de seguridad, ¿Quién? ¿Cuándo? ¿Qué? ¿Cómo?

Son registros de accesos y cambios realizados en una aplicación, en este caso el FXOS gestor del chasis, donde se muestra el día y hora, el usuario, la acción concreta realizada y datos asociados. En el caso de un incidente de seguridad los registros de auditoría son vitales para un adecuado análisis forense. También son muy útiles si se necesita recordar que cambio se realizó y poder volver a revertirlo u obtener algún entendimiento sobre ello.

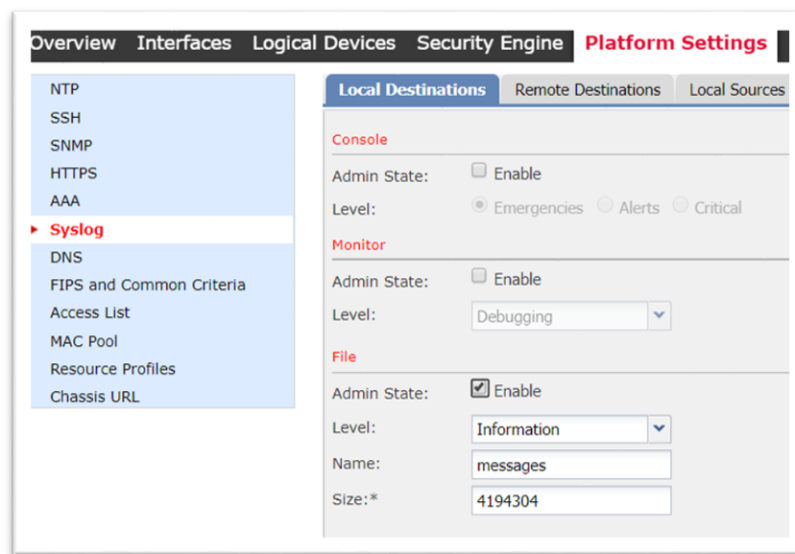
En FXOS los registros de auditoría están deshabilitados por defecto. Se recomienda su habilitación y su envío a un syslog externo.



Para que se registren los logs de auditoría, el nivel debe ser “Information”. Se recomienda filtrar los mensajes en el servidor syslog por “%FPRM-6-AUDIT” si solo se desean grabar los mensajes de auditoría.



Alternativamente, se puede especificar un fichero local para el registro de mensajes.



El acceso a los datos del fichero no se puede realizar vía web, sino por CLI, accediendo a la conexión directa al sistema FXOS.

```
Cisco FPR Series Security Appliance
Successful login attempts for user 'admin' : 6
.
...
.
fp4150-1# connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2019, Cisco Systems, Inc. All rights reserved.
.
...
.
fp4150-1(fxos)# show logging logfile
2019 Apr 26 18:15:57 2019 Apr 26 18:15:56 fp4150-1 %BC01_MEZZ0101_mcp.vnic[122]-6- +0x1000 1
0x12a600c8 0x0004 r---
2019 Apr 26 18:15:57 2019 Apr 26 18:15:56 fp4150-1 %BC01_MEZZ0102_mcp.vnic[122]-6- wq: [21] (n=1)
2019 Apr 26 18:15:57 2019 Apr 26 18:15:56 fp4150-1 %BC01_MEZZ0101_mcp.vnic[122]-6- vnic_resource map
magic 0x766e6963 version 0
.
...
.
2019 Apr 26 19:48:22 fp4150-1 %FPRM-6-AUDIT: [session][internal][creation][internal][75182][sys/user-
ext/web-login-admin-web_63474_A][id:web_63474_A, name:admin, policyOwner:local][] Web A: local user
admin logged in from 10.10.10.7
...
2019 Apr 26 19:57:08 fp4150-1 %FPRM-6-AUDIT: [admin][admin][modification][internal][75198][aaa-log][aaa-
log][] switch A: cmd: connect fxos , logged in from 10.10.10.7 on term /dev/pts/0: Local mgmt command
executed
...
2019 Apr 26 19:59:25 fp4150-1 %FPRM-6-AUDIT: [admin][admin][modification][web_63474_A][75202][sys/svc-
ext/syslog/file][adminState(Old:enabled, New:disabled)][] Syslog File attributes modified
...
```

```

2019 Apr 26 19:59:49 fp4150-1 %FPRM-6-AUDIT: [admin][admin][deletion][web_63474_A][75259][sys/svc-
ext/dns-svc/dns-8.8.8.8][sys/svc-ext/dns-svc/dns-8.8.8.8][ ] DNS server 8.8.8.8 deleted
....
2019 Apr 26 20:00:03 fp4150-1 %FPRM-6-AUDIT: [admin][admin][creation][web_63474_A][75288][sys/svc-
ext/dns-svc/dns-8.8.8.8][name:8.8.8.8][ ] DNS server 8.8.8.8 created

```

Para que se registren los logs de auditoría, el nivel debe ser “Information”. Se recomienda filtrar los mensajes en el servidor syslog por “%FPRM-6-AUDIT” si solo se desean grabar los mensajes específicos de auditoría.

10.4 INSTALACIÓN DE CERTIFICADO HTTPS

En la configuración inicial del dispositivo se genera un certificado auto-firmado para la conexión segura mediante protocolo HTTPS. Este certificado debe ser sustituido por uno de confianza (trusted) con una entidad de certificación (CA) de confianza.

Para generar la nueva llave privada y la petición de certificado es necesario conectarse por CLI (SSH) al sistema FXOS. Se recomienda incluir en el campo SAN (Subject Alternative Name), tanto el hostname completo como la dirección IP, para poder acceder tanto por nombre como directamente por IP desde el navegador.

```

fp4150-1# scope security
fp4150-1 /security # create keyring FP_cert
fp4150-1 /security/keyring* # set modulus mod2048
fp4150-1 /security/keyring* # commit-buffer

fp4150-1 /security/keyring # create certreq
fp4150-1 /security/keyring/certreq* # set country ES
fp4150-1 /security/keyring/certreq* # set state "Lab State"
fp4150-1 /security/keyring/certreq* # set locality "Lab Loc"
fp4150-1 /security/keyring/certreq* # set org-name "CCN CERT"
fp4150-1 /security/keyring/certreq* # set org-unit-name LAB
fp4150-1 /security/keyring/certreq* # set subject-name fp4150-1.test.com
fp4150-1 /security/keyring/certreq* # set dns fp4150-1.test.com
fp4150-1 /security/keyring/certreq* # set ip 10.10.1.44
fp4150-1 /security/keyring/certreq* # commit-buffer

```

Una vez creada la solicitud, la visualización lo mostrará en formato portable PEM que se puede copiar y pegar como solicitud para llevarlo a la autoridad certificadora que generará el certificado.

```

fp4150-1 /security/keyring/certreq # show certreq
Certificate request subject name: fp4150-1.test.com
Certificate request ip address: 10.10.1.44
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:

```

```

Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: ES
State, province or county (full name): Lab State
Locality name (eg, city): Lab Loc
Organisation name (eg, company): CCN CERT
Organisational Unit Name (eg, section): LAB
DNS name (subject alternative name): fp4150-1.test.com
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIC6jCCADICAQAwwDELMakGA1UEBhMCRVMxExAQBgNVBAgMCUxhYiBTdGF0ZTEQ
MA4GA1UEBwwHTGFilExvYzERMA8GA1UECgwIQ0NOIENFUlQxDDAKBgNVBAAsMA0xB
QjEaMBGGA1UEAwwRZnA0MTUwLTUudGVzdC5jb20wggEiMA0GCSqGSIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCwT+DyGOu/JC75UI3ZDakAshIAj5WTITzIowsyRWn89UNm
v9qb9JAditrnvj92jORIXfcDw+y8sTgoBqWaOAgD7EQfP64nviogmv1yy2MSL5aD
qa02pFXlqCMY3s+6Km+CB2rq+ERMPzY+X1MAHc5R+Z4o5EL4FO1UA/A5SscuXsI8
Q1uDJSb5uwBfjXo8C7PsIZSpisd2lQaq6cBY2/DBWY7Lg+cuKocIM6+f3Ys5F+p
qRU5c6k9QPX9rmSH+fcy8AEZMDLNP3vJ1RG1EBvLZiVtWnl35UffQ28nSoXQPgJ
TijEnM5gqqNsYkhyICp5UPHYp1W2JUxhhrqkrP+ZAgMBAAAGNTAzBgkqhkiG9w0B
CQ4xJjAKMCIgA1UdEQQbMBMCEWZwNDE1MC0xLnRlc3QuY29thwQKCgEsMA0GCSqG
SIb3DQEBCwUAA4IBAQBGLG27C0mfyOt8aRqD/qyEicWe35kE2b87AVMtOlptXfio
MgEeGLRPaaSiHjTOS2v5J1gwEMcQDqh5JCg10CjB8y/fwlqZDxwhwmskGsLgKQK
02oELod6j789pvC/DgLRly0/5q0ilQh9VY7PKds7Jl/X/6Dh+y9DS9Btygxe4qHt
9NeVZcrZjLmOAKW3ioSbEw9USmwDNzmOB5+mbh5VsPUopqS1WzVVOFjkzKcCiLy
maJudfj0Tf7YSwkaXtVUISOyjGtvzejK8U2UZgPRPYpToOhoJ4YTLIOLIJdL4
fQt0ENV7TLURv26icncXKCKEihQfT8P/68pgfty
-----END CERTIFICATE REQUEST-----

```

Antes de importar el certificado firmado por la entidad certificadora que usemos, deberemos importar el certificado de esa entidad, tanto intermedio, si lo hubiera, como root. Eso se realiza a través de un punto de confianza (trustpoint).

En este ejemplo vamos a importar el root e intermedio de un servicio de certificados de Internet, Comodo. Normalmente utilizaremos una entidad certificadora interna, no de Internet. Pero el proceso es el mismo.

```

fp4150-1 /security/keyring # top
fp4150-1# scope security
fp4150-1 /security # create trustpoint Comodo_chain
fp4150-1 /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIIEpjCCA46gAwIBAgIQRurwlgVMxeP6Zepun0LGZDANBgkqhkiG9w0BAQUFADBv
>MQswCQYDVQQGEwJTRTEUMBIGA1UEChMLQWRkVHJ1c3QgQUlxdjAKBgNVBAStHUFk
>ZFRydXN0IEV4dGVybmlFRUUCBOZXR3b3JrMStlWlAYDVQQDEElBZGRUcnVzdCBF
>eHRlcm5hbCBDQSB5b290MB4XDTE1MDYwNzA4MDkxMFoXDTEwMDUzMDEwNDgzOFow
>gZMx+CzAJBgNVBAYTAiVTMQswCQYDVQQIEwJVVDEEXMBUGA1UEBxMOU2FsdCBMYWtl
>IENpdHkxHjAcBgNVBAoTFVRoZSBVU0VSFjVU1QgTmV0d29yazEhMB8GA1UECzMV
>aHR0cDovL3d551c2VydhJ1c3QuY29tMRswGQYDVQQDEElVVE4gLSBEQVRBQ29y

>cCBTR0MwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCdf7lgQoitvVcSO
>vy5GCefgCA8uK3oTIBu99raAjmUFkwAevK/iD44ZDRJH7Kyto/oucPjebvtWQhWe
>Llzvi94huQV2JxkPT9bDnLS+IBlj8qYRCutTSJy+8ik7FugaoEymyfyQYWWjAcPJT

```

```

>AMBeUIKIVm82+UrgRlagTU7WR25JSstn16bEBbmOHvT8/83nNuCcBWyyMyIVOLTg
>zBfAssD0/jl/KSqVe9jyp04PVHyhDYCzCQPB/1zdXpo+vK68R4pqrnHKH7EquF9C
>BQvsRjDRcgV6VZt9e/feL5hurKlrgRMvKisaRWXve/rtly/NfjUw9EoDIw6n3AY
>MyB3xKKvAgMBAAGggEXMIIBEzAfBgNVHSMEGDAWgBStvZh6NLQm9/rEJITvA73g
>JMtUGjAdBgNVHQ4EFgQUUzLRs89/+uDxoF2FTpLSnkUdtE8wDgYDVR0PAQH/BAQD
>AgEGMA8GA1UdEwEB/wQFMAMBAf8wIAAYDVR0IBBkwFwYKKwYBBAGCNwoDAwYJYIZI
>AYb4QgQBMBEGA1UdIAQKMAgBgYEVR0gADB7BgNVHR8EdDBYMDigNqA0hjJodHRw
>Oi8vY3JslmNvbW9kb2NlLnNvbS9BZGRUcnVzdEV4dGVybmFsQ0FSb290LmNybdA2
>oDSgMoYwaHR0cDovL2Nybc5jb21vZG8ubmV0L0FkZFRydXN0RXh0ZXJuYWxhDQVJv
>b3QuY3JslmAOGCSqGSIb3DQEBBQUAA4IBAQBjhpIQsRP6N76OKrYbikP1XK4OFN/3
>aUB/vxpxAAAnYv9QkSr/gk/8B2AvGD+x+R5ywXfd8FJ38wDOSHFvSg/RS4ijYdPx
>Gz+no1jaA/288Drk7cwSu8m5rnsEoARYv+neLdKnUWYAc9K9fqeU5Z9ablYP06t
>VIB+99Ww/zliZYKMIlfDj/dg9sKNNif8T0PI278cqvaGzebfET+NB/dtgxPAOlG5
>YKF+MOHjID6ku2NvLOmKaCzulmmsBGHhT04OnXJM9nk4yMdlaw+UD3S0vMjPV025
>dXGWDYOGC+vd0PA8fcYumEZqOMcCtci4smV13tqQCLZ3uFMAJctHynNf
>-----END CERTIFICATE-----
>
>-----BEGIN CERTIFICATE-----
>MIIEHjCCAX6gAwIbAgIBATANBgkqhkiG9w0BAQUFADBvMQswCQYDVQQGEWJTRTEU
>MBIGA1UEChMLQWRkVHJ1c3QgQUlXjAkBgNVBA5THUFkZFRydXN0IEV4dGVybmFs
>IFRUCBOZR3b3JrMStlWYDVQQDElBZGRUcnVzdCBFeHRlcm5hbCBDQSBsb290
>MB4XDTAwMDUzMDUwNDZgZGF0eXN0IEF0eXN0IEF0eXN0IEF0eXN0IEF0eXN0IEF0eXN0
>FDASBgNVBAoTODk0ZFRydXN0IEF0eXN0IEF0eXN0IEF0eXN0IEF0eXN0IEF0eXN0
>bCBUFVAgTmV0d29yazEiMCAgA1UEAxMzQWRkVHJ1c3QgRXh0ZXJuYWxhDQVJv
>dDCCASlWDDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALf3GjPm8gAELTngTlvt
>H7xsD821+ioZ2t6bETOXpCImfZOfvUq8k+0DGuOPz+VtUFRWlymUWoCwSxrbLpX9
>uMq/NzgtHj6RQa1wVsfwTz/oMp50ysiQVOnGXw94nZpAPA6sYapeFI+eh6FqUNzX
>mk6vBbOmcZScbNQYArHE504B4YCqOmoaSYykKtMsE8jqzpPhNjfp/haW+710LX
>a0Tkx63ubUFclpxCDezeWWkWaCUN/cALw3CknLa0Dhy2xSoRcRdKn23tNbE7qzN
>E0S3ySvdQwAl+mG5aWpYlxG3pzOPVnVZ9c0p10a3CitlttNCbxWyuHv77+ldU9U0
>WicCAwEAaOB3DCB2AdBgNVHQ4EFgQUrb2YeJ50Jvf6xCZU7wO94CTLVBowCwYD
>VR0PBAQDAGEGMA8GA1UdEwEB/wQFMAMBAf8wgZkGA1UdIwSBKTCBjoAUrb2YeJ50
>Jvf6xCZU7wO94CTLVBqhc6R6xMG8xCzAJBgNVBAYTAiFMRQwEgYDVQQKEwtBZGRU
>cnVzdCBBOQEmMCQGA1UECmMQWRkVHJ1c3QgRXh0ZXJuYWxhDQVJvVFRQIE5ldHdvcm
>slAgBgNVBAMTGUfKZFRydXN0IEV4dGVybmFsIENBIFJvb3SCAQEwDQYJKoZIhvcN
>AQEFBQADggEBALCb4IUlwtYj4g+WBpKdQZic2YR5gdkeWxQHlZlj7DYd7usQWxH
>YINRsPkyPef89iYTx4AWpb9a/IfPeHmJIZrITackhJW88t5RxNkwt9x+Tu5w/Rw5
>6wwCURQtjr0W4MHfRnXnJK3s9EK0hZNwEGe6nQY1ShjTK3rMUUKhemPR5ruhSvC
>Nr4TDea9Y355e6cJDUCrat2PisP29owaQgVR1EX1n6dilWgVIEM8med8vSTYqZEX
>c4g/VhsxOBI0cQ+azcgOno4uG+GMmIPLHzHxREzGBHNJdmAPx/i9F4BrLunMTA5a
>mnkPIAou125jJh5VkpTYghdae9C8x49OhgQ=
>-----END CERTIFICATE-----
>ENDOFBUF
fp4150-1 /security/trustpoint* # commit-buffer

```

Ahora se procede a importar el certificado firmado por la entidad certificadora.

```

fp4150-1 /security/trustpoint # exit
fp4150-1 /security # scope keyring FP_cert
fp4150-1 /security/keyring # set trustpoint Comodo_chain
fp4150-1 /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIIGYDCCBEigAwIbAgILAJH7oNtHau4j8OcwDQYJKoZIhvcNAQELBQAwXDELMakG
>IFRlbgVjb20gUETJMRkwFwYDVQQDDDBBOaW1hcyBUZwxiY29tIENBMBA4XDE5MDQx
.

```

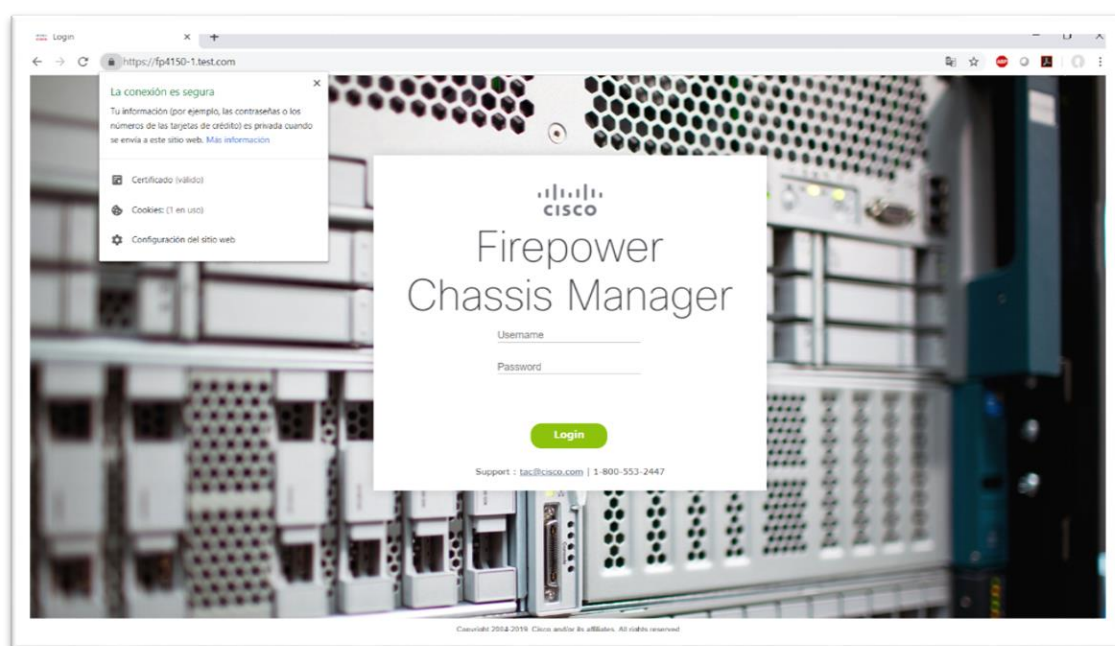


```
...  
.  
>d7f5eQ==  
>-----END CERTIFICATE-----  
>ENDOFBUF  
fp4150-1 /security/keyring* # commit-buffer
```

Por último, se le indica al dispositivo que debe usar el nuevo certificado.

```
fp4150-1 /security/keyring # top  
fp4150-1# scope system  
fp4150-1 /system # scope services  
fp4150-1 /system/services # set https keyring FP_cert  
Warning: When committed, this closes all the web sessions.  
fp4150-1 /system/services* # commit-buffer
```

Una vez realizada la operación, es necesario comprobar que el navegador, que debe tener los certificados de la entidad de confianza instalados, marca el certificado ahora como válido.



10.5 GESTIÓN DE USUARIOS - RADIUS

La gestión de usuarios y permisos en FXOS está basado en roles. A cada usuario se le asigna uno o más roles dentro de los roles predefinidos, que determinan lo que puede hacer.

Los diferentes roles son:

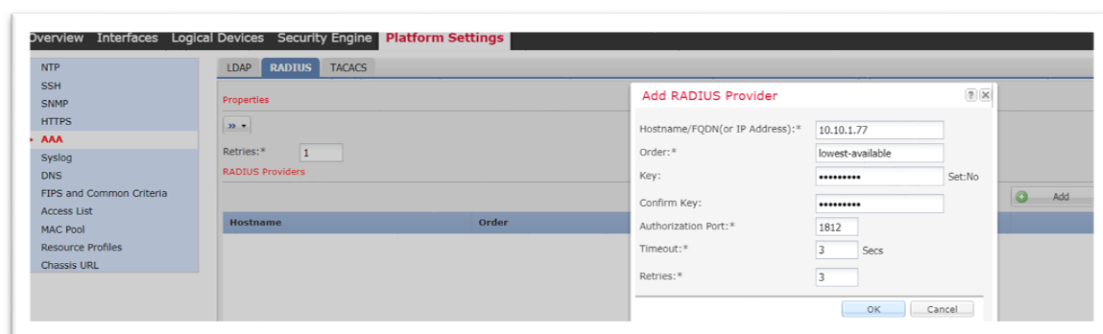
- **Administrator**
Es el de mayor privilegio. Lectura y escritura en todo el sistema. El usuario “admin” por defecto pertenece a este grupo.
- **Read-Only**
Permite tener acceso completo al sistema, pero solo de lectura.
- **Operations**
Permite operar el sistema con permisos básicos.
Acceso de lectura y escrita a la configuración NTP, Smart Call Home para Smart Licensing, logs del sistema, incluyendo syslogs y “faults”.
Acceso de lectura al resto del sistema.
- **AAA Administrator**
Acceso de lectura y escritura de usuarios, asignación de roles y configuración de AAA.
Acceso de lectura al resto del sistema.

Aunque es posible realizar una gestión de usuarios locales, se recomienda el uso de un sistema externo que provea de una política de gestión de contraseñas de acuerdo a las especificaciones en la guía CCN-STIC-301 y otras que sean de aplicación.

El sistema FXOS permite autenticación mediante LDAP, Radius y TACACS. En esta guía vamos a utilizar Radius por ser el sistema más ampliamente utilizado y su capacidad de logging. Cualquier Radius puede ser utilizado, citando los más comunes, Cisco ISE, FreeRadius, WindowsNPS.

Es posible integrar el Radius con un directorio activo que imponga una política de contraseñas (caducidad, bloqueo de reintentos, etc.), en ese caso se recomienda crear un grupo separado (por ejemplo “administradores”) y que solo se permita acceso a los miembros del dominio que pertenezcan a ese grupo.

El primer paso es configurar el servidor o servidores Radius a utilizar. Se recomienda aumentar los reintentos a 3 y bajar el tiempo de timeout a 3. Se recomienda especificar el Radius por IP, ya que en caso de fallo de resolución DNS provocaría timeouts y problemas de entrada al dispositivo. La clave (key) es el secreto (contraseña) compartida con el servidor Radius.



El Radius debe ser configurado para devolverle al dispositivo un atributo que informe del role o roles que deben asignarse al usuario autenticado con éxito. Esto se realiza con el atributo de vendor Cisco-AV-Pair "shell:roles". Por ejemplo: shell:roles="admin". En el caso de que el servidor Radius no disponga por defecto de la configuración de atributos para Cisco, el valor de vendor ID para Cisco es 009 y el valor de vendor ID para el atributo es 001.

El siguiente paso es indicarle al sistema que debe usar el Radius para autenticar a los usuarios. Una vez asignado el Radius, los usuarios locales, como "admin", no podrán ser utilizados. Solo podrán ser usados en caso de fallo con el servidor Radius. Es decir, como "fallback".

Por seguridad se debe usar Radius tanto en Default como en Console.

The screenshot displays the 'User Management' settings in the Cisco Firepower GUI. The 'Settings' tab is active, showing configuration for authentication methods. 'Default Authentication' and 'Console Authentication' are both set to 'RADIUS'. Under 'Remote User Settings', 'No-Login' is selected. Under 'Local User Settings', 'Password Strength Check' is disabled, 'History Count' is 5, 'Change During Interval' is 'Enable', 'Change Interval' is 48 hours, 'Change Count' is 2, and 'No Change Interval' is 24 hours. A note indicates that 'Local is fallback authentication method'.

10.6 COPIAS DE SEGURIDAD - BACKUP

Las copias de seguridad forman una parte importante de la seguridad ya que proveen de respaldo para la restauración del servicio y, también, una imagen en el tiempo de los cambios que puedan haberse realizado inadvertidamente en los sistemas.

En FXOS la configuración es la del Chassis, no la de los cortafuegos, aun así, es conveniente realizar esta copia de seguridad.

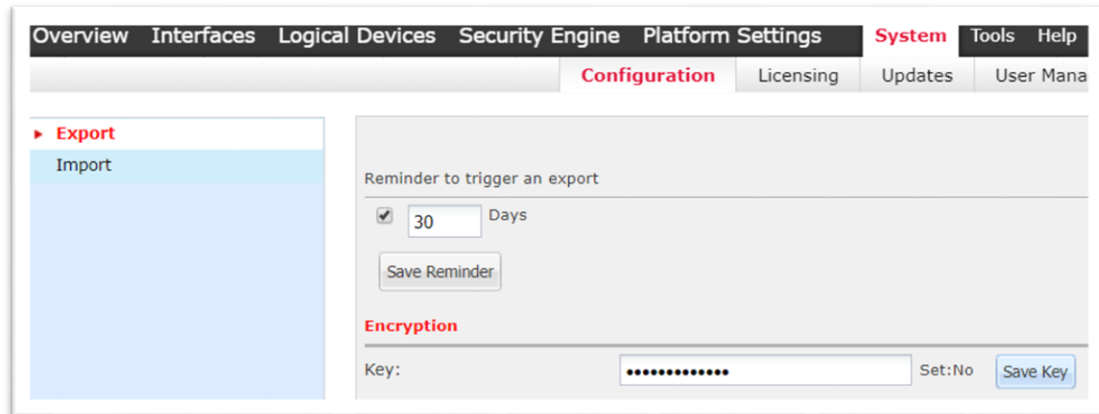
Se recomienda realizar una copia periódica en un dispositivo externo.

Para ello se debe asignar una contraseña de copia de seguridad, que será usada tanto para realizar las copias como para poder realizar la recuperación (import).

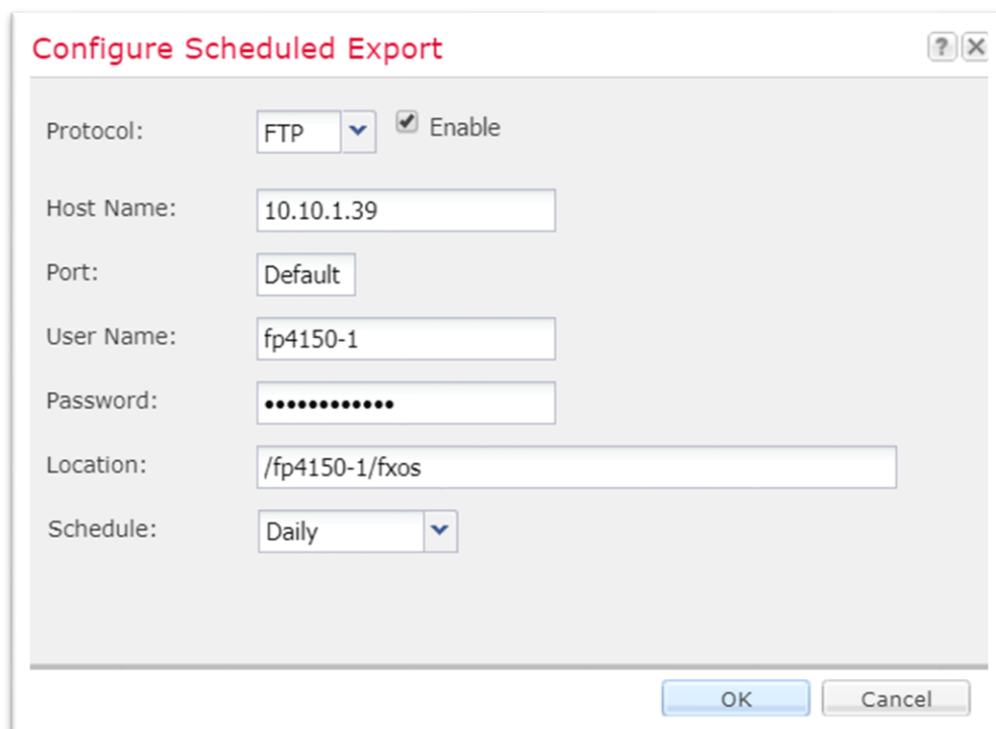
Solo se puede realizar una recuperación en un equipo del mismo modelo que la copia hecha y la misma versión de FXOS. Además de la coincidencia de la contraseña.

Firepower Chassis Manager permite realizar copias periódicas mediante protocolos FTP, SCP, SFTP y TFTP.

Primero se establece la contraseña.



Y luego se configuran los datos de la ubicación externa y la periodicidad. La hora es la de configuración. Al nombre del fichero en "Location" se le añadirá la fecha y la hora de la exportación, por lo que no se sobrescribe.



10.7 CONFIGURACIÓN DE INTERFACES

La configuración, creación, asignación y gestión correcta de interfaces es de gran importancia para los despliegues de los cortafuegos.

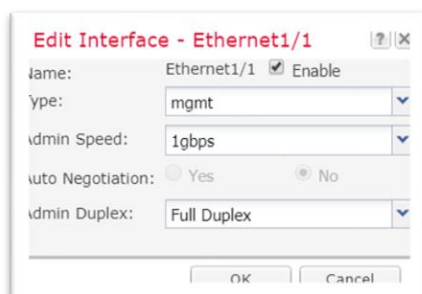
Los equipos 4100 y 9300 soportan interfaces físicas, Etherchannels (agregación de puertos) y subinterfaces VLAN (solo en el caso de cortafuegos en contenedores, para cortafuegos nativos los subinterfaces VLAN se crean en el FMC).

Todas las interfaces en estos equipos usan transceivers, por lo que es necesario configurar la velocidad del interfaz en cada uno de ellos, que dependerá del transceiver utilizado.

Por cada interfaz también es necesario especificar el tipo:

- Data
Tipo regular para tráfico de producción.
- Data-sharing
Son puertos de datos que permiten ser compartidos entre instancias contenedoras de cortafuegos.
- Mgmt
Usado como puerto de gestión fuera de banda para los cortafuegos instalados. Puede ser compartido entre instancias contenedoras.
- Firepower-eventing
Usado como puerto de gestión secundaria. Su uso principal es separar tráfico de gestión general de eventos que puedan ser críticos. No se suele usar.
- Cluster
Puerto utilizado para el montaje en clúster, como el “cluster logical link”. Por defecto se crea el Port-channel 48 para este uso para clúster en Firepower 4100/9300.

Las interfaces deben estar habilitadas (enabled) tanto en la gestión del chassis (FXOS) como en el gestor (FMC) para que puedan ser utilizados.



Edit Interface - Ethernet1/1

Name: Ethernet1/1 ☒ Enable

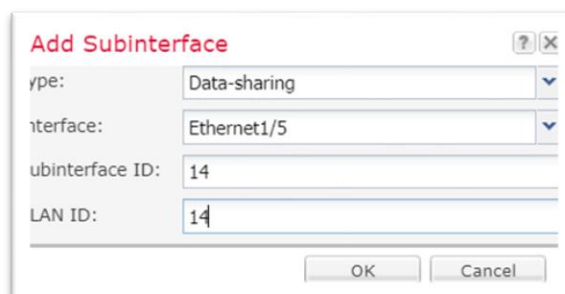
Type: mgmt

Admin Speed: 1gbps

Auto Negotiation: ☐ Yes ☒ No

Admin Duplex: Full Duplex

OK Cancel



Add Subinterface

Type: Data-sharing

Interface: Ethernet1/5

Subinterface ID: 14

LAN ID: 14

OK Cancel

Ejemplos de configuración de interfaces, física y subinterface/VLAN

El sistema permite 2 opciones para configurar agregación de puertos (EtherChannel), LACP en modo activo, o EtherChannel “on” sin negociación.

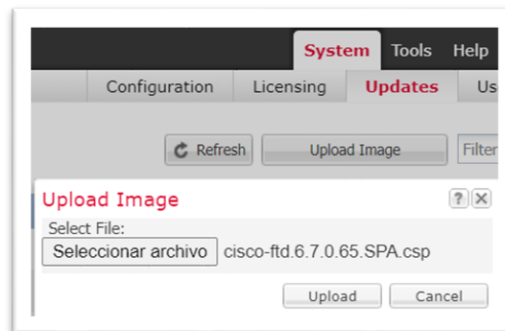
Ejemplo de configuración de Port Channel/EtherChannel (Agregación de Puerto)

La configuración y selección de interfaces dependerá de la integración específica que se desee hacer. Hay que recordar especialmente que se necesita al menos un interfaz en modo “Mgmt” para poder instalar/configurar un cortafuegos FTD.

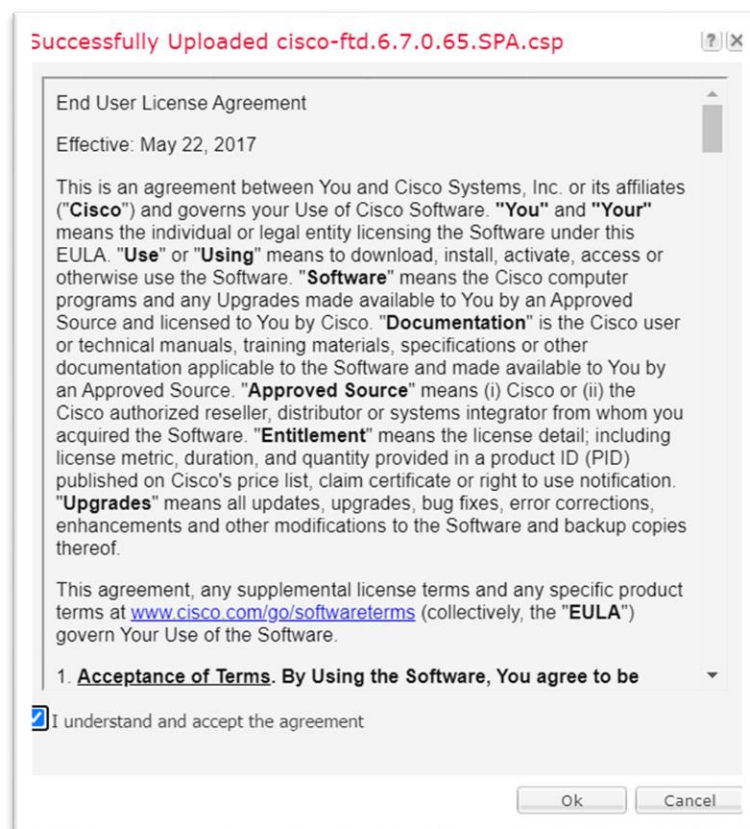
10.8 INSTALACIÓN DE CORTAFUEGOS FTD

Para instalar la imagen Firepower Thread Defense (FTD), que es el verdadero cortafuegos, primero hay que comprobar que se encuentre en el almacenamiento del Chassis. En caso contrario, o que entre las imágenes disponibles no se encuentre la que deseamos instalar, se deberá proceder a la descarga desde la web de Cisco.

Los archivos de imagen instalable tienen extensión CSP (Secure Package files). Una vez descargado el deseado se debe subir al Chassis.



Una vez subida la imagen, esta será verificada criptográficamente para comprobar su validez y procedencia. Se debería aceptar el EULA para que esté disponible.



Las imágenes se instalan en “Logical Devices” que corren sobre los “Security Engine”, que, en realidad, son servidores especializados UCS de Cisco.

Con la imagen ya disponible podremos proceder a realizar una instalación “Native”, que ocupa todo el “Security Engine” con un “Logical Device”, o una instalación de “Container”.

La opción de “Container” está basada en tecnología de contenedores Dockers, donde el “Security Engine” es dividido en cores y memoria y se pueden realizar instalaciones de múltiples instancias diferentes de cortafuegos sobre un mismo “Security Engine”.

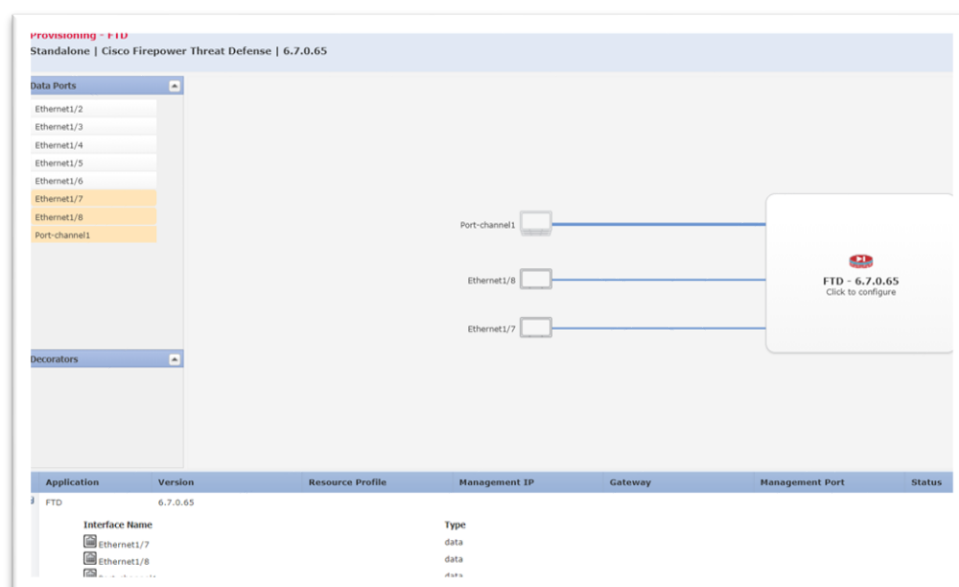
En cambio, la opción “Native” utiliza todos los recursos, cores y memoria, del “Security Engine” para la instalación de un único cortafuegos con capacidad completa.

10.8.1 INSTALACIÓN INSTANCIA FTD NATIVE

Se realiza la instalación de un único “Logical Device”, utilizando la imagen CSP que se desee, seleccionando el modo “Native” y, “Standalone” o “Cluster”, dependiendo de la integración que se quiera realizar. En este ejemplo se usa “Standalone”. Para el modo “Cluster” referirse al punto específico de esa integración en esta misma guía.



En la pantalla de configuración del “Logical Device”, deberemos seleccionar los interfaces de datos que queremos asignarle, pinchando en la parte de la izquierda aparecerán en el dibujo de la derecha conectándolos. Dado que es una instalación “Native” y “Standalone”, se recomienda que se asignen todos los interfaces de datos disponibles.



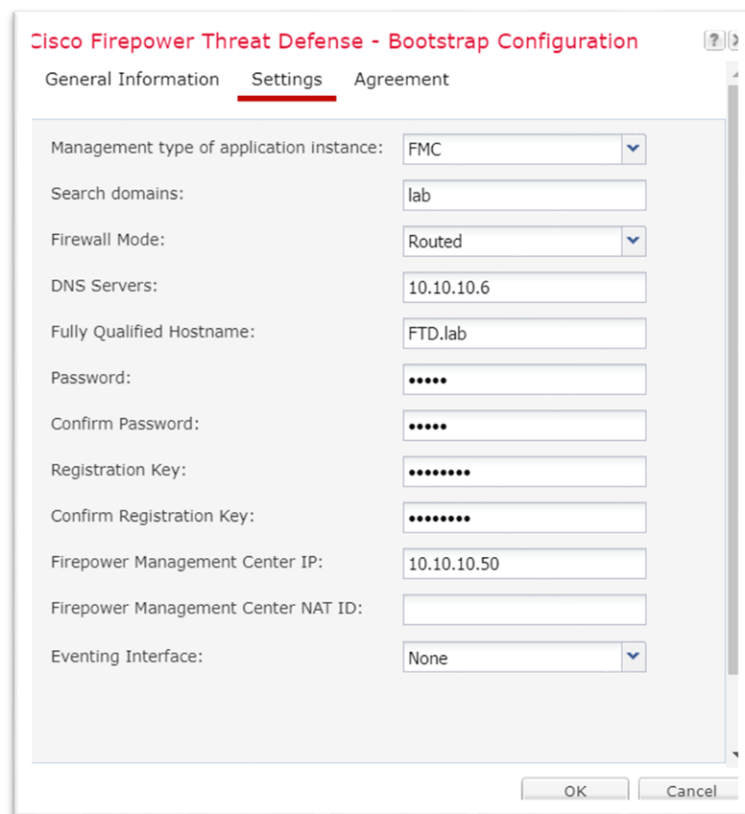
Una vez asignados los interfaces de datos, pinchando en el icono del cortafuegos entraremos en su configuración de “General Information”. Nos pedirá:

- **Management Interface**
Interfaz a utilizar para gestión fuera de banda del FTD (interfaz en modo Mgmt)
- **Management IP / Mask / Gateway**
Dirección IP para la gestión del FTD. Distinta a la del FXOS. Con su Netmask y Gateway correspondiente.

The screenshot shows the 'Cisco Firepower Threat Defense - Bootstrap Configuration' window with the 'General Information' tab selected. The 'Interface Information' section shows 'Management Interface' set to 'Ethernet1/1'. The 'Management' section shows 'Address Type' set to 'IPv4 only'. The 'IPv4' section shows 'Management IP' as '10.10.1.18', 'Network Mask' as '255.255.255.0', and 'Network Gateway' as '10.10.1.254'. 'OK' and 'Cancel' buttons are at the bottom right.

Pulsando sobre Settings se configurará:

- **Registration Key**
Esta es la contraseña que se usará la primera vez para unir el cortafuegos FTD al gestor FMC. Deberá coincidir la contraseña puesta aquí con la introducida posteriormente en el FMC.
- **Password**
Es la contraseña por defecto que tomará el usuario “admin” del FTD.
- **Firepower Management Center IP**
Es la dirección IP del gestor FMC. Solo se aceptará una petición de esta IP.
- **Firewall Mode**
El modo en que operará el cortafuegos, rutado (recomendado) o transparente.



The screenshot shows the 'Cisco Firepower Threat Defense - Bootstrap Configuration' window with the 'Settings' tab selected. The configuration fields are as follows:

Field	Value
Management type of application instance:	FMC
Search domains:	lab
Firewall Mode:	Routed
DNS Servers:	10.10.10.6
Fully Qualified Hostname:	FTD.lab
Password:	
Confirm Password:	
Registration Key:	
Confirm Registration Key:	
Firepower Management Center IP:	10.10.10.50
Firepower Management Center NAT ID:	
Eventing Interface:	None

At the bottom right, there are 'OK' and 'Cancel' buttons.

Una vez terminada la configuración, se pulsa en OK y luego SAVE. Se creará el “Logical Device” y comenzará su instalación.

Una vez que el estado (Status) sea “Online”, habrá concluido la instalación y el cortafuegos está disponible para ser añadido en el gestor FMC.

10.8.2 INSTALACIÓN INSTANCIAS FTD CONTAINER

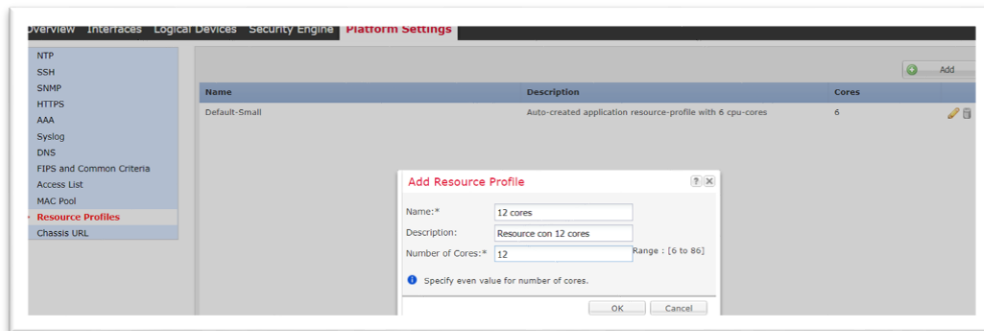
Desde la versión 6.3 de FTD, mediante tecnología de Dockers, es posible instalar instancias múltiples de imagen FTD sobre el mismo “Security Engine”.

Esta funcionalidad reproduce, parcialmente, los contextos múltiples de ASA. A diferencia de estos, las instancias de FTD no comparten recursos, sino que son asignados estrictamente y sustraídos de los recursos totales del “Security Engine”.

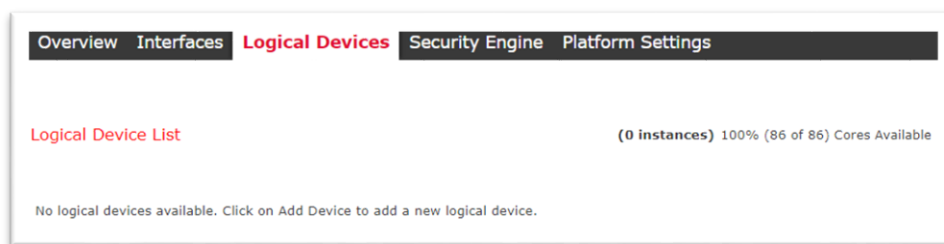
Para cada instancia instalada, el número de núcleos (cores) de CPU es asignado manualmente, donde el número debe ser par, la memoria RAM es dinámicamente asignada dependiendo de los núcleos asignados, y el espacio en disco consumido por instancia es fijo, 40 GB.

El número máximo de instancias soportadas por cada plataforma, junto con el número de cores y la disponibilidad de memoria RAM puede consultarse en la web de Cisco, para el modelo y versión FXOS específica.

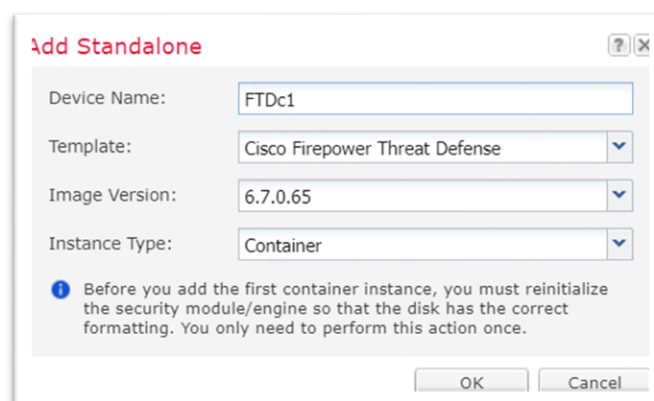
Para definir los recursos utilizados por un “Logical Device” se crean “Resource Profiles”. Por defecto hay uno creado de 6 cores. Podemos añadir otros con el requisito de que el número debe ser par.



En “Logical Devices” pueden verse los cores disponibles en la plataforma, siempre que el “Security Engine” este ya online.



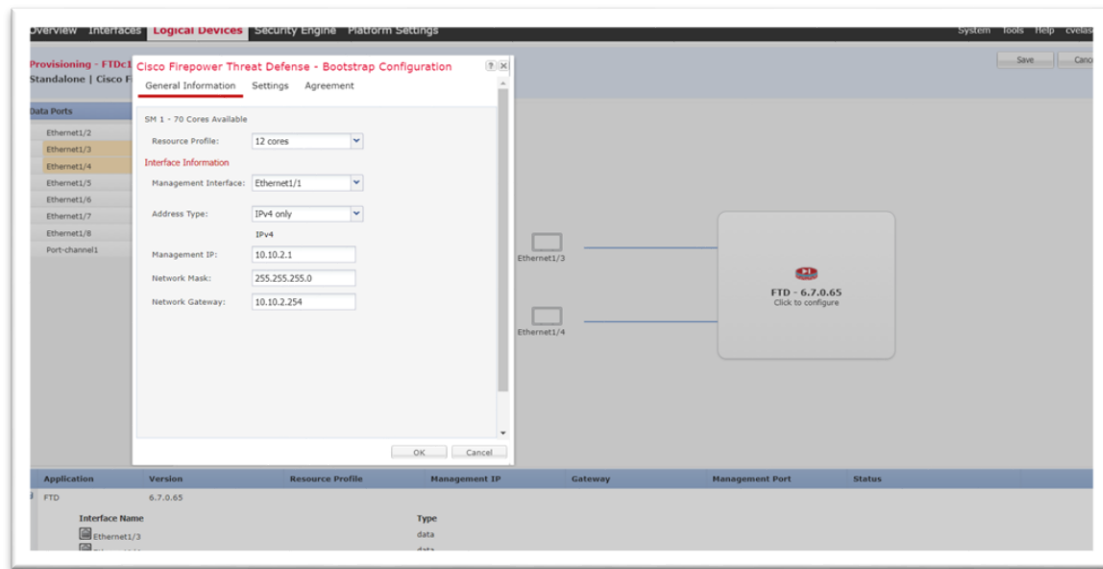
Para crear una nueva instancia en modo Container, se pincha en “Add Device” y se selecciona el tipo de instancia “Container”.



En la sección de configuración del dispositivo, asignamos interfaces igual que en una instancia Native. Es importante recordar que las interfaces pueden ser compartidos

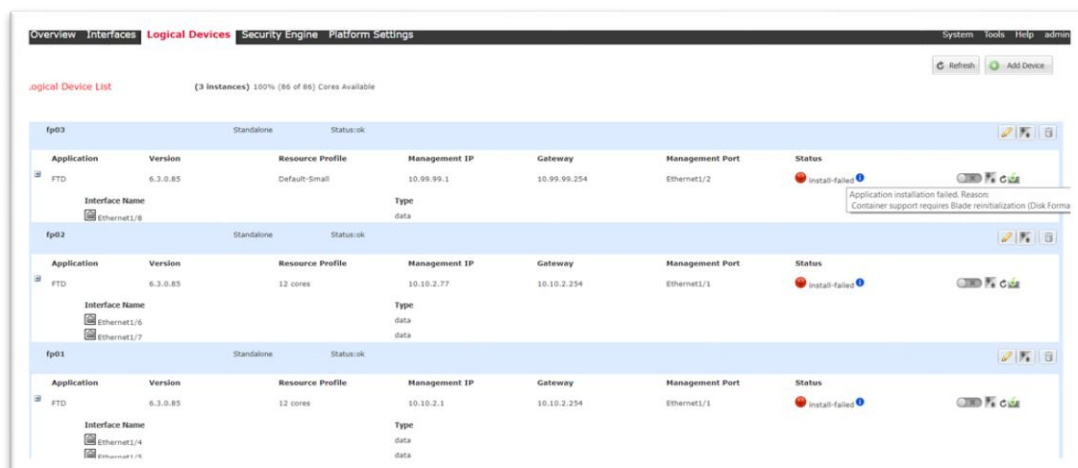
en las múltiples instancias “Container”, tanto Mgmt como Data si están en modo Sharing. Para asignar interfaces con VLAN que puedan ser compartidos, se deben crear en el FXOS y seleccionar el tipo adecuado.

En la sección de configuración del dispositivo aparece una nueva opción con respecto a “Native”, el “Resource Profile” que debemos seleccionar. Para el resto de campos, consultar la sección de instancia “Native”.



Podemos crear varias instancias, por ejemplo 3, y repartir interfaces y recursos.

Importante. La primera vez que configuramos una instancia “Container” veremos que se produce un error “Container support requires Blade reinitialization (Disk Format)”.



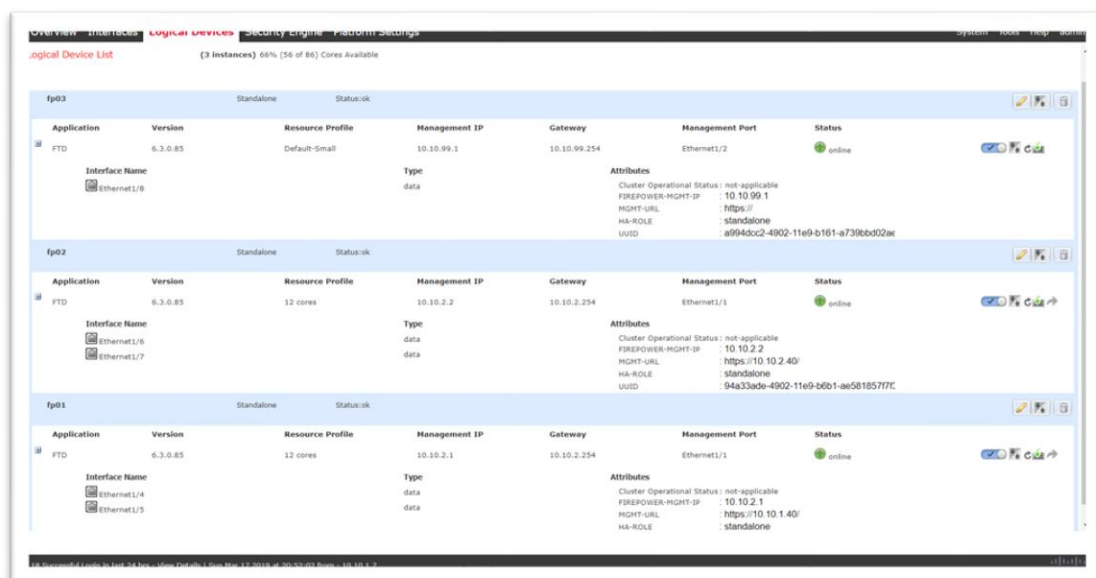
Este error es esperado y es debido a que cuando se utilizan contenedores, el disco del servidor “Security Engine” debe formatearse de una manera especial. Para que esto tenga lugar hay que reinicializar el SE manualmente.

Para ello, en la pantalla de “Security Engine” hay que pulsar sobre el tercer icono, si pasamos el ratón por encima y lo detenemos unos segundos se lee “Reinitialize Security Engine”.



Después de que el SE se reinicie, veremos que los dispositivos lógicos empezarán a instalarse y se pondrán online.

En esta configuración tenemos las 3 instancias sobre 1 único SE.



10.9 ACTUALIZACIÓN SISTEMA FXOS

En un sistema mantenido Firepower, tanto la parte FTD como la parte FXOS deben actualizarse regularmente. Especialmente si se publican avisos de seguridad afectando a las versiones instaladas en funcionamiento.

Las familias de hardware ASA e ISA3000 no tienen software FXOS por lo que esta sección no aplica a estos equipos.

Las familias Firepower 1000 y 2100 utilizan un sistema integrado FXOS+FTD, donde la actualización siempre se produce de los 2 componentes a la vez, solo mostrándose la versión FTD en las actualizaciones.

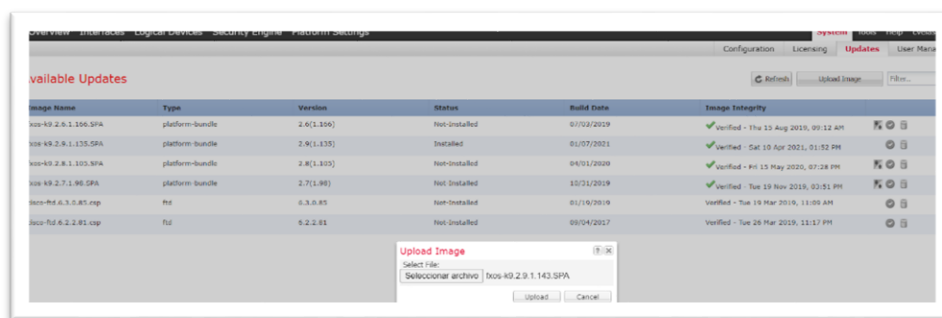
En las familias Firepower 4100 y 9300, en cambio, los sistemas FXOS y FTD se actualizan de manera totalmente independiente. Es necesario consultar las tablas de compatibilidad para verificar que las versiones son compatibles entre sí.

Una actualización de FXOS fuerza la parada de todas las instancias FTD corriendo en la plataforma y su re arranque tras la actualización, por lo que se requiere una ventana de mantenimiento para realizarla. El tiempo depende de la plataforma hardware y el upgrade. Actualmente, por experiencia, pueden ir desde 15 minutos hasta 1 hora.

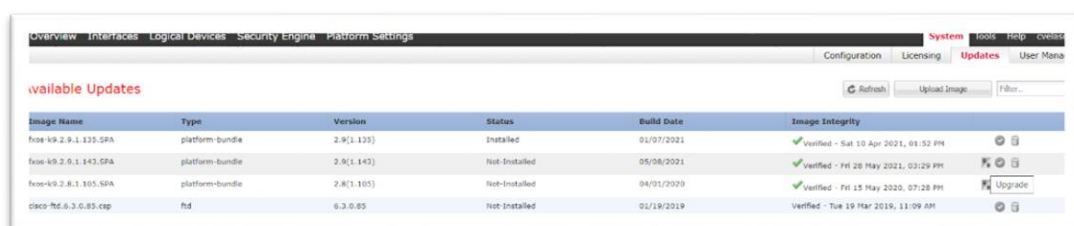
En un sistema de alta disponibilidad activo/pasivo (failover) se debe realizar la actualización del sistema FXOS primero en el equipo pasivo, realizar una conmutación activo<->pasivo y volver a aplicar la actualización en el nuevo pasivo. Esto permite realizar una actualización prácticamente sin cortes ni pérdida de servicio.

Para realizar una actualización de FXOS se debe descargar la imagen desde la web de Cisco, apartado FXOS del modelo exacto. La imagen tiene una extensión SPA (Signed Production key A).

Una vez descargada se debe subir al Chassis Manager, que la verificará.



Una vez aparezca en el listado de imágenes disponibles, se debe usar el primer icono ("Upgrade") para lanzar la actualización. Se recomienda realizar una copia de seguridad antes de la actualización.



Un mensaje advertirá de que se va a producir una actualización con pérdida de servicio y de accesibilidad al FP Chassis Manager.



Una vez terminada la actualización, accediendo al FP Chassis Manager comprobaremos que la actualización se ha realizado con éxito.

Se recomienda volver a realizar una copia de seguridad después de haber realizado la actualización.

11. BORRADO SEGURO DE FIREPOWER - DESMANTELAMIENTO

En ocasiones surgirá la necesidad de borrar todos los datos de configuración y parametrización de equipos Firepower. Bien porque los equipos se van a liberar/desafectar, o porque van a ser desmantelados de producción, o simplemente van a ser asignados a otra unidad.

Para realizar un borrado seguro del dispositivo se deben seguir estos tres pasos completos.

11.1 BORRADO SIMPLE EN FIREPOWER 1000/2100 (OPCIONAL)

En este paso solo realizamos un borrado “estándar” de la configuración, que reiniciará el equipo y parecerá que es la primera instalación.

La ventaja de esta opción es que es muy rápida.

La desventaja es que un equipo especialista podría recuperar la información de configuración y parametrización anterior.

Debemos conectarnos al sistema FXOS por SSH. En equipos Firepower 2100, donde no existe el sistema FXOS separado, esto se consigue entrando por SSH al sistema FTD e introduciendo “connect fxos”.

El procedimiento se basa en introducir el comando de borrado de configuración (“erase configuration”), como se describe en el siguiente cuadro.

```
firepower# connect local-mgmt
firepower(local-mgmt)# erase configuration
All configurations will be erased and system will reboot. Are you sure? (yes/no):yes
```

El equipo se reiniciará y se deberá seguir el procedimiento de “configuración inicial” correspondiente para volver a ser utilizado/desplegado.

11.2 FORMATEO Y BORRADO SEGURO ASA 5500-X/ISA 3000

El objetivo de este paso es realizar un “formateado” del almacenamiento del equipo seguido de un borrado seguro irrecuperable. En los equipos ASA e ISA, al tener ROMmon, este proceso se realiza desde este modo tras el reinicio del equipo:

```
> reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': yes
(...)

Booting from ROMMON

Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot in 7 seconds.
rommon #0> erase disk0:

About to erase the selected device, this will erase
all files including configuration, and images.
Continue with erase? y/n [n]: y

Erasing Disk0:
.....
[...]
```

11.3 FORMATEO Y BORRADO SEGURO FIREPOWER 1000/2100

El objetivo de este paso es realizar un “formateado” del almacenamiento del equipo seguido de un borrado seguro irrecuperable.

Este procedimiento es diferente para los equipos FP 1000/2100 que, para los FP 4100/9300, debido a las diferentes integraciones FXOS-FTD.

Para el procedimiento en Firepower 1000 o 2100, se debe conectar por SSH al sistema FTD y, desde ahí, conectar al sistema FXOS interno utilizando “connect fxos”, se formatea y, siguiendo el primer paso del procedimiento de reimagen, se carga la imagen SPA en memoria.

Esto es necesario para que el borrado seguro incorporado en el sistema FXOS pueda ejecutarse sin bloqueos, ya que de existir ya una imagen instalada e intentar el borrado seguro, este dará un error(2).

> **connect fxos**

Cisco Firepower Extensible Operating System (FX-OS) Software

TAC support: <http://www.cisco.com/tac>

Copyright (c) 2009-2015, Cisco Systems, Inc. All rights reserved.

.

...

.

<http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html>. See User Manual ("Licensing") for details.

fp1-2100# **connect local-mgmt**

fp1-2100(local-mgmt)# **format everything**

All configuration and bootable images will be lost.

Do you still want to format? (yes/no):**yes**

100+0 records in

100+0 records out

51200 bytes (51 kB) copied, 0.00580008 s, 8.8 MB/s

.

...

.

Sending all processes the TERM signal...

SIGKILL_ALL will be delayed for 1 + 5 secs

Sending all processes the KILL signal...

Deactivating swap...

Unmounting local filesystems...

Rebooting... [410.431694] Restarting system.

```
*****
Cisco System ROMMON, Version 1.0.06, RELEASE SOFTWARE
Copyright (c) 1994-2017 by Cisco Systems, Inc.
Compiled Wed 11/01/2017 18:38:59.66 by builder
*****
```

Current image running: Boot ROM1

Last reset cause: ResetRequest

DIMM_1/1 : Present

DIMM_2/1 : Absent

Platform FPR-2110 with 16384 MBytes of main memory

BIOS has been successfully locked !!

MAC Address: 38:90:a5:84:21:00

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

rommon 1 > address 10.10.10.1
rommon 2 > netmask 255.255.255.0
rommon 3 > server 10.10.10.10
rommon 4 > gateway 10.10.10.100
rommon 5 > file cisco-ftd-fp2k.6.3.0-83.SPA
rommon 6 > set
  ADDRESS=10.10.10.1
  NETMASK=255.255.255.0
  GATEWAY=10.10.10.100
  SERVER=10.10.10.10
  IMAGE=cisco-ftd-fp2k.6.3.0-83.SPA
  CONFIG=
  PS1="rommon ! > "

rommon 7 > tftpdnld -b
...
Cisco FPR Series Security Appliance
firepower-2110 login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1
Hello admin. You must change your password.
Enter new password: ***
Confirm new password: ***
Your password was updated successfully.
...
firepower-2110# connect local-mgmt
firepower-2110(local-mgmt)# erase secure all
The physical storages SSD1 and SSD2 will be securely erased.
ALL CONFIGURATION AND DATA WILL BE LOST AND CANNOT BE RECOVERED!
After the erase the device will reboot and will be re-initialized.
DO NOT POWER OFF THE DEVICE DURING THIS OPERATION!
Are you sure? (yes/no):yes
Starting secure erase of all disks.....

Broadcast message from admin@firepower-2130 (Thu May 20 14:27:17 2021):

All shells being terminated due to system /sbin/reboot
```

11.4 BORRADO SEGURO FIREPOWER 4100/9300

Los equipos Firepower 4100/9300 disponen de opción de borrado seguro interna, pero esta debe ser utilizada cuando los almacenamientos no están bloqueados por su uso normal, al menos hasta la versión 2.9 de FXOS, por lo que hay que realizar un arranque del sistema en memoria.

Para el procedimiento de borrado seguro en equipos Firepower 4100 y 9300 se necesita conexión a la consola del chassis, para acceder al “rommon” reiniciando el sistema o apagando/encendiendo el equipo.

Una vez en rommon, se necesita realizar un arranque de sistema mínimo. Para ello lo mejor es buscar dentro del path “/installables/switch/” por las imágenes instaladas que se necesitan para el arranque, que son las imágenes “kickstart” y “system”, con el mismo número de versión. Si no se encontrase ninguna, se puede realizar la carga por TFTP, ver apartado de Reimagen de equipos Firepower 4100/9300.

```
!! Rommon image verified successfully !!
```

```
Cisco System ROMMON, Version 1.0.14, RELEASE SOFTWARE
Copyright (c) 1994-2017 by Cisco Systems, Inc.
Compiled Thu 08/24/2017 15:49:40.98 by builder
Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!
```

```
Platform FPR-4140-SUP with 8192 Mbytes of main memory
MAC Address: 18:80:90:9d:fc:fc
```

```
find the string ! boot bootflash:/installables/switch/pxos-k9-kickstart.5.0.3.N2.4.91.111.SPA
bootflash:/installables/switch/pxos-k9-system.5.0.3.N2.4.91.111.SPA
```

Use BREAK, ESC or CTRL+L to interrupt boot.

Use SPACE to begin boot immediately.
Boot interrupted.

```
rommon 1 > dir installables/switch
Directory of: bootflash:\installables\switch
```

```
05/28/21 06:50p <DIR>      4,096 .
05/28/21 07:07p <DIR>      4,096 ..
05/28/21 06:49p      60,400,640 pxos-k9-kickstart.5.0.3.N2.4.91.111.SPA
05/28/21 06:49p      417,633,376 pxos-k9-manager.4.9.1.111.SPA
05/28/21 06:49p      73,062,856 pxos-k9-mgmttext.2.9.1.63.SPA
05/28/21 06:49p      193,054,029 pxos-k9-system.5.0.3.N2.4.91.111.SPA
      4 File(s) 744,150,901 bytes
      2 Dir(s)
```

```
rommon 2 > boot /installables/switch/pxos-k9-kickstart.5.0.3.N2.4.91.111.SPA /installables/switch/pxos-k9-
system.5.0.3.N2.4.91.111.SPA
```

```
!! Kickstart Image verified successfully !!
```

```
Linux version: 3.14.39ltsi (security@cisco.com) #1 SMP Thu Dec 24 03:18:35 PST 2020
linuxrc.ext Fri May 28 19:42:54 UTC 2021
1+0 records in
1+0 records out
64 bytes (64 B) POST INIT Starts at Fri May 28 19:43:01 UTC 2021
S10mount-ramfs.supnuovaca Mounting /isan 2500m
Mounted /isan
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
```

```
FPGA Version 0x00010600 FPGA Min Version 0x00000600
Checking all filesystems... done.
Checking NVRAM block device ... done
.
FIPS power-on self-test passed
Unpack CMC Application software
1
Loading system software
Uncompressing system image: bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.4.91.111.SPA

Manager image digital signature verification successful
C
11+1 records in
11+1 records out
9577 bytes (9.6 kB) copied, 9.2744e-05 s, 103 MB/s
snm mode on SUP
INIT: Entering runlevel: 3
cmcmon: 160:cmclog_setlevel_modu

-----
enabled fc feature
-----
2021 May 28 21:45:30 %$ VDC-1 %$ %USER-2-SYSTEM_MSG: CLIS: loading cmd files begin - clis
2021 May 28 21:45:39 %$ VDC-1 %$ %USER-2-SYSTEM_MSG: CLIS: loading cmd files end - clis
2021 May 28 21:45:39 %$ VDC-1 %$ %USER-2-SYSTEM_MSG: CLIS: init begin - clis
2021 May 28 21:45:39 %$ VDC-1 %$ %USER-2-SYSTEM_MSG: %SMART_LIC-2-PLATFORM_ERROR:Smart
Licensing has encountered an internal software error. Contact TAC: The platform provided UDI list has invalid
values: ; udi_pid is emp - SMART_AGENT[4893]
System is coming up ... Please wait ...
System is coming up ... Please wait ...
System is coming up ... Please wait ...
System is coming up ... Please wait ...
System is coming up ... Please wait ...
2021 May 28 21:46:22 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: Starting bcm_attach, unit 0 - bcm_usd
System is coming up ... Please wait ...
System is coming up ... Please wait ...
System is coming up ... Please wait ...
2021 May 28 21:46:36 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: Finished bcm_attach..., unit 0 - bcm_usd
2021 May 28 21:46:37 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: Enabling Filter on CPU port - bcm_usd
System is coming up ... Please wait ...
System is coming up ... Please wait ...
2021 May 28 21:46:45 %$ VDC-1 %$ %VDC_MGR-2-VDC_ONLINE: vdc 1 has come online
System is coming up ... Please wait ...

FTD1 login: admin
Password:
Successful login attempts for user 'admin' : 3
System is coming up... Please wait...
...
System is coming up... Please wait...
2021 May 28 21:48:36 FTD1 %$ VDC-1 %$ %ETHPC-2-PORTS_UP:
System is coming up... Please wait...
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2021, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.
```

...

Certain components of this software are licensed under the "GNU Library General Public License, version 2" provided with ABSOLUTELY NO WARRANTY under the terms of "GNU Library General Public License, version 2", available here: <http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html>. See User Manual ("Licensing") for details.

FTD1# **connect local-mgmt**

FTD1(local-mgmt)# **erase secure chassis**

The physical storages in supervisor and all service modules will be securely erased.

ALL DATA AND IMAGES WILL BE LOST AND CANNOT BE RECOVERED!

After the erase the chassis will reboot and need to be re-initialized.

DO NOT POWER OFF THE DEVICE IF YOU DECIDE TO PERFORM THIS TASK!

Are you sure? (yes/no):**yes**

FTD1(local-mgmt)# [410.568308] writing reset reason 9,

Message from syslogd@(none) at May 28 21:49:36 ...

kernel: [410.568308] writing reset reason 9,

INIT: Sending processes the TERM signal

FTD1(local-mg/bin/cp: cannot stat '/tmp/sysmgr_dtrace.dbg.0': No such file or directory

Sending all processes the TERM signal...

Sending all processes the KILL signal...

Copying /bootflash/logs/plog to /mnt/plog

Unmounting filesystems...

/bootflash/sysdebug/tftpd_logs: ignored

/spare : successfully unmounted

/cgroup : successfully unmounted

/workspace : successfully unmounted

/opt/db/nvram : successfully unmounted

/opt : successfully unmounted

/bootflash : successfully unmounted

/mnt/pss : successfully unmounted

/dev/pts : ignored

/var/sysmgr/startup-cfg : ignored

/mnt/cfg/1 : successfully unmounted

/mnt/cfg/0 : successfully unmounted

/mnt/plog : successfully unmounted

/debugfs : successfully unmounted

/dev/mqueue : successfully unmounted

/debug : ignored

/volatile : ignored

/dev/shm : ignored

/callhome : ignored

/var/sysmgr/ftp : ignored

/var/sysmgr : ignored

/var/tmp : ignored

/isan : ignored

/sys : ignored

/proc : ignored

Starting secure erase of supervisor...

Starting secure erase of OBFL devices...

1.2.

The first MTD device has been erased cleanly.

3.4.

The second MTD device has been erased cleanly.

5.6.

The third MTD device has been erased cleanly.

OBFL secure erase done.

Starting secure erase of NVRAM...

1.2.

The first part of NVRAM has been erased cleanly.

3.4.

The second part of NVRAM has been erased cleanly.

NVRAM secure erase done.

Starting secure erase of SSD...

SSD is not frozen. Proceed...

Setting SSD to a correct state for erasing...

SSD is in a correct state. Perform secure erase...

Erase done. Verifying erase result...

SSD is in a correct state after secure erase.

Check on SSD secure erase has passed.

Resetting rommon firmware variables...

Resetting rommon firmware variables done.

Secure erase of supervisor has completed.

[829.609369] Disconnected SATA Storage device(sda) from PCI bus

[905.731056] reboot: Restarting system

```
*
*
* Rom Monitor NVRAM configuration is being initialized to *
* default values. This may be because it was never initialized. *
*
*
*****
```

!! Rommon image verified successfully !!

Cisco System ROMMON, Version 1.0.14, RELEASE SOFTWARE

Copyright (c) 1994-2017 by Cisco Systems, Inc.

Compiled Thu 08/24/2017 15:49:40.98 by builder

Current image running: Boot ROM1

Last reset cause: ResetRequest

DIMM Slot 0 : Present

DIMM Slot 1 : Present

No SATA drive !!

No USB drive !!

BIOS has been locked !!

Platform FPR-4140-SUP with 8192 Mbytes of main memory

MAC Address: 18:80:90:9d:fc:fc

autoboot: Can not find autoboot file 'menu.lst.local'

Or can not find correct boot string !!

rommon 1 >

12. REIMAGEN DEL SISTEMA

Hacer una reimagen del sistema significa volver a introducir una versión base nueva de FXOS o FXOS+FTD (en caso de Firepower 1000/2100) o sólo de FTD en el caso de los ASA/ISA.

Bien por corrupción del sistema, o por downgrade, por inestabilidad, o porque se haya realizado un borrado seguro del dispositivo, a veces es necesario realizar este procedimiento.

Al igual que en los apartados anteriores, el procedimiento es diferente para equipos Firepower 2100 (FXOS+FTD) que para equipos Firepower 4100/9300 (FXOS) que para los equipos ASA/ISA.

12.1 REIMAGEN DE EQUIPOS ASA 5500-X/ISA 3000

Este procedimiento requiere conexión al equipo a través de la consola y que, desde la interfaz Management 1/1, exista conectividad al servidor TFTP/FTP/HTTP donde se encuentre disponible la imagen FTD a instalar.

Tras esto se procederá a los siguientes pasos:

Paso 1	Si el FTD está gestionado a través de una FMC, eliminar el equipo del management center.
Paso 2	Si el equipo usa el manager local FDM, asegúrate de desregistrar el equipo del Smart Software Licensing Server ya sea desde el equipo o desde el portal de licencias..
Paso 5	Reincia el equipo via CLI usando conectándose al equipo por el puerto de consola: > reboot This command will reboot the system. Continue? Please enter 'YES' or 'NO': yes
Paso 6	Pulse Esc durante el proceso de reinicio para entrar en el modo ROMmon cuando se lo indica el sistema: Booting from ROMMON Cisco Systems ROMMON Version (2.1(9)8) #1: Wed Oct 26 17:14:40 PDT 2011 Platform ASA 5508-X with SW, 8 GE Data, 1 GE Mgmt Use BREAK or ESC to interrupt boot. Use SPACE to begin boot immediately. Boot in 7 seconds.
Paso 7	Elimine toda la información del equipo: rommon 1 > erase disk0: erase: Erasing 7583 MBytes rommon 2 >
Paso 8	Configure la interfaz de Management 1/1 y los detalles del servidor desde el que descargar la imagen a instalar: interface interface_id address management_ip_address netmask subnet_mask

	<pre> server tftp_ip_address gateway gateway_ip_address file path/filename set sync tftpdnld </pre> El FTD descargará en este punto la imagen de arranque e iniciará la boot CLI.
Paso 9	Una vez en el boot CLI introducir setup , y configurar la información de red y de la interfaz Management 1/1 para poder establecer la conectividad FTP o HTTP con el servidor desde el que descargar la imagen de software. and configure network settings for the Management interface to establish temporary connectivity to the HTTP or FTP server so that you can download and install the system software package. <pre> Cisco FTD Boot 6.3.0 Type ? for list of commands firepower-boot> firepower-boot>setup </pre> Welcome to Cisco FTD Setup [hit Ctrl-C to abort] Default values are inside [] Enter a hostname [firepower]: example.cisco.com Do you want to configure IPv4 address on management interface?(y/n) [Y]: y Do you want to enable DHCP for IPv4 address assignment on management interface?(y/n) [Y]: n Enter an IPv4 address: 10.123.123.123 Enter the netmask: 255.255.255.0 Enter the gateway: 10.123.123.1 Do you want to configure static IPv6 address on management interface?(y/n) [N]: n Stateless autoconfiguration will be enabled for IPv6 addresses. Enter the primary DNS server IP address [64.102.6.247]: 10.123.123.2 Do you want to configure Secondary DNS Server? (y/n) [y]: n Any previously configured secondary DNS servers will be removed. Do you want to configure Local Domain Name? (y/n) [n]: n Do you want to configure Search domains? (y/n) [y]: n Any previously configured search domains will be removed. Do you want to enable the NTP service? [N]: n Please review the final configuration: Hostname: example.cisco.com

	Management Interface Configuration IPv4 Configuration: static IP Address: 10.123.123.123 Netmask: 255.255.255.0 Gateway: 10.123.123.1 IPv6 Configuration: Stateless autoconfiguration DNS Configuration: DNS Server: 10.123.123.2 NTP configuration: Disabled CAUTION: You have selected IPv6 stateless autoconfiguration, which assigns a global address based on network prefix and a device identifier. Although this address is unlikely to change, if it does change, the system will stop functioning correctly. We suggest you use static addressing instead. Apply the changes?(y,n) [Y]: y Configuration saved successfully! Applying... Restarting network services... Done. Press ENTER to continue... firepower-boot>
Paso 10	Descarga la imagen FTD. Este ejemplo muestra la descarga via HTTP: system install [noconfirm] url Include the noconfirm option if you do not want to respond to confirmation messages. Example: > system install noconfirm http://10.86.118.21/ftd-6.0.1-949.pkg You are prompted to erase the internal flash drive. Enter y. ##### WARNING ##### # The content of disk0: will be erased during installation! # ##### Do you want to continue? [y/N] y

	The installation process erases the flash drive and downloads the system image. You are prompted to continue with the installation. Enter y. Erasing disk0 ... Verifying Downloading Extracting Package Detail Description: Cisco ASA-NGFW 6.3.0 System Install Requires reboot: Yes Do you want to continue with upgrade? [y]: y When the installation finishes, press Enter to reboot the device. Warning: Please do not interrupt the process or turn off the system. Doing so might leave system in unusable state. Starting upgrade process ... Populating new system image Reboot is required to complete the upgrade. Press 'Enter' to reboot the system. El reinicio puede tardar unos 30 minutos. Una vez reiniciado, el equipo tendrá la imagen FTD instalada y lista para funcionar.
Paso 13	En este punto se puede proceder con el setup inicial del equipo descrito en secciones anteriores.

12.2 REIMAGEN DE EQUIPOS FIREPOWER 1000/2100

Para realizar este proceso necesitamos conectarnos tanto por consola al equipo como por IP al interfaz de gestión fuera de banda.

Necesitaremos un PC con un servidor TFTP y, preferiblemente, también FTP. Descargaremos una imagen SPA, esta imagen se encuentra en la web de Cisco en las versiones base, como 6.6.0, 7.0... No se encuentra en las actualizaciones 6.6.1, 6.6.4. La imagen la colocaremos en el directorio principal de descarga del TFTP y FTP, en el path `"/`.

El proceso puede tardar entre 20 y 30 minutos.

Empezaremos arrancando el equipo en rommon e iniciando la carga parcial de la imagen por TFTP. El error "TFTP: out of memory" se debe ignorar si aparece.

```
*****
Cisco System ROMMON, Version 1.0.06, RELEASE SOFTWARE
Copyright (c) 1994-2017 by Cisco Systems, Inc.
Compiled Wed 11/01/2017 18:38:59.66 by builder
*****

Current image running: Boot ROM1
Last reset cause: LocalSoft
DIMM_1/1 : Present
DIMM_2/1 : Absent

Platform FPR-2110 with 16384 MBytes of main memory
BIOS has been successfully locked !!
MAC Address: 38:90:a5:84:21:00

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

rommon 1 > address 10.10.10.1
rommon 2 > netmask 255.255.255.0
rommon 3 > server 10.10.10.10
rommon 4 > gateway 10.10.10.100
rommon 5 > file cisco-ftd-fp2k.6.3.0-83.SPA
rommon 6 > set
  ADDRESS=10.10.10.1
  NETMASK=255.255.255.0
  GATEWAY=10.10.10.100
  SERVER=10.10.10.10
  IMAGE=cisco-ftd-fp2k.6.3.0-83.SPA
  CONFIG=
  PS1="rommon ! > "

rommon 7 > tftpdnld -b
```

```

ADDRESS: 10.10.10.1
NETMASK: 255.255.255.0
GATEWAY: 10.10.10.100
SERVER: 10.10.10.10
IMAGE: cisco-ftd-fp2k.6.3.0-83.SPA
MACADDR: 40:01:7a:9f:64:00
VERBOSITY: Progress
RETRY: 40
PKTTIMEOUT: 7200
BLKSIZE: 1460
CHECKSUM: Yes
PORT: GbE/1
PHYMODE: Auto Detect

link up
Receiving cisco-ftd-fp2k.7.0.0-94.SPA from 10.10.10.10 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
File reception completed.
Boot buffer bigbuf=7d93e3d8
Boot image size = 181793264 (0xad5f1f0) bytes
[image size] 181793264
[MD5 signaure] 9a53089a2912d9e20b35828341853e09
+-----+
+----- SUCCESS -----+
+-----+
|                                     |
|   LFBFF signature authentication passed !!!   |
|                                     |
+-----+
LFBFF signature verified.
+-----+
+----- SUCCESS -----+
+-----+
|                                     |
|   LFBFF controller type check passed !!!   |
|                                     |
+-----+
INIT: version 2.88 booting
Starting udev
Hardware tweak APPLIED: Disable SATA Throttle.1
Hardware tweak APPLIED: Disable SATA Throttle.2
Configuring network interfaces... done.
Populating dev cache
...
d to re-install
Mar 17 07:34:14 firepower-2110 port-manager : portmgr_insert_card: mainboard 0xcdd, ctype 0xcdd
Mar 17 07:34:15 firepower-2110 port-manager : Alert: Internal1/2 link changed to UP

Cisco FPR Series Security Appliance
firepower-2110 login:

```

Una vez con la versión arrancada desde TFTP, se transfiere la imagen completa al almacenamiento del dispositivo y se instalará usando el auto-install, una vez completado todo el proceso el equipo se reiniciará y se deberá seguir el procedimiento de configuración inicial del dispositivo.

Se recomienda el uso de protocolo FTP en esta parte, ya que es mucho más rápido que TFTP.

Las credenciales por defecto son las mismas que en una configuración inicial:

- Usuario: admin
- Contraseña: Admin123

```
Cisco FPR Series Security Appliance
firepower-2110 login: admin
Password:
firepower# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # set out-of-band static ip 10.10.10.1 netmask 255.255.255.0 gw
10.10.10.100
firepower-2110 /fabric-interconnect* # commit-buffer
firepower-2110 /fabric-interconnect # scope firmware
firepower-2110 /firmware # download image ftp://10.10.10.10/cisco-ftd-fp2k.7.0.0-94.SPA
Password:
Please use the command 'show download-task' or 'show download-task detail' to check download progress.
% Download-task cisco-ftd-fp2k.7.0.0-94.SPA : transferring 108465 KB
% Download-task cisco-ftd-fp2k.7.0.0-94.SPA : transferring 598745 KB
% Download-task cisco-ftd-fp2k.7.0.0-94.SPA : transferring 1089310 KB
firepower-2110 /firmware # show download-task

Download task:
  File Name Protocol Server      Port   Userid   State
  -----
  cisco-ftd-fp2k.7.0.0-94.SPA
    Ftp    10.10.10.10      0 anonymous  Downloading

% Download-task cisco-ftd-fp2k.7.0.0-94.SPA : verifying image ...
% Download-task cisco-ftd-fp2k.7.0.0-94.SPA : completed successfully.
firepower-2110 /firmware # show download-task

Download task:
  File Name Protocol Server      Port   Userid   State
  -----
  cisco-ftd-fp2k.7.0.0-94.SPA
    Ftp    10.10.10.10      0 anonymous  Downloaded

firepower-2110 /firmware # show package
Name                               Package-Vers
-----
cisco-ftd-fp2k.7.0.0-94.SPA       7.0.0-94

firepower-2110 /firmware # scope auto-install
firepower-2110 /firmware/auto-install # install security-pack version 7.0.0-94 force

The system is currently installed with security software package not set, which has:
- The platform version: not set
If you proceed with the upgrade 7.0.0-94, it will do the following:
- upgrade to the new platform version 2.9.1.131
- install with CSP ftd version 7.0.0.94
During the upgrade, the system will be reboot

Do you want to proceed ? (yes/no):yes

This operation upgrades firmware and software on Security Platform Components
Here is the checklist of things that are recommended before starting Auto-Install
```

- (1) Review current critical/major faults
- (2) Initiate a configuration backup

Do you want to proceed? (yes/no):**yes**

Triggered the install of software package version 7.0.0-94

Force option: true

Install started. This will take several minutes.

For monitoring the upgrade progress, please enter 'show' or 'show detail' command.

firepower-2110 /firmware/auto-install # **show**

Firmware Auto-Install:

Package-Vers	Oper State	Upgrade State
6.3.0-83	Scheduled	Ready

firepower-2110 /firmware/auto-install # **show**

Firmware Auto-Install:

Package-Vers	Oper State	Upgrade State
6.3.0-83	Scheduled	Validating Images

...

Sending ALL processes the KILL signal ...

Deactivating swap...

Unmounting local filesystems...

Rebooting... [762.611590] reboot: Restarting system

...

Firmware upgrade request encountered.

Scan for firmware elements that need to be updated...

Looking for file 'disk0:installables/switch/fxos-k8-fp2k-firmware.1006.0104.0213.SPA'

Located 'installables/switch/fxos-k8-fp2k-firmware.1006.0104.0213.SPA' @ cluster 11.

...

Upgrading the FPGA (Upgrade) image...

...

Programming new ROMMON: Succeed !

Copy the current configuration data to the upgrade Flash chip.

Rebooting to allow this active ROMMON to test launch the new image...

...

Waiting for Application infrastructure to be ready...

Verifying the signature of the Application image...

May 20 13:04:12 firepower-2130 kernel: [4.236271] Disabling IRQ #16

May 20 13:04:22 firepower-2130 FPRM: <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>

[F1309][critical][default-infra-version-missing][org-root/fw-infra-pack-default] Bundle version in firmware package is empty, need to re-install

May 20 13:05:22 firepower-2130 FPRM: <<%FPRM-2-EQUIPMENT_MISSING>> [F0709][critical][equipment-missing][sys/chassis-1/psu-2] Power supply 2 in chassis 1 presence: missing

May 20 13:05:52 firepower-2130 FPRM: <<%FPRM-2-DEFAULT_INFRA_VERSION_MISSING>>

[F1309][cleared][default-infra-version-missing][org-root/fw-infra-pack-default] Bundle version in firmware package is empty, need to re-install

Threat Defense System: CMD=-install, CSP-ID=cisco-ftd.7.0.0.94__ftd_001_JMX2125Y165NBI5MT1, FLAG="

System begins installation ...

cisco ftd installation finished successfully.

Verifying signature for cisco-ftd.7.0.0.94 ...

Verifying signature for cisco-ftd.7.0.0.94 ... success

Threat Defense System: CMD=-start, CSP-ID=cisco-ftd.7.0.0.94__ftd_001_JMX2125Y165NBI5MT1, FLAG="

System starting ...

Registering to process manager ...

Cisco FTD started successfully.

12.3 REIMAGEN DE EQUIPOS FIREPOWER 4100/9300

Para realizar este proceso necesitamos conectarnos tanto por consola al equipo como por IP al interfaz de gestión fuera de banda.

Necesitaremos un PC con un servidor TFTP y, preferiblemente, también FTP. Descargaremos las imágenes desde la web de Cisco, que se encuentran en el modelo correspondiente, apartado “Firepower Extensible Operating System”. Necesitaremos 4 imágenes, la “kickstart”, la “manager”, la “system” y la completa (solo con número de versión).

El proceso puede tardar entre 20 y 40 minutos.

Se empieza arrancando el equipo en rommon e iniciando la carga de la imagen de arranque “kickstart” a través de protocolo TFTP.

```
!! Rommon image verified successfully !!

Cisco System ROMMON, Version 1.0.10, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Mon 11/30/2015 15:23:18.60 by builder
Current image running: Boot ROM0
Last reset cause: PowerOn
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR-4150-SUP with 8192 Mbytes of main memory
MAC Address: 38:90:a5:f2:34:cc

find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.4.61.131.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.4.61.131.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

rommon 1 > address 10.10.10.1
rommon 2 > netmask 255.255.255.0
rommon 3 > gateway 10.10.10.2
rommon 4 > boot tftp://10.10.10.2/fxos-k9-kickstart.5.0.3.N2.4.31.107.SPA
    ADDRESS: 10.10.10.1
    NETMASK: 255.255.255.0
    GATEWAY: 10.10.10.2
    SERVER: 10.10.10.2
    IMAGE: fxos-k9-kickstart.5.0.3.N2.4.31.107.SPA

TFTP_MACADDR: 70:df:2f:43:4e:70

..
Receiving fxos-k9-kickstart.5.0.3.N2.4.31.107.SPA from 10.10.10.2
#####
#####
#####
#####
```

```
#####
#####
#####
#####
#####
#####
#####
#####
#####
#####
```

!! Kickstart Image verified successfully !!

```
[ 4.358281] physmap-flash physmap-flash.0: Could not reserve memory region
```

INIT: version 2.88 booting

•

•

•

```
switch boot)#
```

Ahora se debe proceder a transferir las 3 imágenes, “kickstart”, “manager” y “system”, preferiblemente por FTP, al almacenamiento del dispositivo. Se creará una copia del “manager” al fichero especial “nuova-sim-mgmt-nsg.0.1.0.001.bin” que suele ser un link que indica el arranque del sistema. Como en este modo no podemos realizar links, se hará como una copia.

Una vez realizadas las transferencias y copia, reiniciamos el sistema. El equipo volverá a rommon porque, en realidad, todavía no se ha realizado una instalación completa con la imagen global.

```
switch(boot)# config terminal
switch(boot)(config)# interface mgmt 0
switch(boot)(config-if)# ip address 10.10.10.1 255.255.255.0
switch(boot)(config-if)# no shutdown
switch(boot)(config-if)# exit
switch(boot)(config)# ip default-gateway 10.10.10.254
switch(boot)(config)# exit
```

Copy complete, now saving to disk (please wait)...

Enter username: **anonymous**

Copy complete, now saving to disk (please wait)...

Enter username: **anonymous**


```

Password:
Copy complete, now saving to disk (please wait)...

switch(boot)# copy bootflash:fxos-k9-manager.4.3.1.107.SPA bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
Copy complete, now saving to disk (please wait)...

switch(boot)# dir bootflash:
 58975232 Jan 01 2012 00:04:38 fxos-k9-kickstart.5.0.3.N2.4.31.107.SPA
441454268 Jan 01 2012 00:06:29 fxos-k9-manager.4.3.1.107.SPA
201923640 Jan 01 2012 00:05:46 fxos-k9-system.5.0.3.N2.4.31.107.SPA
   4096 Jan 01 2012 00:02:45 logs/
  16384 Sep 10 2018 14:56:35 lost+found/
441454268 Jan 01 2012 00:09:05 nuova-sim-mgmt-nsg.0.1.0.001.bin

switch(boot)# reload
This command will reboot this supervisor module. (y/n) ? y
[ 555.263532] reboot: Restarting system

```

En el siguiente paso se realiza un arranque del equipo utilizando como parámetros las imágenes “kickstart” y “system” (deben ser la misma versión) que en realidad obligará a hacer una configuración inicial del dispositivo.

```

!! Rommon image verified successfully !!

Cisco System ROMMON, Version 1.0.14, RELEASE SOFTWARE
Copyright (c) 1994-2017 by Cisco Systems, Inc.
Compiled Thu 08/24/2017 15:49:40.98 by builder
Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

Platform FPR-4140-SUP with 8192 Mbytes of main memory
MAC Address: 70:df:2f:43:4e:70

autoboot: Can not find autoboot file 'menu.lst.local'
          Or can not find correct boot string !!
rommon 1 > dir
Directory of: bootflash:\

01/01/12 12:09a <DIR>      4,096 .
01/01/12 12:09a <DIR>      4,096 ..
09/10/18 02:56p <DIR>    16,384 lost+found
01/01/12 12:02a <DIR>      4,096 logs
01/01/12 12:04a      58,975,232 fxos-k9-kickstart.5.0.3.N2.4.31.107.SPA
01/01/12 12:05a    201,923,640 fxos-k9-system.5.0.3.N2.4.31.107.SPA
01/01/12 12:06a    441,454,268 fxos-k9-manager.4.3.1.107.SPA
01/01/12 12:09a    441,454,268 nuova-sim-mgmt-nsg.0.1.0.001.bin
      4 File(s) 1,143,807,408 bytes
      4 Dir(s)

rommon 2 > boot fxos-k9-kickstart.5.0.3.N2.4.31.107.SPA fxos-k9-system.5.0.3.N2.4.31.107.SPA

```

!! Kickstart Image verified successfully !!

```
Linux version: 3.14.39ltsi (security@cisco.com) #1 SMP Fri Jan 19 15:57:16 PST 2018
[ 4.358051] physmap-flash physmap-flash.0: Could not reserve memory region
Usage: init {-e VAR[=VAL] | [-t SECONDS] {0|1|2|3|4|5|6|S|s|Q|q|A|a|B|b|C|c|U|u}}
INIT: version 2.88 booting
POST INIT Starts at Sun Jan 1 00:13:40 UTC 2012
S10mount-ramfs.supnuovaca Mounting /isan 2500m
Mounted /isan
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
Platform is BS or QP MIO: 31
FPGA Version 0x00010600 FPGA Min Version 0x00000600
lspci: Unable to load libkmod resources: error -12
Checking all filesystems..r.r.r.r done.
Warning: switch is starting up with default configuration
Checking NVRAM block device ... done
.
FIPS power-on self-test passed
Unpack CMC Application software
1
Loading system software
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.31.107.SPA
```

```
Manager image digital signature verification successful
C
12+1 records in
12+1 records out
9618 bytes (9.6 kB) copied, 0.000103714 s, 92.7 MB/s
enabling snm mode on CA
springfield first bring-up done for CA
rm: cannot remove '/mnt/pss/bcm_hw_port_mode': No such file or directory
INIT: Entering runlevel: 3
cmcmmon: 159:cmclog_setlevel_modu
```

enabled fc feature

```
2012 Jan 1 00:16:01 %$ VDC-1 %$ %USER-2-SYSTEM_MSG: CLIS: loading cmd files begin - clis
2012 Jan 1 00:16:09 %$ VDC-1 %$ %USER-2-SYSTEM_MSG: CLIS: loading cmd files end - clis
2012 Jan 1 00:16:09 %$ VDC-1 %$ %USER-2-SYSTEM_MSG: CLIS: init begin - clis
[ 161.296689] 2012 Jan 1 00:16:13 %$ VDC-1 %$ Jan 1 00:16:13 %KERN-0-SYSTEM_MSG: [ 161.296689] <3>[
161.587657] bcm_usd/4979 - No matching bus/addr for dev NUOVA_I2C_DF410 inst 0 - kernel
System is coming up ... Please wait ...
System is coming up ... Please wait ...
System is coming up ... Please wait ...
System is coming up ... Please wait ...
System is coming up ... Please wait ...
System is coming up ... Please wait ...
System is coming up ... Please wait ...
2012 Jan 1 00:17:06 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: Starting bcm_attach, unit 0 - bcm_usd
System is coming up ... Please wait ...
System is coming up ... Please wait ...
System is coming up ... Please wait ...
2012 Jan 1 00:17:20 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: Finished bcm_attach..., unit 0 - bcm_usd
2012 Jan 1 00:17:22 %$ VDC-1 %$ %USER-0-SYSTEM_MSG: Enabling Filter on CPU port - bcm_usd
System is coming up ... Please wait ...
System is coming up ... Please wait ...
2012 Jan 1 00:17:29 %$ VDC-1 %$ %VDC_MGR-2-VDC_ONLINE: vdc 1 has come online
System is coming up ... Please wait ...
```

```
nohup: appending output to 'nohup.out'
```

```
---- Basic System Configuration Dialog ----
```

This setup utility will guide you through the basic configuration of the system. Only minimal configuration including IP connectivity to the Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system.
To back track or make modifications to already entered values, complete input till end of section and answer no when prompted to apply configuration.

You have chosen to setup a new Security Appliance. Continue? (y/n):

Una vez realizada la configuración inicial, se necesita instalar la imagen completa de FXOS. La transferiremos, preferiblemente por FTP, y la instalaremos utilizando auto-install y activación.

```

%$ VDC-1 %$ %FPRM-2-DEFAULT_PLATFORM_VERSION_MISSING: [F1595][critical][default-plaform-version-missing][org-root/fw-platform-pack-default] Platform version is empty in platform firmware package

```

```
test-A# scope firmware
```

```
test-A /firmware # download image ftp://anonymous@10.10.10.2/fxos-k9.2.3.1.99.SPA
```

```
Password:
```

```
Please use the command 'show download-task' or 'show download-task detail' to check download progress.
```

```
test-A /firmware # show download-task
```

```
Download task:
```

File Name	Protocol	Server	Port	Userid	State

fxos-k9.2.3.1.99.SPA					
Ftp	10.10.10.2		0	anonymous	Downloading

```
test-A /firmware # show download-task
```

```
Download task:
```

File Name	Protocol	Server	Port	Userid	State

fxos-k9.2.3.1.99.SPA					
Ftp	10.10.10.2		0	anonymous	Downloaded

```
test-A /firmware # show package
```

Name	Version

fxos-k9.2.3.1.99.SPA	2.3(1.99)

```
test-A /firmware # scope auto-install
```

```
test-A /firmware/auto-install # install platform platform-vers 2.3(1.99)
```

```
The currently installed FXOS platform software package is not set
```

```
INFO: There is no service impact to install this FXOS platform software 2.3(1.99)
```

This operation upgrades firmware and software on Security Platform Components

Here is the checklist of things that are recommended before starting Auto-Install

(1) Review current critical/major faults

(2) Initiate a configuration backup

Do you want to proceed? (yes/no):yes

Triggering Install-Platform with:

FXOS platform software package version 2.3(1.99)

Note: the upgrade status can be monitored with 'show firmware monitor' under system scope command executed

test-A /firmware/auto-install # **scope system**

test-A /system # **show firmware monitor**

FPRM:

Package-Vers: 2.3(1.99)

Upgrade-Status: Ready

Fabric Interconnect A:

Package-Vers: 2.3(1.99)

Upgrade-Status: Ready

Chassis 1:

Server 1:

Package-Vers: 2.3(1.99)

Upgrade-Status: Upgrading

test-A /system # **show firmware monitor**

FPRM:

Package-Vers: 2.3(1.99)

Upgrade-Status: Ready

Fabric Interconnect A:

Package-Vers: 2.3(1.99)

Upgrade-Status: Ready

Chassis 1:

Server 1:

Package-Vers: 2.3(1.99)

Upgrade-Status: Ready

test-A /firmware/auto-install # **top**

test-A# **scope fabric-interconnect a**

test-A /fabric-interconnect # **show firmware**

Fabric Interconnect A:

Running-Kern-Vers: 5.0(3)N2(4.31.107)

Running-Sys-Vers: 5.0(3)N2(4.31.107)

Package-Vers: 2.3(1.99)

Startup-Kern-Vers:

Startup-Sys-Vers:

Act-Kern-Status: Ready

Act-Sys-Status: Ready

Bootloader-Vers:

test-A /fabric-interconnect # **activate firmware kernel-version 5.0(3)N2(4.31.107) system-version 5.0(3)N2(4.31.107)**

Warning: When committed this command will reset the end-point

test-A /fabric-interconnect* # **commit-buffer**

test-A /fabric-interconnect # **show activate status**

Kernel-State: Activating

System-State: Activating

```

test-A /fabric-interconnect # show activate status
Kernel-State: Ready
System-State: Ready
test-A /fabric-interconnect # show firmware
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.31.107)
  Running-Sys-Vers: 5.0(3)N2(4.31.107)
  Package-Vers: 2.3(1.99)
  Startup-Kern-Vers: 5.0(3)N2(4.31.107)
  Startup-Sys-Vers: 5.0(3)N2(4.31.107)
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers:

test-A /fabric-interconnect # top
test-A# scope chassis 1
test-A /chassis # reboot no-prompt
Starting chassis reboot. Monitor progress with the command "show fsm status"
test-A /chassis #
Broadcast message from root@test-A (Sun Jan 1 01:56:09 2012):

All shells being terminated due to system /sbin/reboot
[ 1072.787266] writing reset reason 9,

```

Una vez reiniciado, el proceso de reimagen habrá concluido.

13. GESTOR FIREWALL MANAGEMENT CENTER (FMC)

El Firewall Management Center (FMC), conocido como Firepower Management Center, es el centro neural de la solución Firepower de Cisco. Desde él se realizan todas las tareas de configuración, monitorización visualización, análisis y realización de informes.

Una vez añadidos los dispositivos al gestor FMC, el acceso directo a los dispositivos solo es necesario para labores de solución de problemas (troubleshooting).

Cisco ofrece equipos físicos de FMC como “appliance” que pueden ser instalados en la red de Gestión solos o en alta disponibilidad.

Para despliegues pequeños, Cisco también ofrece el FMCv como una plataforma virtual que puede gestionar 25 o 300 equipos, dependiendo de la versión.

En los sucesivos apartados de este punto se van a desarrollar los puntos principales de la solución FMC.

13.1 EQUIPOS FÍSICOS FMC

Todos los equipos disponen de doble puerto de red (alta disponibilidad) para gestión fuera de banda, tamaño de 1U, con doble fuente de alimentación. Sus diferentes

especificaciones que determinan el número máximo de dispositivos que pueden gestionar. En esta tabla se relacionan los equipos con sus capacidades:

Rendimiento y Funcionalidad	FMC 1600	FMC 2600	FMC 4600
Número máximo de dispositivos gestionados	50	300	750
Número máximo de eventos IPS	30 million	60 million	300 million
Memoria	32 GB	64 GB	128 GB
CPU	1x Intel Xeon 4110	2x Intel Xeon 4110	2x Intel Xeon 4116
Espacio del almacenamiento de eventos	900 GB	1.8 TB	3.2 TB
Secure boot	Yes	Yes	Yes
Soporte RAID	RAID 1	RAID 5	RAID 6

13.1.1 CONFIGURACIÓN INICIAL

Aunque los equipos disponen de un puerto de consola serie, este no puede ser usado para la configuración inicial.

Se recomienda el uso de un portátil o PC directamente conectado por red al puerto de gestión fuera de banda del equipo. Es necesario configurar el equipo conforme a los siguientes parámetros:

- Dirección IP: 192.168.45.2
- Máscara: 255.255.255.0
- Ruta por defecto: 192.168.45.1

Una vez conectado se debe acceder al dispositivo a su dirección IP por defecto a través de HTTPS: <https://192.168.45.45>

Las credenciales por defecto son:

- Usuario: admin
- Contraseña: Admin123

La pantalla inicial pedirá los datos de configuración del equipo:

- Change Password

Cambiar contraseña del usuario “admin”.

- Network Settings
Establece la dirección IP, ruta por defecto, máscara, nombre de host, DNS.
- Time Settings
Configura la sincronización de tiempo (NTP).
- Recurring Rule Update Imports
Configura la actualización de reglas NGIPS. Se recomienda configurar más adelante.
- Recurring Geolocation Updates
Configura la actualización de información de geolocalización. Se recomienda configurar más adelante.
- Automatic Backups
Configura las copias de seguridad recurrentes. Se recomienda configurar más adelante.
- License Settings y Device Registration
Gestión de licencias. No es aplicable en equipos FTD.
- End User License Agreement
Acuerdo de licencia que hay que aceptar.

Una vez configurados los parámetros correctamente, desconectaremos el PC y conectaremos el equipo al puerto correspondiente dentro de la red de gestión.

Se recomienda que el FMC esté en la misma red/VLAN que los dispositivos a gestionar.

13.2 EQUIPOS VIRTUALES FMCv

Los gestores FMC virtuales (FMCv) pueden gestionar 25 o 300 dispositivos, dependiendo de la versión usada.

Se deben adquirir las licencias correspondientes de los dispositivos a gestionar.

Actualmente el gestor virtual FMCv está disponible para hipervisores e infraestructuras en la nube: VMware, KVM, AWS, Azure, GCP, OCI.

Los requisitos de los tipos de máquina virtual FMCv son:

Rendimiento y Funcionalidad	FMCv	FMCv300
Número máximo de dispositivos gestionados	25-10-2	300
Número máximo de eventos IPS	10 million	60 million

Rendimiento y Funcionalidad	FMCv	FMCv300
Memoria	32 GB	64 GB
CPU	4/8 vCPUs	32 vCPUs
Espacio en disco	250 GB	2.2 TB
Secure boot	Yes	Yes

Se recomienda utilizar almacenamiento SSD para tener una experiencia fluida en el gestor.

13.2.1 INSTALACIÓN Y CONFIGURACIÓN INICIAL EN VMWARE

El primer paso es descargar la imagen desde la web de Cisco, dentro de la sección “Downloads Home/Security/Firewalls/Firewall Management/Firepower Management Center Virtual Appliance/Firepower Management Center Software”. Dentro de la versión base 7.0, se encuentran los ficheros con encabezados “FMCv: VMware install package for ESXi 6.5, 6.7, or 7.0” y “FMCv300. Seleccionar el que se desea descargar para instalar.

Se debe descomprimir el archivo, usando por ejemplo la herramienta 7Zip, y aparecerán una serie de ficheros, de los que debemos fijarnos en 2:

- Fichero ovf “VI”. Para despliegue con VCenter/VSphere (VI - Virtual Infrastructure).
- Fichero ovf “ESXi”. Despliegue para ESXi sin VCenter/VSphere.

Dependiendo del sistema de virtualización VMWare desplegado, se deberá usar uno u otro.

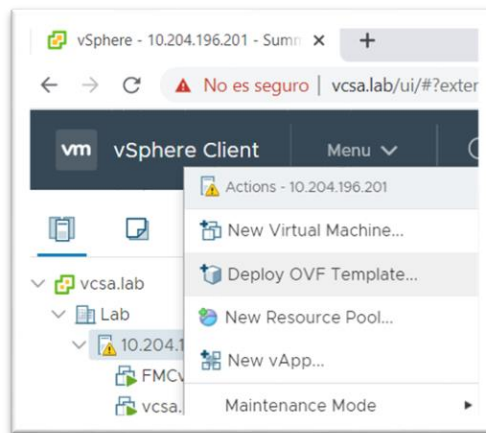
13.2.1.1 INSTALACIÓN Y CONFIGURACIÓN CON VCENTER/VSPHERE

Esta instalación es la más sencilla, puesto que el OVF tiene un asistente de configuración que realiza la configuración inicial a la vez que la instalación.

En esta instalación se debe usar el fichero “VI”. Ejemplo: “Cisco_Firepower_Mgmt_Center_Virtual_VMware-VI-7.0.0-94.ovf”

Dependiendo de la versión de VMWare usada los puntos o pantallas aquí expuestos pueden variar.

Se debe acceder al VCenter/VSphere y usar la opción “Deploy OVF template”.



Aquí es donde se debe seleccionar la imagen “VI” con extensión .ovf y el disco .vmdk, ambos, como “Local file” del PC que estemos usando para conectarnos al VCenter.

Deploy OVF Template

1 Select an OVF template

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

☐ URL

<http://remoteserver-address/filetoinstall.ovf>

☒ Local file

Elegir archivos 2 archivos

Cisco_Firepower_Mgmt_Center_Virtual_VMware-6.7.0-65-disk1.vmdk
Cisco_Firepower_Mgmt_Center_Virtual_VMware-VI-6.7.0-65.ovf

Se debe entrar el nombre que se asignará a la máquina virtual y el Datacenter donde se creará.

Deploy OVF Template

✓ **1 Select an OVF template**

2 Select a name and folder

Select a name and folder

Specify a unique name and target location

Virtual machine name: FMCv

Select a location for the virtual machine.

vcsla.lab
Lab

Se debe seleccionar un Host, o Cluster, donde se ejecutará la máquina.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select a compute resource
Select the destination compute resource for this operation

- Lab
- Cluster
 - 10.204.196.201

Revisión de detalles:

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Review details
Verify the template details.

Publisher	No certificate present
Product	Firepower Management Center Virtual
Version	6.7.0
Vendor	Cisco Systems, Inc.
Description	Cisco Firepower Management Center Virtual Cisco Systems, Inc. 170 West Tasman Dr San Jose, CA 95134 USA
Download size	2.4 GB
Size on disk	5.3 GB (thin provisioned) 250.0 GB (thick provisioned)

Una vez aceptada la licencia, se selecciona el almacenamiento para la máquina virtual. Se recomienda Thick Provision para mejorar el rendimiento.

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- ✓ 4 Review details
- ✓ 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Select storage
Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

Select virtual disk format: Thick Provision Lazy Zeroed

VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free	Type	Cluster
datastore1	1.81 TB	573.42 GB	1.28 TB	VMFS 6	

Compatibility
✓ Compatibility checks succeeded.

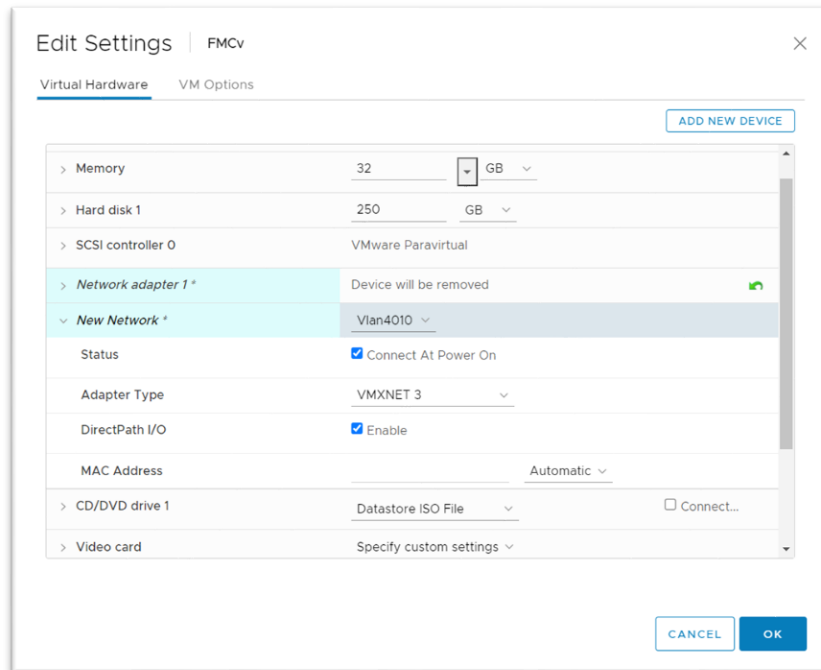
CANCEL BACK NEXT

Lo siguiente es seleccionar la red donde se conectará el interfaz de gestión.

Por último, la plantilla final permite asignar los datos de red y la contraseña.

Una vez terminado, accediendo vía HTTPS se solicitará el registro de la licencia del dispositivo mediante Smart Licensing.

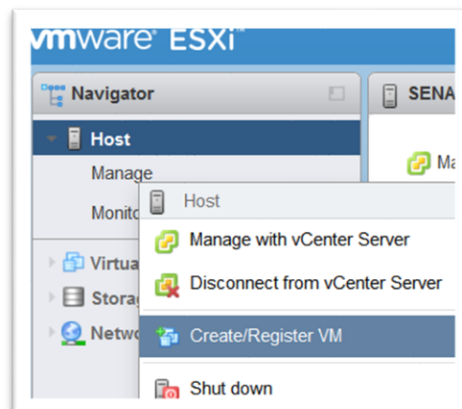
Nota: Se recomienda cambiar el tipo de interfaz de red de E1000 a VMXNET3. Para ello se debe apagar la máquina virtual, editar su configuración y luego volverla a arrancar.

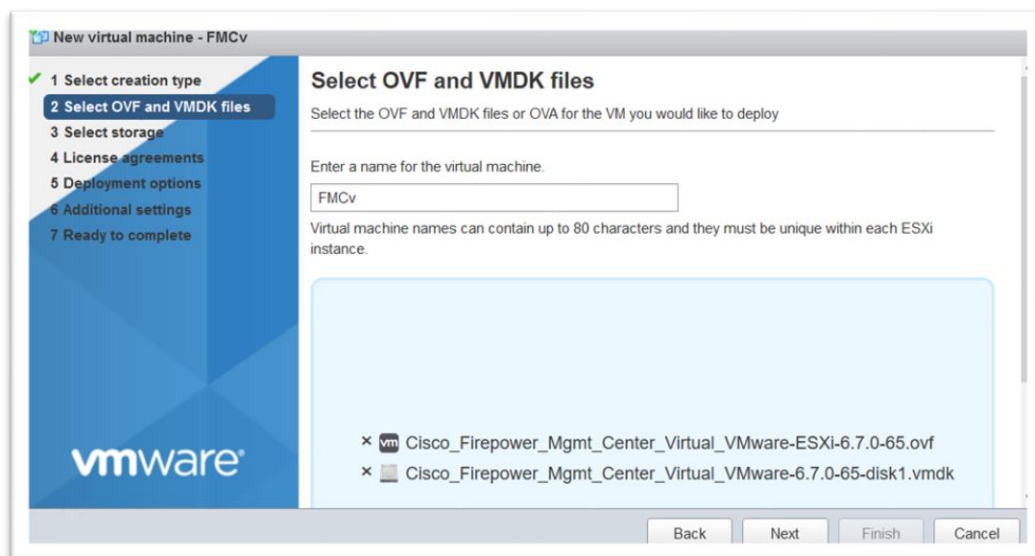
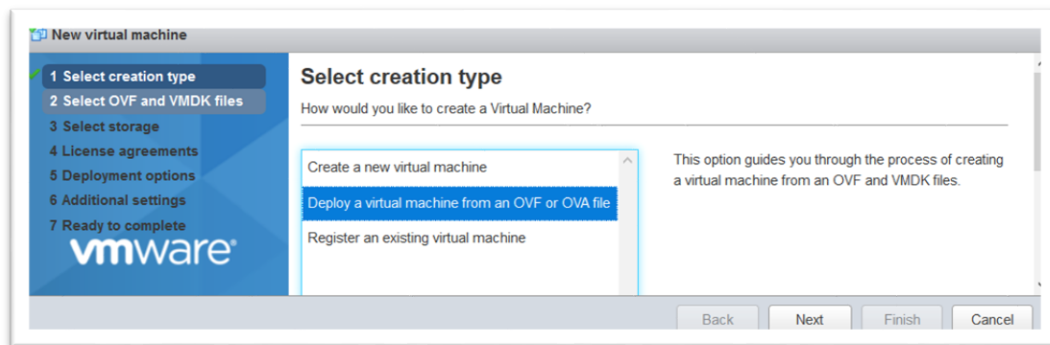


13.2.1.2 INSTALACIÓN Y CONFIGURACIÓN SIN VCENTER/VSPHERE

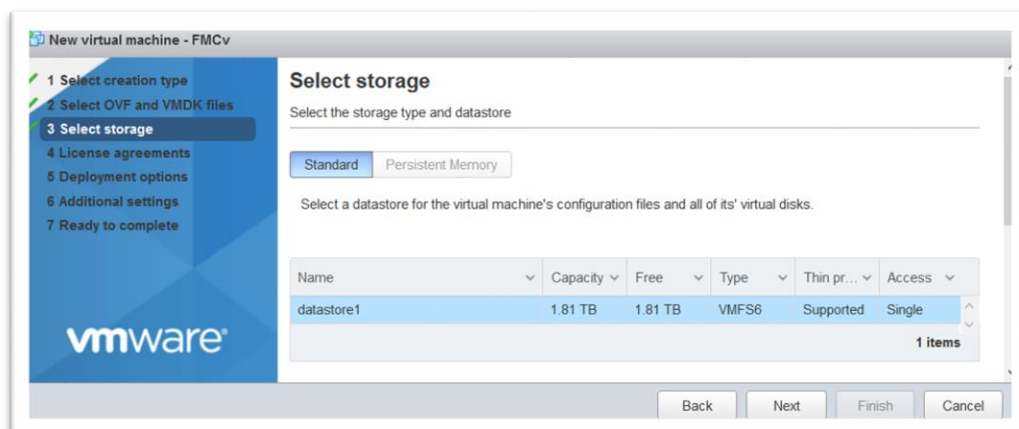
Este proceso se lleva a cabo en varios pasos. El primero consiste en la creación de la máquina virtual a través del OVF con nombre “ESXi”. Ejemplo: “Cisco_Firepower_Mgmt_Center_Virtual_VMware-ESXi-7.0.0-94.ovf”.

En la pantalla de selección de ficheros (Click to select files or drag/drop), se deben especificar los 2 ficheros, tanto el .ovf como el .vmdk.

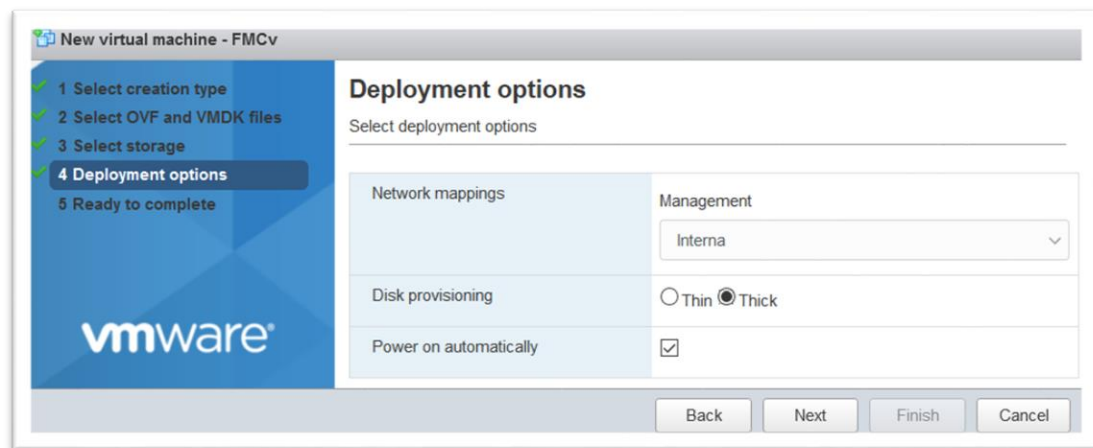




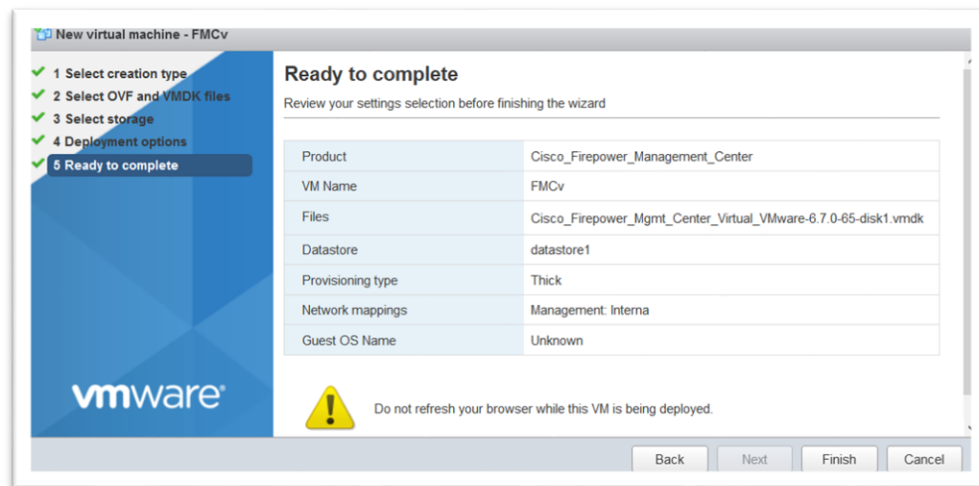
En la siguiente pantalla se debe seleccionar el almacenamiento. Debe contener suficiente espacio disponible conforme a los requisitos mencionados anteriormente.



Por último, se debe seleccionar la red correspondiente a la Gestión fuera de banda de los cortafuegos y el tipo de provisión del disco. Se recomienda “Thick” para un mejor rendimiento.



La Última pantalla muestra un resumen de la instalación que se va a realizar. Se deben comprobar los parámetros y si todo es correcto, se iniciará la instalación pulsando en “Finish”.



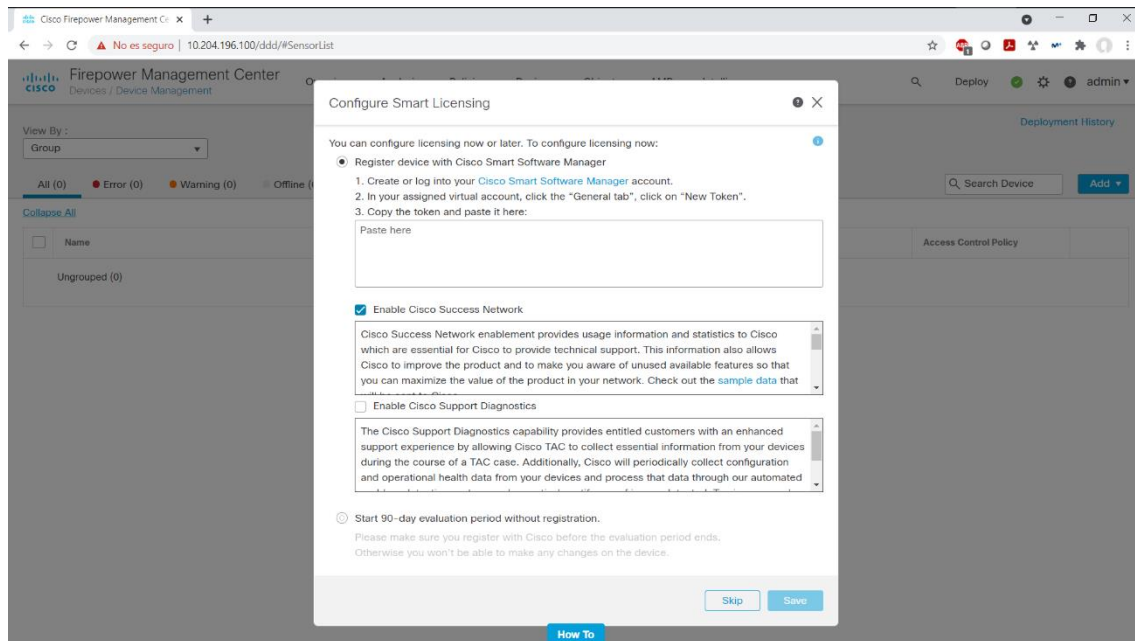
Comenzará el proceso de instalación. Una vez terminado, se debe abrir la consola KVM de la máquina virtual instalada. Si la instalación ha terminado el sistema estará pidiendo un “login”.

Las credenciales por defecto son:

- Usuario: admin
- Contraseña: Admin123

Pedirá que se acepte la licencia (EULA), pedirá una nueva contraseña y se solicitarán los datos de red para su configuración.

Una vez terminado, accediendo vía HTTPS se solicitará el registro de la licencia del dispositivo mediante Smart Licensing.



Nota: Se recomienda cambiar el tipo de interfaz de red de E1000 a VMXNET3. Para ello se debe apagar la máquina virtual, editar su configuración y volverla a arrancar.

13.2.2 INSTALACIÓN Y CONFIGURACIÓN INICIAL EN KVM

Como paso previo se debe descargar la imagen desde la web de Cisco, sección “Downloads Home/Security/Firewalls/Firewall Management/Firepower Management Center Virtual Appliance/Firepower Management Center Software”. Dentro de la versión base 7.0, se encuentra un fichero “qcow2” con descripción “FMCv: KVM install package”.

La instalación dependerá, en gran medida, de la distribución y sistema de virtualización en uso: RedHat Virtualization, Proxmox, virt-manager, qemu...

Se deberá copiar el fichero descargado al almacenamiento del sistema virtual.

El primer paso es crear la máquina virtual. Lo haremos usando la herramienta correspondiente de nuestra instalación, deben configurarse los siguientes parámetros:

- Tipo de Sistema Operativo: Linux 64 bits 2.6.25 o mayor.
- Memoria RAM: 32GB.
- CPUs: 4.

- Disco: usar Virtio con imagen importada formato qcow y seleccionar el fichero que se ha descargado.
- Red: se debe seleccionar la red de gestión, usando bridging o macvtap. Se recomienda que el gestor FMC y los dispositivos a manejar estén en el mismo rango IP y misma VLAN.

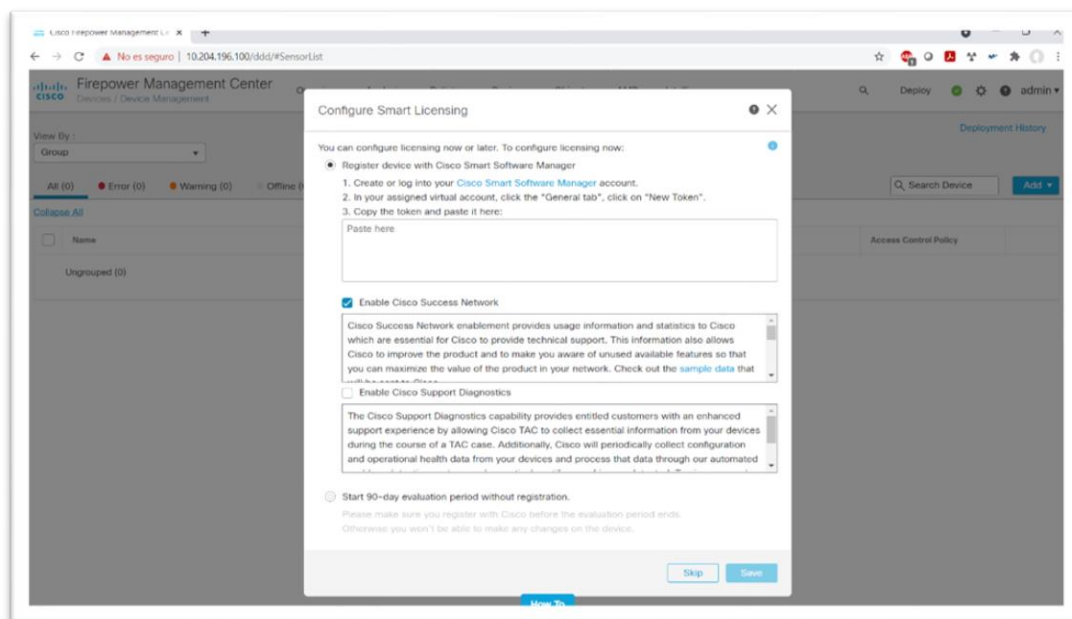
Una vez creada la máquina y encendida, se debe abrir la consola KVM de la máquina virtual instalada. Si la instalación ha terminado el sistema estará pidiendo un "login".

Las credenciales por defecto son:

- Usuario: admin
- Contraseña: Admin123

Pedirá que se acepte la licencia (EULA), pedirá una nueva contraseña y se solicitarán los datos de red para su configuración.

Una vez terminado, accediendo vía HTTPS se solicitará el registro de la licencia del dispositivo mediante Smart Licensing.

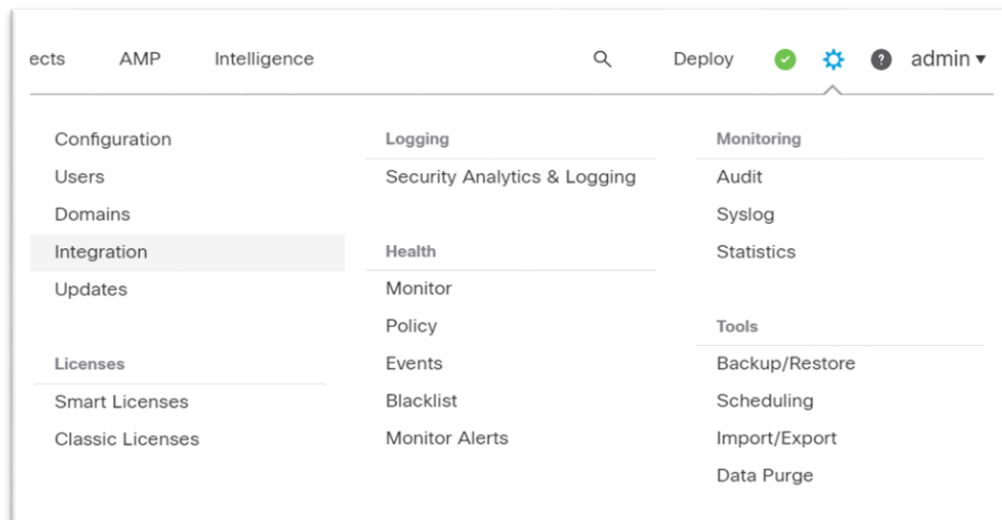


13.3 ALTA DISPONIBILIDAD FMC

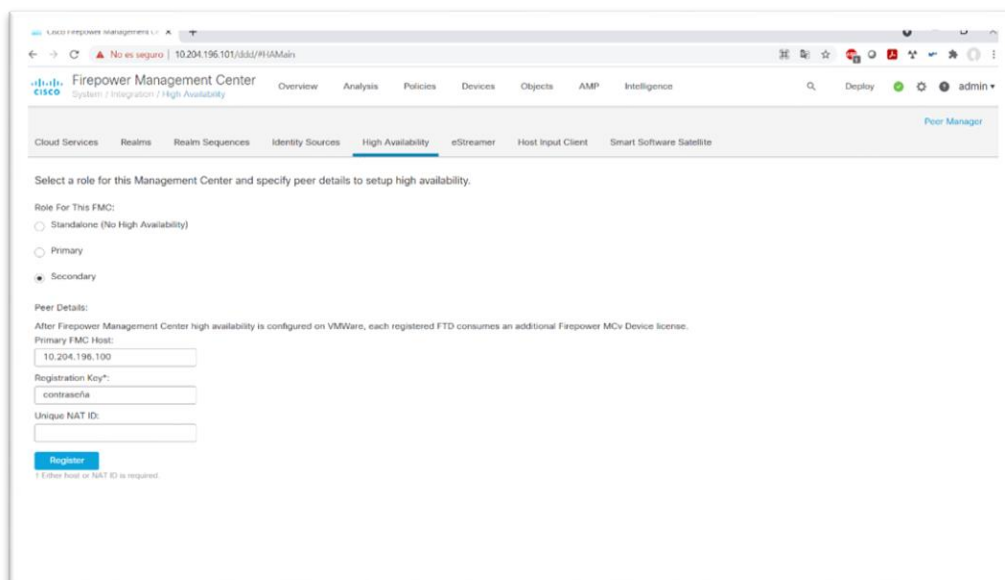
Tanto los equipos físicos, como algunos Firepower Management Center virtuales o en cloud (no todos), soportan alta disponibilidad activo/pasivo. La tabla de compatibilidad se debe consultar en la web de Cisco.

Para poder formar la alta disponibilidad, los modelos deben ser idénticos y corriendo la misma versión.

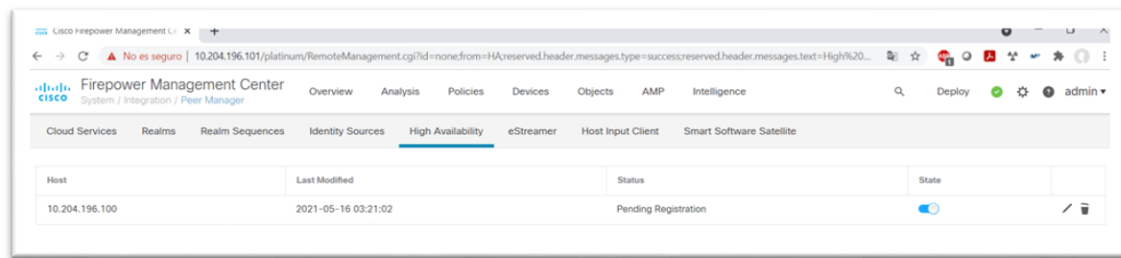
Accediendo al menú de “Integration”, se encuentra la pestaña de “High Availability”.



Se debe empezar primero por la configuración del secundario, o pasivo, configurando la dirección IP del primario, una contraseña compartida, y un NAT ID, opcional, que normalmente no se usa. Es para cuando existen varios dispositivos detrás de un mismo NAT (PAT) y, en ese caso, poder seleccionar la conexión correcta por el NAT ID.

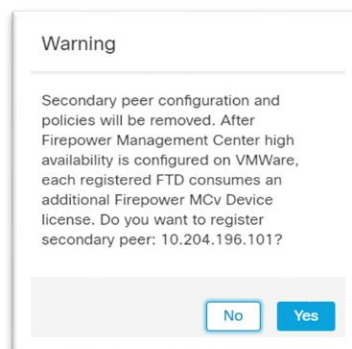
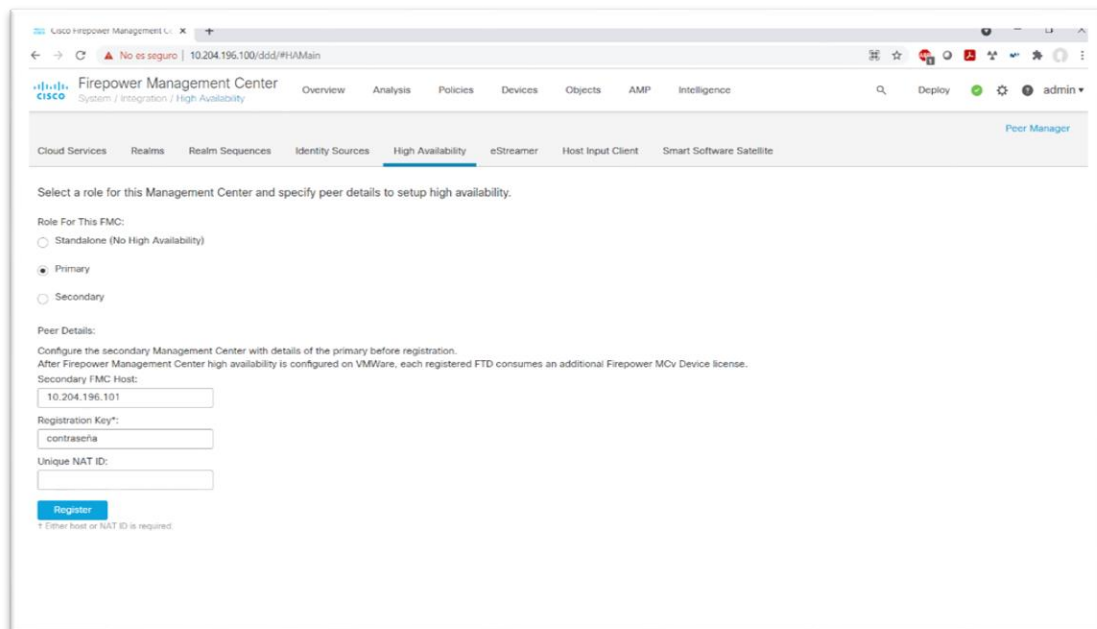


El equipo debe quedarse esperando a comunicarse con su primario.

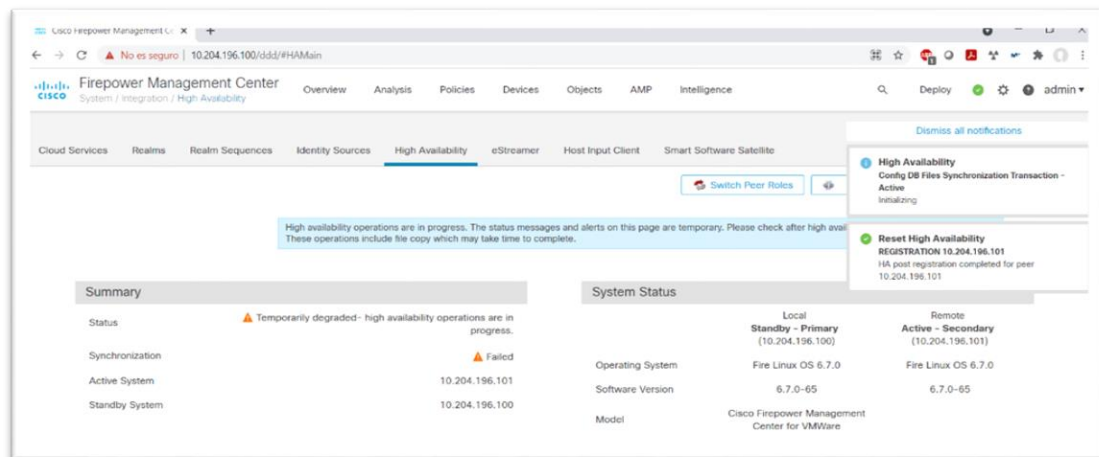


Hay que tener en cuenta que la configuración que quedará en los dos equipos será la del equipo primario/activo.

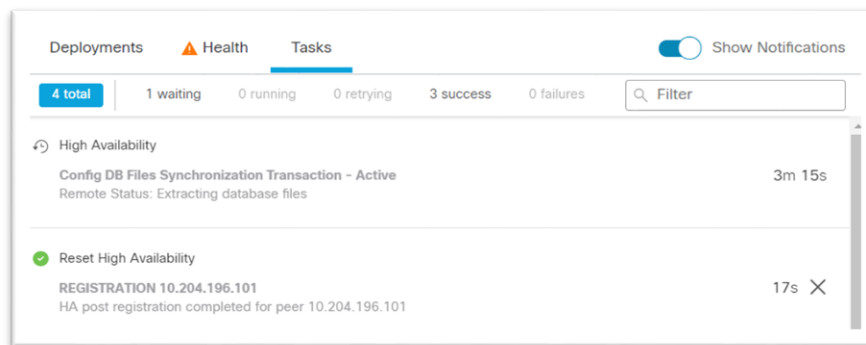
En el primario se realiza la misma operación.



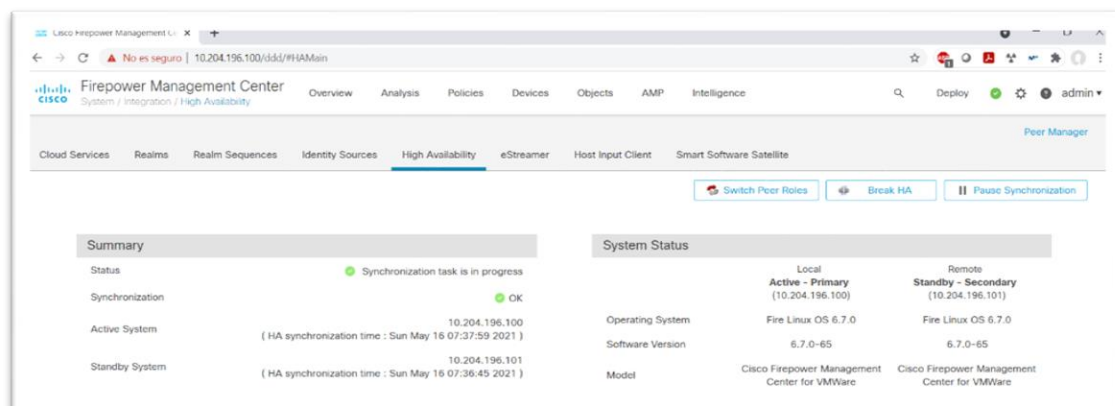
La sincronización empezará y los datos tardarán un tiempo en replicarse.



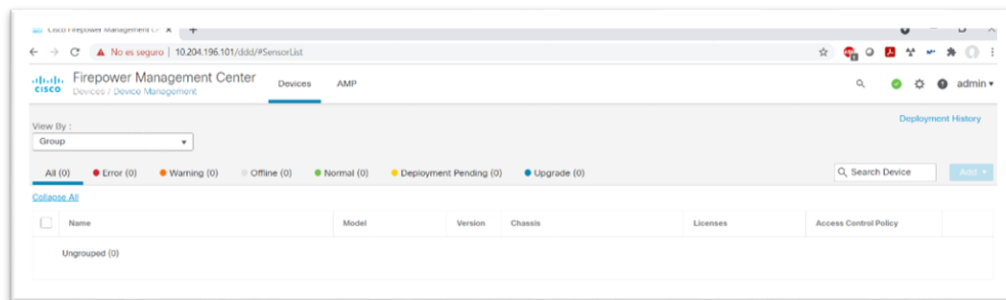
En tareas pueden verse las relacionadas con la alta disponibilidad y su estado.



Un estado correcto de sincronización se refleja así.

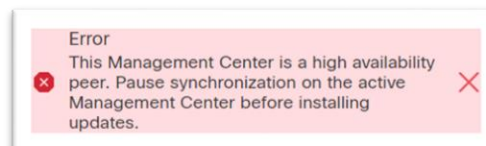


En el secundario desaparecen las opciones de configuración, dejando un menú mínimo.

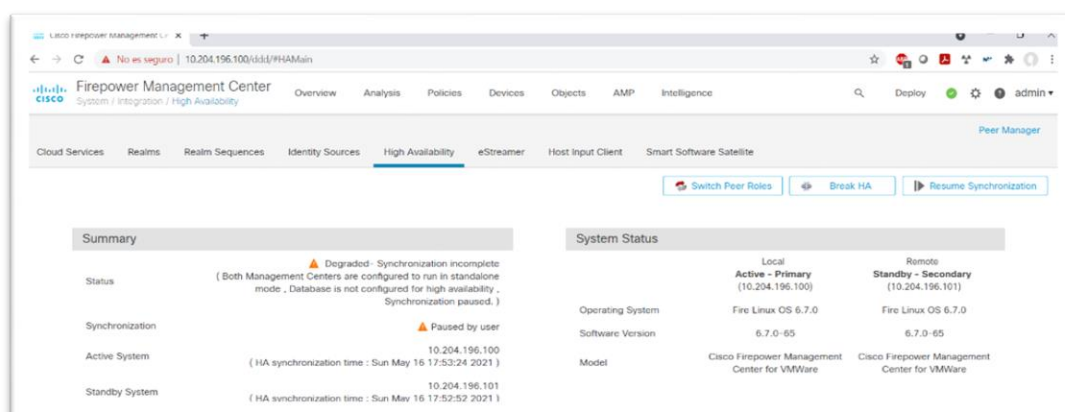
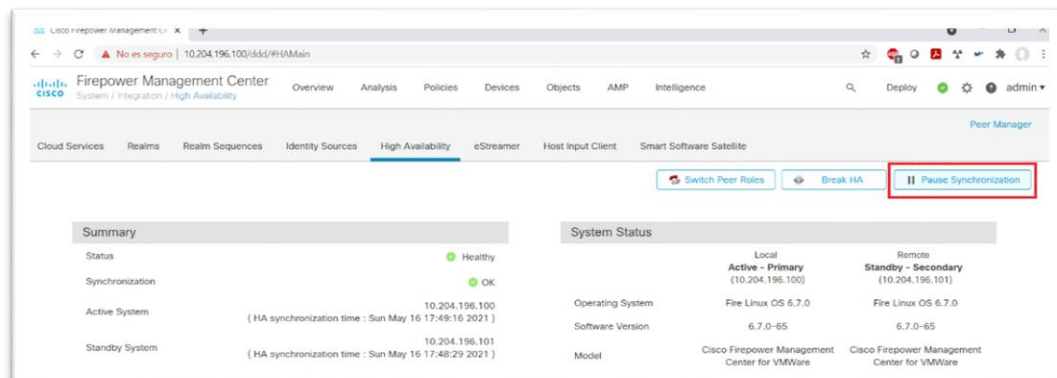


Las actualizaciones en un escenario FMC con alta disponibilidad deben seguir un procedimiento ordenado, si se intenta realizar una actualización normal, da error.

El procedimiento debe realizarse en una ventana de mantenimiento, donde no estará disponible la gestión de los cortafuegos a través de los FMC.



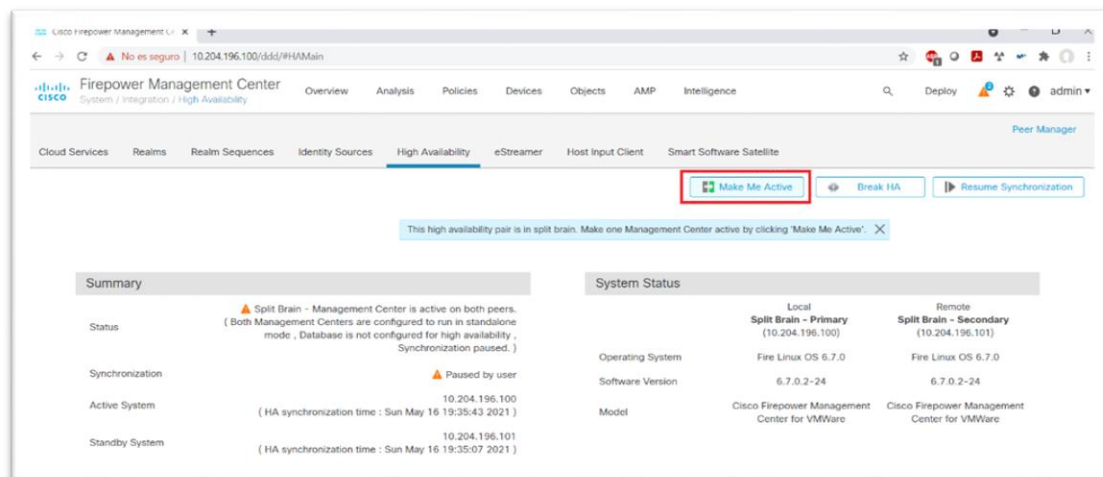
Primero, se debe entrar en el primario/activo y pausar la sincronización.



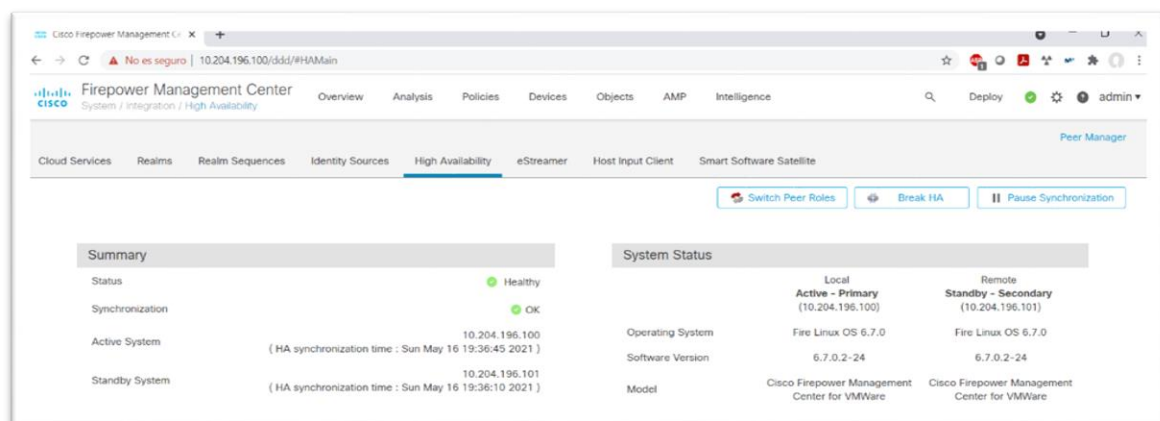
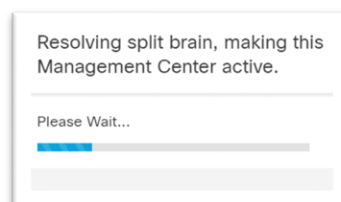
Segundo, se actualiza el FMC secundario/pasivo, entrando en el dispositivo y realizando una actualización normal, que dará avisos de “Split-brain” debido a la pausa de la sincronización entre FMCs.

Tercero, concluida esta actualización, se actualiza ahora el primario.

Una vez con los dos FMC actualizados, se debe decidir cual va a quedarse como activo/primario. Si se ha hecho en ventana de mantenimiento, sin cambios, será el mismo que estaba al inicio, sin embargo, si se han hecho cambios en el FMC secundario (primero que se actualiza) mientras el otro se actualizaba, ese deberá ser el nuevo primario, o esos cambios se perderían.



Una vez confirmada la elección el sistema reactiva la sincronización, empieza la transferencia y finaliza dejando la sincronización de manera correcta.



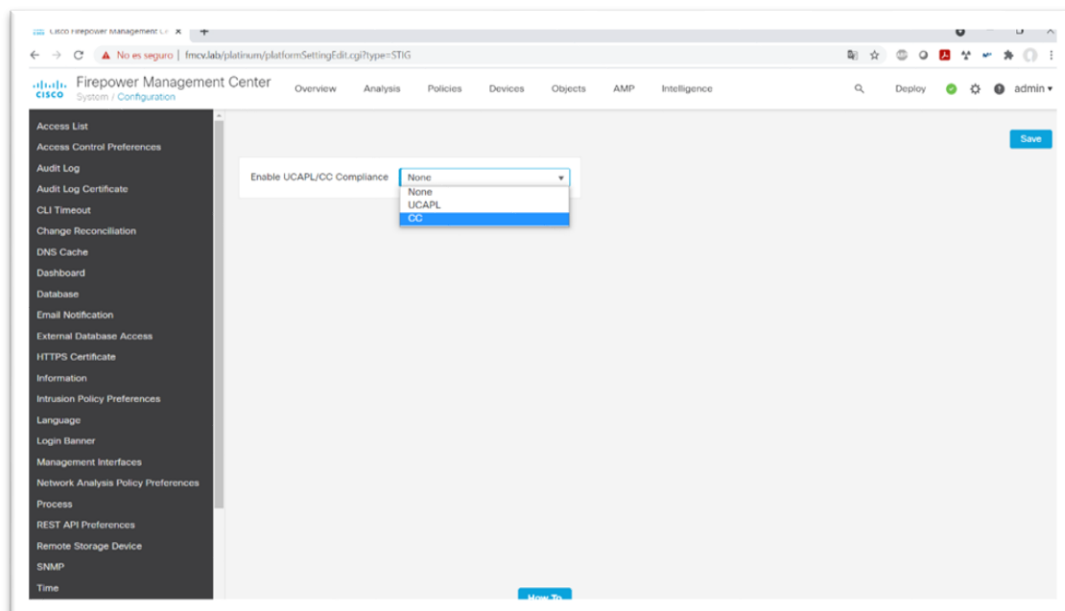
13.4 MODO COMMON CRITERIA

La primera configuración a realizar dentro del gestor es habilitar el modo Common Criteria. Este modo reconfigura el sistema para dar cumplimiento al CC, modificando cifrados, timeouts y otros parámetros.

Si se activa el modo Common Criteria, este no puede ser desactivado. Debiendo procederse a una reinstalación del sistema en tal caso.

Un gestor FMC en modo Common Criteria debe manejar dispositivos también operando en Common Criteria. No deben mezclarse instalaciones.

Para activar el modo se accede al gestor por HTTPS y en los menús System->Configuration->UCAPL/CC Compliance. Se debe seleccionar el modo y Save.



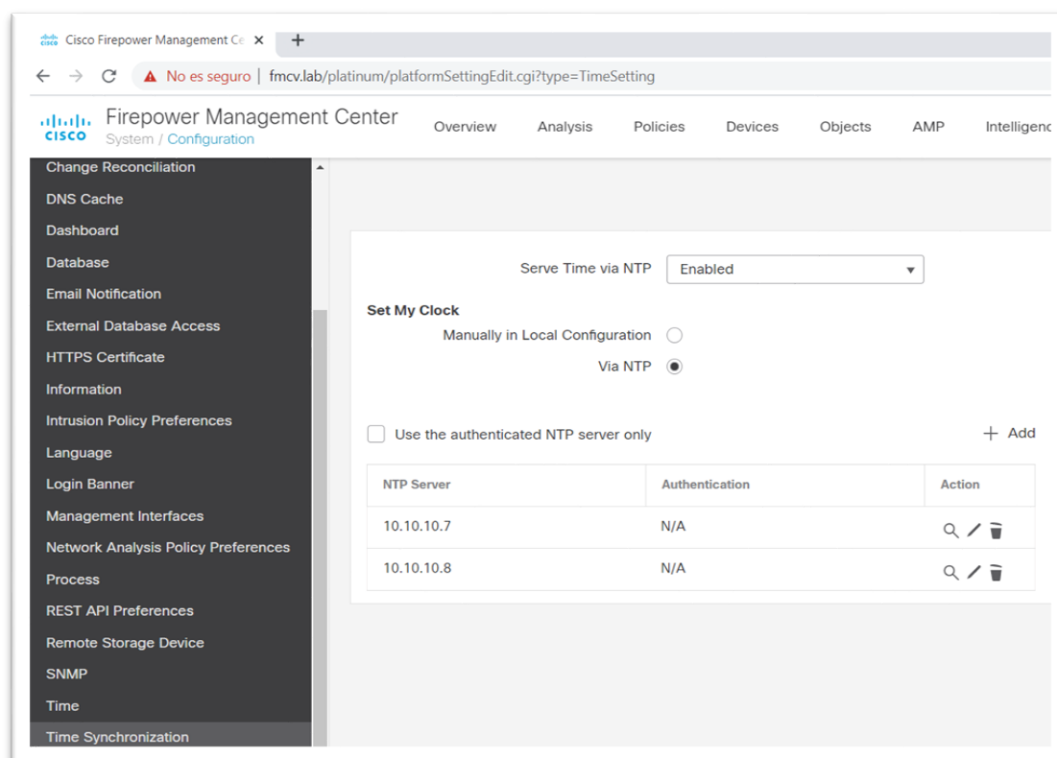
Una vez grabado el sistema se aplicarán los cambios y el equipo se reiniciará en modo Common Criteria.

13.5 SINCRONIZACIÓN DE HORA (NTP)

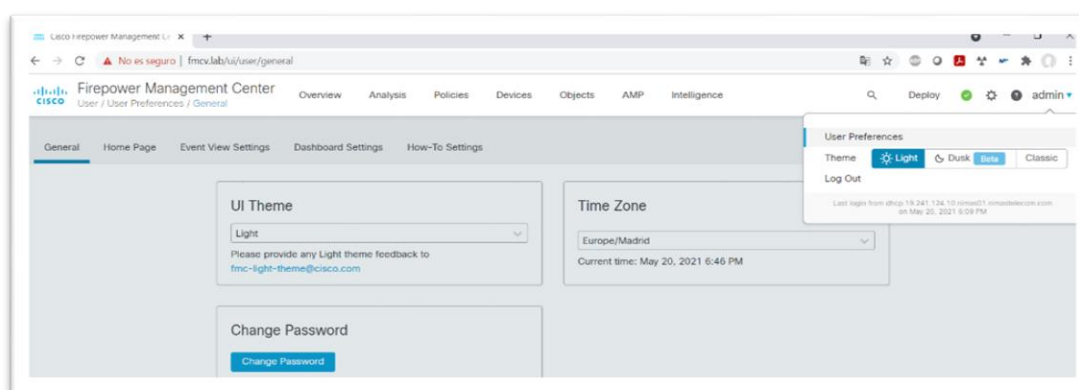
Por defecto, el sistema FMC usa los pooles de NTP para sincronización de hora. Sin embargo, estos pooles requieren que el equipo tenga acceso a Internet.

Se deberá modificar y seleccionar el servidor o servidores NTP de la red de Gestión.

El menú se encuentra en System->Configuration->Time Synchronization. Se pueden especificar varios servidores.



La hora se muestra en UTC, pero puede ser más conveniente que la información que consultemos y usemos en el gestor sea la local correcta, para ello hay que especificarlo por usuario. En USUARIO->User Preferences->Time Zone Preference podemos especificar nuestra zona horaria.

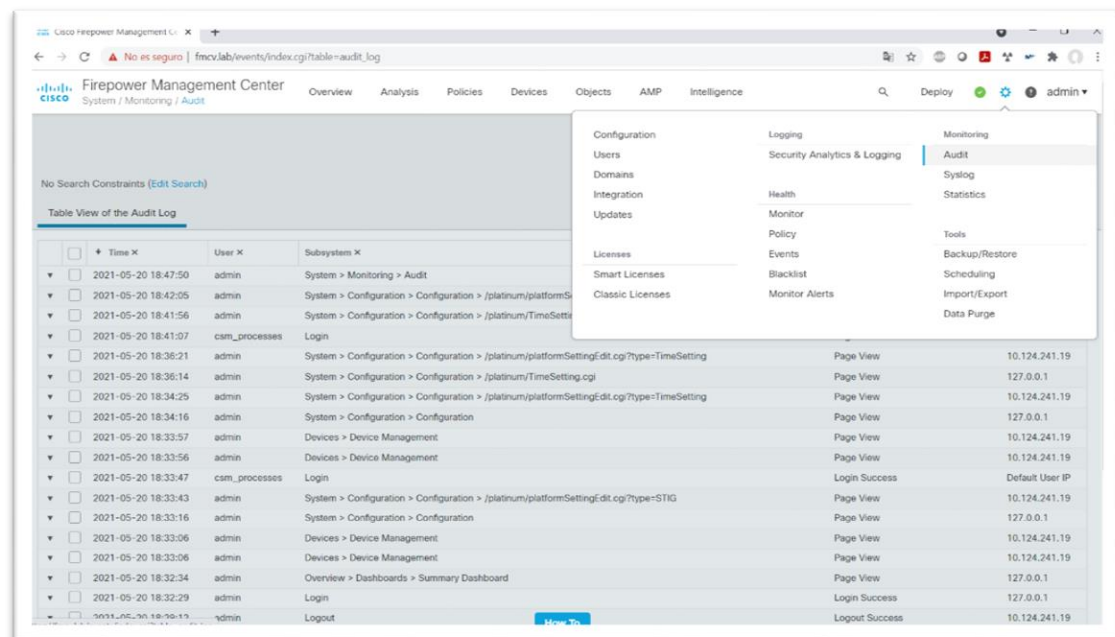


13.6 REGISTROS DE AUDITORÍA - AUDIT LOG

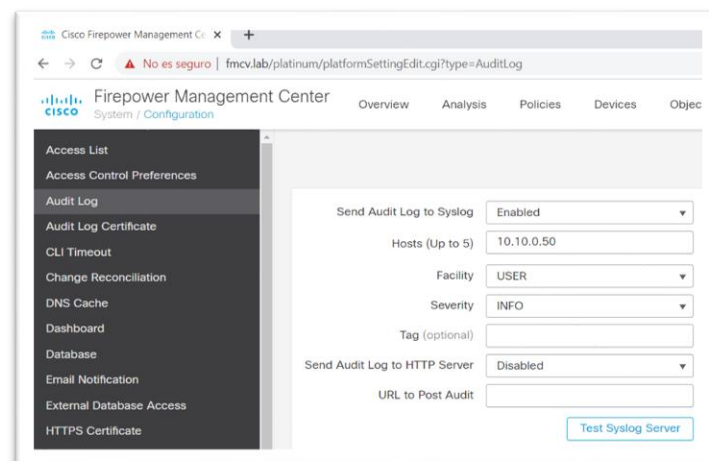
Los registros, o logs, de auditoría, responden a las preguntas de seguridad, ¿Quién? ¿Cuándo? ¿Qué? ¿Cómo?

Son registros de accesos y cambios realizados en una aplicación, en este caso el gestor FMC, donde se muestra el día y hora, el usuario, la acción concreta realizada y datos asociados. En el caso de un incidente de seguridad los registros de auditoría son vitales para un adecuado análisis forense. También son muy útiles si se necesita recordar que cambio se realizó y poder volver a revertirlo u obtener algún entendimiento sobre ello.

En FMC los registros de auditoría están habilitados por defecto y pueden ser consultados vía web usando el menú System-Monitoring->Audit.



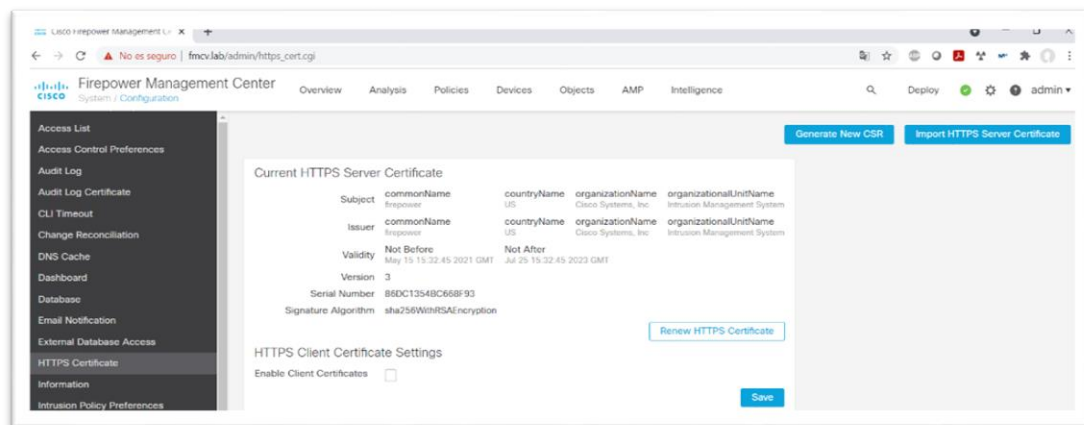
El sistema permite su envío a un Syslog externo y también a una web mediante HTTP POST con unos campos predefinidos. Se recomienda su habilitación y su envío a un servidor syslog externo, para ello se debe habilitar a través del menú System->Configuration->Audit Log.



13.7 INSTALACIÓN DE CERTIFICADO HTTPS

En la configuración inicial del dispositivo se genera un certificado auto-firmado para la conexión segura mediante protocolo HTTPS. Este certificado debe ser sustituido por uno de confianza (trusted) con una entidad de certificación (CA) de confianza.

Para generar la nueva llave privada y la petición de certificado es necesario conectarse al gestor por HTTPS y acceder al menú System->Configuration->HTTPS Certificate.



Se debe pinchar sobre “Generate New CSR” y rellenar los campos.

Generate Certificate Signing Request

Subject

Country Name (two-letter code)

State or Province

Locality or City

Organization

Organizational Unit (Department)

Common Name

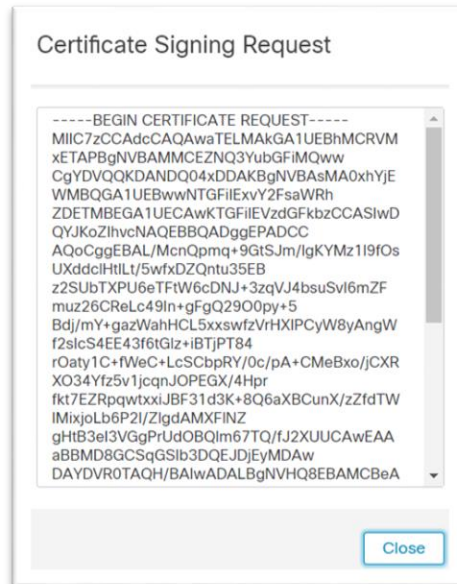
Subject Alternative Name

Domain Names

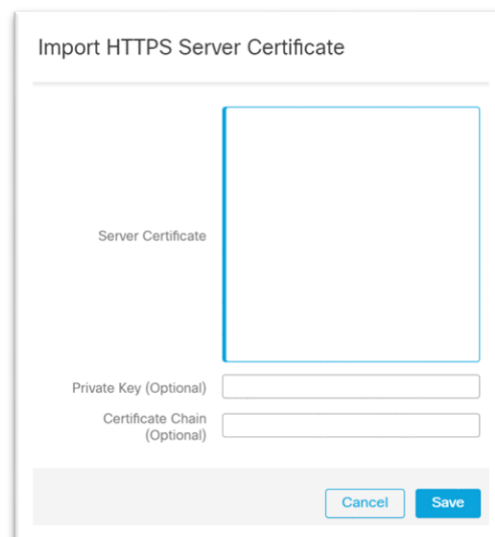
IP Addresses

Se obtendrá una solicitud de certificado en formato PEM que deberemos llevar a la autoridad certificadora para la obtención del certificado.

Se recomienda que la autoridad certificadora añada los campos SAN (Subject Alternative Name) para ambos, el nombre DNS y la IP.



Una vez obtenido el certificado deberemos importarlo pinchando sobre “Import HTTPS Server Certificate”. En el desplegable deberemos pegar el certificado en formato PEM y, adicionalmente, la cadena de certificación, certificado de la CA root e intermedia.



Si al importar el certificado el equipo devuelve el error “Basic constraints are not critical or not defined” es porque el FMC es estricto en cuanto a que el certificado generado debe contener la restricción “critical”:

X509v3 extensions:

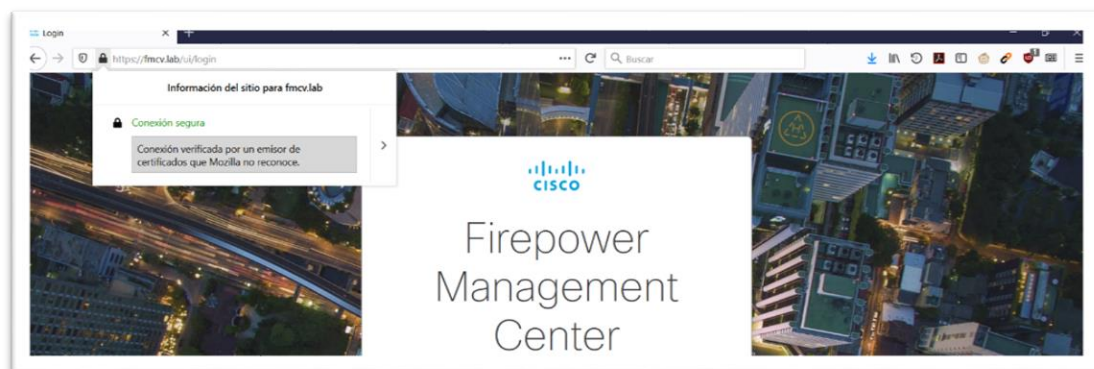
X509v3 Basic Constraints: critical

Se deberá generar un certificado con esa extensión.

En las versiones recientes de FMC este atributo ya no es requerido.

Una vez importado con éxito el certificado, se debe dar a SAVE para que el servicio se reinicie con el nuevo certificado.

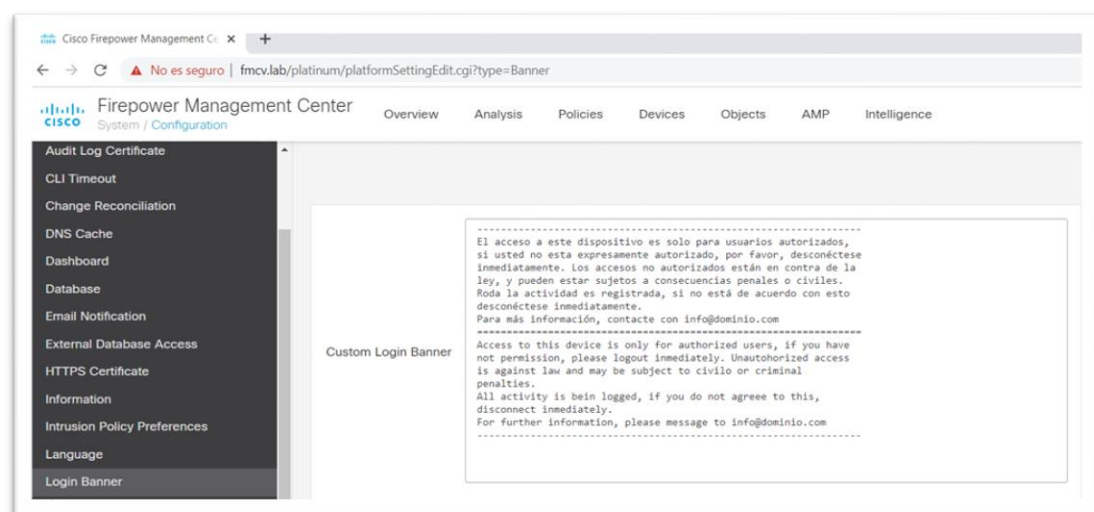
Se vuelve a acceder a la pantalla de login HTTPS y se verifica que el certificado es ahora correcto.



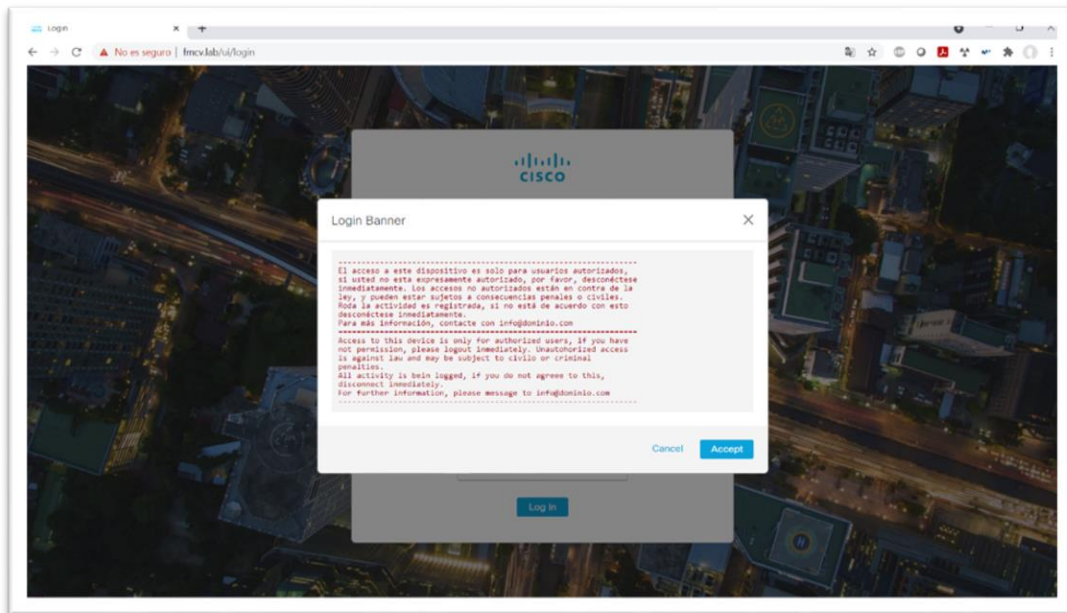
13.8 CONFIGURACIÓN DE BANNER

Es conveniente y requisito en ciertos entornos de seguridad la configuración de un banner de acceso.

Para configurarlo se debe acceder al gestor por HTTPS y al menú System->Configuration->Login Banner. Se introducirá el texto y se grabará.



Vía web, el banner es visible después de la pantalla de login.



13.9 GESTIÓN DE USUARIOS - RADIUS

La gestión de usuarios y permisos en FMC está basado en roles. A cada usuario se le asigna uno o más roles dentro de los roles definidos, que determinan lo que este puede hacer.

Existen una serie de roles predefinidos, pudiendo crear nuevos con mezcla de permisos.

Los diferentes roles principales son:

- **Administrator**
Es el de mayor privilegio. Lectura y escritura en todo el sistema. El usuario "admin" por defecto pertenece a este grupo.
- **Access Admin**
Da acceso a las ACP (Access Control Policy) y características asociadas en el menú de políticas. No pueden realizar Deploys.
- **Discovery Admin**
Permite acceso a Network Discovery, Application Detection y características de Correlación en el menú de políticas. No pueden realizar Deploys.
- **External Database User**
Provee de acceso solo-lectura a la base de datos del sistema Firepower, que soporta conexiones JDBC SSL. Para permitir aplicaciones de terceros

interactuar con la base de datos se debe habilitar primero el acceso mediante el menú de system settings.

- **Intrusion Admin**
Permite acceso a las políticas de intrusión (IPS), reglas de intrusión y network analysis. No pueden realizar Deploys.
- **Maintenance User**
Provee de acceso a características de monitorización y mantenimiento. Principalmente del menú Health.
- **Network Admin**
Permite administración de política de acceso ACP, inspección SSL, políticas DNS, políticas de identidad, así como a la configuración de características de dispositivos en el menú Devices. Pueden realizar Deploys.
- **Security Analyst**
Provee de acceso a las características de análisis de eventos de seguridad y acceso de solo lectura a eventos de Health, Overview, Análisis y menú System.
- **Security Analyst (Read Only)**
Provee de acceso de solo-lectura a las características de análisis de eventos de seguridad además de a eventos de Health, Overview, Análisis y menú System.
- **Security Approver**
Permite acceso limitado a las políticas de acceso ACP y network Discovery. Pueden visualizar y hacer Deploy de estas políticas, pero no hacer cambios.
- **Threat Intelligence Director (TID) User**
Provee de acceso al Threat Intelligence Director (si se encuentra activado). Estos usuarios pueden ver y configurar el TID.

Aunque es posible realizar una gestión de usuarios locales, se recomienda el uso de un sistema externo que provea de una política de gestión de contraseñas de acuerdo a las especificaciones en la guía CCN-STIC-301 y otras que sean de aplicación.

El sistema FMC permite autenticación mediante LDAP y Radius. En esta guía vamos a utilizar Radius por ser el sistema más ampliamente utilizado y su capacidad de logging. Cualquier Radius puede ser utilizado, citando los más comunes, Cisco ISE, FreeRadius, NPS.

Es posible integrar el Radius con un directorio activo que imponga una política de contraseñas (caducidad, bloqueo de reintentos, etc.), en ese caso se recomienda crear un grupo separado (por ejemplo “administradores”) y que solo se permita acceso a los miembros del dominio que pertenezcan a ese grupo.

Se debe configurar el servidor o servidores Radius a utilizar. Se recomienda establecer los reintentos a 3 y el tiempo de timeout a 3. Se recomienda especificar el Radius por IP, ya que en caso de fallo de resolución DNS provocaría timeouts y problemas de entrada al dispositivo. La clave (key) es el secreto compartido con el Radius.

La configuración se realiza en System->Users->External Authentication.

The screenshot shows the 'External Authentication Object' configuration page in the Cisco Firepower Management Center. The page is titled 'System / Users / Create External Authentication Object'. The configuration includes the following fields:

- Authentication Method:** RADIUS (selected from a dropdown)
- Name:** FP_RADIUS
- Description:** (empty field)
- Primary Server:**
 - Host Name/IP Address: 10.10.0.70
 - Port: 1812
 - RADIUS Secret Key: (empty field)
- Backup Server (Optional):**
 - Host Name/IP Address: 10.10.0.70
 - Port: 1812
 - RADIUS Secret Key: (empty field)
- RADIUS-Specific Parameters:**
 - Timeout (Seconds): 3
 - Retries: 3
 - Access Admin: (empty field)
 - Administrator: (empty field)

Para la asignación de roles a los usuarios se recomienda la asignación a través del Radius. El gestor FMC permite la asignación usando cualquier atributo. Se recomienda usar el atributo de Radius “Class” (25). En este ejemplo, se asigna el role “Administrator” al atributo Class con valor “Administrator”.

The screenshot shows the 'RADIUS-Specific Parameters' section of the configuration page. The fields are:

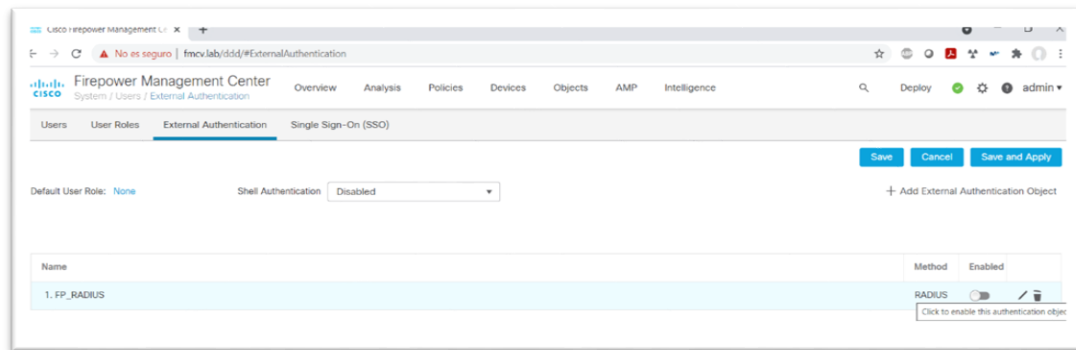
- Timeout (Seconds):** 3
- Retries:** 3
- Access Admin:** (empty field)
- Administrator:** (empty field)

Below the Administrator field, the text 'Class=Administrator' is visible, indicating the attribute being assigned.

Ejemplo de configuración en FreeRADIUS:

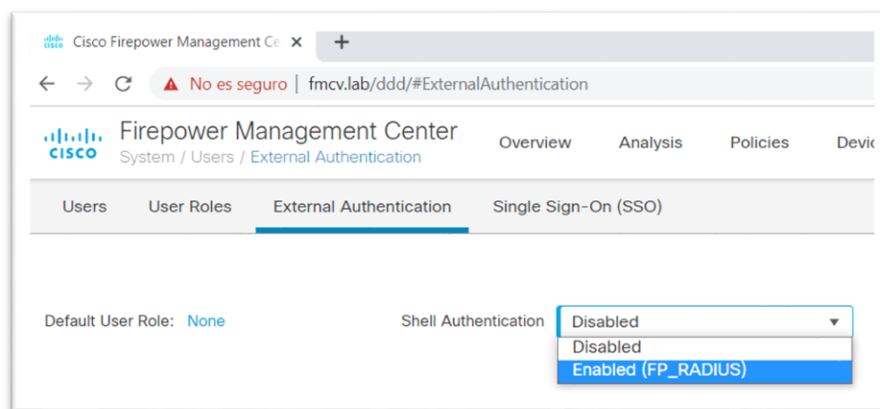
```
post-auth {
  update reply {
    Class = Administrator
  }
}
```

El siguiente paso es indicarle al sistema que debe usar el Radius para autenticar a los usuarios. Se realiza habilitando “Enabled”.



Importante. Una vez asignado el Radius, los usuarios locales, como “admin”, seguirán pudiendo ser utilizados. Se recomienda, dejar solo el usuario “admin” como local y ponerle una contraseña muy compleja que solo se use en caso de problemas de acceso. O bien, si se ha habilitado el modo Common Criteria, establecer el número de fallos de contraseña para bloqueo a 1 para el usuario “admin” y fallarlas para que se bloquee.

Para poder acceder con los usuarios de Radius al CLI/SSH del gestor FMC, se debe seleccionar en el campo “Shell Authentication” el Radius correspondiente.



Hay que recordar grabar con Save and Apply.

13.10 LICENCIAMIENTO – SMART LICENSING

El sistema de licenciamiento de los equipos Firepower, incluyendo el gestor FMC está basado en licenciamiento “en la nube”, Smart Licensing. Los equipos se registran, y acceden periódicamente, a través de Internet, con el sistema Smart Licensing para obtener y validar sus licencias.

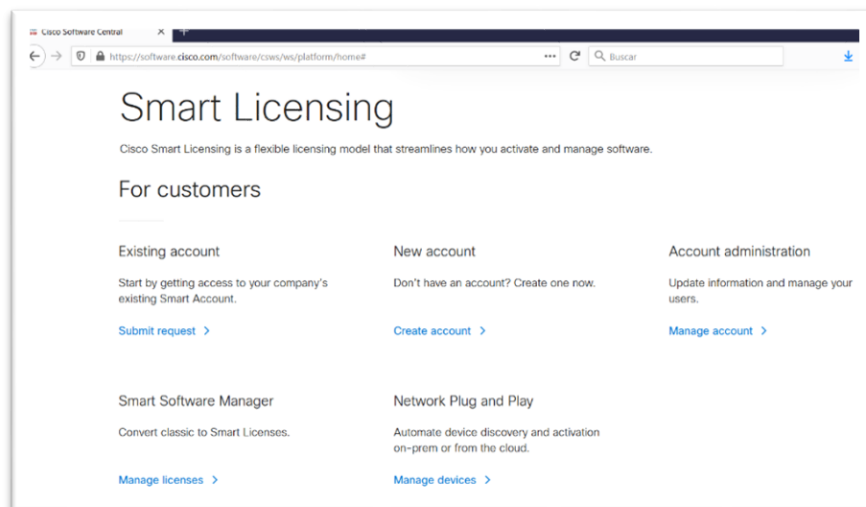
Para ello, el primer paso es obtener una Smart Account para la organización.

Se necesita darse de alta en la web de Cisco con el email corporativo.

Luego pulsar sobre el siguiente link:

<https://software.cisco.com/software/cswws/platform/home>

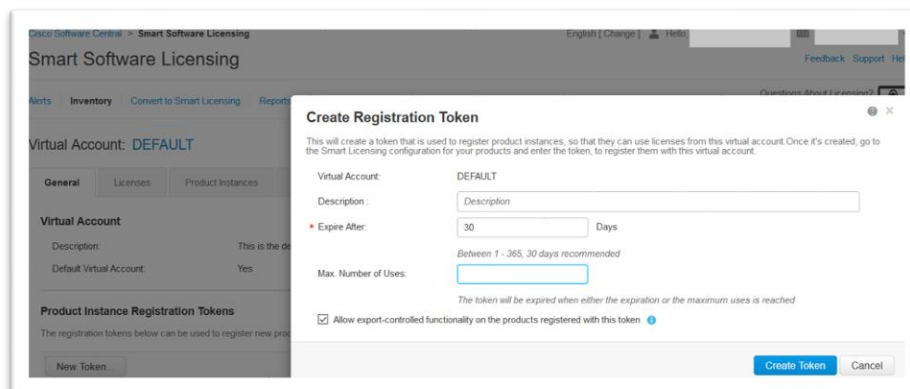
Siguiendo “New account” o “Existing account” se creará una nueva cuenta “Smart account” o se usará una pre-existente en tu perfil de Cisco.



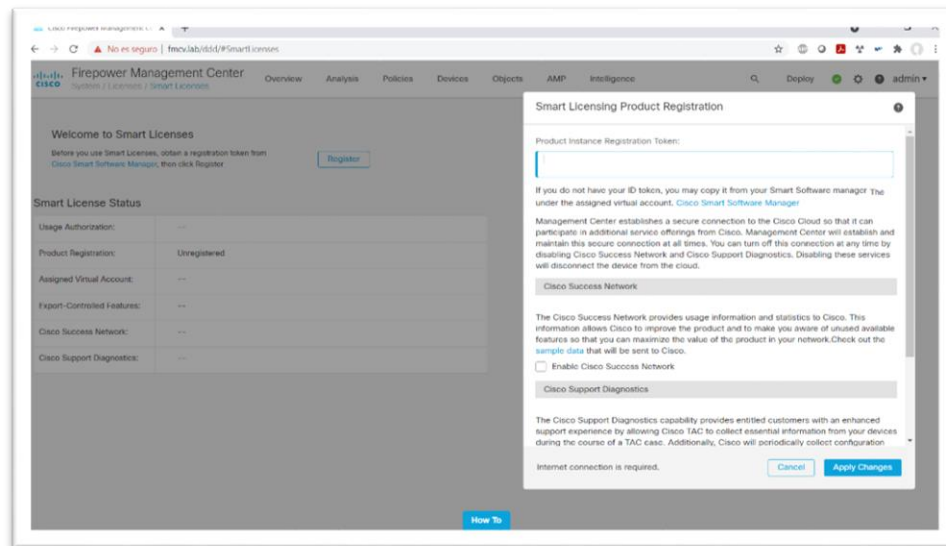
Siguiendo los pasos de los formularios se procederá a crear la cuenta. Cisco ha publicado un video explicativo sobre estos pasos:

<https://www.youtube.com/watch?v=1F7c1jifetuY>

Una vez obtenida la Smart Account, se debe generar un “token” desde la parte de gestión de Smart Licensing de Cisco.



El token generado debe copiarse en el FMC.

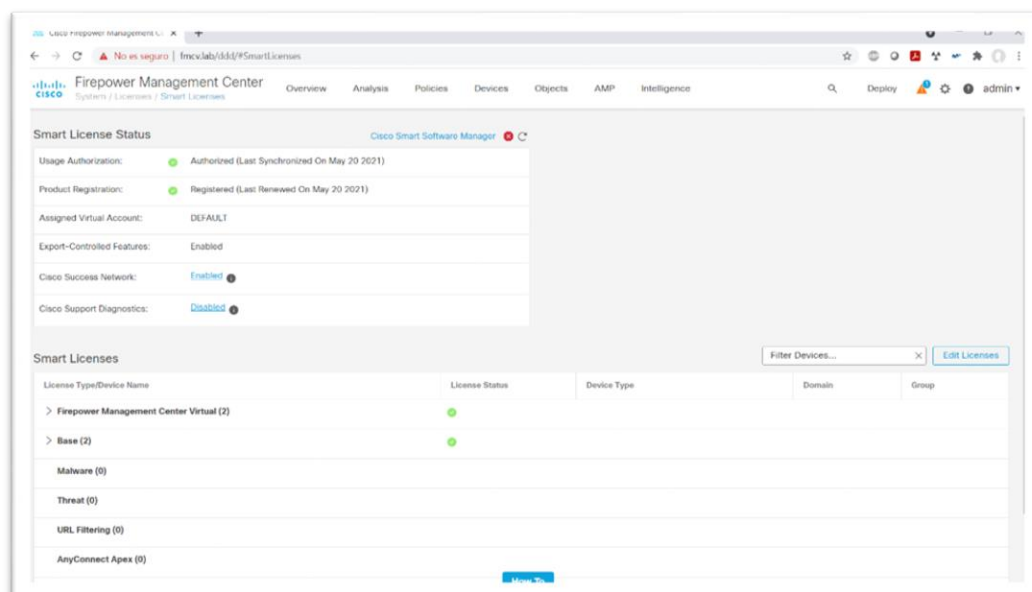


La opción de Cisco Success Network es opcional, lo que hace es enviar datos estadísticos de uso a Cisco Systems.

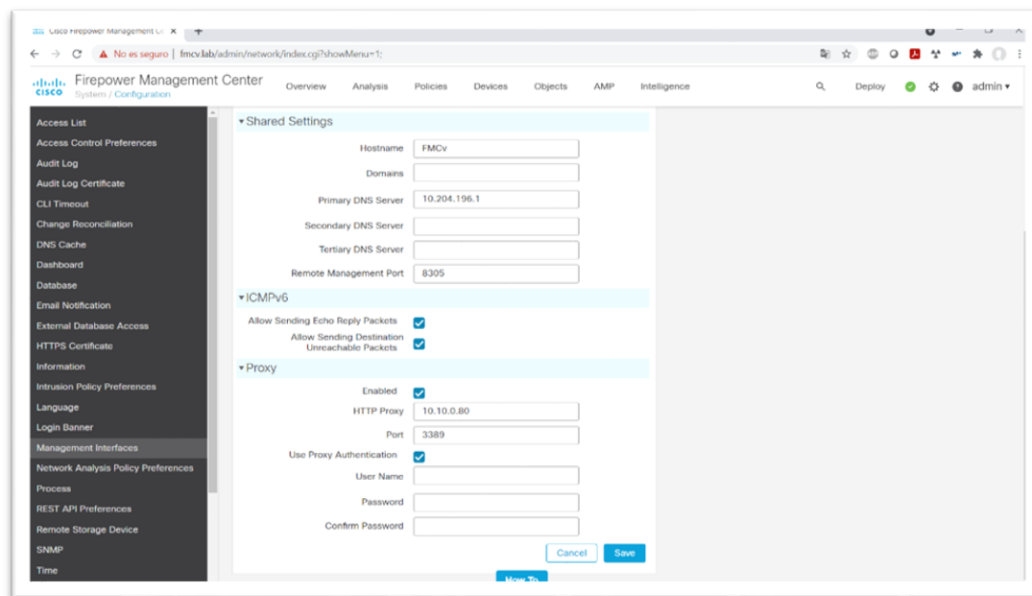
Una vez conectado, si es un FMC virtual se licenciará con el número de dispositivos que puede gestionar.

Aparecerán también licencias “Base” que son gratuitas y auto-generadas. Son para uso de cortafuegos con capacidad de filtrado y AVC.

Las licencias Threat (IPS), URL Filtering, Anyconnect (en todas sus modalidades), y Malware, aparecerán aparte.



En ocasiones será preferible el uso de un proxy en vez del acceso directo del FMC. Para ello se puede configurar a través del menú System->Configuration->Management Interfaces. Se habilitará la opción de proxy y se introducirán los parámetros.



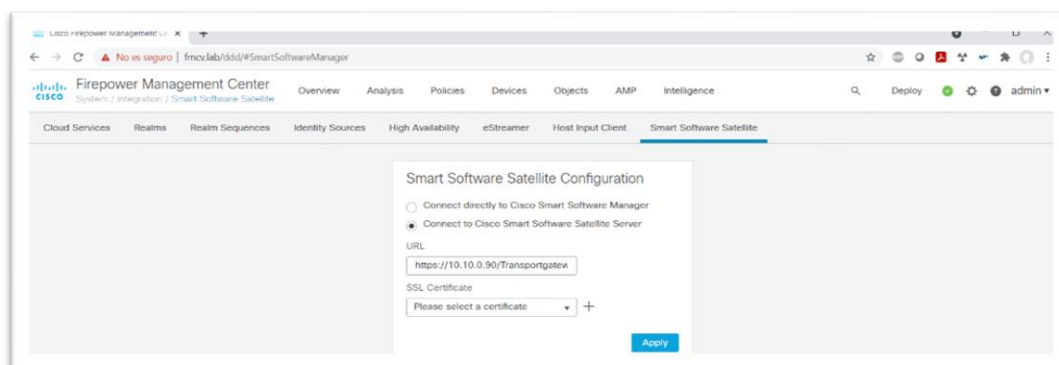
Todas las licencias de los equipos Firepower FTD y FMC se gestionan a través del FMC. Sólo el FMC realiza y necesita las conexiones a la Smart Account.

Para redes sin conexión a Internet (air-gapped) se pueden licenciar los equipos mediante el uso de, o bien un Smart Software Manager On-Prem (antiguo Cisco Satellite) o bien el uso de licencias SLR (Specific License Reservation).

Nota: hay que tener en cuenta que en un sistema Firepower sin conexión a Internet, las actualizaciones de los sistemas IPS, URL Filtering o Malware Protection hay que realizarlas manualmente.

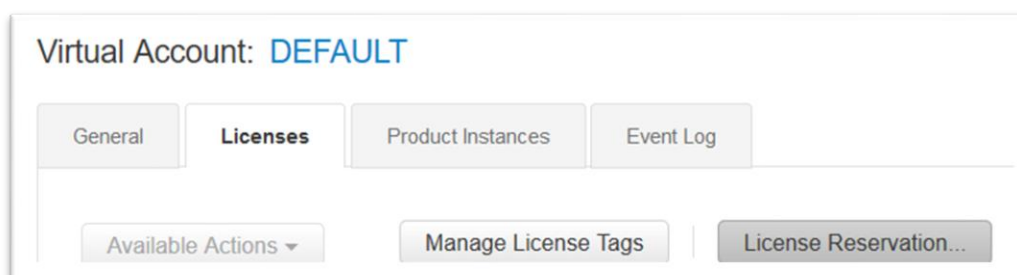
Un Cisco Smart Software Manager (SSM) On-Prem (on premise) es un software instalado en virtual, que hace una delegación de licencias desde Smart Licensing. El SSM se puede sincronizar manualmente mediante paso de ficheros simples entre el acceso web de Cisco de Smart Licensing y la conexión al SSM. El tiempo máximo entre sincronizaciones manuales es de 1 año. Es decir, se debe proceder a la sincronización manual, al menos, 1 vez al año.

La instalación y configuración del Cisco SSM no se encuentra en el alcance de esta guía. La configuración en el FMC de la conexión con el SSM se realiza mediante el menú System->Integration->Smart Software Satellite. Se debe introducir la URL y el certificado del SSM para establecer la relación de confianza.



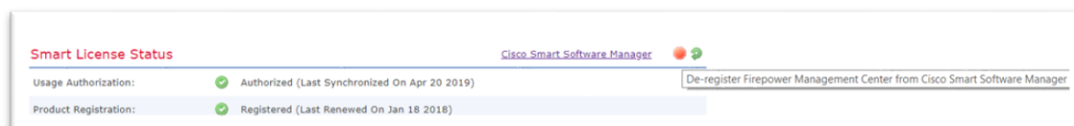
Desde la versión 6.3 Cisco dispone de un nuevo sistema de licenciamiento permanente, SLR (Specific License Reservation).

Este sistema debe ser habilitado en la Smart Account, para lo que se necesita intervención del representante de cuenta (Account Manager) de Cisco asignado a la organización. Una vez aprobada la petición, se encontrará disponible la opción en Smart Licensing.



IMPORTANTE. Si se va a activar SLR cuando se está usando ya conexión de Smart Licensing, bien vía conexión directa o a través de un SSM, se debe des-registrar primero el FMC de la Smart Account. Esto debe hacerse para liberar las licencias y que vuelvan a estar disponibles en la Smart Account para que se puedan posteriormente asignar a través del SLR.

Se debe usar el botón rojo:



Para licenciar el FMC a través de SLR, se deben seguir los siguientes pasos:

- Activar el sistema SLR en el FMC

Mediante conexión por SSH al FMC, se debe ir al sistema experto (expert) y en la shell ejecutar el comando “sudo manage_slr.pl” que muestra el menú de activación. Se debe seleccionar “Enable SLR”, que debe devolver “Successfully Enabled SLR”.

```
> expert
admin@FMCv:~$ sudo manage_slr.pl
Password:

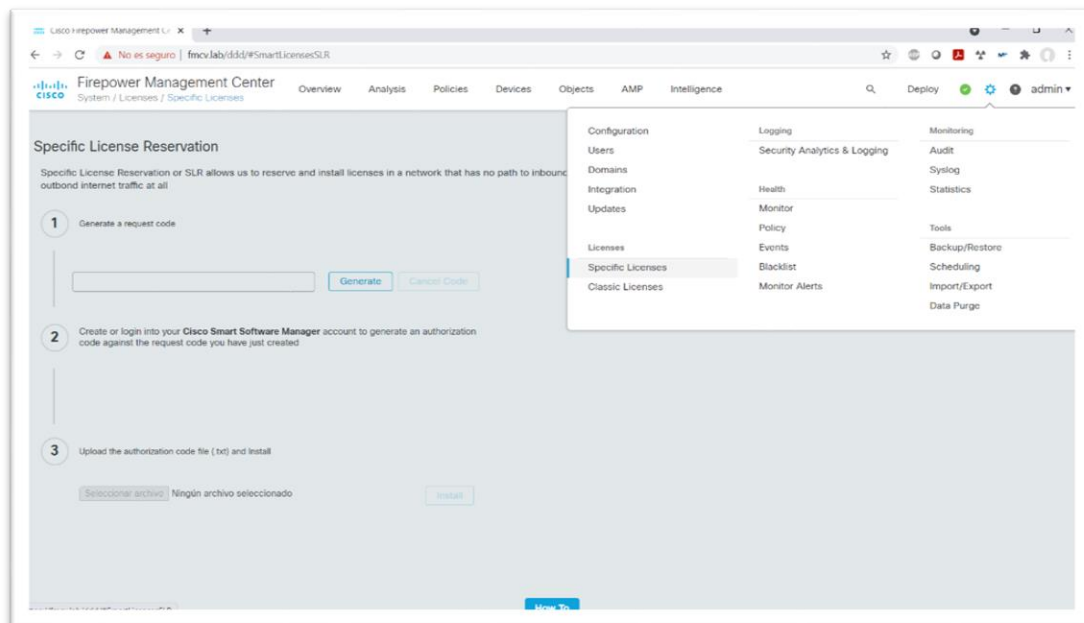
***** Configuration Utility *****

1 Show SLR Status
2 Enable SLR
3 Disable SLR
0 Exit

*****
Enter choice: 2

Successfully Enabled SLR
```

Observaremos que el menú System->Licenses->Smart Licensing ha desaparecido y, en su lugar aparece System->Licenses->Specific Licenses.



El funcionamiento es muy simple, se genera un código en el menú SLR del FMC. Ese código se escribe en la pantalla correspondiente de la web pinchando en License Reservation. Se puede escribir a mano o leer de fichero “Browse”.

Smart License Reservation

STEP 1 Enter Request Code | STEP 2 Select Licenses | STEP 3 Review and confirm | STEP 4 Authorization Code

You can reserve licenses for product instances that cannot connect to the Internet for security reasons. You will begin by generating a Reservation Request Code from the product instance. To learn how to generate this code, see the configuration guide for the product being licensed.

Once you have generated the code:

- 1) Enter the Reservation Request Code below
- 2) Select the licenses to be reserved
- 3) Generate a Reservation Authorization Code
- 4) Enter the Reservation Authorization Code on the product instance to activate the features

• Reservation Request Code:

Se seleccionan las licencias que se quieren asignar al FMC permanentemente. Las licencias base son gratuitas. Y se obtiene el fichero con el Authentication Code.

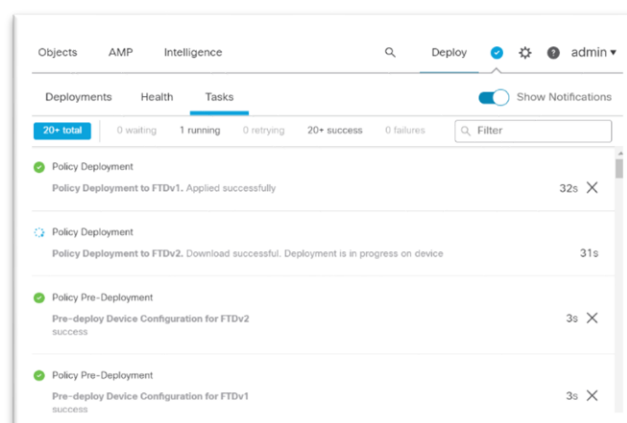
Descargado el fichero de Authorization Code se selecciona luego en la pantalla SLR del FMC y se pincha sobre INSTALL. Las licencias quedarán instaladas.

13.11 CONSIDERACIONES GENERALES: DEPLOY/TASKS/HEALTH

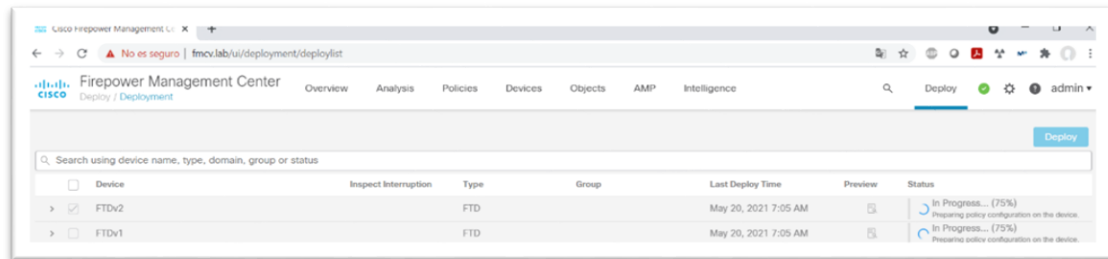
Las gestiones o cambios de configuración hechos en el gestor FMC nunca realizan cambios directos en los dispositivos, salvo excepciones.

Por lo tanto, se pueden ir realizando cambios de configuraciones y reglas con seguridad hasta que se decidan aplicar los cambios.

Algunas de las acciones del gestor generan tareas en segundo plano “background” que pueden ser visualizados en “Tasks”. A la izquierda del botón de “System” existe un círculo, pinchándolo nos aparece un desplegable donde pueden consultarse las tareas en ejecución y las pasadas.

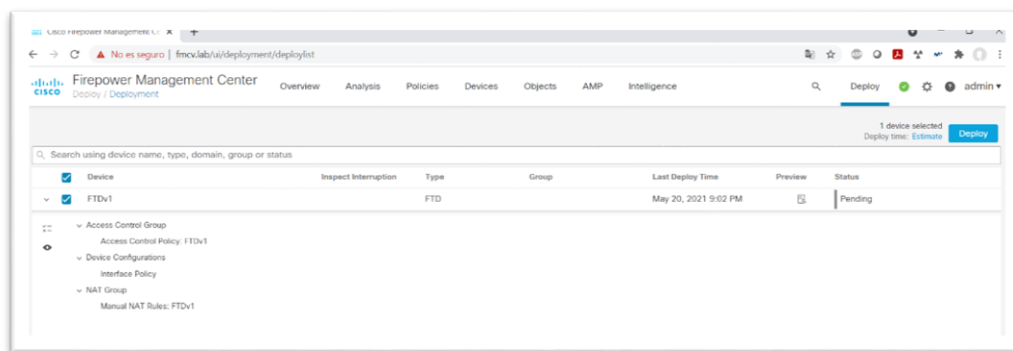


En Deploy pueden verse las actividades de despliegue en curso, así como realizar nuevos.



Cuando queramos que los cambios realizados en el gestor FMC se apliquen en los firewalls, se debe realizar un Deploy.

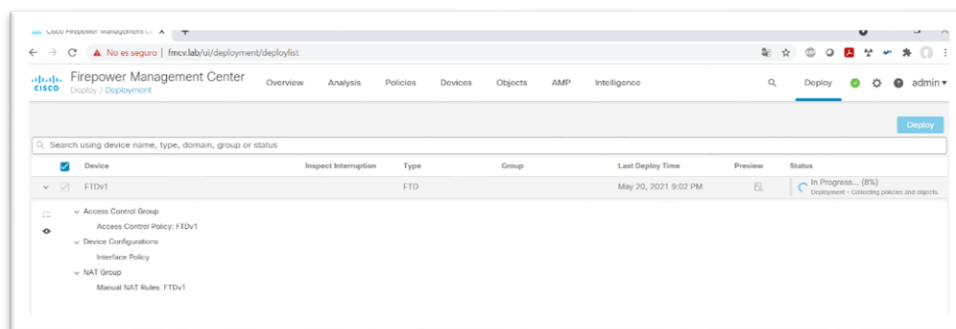
Pinchando en el botón a la izquierda del círculo, se inicia el proceso.

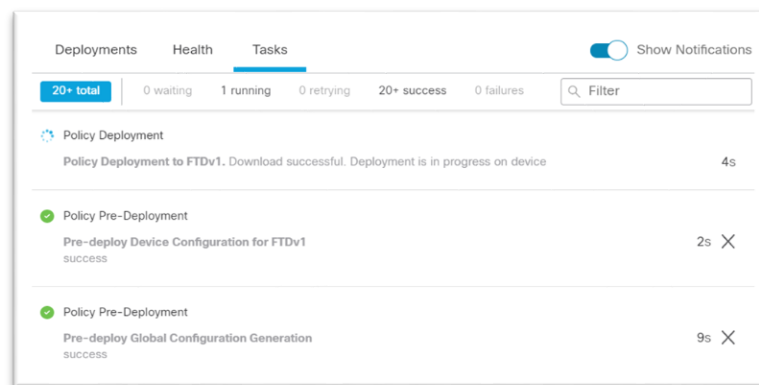


El sistema detecta en que dispositivos se han realizado cambios y muestra un desplegable con los cortafuegos en los que se aplican esos cambios, pudiendo seleccionar el que nos interese. También se muestra qué cambios son los que se van a realizar, con detalles desplegables si pasamos el puntero por encima.

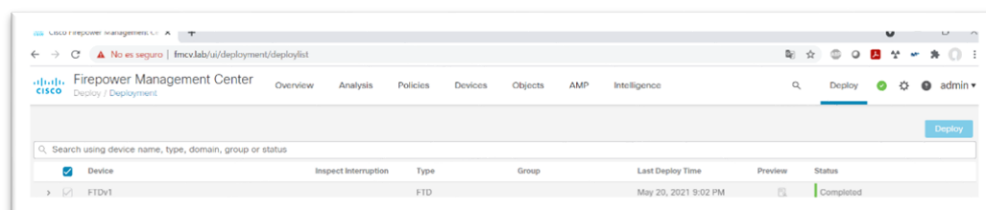
Una vez que decidimos realizar un Deploy presionaremos el botón y se realizarán las tareas en segundo plano relacionadas con ese Deploy.

Los pasos del Deploy pueden verse tanto en la pestaña de Deploy como en Tasks.





Para comprobar que se ha terminado el Deploy con éxito se consulta su pestaña.

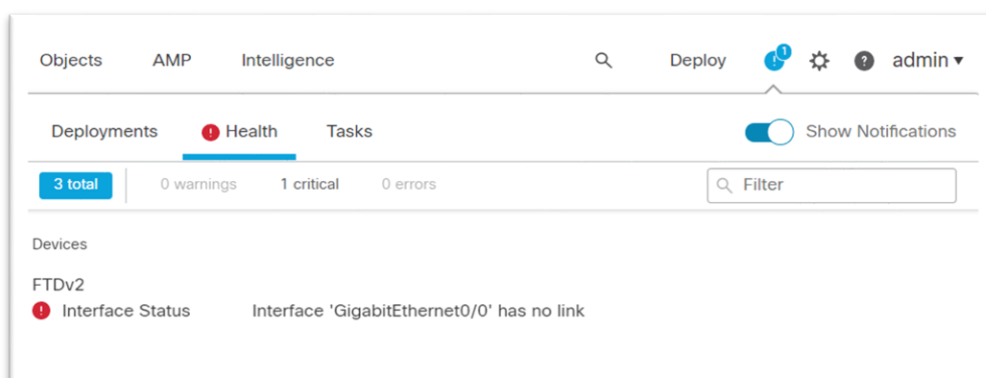


El círculo intermedio que permite el acceso a Tasks y Deployments, cambia de color verde a amarillo o rojo, en caso de problemas.

Los problemas pueden ser fallos en Tasks o Deploys o prevenir de eventos a partir de las políticas Health.

Las políticas Health monitorizan el estado tanto del gestor como de los cortafuegos a intervalos regulares y pueden configurarse y parametrizarse de acuerdo a las necesidades.

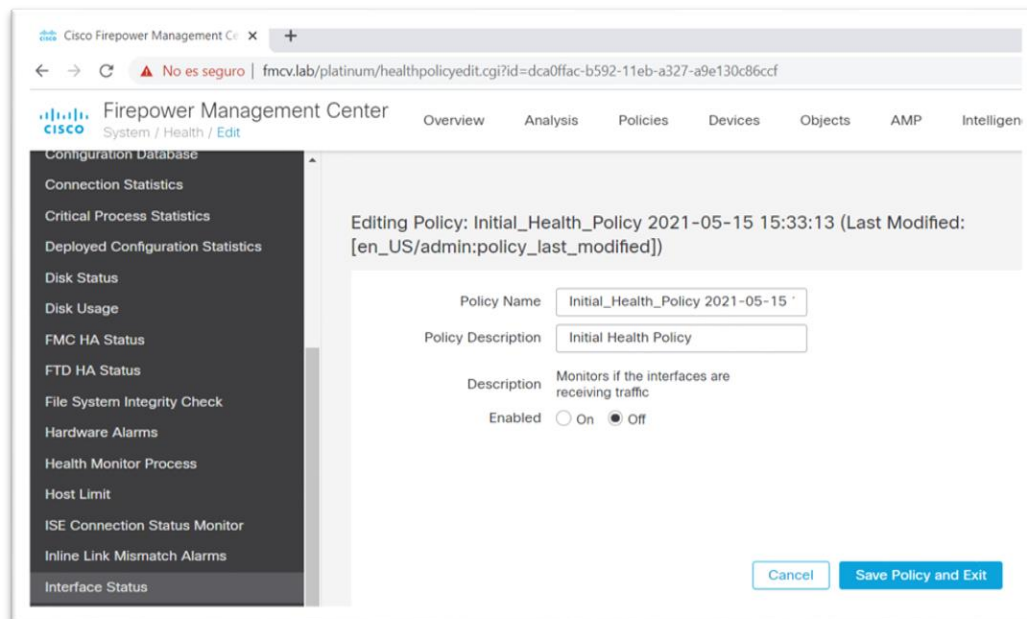
Por ejemplo, el botón usado en los ejemplos está en rojo, porque una política Health ha reportado un problema.



Sin embargo, este problema podría no ser relevante en este caso si se está pendiente de conectar esos cables, que se harán otro día, por ejemplo.

A través del menú System->Health->Policy se pueden configurar estas políticas.

Podríamos, por ejemplo, modificar la política y desactivar el chequeo de “Interface Status”. O crear una política nueva solo para ese dispositivo “fp2110-1” con el chequeo deshabilitado y asignársela. Y volver al caso anterior cuando se hayan conectado.



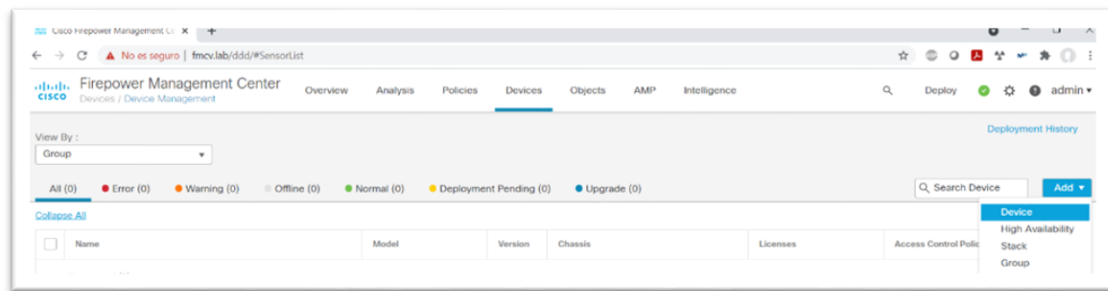
13.12 GESTIÓN DE DISPOSITIVOS

La pantalla principal de gestión de dispositivos es una de las más importantes y relevantes del gestor FMC. Devices->Device Management.

Muestra todos los dispositivos (cortafuegos) registrados con el gestor y su estado. Además, se utiliza para configurar interfaces, routing, multicast, gestión de alta disponibilidad y, en general, todas las configuraciones esenciales de los dispositivos.

13.12.1 AÑADIR DISPOSITIVO

Para realizar configuraciones sobre un nuevo dispositivo lo primero es añadirlo al gestor FMC. Esto se realiza mediante su dirección y su contraseña, que se especificó en la parte de configuración inicial del dispositivo Firepower FTD.



La siguiente pantalla pide los datos para el acceso al dispositivo. El Host se puede especificar como nombre DNS o por IP. El Display Name es el nombre con el cual se mostrará en el FMC, la Registration Key es clave de “configure manager add”. El Group son grupos que podemos crear, si tuviésemos muchos cortafuegos sería recomendable. Se debe asignar una Access Control Policy inicial. Se recomienda usar una ACP simple de para bloquear todo en este punto. Se deben asignar las licencias requeridas para el dispositivo.

Add Device

Host:†

Display Name:

Registration Key: *

Group:

Access Control Policy: *

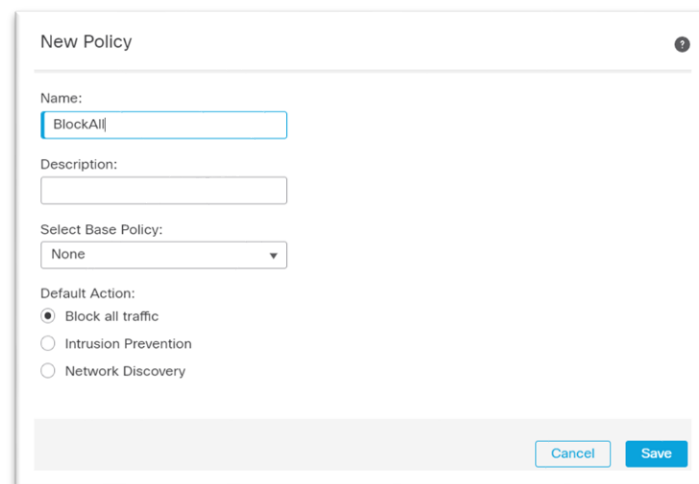
☒ Malware
☒ Threat
☒ URL Filtering

Advanced

Unique NAT ID: †

☒ Transfer Packets

Access control policy is required.

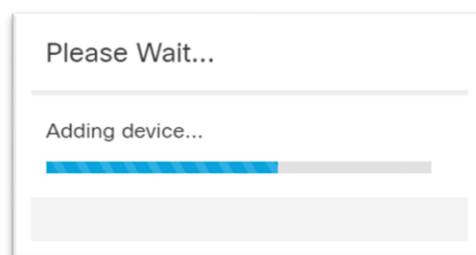


A dialog box titled "New Policy" with a help icon in the top right corner. It contains the following fields and options:

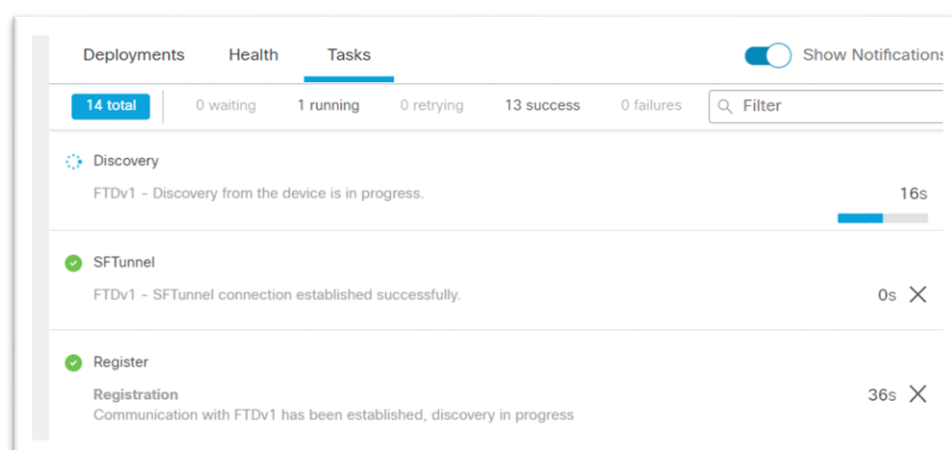
- Name:** A text input field containing "BlockAll".
- Description:** An empty text input field.
- Select Base Policy:** A dropdown menu currently showing "None".
- Default Action:** Three radio button options:
 - ☒ Block all traffic
 - ☐ Intrusion Prevention
 - ☐ Network Discovery

At the bottom right, there are "Cancel" and "Save" buttons.

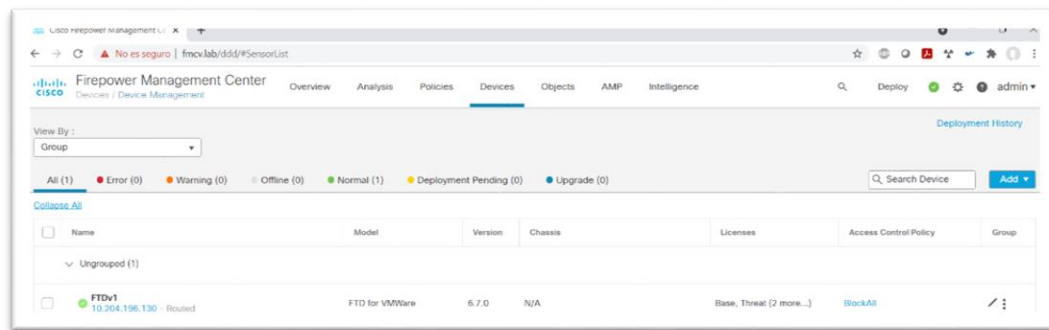
El sistema empezará la tarea de descubrimiento y añadirá el dispositivo.



En Tasks puede verse la tarea ejecutándose.



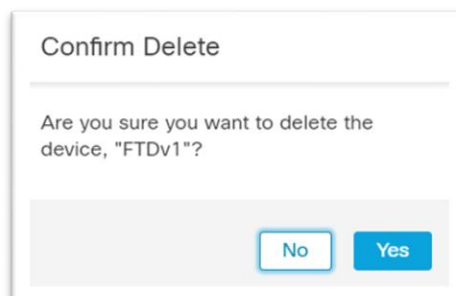
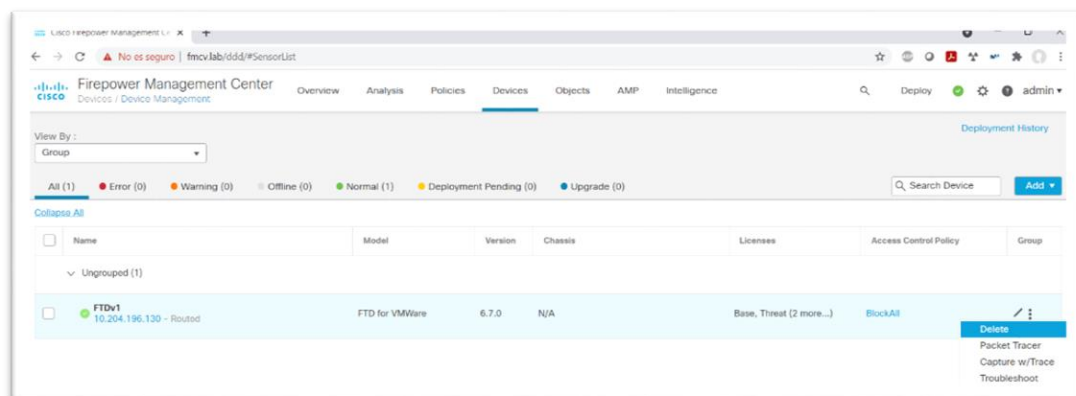
Una vez registrado aparecerá en la pantalla y se le asignará una Health Policy y la ACP BlockAll que hemos creado, para lo que se le hará un Deploy automático.



El seguimiento del proceso se puede seguir en Tasks. El estado final debe quedar registrado, con sus licencias y en estado Normal.

13.12.2 ELIMINAR DISPOSITIVO

Para eliminar un dispositivo de la gestión del FMC hay que pinchar en el icono del menú y seleccionar "Delete". Se pedirá una confirmación.



13.12.3 GESTIÓN DE INTERFACES

Una de las tareas más importantes de una integración es la correcta y adecuada configuración de las interfaces y zonas de seguridad.

13.12.3.1 ZONAS DE SEGURIDAD

El concepto de zonas de seguridad se basa en la compartimentación, agrupando equipos de funcionamiento similar en cuanto a red dentro de la misma zona.

Las definiciones de las zonas de seguridad también están sujetas a valoraciones subjetivas. Por ejemplo, una zona de seguridad “Servidores” la podemos definir como equipos a los que acceden los usuarios para sus peticiones y trabajo. Pero unos equipos, por ejemplo, bases de datos, a los que acceden otros servidores, podrían tratarse de la misma zona de seguridad, porque son servidores, o podría crearse otra zona nueva distinta “BackEnd” que se defina como de acceso solo desde “Servidores”.

Es por ello importante que las zonas de seguridad se creen con definiciones formales que ayuden a entender por qué han sido creadas. Entender la lógica de compartimentación.

En Firepower, 1 interface de red puede ser asignado solo a 1 zona de seguridad.

Pero 1 zona de seguridad puede contener varias interfaces. O, lo que es lo mismo, varias interfaces pueden ser asignadas a la misma zona de seguridad.

La zona de seguridad es importante porque se puede hacer referencia a ella en la política de seguridad ACP (Access Control Policy) y crear reglas sobre ellas.

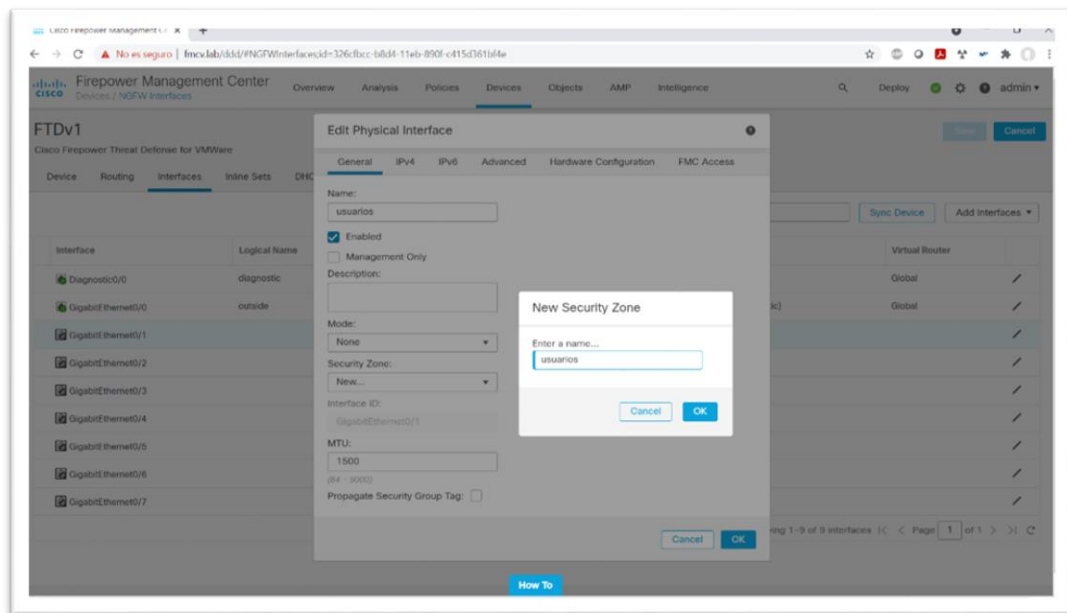
Las zonas de seguridad pueden crearse en la sección de objetos Objects->Object Management o bien al tiempo de edición de un interfaz. En la creación y gestión de interfaces suele ser más conveniente.

13.12.3.2 ASIGNACIÓN DE DIRECCIONAMIENTO IP

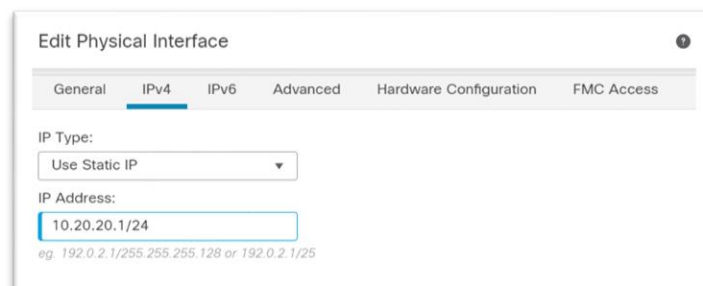
Las direcciones IP son asignadas a las interfaces, que pueden ser interfaces físicos, EtherChannels (agregación de puertos), Subinterfaces (VLAN), o incluso Bridging (BVI).

En Device Management, seleccionando un cortafuegos, podemos acceder a su sección de Interfaces, y editar una interfaz para asignarle direccionamiento.

El interfaz debe asignarse a una zona de seguridad y tener un nombre (Name). Si la zona de seguridad no existe, la podemos crear desde el menú.



El direccionamiento se especifica en la pestaña de IPv4 (o IPv6). La notación puede ser con máscara con barra diagonal o clásica.



Varios interfaces pueden ser asignados a las mismas zonas de seguridad.

The screenshot shows the Cisco Firepower Management Center (FMC) interface, specifically the 'Interfaces' tab. It displays a table of interfaces and their assigned security zones.

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Virtual Router
Diagnostic0/0	diagnostic	Physical				Global
GigabitEthernet0/0	outside	Physical	outside		7.7.7.1/24(Static)	Global
GigabitEthernet0/1	usuarios	Physical	usuarios		10.20.20.1/24(Static)	Global
GigabitEthernet0/2	usuarios2	Physical	usuarios		10.20.30.1/24(Static)	Global

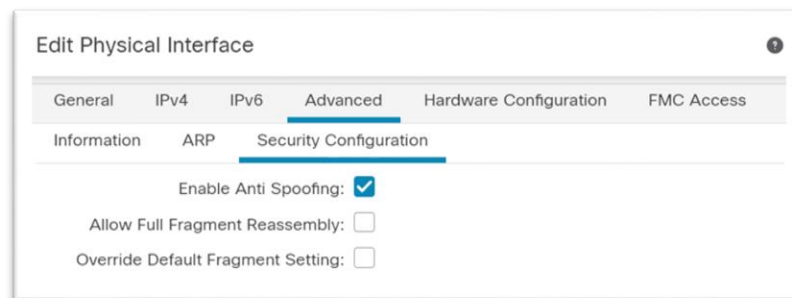
Hay que recordar que, para que los cambios sean efectivos se requiere un Deploy al dispositivo cortafuegos.

13.12.3.3 ANTI-SPOOFING

Por norma general se debe habilitar la característica anti-spoofing de Cisco Firepower.

Esta funcionalidad prohíbe que lleguen paquetes con IP origen desde interfaces que, desde el punto de vista del cortafuegos, no están en ese rango. Es decir, que ni la IP del firewall está en ese rango, ni existe ruta hacia esa IP por ese interfaz.

Para activarlo, se realiza en la parte Advanced de la edición del interfaz, que debe tener direccionamiento IP asignado.

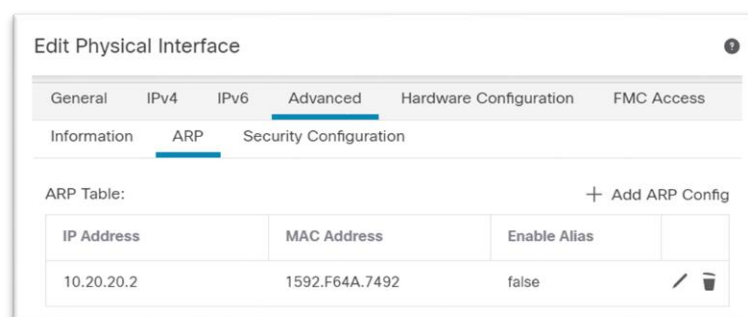


13.12.3.4 ARP ESTÁTICO

En ocasiones se deberá asignar un ARP estático a una IP determinada. Bien para intentar prevenir un ataque del tipo Man-In-The-Middle o ARP spoofing.

Un caso de uso típico para esto es una red de interconexión WAN compartida donde quieres asegurar que tus paquetes siempre irán directamente al peer de conexión, evitando cualquier spoofing simple.

La configuración se realiza en el apartado Advanced del interfaz, que debe tener direccionamiento IP asignado. El "Enable Alias" no se debe habilitar.

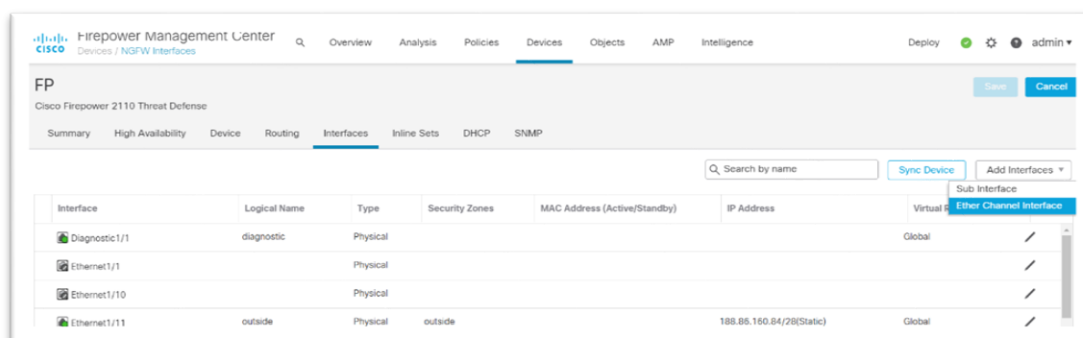


13.12.3.5 CREACIÓN DE ETHERCHANNELS – ASA, ISA 3000 & FIREPOWER 2100/1000

Las agregaciones de puertos, o EtherChannels, para las familias ASA, ISA 3000 y Firepower 1000/2100 deben hacerse en el gestor FMC.

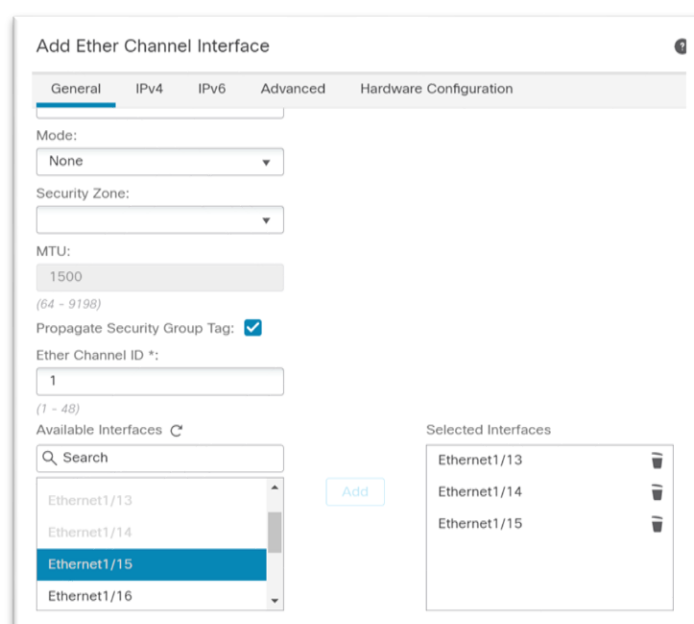
Los equipos Firepower 4100/9300 disponen de sistema FXOS separado y es ahí donde deben ser configurados y asignados al FTD.

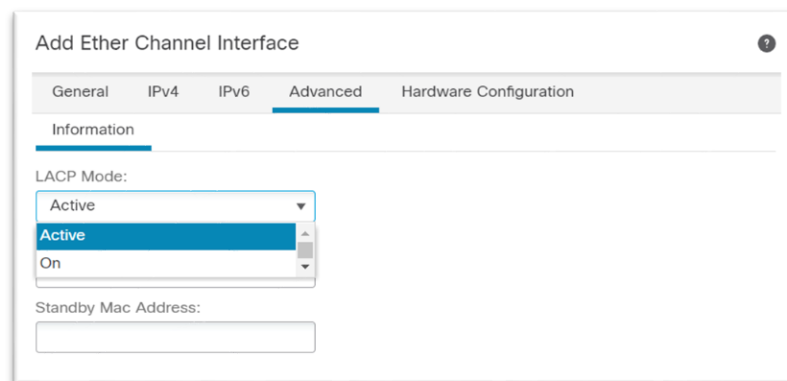
Para los que son creados en el FMC, pulsando sobre el dispositivo en Device Management y en la pestaña de Interfaces, se muestra el botón “Add Interfaces”, “EtherChannel Interface”.



Podemos asignar interfaces físicas al EtherChannel y el modo LACP/On. Se recomienda el modo LACP.

Dependiendo de la integración, podemos no asignar direccionamiento IP, ni Name, ni zona de seguridad al interfaz, si lo que vamos a hacer luego es crear subinterfaces a partir de este EtherChannel para usar VLANs.





The screenshot shows the 'Add Ether Channel Interface' configuration page with the 'Advanced' tab selected. The 'Information' section is visible, showing the 'LACP Mode' dropdown menu with 'Active' selected. Below it is a 'Standby Mac Address' text field.

Add Ether Channel Interface

General IPv4 IPv6 **Advanced** Hardware Configuration

Information

LACP Mode:

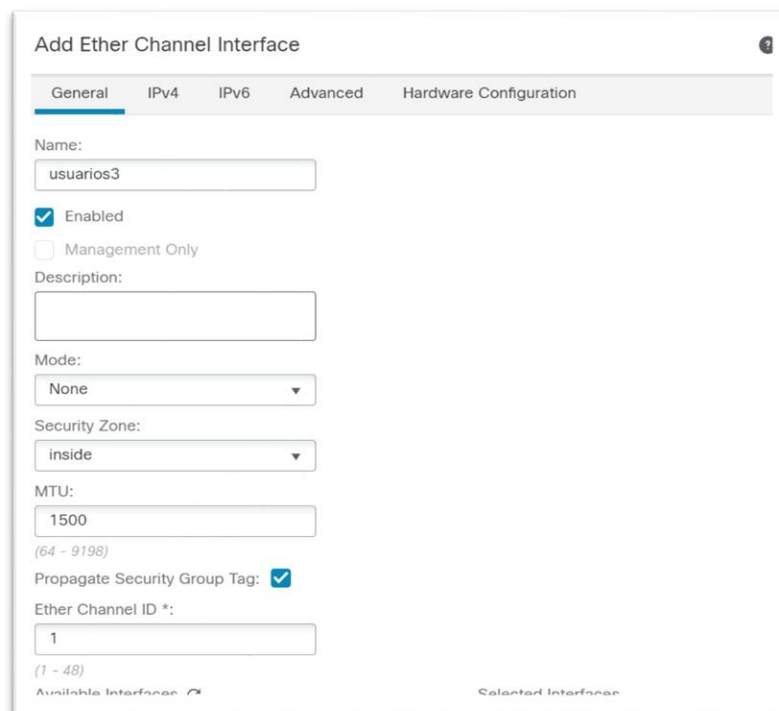
Active

Active

On

Standby Mac Address:

O bien, podemos crearlo con direccionamiento IP para el tráfico nativo y, opcionalmente, también crear Subinterfaces con VLAN sobre este EtherChannel luego.



The screenshot shows the 'Add Ether Channel Interface' configuration page with the 'General' tab selected. The 'Name' field is set to 'usuarios3'. The 'Enabled' checkbox is checked. The 'Description' field is empty. The 'Mode' dropdown is set to 'None'. The 'Security Zone' dropdown is set to 'inside'. The 'MTU' field is set to '1500'. The 'Propagate Security Group Tag' checkbox is checked. The 'Ether Channel ID' field is set to '1'.

Add Ether Channel Interface

General **IPv4** IPv6 Advanced Hardware Configuration

Name:

usuarios3

☒ Enabled

☐ Management Only

Description:

Mode:

None

Security Zone:

inside

MTU:

1500

(64 - 9198)

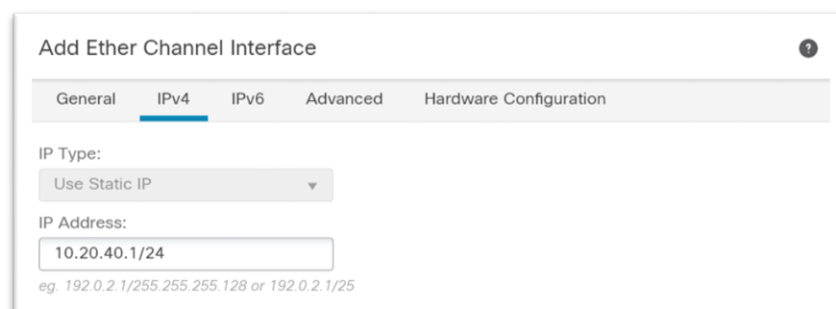
Propagate Security Group Tag: ☒

Ether Channel ID *:

1

(1 - 48)

Available Interfaces:  Selected Interfaces: 



The screenshot shows the 'Add Ether Channel Interface' configuration page with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use Static IP'. The 'IP Address' field is set to '10.20.40.1/24'.

Add Ether Channel Interface

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type:

Use Static IP

IP Address:

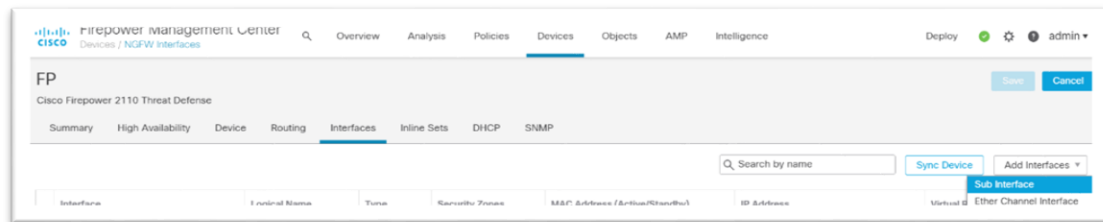
10.20.40.1/24

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

13.12.3.6 CREACIÓN DE SUBINTERFACES

Las subinterfaces proveen de acceso a VLAN a través de 802.1q sobre un puerto físico o sobre un EtherChannel.

Pulsando sobre el dispositivo en Device Management y en la pestaña de Interfaces, se muestra el botón “Add Interfaces”, “Sub Interface”.



En este ejemplo se muestra sobre un EtherChannel (Port-channel1) creado anteriormente.

Add Sub Interface

General
IPv4
IPv6
Advanced

Name:

☒ Enabled
☐ Management Only

Description:

Security Zone:

MTU:

(64 - 9198)

Propagate Security Group Tag: ☒

Interface *:

Sub-Interface ID *:

(1 - 4294967295)

VLAN ID:

(1 - 4094)

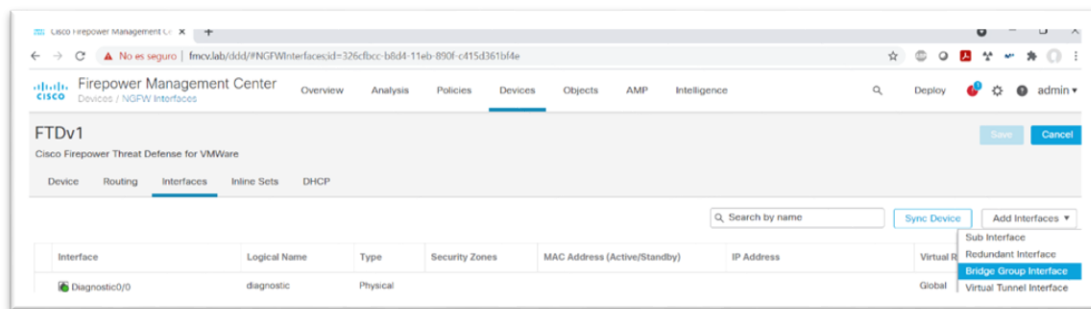
Ethernet1/8	Physical	
Ethernet1/9	Physical	
Port-channel1	EtherChannel	
Port-channel1 17	usuarios5	Subinterface inside

Recordar que se debe hacer Deploy para que estos cambios se hagan reales.

13.12.3.7 CREACIÓN DE BRIDGE GROUP – FIREPOWER 4100/9300

Los modelos Firepower 4100/9300 y el NGFW Virtual permiten la creación de bridges en el modo rutado. Los Firepower 1000/2100 no tienen esta capacidad.

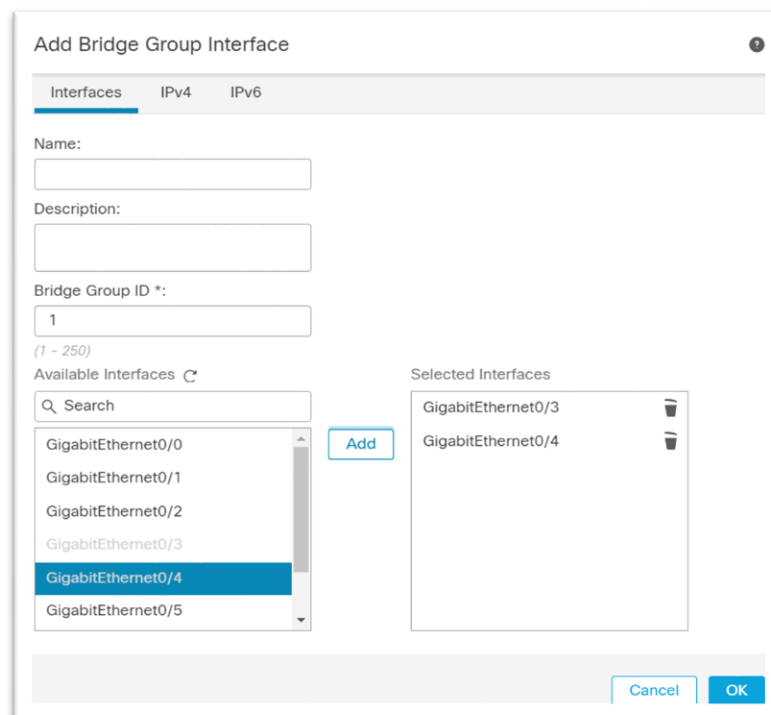
Pulsando sobre el dispositivo en Device Management y en la pestaña de Interfaces, se muestra el botón “Add Interfaces”, “Bridge Group Interface”.



Siempre hay que asignar una IP dentro del rango del bridging.

Pero hay 2 opciones, crearlo sin Name, donde entonces el bridge group actúa sin routing. O crear con Name y entonces la IP asignada al bridge puede ser usada para rutar tráfico y se incorpora a la tabla de rutas del equipo.

Ejemplo sin Name, bridging aislado, sin routing.



Se debe asignar siempre una IP del rango del bridging para que este sea operativo.

Add Bridge Group Interface

Interfaces **IPv4** IPv6

IP Type:
Use Static IP

IP Address:
10.20.60.1/24
eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

Opción con Name, bridging integrado con routing.

Add Bridge Group Interface

Interfaces **IPv4** IPv6

Name:
BridgingRouting

Description:

Bridge Group ID *:
1
(1 - 250)

Available Interfaces

Search

- GigabitEthernet0/0
- GigabitEthernet0/1
- GigabitEthernet0/2
- GigabitEthernet0/3
- GigabitEthernet0/4**
- GigabitEthernet0/5

Selected Interfaces

- GigabitEthernet0/3
- GigabitEthernet0/4

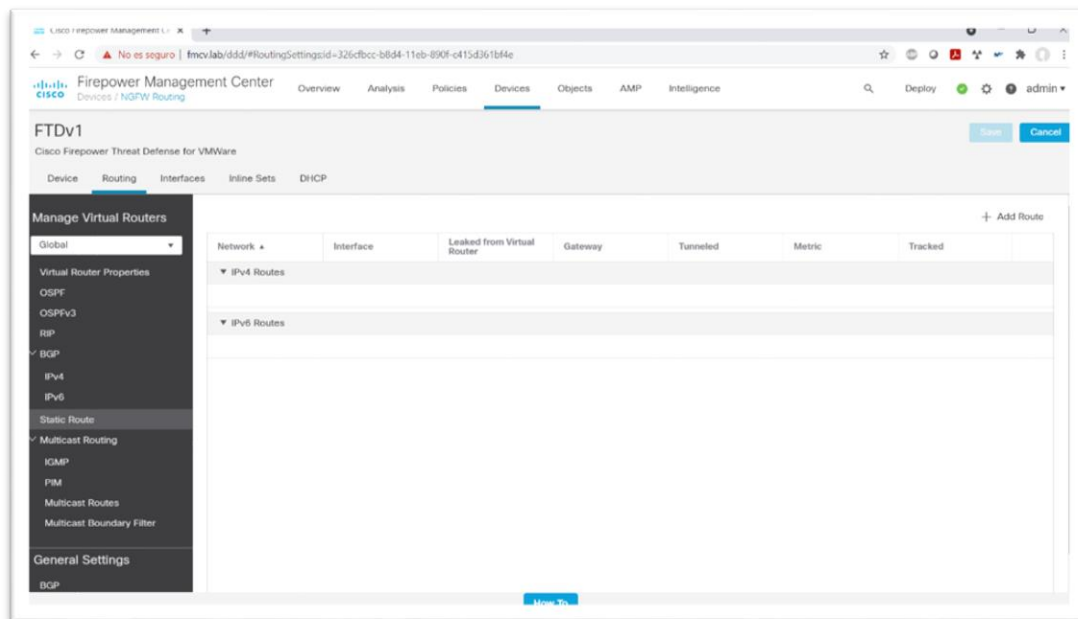
Buttons: Add, Cancel, OK

13.12.4 ROUTING

En “Device Management” seleccionando el dispositivo, en la pestaña “Routing”, accedemos a la parte de routing dinámico (RIP, OSPF, BGP, Multicast routing) y rutas estáticas.

Lo más común es usar rutas estáticas.

Pinchando en “Static Route” podemos añadir rutas “Add Route”.



En Firepower se configuran las rutas indicando el interfaz por donde se produce la salida. Se pueden especificar las redes destino por nombre (objeto) o usar predefinidos como any-ipv4 y la IP destino de la ruta (gateway), se puede especificar por nombre (objeto) o especificar manualmente.

Se puede especificar también un tracking (IP SLA) para que la ruta solo esté activa si se cumple una condición.

Add Static Route Configuration

Type:
☒ IPv4
☐ IPv6

Interface*

outside

(Interface starting with this icon signifies it is available for route leak)

Available Network

Q Search

any-ipv4
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8
IPv4-Private-172.16.0.0-12

Selected Network

any-ipv4

Gateway*

10.44.44.254

Metric:

1

(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:

New SLA Monitor Object

Name: Description:

Frequency (seconds): SLA Monitor ID*:
(1-604800)

Threshold (milliseconds): Timeout (milliseconds):
(0-60000) (0-604800000)

Data Size (bytes): ToS:
(0-16384)

Number of Packets: Monitor Address*:

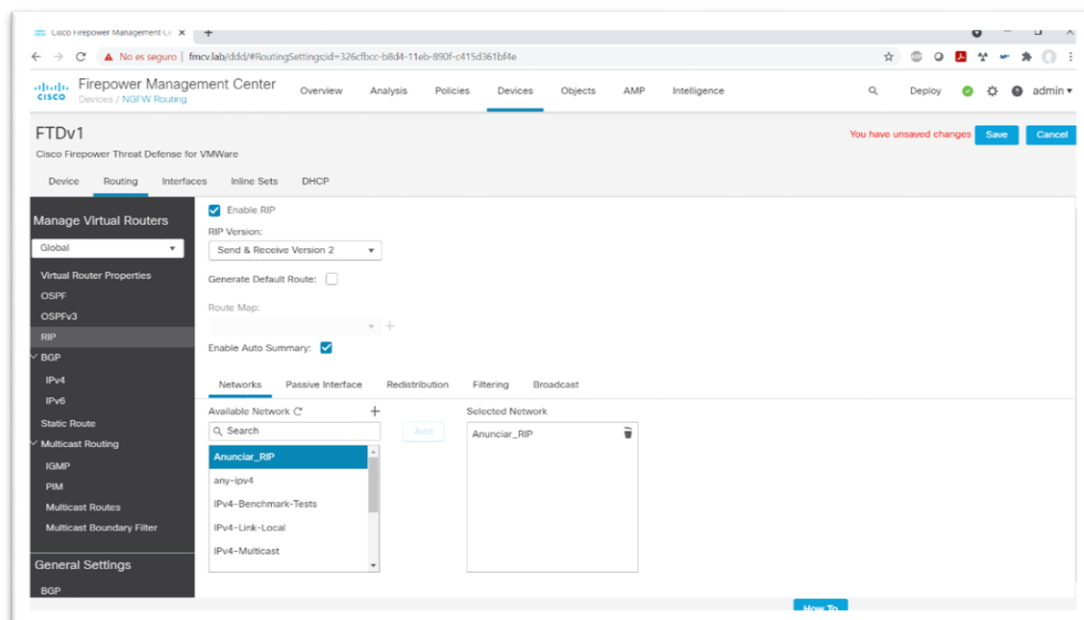
Available Zones

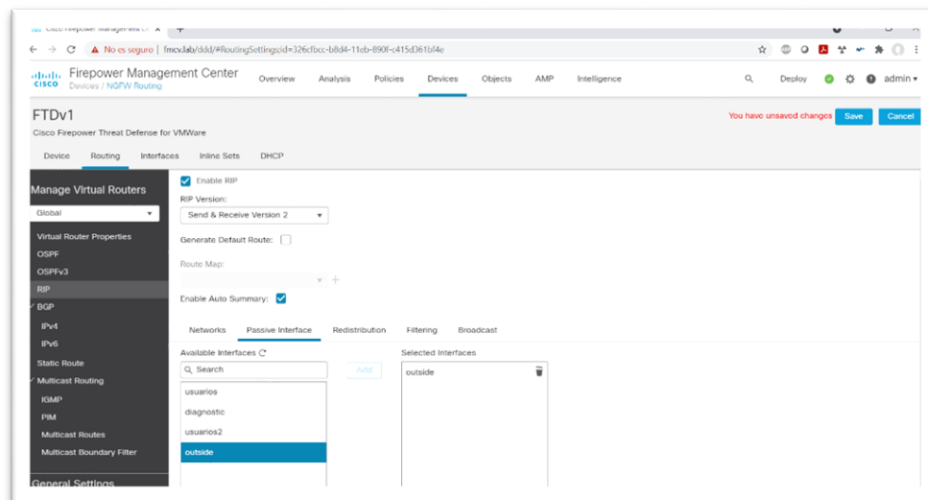
outside

usuarios

Un protocolo de routing que podemos emplear a modo de ejemplo para un cortafuegos es RIP.

Por ejemplo, podemos habilitar la v2 de RIP, especificar unos rangos de red para publicar en RIP “Anunciar_RIP”, y especificar como pasivo el interfaz “outside”.





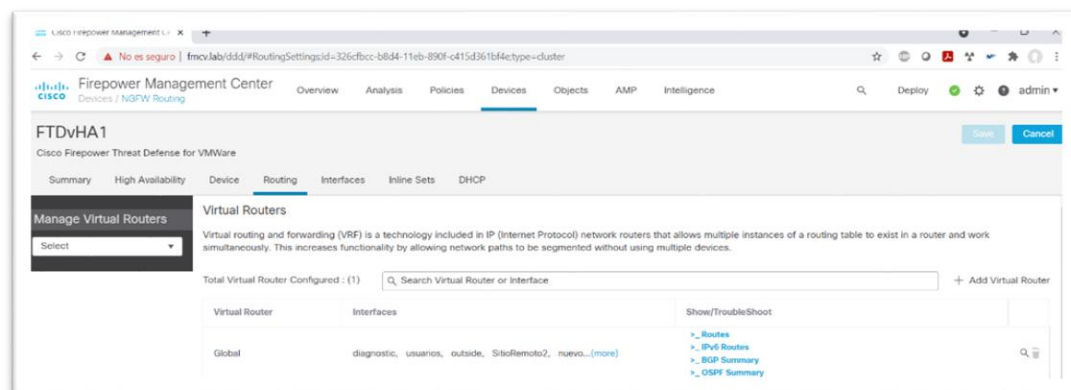
13.12.5 VIRTUAL ROUTER (VRF)

A partir de la versión 6.6 de FTD, está disponible la funcionalidad de Virtual Router, más conocida técnicamente como VRF o VRF-Lite.

Esta característica provee de una separación de direccionamientos IPs, incluyendo interfaces, y tablas de enrutamiento.

Nota: aunque existe la posibilidad de tratar esta característica como los contextos virtuales de ASA o como si fueran “cortafuegos virtuales”, ya que otros fabricantes, así lo hacen, esta práctica está desaconsejada por motivos de seguridad. Para una separación completa de cortafuegos se debe usar la funcionalidad de contenedores, descrita en el apartado de FXOS.

Para acceder al apartado principal de esta característica se edita el equipo donde se quiere habilitar y en el apartado de Routing, pinchando en Manage Virtual Routers.



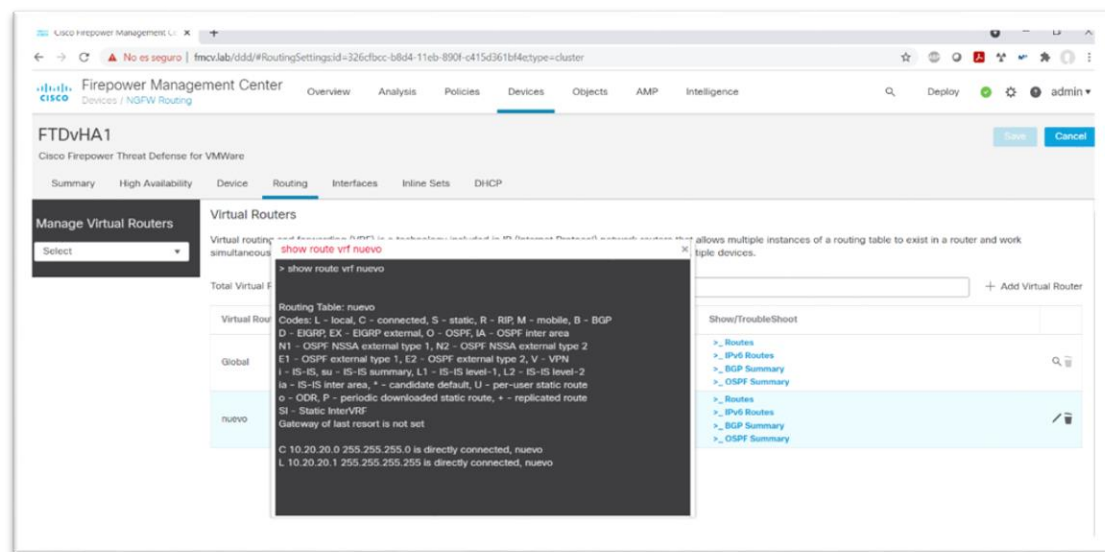
Para demostrar la separación, se puede crear un nuevo Virtual Router y asignarle una interfaz con el mismo direccionamiento IP que uno existente.

Dialog box titled "Add Virtual Router". It contains a "VRF Name*" field with the value "nuevo" and an empty "Description" field.

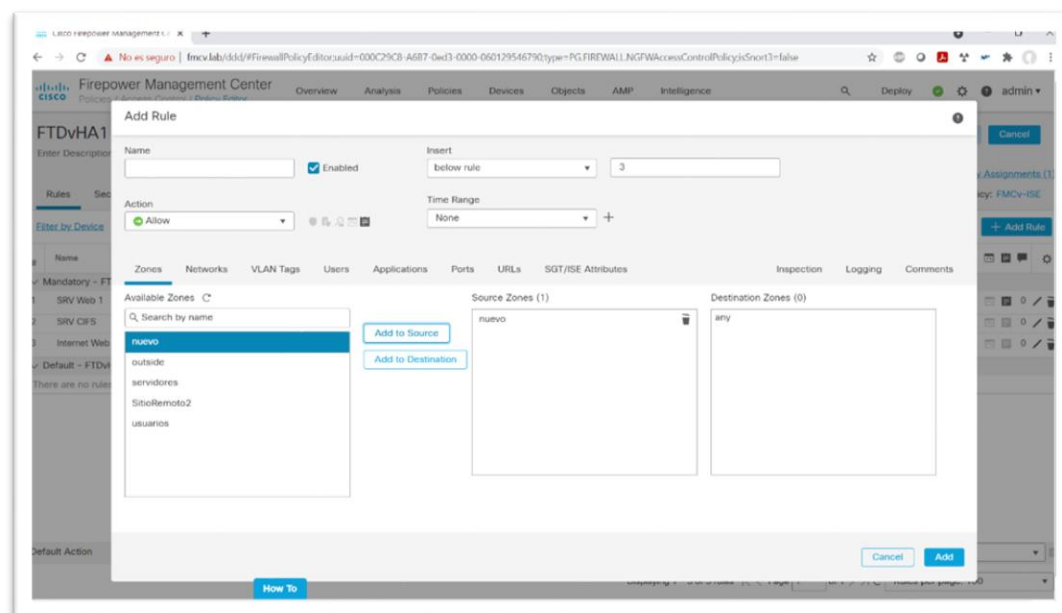
The screenshot shows the "Virtual Router Properties" configuration page for a new VRF named "nuevo". The "Available Interfaces" list on the left includes "outside", "usuarios", "usuarios2", "servidores", and "nuevo". The "Selected Interfaces" list on the right contains "nuevo".

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Virtual Router
Diagnostic0/0	diagnostic	Physical				Global
GigabitEthernet0/0	outside	Physical	outside		7.7.7.1/24(Static)	Global
GigabitEthernet0/1	usuarios	Physical	usuarios		10.20.20.1/24(Static)	Global
GigabitEthernet0/2	usuarios2	Physical	usuarios		10.20.30.1/24(Static)	Global
GigabitEthernet0/3	servidores	Physical	servidores			Global
GigabitEthernet0/4	nuevo	Physical	nuevo		10.20.20.1/24(Static)	nuevo

Si ya se ha realizado un Deploy de la configuración de Virtual Routers, se pueden usar los comandos de resolución de problemas.



Si bien la separación que se realiza es a nivel de direcciones IP, hay que recordar que las políticas, como el control de acceso, sigue siendo la principal asignada al dispositivo.

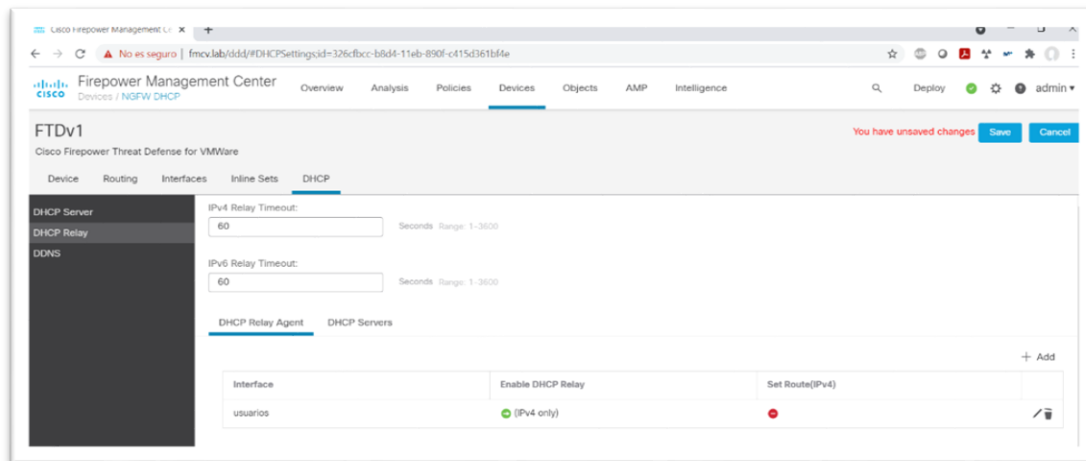


13.12.6 DHCP RELAY

El DHCP Relay “captura” los paquetes broadcast de un interfaz y los transmite de manera unicast a los DHCP servers de otro interfaz.

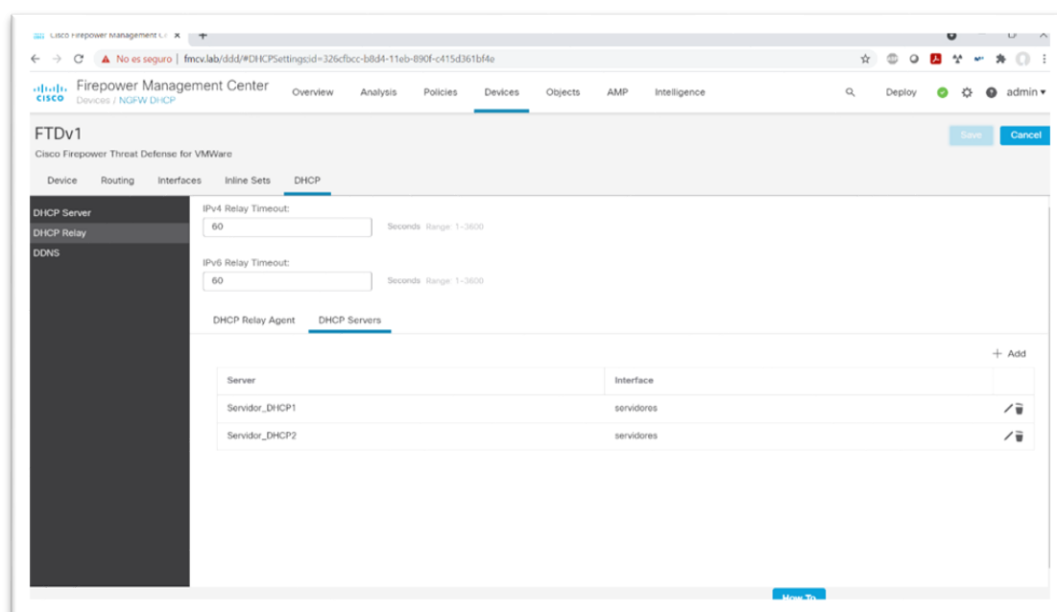
Un caso de uso típico de DHCP Relay es cuando debemos integrar un cortafuegos de Centro de Datos y separamos la red de clientes-usuarios, que usan DHCP (DHCP Client) de los servidores, donde se sitúan los servidores DHCP.

Se configura en “Device Management” pinchando sobre el dispositivo deseado, pestaña DHCP->DHCP Relay. Primero configuramos la interfaz por el que debemos “capturar” los broadcast DHCP.



Y luego se configuran los servidores DHCP donde se van a enviar las peticiones en unicast. Se deben usar objetos, que se pueden crear directamente usando el botón del “+”.

Normalmente en una red hay más de 1 servidor DHCP por redundancia, se deben especificar todos en la configuración.

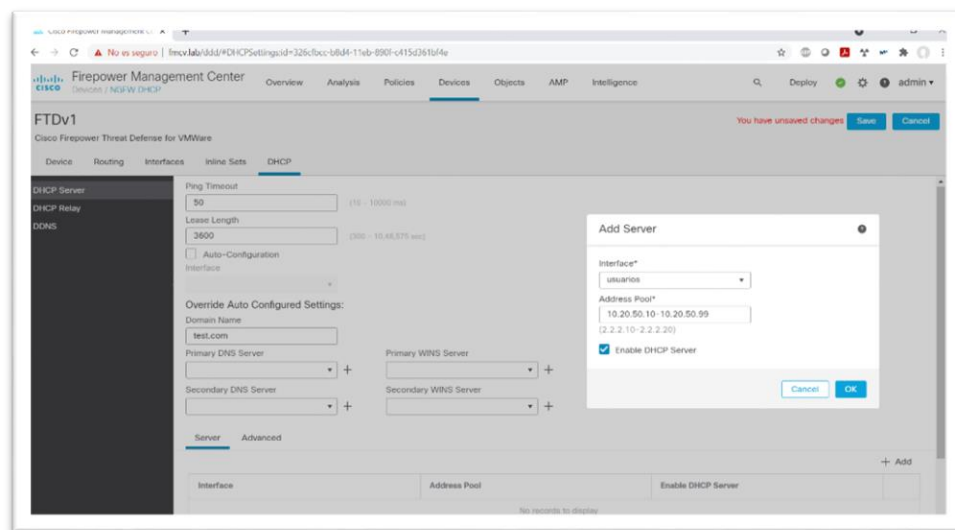


13.12.7 DHCP SERVER

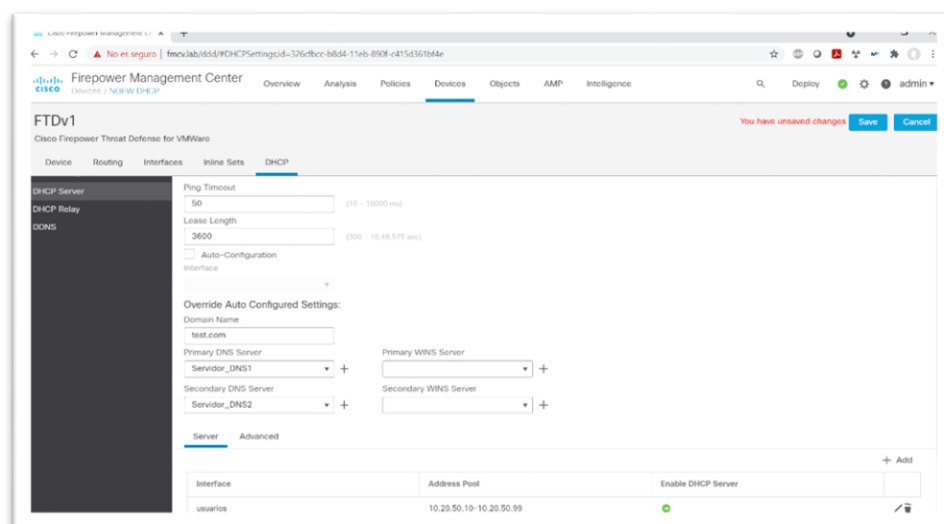
El cortafuegos Firepower también puede utilizarse como DHCP Server.

Un caso de uso típico de DHCP Server es, por ejemplo, en un cortafuegos perimetral donde existe una zona de seguridad de invitados o “externos” que no queremos que tengan acceso a recursos internos.

Se configura en “Device Management” pinchando sobre el dispositivo deseado, pestaña DHCP->DHCP Server. Se debe configurar un pool y asociarlo a una interfaz por el que se va a servir.



Se deben crear también valores como el dominio por defecto y servidores DNS. Se especifican como objetos que pueden crearse pulsando el “+”.



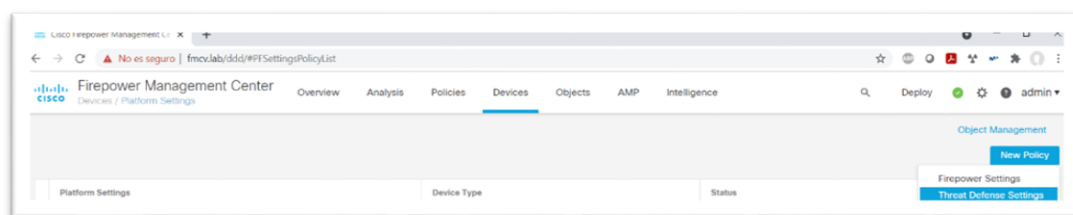
13.13 CONFIGURACIÓN DE PLATAFORMA

Se debe asignar una política de configuración de plataforma “Threat Defense Settings Policy” a los dispositivos FTD.

Se recomienda crear y asignar una por dispositivo o por grupo de alta disponibilidad.

Al menú se accede a través de Devices->Platform Settings. Por defecto no hay ninguna política creada y entonces se les asigna una por defecto a los equipos que se añadan al gestor.

Se deben crear a través de “New Policy”.



Se puede asignar a un dispositivo en el momento de creación.

A screenshot of the 'New Policy' configuration form in the Cisco Firepower Management Center. The form has a title 'New Policy' and a help icon. It contains several input fields: 'Name' (with the text 'ftdv-a'), 'Description', and 'Targeted Devices'. Below the 'Targeted Devices' section, there is a search bar labeled 'Search by name or value'. Under 'Available Devices', there is a list with 'FTDv1' and 'FTDv2'. A blue button labeled 'Add to Policy' is positioned between the 'Available Devices' and 'Selected Devices' sections. The 'Selected Devices' section currently contains 'FTDv1' with a trash icon next to it.

Dentro de la política se pueden configurar diversos ajustes. Resaltamos los más importantes a tener en cuenta desde el punto de vista de seguridad.

Una vez aplicados los ajustes en la política debe grabarse “Save” y aplicar con un Deploy.

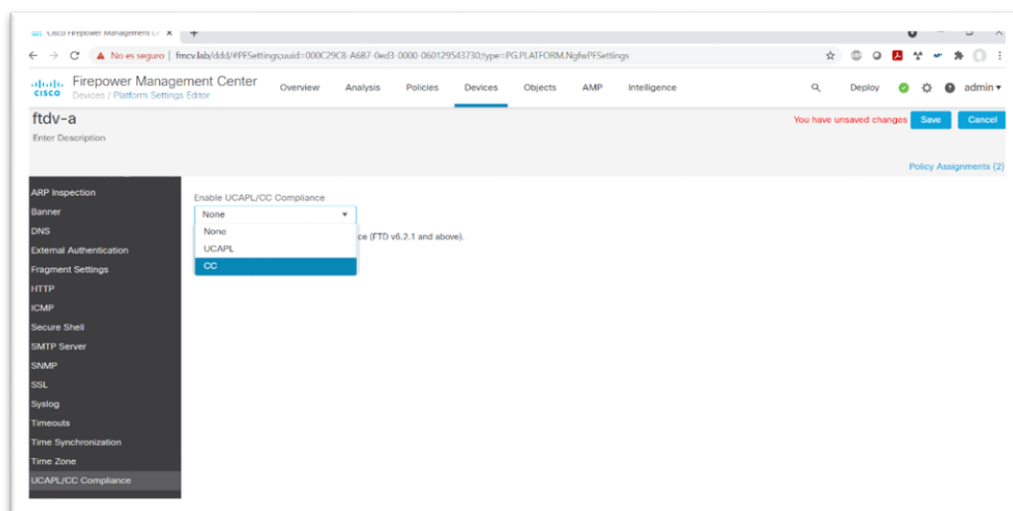
13.13.1 MODO COMMON CRITERIA

Se debe habilitar el modo Common Criteria como bastionado del equipo. Este modo reconfigura el sistema para dar cumplimiento al esquema CC, modificando cifrados, timeouts y otros parámetros del dispositivo.

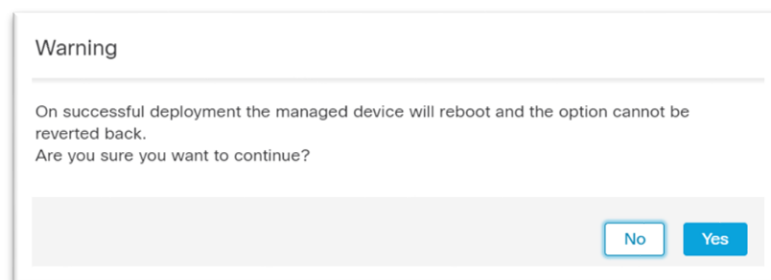
Si se activa el modo Common Criteria, este no puede ser desactivado. Debiendo procederse a una reimagen del dispositivo en tal caso.

Un cortafuegos FTD en modo Common Criteria debe ser gestionado por un FMC en modo Common Criteria también. No deben mezclarse instalaciones.

Para activar el modo se accede a la pestaña UCAPL/CC Compliance de la política.



Se mostrará un aviso de confirmación.



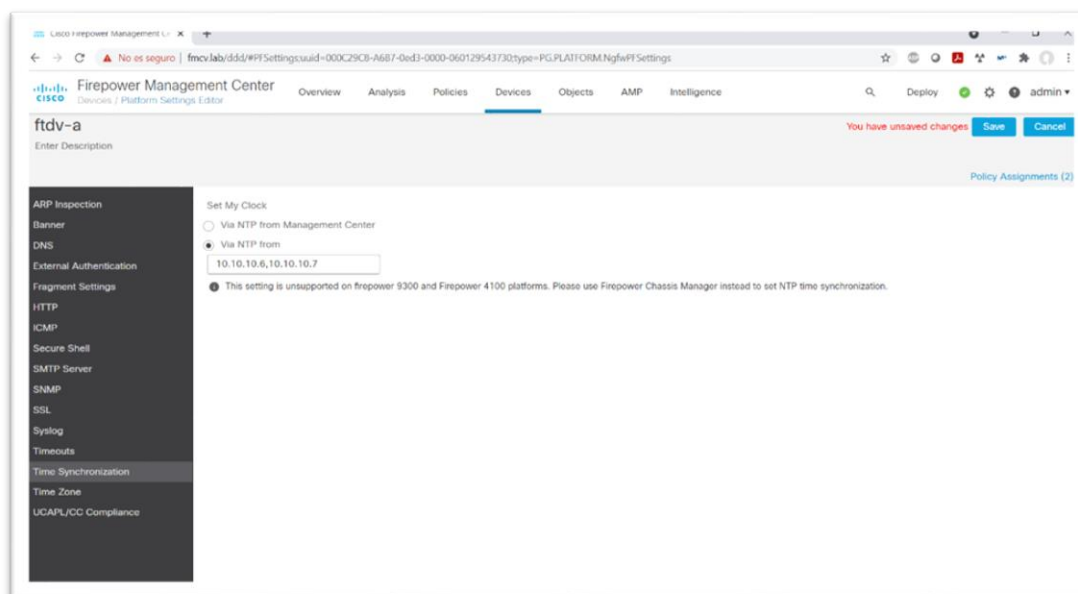
13.13.2 SINCRONIZACIÓN DE HORA (NTP)

Los equipos Firepower 4100/9300 sincronizan su hora a través del sistema FXOS, esta opción no se aplica a estos equipos.

Los equipos ASA, ISA 3000 y Firepower 1000/2100, en cambio, deben ser configurados a través de una política de plataforma.

Por defecto sincronizan su hora a través del FMC que actúa como servidor NTP. Se recomienda, en cambio, que los dispositivos se sincronicen directamente con el servidor o servidores NTP de la red de Gestión.

Para configurarlo se accede a la pestaña Time Synchronization de la política. Se pueden especificar varios servidores separados por comas.

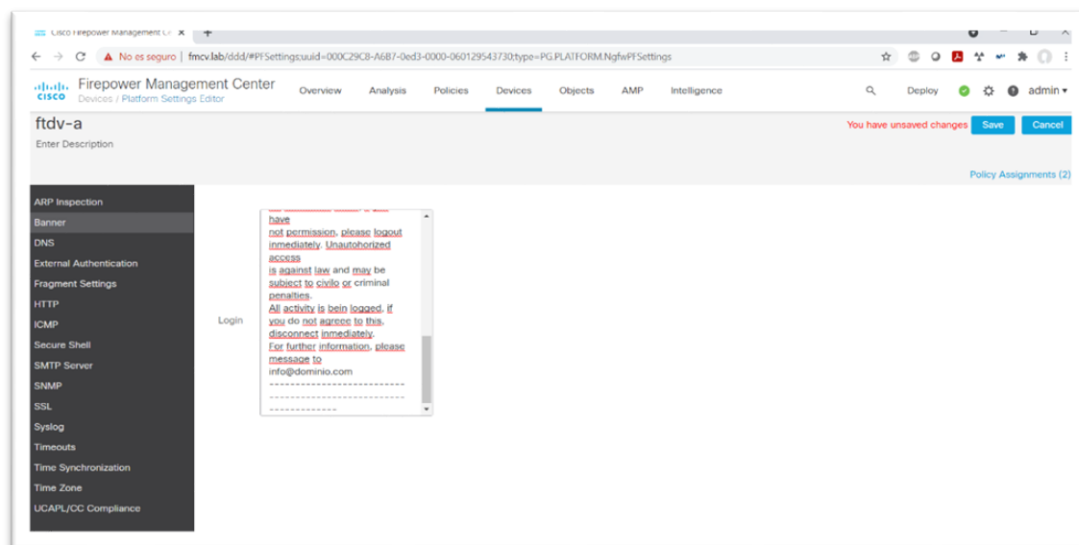


13.13.3 CONFIGURACIÓN DE BANNER

Es conveniente y requisito en ciertos entornos de seguridad la configuración de un banner de acceso.

En este caso el banner se muestra en los accesos SSH a los dispositivos, que se usa para depuración de problemas.

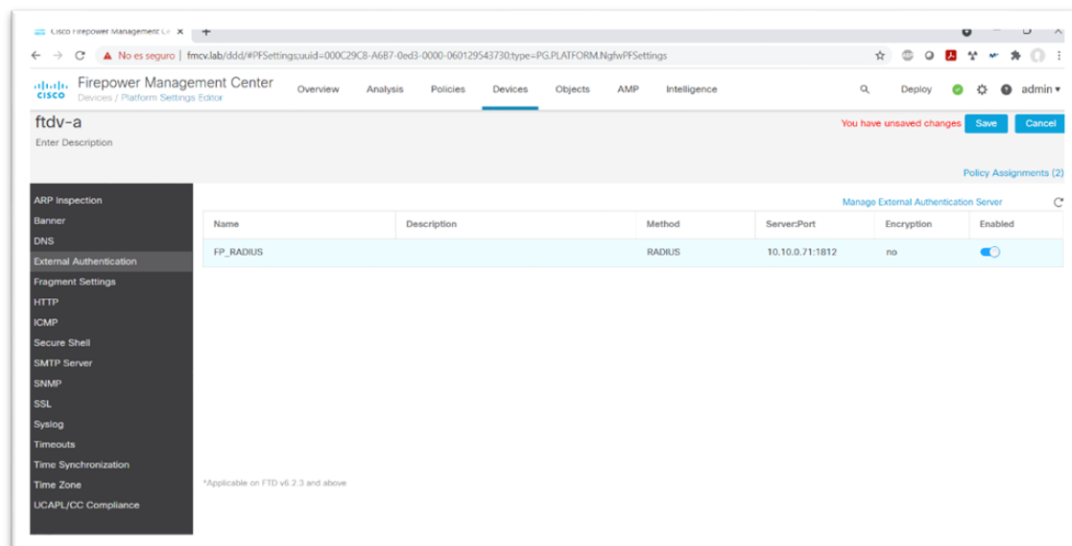
Para configurarlo se accede a la pestaña Banner de la política y se introduce el texto legal.



13.13.4 GESTIÓN DE USUARIOS – RADIUS

Se puede, y se recomienda, utilizar el mismo Radius de autenticación de FMC en los dispositivos FTD, en vez de gestión de usuarios locales.

Para configurarlo se accede a la pestaña External Authentication de la política. Aparecerá la autenticación externa Radius configurada para el FMC pero deshabilitada. Se cambia el switch a “Enabled”.



Existen 2 tipos de usuarios privilegiados en el acceso por CLI/SSH a los dispositivos FTD: “Basic” y “Config”. El usuario “Basic” solo tiene acceso de lectura.

En versiones 6.3 e inferiores, la lista de usuarios con permisos para acceder a los dispositivos FTD debe especificarse manualmente en la pantalla de configuración del Radius y los usuarios siempre acceden con privilegio “Config”. Ejemplo:

Shell Access Filter

Administrator Shell Access User List ⁱ admin,usuario1,usuario2 ex. user1, user2, user3
 (Mandatory for FTD devices)

► **Define Custom RADIUS Attributes**

Additional Test Parameters

User Name

Password

*Required Field

A partir de la versión 6.4, se recomienda dejar el campo “Shell Access Filter” vacío y utilizar el nuevo método a través del atributo “Service-Type”.

Si se deja el campo vacío y se accede a un dispositivo FTD con un usuario del Radius, se muestra el error:

```
Cisco FPR Series Security Appliance
Last login: Sat Apr 27 09:59:46 UTC 2019 from 10.124.241.7 on pts/1
Successful login attempts for user 'test' : 1
!!! Your username is not defined with a service type that is valid for this system. You are not authorized to access the system !!!
```

Se debe configurar correctamente el atributo “Service-Type” de respuesta desde el Radius. Si el atributo de respuesta es “Service-Type = Administrative-User” (valor 6), el privilegio concedido es “Config”. Si el atributo es “Service-Type = NAS-Prompt-User” (valor 7) o cualquier otro, el privilegio concedido es “Basic”.

En el primer acceso el usuario siempre será desconectado automáticamente, debido a su creación en el dispositivo (con autenticación externa), con el siguiente error:

```
Cisco FPR Series Security Appliance
Last login: Sat Apr 27 10:01:56 UTC 2019 from 10.124.241.7 on pts/1
Successful login attempts for user 'test' : 2
!!! New external username identified. Please log in again to start a session !!!
```

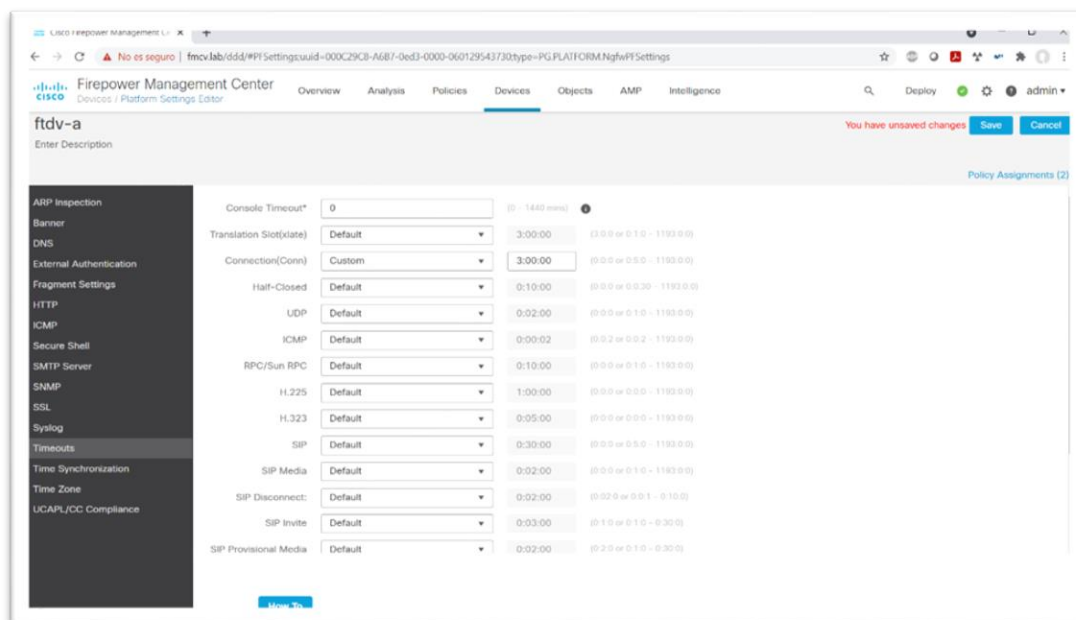
Si se cambia al usuario de privilegios, modificando su “Service-Type”, también se producirá una desconexión automática.

13.13.5 TIMEOUTS

La configuración de timeouts de conexiones del cortafuegos se gestiona a través de la pestaña “Timeouts”.

Dependiendo del entorno es posible que haya que alterar los valores por defecto.

Se recomienda alterar el valor de conexión establecida (Conn) a 3 horas, debido a que los keepalive de TCP de los equipos Windows suelen tener un valor por defecto de 2 horas, esto puede provocar el cierre prematuro de conexiones que están siendo usadas aún sin circulación de tráfico.



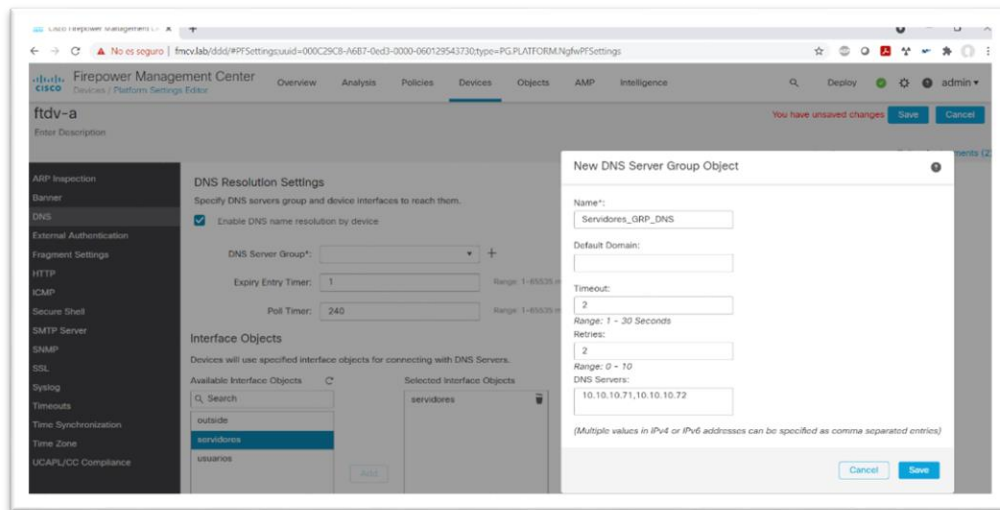
13.13.6 RESOLUCIÓN DNS

Desde la versión 6.3 es posible crear reglas en la política de acceso (ACP) con nombres en vez de direcciones IP.

Este funcionamiento se basa en la resolución periódica de esos nombres a través de servidores DNS con una expiración sobre el TTL (Time To Live) DNS configurable, y un parámetro global de polling.

Para configurar esos parámetros se debe acceder a la pestaña DNS de la política.

Se debe especificar el interfaz desde donde se realizarán las consultas y crear un objeto (grupo) de servidores DNS.

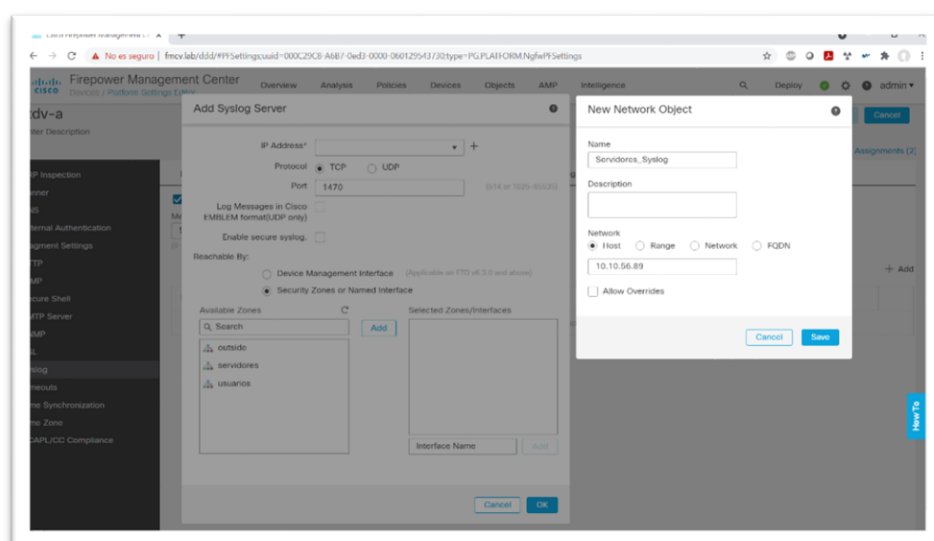


13.13.7 SYSLOG

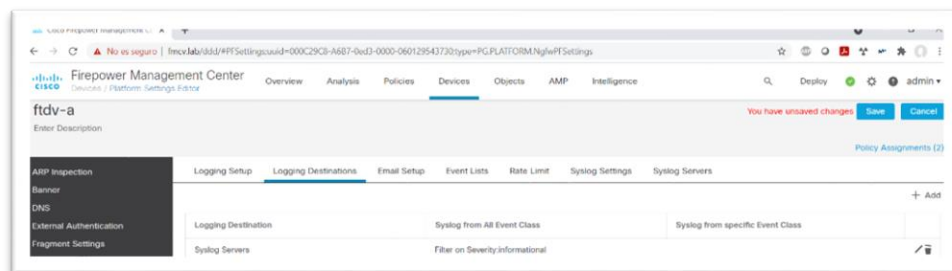
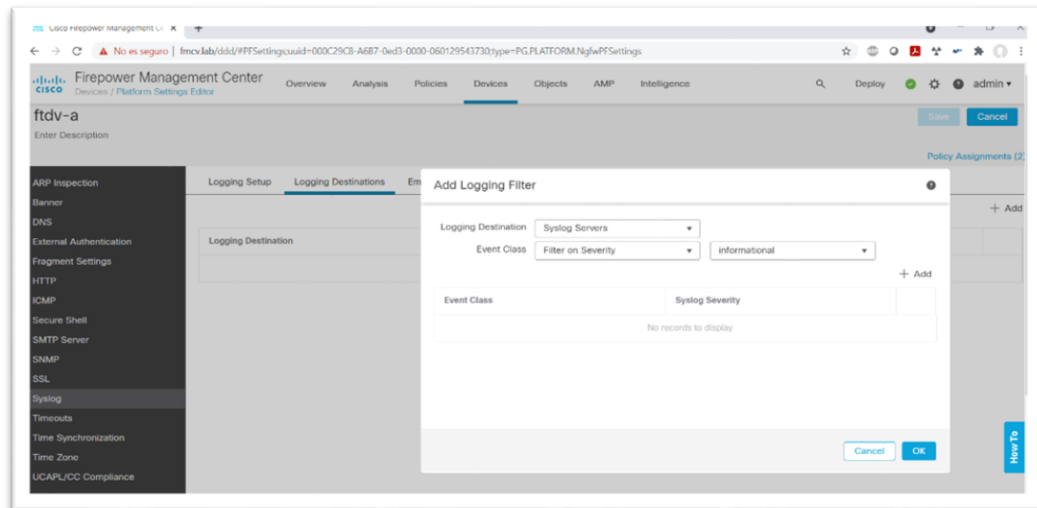
Los logs internos generados por los cortafuegos pueden ser necesarios para depurar problemas y/o, además, ser usados para almacenar toda la información de las conexiones realizadas a través del mismo.

Se accede a través de la pestaña Syslog de la política.

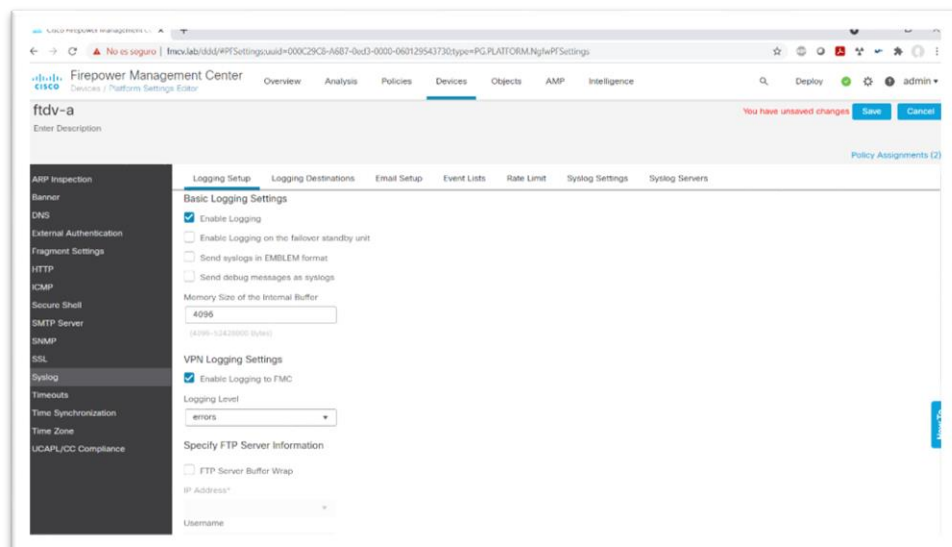
El primer paso es crear el servidor Syslog que será el destinatario de la información, con su protocolo UDP/TCP y la interfaz por donde se va a acceder a él. En la versión 6.3 se puede usar el interfaz de gestión fuera de banda.



Un ajuste que suele servir para depurar problemas es loggear todos los eventos en de nivel informational o inferior. Se debe configurar de esta manera pulsando OK, no ADD.



Por último, hay que recordar habilitar el logging.



13.14 ALTA DISPONIBILIDAD

Todos los equipos Firepower de Cisco soportan configuración en alta disponibilidad.

La alta disponibilidad es una característica de vital importancia en cortafuegos de centro de datos, no solo por la mitigación de problemas hardware, sino para realizar las actualizaciones de los equipos con un corte mínimo o inapreciable.

Además, la alta disponibilidad puede aumentar las capacidades de los cortafuegos si el funcionamiento es Activo/Activo.

13.14.1 ALTA DISPONIBILIDAD ACTIVO/PASIVO – FAILOVER

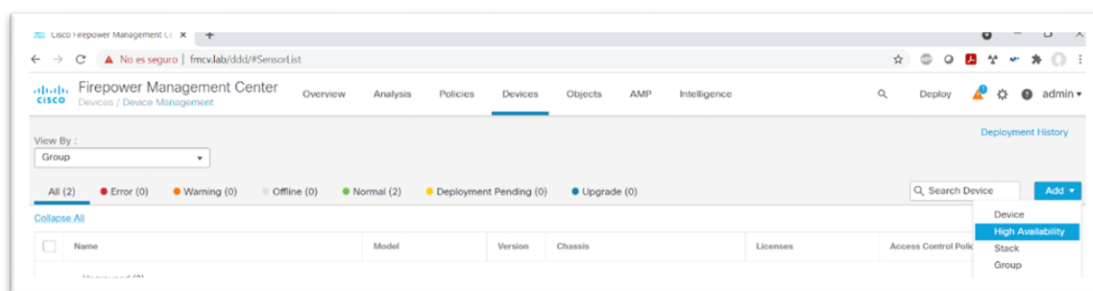
Este es el modo “típico” de alta disponibilidad, donde uno de los cortafuegos es el activo y maneja todo el tráfico, mientras que el otro está en modo “standby”, con la misma configuración, listo para intervenir en caso de fallo del activo, y replicando en su memoria la tabla de conexiones.

La ventaja de este modo de alta disponibilidad es que todas las características están disponibles. Ninguna está restringida.

Para su funcionamiento se requiere:

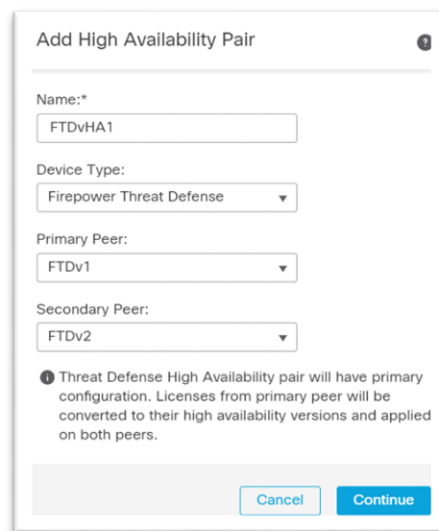
- Cortafuegos del mismo modelo y versión.
- Idénticas interfaces configurados en ambos (EtherChannels, Subinterfaces).
- 1 o 2 conexiones entre los cortafuegos y sus respectivas redes de interconexión. Se recomiendan conexiones directas, no por conmutador.
- Opcional: 2 direcciones IP en cada rango, una activa (producción) y otra pasiva (standby).

Para su configuración se accede a la página de “Device Management”. Se parte de la base de tener 2 equipos ya añadidos al gestor. Ahora se añade uno nuevo de tipo “High Availability”.



Hay que darle un nombre al nuevo dispositivo lógico que se creará que agrupará a los otros dos. Hay que seleccionar cuál de los 2 dispositivos será el primario y cual el secundario.

Nota: una vez creado el “failover” la configuración del equipo secundario será borrada y la del primario será la aplicada a ambos equipos.



Para el funcionamiento de la alta disponibilidad en este modo “failover” se necesitan 1 o 2 conexiones entre los firewalls.

Una de las conexiones “High Availability Link” monitoriza el estado de ambos equipos y la réplica de la configuración.

La otra conexión “State Link” se encarga de replicar las conexiones activas. Dependiendo de las necesidades y la carga de los equipos se pueden agrupar ambas conexiones en una única conexión.

En este ejemplo se muestra en una única conexión. Se recomienda el uso de cables de red (cruzados) entre los dispositivos, en vez de pasar por switch.

Se necesita un direccionamiento IP en este enlace, que no forma parte del “data-path” de producción de los cortafuegos. El cifrado IPSec en este enlace es opcional, pero recomendado, por la información sensible de configuración que se pasa por este enlace.

Una vez comprobamos que los datos son correctos, pulsaremos sobre ADD y se iniciará la tarea de creación del “failover”. Visualmente veremos en pantalla como se crea un nuevo dispositivo lógico que agrega a ambos equipos.

FTDvHA1 High Availability							
FTDv1(Primary, Unknown) 10.204.196.130 - Routed	FTD for VMWare	6.7.0	N/A	Base, Threat (3 more...)	FTDv1		
FTDv2(Secondary, Unknown) 10.204.196.131 - Routed	FTD for VMWare	6.7.0	N/A	Base, Threat (3 more...)	FTDv1		

Una vez terminada la tarea, veremos que figuran correctamente (en verde) y que la configuración se realiza sólo en el agregado.

FTDvHA1

High Availability

FTDv1(Primary, Active)

10.204.196.130 - Routed

FTD for VMWare

6.7.0

N/A

Base, Threat (3 more...)

FTDv1

FTDv2(Secondary, Standby)

10.204.196.131 - Routed

FTD for VMWare

6.7.0

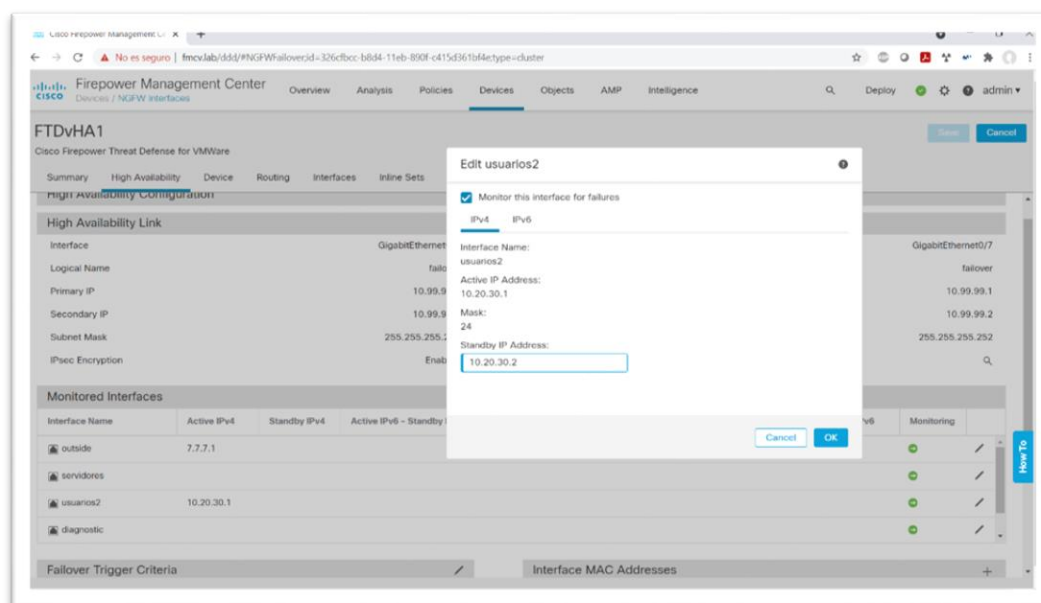
N/A

Base, Threat (3 more...)

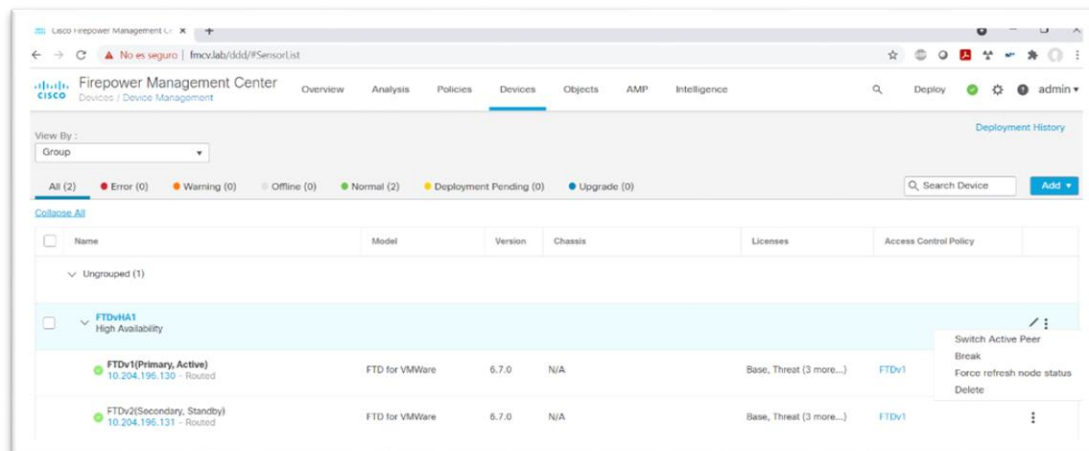
FTDv1

Se recomienda que en cada interfaz con IP se configure la IP de standby, esto mejora la detección de fallos al monitorizarse los cortafuegos uno a otro a nivel IP.

En este ejemplo podemos ver una interfaz configurada, para producción, con IP 10.55.55.1 y como IP de standby 10.55.55.2. Esto se realiza en la pestaña de “High Availability”. Se debe repetir una operación similar por cada interfaz.



Aparecen nuevas opciones de menú que permiten realizar una conmutación de activo/pasivo, romper el modo de alta disponibilidad y realizar un refresco de la alta disponibilidad.



Si se realiza una conmutación el Activo pasará a Standby y viceversa. Esta operación no suele conllevar un corte perceptible.

Nota: En caso de romper el clúster, el equipo en Activo en ese momento retendrá la configuración, mientras que el standby perderá la configuración. Esto permite romper la alta disponibilidad de manera segura en caso de que queramos que un equipo se quede funcionando.

13.14.2 ALTA DISPONIBILIDAD ACTIVO/ACTIVO – CLUSTER

En esta configuración, 2 o más equipos, funcionan de manera paralela dando servicio de producción. El rendimiento no se dobla, pero se calcula una media del 70% de mejora de rendimiento. Cisco, en base a sus pruebas de rendimiento, da unos valores de mejora de entre un 60% y 80%, por equipo.

La desventaja de este modo es que hay características que no pueden usarse:

- VPN de acceso remoto.
- DHCP, modo cliente y servidor (DHCP Relay sí funciona).

Otras funcionalidades, como VPN Lan-to-Lan funcionan solo desde el nodo principal.

Los equipos Firepower 1000/2100 no pueden utilizarse en clúster.

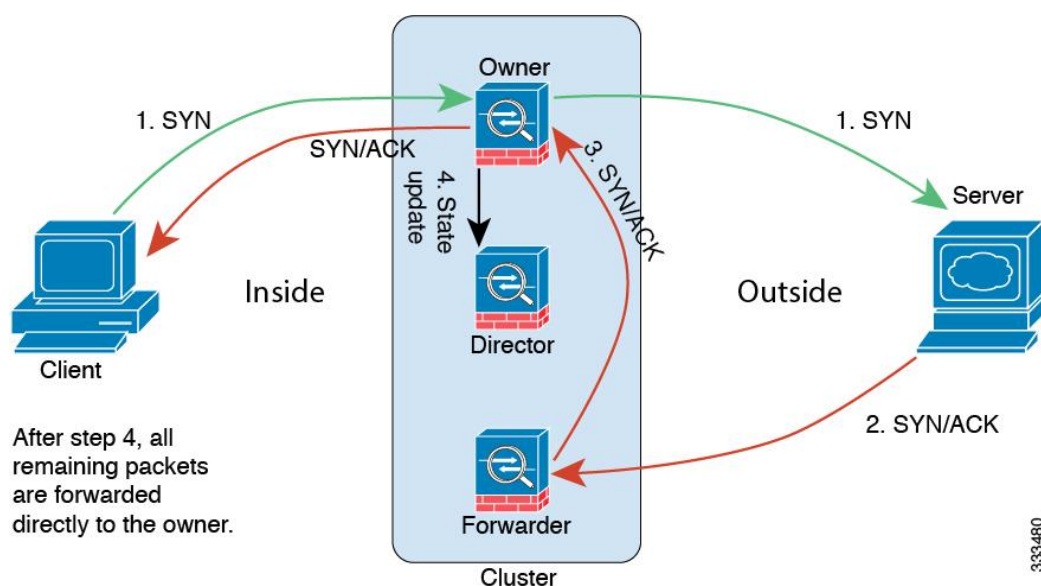
Los requisitos para la configuración de este modo de alta disponibilidad son:

- Mismos modelos de equipos exactos y versiones.
- Misma configuración de interfaces (Etherchannels).
- Inter-cluster link en PortChannel 48.

El Cluster requiere que se instale la imagen específicamente en modo clúster desde FXOS.

El funcionamiento del sistema Cluster consiste en utilizar agregación de puertos (EtherChannels) para distribuir el tráfico entre miembros del Cluster. Si las conexiones son asimétricas, es decir, la ida y la vuelta no coinciden con el mismo nodo cortafuegos, se usa el inter-cluster link para redirigir el paquete de vuelta al “owner” de la conexión.

El funcionamiento se muestra en este esquema:

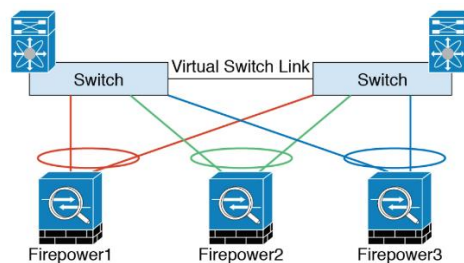


El inter-luster link siempre es un EtherChannel, el PortChannel 48.

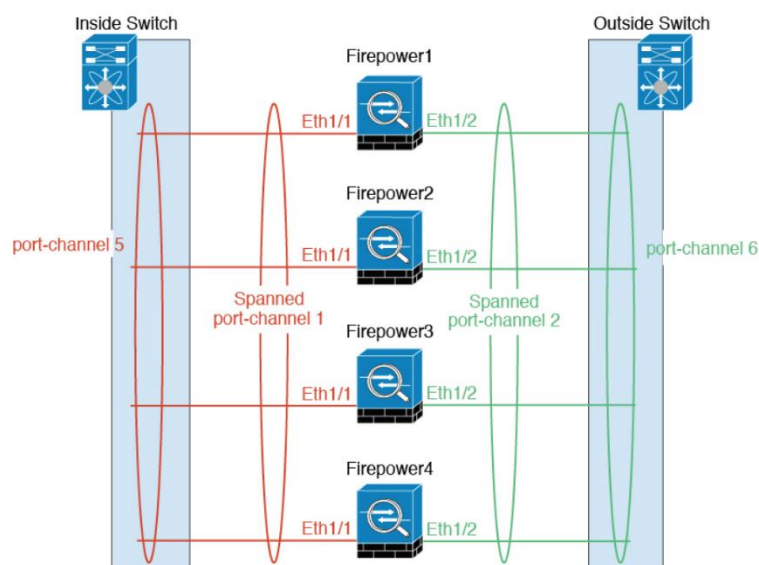
El correcto dimensionamiento de esta unión es importante para el bien funcionamiento de este sistema.

Nota: En la unión inter-cluster NO se puede usar un cable cruzado entre dos equipos, aunque se forme un Cluster de solo 2 equipos, ya que la monitorización del link es vital para el funcionamiento del nodo. En caso de perder el link el nodo deja de funcionar. Por tanto, si uno de los nodos fallara, el otro, aun siendo funcional, se quedaría sin link, y entonces tampoco daría servicio, originando una caída completa del servicio.

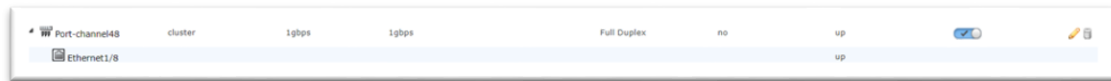
Idealmente, un inter-cluster link debería usar 2 switches con EtherChannel multichassis (vPC).



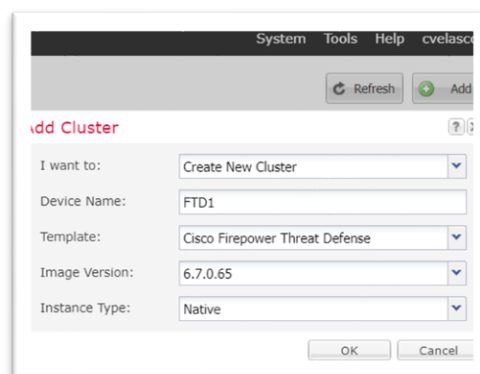
Para el tráfico de datos de producción, lo que se pretende es la distribución de tráfico mayor posible entre los nodos, para lo que se crean también agregaciones de puertos (EtherChannels) en todas las interfaces de datos.



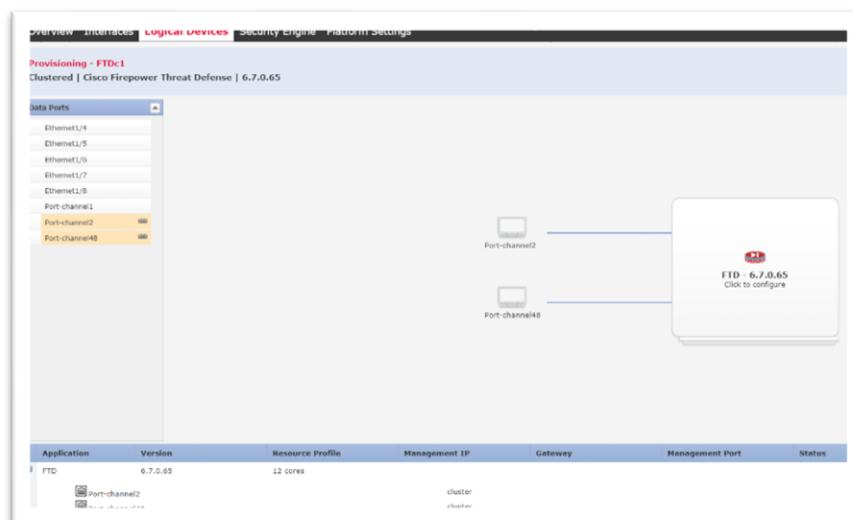
Para la configuración del Cluster, el primer paso es configurar las interfaces en FXOS y asignar interfaces reales al PortChannel 48. En este caso vamos a usar solo un interfaz físico. Lo asignamos en ambos cortafuegos, mediante el FXOS Chassis Manager.



Empezaremos creando el Logical Device del primero nodo, Master o Primario. Debe ser creado específicamente en modo Cluster, y como nuevo.



En la configuración del Logical Device debemos seleccionar tanto el PortChannel 48 de Inter-cluster link como las interfaces de datos, en este caso hemos creado otro PortChannel 1 para datos. Recordad que deben ser Port Channels para la distribución del tráfico de producción.



Se debe asignar un número de chasis y una contraseña de Cluster.

Cisco Firepower Threat Defense - Bootstrap Configuration

Cluster Information Settings Interface Information Agreement

Interface Information

Chassis ID: 1

Site ID:

Cluster Key:

Confirm Cluster Key:

Cluster Group Name: FWCLUSTER1

Management Interface: Ethernet1/1

El resto de parámetros es igual que una instalación normal, especificando la IP de gestión fuera de banda, y el gestor FMC. Aceptar el acuerdo de licencia.

Cisco Firepower Threat Defense - Bootstrap Configuration

Cluster Information Interface Information Settings Agreement

Registration Key:

Confirm Registration Key:

Password:

Confirm Password:

Firepower Management Center IP: 10.40.40.1

Permit Expert mode for FTD SSH sessions: yes

Search domains:

Firewall Mode: Routed

DNS Servers: 10.10.10.56

Firepower Management Center NAT ID:

Fully Qualified Hostname: FTDcl.lab

Eventing Interface: None

Cisco Firepower Threat Defense - Bootstrap Configuration

Cluster Information Settings Interface Information Agreement

Address Type: IPv4 only

Security Module 1

IPv4

Management IP: 10.10.10.3

Network Mask: 255.255.255.0

Gateway: 10.10.10.1

Una vez instalado y online, se debe comprobar que el estado es “in-cluster”. Podemos extraer la configuración pinchando en el icono. Esta configuración la usaremos para añadir más nodos al clúster de manera fácil.

Cisco Firepower Threat Defense - Bootstrap Configuration

Cluster Information Settings Interface Information Agreement

Management Port

Ethernet1/1

Status

Online

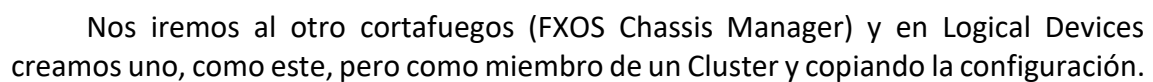
Attributes

Cluster Operational Status: in-cluster

Delete

Set version

Show Configuration



Copy Cluster Details

```
ed", "inlinePeerName": "", "adminDuplex": "fullDuplex", "autoNeg": "no"},  
eed": "10gbps", "adminState": "disabled", "aggrPortId": "0", "chassisId": "/N/  
:"104", "flowCtrlPolicy": "default", "ifType": "physical", "locale": "external", "m  
ortId": "4", "slotId": "1", "ssaPortType": "data", "ssaVlanId": "104", "switchId  
-admin-  
urlink": "https://10.149.224.6/api/ports/ep/Ethernet1_API_SLASH_4", "vl  
abled", "inlinePeerName": "", "adminDuplex": "fullDuplex", "autoNeg": "no"},  
eed": "10gbps", "adminState": "enabled", "aggrPortId": "0", "chassisId": "/N/  
:"101", "flowCtrlPolicy": "default", "ifType": "physical", "locale": "external", "m  
t": "1", "slotId": "1", "ssaPortType": "mgmt", "ssaVlanId": "101", "switchId": "A  
min-  
urlink": "https://10.149.224.6/api/ports/ep/Ethernet1_API_SLASH_1", "vl  
pled", "inlinePeerName": "", "adminDuplex": "fullDuplex", "autoNeg": "no"}]]
```

OK Cancel

Se asignarán el número de chasis y los datos de IP de gestión, contraseñas y aceptación de acuerdo de licencia.

Esperamos la instalación y comprobamos que queda online y el estado “in-cluster”.

Application	Version	Management IP	Gateway	Management Port	Status
FTD	6.2.3.83	10.149.224.11	10.149.224.1	Ethernet1/1	online

Ports: Data Interfaces: Port-channel1, Cluster Interfaces: Port-channel148

Attributes: Cluster Operational Status: in-cluster, Firepower Management IP: 10.149.224.11, Cluster Role: master, Management URL: https://10.149.224.5/, UUID: b718ce60-b6ab-11e8-b1c1-921ed0cc56b

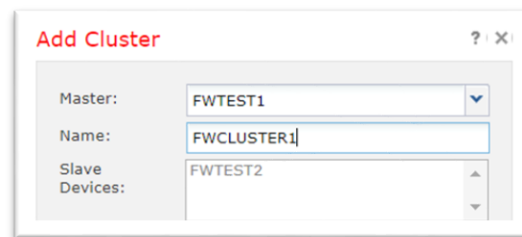
El paso siguiente se realiza desde el gestor FMC, el cual hemos configurado en los Logical Devices instalados.

En la pantalla de Device Manager, añadimos primero los equipos por separado con Add Device.

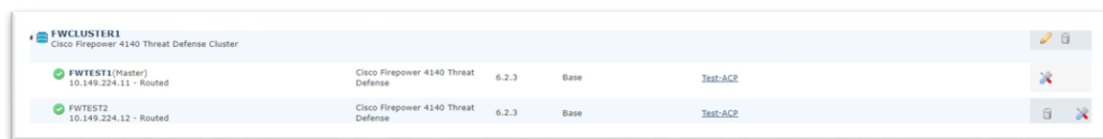
Una vez que aparezcan los 2 como disponibles procederemos a añadirlos como Clusters.



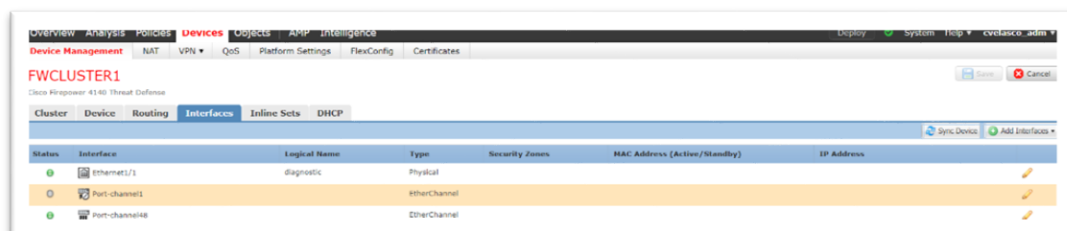
Seleccionamos el Master/Primario del Cluster y le asignamos un nombre, que será el del agregado de los 2 equipos.



Una vez terminada la tarea, comprobaremos que aparece el Cluster agregado correctamente al FMC.



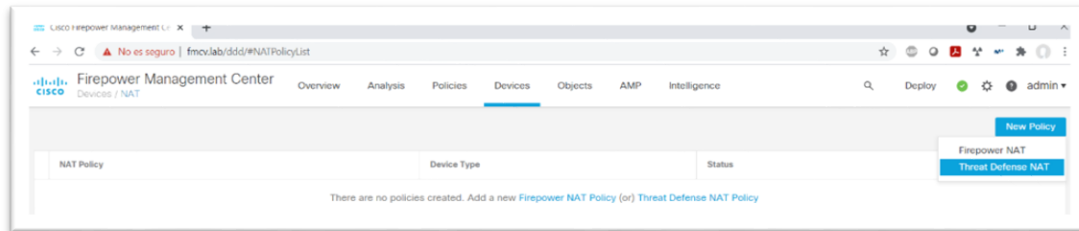
Si editamos el dispositivo, veremos que tenemos en Interfaces nuestro PortChannel 1 desde el que derivar subinterfaces VLAN de datos y el 48 de inter-cluster link.



13.15 POLÍTICA DE NAT

La configuración de traducción de direcciones (NAT) se realiza en una política separada específica para ello.

Se accede a la configuración a través de Devices->NAT y se crea de tipo “Threat Defense NAT” para dispositivos FTD.



Existen 2 tipos de reglas de NAT, automáticas y manuales. Las automáticas requieren menos configuración, pero son menos flexibles y ofrecen menos posibilidades.

Existe un orden de precedencia de reglas, según el tipo (auto/manual) y donde insertemos las manuales (before/after). El orden es:

- Manual Before.
- Auto.
- Manual After.

En esta guía vamos a utilizar reglas Manual, ya que son las que ofrecen mayor control. Por lo general se usan reglas Before.

Nota: las reglas de NAT se evalúan de arriba a abajo, donde la primera coincidencia (match) que se encuentre será la regla utilizada. Por lo tanto, la política se debe configurar con reglas más específicas en la parte alta y genéricas en la parte baja.

En general todas las traducciones (NAT) deben ser evitadas, y solo usarse cuando sea requerido, como conexiones a Internet.

La única razón, desde el punto de vista de seguridad, para su uso es el mismo que desaconseja su uso. Los NAT “esconden” la verdadera IP origen o destino, y eso puede resultar beneficioso o perjudicial dependiendo del lado en el que estemos mirando.

13.15.1 NAT DINÁMICO

Estos NAT son de “salida”. Agrupan un conjunto de direcciones IP en 1 sola IP mediante traducción de puertos (NAT/PAT). Es el equivalente en Cisco IOS de NAT overload.

Un ejemplo típico de este NAT es una conexión a Internet. Creamos una regla de NAT dinámico, desde la zona de Usuarios (entrada) a la zona de Internet (Salida).

Add NAT Rule

NAT Rule:
Manual NAT Rule

Insert:
In Category NAT Rules Before

Type:
Dynamic

☒ Enable

Description:
NAT ~~Generico~~ - Todos los usuarios

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

Q Search by name

outside
servidores
usuarios

Add to Source
Add to Destination

Source Interface Objects (1)
usuarios

Destination Interface Objects (1)
outside

Como es una regla genérica para todos los usuarios, especificamos any-ipv4 en rango de origen. Y vamos a convertir la IP origen en la del propio interfaz del cortafuegos.

Add NAT Rule

NAT Rule:
Manual NAT Rule

Insert:
In Category NAT Rules Before

Type:
Dynamic

☒ Enable

Description:
NAT ~~Generico~~ - Todos los usuarios

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:*
any-ipv4 +

Original Destination:
Address +

Original Source Port:
+ +

Original Destination Port:
+ +

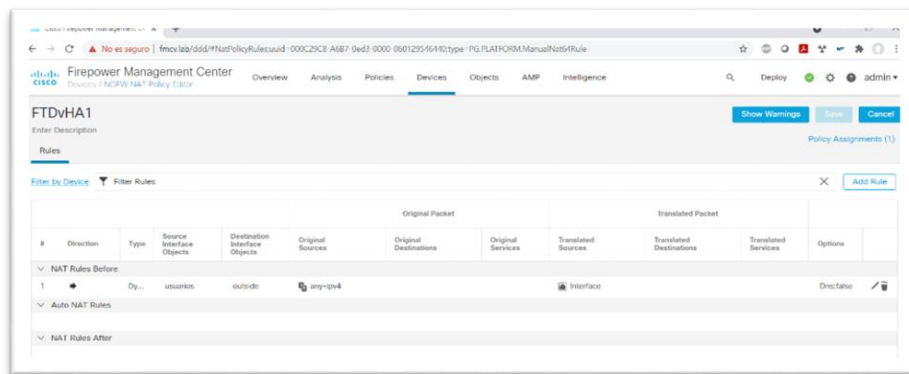
Translated Packet

Translated Source:
Destination Interface IP
The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Destination:
+ +

Translated Source Port:
+ +

Translated Destination Port:
+ +



Ya tenemos creado el NAT y los usuarios pueden salir a Internet.

Pero ahora, nos indican que un usuario debe usar otra salida especial a través de una IP.

Este es un ERROR muy común. Supongamos que repetimos la operación, esta vez, poniendo el rango/host del usuario "vip".

New Network Object

Name
Internet_VIP

Description

Network
☒ Host ☐ Range ☐ Network ☐ FQDN
 7.7.7.7

New Network Object

Name
Usuario_VIP

Description

Network
☒ Host ☐ Range ☐ Network ☐ FQDN
 10.10.10.44

Edit NAT Rule

NAT Rule:
Manual NAT Rule

Insert:
In Category NAT Rules Before

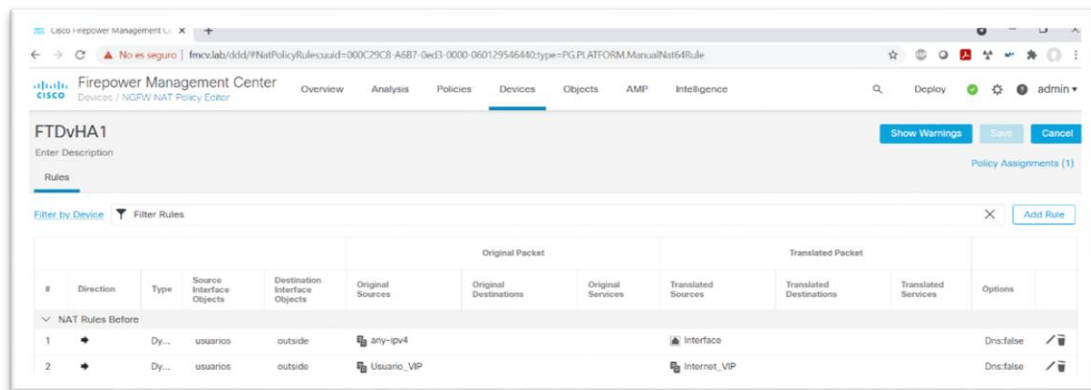
Type:
Dynamic

☒ Enable

Description:
NAT Usuario VIP

Interface Objects Translation PAT Pool Advanced

Original Packet	Translated Packet
Original Source: Usuario_VIP	Translated Source: Address
Original Destination: Address	Translated Destination: Internet_VIP
Original Source Port: Address	Translated Source Port: Address
Original Destination Port: Address	Translated Destination Port: Address

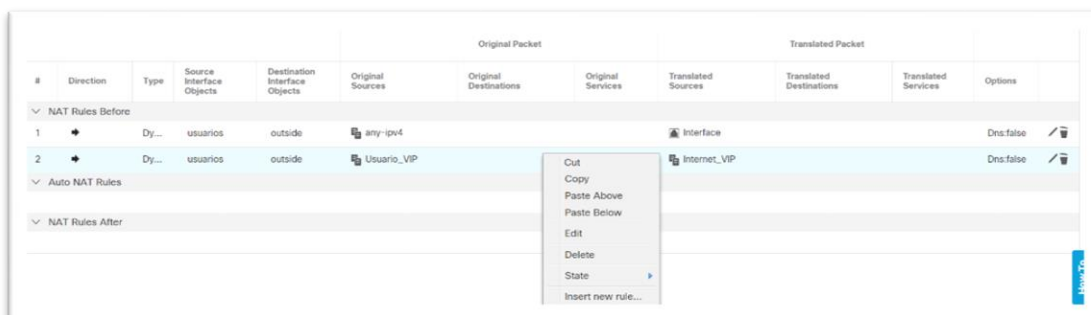


Pensamos que está correcto, pero es un error. Si comprobamos con un packet-tracer, el cortafuegos nos dice que sale por la primera regla traduciendo a la IP del interfaz.

Phase: 6
 Type: NAT
 Subtype:
 Result: ALLOW
 Config:
 nat (usuarios,outside) source dynamic any interface description **NAT Generico - Todos los Usuarios**
 Additional Information:
 Dynamic translate 10.10.10.44/2335 to 10.50.50.1/2335

El error se debe a que se ha puesto la regla de usuario VIP debajo de la genérica, cuando esta es más específica, y debe ser al revés, debe estar arriba.

Pulsando botón derecho del ratón, podemos fácilmente cortar la segunda regla.



Y pegarla por encima de la primera ("Paste Above").

					Original Packet			Translated Packet				
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
NAT Rules Before												
1	+	Dy...	usuarios	outside	any-ipv4			Interface			Dns:false	/
2	+	Dy...	usuarios	outside	Usuario_VIP			Internet_VIP			Dns:false	/
Auto NAT Rules												
NAT Rules After												

					Original Packet			Translated Packet				
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
NAT Rules Before												
1	+	Dy...	usuarios	outside	Usuario_VIP			Internet_VIP			Dns:false	/
2	+	Dy...	usuarios	outside	any-ipv4			Interface			Dns:false	/

Ahora, en el orden correcto, el equipo hace justamente lo que se requería.

Phase: 5
 Type: NAT
 Subtype:
 Result: ALLOW
 Config:
 nat (usuarios,outside) source dynamic Usuario_VIP Internet_VIP description **NAT Usuario VIP**
 Additional Information:
 Dynamic translate 10.10.10.44/2336 to 7.7.7.7/2336

13.15.2 NAT ESTÁTICO

El uso común de estos NAT es realizar una traducción 1:1 bien de IP a IP o de puerto. En el caso de Internet es la publicación de un puerto de una IP privada de nuestra red.

Como norma general se recomienda que los NAT estáticos figuren por encima de los dinámicos.

En este ejemplo vamos a publicar un servidor en Internet. La regla siempre se mira desde nuestra entrada. Es decir, el origen es nuestra zona de servidores y la salida es Internet.

Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category NAT Rules Before

Type: Static

☒ Enable

Description: Publicacion_Servidor

Interface Objects Translation PAT Pool Advanced

Available Interface Objects

- outside
- servidores
- usuarios

Source Interface Objects (1) Destination Interface Objects (1)

servidores outside

Add to Source Add to Destination

New Network Object

Name: Servidor_publico

Description:

Network: ☒ Host ☐ Range ☐ Network ☐ FQDN

10.30.30.10

☐ Allow Overrides

New Port Objects

Name: tcp_10180

Protocol: ☒ TCP ☐ UDP ☐ ICMP ☐ IPv6-ICMP ☐ Other

All

Port: 10180

☐ Allow Overrides

Cancel Save

Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: In Category NAT Rules Before

Type: Static

☒ Enable

Description: Publicacion_Servidor

Interface Objects Translation PAT Pool Advanced

Original Packet Translated Packet

Original Source:* Servidor_publico +

Original Destination: Address +

Original Source Port: HTTP +

Original Destination Port: +

Translated Source: Destination Interface IP

Translated Destination: +

Translated Source Port: tcp_10180 +

Translated Destination Port: +

					Original Packet			Translated Packet				
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options	
NAT Rules Before												
1	→	Dy...	usuarios	outside	Usuario_VIP			Internet_VIP			Dns:false	🗑️
2	→	Dy...	usuarios	outside	any-ipv4			Interface			Dns:false	🗑️
3	↔	St...	servidores	outside	Servidor_publico		HTTP Original	Interface		top_10180 Original	Dns:false	🗑️

Comprobamos que la traducción funciona correctamente.

Phase: 2
 Type: UN-NAT
 Subtype: static
 Result: ALLOW
 Config:
 nat (servidores,outside) source static Servidor_publico interface service SVC_30064774696 SVC_30064774697
 description **Publicacion Servidor**
 Additional Information:
 NAT divert to egress interface Servidores
 Untranslate 10.50.50.1/10180 to 10.30.30.10/80

Nota: Desde el punto de vista de la política de control acceso (ACP), las direcciones IP son las reales, no las de NAT. Es decir, si queremos hacer una regla que permita el tráfico entrante desde Internet al servidor que hemos publicado, se debe usar como destino la IP Real del servidor (10.30.30.10), y no la publicación de la IP del interfaz del cortafuegos (10.50.50.1).

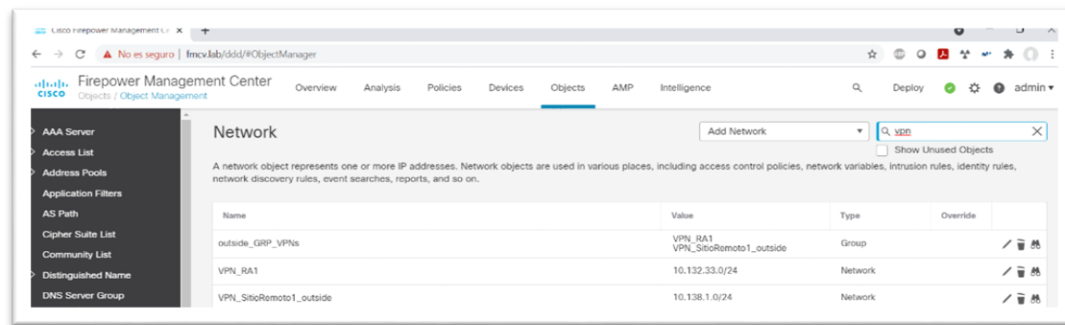
13.15.3 NAT DE IDENTIDAD – IDENTITY NAT

En ocasiones, especialmente cuando se configuran redes virtuales (VPN), es necesario especificar una traducción de direcciones que traduce a las mismas direcciones. Es decir, no traducir, o realizar una exención de traducción.

Por ejemplo, si existe un NAT dinámico (genérico) para que diversos equipos de nuestra red accedan a Internet, y se establece una VPN, si esos rangos se traducen en el NAT dinámico genérico, nunca irán por la red privada virtual (VPN).

Para un NAT de identidad se crea un NAT estático que no hace una traducción de las direcciones IP origen y que su coincidencia “match” se especifica por destino.

Aunque se puede configurar la regla de NAT directamente, es mejor crear los objetos primero. En este ejemplo tenemos 2 rangos de redes VPN agrupados en un objeto de grupo. Menú Objects->Object Management->Network.



La regla de NAT debe configurarse especificando “any” o “any-ipv4” para el origen, tanto en el paquete original como el traducido. En el traducido se consigue dejándolo en blanco. Y para el destino se debe especificar, tanto en origen como destino, el objeto que hemos creado previamente. Es conveniente también seleccionar que no se haga proxy-arp en “Advanced”.

Add NAT Rule

NAT Rule: Manual NAT Rule

Insert: Above Rule 1

Type: Static

☒ Enable

Description: NAT de Identidad para VPNs

Interface Objects Translation PAT Pool Advanced

Original Packet

Original Source:* any-ipv4 +

Original Destination: Address +

outside_GRP_VPNs +

Original Source Port: +

Original Destination Port: +

Translated Packet

Translated Source: Address +

Translated Destination: outside_GRP_VPNs +

Translated Source Port: +

Translated Destination Port: +

Las traducciones deben quedar, por tanto, de esta manera:

					Original Packet			Translated Packet			
#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
NAT Rules Before											
1		St...	any	any	any-ipv4	outside_GRP_VPNs		any-ipv4	outside_GRP_VPNs		Dns:false
2		Dy...	usuarios	outside	Usuario_VIP			Internet_VIP			Dns:false
3		Dy...	usuarios	outside	any-ipv4			Interface			Dns:false

Nota: No debe especificarse ningún interfaz como origen, y como destino se debe especificar la salida a Internet o el interfaz correspondiente que da a la VPN. Si se configura un interfaz origen podría entrar en funcionamiento el mecanismo de “NAT Divert” que se salta la tabla de rutas para dirigir un paquete traducido rápidamente al interfaz origen en el NAT. Esto normalmente no es deseado para este tipo de NAT.

13.16 POLÍTICA DE ACCESO – ACCESS CONTROL POLICY (ACP)

La Access Control Policy es el punto principal de filtrado del cortafuegos.

En ella se crean las reglas que permiten o deniegan conexiones conforme a diferentes parámetros y otras políticas.

Se accede desde el FMC a través de Políticas->Access Control->Access Control.

Como norma general, las ACP deben denegar todo el tráfico (default Block) y se crean reglas para permitir el tráfico deseado.

Existen 2 secciones donde añadir reglas, Mandatory y Default. Se diferencian en la precedencia de las reglas y, especialmente si se trabaja con herencia de políticas de acceso.

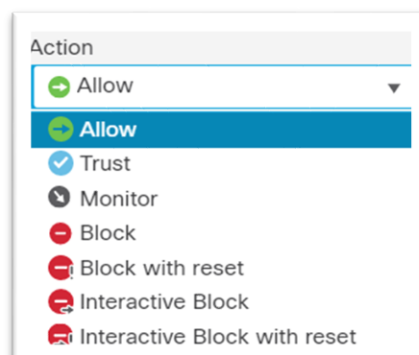
Se pueden crear Categorías, por ejemplo “Usuarios a Servidores Web”, y agrupar reglas por categorías para facilitar la legibilidad y búsqueda.

Vamos a repasar los conceptos básicos de una regla ACP.

Una regla debe tener un nombre (Name) único. Se puede recurrir al truco de añadir un número al final.

Las acciones normales son Allow y Block with Reset.

Trust es igual que Allow pero se salta la política IPS y AMP y el tráfico es permitido, mientras que Allow está sujeto a esas inspecciones.



Add Rule

Name: SRV Web 1 ☒ Enabled Insert: into Mandatory

Action: Allow Time Range: None

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comments

Available Zones: Q Search by name

- outside
- servidores
- usuarios

Source Zones (2): servidores, usuarios

Destination Zones (1): outside

Buttons: Add to Source, Add to Destination

Las reglas contienen varias pestañas que reflejan opciones de configuración para lograr “matches”.

Simplificándolo, dentro de la misma pestaña, en vertical, la lógica es un OR y en horizontal es un AND.

Por ejemplo, esa regla permite tráfico que va desde las zonas de seguridad Servidores OR Usuarios a la de destino Internet, y además el puerto destino es HTTP(80) or HTTPS(443).

Add Rule

Name: SRV Web 1 ☒ Enabled Insert: into Mandatory

Action: Allow Time Range: None

Zones Networks VLAN Tags Users Applications **Ports** URLs SGT/ISE Attributes Inspection Logging Comments

Available Ports: Q http

- HTTP
- HTTPS

Selected Source Ports (0): any

Selected Destination Ports (2): HTTP, HTTPS

Buttons: Add to Source, Add to Destination

Protocol: TCP (6) Port: Enter a Add Protocol: TCP (6) Port: Enter a Add

Buttons: Cancel Add

Se puede mezclar cualquier pestaña, por ejemplo, zones+networks+ports.

Add Rule

Name: ☒ Enabled Insert:

Action: Time Range:

Zones Networks VLAN Tags Users Applications Ports URLs SGT/ISE Attributes Inspection Logging Comm

Available Networks

Source Networks (0) Destination Networks (1)

Source: any Destination: Servidores_CIFS

Enter an IP address Enter an IP address

Rules														Security Intelligence		HTTP Responses		Logging		Advanced		Prefilter Policy: Default Prefilter Policy				SSL Policy: None		Identity Policy: None					
Filter by Device														Search Rules														☐ Show Rule Conflicts		+ Add Category		+ Add Rule	
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applica...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action	     																		
✓ Mandatory - FTDvIA1 (1-2)																																	
1	SRV Web 1	servidores usuarios	outside	Any	Servidores_CIFS	Any	Any	Any	Any	HTTP HTTPS	Any	Any	Any	 Allow	     																		
2	CDU FIRE	...	...	...	...	...	...	...	...	...	...	...	...	 Allow	     																		

13.16.1 LOG DE CONEXIONES – SYSLOG

Para poder utilizar un syslog externo y logear eventos de reglas, se recomienda configurar el syslog de manera global en la ACP.

Create Syslog Alert Configuration

Name:

Host:

Port:

Facility:

Severity:

Tag:

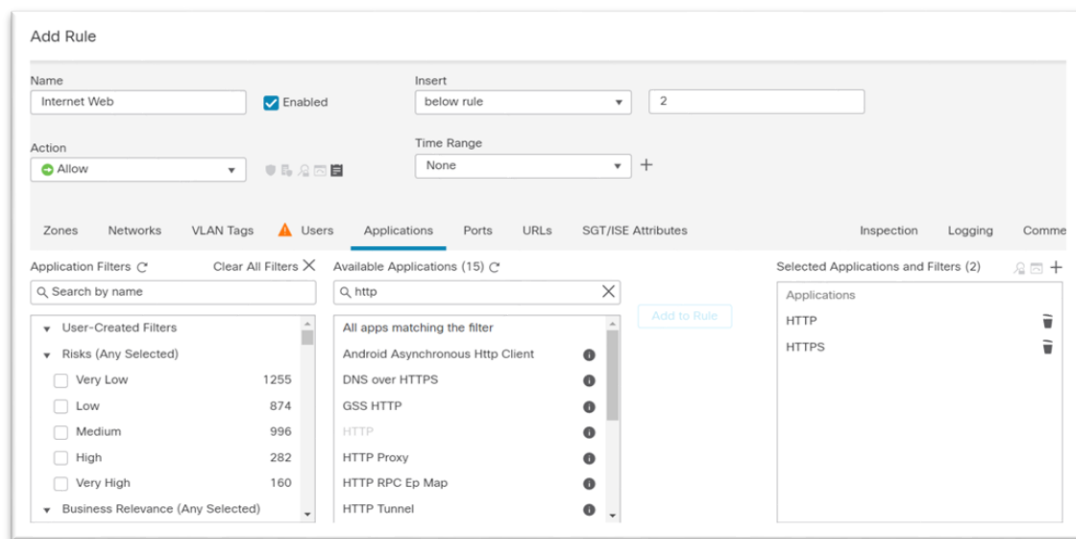
Luego en cada regla podemos decidir si se logeará al comienzo de la conexión y/o al final. También si se enviará el log al FMC (Event Viewer) y al syslog externo.

Dentro del FMC, se pueden visualizar las conexiones en Analysis->Connections->Events.

Time	Action	Reason	Initiator IP	Initiator Country	Initiator User	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Type
2021-05-21 05:51:55	Block with reset		192.168.100.9			172.20.2.6			dmz	inside	5566 / tcp	139 / tcp
2021-05-21 05:29:29	Allow	File Monitor	192.168.100.9			77.209.227.9	ESP		dmz	outside	4777 / tcp	80 / http
2021-05-21 05:28:45	Allow	File Monitor	192.168.100.9			205.185.216.10	USA		dmz	outside	4733 / tcp	80 / http
2021-05-21 05:28:03	Allow	File Monitor	192.168.100.9			205.185.216.42	USA		dmz	outside	4685 / tcp	80 / http
2021-05-21 05:28:03	Allow	File Monitor	192.168.100.9			205.185.216.10	USA		dmz	outside	4686 / tcp	80 / http
2021-05-21 05:24:44	Allow	File Monitor	192.168.100.9			8.238.15.126	USA		dmz	outside	4568 / tcp	80 / http
2021-05-21 05:23:25	Allow	File Monitor	192.168.100.9			77.209.227.9	ESP		dmz	outside	4495 / tcp	80 / http
2021-05-21 05:23:13	Allow	File Monitor	192.168.100.9			205.185.216.10	USA		dmz	outside	4472 / tcp	80 / http
2021-05-21 05:23:13	Allow	File Monitor	192.168.100.9			205.185.216.42	USA		dmz	outside	4473 / tcp	80 / http
2021-05-21 05:07:48	Allow	File Monitor	192.168.100.9			212.145.209.99	ESP		dmz	outside	3881 / tcp	80 / http
2021-05-21 05:04:03	Allow	File Monitor	192.168.100.9			205.185.216.10	USA		dmz	outside	3734 / tcp	80 / http
2021-05-21 05:04:03	Allow	File Monitor	192.168.100.9			205.185.216.42	USA		dmz	outside	3735 / tcp	80 / http
2021-05-21 05:02:01	Allow	File Monitor	192.168.100.9			212.145.41.66	ESP		dmz	outside	3605 / tcp	80 / http

13.16.2 FILTRO DE APLICACIONES - AVC

El AVC, Application Visibility and Control, permite especificar en las reglas filtros por detección de aplicaciones.

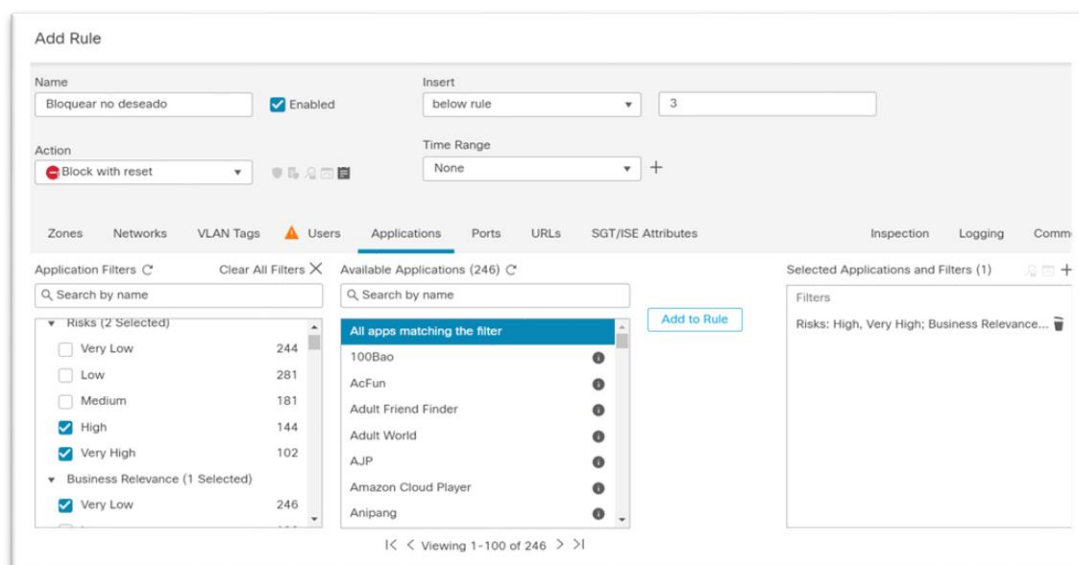


Nota: cuando se usa un filtro de aplicación, el cortafuegos dejará pasar un número de paquetes **en cualquier puerto** y según los parámetros asociados a la regla donde esté definida, en las redes o zonas especificadas. Esto es necesario porque la detección de aplicación necesita ver unos cuantos paquetes de comunicación para identificar correctamente la aplicación. Esto puede comprometer la seguridad. Se recomienda, por lo tanto, siempre especificar un filtro de aplicación, junto a un puerto o restricciones más específicas para que actúen como AND.

Podemos especificar, como en el ejemplo de arriba, filtro de aplicación por HTTP o HTTPS sin puerto, lo cual identificará el protocolo en cualquier puerto y lo permitirá.

Rules													
Filter by Device													
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applicat...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT
Mandatory - FTDvHA1 (1-3)													
1	SRV Web 1	servidores usuarios	outside	Any	Servidores_f	Any	Any	Any	Any	HTTP HTTPS	Any	Any	Any
2	SRV CIFS	usuarios	servidores	Any	Servidores_f	Any	Any	Any	Any	TCP (8):445	Any	Any	Any
3	Internet Web	servidores usuarios	outside	Any	Any	Any	Any	HTTP HTTPS	Any	Any	Any	Any	Any

También se puede bloquear por categorías de aplicaciones, en vez de individuales, especificando las categorías peligrosas o de poca relevancia de negocio.



Existen más de 3.500 aplicaciones reconocidas.

Si queremos identificar como los cortafuegos Firepower reconocen cierto tráfico en nuestra red, deberemos logearlo al FINAL de la conexión, donde el Firepower añadirá al paquete de syslog el nombre de la aplicación reconocida.

13.16.3 FILTRO POR URL - URL FILTERING

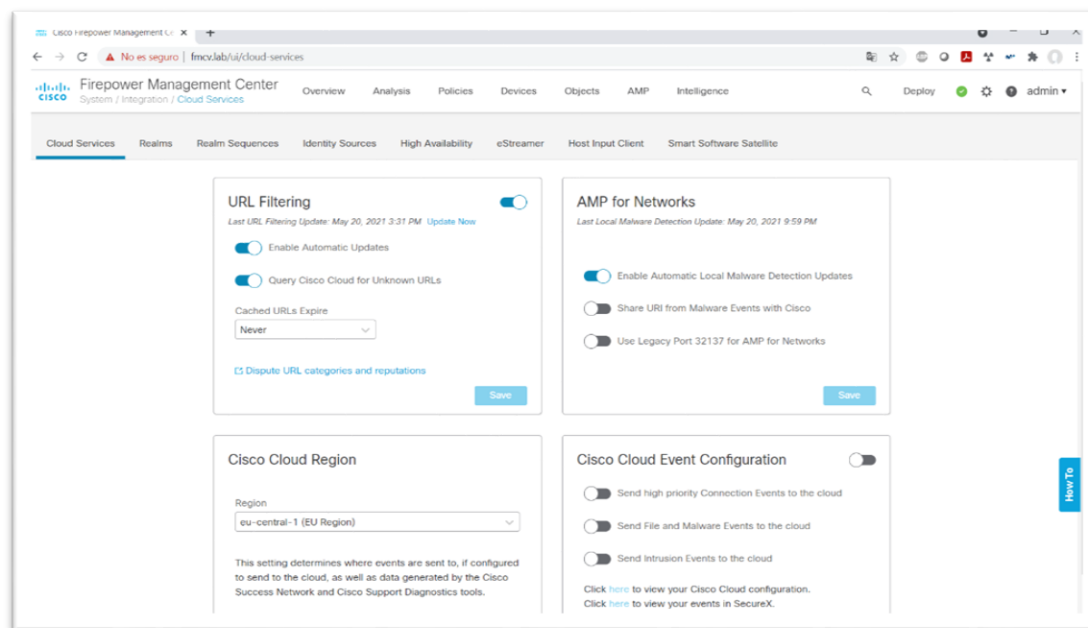
El filtro por URL es una eficaz protección contra el malware, bloqueando webs conocidas como maliciosas antes de que un usuario o cliente inadvertidamente, mediante engaño o redirección, acceda a ellas y se infecte.

Este servicio requiere licencia de suscripción URL-Filtering.

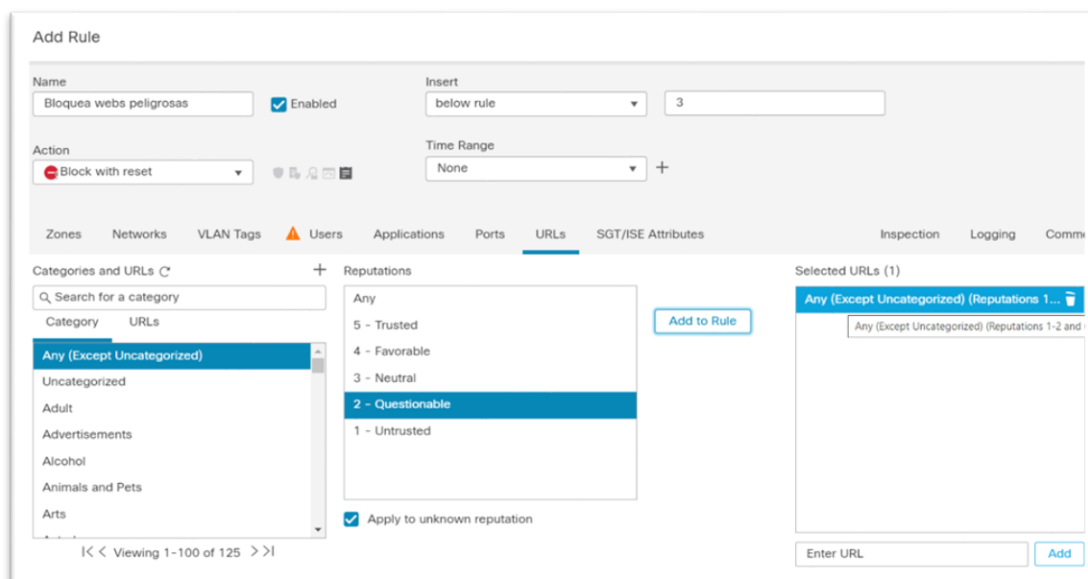
No se puede utilizar este servicio en una instalación sin conexión a Internet del FMC. El gestor necesita acceder a Internet cada 30 minutos para actualizaciones de categoría de URL.

La información proviene del servicio Cisco CSI (Collective Security Intelligence), y se realiza por conexión directa. No se puede actualizar manualmente.

La configuración de URL Filtering se puede consultar en System->Integration->Cisco CSI. Se autoconfigura en el momento de activación de una licencia URL-Filtering en un dispositivo FTD.



Si la licencia está activada y funcionando correctamente, podemos crear, por ejemplo, una regla que desde cualquier zona origen, a Internet, por los puertos HTTP(80) y HTTPS(443), bloquee las URLs en base a Reputación, bloqueando Sospechosas y de Alto Riesgo.



También se pueden especificar individualmente por Categorías.

Otra opción es bloquear URLs introducidas manualmente. Esto no requiere licencia, ya que no forma parte del sistema categorizado de URL-Filtering.

La categoría “Uncategorized” cubre cualquier URL que todavía no esté categorizado por el servicio de Cisco.

En entornos de alta seguridad, se deben especificar como permitidas las categorías estrictamente necesarias para la organización, denegando el resto y “uncategorized”.

13.16.4 FILTRO SECURITY INTELLIGENCE

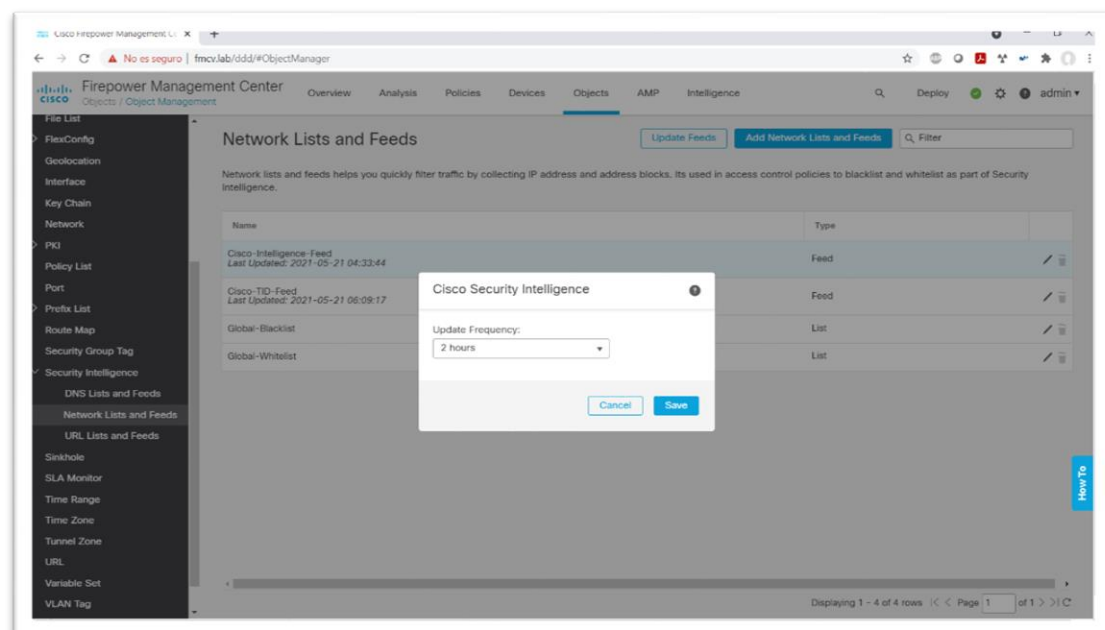
El filtro Security Intelligence es una de las mejores protecciones ofrecidas por Cisco. El centro de gestión e información de Cisco Talos provee de “feeds” a los cortafuegos y sistemas Cisco sobre direcciones IP y nombres DNS de atacantes y fuentes de actividades maliciosas.

Este servicio requiere licencia de suscripción “Threat”.

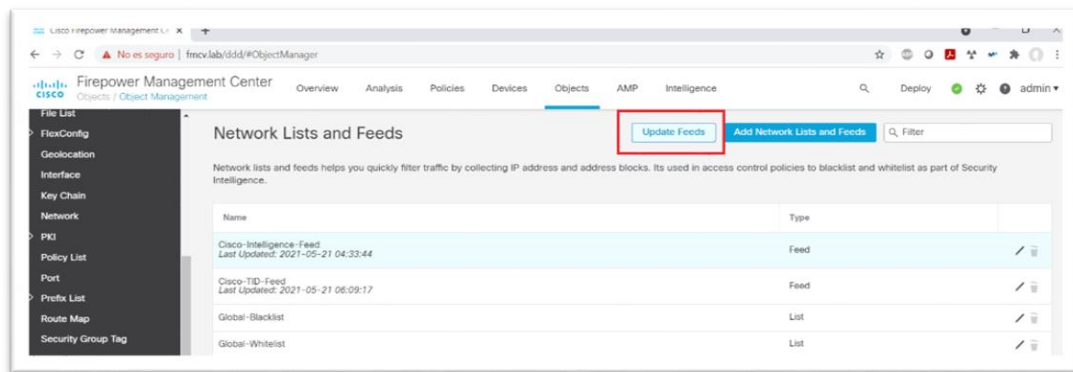
No se puede utilizar este servicio en una instalación sin conexión a Internet del FMC. El gestor necesita acceder a Internet periódicamente para las actualizaciones de los “feeds” desde Talos. No se puede actualizar manualmente.

La configuración de actualización se puede consultar en Objects->Object Management>Security Intelligence. Dentro de Network Lists and feeds y DNS Lists and Feeds se encuentran los objetos Cisco-Intelligence-Feed y Cisco-DNS-and-URL-Intelligence-Feed.

Los objetos se actualizan, de manera predeterminada, cada 2 horas.

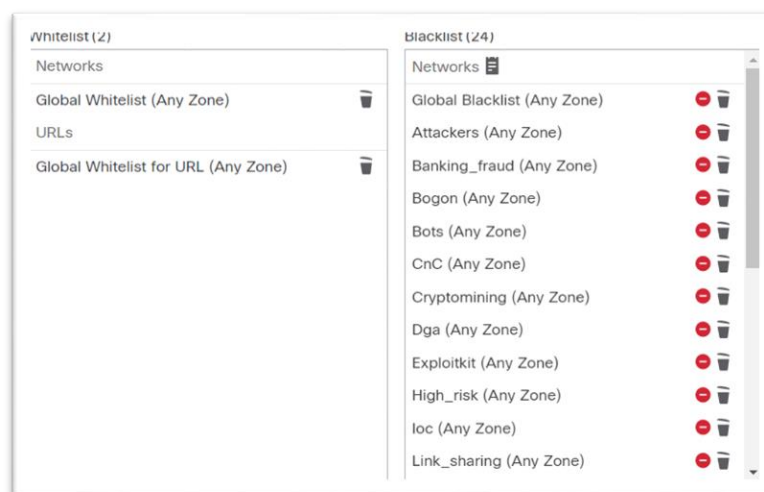
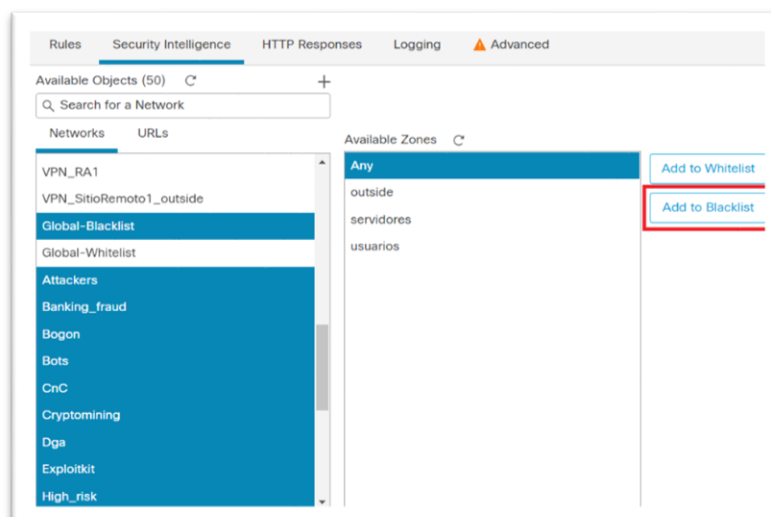


Pulsando sobre Update Feeds se puede forzar una actualización inmediata.

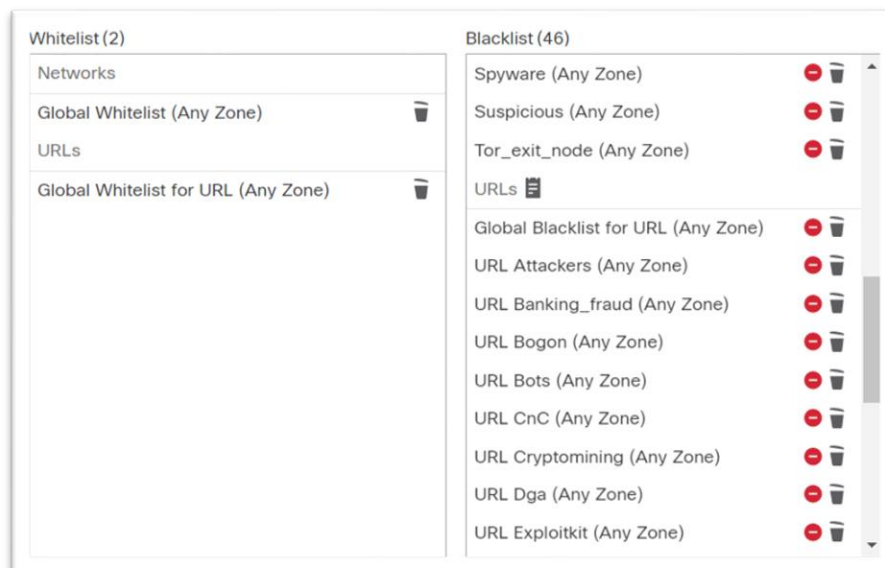
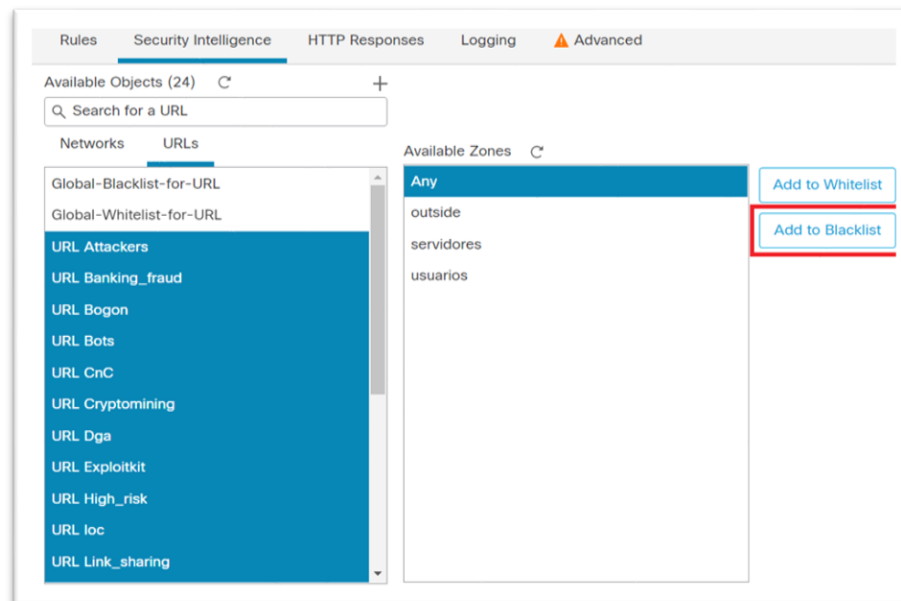


La configuración de Security Intelligence se debe realizar manualmente.

Sobre la política ACP en la que queremos añadir la característica, pulsamos en la pestaña “Security Intelligence”. En el desplegable seleccionamos Networks y añadimos a Blacklist todos los objetos de atacantes y maliciosos.



Seleccionamos luego URLs y realizamos la misma operación.



Por último, debemos crear una nueva política DNS para bloquear las consultas a sitios maliciosos, siempre que estas consultas atraviesen el cortafuegos.

Accediendo a Políticas->Access Control->DNS. Creamos una nueva política DNS "Add DNS Policy" y añadimos una regla que bloquee devolviendo "Domain not found" a todas las categorías DNS proveídas por Security Intelligence.

Add Rule

Name: ☒ Enabled

Action:

Zones Networks VLAN Tags **DNS**

DNS Lists and Feeds

Selected Items (23)

- DNS Attackers
- DNS Banking_fraud
- DNS Bogon
- DNS Bots
- DNS CnC
- DNS Cryptomining
- DNS Dga

DNS Lists and Feeds

- DNS Spam
- DNS Spyware
- DNS Suspicious
- DNS Tor_exit_node
- Global-Blacklist-for-DNS**
- Global-Whitelist-for-DNS

SI_DNS_Policy

Enter Description

Rules

[+ Add DNS Rule](#)

#	Name	Source Zones	Source Networks	VLAN Tags	DNS Lists	Action
Whitelist						
1	Global Whitelist for DNS	any	any	any	Global-Whitelist-for-DNS	Whitelist
Blacklist						
2	Global Blacklist for DNS	any	any	any	Global-Blacklist-for-DNS	Domain Not Found
3	Security Intelligence	any	any	any	DNS Attackers DNS Banking_fraud DNS Bogon DNS Bots (19 more...)	Domain Not Found

Volviendo a la ACP, en Security Intelligence, se activa la política DNS creada.

Firepower Management Center

Overview Analysis **Policies** Devices Objects AMP Intelligence

FTDvHA1

Enter Description

Rules Security Intelligence HTTP Responses Logging Advanced

Available Objects (50)

Available Zones

DNS Policy

- Default DNS Policy
- SI_DNS_Policy**
- Default DNS Policy

Global Whitelist (Any Zone)

Global Whitelist for URL (Any Zone)

Blacklist (46)

- Attackers (Any Zone)
- Banking_fraud (Any Zone)
- Bogon (Any Zone)
- Bots (Any Zone)
- CnC (Any Zone)
- Cryptomining (Any Zone)
- Dga (Any Zone)
- Exploit (Any Zone)
- High_risk (Any Zone)
- loc (Any Zone)
- Link_sharing (Any Zone)
- Malicious (Any Zone)

[How To...](#)

Para visualizar los eventos de bloqueo de Security Intelligence y comprobar que funciona correctamente, se puede acceder a Analysis->Connections->Security Intelligence Events. Ejemplo de eventos bloqueados:

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Security Intelligence Category	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application
2021-05-21 08:55:40		Block	IP Block	78.142.35.7	BGR	192.168.100.8		Malware	outside	dmz	49041 / tcp	22 (ssh) / tcp			
2021-05-21 08:40:04		Block	IP Block	185.94.111.1	RUS	192.168.100.16		Suspicious	outside	dmz	53175 / udp	111 (sunrpc) / udp			
2021-05-21 08:31:01		Block	IP Block	178.165.72.177	UKR	192.168.100.8		Tor_exit_node	outside	dmz	36886 / tcp	80 (http) / tcp			
2021-05-21 08:30:58		Block	IP Block	192.168.100.16		209.99.40.222	ARE	Response	dmz	outside	36414 / tcp	25 (smtp) / tcp			
2021-05-21 08:30:51		Block	IP Block	185.220.102.248	DEU	192.168.100.8		Tor_exit_node	outside	dmz	17206 / tcp	80 (http) / tcp			
2021-05-21 08:30:41		Block	IP Block	198.144.121.93	BLZ	192.168.100.8		Tor_exit_node	outside	dmz	38047 / tcp	80 (http) / tcp			
2021-05-21 08:28:03		Block	IP Block	199.249.230.110	USA	192.168.100.8		Tor_exit_node	outside	dmz	43120 / tcp	80 (http) / tcp			
2021-05-21 08:27:49		Block	IP Block	74.82.47.194	USA	192.168.100.8		Tor_exit_node	outside	dmz	27915 / tcp	80 (http) / tcp			
2021-05-21 08:27:38		Block	IP Block	185.94.111.1	RUS	192.168.100.8		Suspicious	outside	dmz	34869 / udp	111 (sunrpc) / udp			
2021-05-21 08:27:33		Block	IP Block	45.153.160.134	NLD	192.168.100.8		Tor_exit_node	outside	dmz	44468 / tcp	80 (http) / tcp			
2021-05-21 08:27:23		Block	IP Block	213.164.206.124	SWE	192.168.100.8		Tor_exit_node	outside	dmz	39796 / tcp	80 (http) / tcp			
2021-05-21 08:27:13		Block	IP Block	94.16.121.91	DEU	192.168.100.8		Tor_exit_node	outside	dmz	45895 / tcp	80 (http) / tcp			
2021-05-21 08:27:02		Block	IP Block	162.247.74.27	USA	192.168.100.8		Tor_exit_node	outside	dmz	36766 / tcp	80 (http) / tcp			
2021-05-21 08:26:55		Block	IP Block	185.100.87.241	ROU	192.168.100.8		Tor_exit_node	outside	dmz	34990 / tcp	80 (http) / tcp			

13.17 DESCUBRIMIENTO EN RED – NETWORK DISCOVERY

Una de las funciones más importantes de los equipos Firepower y el gestor FMC es el análisis de los equipos que conectan, o intentan conectar, a través de ellos.

A través de la política de descubrimiento los equipos alimentan una base de datos en el FMC de Hosts indicando su sistema operativo, aplicaciones que corren sobre ellos e incluso usuarios detectados.

Se necesita configurar correctamente la política de descubrimiento.

Accediendo al FMC y en el menú Policies->Network Discovery veremos la política de descubrimiento actual.

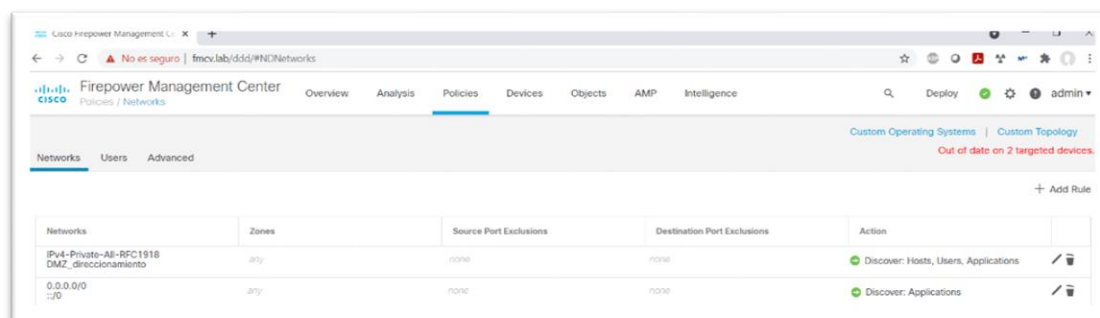
Networks	Zones	Source Port Exclusions	Destination Port Exclusions	Action
0.0.0.0/0 ::/0	any	none	none	Discover: Applications

La política por defecto inspecciona todas las redes descubriendo aplicaciones.

Se recomienda añadir una nueva regla que incluya las redes que gestionemos y que descubra Hosts y Applications, y si es posible, Users.

Se puede añadir genéricamente el objeto “IPv4-Private-All-RFC1918” que comprende todo el direccionamiento privado, así como algún direccionamiento público que pudiera haber en DMZ. Esto es válido si no hay interconexión con otras redes y gestionamos todos los direccionamientos privados.

Ejemplo:



La función de descubrimiento de red utiliza la información de la base de datos de vulnerabilidades (VDB). Se debe actualizar la base de datos “Vulnerability Database” de manera frecuente. Consultar el punto de esta guía sobre ese punto.

13.18 POLÍTICA DE INTRUSIÓN – INTRUSION POLICY (NGIPS)

El IPS de Nueva Generación de Cisco es el sistema de protección principal de la solución Firepower de Cisco.

Con la compra de SourceFire, Cisco se ha proveído de la mayor base de instalaciones IDS/IPS del mundo, basadas en Snort, esto hace que sus firmas sean las más completas del mercado en la actualidad. Las firmas son proveídas por Cisco Talos y se deben tener actualizadas.

Este servicio requiere licencia de suscripción Threat.

Aunque se puede usar esta funcionalidad sin acceso a Internet por parte del FMC, no se recomienda. Las actualizaciones de firmas de IPS son muy frecuentes y la instalación manual está desaconsejada.

Consultar en esta guía la gestión y actualización de “Rule Updates”.

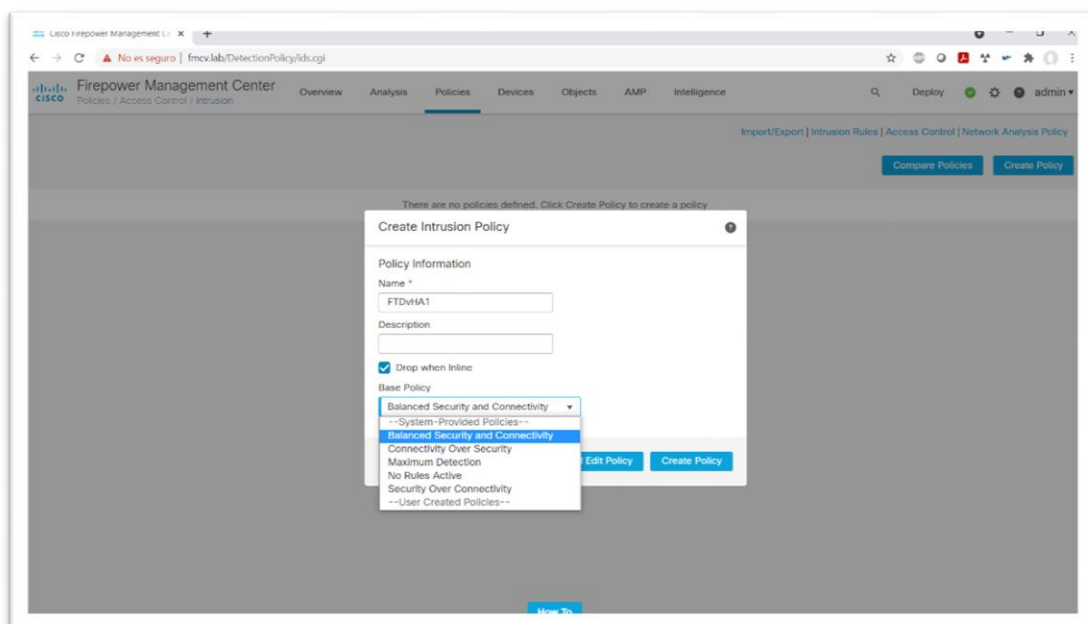
Una comparativa actualizada sobre la prevalencia de las fuentes de Cisco en seguridad.

	Cisco	Palo Alto Networks	Fortinet	Check Point Software Technologies
Threat Intelligence (Talos)				
Unique malware samples per day	1.5 million	10s of thousands	10s of thousands	10s of thousands
Threats blocked per day	19.7 billion Excludes email	Not reported	Not reported	Not reported
Email messages scanned per day	600 billion Of the 600B scanned, more than 85% are spam.	Not reported	6 million	Not reported
Web requests monitored per day	16 billion Web requests monitored by WSA/CWS per day. For perspective, Google processes 3.5 billion searches per day.	Not reported	35 million	Not reported
Automated intelligence feeds	✓ Security intelligence feeds are updated every 2 hours, adjustable to 5-minute intervals.	✓	✓	✓

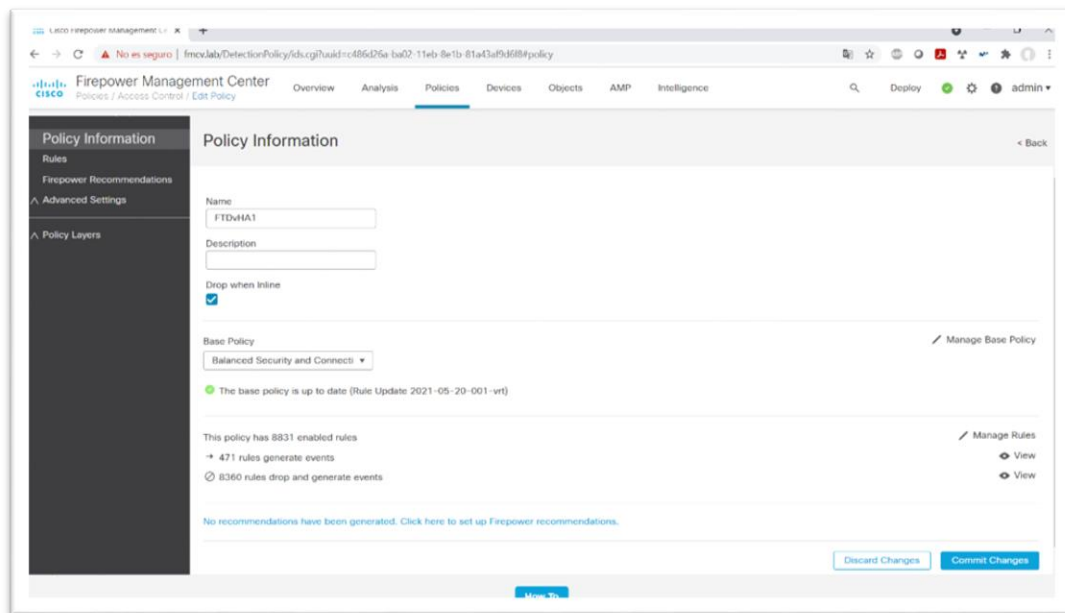
Para la configuración del sistema IPS se debe crear una política de Intrusión. Menú Policies->Access Control->Intrusion. Pulsando en “Create Policy”.

Cuando se crea la política, hay que seleccionar el conjunto de reglas a activar por defecto, política base. El valor por defecto es “Balanced Security and Connectivity”, que es una política con análisis intermedio que funciona bien en la mayoría de los casos. Otra política bastante usada, más restrictiva y con uso de más reglas y recursos es “Security over Connectivity”.

Creamos y editamos la política.



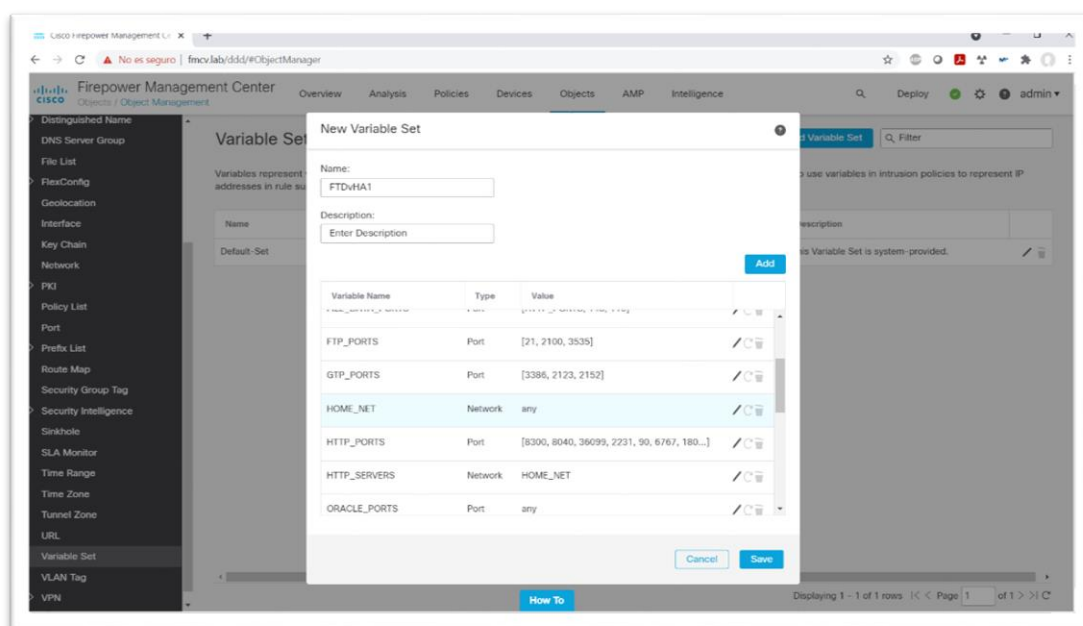
Comprobamos las reglas que tiene activadas en el modo seleccionado.



Aplicamos los cambios (solo la creación).

Necesitamos indicarle al IPS cuáles son las direcciones IP de nuestra red, las cuales nos interesa proteger. Para ello debemos crear un objeto "Variable Set".

En menú Objects->Object Management->Variable Set, encontramos el set por defecto. Se añade uno nuevo para personalizarlo al entorno.



Editamos el objeto HOME_NET y debemos incluir en ese objeto todas nuestras redes, pero solo nuestras redes, excluyendo Internet y otras que no están en nuestro control, con especial atención a VPN Site to Site.

En este ejemplo vamos a incluir todo el direccionamiento privado y un direccionamiento público de DMZ.

Con EXTERNAL_NET podemos usar una lógica negativa, vamos a considerar que es “any” menos HOME_NET.

Cualquier información que podamos añadir sobre nuestra red en esas variables, ayudará al IPS a realizar su trabajo.

Verificamos los valores y grabamos.

New Variable Set

Name:

Description:

You have unsaved changes **Add**

Variable Name	Type	Value
Customized Variables		
EXTERNAL_NET	Network	!HOME_NET
HOME_NET	Network	[IPv4-Private-All-RFC1918, DMZ_direccio...]
Default Variables		
DNS_SERVERS	Network	HOME_NET
FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]
FTP_PORTS	Port	[21, 2100, 3535]

Cancel **Save**

Una vez que tenemos la política creada y la variable personalizada, tenemos que activar el IPS. Esto se hace dentro de la ACP. En cada regla, se puede especificar una política de Inspección o no. Se debe configurar la política creada y el Variable Set.

Se recomienda aplicarla en todas las reglas posibles.

Editing Rule - SRV Web 1

Name: ☒ Enabled **Move**

Action: **Time Range**: **+**

Zones **Networks** **VLAN Tags** **Users** **Applications** **Ports** **URLs** **SGT/ISE Attributes** **Inspection** **Logging** **Comments**

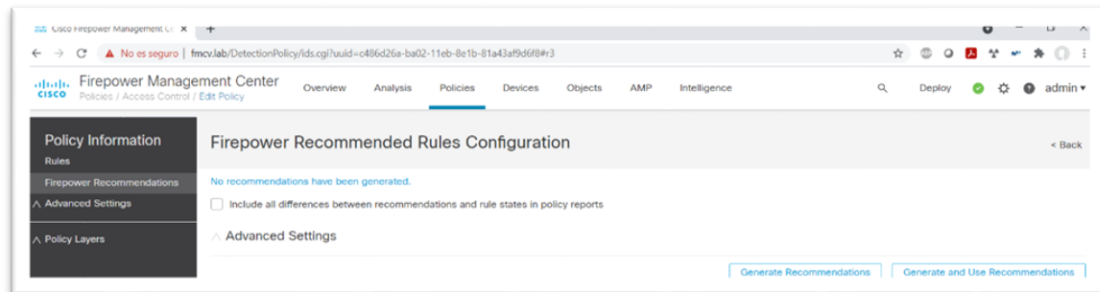
Intrusion Policy: **Variable Set**:

File Policy:

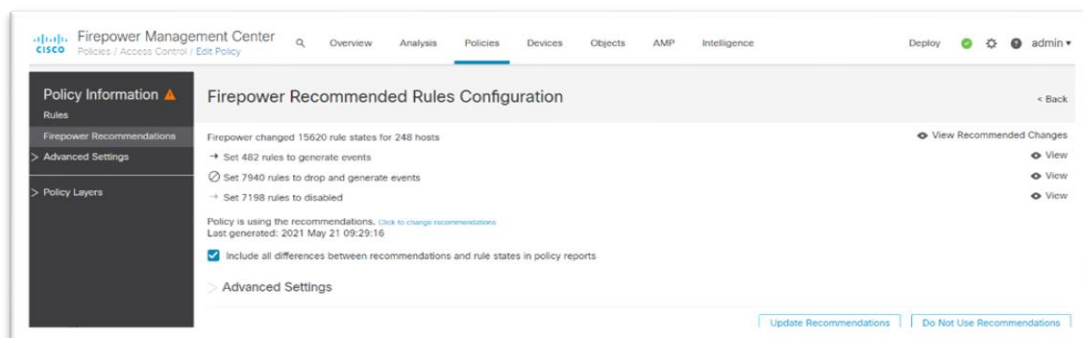
Cancel **Save**

Una vez aplicada a las reglas ACP y realizado el Deploy, el IPS empezará a detectar tráfico anómalo, ataques y amenazas.

Se recomienda dejar pasar unas horas antes de hacer un “Auto-Tuning” del IPS para que el sistema Firepower descubra el funcionamiento de la red, tras un tiempo acceder a la política de intrusión aplicada y pulsar sobre “Generate Recommendations”.



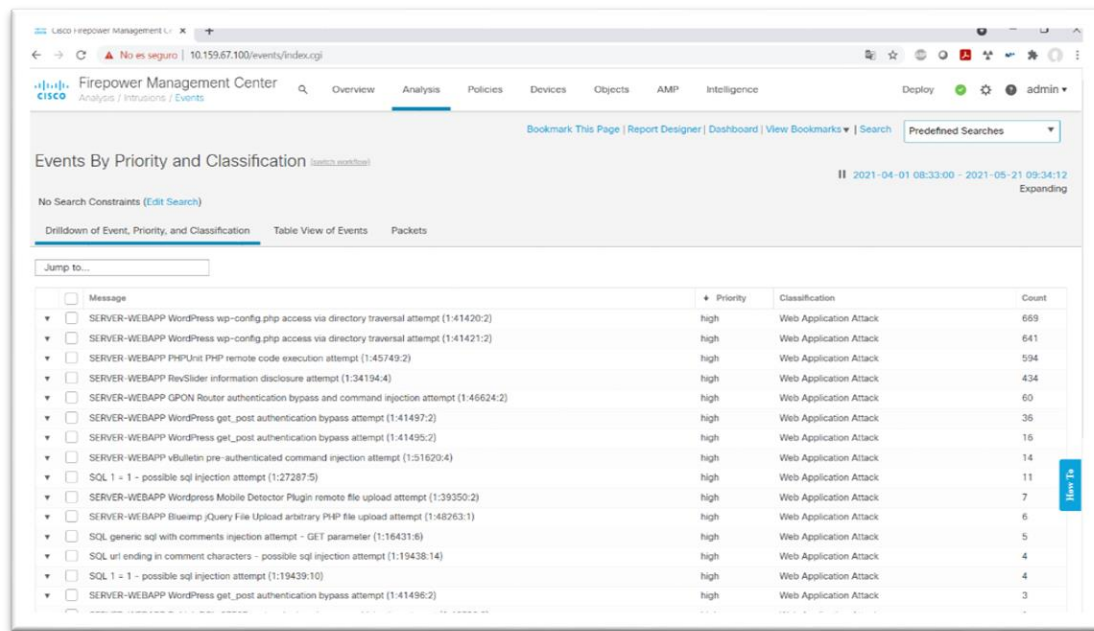
El sistema generará unas recomendaciones de “auto-tuning” sugiriendo deshabilitar y habilitar reglas dependiendo de la información obtenida de la red. Es decir, propone la deshabilitación de reglas para servicios que no se encuentran en la red y/o habilitación de reglas para servicios encontrados y no activadas.



Se recomienda usar el auto-tuning (las recomendaciones). Y realizar Update Recommendations de manera periódica y reaplicar los cambios.

El funcionamiento del IPS filtrará (drop) paquetes de atacantes usando los patrones de ataque reconocidos en las firmas, protegiendo los equipos de red.

Sin embargo, conviene revisar diariamente el log de eventos de intrusiones. Analysis->Intrusions->Events.



En el Dashboard, el Widget de eventos de Intrusión da una imagen visual rápida de la situación de la red, desde el punto de vista del detector de intrusiones (IPS).



El significado de los niveles de impacto de la izquierda, es la siguiente:

- 0 – host not on monitored networks
- 4 – no entry for the host in the network map
- 3 – host not running the service or protocol that was attacked
- 2 – host is running the service or protocol that was attacked
- 1 – host is running the service or protocol that was attacked and a vulnerability is against the service or protocol is mapped to the host

Como puede verse, los niveles donde hay que centrarse en manejar son los peligros de los niveles 1 y 2.

El FMC genera información de vulnerabilidades e indicadores de compromiso, los cuales se pueden analizar en diversos menús.

El Host Profile es un detalle de un equipo en concreto. Con sus IOC, servicios de servidor corriendo, sistema operativo detectado.

OSI FIVE

[Select Host](#)
[Configure View List Filter](#)

IP Addresses	192.168.1.1
NetBIOS Name	
Device (Hops)	Ip01 (0)
AC Addresses (TTL)	00:50:56:AB:66:51 (vMware, Inc.) (128)
Host Type	Host
Last Seen	2021-05-21 09:08:17
Current User	Discovered Identities\Administrator (LDAP)
View	Context Explorer Connection Events Intrusion Events File Events Malware Events

Indications of Compromise (6)

[Edit Rule States](#)
[Mark All Resolved](#)

Category	Event Type	Description	First Seen	Last Seen	
CnC Connected	Security Intelligence Event - CnC	The host may be under remote control	🔍 2020-09-24 13:00:30	🕒 2021-05-20 12:59:41	⌵
Malware Download	Security Intelligence Event - URL, Malware	The host may connect to a malware URL	🔍 2019-11-11 08:37:43	🕒 2021-04-29 11:44:31	⌵
Phishing Target	Security Intelligence Event - URL, Phishing	The host may connect to a phishing URL	🔍 2020-02-06 10:42:13	🕒 2021-03-11 13:05:55	⌵
CnC Connected	Security Intelligence Event - URL, CnC	The host may be under remote control	🔍 2020-02-06 13:21:39	🕒 2021-02-11 11:49:11	⌵
Malware Detected	Threat Detected in File Transfer	The host has encountered malware	🔍 2020-02-28 13:56:53	🕒 2020-03-11 16:38:19	⌵
Malware Download	Security Intelligence Event - DNS, Malware	The host may connect to a malware host	🔍 2020-02-03 12:40:41	🕒 2020-02-03 12:40:41	⌵

Operating System
[Edit Operating System](#)

Vendor	Product	Version	Source
Microsoft	Windows	2000, XP, Server 2003	Firepower

Invers (3)

Protocol	Port	Application Protocol	Vendor and Version	
csp	443	pending		⌵ 🔍 ⌶ ⌷
icmp	0	ICMP		⌵ 🔍 ⌶ ⌷
http	80	HTTP	Apache 2.4.29 (Ubuntu)	⌵ 🔍 ⌶ ⌷

Applications (157)

Especialmente el apartado de Vulnerabilidades indica que el Host está desactualizado y que conviene actualizarlo urgentemente.

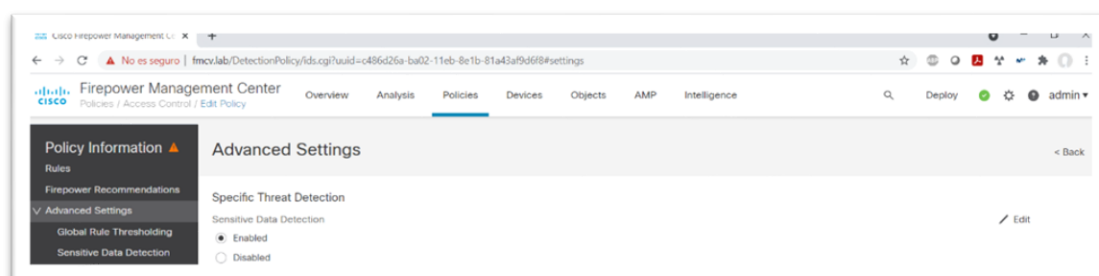
Vulnerabilities (915)		Edit Vulnerabilities	
Name	Remote	Component	Port
4D WebStar Symbolic Link Vulnerability		Windows 2000, XP, Server 2003	
A certain ActiveX control in the Indexing Service in Microsoft Windows 2000 SP4, XP SP2 and SP3, and Server 2003 SP2 does not properly process URLs, which allows remote attackers to execute arbitrary programs via unspecified vectors that cause a "vulnerab		Windows 2000, XP, Server 2003	
Active Directory Federation Services (ADFS) in Microsoft Windows Server 2003 SP2 and Server 2008 Gold and SP2 does not properly validate headers in HTTP requests, which allows remote authenticated users to execute arbitrary code via a crafted request to a		Windows 2000, XP, Server 2003	
Adobe Flash Player Multiple Remote Code Execution Vulnerabilities	Yes	Windows 2000, XP, Server 2003	
Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary		Windows 2000, XP, Server 2003	
Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary		Windows 2000, XP, Server 2003	
Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary		Windows 2000, XP, Server 2003	
Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to execute arbitrary		Windows 2000, XP, Server 2003	
Adobe Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to obtain sensitive		Windows 2000, XP, Server 2003	
Apple Safari and Microsoft Windows Client-side Code Execution Vulnerability	Yes	Windows 2000, XP, Server 2003	
ATMFD.DLL in the Adobe Type Manager Font Driver in Microsoft Windows Server 2003 SP2, Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8, Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT Gold and 8.1 allows remote attackers to obtain sensitive		Windows 2000, XP, Server 2003	
Buffer overflow in GDI+ in Microsoft Internet Explorer 6 SP1, Windows XP SP2 and SP3, Office XP SP3, Office 2003 SP3, 2007 Microsoft Office System SP1 and SP2, Office Project 2002 SP1, Visio 2002 SP2, Office Word Viewer, Word Viewer 2003 Gold and SP3, Off		Windows 2000, XP, Server 2003	

13.18.1 PREVENCIÓN DE PERDIDAS DE DATOS (DLP)

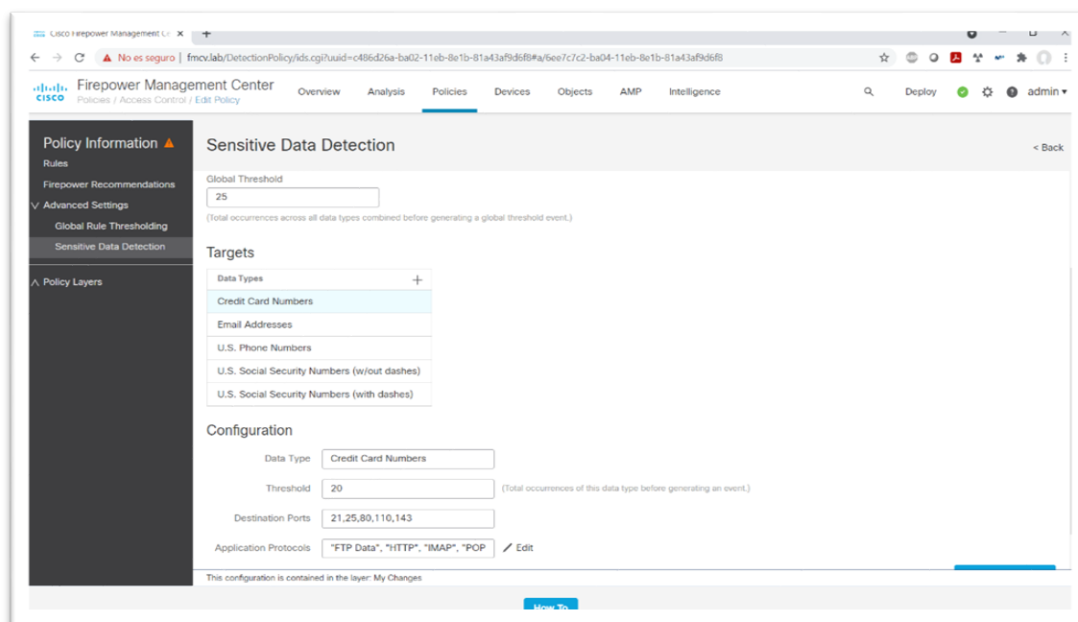
La prevención de pérdidas de datos (DLP – Data Loss Prevention), es un sistema diseñado para detectar potenciales brechas/transmisiones de datos y prevenirlos a través de monitorización, detección y bloqueo de información sensible mientras está en movimiento (tráfico de red).

El sistema NGIPS de Firepower dispone de una configuración específica para DLP, que debe ser activada.

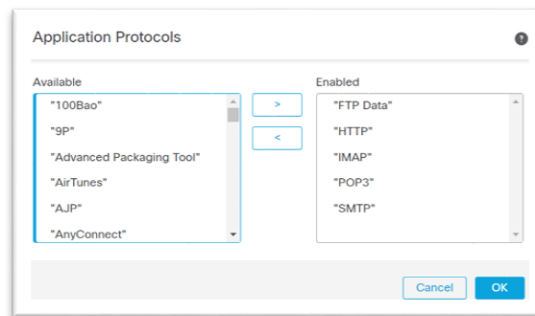
Editando la política de Intrusión, en Advanced Settings, encontramos Sensitive Data Detection.



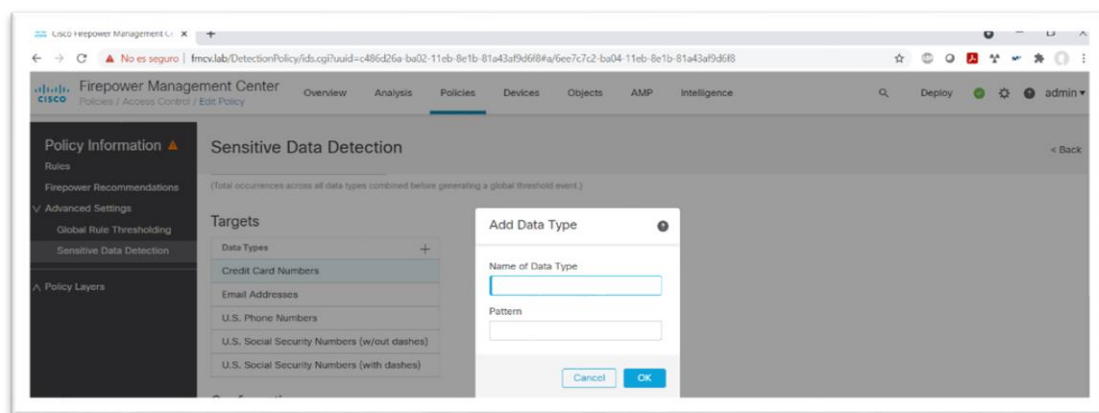
Editándolo nos lleva a la pantalla principal de configuración de DLP.



En esta pantalla podemos modificar el Threshold, que determina el número de ocurrencias del tipo de datos para hacer un “trigger” de la alerta o acción. También podemos añadir protocolos de monitorización, por tipo de dato.

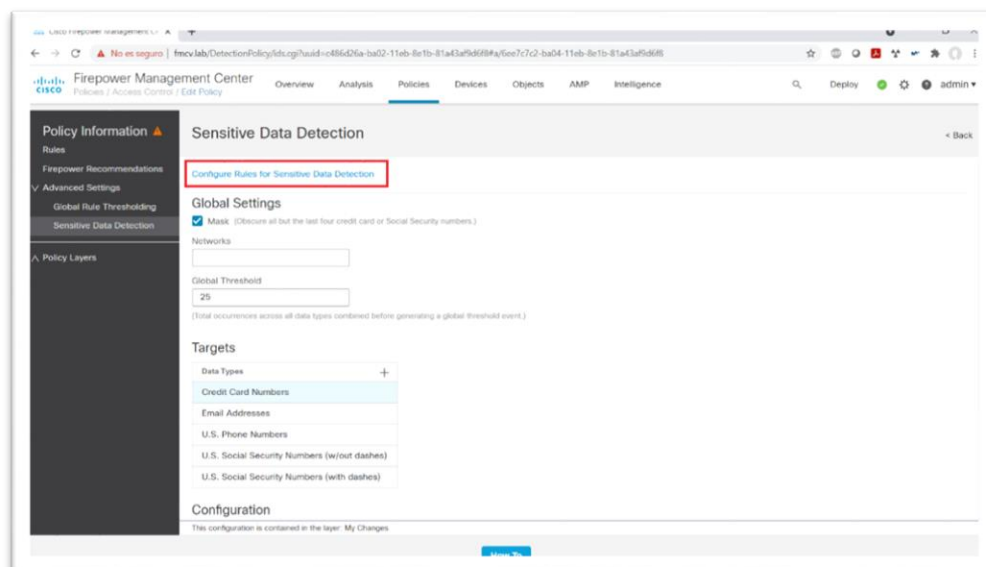


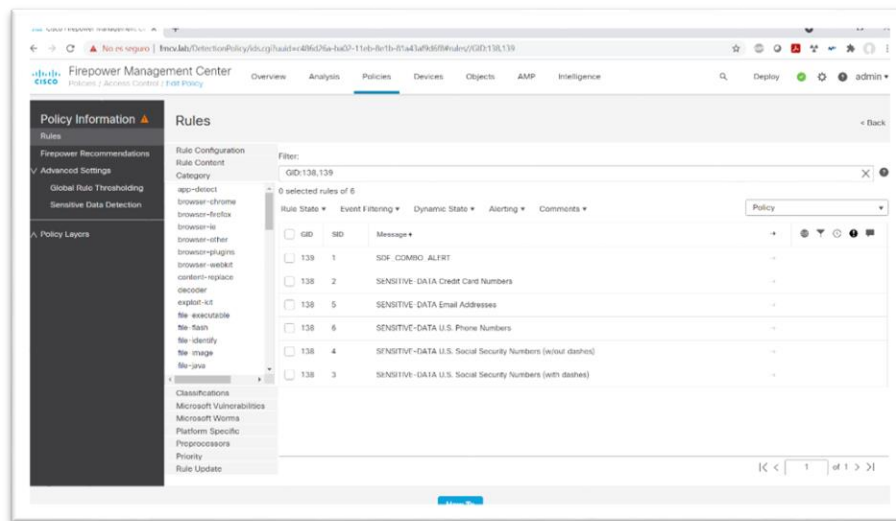
En los tipos de datos, podemos añadir específicos para nuestra organización.



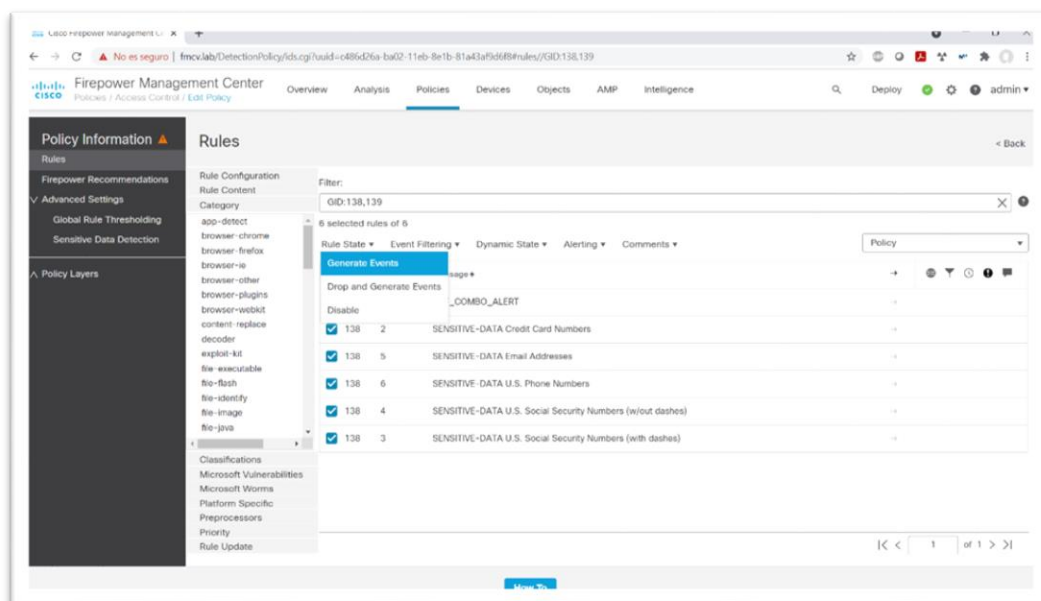
Aunque esta es la pantalla principal de configuración DLP, es necesario activar las firmas para que se generen alertas o se tomen acciones.

Pulsando sobre la parte superior lleva a la edición de reglas, seleccionando específicamente las de DLP.





Seleccionar todas y en “Rule State”, utilizar “Generate Events”.



Una vez activadas las reglas, pulsar en “Commit Changes” de la política y realizar Deploy, el sistema DLP quedará activado, generando alertas cuando se sobrepase el “threshold” e incluso ofuscando la información extraída.

13.19 DESCUBRIMIENTO DE IDENTIDADES (IDENTITY POLICY)

Los cortafuegos Firepower disponen de diversos métodos y funcionalidades para obtener la identidad de una conexión. Es decir, identificar que usuario (incluyendo su pertenencia a grupos) es el que realiza una conexión.

Algunos de los métodos usados por Firepower son:

- Descubrimiento pasivo, mediante Network Discovery.
- Portal cautivo, mediante la autenticación forzosa de usuarios previo a permitir conexiones.
- Integración con Cisco ISE (Identity Services Engine) e ISE-PIC (ISE-Passive Identity Connector).
- Cisco Terminal Services Agent, para integración con un Terminal Server de Windows o servidor Citrix.

Nota: El servicio ofrecido por User Agent para detección de identidad a través de Directorio Activo de Windows ha sido discontinuado en versión 6.7. El reemplazo de este servicio es ISE-PIC, o ISE (completo) si se quiere una funcionalidad mayor.

El descubrimiento de identidades permite crear reglas de control de acceso (ACP) especificando usuarios/grupos, es decir, políticas de acceso por selección de usuarios.

The screenshot displays the 'Add Rule' configuration interface. At the top, there are input fields for 'Name', an 'Enabled' checkbox, an 'Insert' dropdown menu (currently showing 'below rule'), and a numeric input field (showing '3'). Below these, the 'Action' is set to 'Allow' and the 'Time Range' is set to 'None'. A horizontal tab bar includes 'Zones', 'Networks', 'VLAN Tags', 'Users' (which is active and highlighted with a blue underline), 'Applications', 'Ports', 'URLs', 'SGT/ISE Attributes', 'Inspection', 'Logging', and 'Comm'. Under the 'Users' tab, there are two main sections: 'Available Realms' and 'Available Users', each containing a search bar with the placeholder text 'Search by name or value'. To the right of these is a 'Selected Users (0)' section containing the text 'any'. An 'Add to Rule' button is positioned between the 'Available Users' and 'Selected Users' sections.

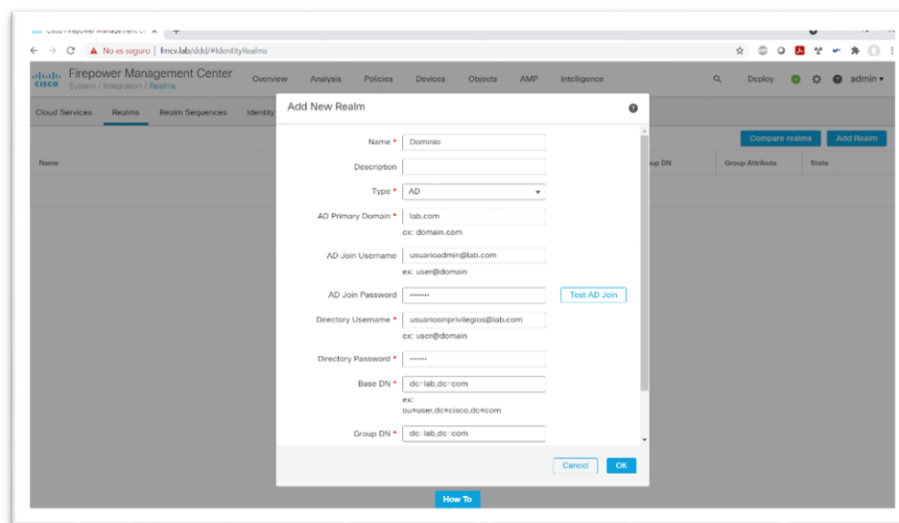
En esta guía vamos a tratar la integración con Directorio Activo de Windows para su uso con un ISE-PIC o ISE.

El ISE-PIC es un software (reducido de ISE), basado en Linux, que se instala como máquina virtual, soportado en los hipervisores ESXi, KVM, Hyper-V. Se puede instalar 1 instancia o 2 por redundancia. Este software se conecta a los controladores de dominio de Windows, y mediante WMI va obteniendo información sobre los inicios y cierres de sesión (login/logout) de los usuarios, obteniendo así su dirección IP asignada.

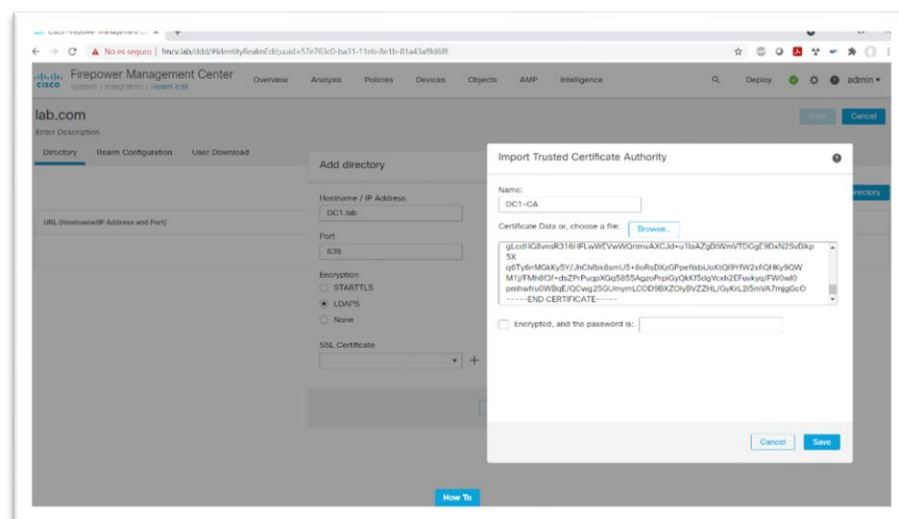
Para realizar una integración con ISE/ISE-PIC el primer requisito es crear un “Realm” en el FMC. El Realm es una conexión del FMC con un LDAP/Directorio Activo para obtención de información periódica sobre usuarios y grupos de manera genérica. Esta información se refresca cada 24 horas por defecto, aunque se puede bajar el tiempo de refresco a 1 hora.

Para la creación del Realm se accede al menú System->Integration->Realms. Seleccionar “New Realm”.

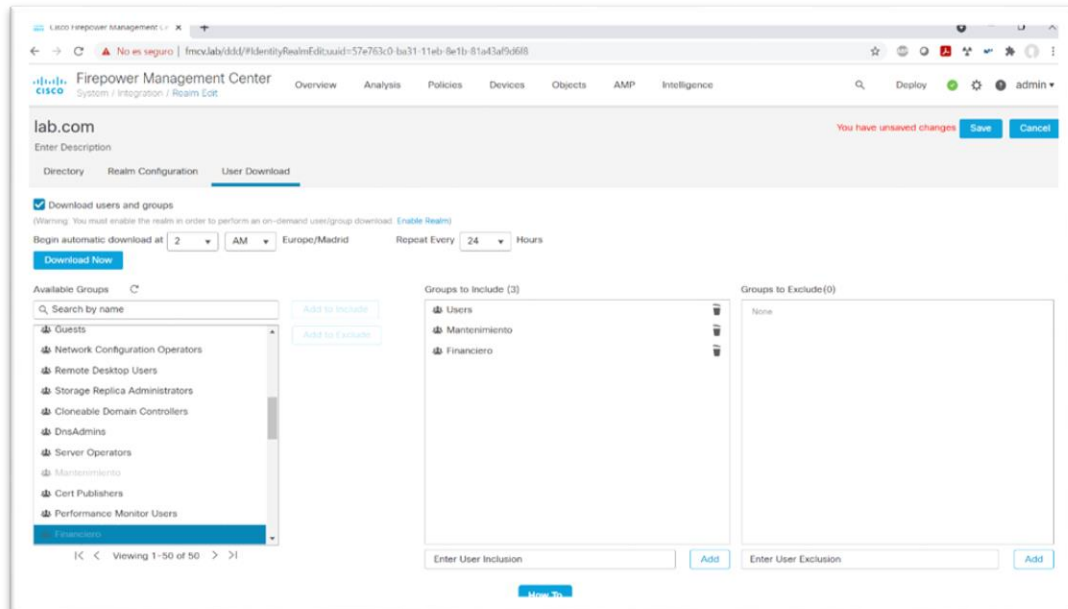
Se deben especificar los campos de nombre de dominio, usuario con privilegios para unir al dominio, usuario sin privilegios para consultas al directorio y el Base y Group DN (LDAP).



Una vez creado se deben especificar las conexiones LDAP a los controladores de dominio. Para ello se debe usar conexión con certificado, importando el certificado de la CA firmante.

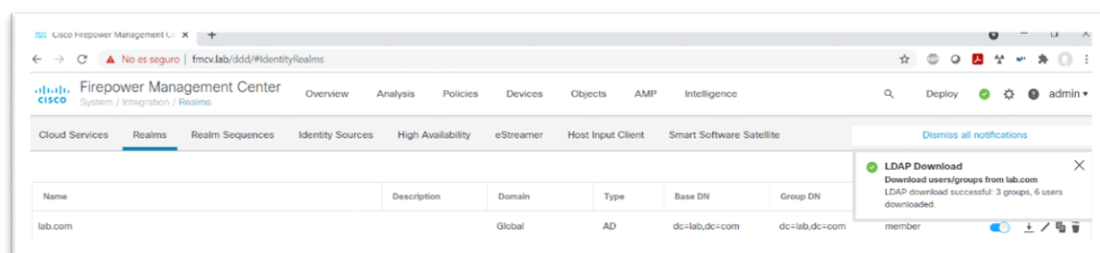


Por último, se debe activar la descarga de usuarios y grupos, especificar la periodicidad e incluir los objetos que se desean descargar.



Nota: cualquier grupo o usuario no incluido no se podrá utilizar en las reglas de control de acceso. Si se crea un grupo o usuario nuevo en Directorio Activo y se desea especificar una regla para ese grupo, debe editarse el Realm e incluirlo.

El último paso de la creación del Realm es salvarlo y habilitarlo (enable). Se puede utilizar también la opción de descarga manual inmediata “Download now” para lanzar la tarea en segundo plano.



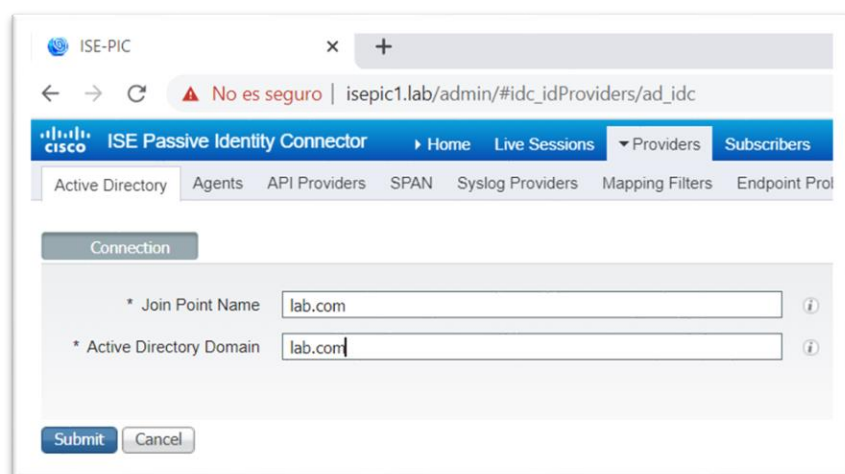
Mientras que tener configurado el Realm y la política de identidad, que citaré más tarde, permite definir reglas con usuarios/grupos ya conocidos por el sistema FMC, todavía no se está identificando/asociando las conexiones con los usuarios. Para eso se debe integrar con el software ISE/ISE-PIC.

En esta guía se va a cubrir, en parte, la integración con ISE-PIC.

El ISE-PIC se instala como máquina virtual, su instalable es una imagen ISO. Consultar la web de Cisco para ISE/ISE-PIC por sus requisitos exactos de instalación en entorno virtual.

La instalación de ISE-PIC desde la imagen ISO termina en un login en el que hay que poner “setup” para configurar los datos iniciales, como nombre de host y el direccionamiento IP.

En la configuración del ISE-PIC se debe añadir el directorio activo como proveedor, utilizando una cuenta con privilegios.



ISE-PIC

No es seguro | isepic1.lab/admin/#idc_idProviders/ad_idc

ISE Passive Identity Connector

Home Live Sessions Providers Subscribers

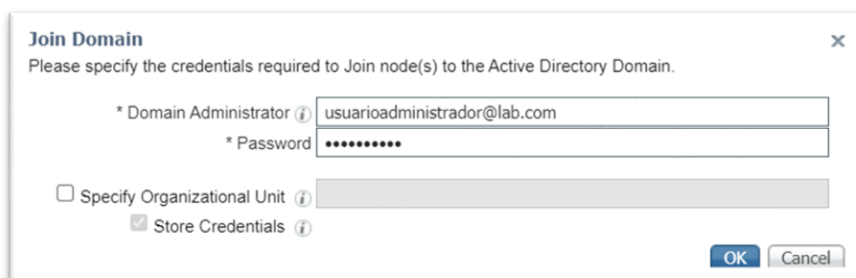
Active Directory Agents API Providers SPAN Syslog Providers Mapping Filters Endpoint Probes

Connection

* Join Point Name lab.com

* Active Directory Domain lab.com

Submit Cancel



Join Domain

Please specify the credentials required to Join node(s) to the Active Directory Domain.

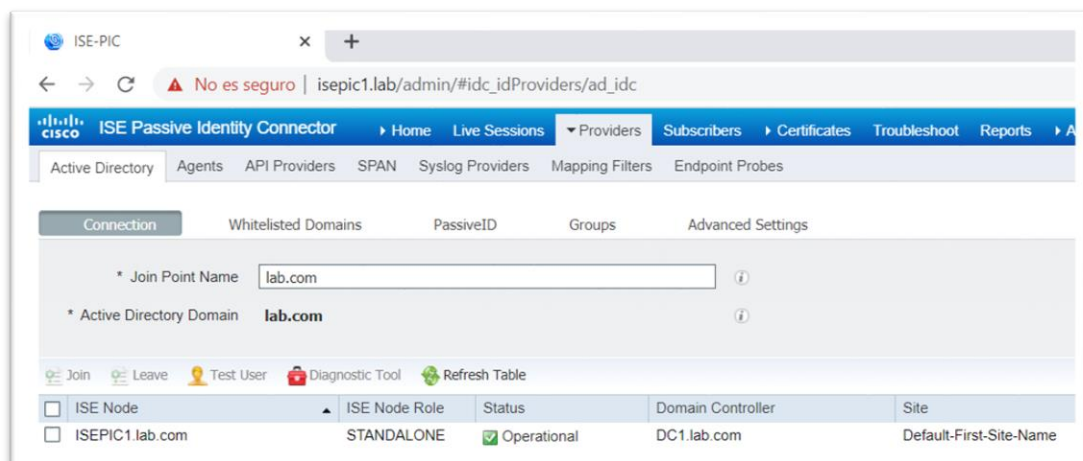
* Domain Administrator usuarioadministrador@lab.com

* Password

☐ Specify Organizational Unit

☒ Store Credentials

OK Cancel



ISE-PIC

No es seguro | isepic1.lab/admin/#idc_idProviders/ad_idc

ISE Passive Identity Connector

Home Live Sessions Providers Subscribers Certificates Troubleshoot Reports

Active Directory Agents API Providers SPAN Syslog Providers Mapping Filters Endpoint Probes

Connection Whitelisted Domains PassiveID Groups Advanced Settings

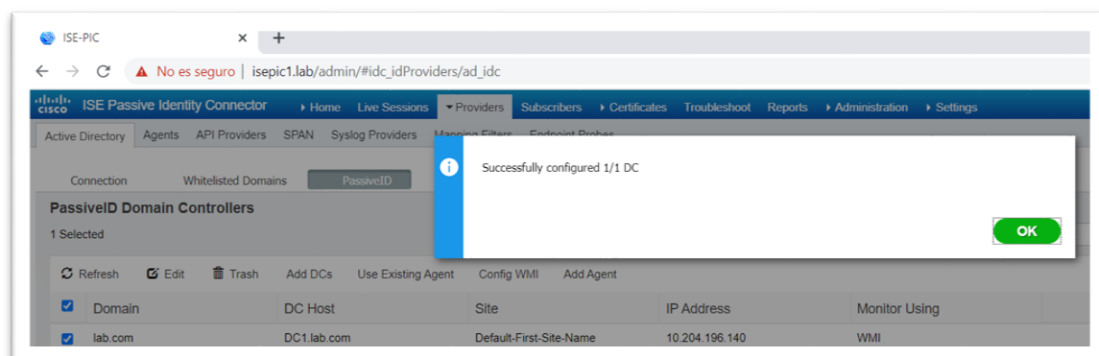
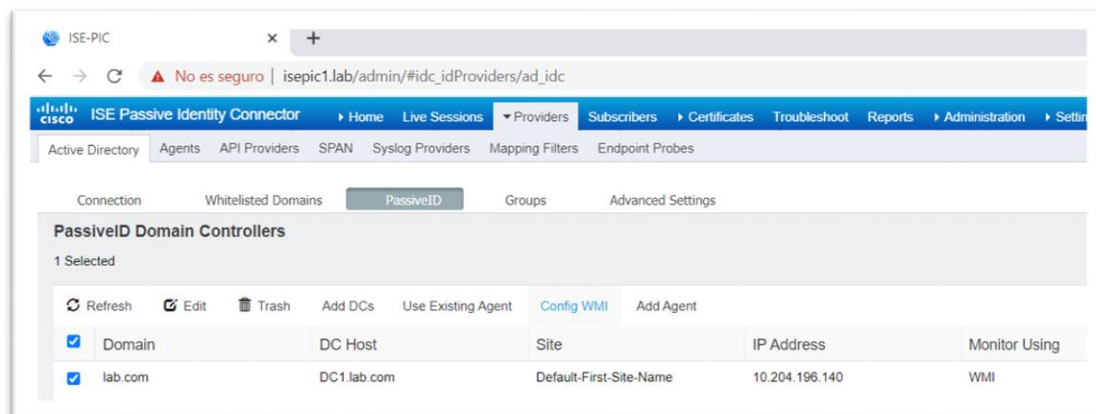
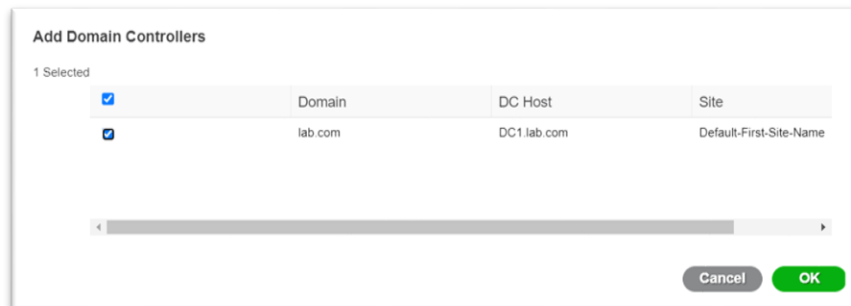
* Join Point Name lab.com

* Active Directory Domain lab.com

Join Leave Test User Diagnostic Tool Refresh Table

ISE Node	ISE Node Role	Status	Domain Controller	Site
☐ ISEPIC1.lab.com	STANDALONE	Operational	DC1.lab.com	Default-First-Site-Name

Ahora hay que activar la identificación pasiva usando la pestaña “PassiveID”, añadiendo los controladores de dominio, para luego realizar la configuración del WMI. Esta parte se realiza fácilmente con la opción de menú, que realizará los cambios automáticamente en el dominio.

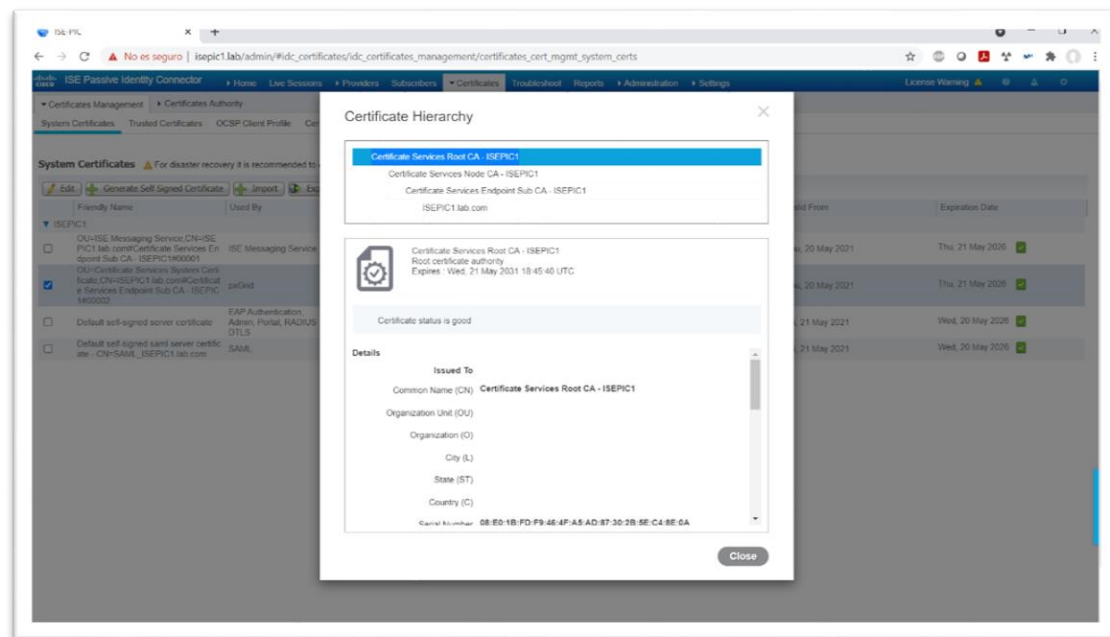


La comunicación entre el FMC y el ISE/ISE-PIE se realiza mediante protocolo pxGrid. Este protocolo requiere el uso de certificados.

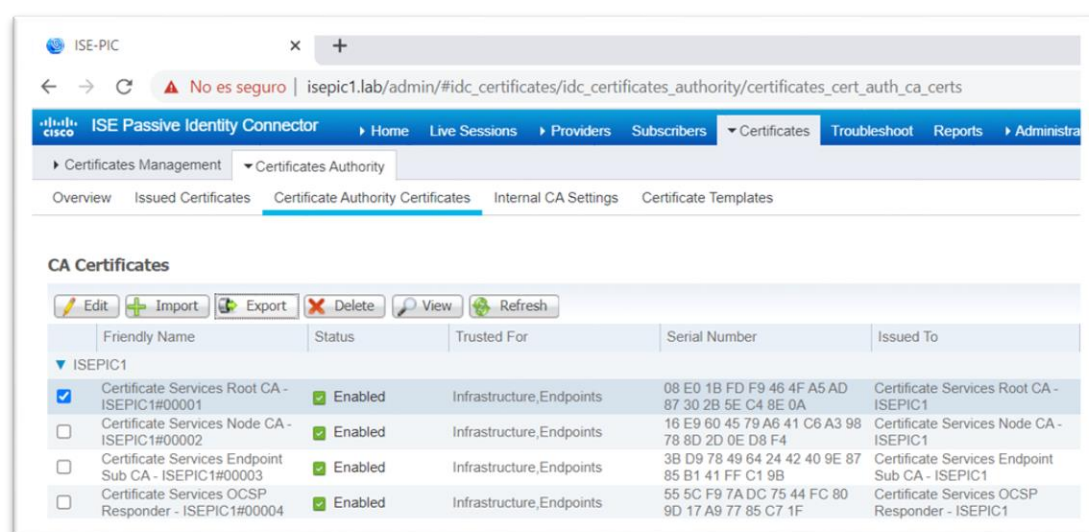
Nota: Se recomienda el uso de una CA fuera de línea (offline) para la emisión de los certificados digitales necesarios dentro de la organización.

En este ejemplo se van a usar certificados firmados por CAs internas de cada dispositivo, ISE-PIC y FMC.

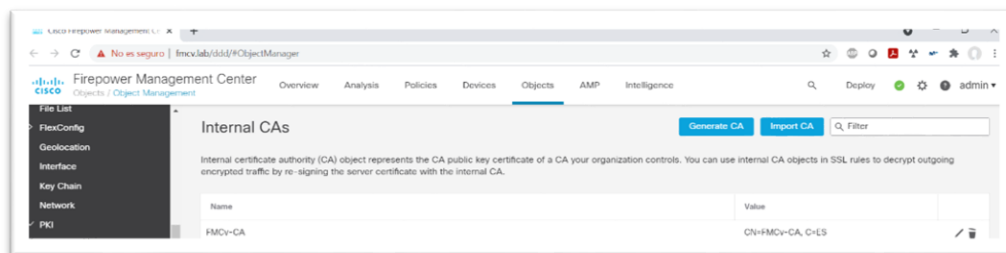
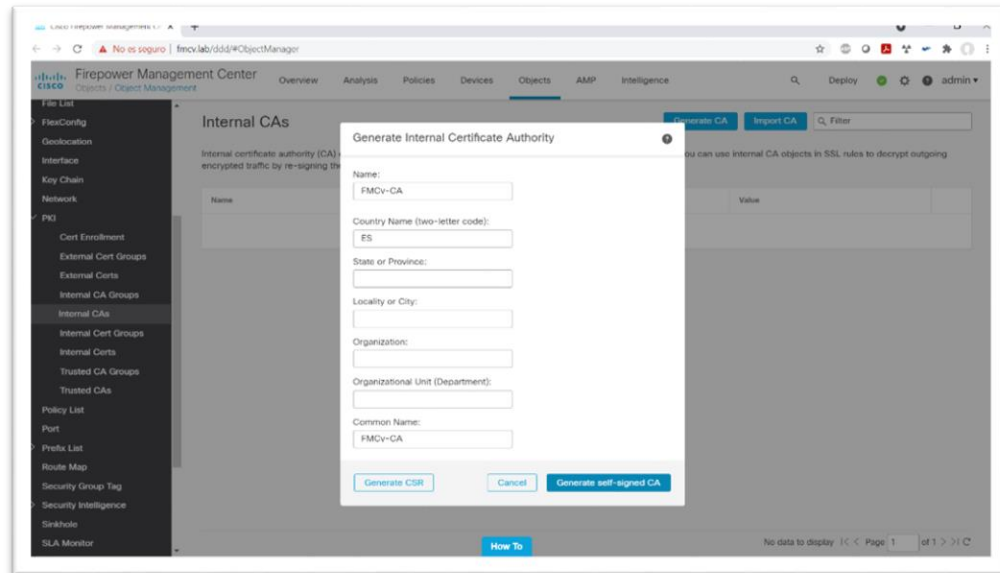
El certificado para uso de pxGrid en el ISE-PIC se encuentra correctamente instalado desde la instalación de las versiones más recientes del software. Es necesario localizar y descargar el certificado raíz.



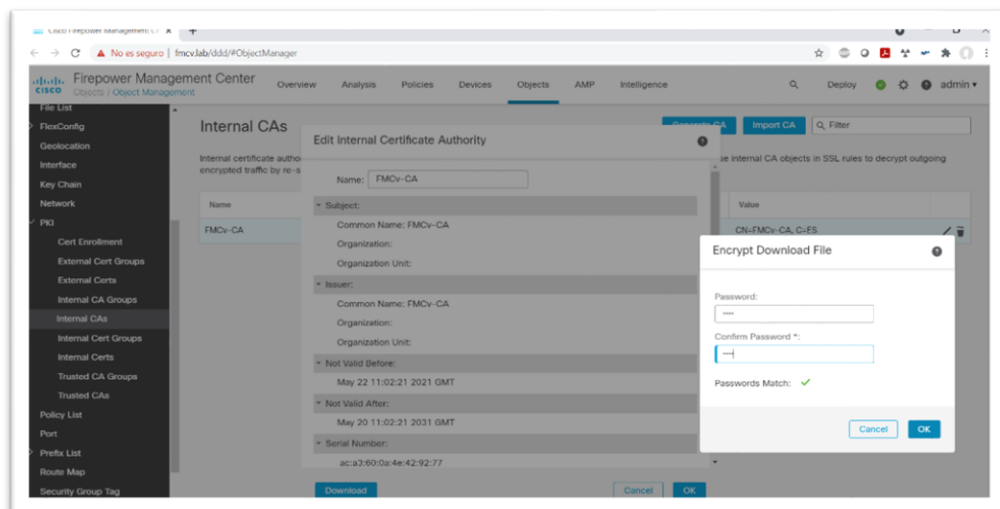
Una vez localizado, hay que proceder a su exportación, para su instalación posterior en el FMC.



En el FMC se va a crear un certificado firmado con una CA interna del propio FMC, utilizando la misma clave privada por simplicidad.



Se procede a la descarga del certificado con su clave privada, ya que vamos a necesitarlo para generar el certificado que el equipo FMC usará para autenticarse con el ISE-PIC.



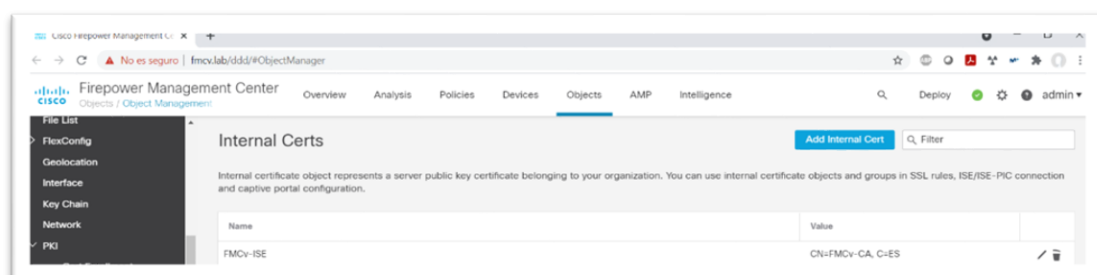
La mejor forma de tratar el fichero PKCS12 generado, es usar OpenSSL, que se encuentra instalado en casi cualquier sistema Linux. Ejecutar estos comandos, ajustando el nombre del fichero al generado en la exportación:

```
openssl pkcs12 -nokeys -clcerts -in 164a9a24-baed-11eb-81d6-a8c6d111f1dd.p12 -out cert.pem
```

```
openssl pkcs12 -nocerts -in 164a9a24-baed-11eb-81d6-a8c6d111f1dd.p12 -out key.pem
```

De esta manera se encontrarán separados el certificado de la CA interna (cert.pem) y su clave privada (key.pem).

Ahora se procede a añadir un certificado interno (Internal Cert), utilizando el mismo certificado y clave privada.



El certificado de la CA Interna del FMC debe ser instalado como certificado de confianza (Trusted Certificate) en el ISE-PIC.

ISE-PIC

ISE Passive Identity Connector

Certificates Management

System Certificates Trusted Certificates OSCP Client Profile Certificate Signing Requests Certificate Periodic Check Settings

Import a new Certificate into the Certificate Store

* Certificate File InternalCA.pem

Friendly Name

Trusted For:

☒ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for certificate based admin authentication

☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description

Ahora se procede a la configuración de fuente de identificación, a través de System/Configuration/Integration/Identity Sources. Se añade el certificado exportado del ISE-PIC.

Cisco Firepower Management Center

System / Integration / Identity Sources

Identity Sources

Service Type ☐ None ☒ Identity Services Engine

Primary Host Name/IP Address

Secondary Host Name/IP Address

pxGrid Server CA

MNT Server CA

FMC Server Certificate

ISE Network Filter

Subscribe To:

Session Directory Topic ☒

SXP Topic ☐

* Required Field

Import Trusted Certificate Authority

Name:

Certificate Data or, choose a file:

-----BEGIN CERTIFICATE-----
 MIIFLCCAxagAwIBAgIQCOAb/1fGT6WthzArXsSOCjANBgkqhkiG9w0BAQwFADAx
 MSBwLQYDVQQDDCZDZXJ0aWZpY2F0ZSB1ZSBJZCJ2aWVncyBSb290IENBIC0gSVNFU
 EID
 MTAEFw0yMTA1MTAxODQ1NDBaFw0zMTA1MTAxODQ1NDBaMDEuLzAtBgNVBAM
 MJkNII

☐ Encrypted, and the password is:

Como certificado del FMC se usa el que hemos configurado anteriormente dentro del propio dispositivo.

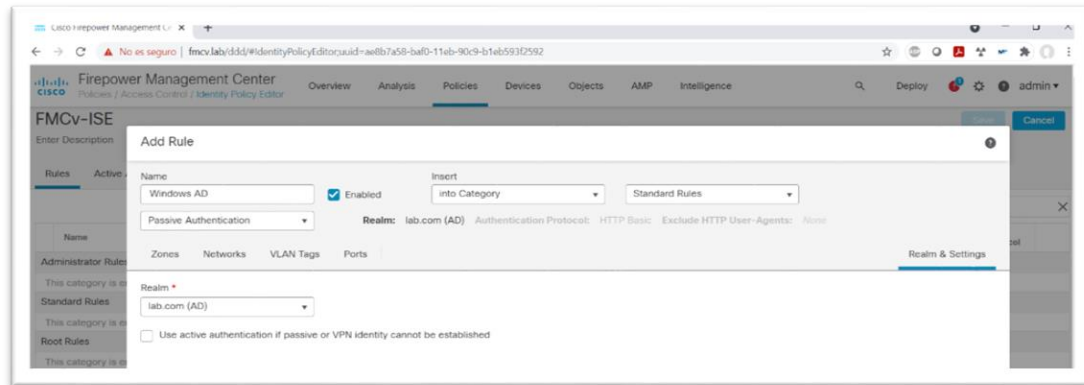
Al realizar el Test, es posible que de este error.

Esto es debido a que el ISE-PIC está configurado para requerir aprobación al añadir nuevos suscriptores. Esto es configurable. En caso de necesitar aprobación, se realiza en “Subscribers”.

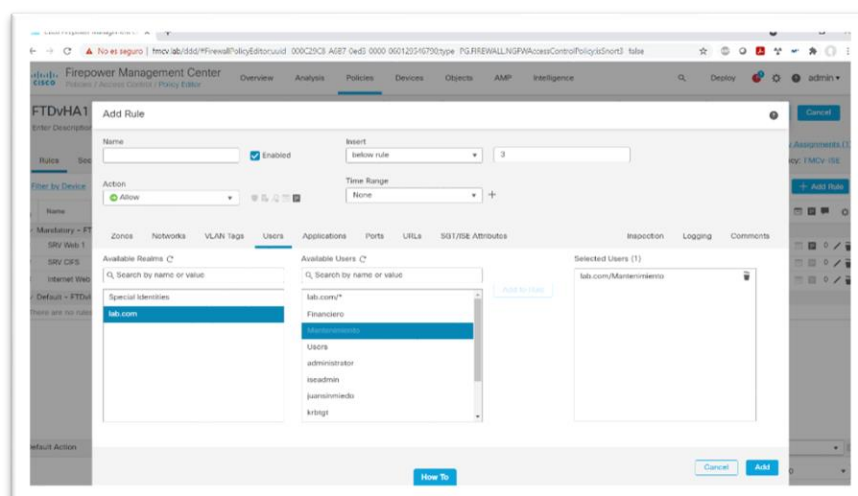
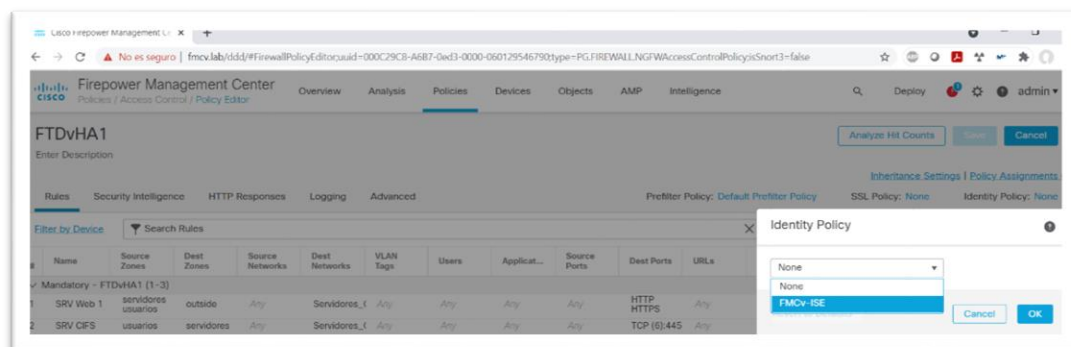
Client Name	Description	Capabilities	Status
ise-pubsub-isepic1		Capabilities(0 Pub, 0 Sub)	Online (XMPP)
ise-fanout-isepic1		Capabilities(0 Pub, 0 Sub)	Online (XMPP)
ise-mnt-isepic1		Capabilities(2 Pub, 1 Sub)	Online (XMPP)
ise-bridge-isepic1		Capabilities(0 Pub, 4 Sub)	Online (XMPP)
ise-admin-isepic1		Capabilities(5 Pub, 2 Sub)	Online (XMPP)
t-fmc-ec73bd46b58f11eba2573b...		Capabilities(0 Pub, 0 Sub)	Pending

Una vez que el Test pase con éxito se graba y ya estará realizada la interconexión entre los 2 dispositivos.

El siguiente paso es crear una política de identidad que utilice la integración de conexión pasivo que se ha creado, en Policies/Identity.



El último paso es asociar la política de identidad a la política de control de acceso. Una vez asociada, ya se podrán utilizar usuarios/grupos en las reglas.



13.20 PROTECCIÓN DE MALWARE (AMP)

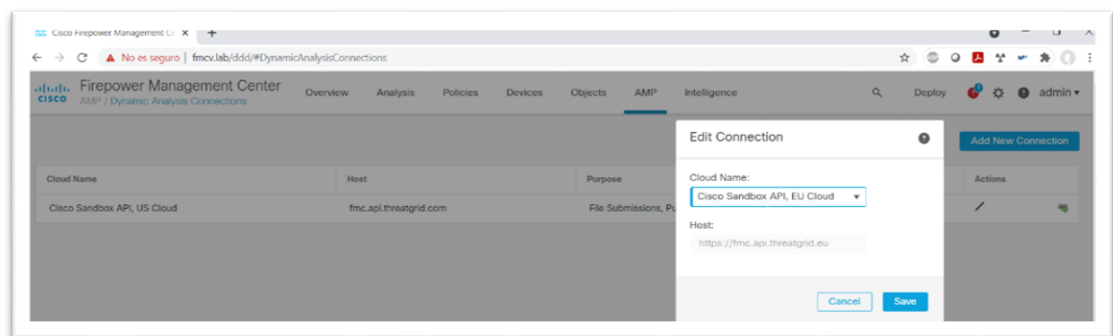
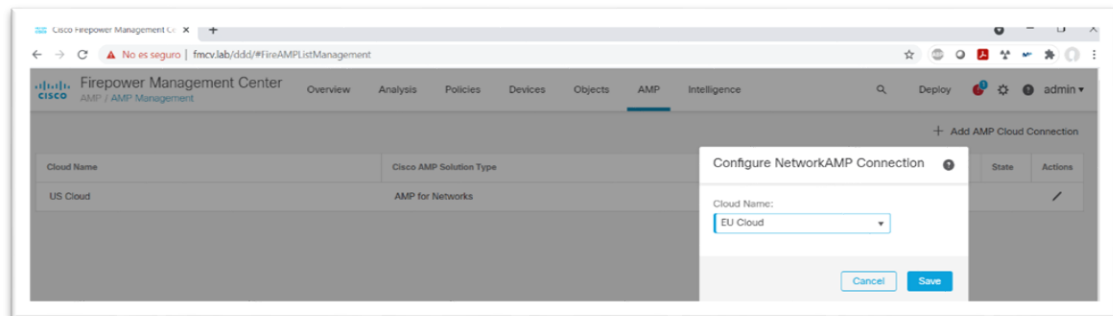
El sistema AMP de Firepower es el encargado del análisis de ficheros en busca de malware, con interceptación inline y cuarentena.

Este servicio requiere de conexión a Internet del FMC y licencia de suscripción AMP. No puede funcionar en “air-gap”.

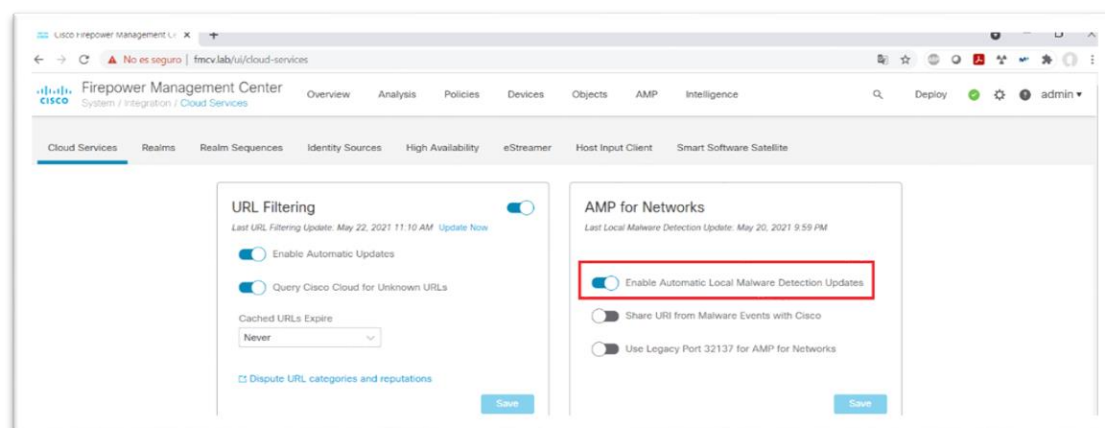
Cisco utiliza análisis en la nube, descarga de firmas y hashes y análisis heurísticos para este servicio.

Para su correcta configuración se debe verificar que la conexión a los servicios AMP de Cisco están en el continente correcto UE.

En el menú AMP, tanto AMP Management como Dynamic Analysis Connections, deben tener seleccionados los servicios de la UE. Por defecto están en US. Se deben editar y cambiar.

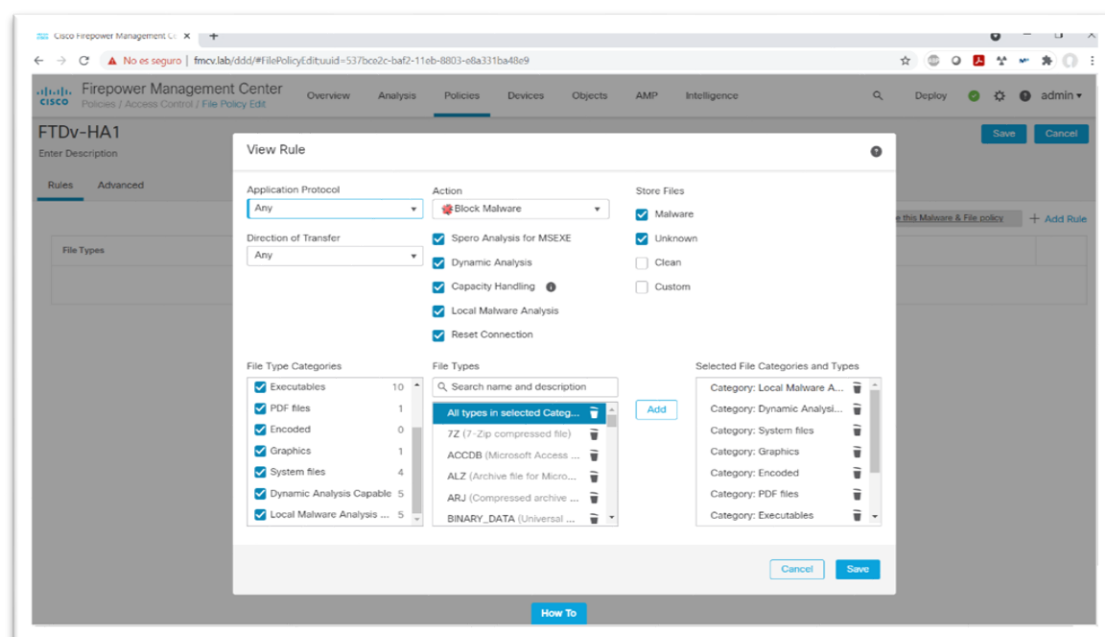


También se debe comprobar que las actualizaciones están activadas. En el menú System->Integration->Cloud Services.

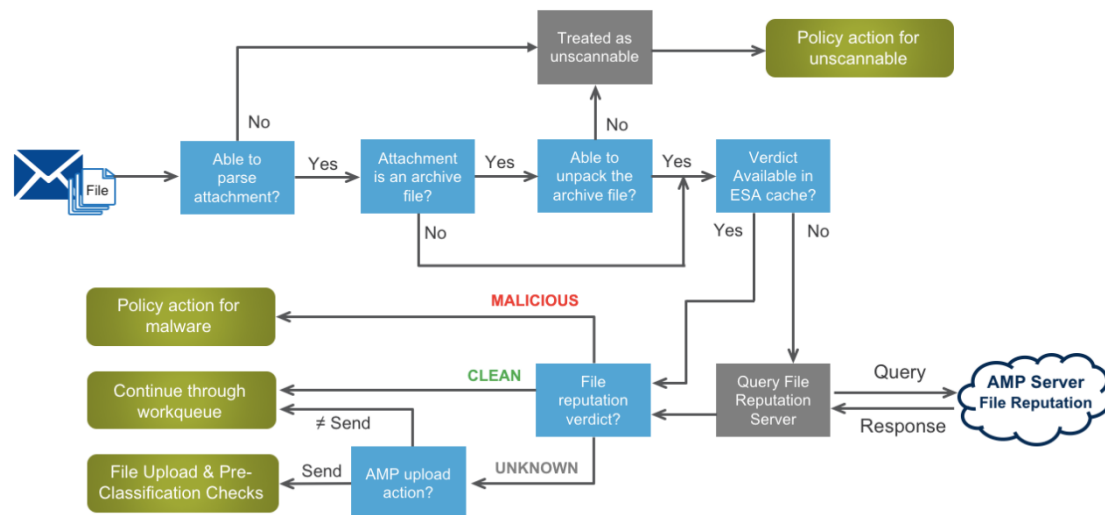


Se debe crear una política de análisis de fichero. Menú Policies->Access Control->Malware & File. “New File Policy”.

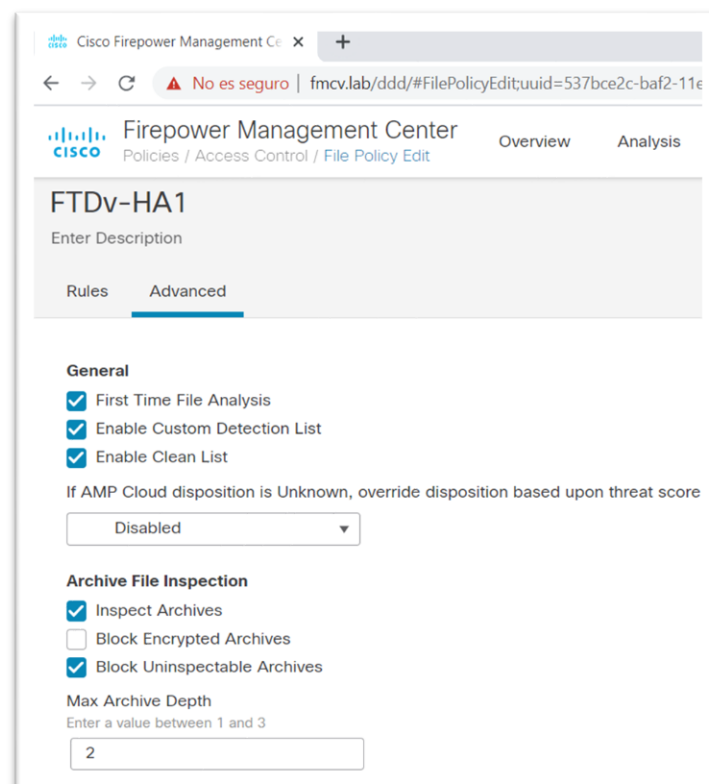
Para una máxima protección se recomienda crear una regla con todo activado, todas las categorías, acción bloqueo y almacenamiento de malware y unknown para análisis.



A continuación, se muestra una explicación gráfica del funcionamiento del motor AMP configurado:

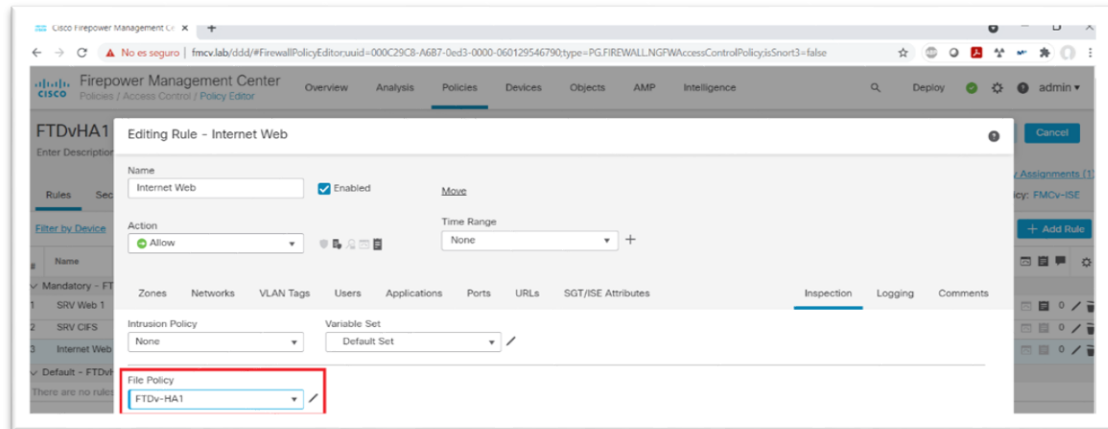


En Advanced habilitamos la inspección de archivos comprimidos con máxima profundidad 3.



Una vez que tenemos la política creada, tenemos que activarla. Esto se hace dentro de la ACP. En cada regla, se puede especificar una política de Inspección de ficheros (File Policy) o no. Se debe configurar en la ACP y se recomienda aplicarla en

todas las reglas posibles que tengan relación con almacenamiento, incluyendo web, CIFS, NFS, etc.



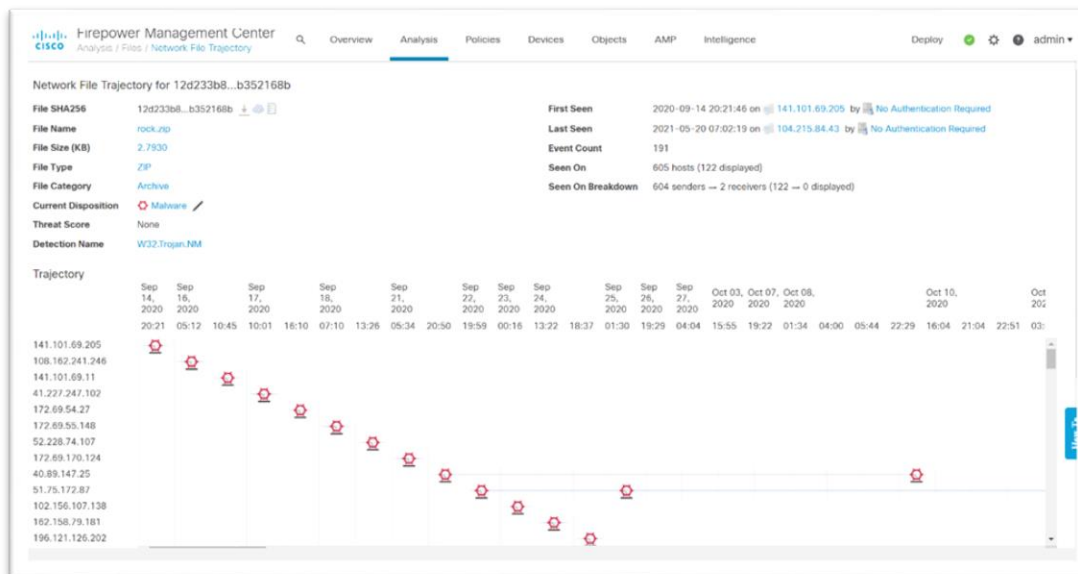
Se pueden seguir los eventos de análisis de ficheros, con sus resultados, utilizando el menú Analysis->File->File Events.

Time	Action	Sending IP	Sending Country	Receiving IP	Receiving Country	Sending Port	Receiving Port	SSL Status	User	File Name
2021-05-22 13:44:14	Malware Cloud Lookup	192.168.100.8	USA	66.249.75.58	USA	80	47647	Unknown (Unknown)	No Authentication Required	PROGRAMA - BI - JORNA
2021-05-22 13:42:28	Malware Cloud Lookup	172.20.2.15	USA	74.125.140.27	USA	59826	25	Unknown (Unknown)	No Authentication Required	Entradas-1621683062
2021-05-22 13:36:15	Malware Cloud Lookup	212.145.41.66	ESP	192.168.100.9	ESP	80	43399	Unknown (Unknown)	No Authentication Required	v32_16.0.13929.2038
2021-05-22 13:36:15	Malware Cloud Lookup	192.168.100.9	ESP	172.20.12.159	ESP	80	52420	Unknown (Unknown)	No Authentication Required	v32_16.0.13929.2038
2021-05-22 13:36:15	Malware Cloud Lookup	212.145.41.67	ESP	192.168.100.9	ESP	80	43181	Unknown (Unknown)	No Authentication Required	v32_16.0.13929.2038
2021-05-22 13:36:15	Malware Cloud Lookup	192.168.100.9	ESP	172.20.12.159	ESP	80	52421	Unknown (Unknown)	No Authentication Required	v32_16.0.13929.2038
2021-05-22 13:30:52	Malware Cloud Lookup	212.145.41.66	ESP	172.20.19.137	ESP	80	59252	Unknown (Unknown)	No Authentication Required	v32_16.0.13929.2038
2021-05-22 13:30:52	Malware Cloud Lookup	212.145.41.66	ESP	172.20.19.137	ESP	80	59248	Unknown (Unknown)	No Authentication Required	v32_16.0.13929.2038
2021-05-22 13:30:46	Malware Cloud Lookup	172.20.2.15	USA	74.125.140.27	USA	59802	25	Unknown (Unknown)	No Authentication Required	Entradas-162168
2021-05-22 13:29:23	Malware Cloud Lookup	192.168.100.8	RUS	79.110.72.25	RUS	80	53687	Unknown (Unknown)	No Authentication Required	INFORMACIÓN-PRÁCT
2021-05-22 13:28:14	Malware Cloud Lookup	172.20.2.15	USA	74.125.140.27	USA	59786	25	Unknown (Unknown)	No Authentication Required	Entradas-1621682284
2021-05-22 13:26:37	Malware Cloud Lookup	172.20.2.15	USA	104.47.57.33	USA	42498	25	Unknown (Unknown)	No Authentication Required	Entradas-1621682118
2021-05-22 13:23:37	Malware Cloud Lookup	77.209.227.10	ESP	172.20.16.13	ESP	80	60347	Unknown (Unknown)	No Authentication Required	disallowedcartel.cab
2021-05-22 13:21:31	Malware Cloud Lookup	212.145.41.67	ESP	172.20.19.113	ESP	80	64193	Unknown (Unknown)	No Authentication Required	v32_16.0.13929.2038

Se pueden ver solo las detecciones de malware (positivos). “Malware Events”.

Detection Name	File Name	File SHA256	File Type	Count
Xis.Downloader.Generic::in05.talos		bc1d9786...d8ae8d56	NEW_OFFICE	150
W32.Trojan.NM	rock.zip	12d733b8...b352168b	ZIP	60
SPAM.ATCh.ec29eb36a.in05.Talos	Statement of Account as of_01_25_2021.xlsm	ec29eb36...31d25954	NEW_OFFICE	47
Win.Dropper.Malseript:95.sbx.tg	revslider.zip	d0dabae1...fa2e4c8c	ZIP	39
Html.Dropper.Generic::mash.sr.sbx.vloc	rock.zip	a499c393...009c0788	ZIP	20
Xis.Downloader.Generic::in05.talos	test report-black.pdf	bc1d9786...d8ae8d56	NEW_OFFICE	2
Xis.Downloader.Generic::in05.talos	t.gif	bc1d9786...d8ae8d56	NEW_OFFICE	1
Xis.Downloader.Generic::in05.talos	Presentacion_ADFB 2021.pptx	bc1d9786...d8ae8d56	NEW_OFFICE	1
Xis.Downloader.Generic::in05.talos	image001.png	bc1d9786...d8ae8d56	NEW_OFFICE	1
Xis.Downloader.Generic::in05.talos	IDEARO 2021o.pdf	bc1d9786...d8ae8d56	NEW_OFFICE	1
Xis.Downloader.Generic::in05.talos	Carta Sector Ferreteria y Bricolaje _ FEBRERO 2021_ Servicio esencial.DG Comercio_Andalucia.pdf	bc1d9786...d8ae8d56	NEW_OFFICE	1
Xis.Downloader.Generic::in05.talos	=?windows-12587Q7NP_ALIANZA__co=CCpia.docx?:	bc1d9786...d8ae8d56	NEW_OFFICE	1
W32.Auto.000a17b55.in03.Talos		000a17b...919d1b96		1

Se puede visualizar también la retrospectiva de cualquier fichero detectado como malware, viendo los puntos de propagación en el tiempo y las IPs involucradas.



13.21 INTERCEPCIÓN SSL – SSL POLICY

En la actualidad la mayoría del tráfico que cursamos, por ejemplo, a webs y correo electrónico, va cifrado. El tráfico cifrado no puede ser analizado por el NGIPS ni AMP.

Para solventar este problema, se utiliza Intercepción SSL/TLS. Lo que realiza esta funcionalidad, en realidad, es un “ataque Man-In-The-Middle”, consentido.

El funcionamiento abreviado es el siguiente:

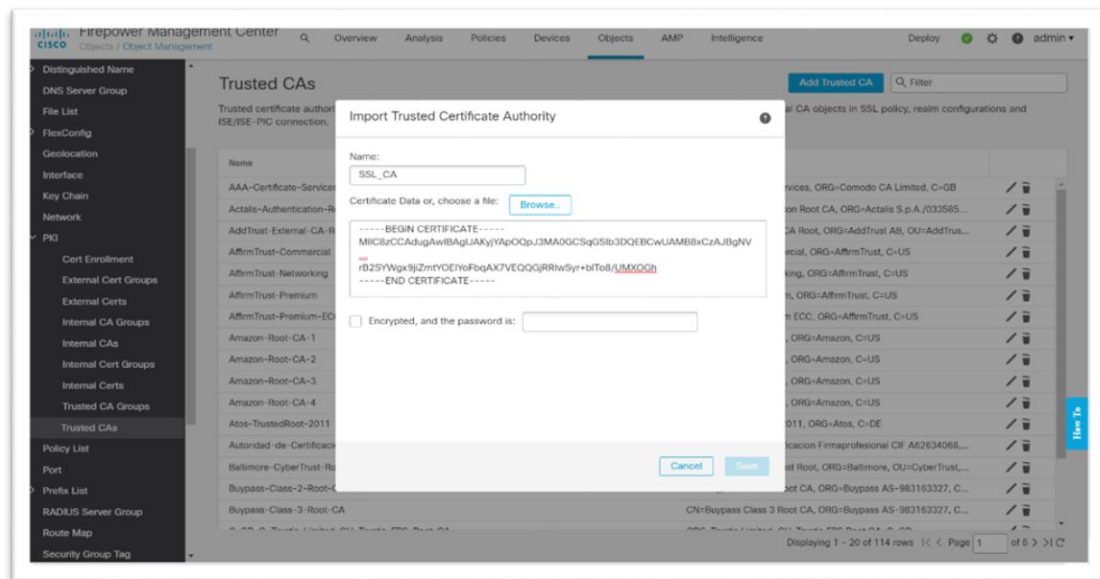
- La solicitud de acceso (cifrado) llega al cortafuegos por parte del cliente, este negocia el cifrado con el cliente como si el cortafuegos fuera el sitio destino, generando un certificado sobre la marcha, con un certificado CA de confianza por el cliente instalado en el cortafuegos.
- El cortafuegos realiza la petición por su cuenta al sitio destino y analiza el tráfico devuelto.
- Si el contenido no es malicioso, lo transmite al cliente con el cifrado “spoofed” creado en el primer paso.

Nota: esta funcionalidad requiere romper la cadena de cifrado de extremo a extremo es, en realidad, una interceptación de comunicaciones. Esto puede tener implicaciones legales según la legislación española. Si se va a activar esta funcionalidad, estas consideraciones legales deben ser tenidas en cuenta y evaluadas adecuadamente.

Como se ha expuesto en el funcionamiento de la característica, el cortafuegos tiene que realizar un importante trabajo de cifrado y descifrado, doble por cada conexión, por lo que esta funcionalidad impacta negativamente el rendimiento del cortafuegos. Se deberá estudiar este impacto en la implementación.

Para activar esta funcionalidad el primer requisito es instalar en el cortafuegos el certificado de la CA, casi siempre interna (no de Internet), que los clientes también tendrán que tener instalada como CA de confianza. En equipos Windows con Directorio Activo, esto se puede automatizar con una política de grupo GPO que puede instalar un certificado automáticamente. Para equipos MAC o Linux la instalación deberá ser manual o por algún software de distribución.

Para la instalación del certificado CA en el cortafuegos se debe ir al menú Objects->Object Management, buscar PKI->Trusted CAs. Seleccionar “Add Trusted CA”. Se puede introducir el certificado realizando un pegado desde el portapapeles o seleccionando un fichero. Si el fichero está cifrado se introduce la contraseña habilitando el “check”.



El siguiente paso es generar una CA intermedia en el cortafuegos. Para ello hay que ir a PKI->Internal CAs y seleccionar “Generate CA”. Hay que rellenar los datos y seleccionar “Generate CSR”.

Generate Internal Certificate Authority

Name:
FP-CA

Country Name (two-letter code):
ES

State or Province:

Locality or City:

Organization:
CCN

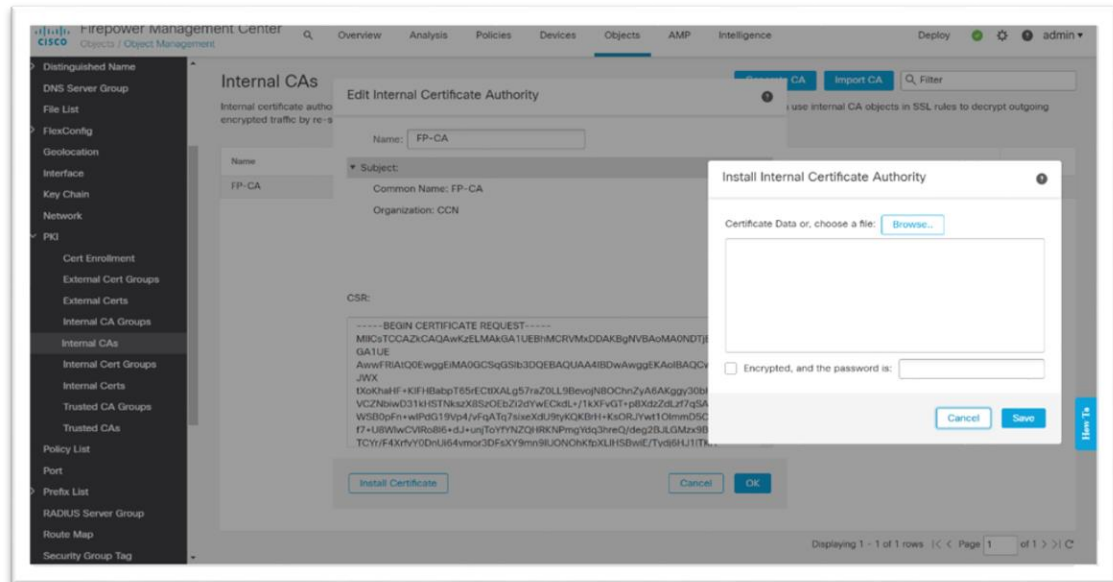
Organizational Unit (Department):

Common Name:
FP-CA

Generate CSR
Cancel
Generate self-signed CA

La solicitud de certificado debe ser pasado a la CA instalada anteriormente para su firma mediante emisión de un nuevo certificado.

Para instalar el certificado, ya emitido por la CA, editamos el objeto y aparecerá la opción “Install Certificate”.



Con los certificados instalados y la CA interna del cortafuegos funcionando, debemos crear la política SSL. En el menú Policies->Access Control->SSL, seleccionamos “New Policy”.

Se recomienda que la política por defecto sea “Block with reset”.

New SSL Policy

Name:

FTDvHA1

Description:

Default Action:

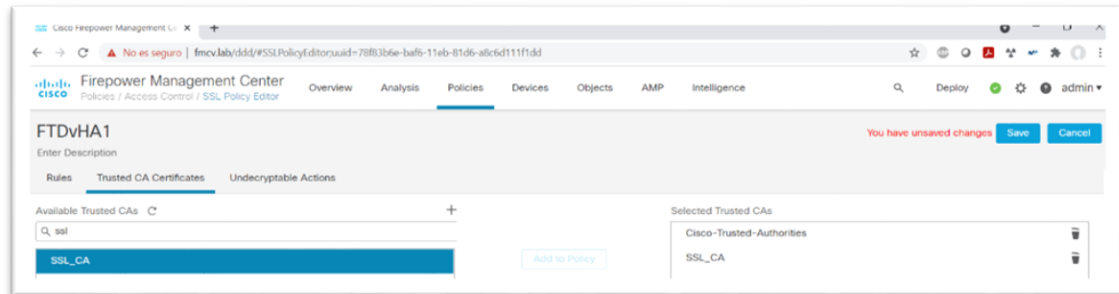
Do not decrypt

Block

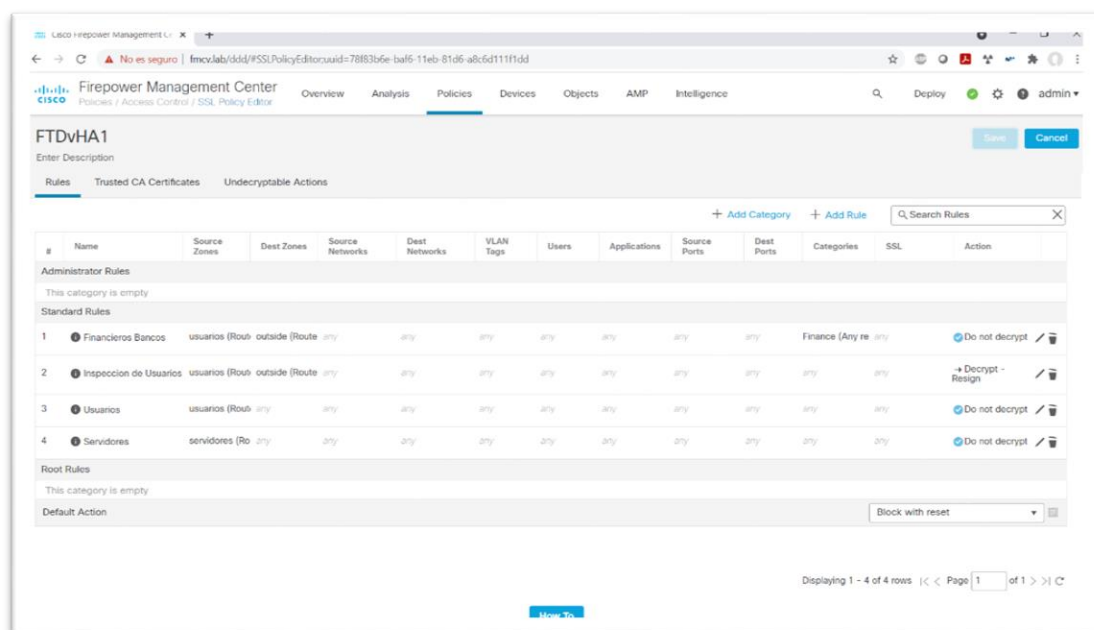
☒ Block with reset

Vamos a mostrar como ejemplo un caso de uso bastante utilizado. Vamos a inspeccionar todo lo que vaya desde la zona de Usuarios a Internet, salvo el acceso a entidades financieras (bancos). El resto (tráfico desde servidores, por ejemplo) no lo vamos a inspeccionar y vamos a dejar que pase sin inspección.

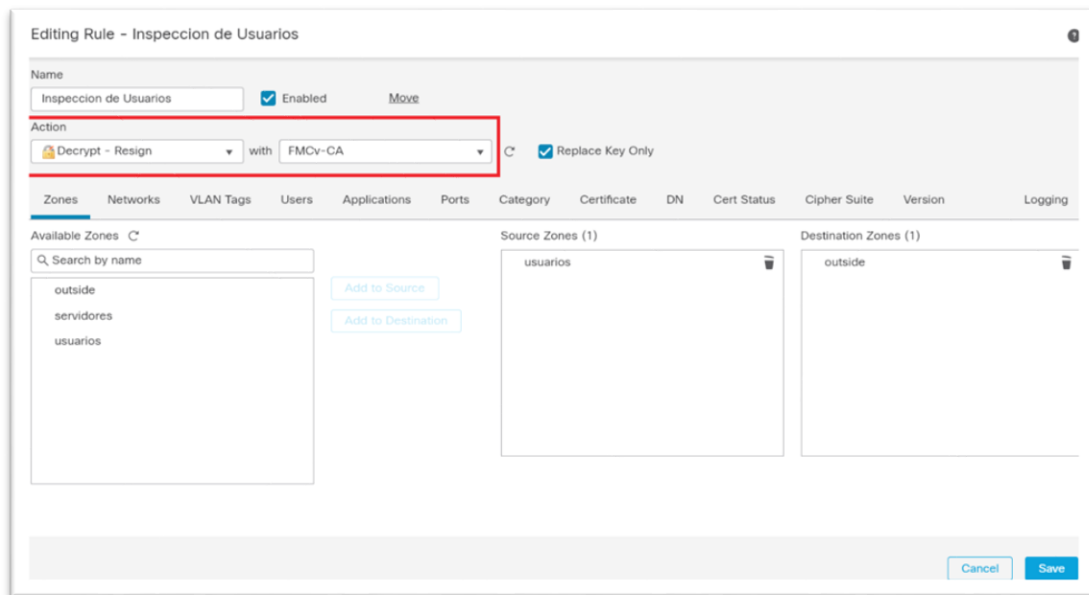
Antes de configurar las reglas, hay que establecer la confianza con la CA que instalamos. Se añade en Trusted CA Certificates.



Muestra de 4 reglas de ejemplo. La política funciona cogiendo la primera coincidencia, es decir, las reglas más específicas deben ir arriba.



La segunda regla es la que realiza la interceptación TLS, desde Usuarios a Internet, el resto que no ha hecho “match” en la primera regla, la acción es “Decrypt – Resign”, que significa, descifra y vuelve a firmar con la CA interna, que se especifica en la regla.

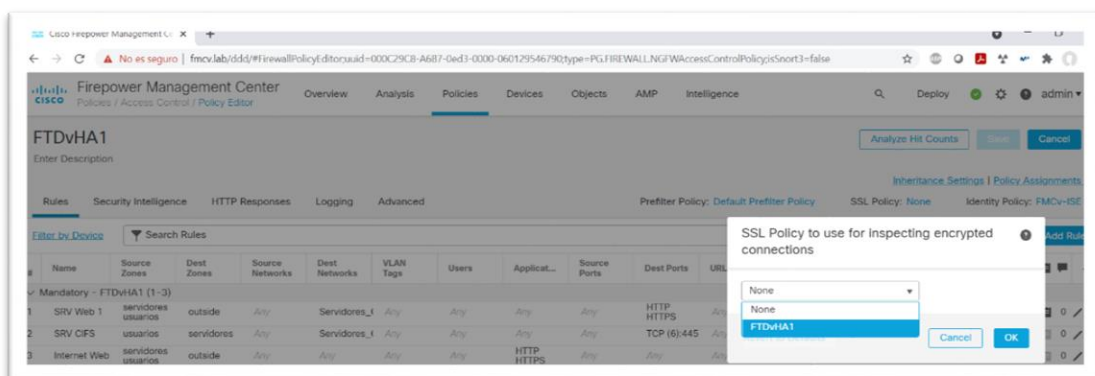


La tercera regla permite que desde la zona de Usuarios se acceda a cualquier otra zona con acción “no hacer nada”. Es decir, si van a “Servidores” no se intercepta.

Y la cuarta regla hace que desde la zona de “Servidores” no se intercepte.

Una vez creada la política SSL y parametrizada, falta el último paso, incorporarla a la ACP para que funcione.

Se accede a Políticas->Access Control->Access Control. Se selecciona la política donde asociada al cortafuegos donde nos interesa realizar la interceptación y la seleccionamos del desplegable en SSL Policy.



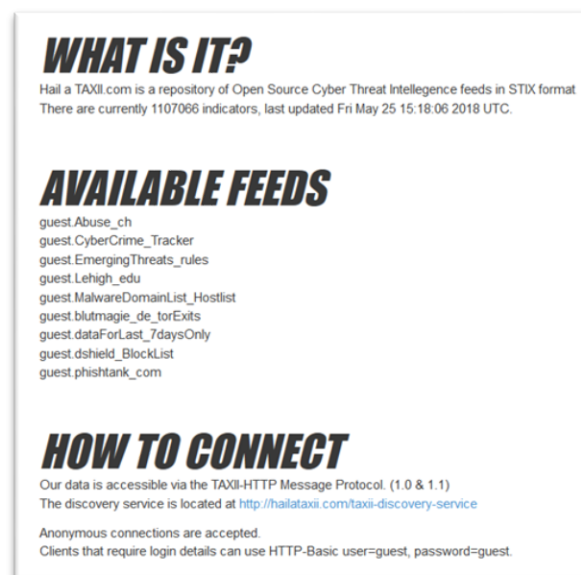
Tras realizar Deploy la interceptación quedará activada.

13.22 THREAT INTELLIGENCE DIRECTOR (TID)

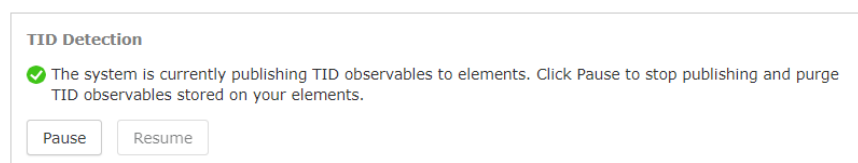
Esta funcionalidad posibilita integrar firmas de terceros dentro del motor IPS de Cisco.

Los protocolos soportados son TAXII, STIX o fichero plano.

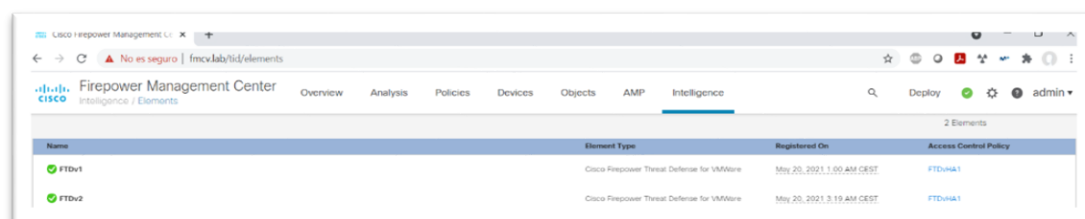
En este ejemplo vamos a usar las firmas gratuitas del proyecto “Hail a TAXII” (<http://hailataxii.com/>)



Se debe comprobar que el TID está corriendo y funcionando correctamente. En el menú Intelligence->Settings debe aparecer en verde.



Y en Intelligence->Elements debe aparecer algún dispositivo FTD con IPS con el que podamos comunicar.



En Intelligence->Sources añadimos una nueva fuente con los datos de “hail a taxi”. Podemos seleccionar las FEEDS que deseemos. Y modificar el período de “updates” al valor que consideremos.

Add Source

DELIVERY: **TAXII** | URL | Upload

URL*: SSL Settings ▾

USERNAME:

PASSWORD:

⚠ Credentials will be sent using an unsecured HTTP connection

FEEDS*

- ☒ guest Abuse_ch
- ☒ guest CyberCrime_Tracker
- ☒ guest EmergingThreats_rules
- ☒ guest EmergingThreats_rules
- ☒ guest Lehigh_edu
- ☒ guest MalwareDomainList_Hostlist
- ☒ guest blumagie_de_toExits
- ☒ guest dataForLast_7daysOnly
- ☒ guest dshield_BlockList
- ☒ guest phantank_com

Note: A separate source will be added for each feed selected. The name will default to the name of the feed and can be edited later.

ACTION: **Monitor**

UPDATE EVERY (MINUTES): ☐ Never Update

TTL (DAYS):

PUBLISH: ☒

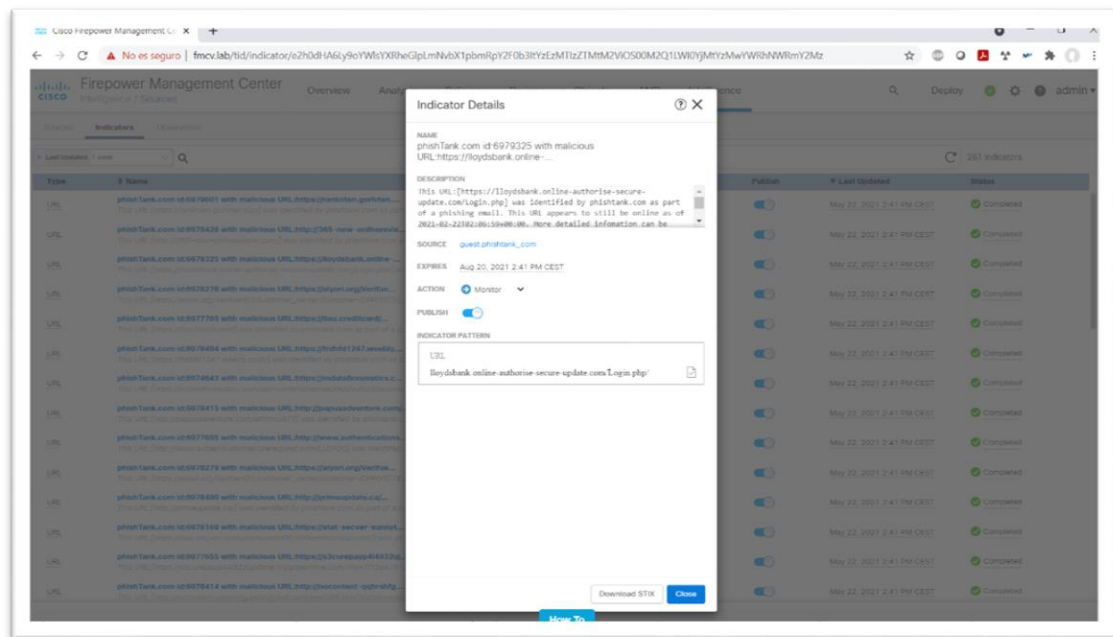
Save Cancel

Una vez añadidos, veremos que el sistema empezará con el “Parsing” y a descargar las firmas.

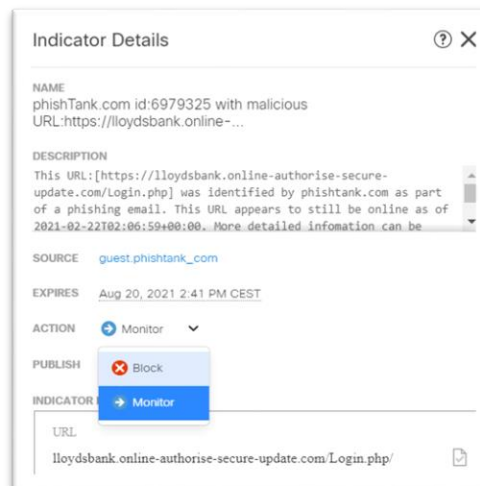
Name	Type	Delivery	Action	Publish	Last Updated	Status
guest.EmergingThreats_rules	STIX	TAXII	Monitor	On	2 seconds ago Pause Updates	Completed
guest.CyberCrime_Tracker	STIX	TAXII	Monitor	On	7 seconds ago Pause Updates	Completed
guest.Lehigh_edu	STIX	TAXII	Monitor	On	11 seconds ago Pause Updates	Completed
guest.MalwareDomainList_Hostlist	STIX	TAXII	Monitor	On	16 seconds ago Pause Updates	Completed
guest.blumagie_de_toExits	STIX	TAXII	Monitor	On	21 seconds ago Pause Updates	Completed
guest.EmergingThreats_rules	STIX	TAXII	Monitor	On	25 seconds ago Pause Updates	Completed
guest.Abuse_ch	STIX	TAXII	Monitor	On	25 seconds ago Pause Updates	Completed
guest.dataForLast_7daysOnly	STIX	TAXII	Monitor	On	Never Pause Updates	Scheduled
guest.dshield_BlockList	STIX	TAXII	Monitor	On	Never Pause Updates	Scheduled
guest.phantank_com	STIX	TAXII	Monitor	On	Never Pause Updates	Scheduled

En Indicators empezarán a aparecer objetos y en Observables aparecerán los objetos asociados a los Indicators.

Pulsando dentro de un Indicator podremos ver su descripción e información.



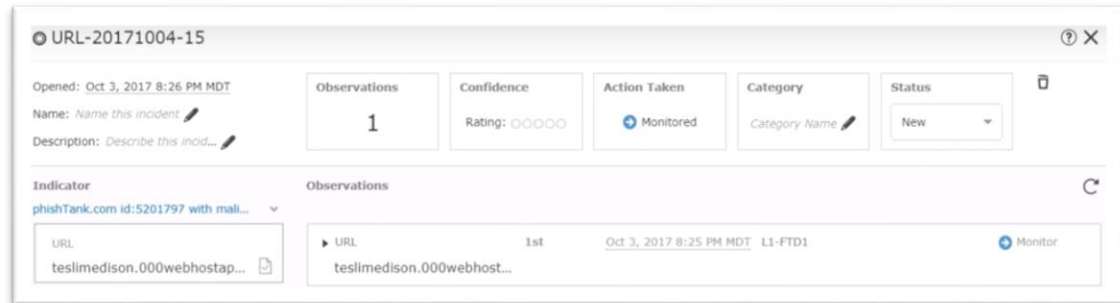
La acción por defecto es Monitor, y no se puede modificar de entrada por el funcionamiento de los objetos STIX usados en TAXII. Pero una vez cargados se pueden modificar en el menú.



Si navegamos a algún objeto URL incluido en algún Indicator, en el menú Incident aparecerá el incidente.

Last Updated	Incident ID	Indicator Name	Type	Action Taken	Status
2 seconds ago	URL-20171004-15	phishtank.com id:5201797 with malicious URL:https://teslimedison.000...	URL	Monitored	New

Pinchando sobre el incidente podremos tener más información y operar sobre él, cambiar su estado, Confidence, etc.



Recordad que como la acción está puesto en Monitor la conexión se permite. Si la cambiamos a Block podremos bloquear futuros accesos si es necesario.

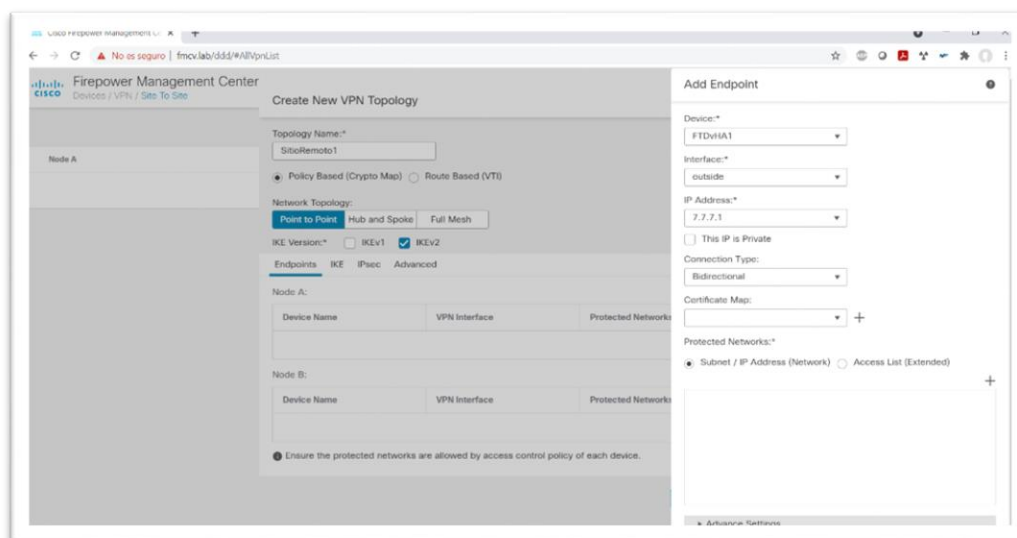
13.23 RED PRIVADA VIRTUAL - VPN SITE TO SITE

El sistema de Redes Privadas Virtuales (VPN) Site to Site (o Lan to Lan) permite extender nuestra red, o conectar a otra de un tercero, a través de otra red insegura, como Internet, mediante el uso de túneles cifrados.

El protocolo utilizado es IPSec.

Firepower soporta IPSec tanto en IKEv1 como IKEv2. Se recomienda el uso de IKEv2 siempre que sea posible, por su mayor seguridad.

Para crear una nueva VPN hay que acceder al menú Device->VPN->Site to Site y pinchar en “Add VPN” de tipo “Firepower Threat Defense Device”.



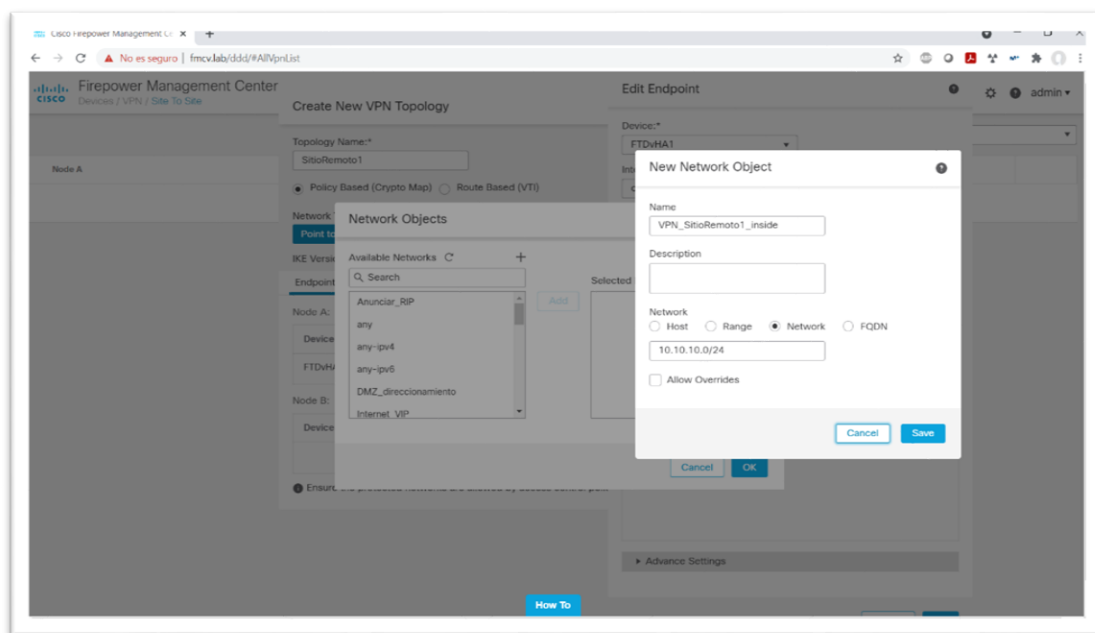
Hay que introducir los nodos de un lado y el otro, Nodo A y B.

El sistema permite crear VPNs sencillas en el caso de que ambos equipos estén gestionados por el mismo FMC. En el caso de que el equipo remoto no pertenezca al FMC o sea de un tercero u otro fabricante, se configure como “External”.

En este ejemplo vamos a crear una conexión con un dispositivo External, con IKEv2 y clave compartida “PSK”.

Hay que especificar la red “protegida” en nuestro lado, nodo A, “fp2110-1” a la que queremos que tenga acceso el otro lado, nodo B, “External”.

Todos los objetos se pueden crear directamente pinchando en los “+”.



Add Endpoint

Device:*
FTDvHA1

Interface:*
outside

IP Address:*
7.7.7.1

☐ This IP is Private

Connection Type:
Bidirectional

Certificate Map:
+

Protected Networks:*
☒ Subnet / IP Address (Network) ☐ Access List (Extended)

VPN_SitioRemoto1_inside

Add Endpoint

Device:*
Extranet

Device Name:*
SitioRemoto1

IP Address:*
☒ Static ☐ Dynamic
8.8.8.8

Certificate Map:
+

Protected Networks:*
☒ Subnet / IP Address (Network) ☐ Access List (Extended)

VPN_SitioRemoto1_outside

Create New VPN Topology

Topology Name:*
SitioRemoto1

☒ Policy Based (Crypto Map) ☐ Route Based (VTI)

Network Topology:
Point to Point Hub and Spoke Full Mesh

IKE Version:* ☐ IKEv1 ☒ IKEv2

Endpoints **IKE** IPsec Advanced

Node A:		
Device Name	VPN Interface	Protected Networks
FTDvHA1	outside/7.7.7.1	VPN_SitioRemoto1_inside

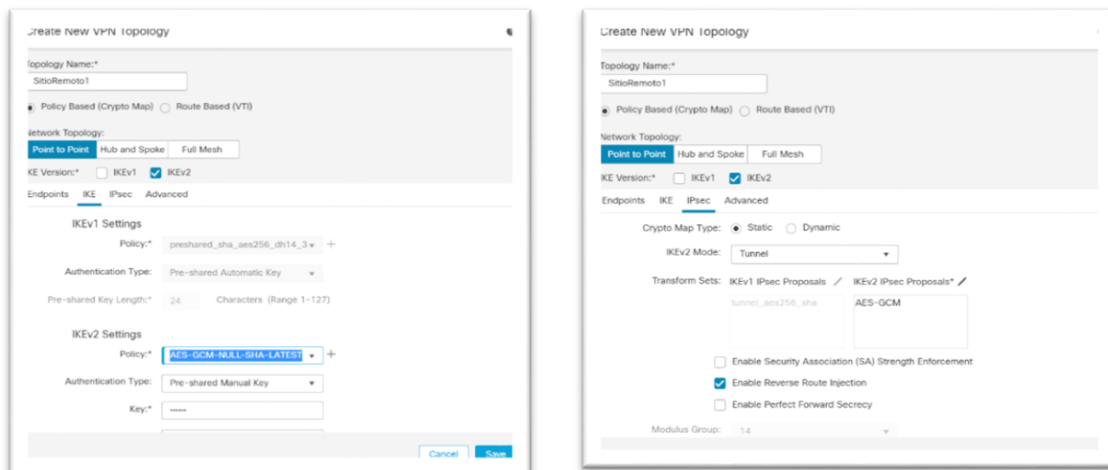
Node B:		
Device Name	VPN Interface	Protected Networks
SitioRemoto1	8.8.8.8	VPN_SitioRemoto1_outside

☒ Ensure the protected networks are allowed by access control policy of each device.

Cancel Save

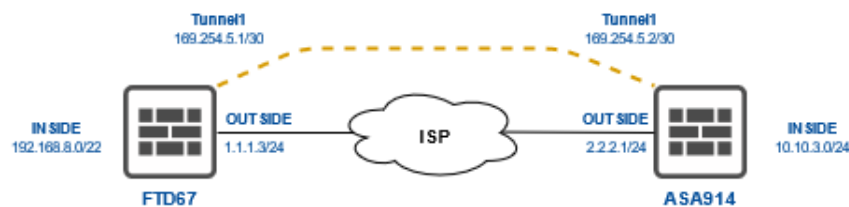
Los cifrados IKE e IPsec deben coincidir con los del otro extremo.

Se recomienda el uso siempre de algoritmos según las exigencias de la CCN-STIC 807 Criptografía de empleo del ENS, para categoría Alta. En caso de crear uno nuevo se pueden especificar varios algoritmos o ajustes y el sistema negociará siempre prefiriendo el más seguro.

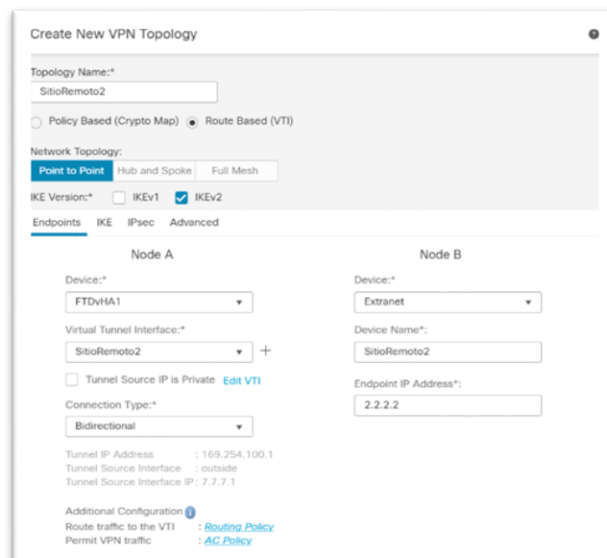
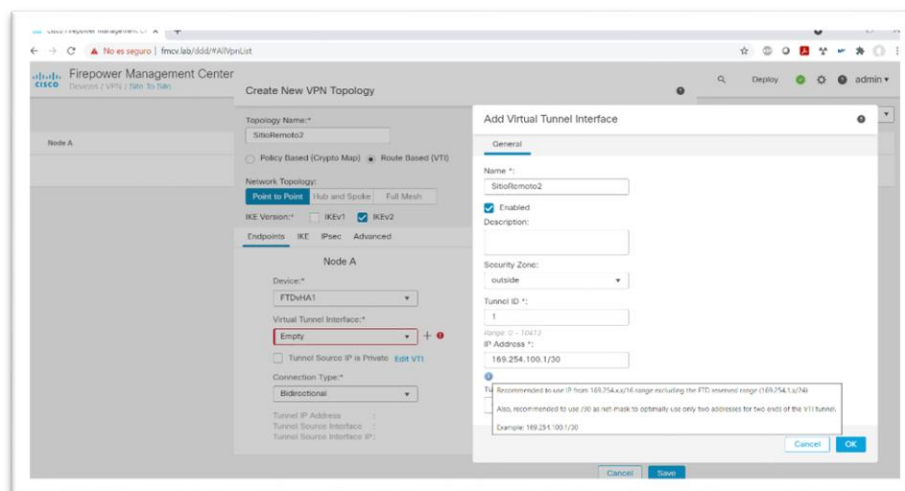


Una vez creada la política de VPN, es importante crear las reglas correspondientes en la política de acceso (ACP) que permitan el tráfico necesario entre la red protegida del nodo A y la red protegida del nodo B. Así mismo revisar la política de NAT aplicada al dispositivo para verificar la exención de los rangos de direcciones IP aplicados NAT. Especialmente evaluar la necesidad de reglas de NAT de Identidad.

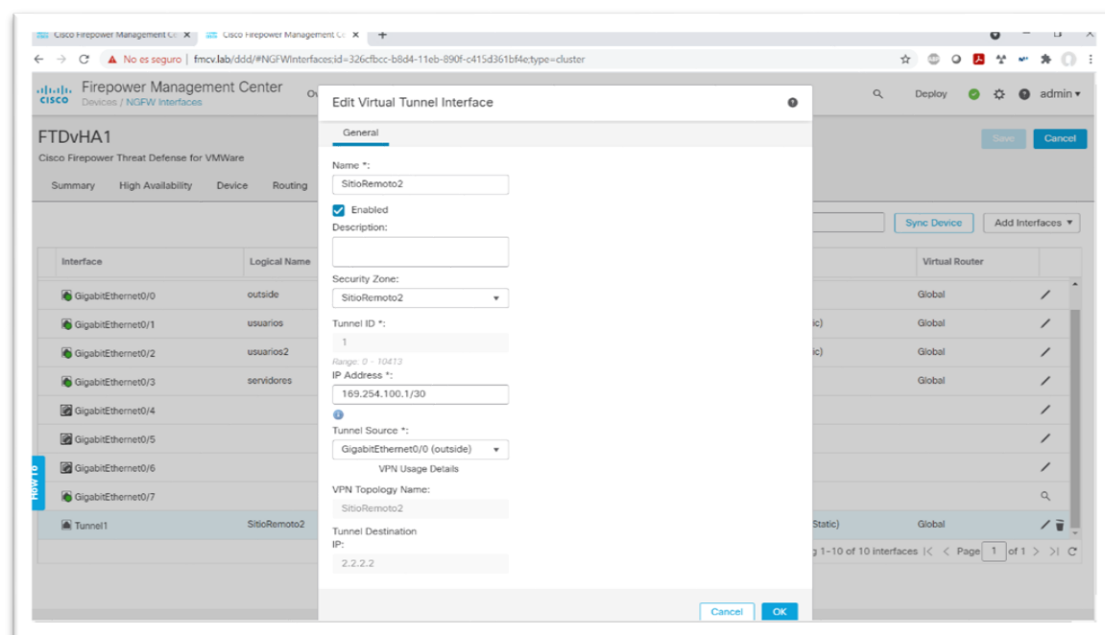
Desde la versión 6.7, se permite crear una VPN utilizando Virtual Tunnel Interfaces (VTI). Esto es una clara mejora con respecto al modo “estático”, permitiendo, incluso, el uso de alta disponibilidad y/o balanceo de carga si se combina con el uso de protocolo de rutado (routing).



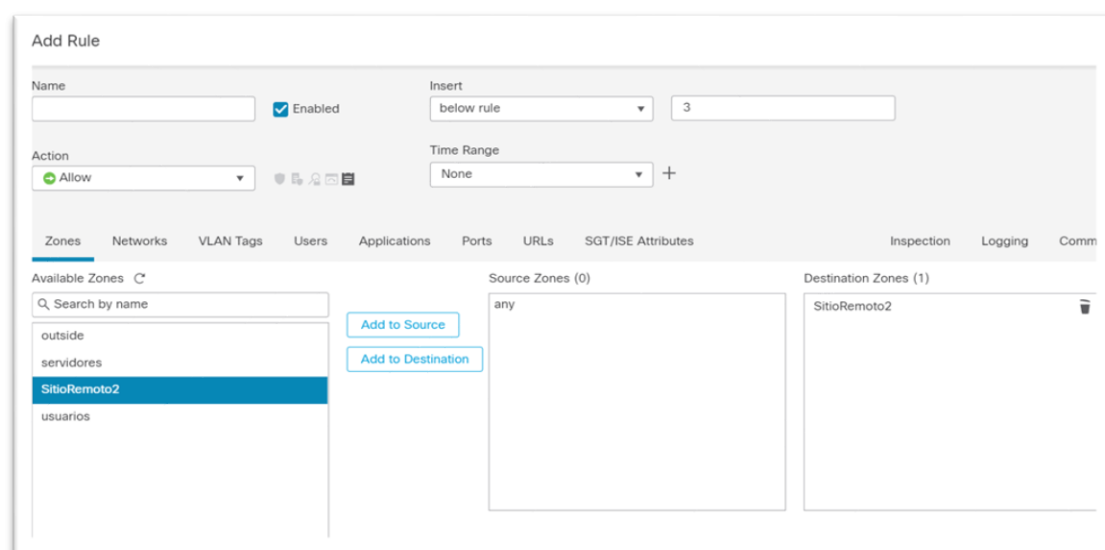
Para configurarlo, en vez de configurar redes, se crean los túneles VTI.



En la sección de Interfaces del Dispositivo pueden verse los VTIs, a los cuales se les puede asignar una nueva zona de seguridad.



De esta manera pueden definirse reglas para filtrar el tráfico a través del túnel VTI.



13.24 RED PRIVADA VIRTUAL - VPN DE ACCESO REMOTO

Las VPN de acceso remoto posibilitan que un usuario remoto se conecte, normalmente a través de Internet, a una red interna.

Firepower soporta conexiones dinámicas de usuarios remotos vía cliente Cisco Anyconnect. Este usa protocolos cifrados TLS o IPSec/IKEv2.

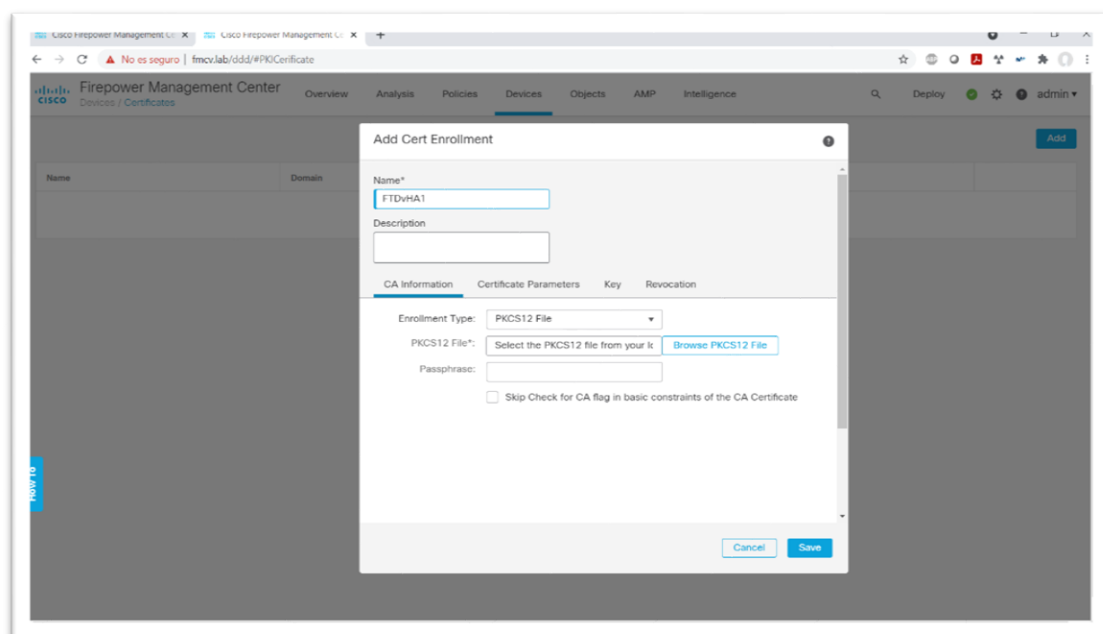
Esta característica requiere licencia de suscripción Anyconnect Plus, Apex o VPN Only.

Para el uso de esta característica se necesita:

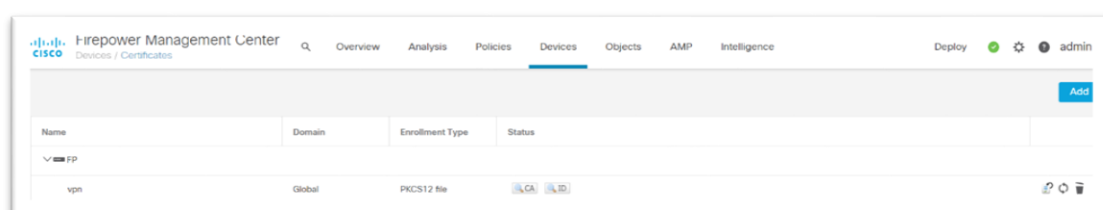
- Certificado digital. Se recomienda uno que sea válido/público, comúnmente, provisto por una CA externa, no interna.
- Servidor RADIUS o LDAP para autenticar a los usuarios. No se soportan usuarios locales en el dispositivo.

El primer paso es importar el certificado, incluyendo sus certificados de CA root e intermedia si la hubiera.

En Devices->Certificates, pinchar en "Add". En este ejemplo vamos a importar un PKCS12 que incluye la clave privada, el certificado y el de la CA.



Una vez importado correctamente debe aparecer con los iconos de CA e ID.



Ahora se debe crear la configuración de VPN de acceso remoto. En el menú Devices->VPN->Remote Access. La primera vez que se pulse sobre "Add" se lanzará un

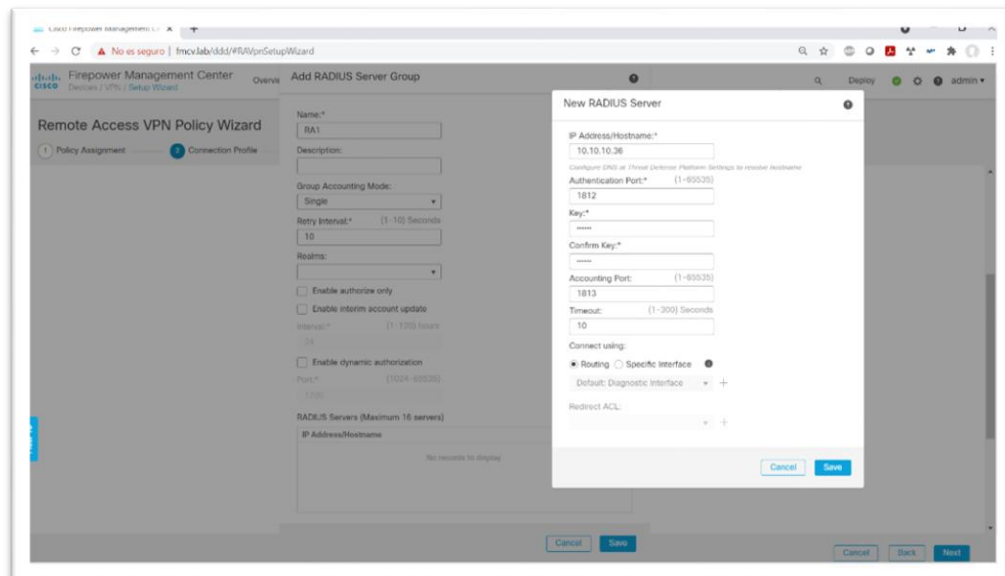
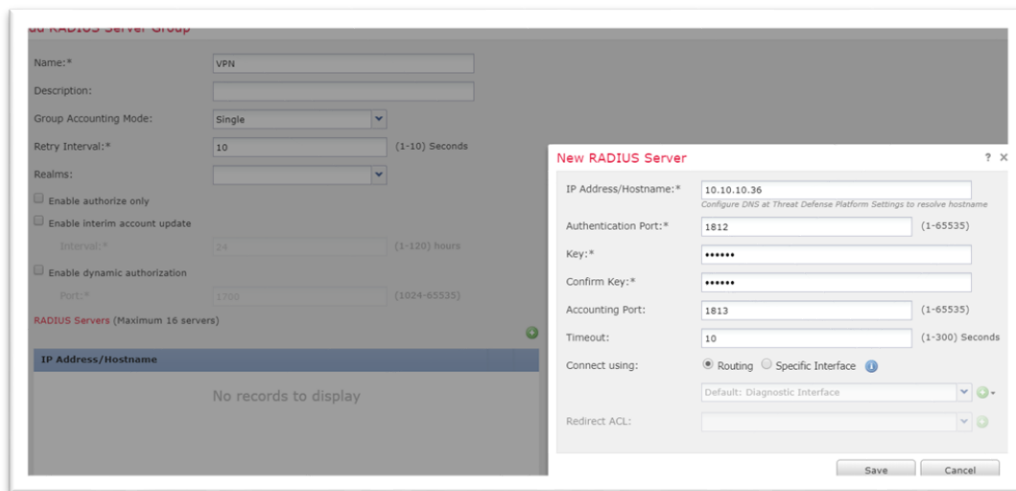
asistente de configuración para crear la primera. En sucesivas nuevas VPN de acceso remoto no.

Se asigna nombre y dispositivo.

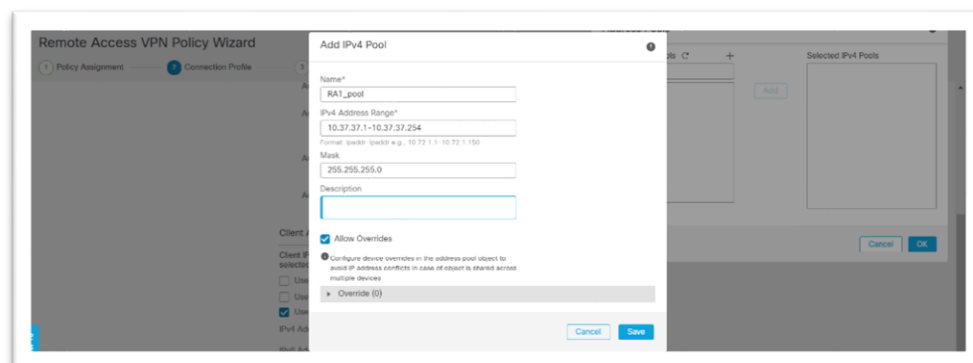
The screenshot shows the 'Remote Access VPN Policy Wizard' in the Cisco Firepower Management Center. The wizard is at the 'Policy Assignment' step (Step 1 of 5). The 'Targeted Devices and Protocols' section includes a 'Name' field with 'RA1' entered, a 'Description' field, and 'VPN Protocols' with 'SSL' and 'IPsec-IKEv2' selected. Under 'Targeted Devices', 'FTDxHA1' is selected from the 'Available Devices' list. A 'Before You Start' sidebar on the right provides instructions on configuration prerequisites, including setting up an authentication server (Realm or RADIUS Server Group) and ensuring the AnyConnect client package is installed on the device interface.

Se añade el servidor Radius.

The screenshot shows the 'Remote Access VPN Policy Wizard' at the 'Connection Profile' step (Step 2 of 5). The 'Connection Profile Name' is 'RA1'. A note indicates this name is configured as a connection alias. The 'Authentication, Authorization & Accounting (AAA)' section is active, showing the 'Authentication Method' set to 'AAA Only'. The 'Authentication Server' is set to 'RADIUS Server Group' (selected from a dropdown that also shows 'Realm'). The 'Authorization Server' is set to 'Use same authentication server', and the 'Accounting Server' is set to 'RADIUS'.



Se crea el Pool de direcciones IP. Al conectarse con éxito el usuario se le asignará una IP de este pool.



Se recomienda crear una nueva Group Policy parametrizándolo específicamente según necesidades, asignando Banner, servidor DNS interno.

The image displays two screenshots of the Cisco Firepower Group Policy configuration interface, specifically the 'Add Group Policy' page.

Left Screenshot (Banner Tab):

- Name:** RA1
- Description:**
- General Tab:**
 - VPN Protocols:**
 - IP Address Pools:**
 - Banner:** (Selected)
 - Maximum total size: 3999, Maximum characters in a line: 497. In case of a line spanning more than 497 characters, split the line into multiple line.
 - Only plain text is supported (symbols "<code>\"
 - DNS/WINS:**
 - Split Tunneling:**

Right Screenshot (DNS/WINS Tab):

- Name:** RA1
- Description:**
- General Tab:**
- AnyConnect Tab:**
- Advanced Tab:**
 - VPN Protocols:**
 - IP Address Pools:**
 - Banner:**
 - DNS/WINS:** (Selected)
 - Primary DNS Server:** Servidores_DNS
 - Secondary DNS Server:**
 - Primary WINS Server:**
 - Secondary WINS Server:**
 - DHCP Network Scope:**
 - Default Domain:** test.com
 - Split Tunneling:**

Los parámetros de Split Tunneling definen que redes se van a publicar y ser accesibles por el usuario remoto, y que dominios se deben resolver usando el DNS interno, el resto usará el servidor DNS propio del usuario remoto.

Add Group Policy

Name:*
RA1

Description:

General AnyConnect Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

IPv4 Split Tunneling:
Tunnel networks specified below▼

IPv6 Split Tunneling:
Allow all traffic over tunnel▼

Split Tunnel Network List Type:
☒ Standard Access List
 ☐ Extended Access List

Standard Access List:
RA1▼ +

DNS Request Split Tunneling
 DNS Requests:
Send only specified domains over▼
 Domain List:
test.com,lab.com

En los parámetros de Anyconnect, se debe usar un perfil descargable por los clientes. Este perfil es un fichero XML que se puede generar usando la herramienta “VPN Profile Editor” que se puede descargar desde la web de Cisco en la sección de Anyconnect, Profile Editor.

Add AnyConnect File

Name:*
Ra1

File Name:*
RA1.xml [Browse..](#)

File Type:*
AnyConnect VPN Profile▼

Description:

[Cancel](#) [Save](#)

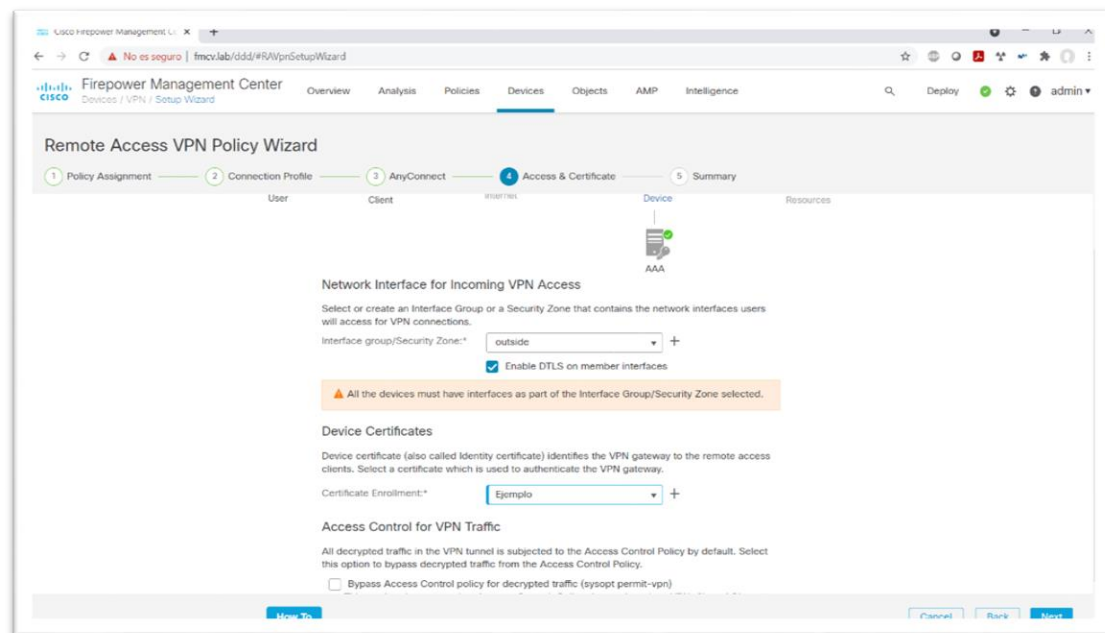
Se pueden especificar restricciones de accesos simultáneos, tiempos máximos de conexión, y horarios de acceso, en la parte Advanced.

The screenshot shows the 'Add Group Policy' configuration window. The 'Name' field is 'RA1'. The 'Description' field is empty. The 'Advanced' tab is selected. Under 'Session Settings', the 'Access Hours' dropdown is set to a plus sign. 'Simultaneous Login Per User' is set to 3. Under 'Connection Time', 'Max Connection Time' is set to 1 minute. Under 'Idle Time', 'Idle Timeout' is set to 30 minutes. Both 'Alert Interval' fields are set to 1 minute.

El siguiente paso conlleva descargar una o varias imágenes del cliente (software) Anyconnect desde la web de Cisco y subirlas. Esto permitirá que los clientes puedan instalarse y auto-actualizarse el cliente en la conexión. En el ejemplo usamos una imagen Windows de despliegue “Headend”.

The screenshot shows the 'Add AnyConnect File' configuration window. The 'Name' field is 'anyconnect-win-4.10.00093-web'. The 'File Name' field is also 'anyconnect-win-4.10.00093-web'. The 'File Type' dropdown is set to 'AnyConnect Client Image'. The 'Description' field is empty. The 'Save' button is highlighted.

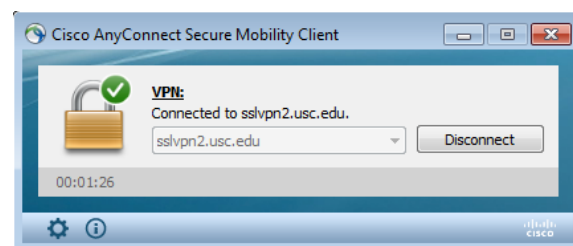
Por último, seleccionamos el interfaz por donde se va a permitir el acceso. Normalmente es el que da a Internet. Y seleccionamos el certificado que importamos al principio.



El asistente mostrará en resumen de parámetros, tras revisarlo y aceptarlo, la VPN estará configurada.

Una vez creada la VPN de acceso remoto, es importante crear las reglas correspondientes en la política de acceso (ACP) que permitan el tráfico necesario desde el Pool de direcciones IP que se asignarán a los clientes y la red interna publicada. Así mismo se debe revisar la política de NAT aplicada al dispositivo para verificar la exención de los rangos de direcciones IP internos al Pool de IP. Especialmente evaluar la necesidad de reglas de NAT de Identidad.

La siguiente imagen muestra una conexión establecida a una VPN de acceso remoto mediante el cliente VPN de Cisco AnyConnect.



Desde la versión 6.4 es posible requerir a los usuarios remotos una doble autenticación. No confundir con doble factor. La doble autenticación se realiza sobre servidores de autenticación diferentes (en doble factor solo se usa uno) y el usuario debe pasar ambas autenticaciones.

Se puede especificar que el nombre de usuario sea el mismo en ambas autenticaciones.

También se permite autenticación mediante certificado digital y, además, usuario y contraseña, pudiendo derivar el usuario desde el certificado.

The screenshot shows the 'AAA' tab in the configuration interface. Under the 'Authentication' section, the 'Authentication Method' is set to 'AAA Only' and the 'Authentication Server' is 'SRADIUS01 (RADIUS)'. The 'Use secondary authentication' checkbox is checked. Below this, the 'Authentication Server' for secondary authentication is set to a dropdown menu. Under the 'Username for secondary authentication' section, the 'Prompt' radio button is selected. Other options include 'Use primary authentication username', 'Map username from client certificate', and 'Use secondary username for VPN session'.

13.25 COPIAS DE SEGURIDAD – BACKUP

Las copias de seguridad forman parte de la seguridad ya que proveen de respaldo para la restauración del servicio y, también, una imagen en el tiempo de los cambios que puedan haberse realizado inadvertidamente en los sistemas.

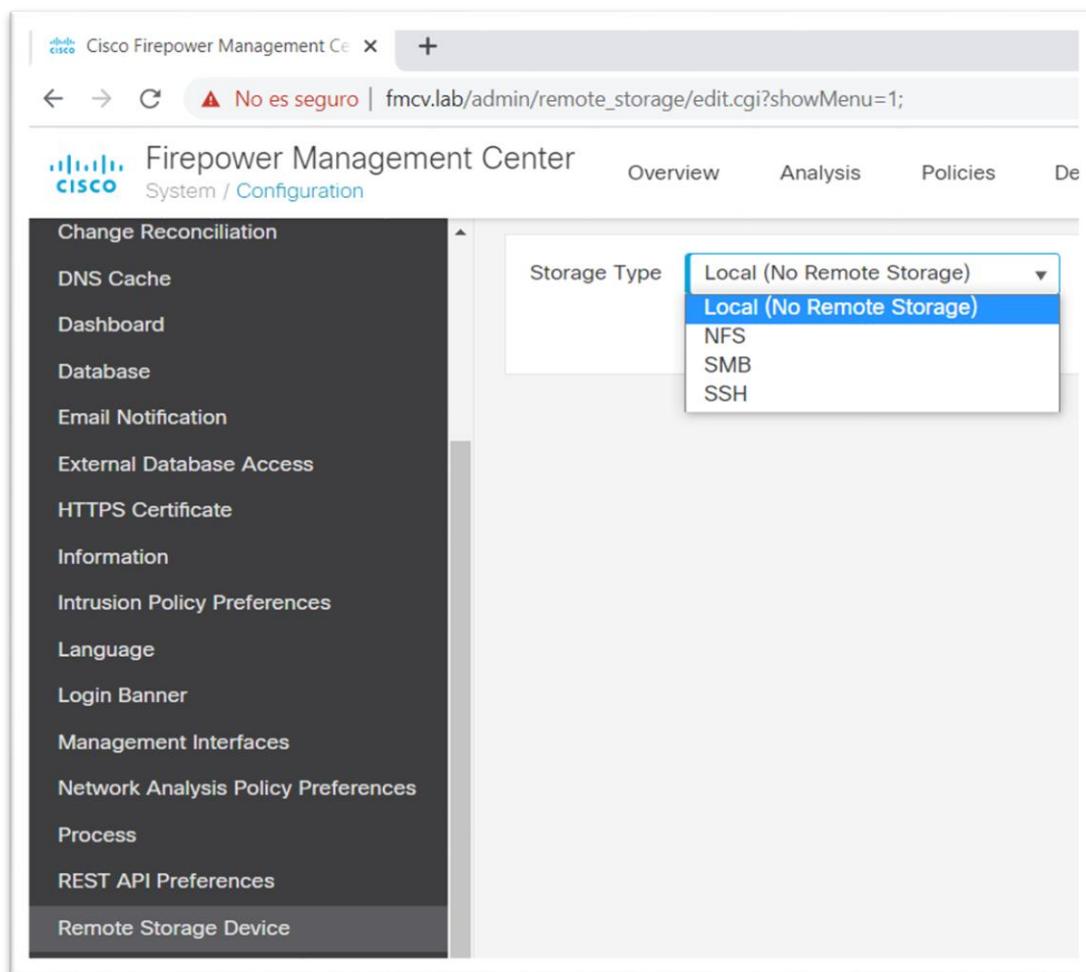
Existen 2 tipos de copia de seguridad, copia de seguridad del gestor, Firepower Management Center, y copia de seguridad de los dispositivos.

Se debe realizar una copia de seguridad periódica del gestor. El gestor contiene toda la información de policía de seguridad, configuraciones, interfaces, etc.

Se deben realizar también copias de seguridad periódica de los dispositivos, especialmente cuando se vaya a realizar un upgrade de versión mayor del dispositivo o se requiera tener una copia de respaldo por algún motivo específico. Una copia puede ser restaurada en un equipo de sustitución para facilitar su reemplazo en una arquitectura de alta disponibilidad.

Las copias de seguridad pueden realizarse directamente en el almacenamiento local del gestor o en un almacenamiento remoto. Se recomienda el almacenamiento remoto.

Para configurar el almacenamiento remoto se debe ir al menú System->Configuration->Remote Storage Device. Si el equipo está en modo Common Criteria, el tipo "SSH" (SCP/SFTP) no funcionará. Tipos disponibles:



En este ejemplo vamos a usar NFS.

Success
Connection Tested Successfully

Storage Type: NFS

Connection

Host: 10.124.241.211 (IP or hostname)

Directory: /storage

Advanced

Use Advanced Options: ☐

System Usage

Use for Backups: ☐

Use for Reports: ☐

Disk Space Threshold: 90 %

Test Save

Para realizar las copias de seguridad (backup) hay que acceder al menú System->Tools->Backup/Restore.

Para configurar un backup periódico del gestor, se debe crear un perfil. Pestaña "Backup Profile", pulsar sobre "Create Profile". Se recomienda realizar copia de la configuración y el TID. La copia de los Eventos requiere mucho espacio, seleccionar si se requiere, por auditoría u otra razón. Seleccionar "Save As New".

The screenshot shows the 'Create Backup' form in the Firepower Management Center. The form is titled 'Create Backup' and is located under the 'Backup Profiles' tab. It contains the following fields and options:

- Name:** fmc
- Storage Location:** /var/sf/backup/
- Back Up Configuration:** ☒
- Back Up Events:** ☐
- Back Up Threat Intelligence Director:** ☒
- Email:** Not available. You must set up your mail relay host.
- Copy when complete:** ☐

At the bottom of the form, there are three buttons: 'Cancel', 'Save As New', and 'Start Backup'.

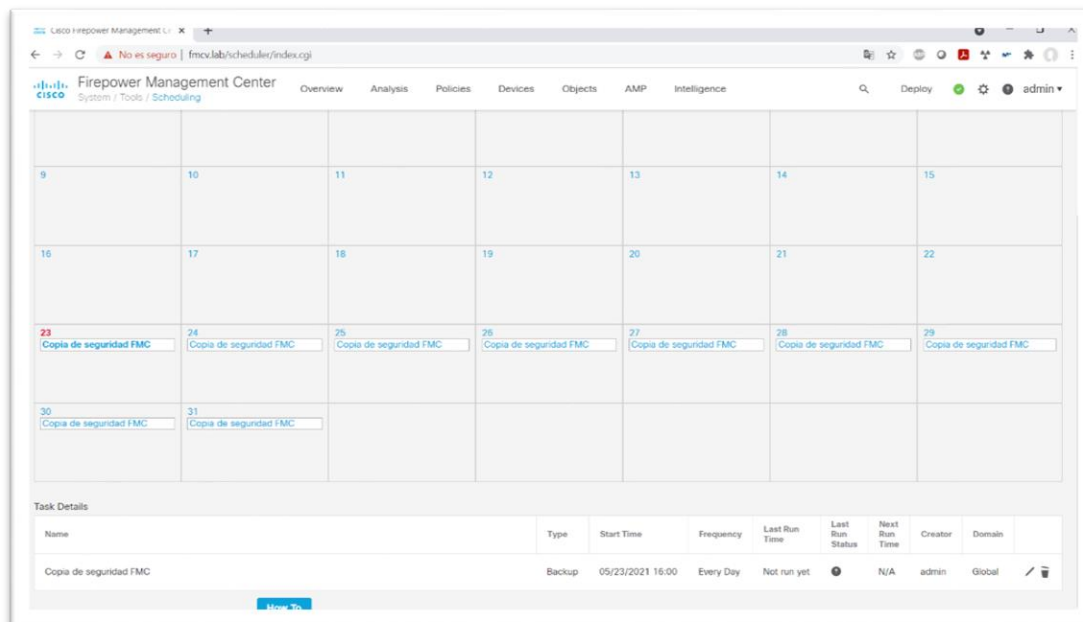
Una vez creado el perfil se debe crear la tarea periódica. Menú System->Tools->Scheduling. Seleccionar "Add Task". Creamos, por ejemplo, una tarea periódica diaria realice la copia a las 4 am.

The screenshot shows the 'New Task' form in the Firepower Management Center. The form is titled 'New Task' and is located under the 'Scheduling' tab. It contains the following fields and options:

- Job Type:** Backup
- Schedule task to run:** ☐ Once ☒ Recurring
- Start On:** May 22, 2021 Europe/Madrid
- Repeat Every:** 1 Days
- Run At:** 4:00 Pm
- Job Name:** Copia de seguridad FMC
- Backup Type:** ☒ Management Center ☐ Device
- Backup Profile:** fmc
- Comment:** (Empty text area)
- Email Status To:** Not available. You must set up your mail relay host.

At the bottom of the form, there are two buttons: 'Cancel' and 'Save'.

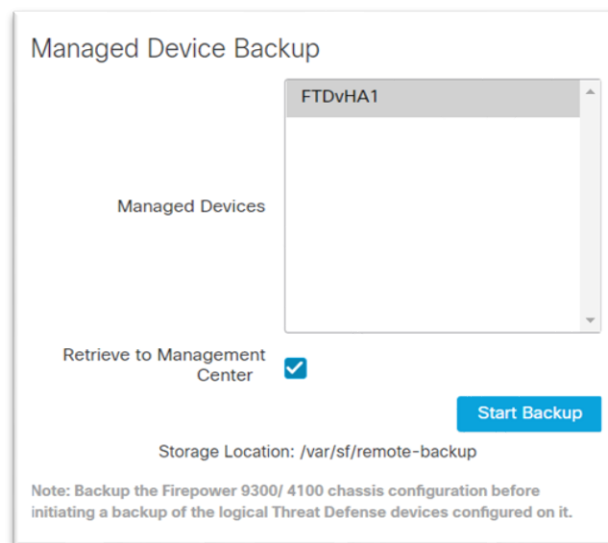
Las tareas programadas aparecen abajo.



Para restaurar una copia de seguridad se debe seleccionar en el menú y pulsar sobre “Restore”. El proceso provocará un reinicio del gestor y la configuración volverá a ser la del momento de la copia.

Para realizar una copia de seguridad de un dispositivo FTD, se debe acceder al menú System->Tools->Backup/Restore y seleccionar “Managed Device Backup”.

Se debe seleccionar el dispositivo o dispositivos a realizar copia y se recomienda chequear la opción “Retrieve to Management Center”, si no la copia se realizará localmente en el mismo dispositivo. La copia se lanza manualmente con “Start Backup”. Se lanzará una tarea en segundo plano.



Managed Device Backup

Managed Devices

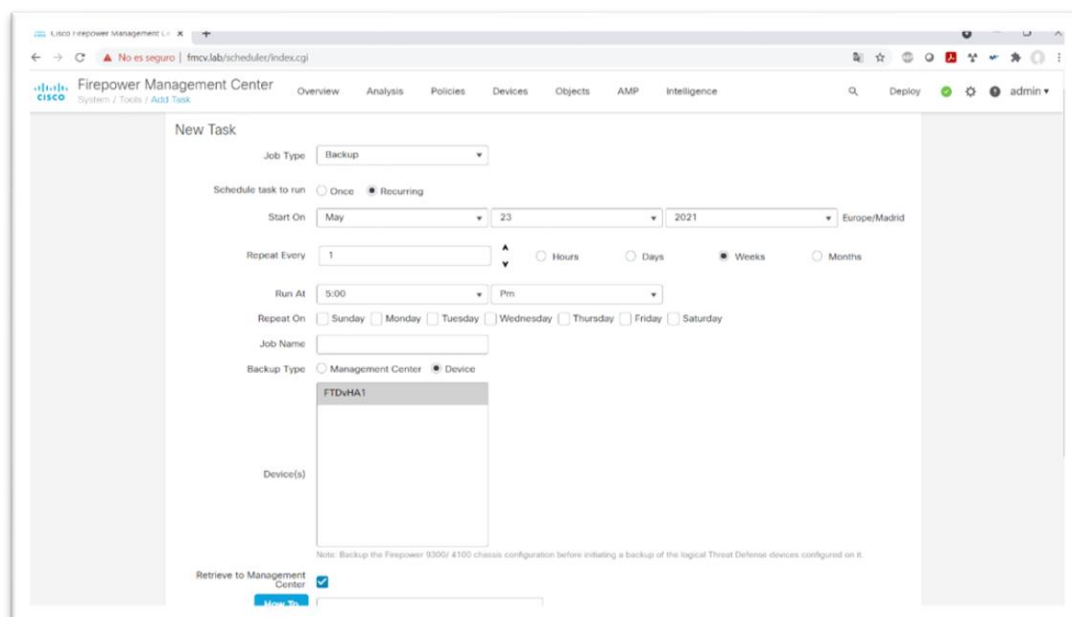
Retrieve to Management Center ☒

Start Backup

Storage Location: /var/sf/remote-backup

Note: Backup the Firepower 9300/ 4100 chassis configuration before initiating a backup of the logical Threat Defense devices configured on it.

La tarea se programa de igual manera que la copia de seguridad del gestor de los firewalls.



New Task

Job Type: Backup

Schedule task to run: ☐ Once ☒ Recurring

Start On: May 23, 2021 Europe/Madrid

Repeat Every: 1 Hours Days Weeks Months

Run At: 5:00 Pm

Repeat On: ☐ Sunday ☐ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday

Job Name:

Backup Type: ☐ Management Center ☒ Device

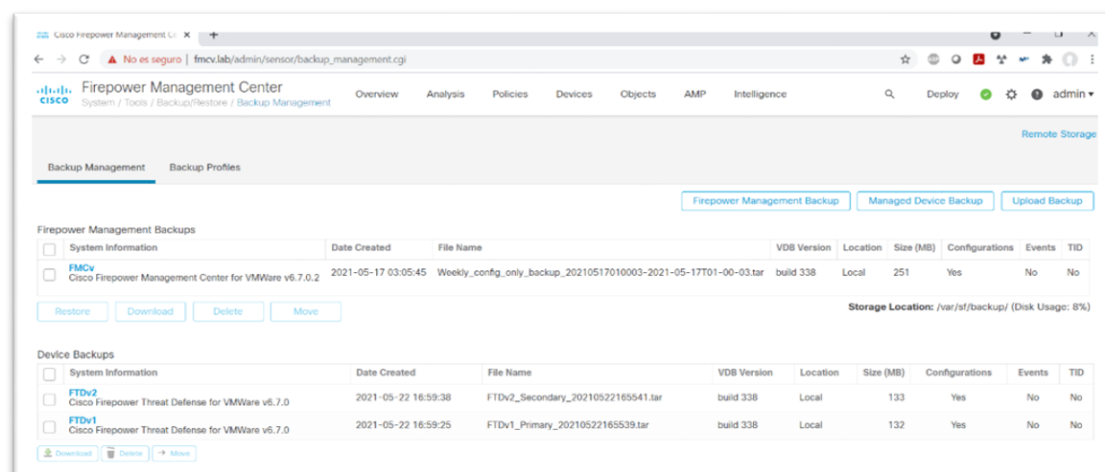
Device(s): FTDvHA1

Note: Backup the Firepower 9300/ 4100 chassis configuration before initiating a backup of the logical Threat Defense devices configured on it.

Retrieve to Management Center ☒

View Log

Realizada la copia, figurará en el menú. Internamente se almacena como “remote-backups” en almacenamiento local o remoto. Cuando se hace una copia de un sistema de alta disponibilidad (failover), se realiza la operación por separado, en 2 ficheros.



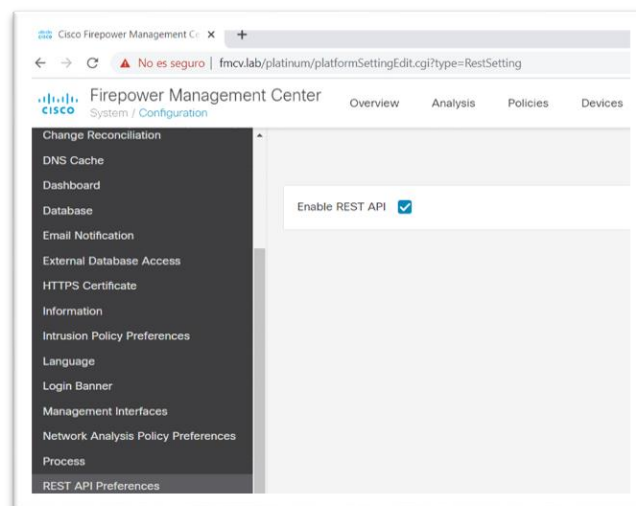
Para restaurar una copia de un dispositivo se debe realizar mediante acceso CLI (SSH) al dispositivo y el comando “restore”. Consultar la guía de Administración de Firepower Management Center para detalles sobre el procedimiento.

13.26 INTERFAZ PROGRAMÁTICA REST API

El sistema Firepower Management Center (FMC) dispone de una interfaz de acceso web programática. La interfaz utiliza REST y objetos JSON para permitir la operación desde cualquier lenguaje que sea capaz de comunicarse vía web con una interfaz REST.

El API REST es muy útil para realizar protocolos o cualquier acción que requiera ser automatizada, incluso disparada desde cualquier otro sistema de control. Por ejemplo, permite la creación de un “botón rojo” que, ante determinados eventos, cierre la comunicación en ciertos puntos o apague los cortafuegos.

La interfaz viene activada por defecto. Si no se va a utilizar, debe ser desactivada. Se realiza desde el menú de Configuration.



Si la interfaz REST se va a utilizar, se debe crear un usuario específico para ello, no usar el “admin”, con los permisos estrictamente necesarios para su funcionamiento.

Se puede explorar el árbol del interfaz REST, a través del “explorer”:

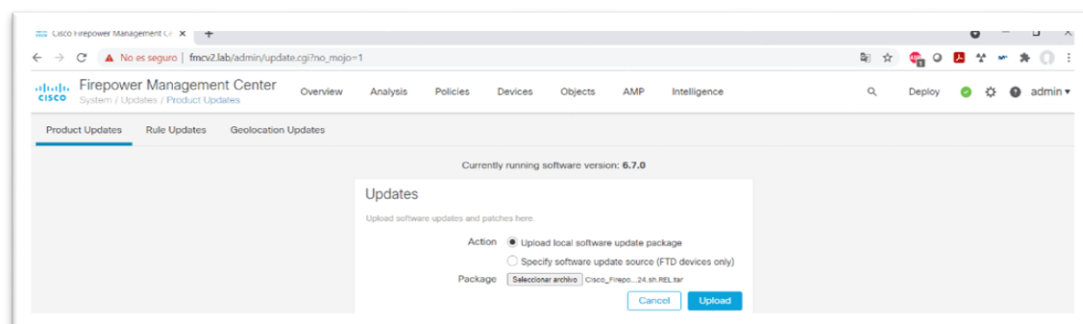
`https://<management_center_IP_or_name>:<https_port>/api/api-explorer`

13.27 ACTUALIZACIÓN DEL SISTEMA FMC

Se recomienda tener actualizado el sistema a las últimas versiones recomendadas por el fabricante dentro de la versión mayor estable.

Para actualizar el sistema FMC se deberá descargarse la imagen desde la web de Cisco, dentro del modelo correspondiente, Firepower Management Center Virtual Appliance si es un virtual. El fichero es un “tar” que no se debe descomprimir.

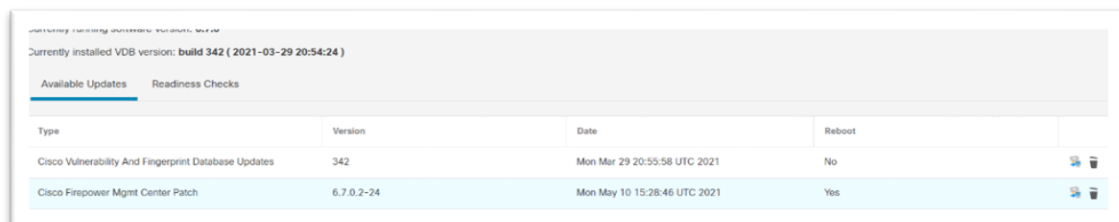
Para realizar la actualización se debe ir al menú System->Updates. Se debería realizar la subida de la imagen a través de la web, “Upload Update” y seleccionando el fichero.



Dando a “Upload” se subirá y se verificará la imagen criptográficamente y el sistema indicará “Upload Succeeded”.

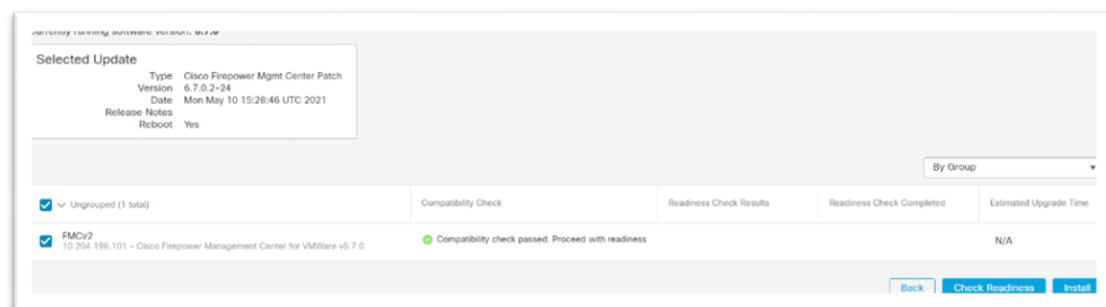
Seleccionando el icono de la caja abierta, se solicita la instalación del paquete. La columna “Reboot” indica que la actualización requiere reinicio del gestor FMC.

Nota: El reinicio del gestor FMC no genera pérdida de servicio en la red. Únicamente el gestor se reinicia, los dispositivos siguen funcionando normalmente. Sí que habrá una pérdida de información de eventos de conexiones y de seguridad que no son reportados al gestor durante su reinicio.



Type	Version	Date	Reboot
Cisco Vulnerability And Fingerprint Database Updates	342	Mon Mar 29 20:55:58 UTC 2021	No
Cisco Firepower Mgmt Center Patch	6.7.0.2-24	Mon May 10 15:28:46 UTC 2021	Yes

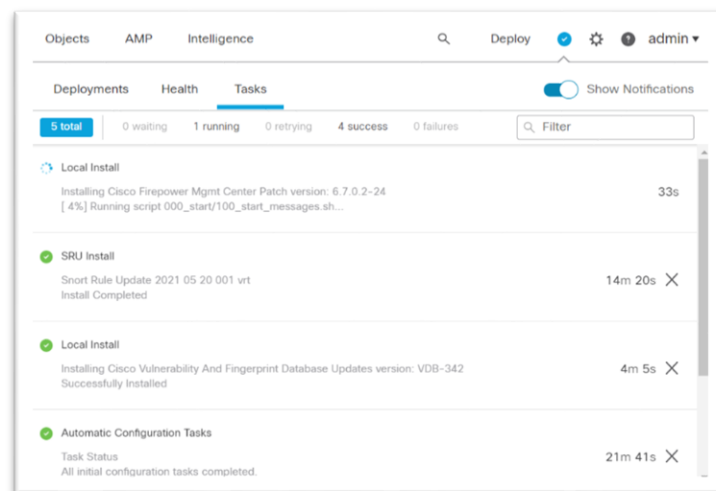
El sistema de actualización detectará qué dispositivos son aplicables, se seleccionará el FMC y se pulsará en “Install”, que lanzará el proceso, avisándonos del reinicio.



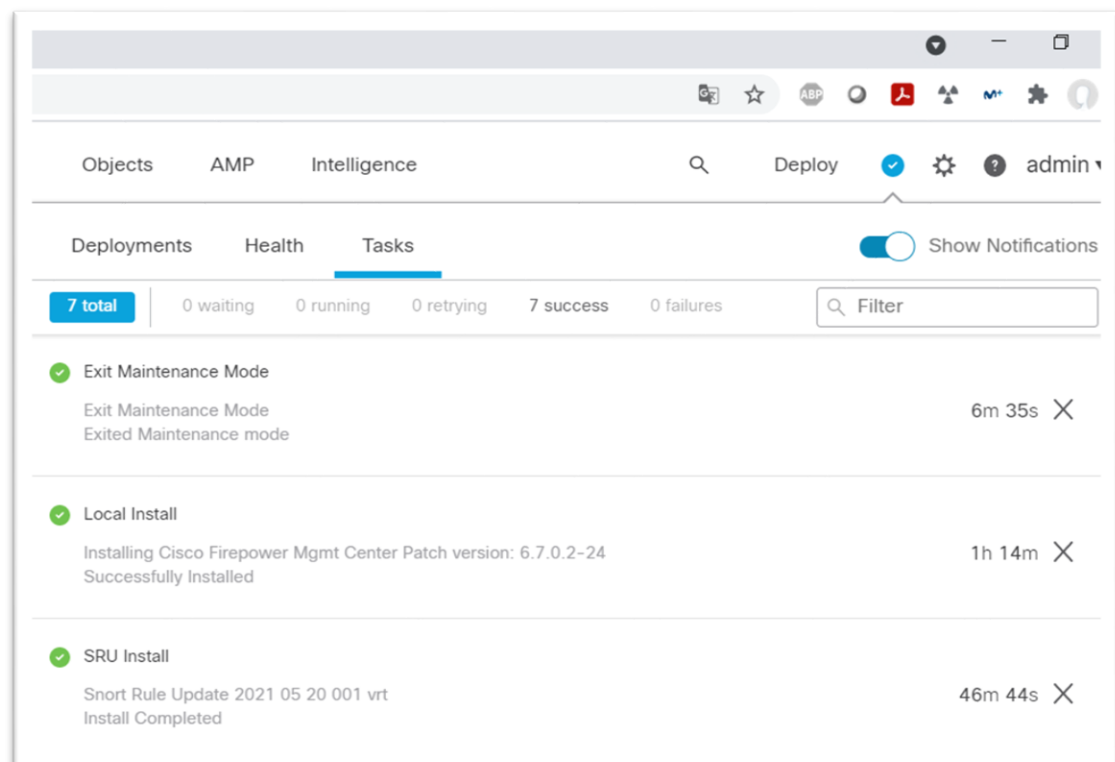
Type	Version	Date	Release Notes	Reboot
Cisco Firepower Mgmt Center Patch	6.7.0.2-24	Mon May 10 15:28:46 UTC 2021	Yes	Yes

Compatibility Check	Readiness Check Results	Readiness Check Completed	Estimated Upgrade Time
Compatibility check passed. Proceed with readiness			N/A

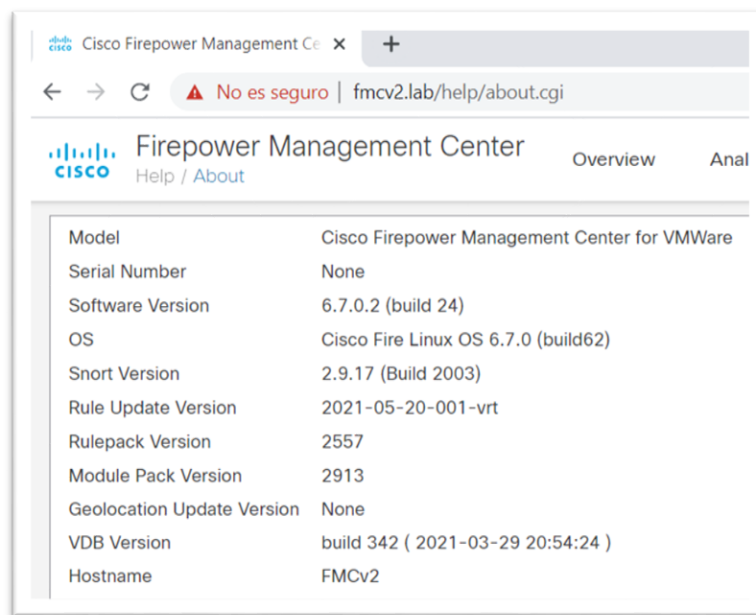
En Tasks puede seguirse la tarea de actualización hasta que el sistema se reinicie.



Una vez reiniciado el servidor debemos comprobar que la tarea se ha terminado con éxito.



Y que la nueva versión es la que se está ejecutando, en Help->About.



13.28 ACTUALIZACIÓN CORTAFUEGOS FTD

Se recomienda tener actualizados los dispositivos a las últimas versiones recomendadas por el fabricante dentro de la versión mayor estable.

Nota: La versión del gestor FMC debe ser siempre igual o superior a la de los dispositivos FTD que gestiona. Se debe comprobar antes de intentar realizar una actualización de FTD.

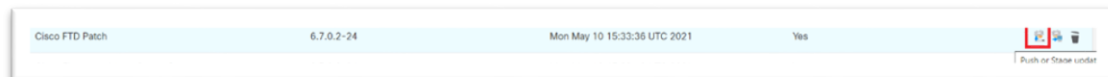
Nota: En el caso de modelos Firepower 4100/9300, la versión FTD a la que se va a actualizar debe ser compatible con el FXOS ejecutándose en el chasis. Se debe comprobar la compatibilidad y actualizar el sistema FXOS previamente de ser necesario.

Para las actualizaciones se deben descargar las imágenes necesarias desde la web de Cisco, dentro del modelo correspondiente y dentro de “Firepower Threat Defense Software”. El fichero es un “tar” que no se debe descomprimir.

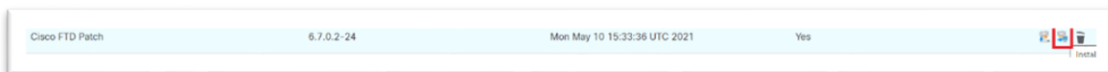
Para realizar la actualización se debe ir al menú System->Updates. Se debería realizar la subida de la imagen a través de la web, “Upload Update” y seleccionando el fichero.

Seleccionando “Upload” se subirá y se verificará la imagen criptográficamente y el sistema indicará “Upload Succeeded”.

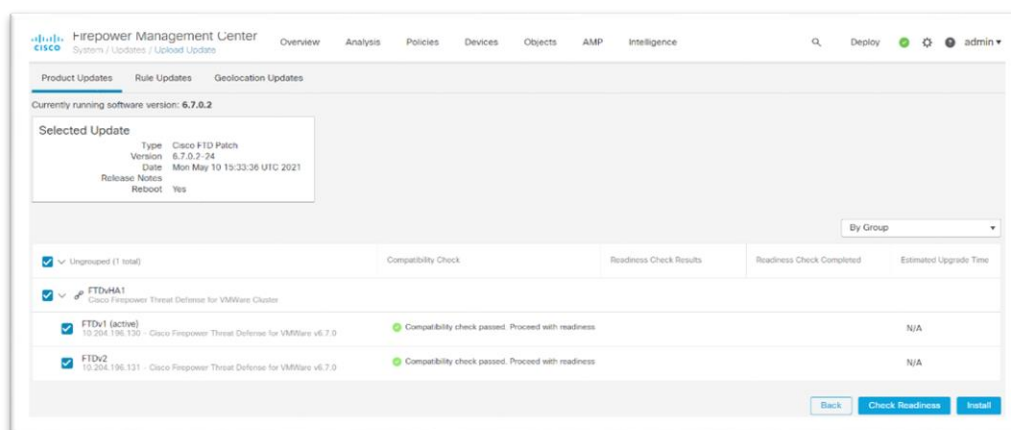
En estas imágenes se puede realizar una “carga previa” de la imagen a los dispositivos, esto puede reducir el tiempo requerido en la ventana de mantenimiento para la actualización, especialmente cuando se van a actualizar muchos equipos a la vez. Se hace con el primer icono “push or Stage Update”.



Para la instalación, seleccionando el icono de la caja abierta, se solicita la instalación del paquete. La columna “Reboot” indica que la actualización requiere reinicio del dispositivo.

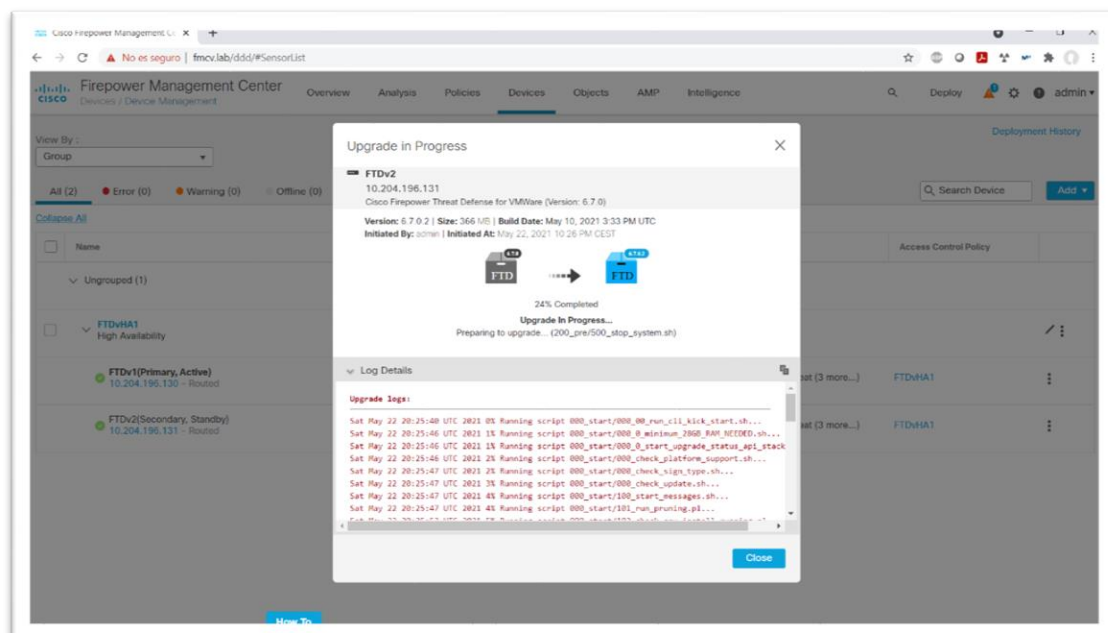
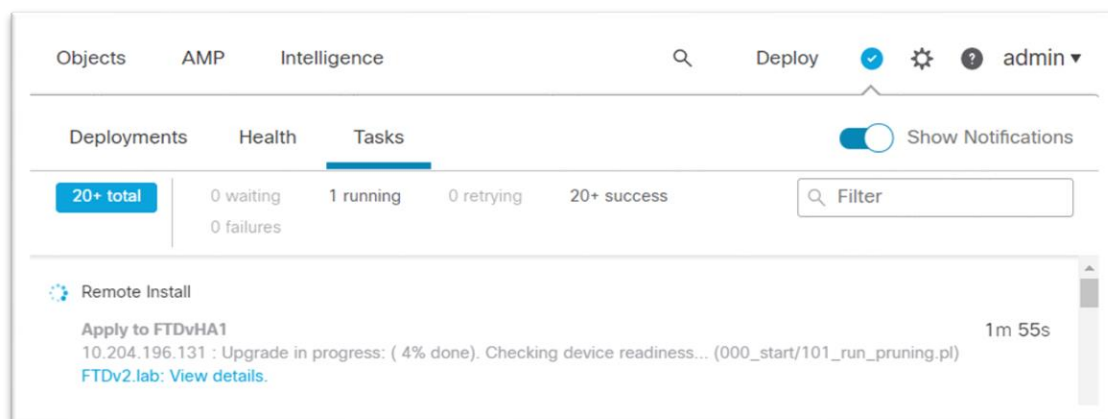


El sistema de actualización detectará a que dispositivos es aplicable la actualización, seleccionar los que interesan y pulsar en “Install”, que lanzará el proceso, avisándonos del reinicio.



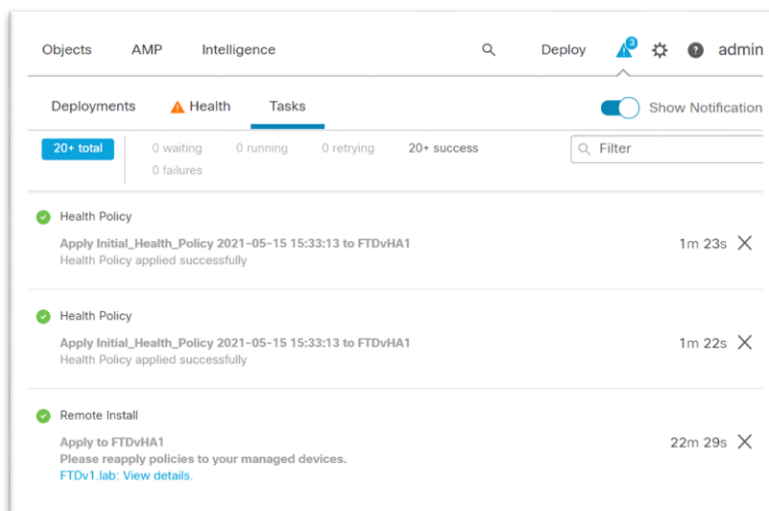
Nota: En dispositivos en alta disponibilidad activo/pasivo (failover) y activo/activo (cluster), la actualización se realiza sobre la agrupación completa. El sistema tiene en cuenta que los equipos están en alta disponibilidad y realiza las actualizaciones de manera secuencial uno por uno, empezando por el pasivo en el caso de “failover”. La pérdida de servicio, por lo tanto, será inapreciable o inexistente. Aun así, se recomienda realizar las actualizaciones en una ventana de mantenimiento con poco tráfico.

En Tasks puede seguirse la tarea de actualización. Permitiendo acceder a una página de detalles donde puede verse el progreso, incluyendo logs.



Una vez reiniciado el cortafuegos debemos comprobar que la tarea se ha terminado con éxito. Normalmente el proceso termina pidiendo un “Deploy”. En el caso de equipos en alta disponibilidad activo/pasivo (failover), se debe comprobar que el

cortafuegos activo es el deseado. Si no es así, se debe proceder a una conmutación activo<->pasivo, en el menú Device->Device Management.



También hay que comprobar que la nueva versión es la que se está ejecutando, en Device->Device Management.

☐	▼ FTDvHA1 High Availability		
▲	FTDv1(Primary, Standby) 10.204.196.130 - Routed	FTD for VMWare	6.7.0.2
▲	FTDv2(Secondary, Active) 10.204.196.131 - Routed	FTD for VMWare	6.7.0.2

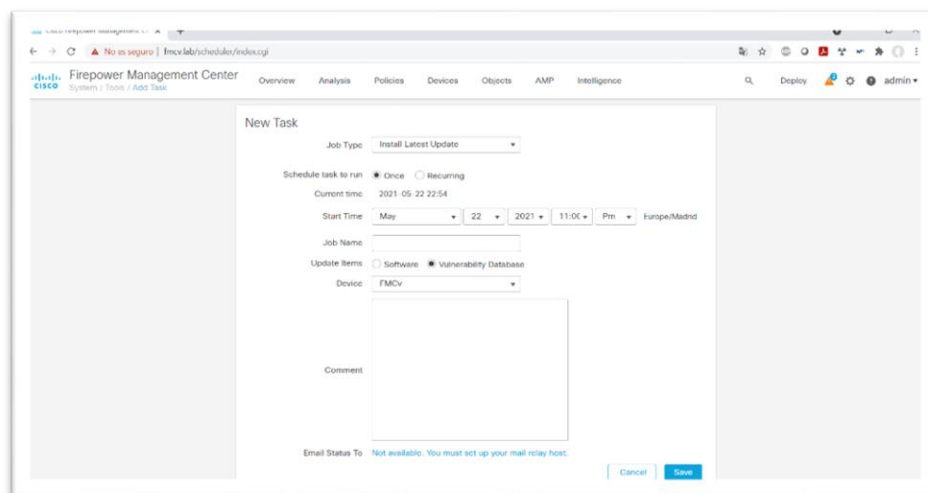
13.29 ACTUALIZACIÓN VULNERABILITY DATABASE (VDB)

La base de datos de vulnerabilidades es compilada por Talos y distribuida a través de la web de soporte.

Se puede instalar manualmente, descargando su última versión desde la web de Cisco, por el modelo de FMC y “Firepower SRU-VDB-GeoDB Content Updates” – VDB.

Una vez descargado, se puede subir mediante System->Updates, e instalar como si fuera una actualización de FMC.

La actualización se puede automatizar mediante el uso de tareas programadas. System->Tools->Scheduling.



Consultar la guía de Cisco de administración de Firepower Management Center para conocer con detalle las opciones de actualización de VDB.

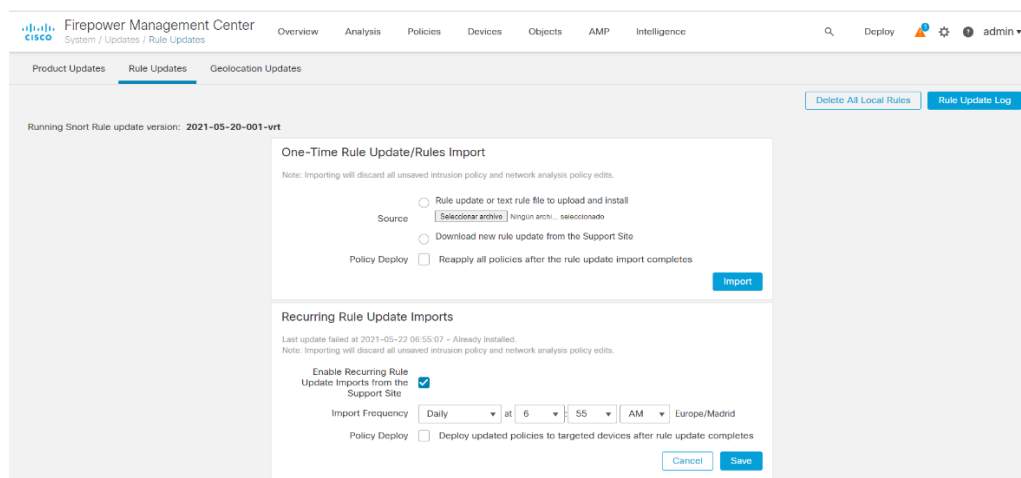
13.30 ACTUALIZACIÓN SNORT RULE UPDATES (SRU)

Las firmas o reglas de Snort deben actualizarse frecuentemente.

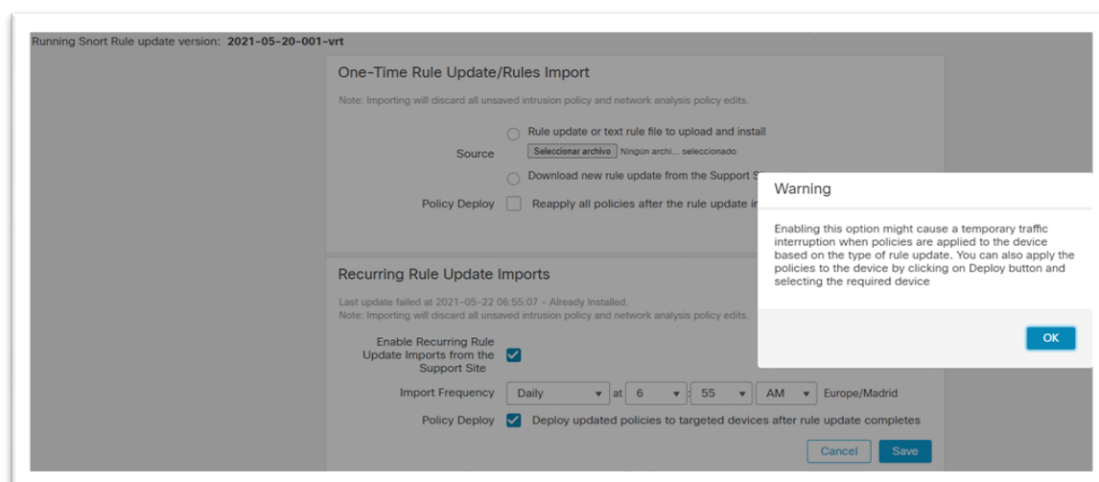
Si se decide usar el sistema NGIPS de Firepower, se recomienda su actualización automática diaria a través de conexión a Internet del FMC.

Las reglas pueden ser actualizadas manualmente (air-gapped) o automáticamente y de manera recurrente, mediante el menú del FMC System->Updates->Rule Updates

Desde el menú podemos subir el fichero desde el PC local. Para ello se deben descargar las firmas de la web de soporte de Cisco, en el modelo de FMC, sección "Firepower SRU-VDB-GeoDB Content Updates - SRU".



La actualización automática y/o periódica requiere conexión a Internet por parte del FMC, se configura en el mismo menú, y se puede habilitar el Deploy automático a dispositivos para actualización de reglas. Sin embargo, esto puede ocasionar algún corte. Aun así, se recomienda realizar el Deploy automático para estar protegidos.



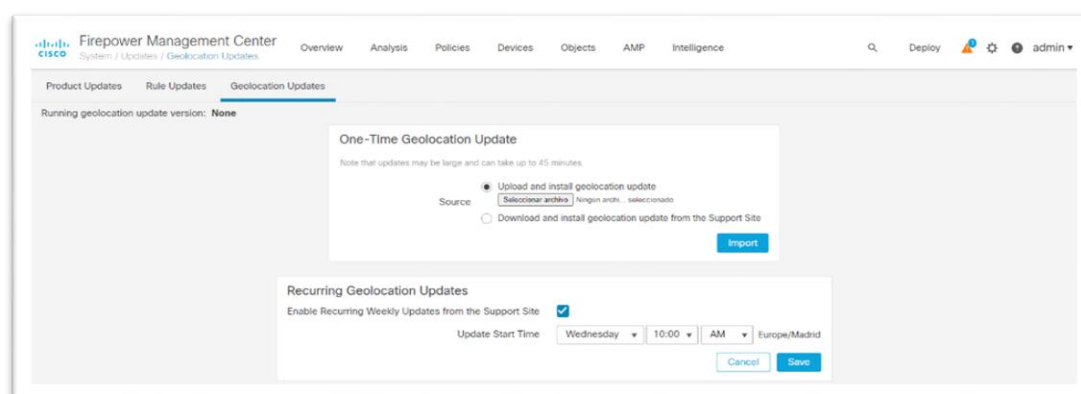
13.31 ACTUALIZACIÓN DE GEOLOCALIZATION

El sistema Firepower utiliza la información de geolocalización tanto para análisis de información como para ciertas reglas y correlación de eventos.

Conviene que esta información este actualizada.

Se puede actualizar manualmente o de manera automática y/o recurrente mediante el menú del FMC System->Updates->Geolocation Updates

Desde el menú podemos subir el fichero desde el PC local. Para ello se deben descargar las firmas de la web de soporte de Cisco, en el modelo de FMC, sección "Firepower SRU-VDB-GeoDB Content Updates - GeoDB".



La actualización automática y/o periódica requiere conexión a Internet por parte del FMC, se configura en el mismo menú y se realiza de manera semanal.

The screenshot shows a configuration window for geolocation updates. The top section, titled "One-Time Geolocation Update", includes a note: "Note that updates may be large and can take up to 45 minutes." Below this, there are two radio buttons under the "Source" label. The first option, "Upload and install geolocation update", is selected and has a "Seleccionar archivo" button next to it, which currently shows "Ningún archi... seleccionado". The second option is "Download and install geolocation update from the Support Site". An "Import" button is located to the right of these options. The bottom section, titled "Recurring Geolocation Updates", has a checkbox "Enable Recurring Weekly Updates from the Support Site" which is checked. Below this, the "Update Start Time" is configured with dropdowns for "Wednesday", "10:00", "AM", and a time zone of "Europe/Madrid". "Cancel" and "Save" buttons are at the bottom right.

14. GESTOR FIREPOWER DEVICE MANAGER (FDM)

El gestor Firepower Device Manager (FDM) es un gestor interno que se encuentra instalado dentro de los dispositivos, sin necesidad de un gestor externo, como el FMC.

Viene instalado por defecto y solo se activa o se desactiva dependiendo de si se quiere usar o se quiere que el equipo lo gestione el otro gestor (externo), el FMC.

El FDM es un gestor muy rápido que tiene la ventaja de no necesitar infraestructura adicional para gestionar los cortafuegos. Aunque ha ido creciendo en funcionalidad, carece, de momento, de algunas funcionalidades, entre las que destacan:

- Solo permite el funcionamiento del cortafuegos en modo rutado.
- El análisis de amenazas y vulnerabilidades es más limitado.
- No permite auto-tuning del IPS.
- No permite correlación ni remediation.

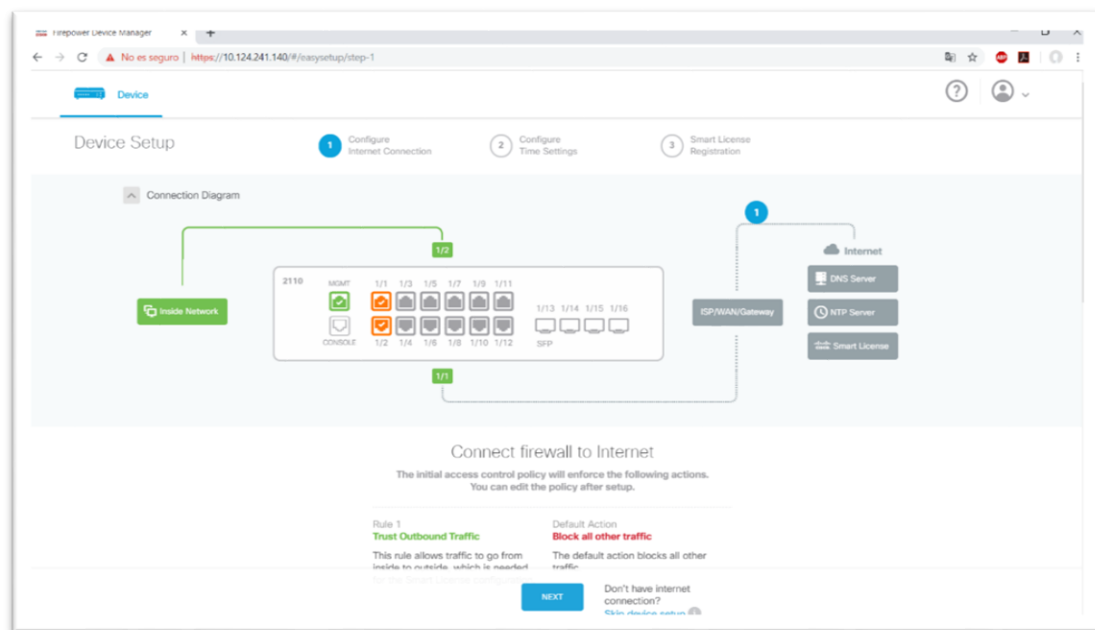
Nota: la utilización del gestor FDM actualmente no está certificado por Common Criteria. Si la red donde se desea integrar el cortafuegos está sujeta a esa restricción se deberá usar el gestor FMC.

Existe un bug registrado en Cisco CSCvp07593 (ENH: FIPS - Common Criteria not supported in FTD managed by FDM) que debe ser consultado por su resolución para conocer si ya ha sido certificado o no.

En esta guía se expone el funcionamiento básico del gestor, sin entrar en las funcionalidades IPS/AMP.

14.1 ASISTENTE DE CONFIGURACIÓN

En la primera conexión al gestor FDM se lanza un asistente de configuración que sirve para realizar rápidamente una configuración básica.



El asistente pedirá la zona horaria (time zone) y la configuración de sincronización horaria (NTP).

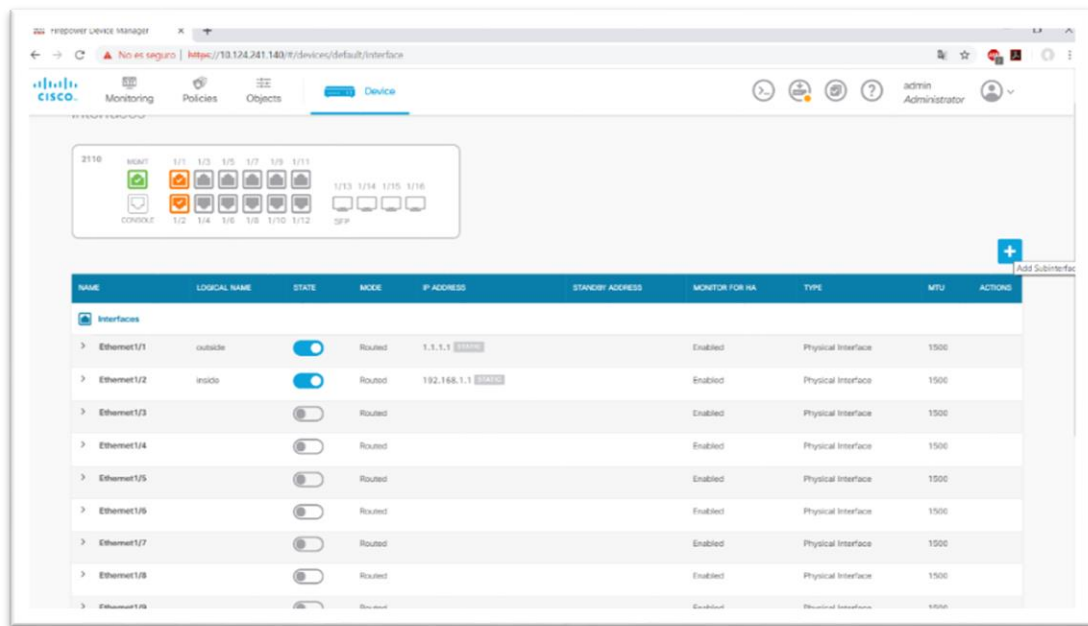
The screenshot shows the 'Time Setting (NTP)' configuration page. At the top, it displays the 'System Time: 12:22:46PM March 17 2019 +01:00'. Below this is a 'Time Zone' dropdown menu set to '(+01:00) Europe/Madrid'. Underneath is an 'NTP Time Server' dropdown menu set to 'Default NTP Time Server', with a small information icon to its right. A 'Server Name' section lists three options: '0.sourcefire.pool.ntp.org', '1.sourcefire.pool.ntp.org', and '2.sourcefire.pool.ntp.org'. At the bottom, there are 'BACK' and 'NEXT' buttons.

También pedirá el registro con la Smart Account, para lo que se requiere acceso a Internet desde el interfaz fuera de banda del cortafuegos.

The screenshot shows the 'Register with Cisco Smart Software Manager' page. It includes a sub-header 'Register with Cisco Smart Software Manager to use the full functionality of this device and to apply subscription licenses.' and a link 'What is smart license?'. There are two main options: a selected radio button for 'Register device with Cisco Smart Software Manager' and an unselected one for 'Start 90-day evaluation period without registration'. The first option has three numbered steps: 1. 'Create or log into your Smart Software Manager account', 2. 'On your assigned virtual account, click on Inventory. Under "General" tab, click on "New Token" to create token.', and 3. 'Copy the token from "Actions" and paste it here.' Below these steps is a large text input field. The second option has a note: 'Please make sure you register with Cisco before the evaluation period ends. Otherwise you will not be able to make any changes to the device configuration.' At the bottom, there are 'BACK' and 'FINISH' buttons.

14.2 GESTIÓN DE INTERFACES

En la página de gestión del dispositivo "Device", se visualiza gráficamente el cortafuegos, con sus interfaces y conexiones. Se pueden crear Subinterfaces adicionales.



Las subinterfaces gestionan VLAN en enlaces 802.1q

Add Subinterface

Parent Interface

Ethernet1/3

Subinterface Name

dmz

Status

☒

Most features work with named interfaces only, although some require unnamed interfaces.

Description

VLAN ID

17

Subinterface ID

17

1 - 4094

IPv4 Address

IPv6 Address

Advanced Options

Type

Static

IP Address and Subnet Mask

192.168.50.1 / 255.255.255.0

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

e.g. 192.168.5.16

CANCEL

OK

Desde el mismo menú también se pueden gestionar las interfaces físicas.

The screenshot shows the 'Edit Physical Interface' configuration window. At the top, the 'Interface Name' is 'outside', the 'Mode' is 'Routed', and the 'Status' is enabled. Below this is a 'Description' field. The 'IPv4 Address' tab is selected, showing a 'Type' of 'Static'. The 'IP Address and Subnet Mask' is '1.1.1.1 / 255.255.255.0', with a hint 'e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0'. The 'Standby IP Address and Subnet Mask' field is empty, with a hint 'e.g. 192.168.5.16'. At the bottom are 'CANCEL' and 'OK' buttons.

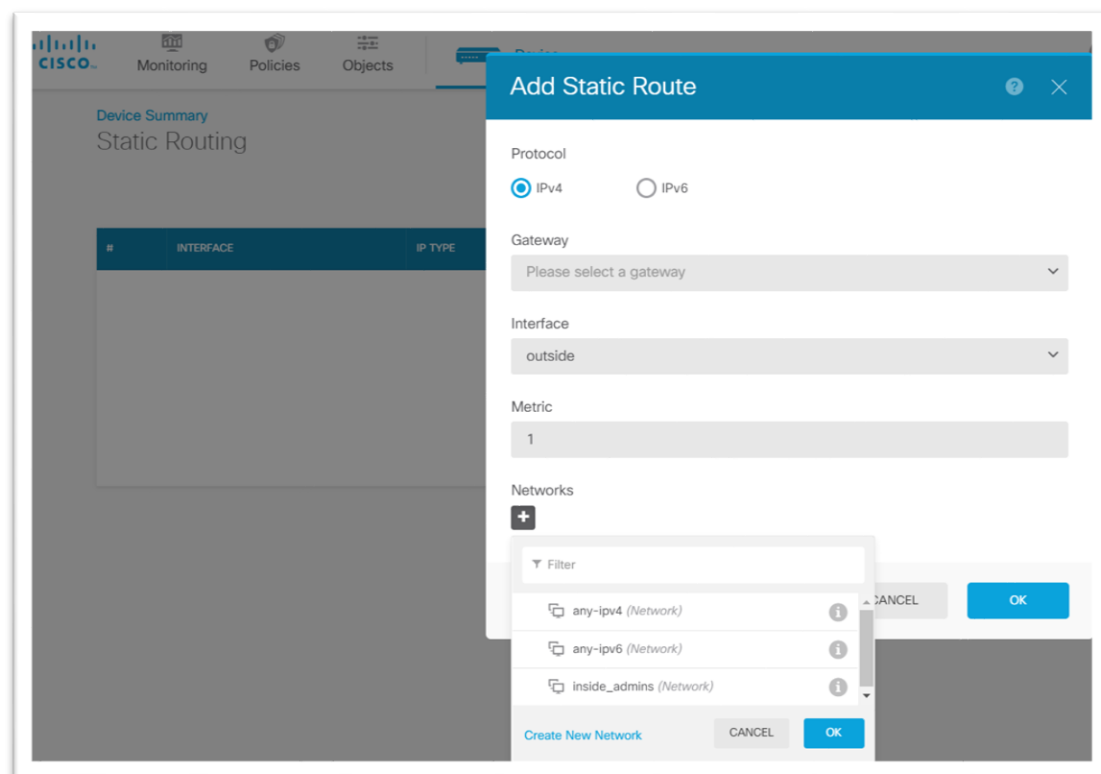
14.3 ZONAS DE SEGURIDAD

En FDM las zonas de seguridad se pueden gestionar desde la sección correspondiente dentro de Objects.

The screenshot shows the 'Add Security Zone' configuration window. The 'Name' is 'dmz', and the 'Description' is empty. The 'Mode' is 'Routed' (selected) and 'Passive'. The 'Interfaces' section shows a list of interfaces: 'unnamed (Ethernet1/14)', 'unnamed (Ethernet1/15)', 'unnamed (Ethernet1/16)', 'unnamed (Ethernet1/3)', and 'dmz (Ethernet1/3.17)'. The 'dmz (Ethernet1/3.17)' interface is selected. At the bottom, it says '1 item(s) selected' and has 'Create New Subinterface', 'CANCEL', and 'OK' buttons.

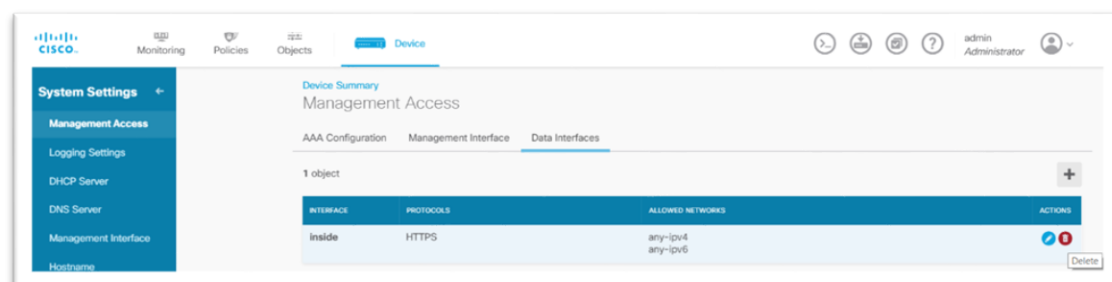
14.4 ROUTING

En la parte de gestión del dispositivo (Device) también se puede configurar el routing, principalmente rutas estáticas.



14.5 FILTRO DE GESTIÓN DE PLANO DE DATOS

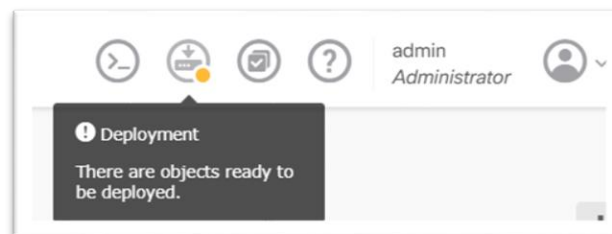
Por defecto está permitida la gestión desde el interfaz inside, esto se debe eliminar. Toda la gestión debe ser realizada por el interfaz de gestión fuera de banda y ese enlace debe ser considerado Red de Gestión.



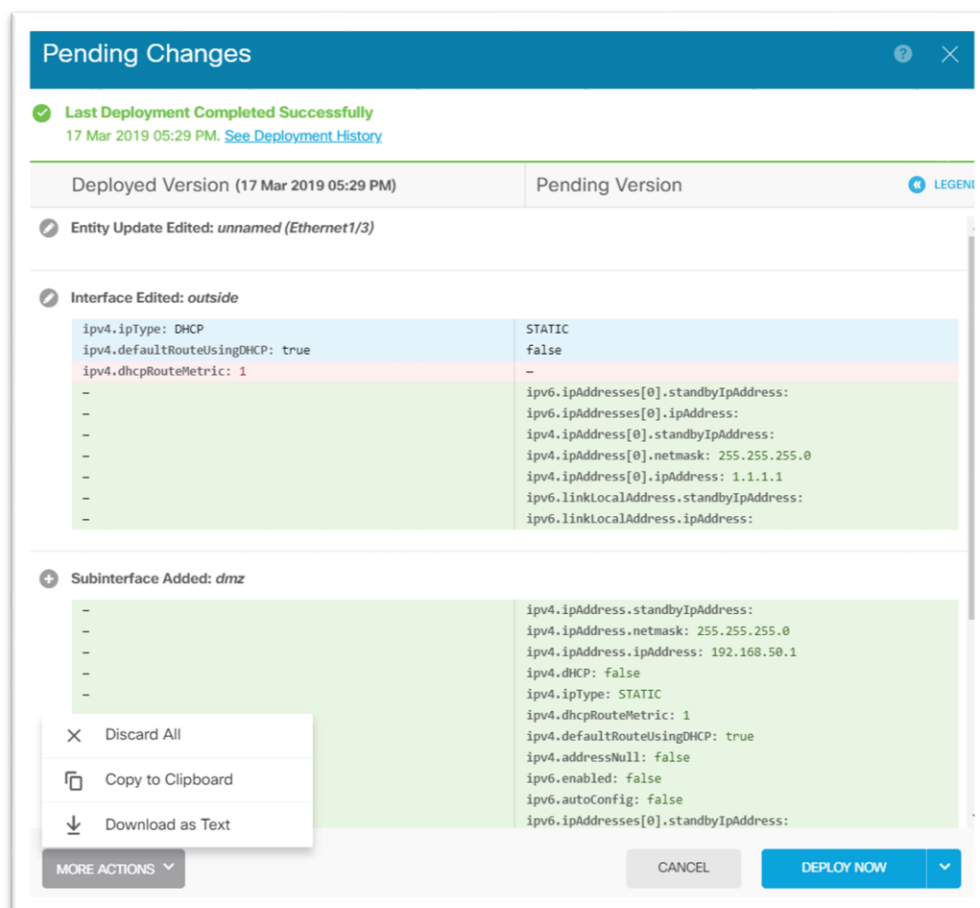
14.6 DEPLOY/TASKS

Igual que con el gestor FMC, cualquier cambio realizado se realiza solo en el gestor, si se quieren que se aplique al dispositivo hay que realizar un Deploy.

El icono avisa cuando hay cambios sin aplicar y se necesita realizar un Deploy.



La información de los Deploys es mucho más detallada que en FMC.



Las tareas en segundo plano, igual que en el FMC, aparecen como Tasks.

Task List					
3 total 1 running 2 completed 0 failures Delete all finished tasks					
Name	Start Time	End Time	Status	Actions	
User (admin) Triggered Deployment	18 Mar 2019 12:54 PM		Deployment Task: User (admin) Triggered Deployment Started		
Export Config	17 Mar 2019 05:30 PM	17 Mar 2019 05:30 PM	The export config file successfully completed		
User (admin) Triggered Deployment	17 Mar 2019 05:26 PM	17 Mar 2019 05:29 PM	Deployment Task: User (admin) Triggered Deployment Completed in 2m 12.57s		

14.7 POLÍTICA DE ACCESO – ACCESS CONTROL POLICY (ACP)

En Políticas podemos acceder a la política de acceso donde se definen las reglas. Las acciones y opciones son algo más limitadas.

Add Access Rule

Order	Title	Action
2	Es Unico	Allow

Source/Destination

Applications

URLs

Users

SOURCE

Zones

+

Networks

+

Ports

+

ANY

ANY

ANY

DESTINATION

Zones

+

Networks

+

Ports

+

ANY

ANY

ANY

Add Access Rule

Order	Title	Action
2	Es Unico	Allow

Source/Destination

Applications

URLs

Users

Intrusion Policy

File policy

Logging

SOURCE

Zones

+

Networks

+

Ports

+

inside_zone

inside_admins

TCP high ports

DESTINATION

Zones

+

Networks

+

Ports/Protocols

+

outside_zone

ANY

ANY

14.8 FILTRO DE APLICACIONES - AVC

Dentro de las reglas de la política de acceso, una de las pestañas en Applications, que es donde se pueden seleccionar, individualmente y por categorías.

Filter Applications RESET FILTER

Risks
Any

Business Relevance
Any

Types
Any

Categories **Any selected**
Search Categories
email
social networking
remote file storage
business

Tags **Any selected**
Search Tags
displays ads
not work related
share media
high bandwidth
file sharing/transfer

Filter the list of applications 2 Applications

▼ kerberos

Application	Description
All applications that match the filters (2)	
Kerberos	Kerberos is a network authentication protocol designed to provide stron...
Kerberos Administration	Kerberos is a network authentication protocol.

14.9 LOG DE CONEXIONES – SYSLOG

La última opción de una regla de política de acceso permite realizar logging al comienzo y al final de la conexión.

Add Access Rule

Order: 2 Title: Es Unico Action: Allow

Source/Destination Applications URLs Users Intrusion Policy File policy **Logging**

SELECT LOG ACTION

☐ At Beginning and End of Connection

☒ At End of Connection

☐ No Connection Logging

SEND CONNECTION EVENTS TO:

Select a Syslog Alert Configuration...

FILE EVENTS

☐ Log Files

14.10 POLÍTICA DE NAT

Las traducciones de red se configuran en la sección de Políticas del FDM.

Existen 2 tipos de reglas de NAT, automáticas y manuales. Las automáticas requieren menos configuración, pero son menos flexibles y ofrecen menos posibilidades.

Existe un orden de precedencia de reglas, según el tipo (auto/manual) y donde insertemos las manuales (before/after). El orden es:

- Manual Before
- Auto
- Manual After

En esta guía vamos a utilizar reglas Manual, ya que son las que ofrecen mayor control. Por lo general se usan reglas Before.

Nota Importante: las reglas de NAT se evalúan de arriba abajo, donde la primera coincidencia (match) que se encuentre será la regla utilizada. Por lo tanto, la política se debe configurar con reglas más específicas en la parte alta y genéricas en la parte baja.

En general todas las traducciones (NAT) deben ser evitadas, y solo usarse cuando sea requerido, como conexiones a Internet.

La única razón, desde el punto de vista de seguridad, para su uso es el mismo que desaconseja su uso. Los NAT “esconden” la verdadera IP origen o destino, y eso puede resultar beneficioso o perjudicial dependiendo del lado en el que estemos mirando.

14.10.1 NAT DINÁMICO

Estos NAT son de “salida”. Agrupan un conjunto de direcciones IP en 1 sola IP mediante traducción de puertos (NAT/PAT). Es el equivalente en Cisco IOS de NAT overload.

Un ejemplo típico de este NAT es una conexión a Internet. Creamos una regla de NAT dinámico, desde la zona de Usuarios (entrada) a la zona de Internet (Salida).

14.10.2 NAT ESTÁTICO

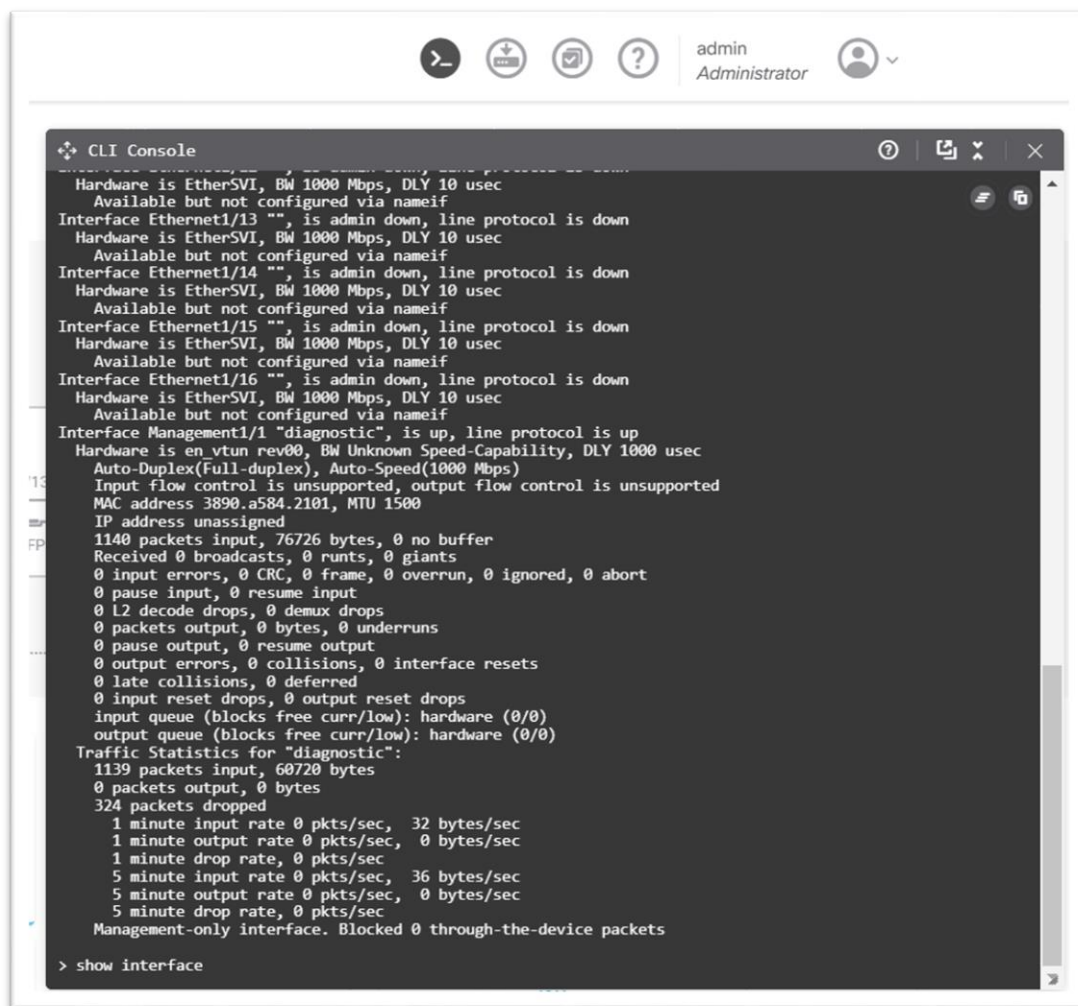
El uso común de estos NAT es realizar una traducción 1:1 bien de IP a IP o de puerto. En el caso de Internet es la publicación de un puerto de una IP privada de nuestra red.

Como norma general se recomienda que los NAT estáticos figuren por encima de los dinámicos.

Nota Importante: Desde el punto de vista de la política de control acceso (ACP), las direcciones IP son las reales, no las de NAT. Es decir, si queremos hacer una regla que permita el tráfico entrante desde Internet a un servidor que hemos publicado, se debe usar como destino la IP Real del servidor (Ej. 10.30.30.10), y no la publicación de la IP del interfaz del cortafuegos (Ej. 185.43.182.83).

14.11 CONSOLA CLI INTEGRADA

Desde el FDM se puede abrir directamente una consola al cortafuegos. Esta opción es extremadamente útil para depuraciones y chequeos rápidos, como “pings”, visualizar el estado exacto de las interfaces, etc.

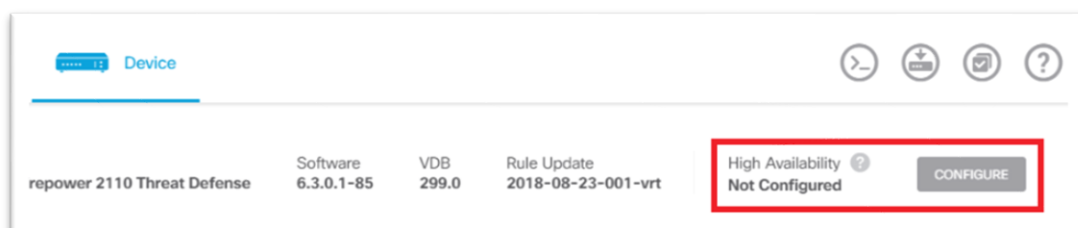


14.12 ALTA DISPONIBILIDAD ACTIVO/PASIVO – FAILOVER

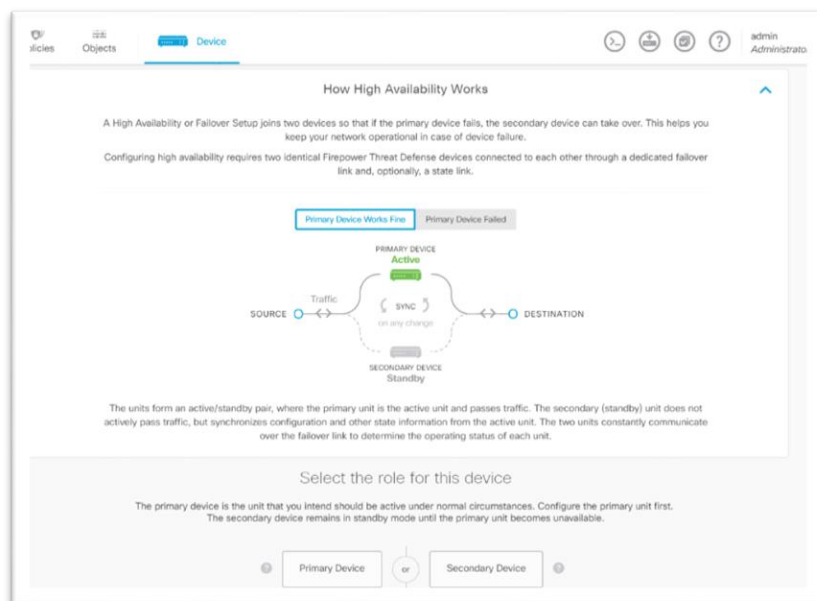
Desde la versión 6.3 es posible gestionar 2 cortafuegos en alta disponibilidad en modo failover con FDM.

Los equipos deben ser el mismo modelo exacto, con los mismas interfaces y versión.

En la parte de gestión del dispositivo aparece el apartado de alta disponibilidad.



Al configurar se inicia un asistente muy visual que hace de guía.



La alta disponibilidad en modo failover requiere 1 o 2 conexiones entre los cortafuegos. Se recomienda usar cables directos, sin pasar por conmutadores. El “failover link” mantiene el estado y replica las configuraciones. El “Stateful failover link” replica las conexiones. Pueden usarse 1 única interfaz para ambos, dependerá del dimensionamiento y despliegue específico de la integración.

Primary Device or **Secondary Device**

I have configuration of peer device in clipboard **PASTE FROM CLIPBOARD**

FAILOVER LINK

Physical Interface: Ethernet1/12

Type: ☒ IPv4 ☐ IPv6

Primary IP: 10.110.10.1 (e.g. 192.168.10.1)

Secondary IP: 10.110.10.2 (e.g. 192.168.10.2)

Netmask: 255.255.255.252 (e.g. 255.255.255.0 or 24)

STATEFUL FAILOVER LINK ☒ Use the same interface as the Failover Link

Physical Interface: Ethernet1/12

Type: ☒ IPv4 ☐ IPv6

Primary IP: 10.110.10.1 (e.g. 192.168.11.1)

Secondary IP: 10.110.10.2 (e.g. 192.168.11.2)

Netmask: 255.255.255.252 (e.g. 255.255.255.0 or 24)

IPSec Encryption Key (optional)

For security purposes, the encryption key will not be included in the configuration copied to the clipboard when you activate HA. You will need to manually enter the key when you configure HA on the peer device.

IMPORTANT

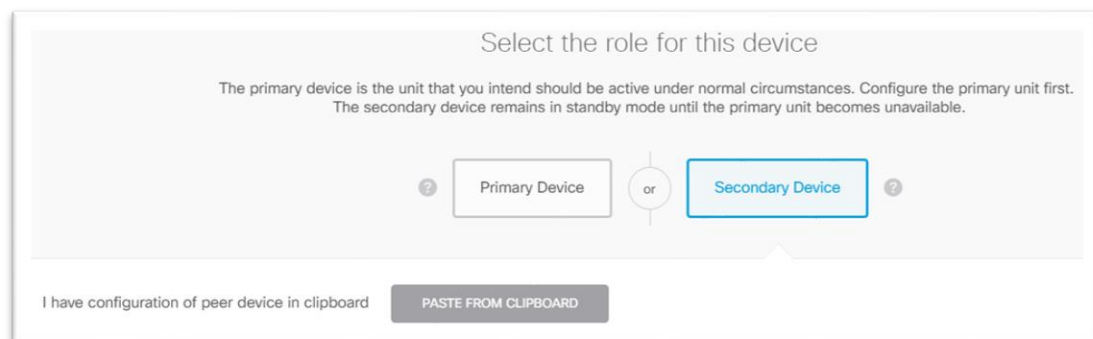
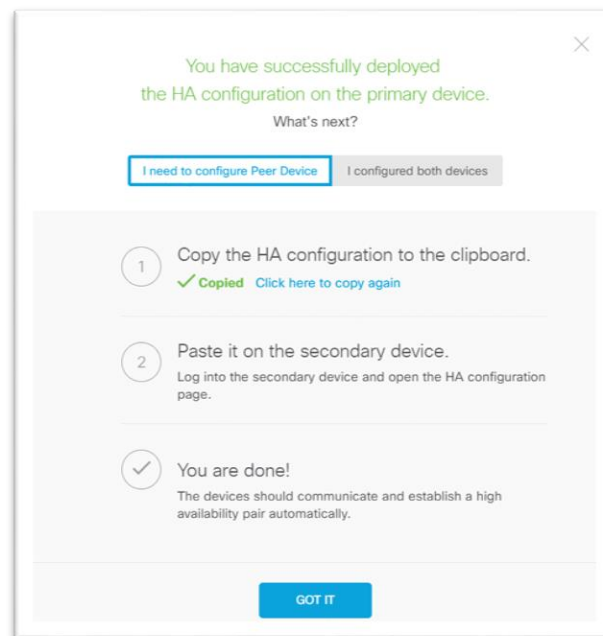
If you configure an IPSec encryption key with inconsistent settings for export controlled features, both devices will become active after you activate HA. [Learn More](#)

When you click Activate HA, these settings are automatically deployed to the device. The deployment might restart inspection engines, which can result in the momentary traffic loss. It might take a few minutes for deployment to finish.

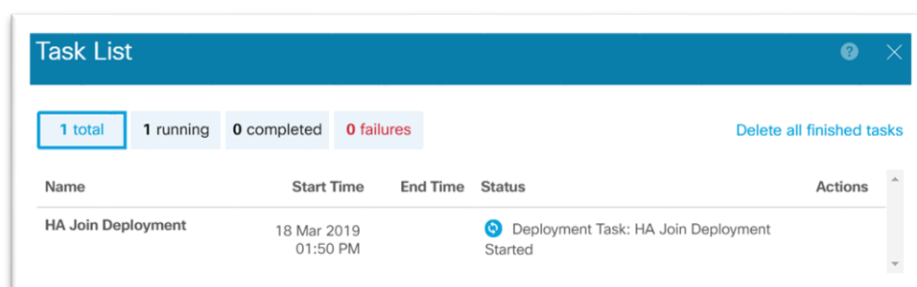
Information is copied to the clipboard when deployment is done. You must allow the browser to access your clipboard for the copy to be successful.

ACTIVATE HA

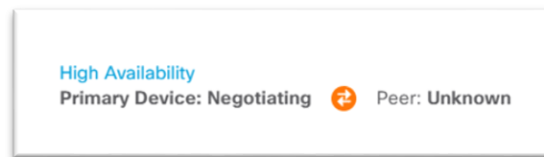
Una vez terminada la configuración del primario, se realiza la del secundario. En este caso la configuración es simplificada mediante un “copia y pega” de la configuración.



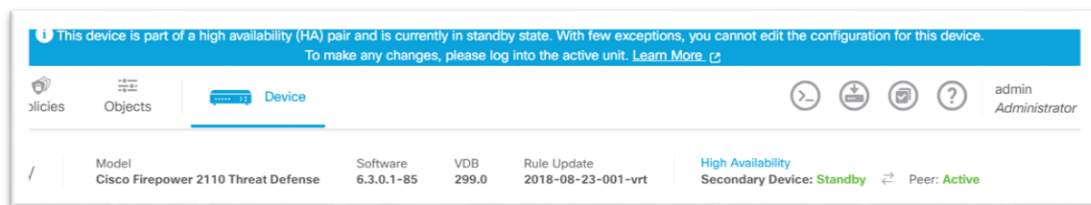
Una vez terminada la configuración global de alta disponibilidad, se lanza una tarea en segundo plano.



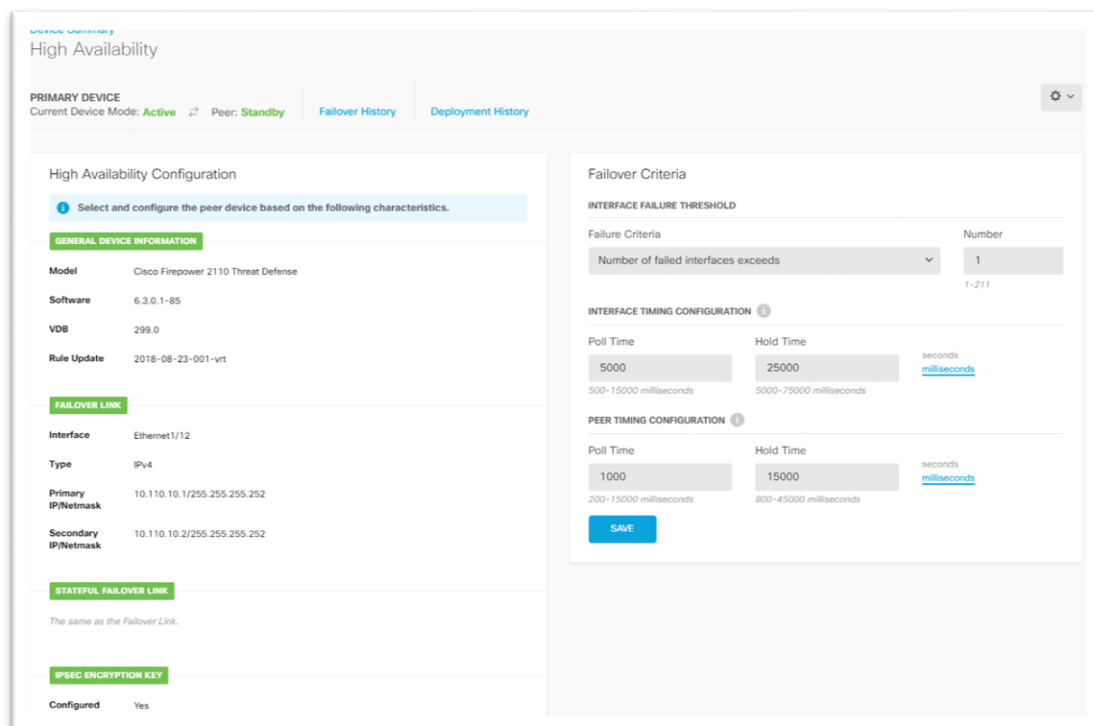
En la página de gestión del dispositivo también se muestra el estado.



Una vez formada la alta disponibilidad, solo se podrá modificar la configuración desde el equipo activo. Si se accede al secundario se puede visualizar, pero no configurar.



Una vez formada la alta disponibilidad, en su configuración podemos establecer los valores de fallo y conmutación.



Utilizando el CLI integrado se puede ver el detalle del estado de la alta disponibilidad failover.

```

slot 0: FPR-2110 hw/sw rev (49.46/9.10(1)8) status (Unknown/Unknown)
  Interface outside (0.0.0.0): Unknown (Waiting)
  Interface inside (0.0.0.0): Unknown (Waiting)
  Interface diagnostic (0.0.0.0): Unknown (Waiting)
  Interface dmz (0.0.0.0): Unknown (Waiting)
slot 1: snort rev (1.0) status (up)
slot 2: diskstatus rev (1.0) status (up)

Stateful Failover Logical Update Statistics
Link : failover-link Ethernet1/12 (Failed)
Stateful Obj      xmit      xerr      rcv      rerr
General           250         0        249         0
sys cmd           249         0        249         0
up time           0         0         0         0
RPC services      0         0         0         0
TCP conn          0         0         0         0
UDP conn          0         0         0         0
ARP tbl           0         0         0         0
Xlate Timeout     0         0         0         0
IPv6 ND tbl       0         0         0         0
VPN IKEv1 SA      0         0         0         0
VPN IKEv1 P2      0         0         0         0
VPN IKEv2 SA      0         0         0         0
VPN IKEv2 P2      0         0         0         0
VPN CTCP upd      0         0         0         0
VPN SDI upd       0         0         0         0
VPN DHCP upd      0         0         0         0
SIP Session       0         0         0         0
SIP Tx            0         0         0         0
SIP Pinhole       0         0         0         0
Route Session     0         0         0         0
Router ID         0         0         0         0
User-Identity     1         0         0         0
CTS SGTNAME       0         0         0         0
CTS PAC           0         0         0         0
TrustSec-SXP      0         0         0         0
IPv6 Route        0         0         0         0
STS Table         0         0         0         0
Umbrella Device-ID 0         0         0         0

Logical Update Queue Information
Cur  Max  Total
Recv Q:  0  10  249
Xmit Q:  0  11 2233

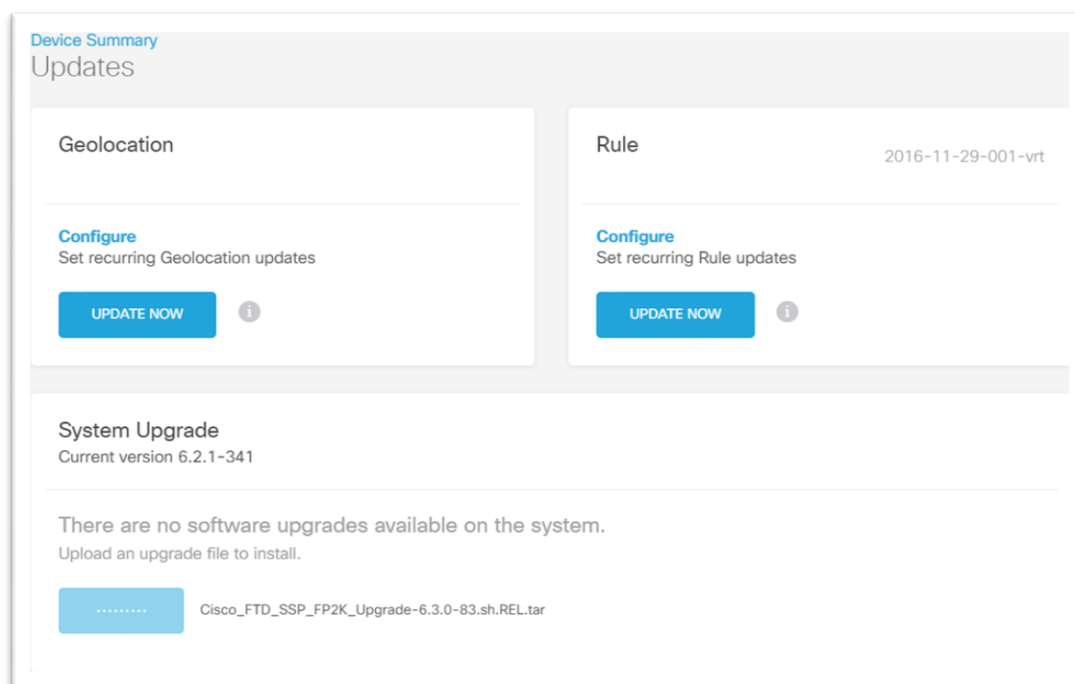
> show failover

```

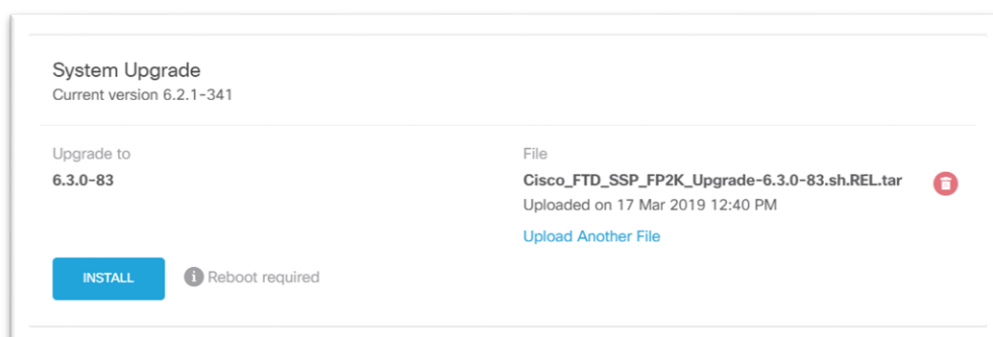
14.13 ACTUALIZACIÓN SISTEMA FTD Y FDM

Dentro de la gestión del dispositivo se encuentra el apartado de actualizaciones (Upgrades). La actualización del cortafuegos FTD implica la actualización también del gestor FDM, ya que están integrados.

Se realiza la subida del fichero vía web.



Normalmente indicará que requiere un reinicio. Se aplica pulsando el botón de Install.



14.14 ACTUALIZACIÓN DE GEOLOCATION, RULE, VDB, SI

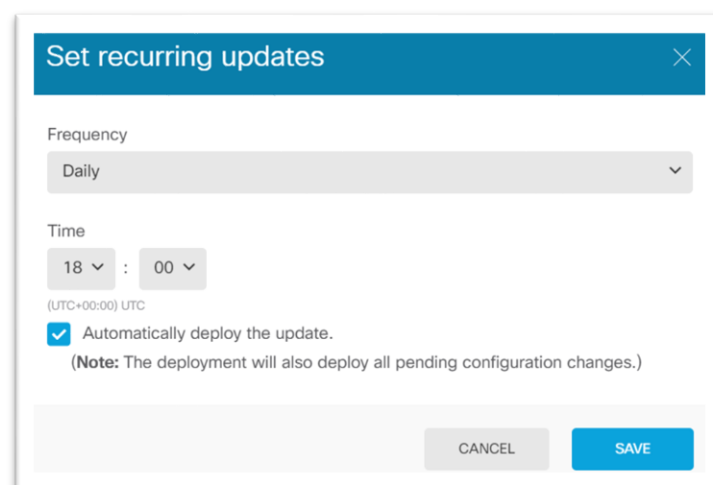
Se recomienda la configuración de actualizaciones recurrentes de los diferentes elementos del cortafuegos:

- **Geolocation**
Proporciona información sobre el origen de direcciones IP.
- **Rule**
Son las Snort Rules. Se deben mantener actualizadas para la correcta funcionalidad del sistema NGIPS.

- VDB
Base de datos de vulnerabilidades.
- Security Intelligence Feeds
Base de datos proveída por Cisco TALOS sobre reputaciones de direcciones IP, URL, hosts.

La configuración de las actualizaciones se realiza desde el apartado de dispositivo, en el mismo menú de actualización del sistema FTD/FDM.

Algunas actualizaciones deben realizar un Deploy para aplicarse. Se recomienda activar el Deploy automático del menú.



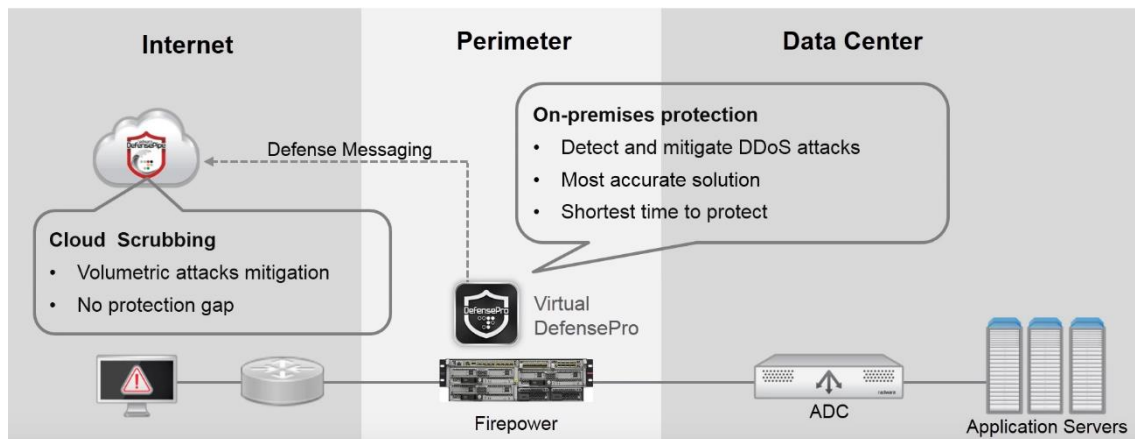
15. PROTECCIÓN DE DENEGACIÓN DE SERVICIO - DDOS

Los cortafuegos Firepower 4100/9300 soportan la integración en el mismo dispositivo del software de mitigación de ataques de denegación de servicio “Radware’s Virtual DefensePro (vDP)”.

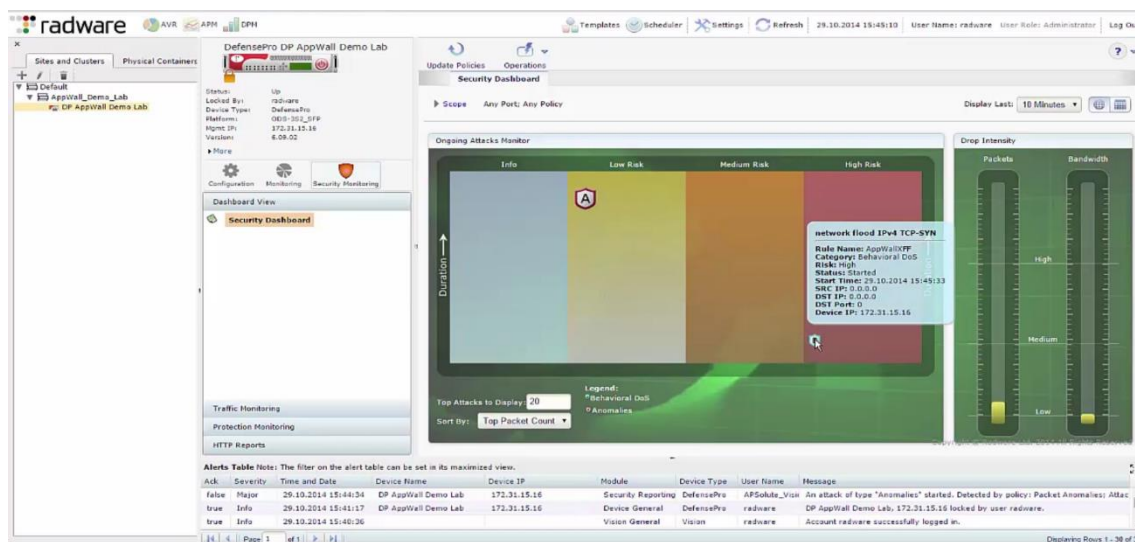
Esta funcionalidad necesita de licencia específica suministrada por Cisco.

Esta imagen es proveída y soportada por Cisco e instalada en los modelos de cortafuegos soportados en la modalidad de encadenamiento de servicio “Service-Chaininig”. Esto sitúa al sistema vDP en la punta de entrada, haciendo cadena, entre Internet y el cortafuegos FTD.

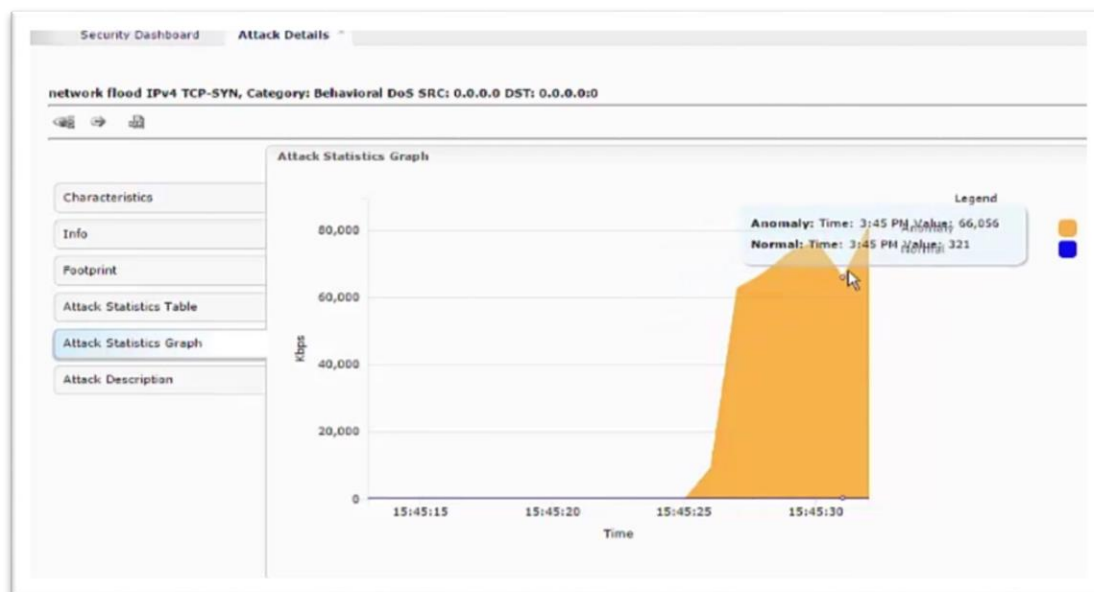
El vDP actúa como detector de ataques de denegación de servicio y filtra los intentos de conexión de los atacantes antes de que lleguen a la red. Para ello, el vDP cuenta con conexión a la nube de Radware, con acceso a su base de datos que le permite disponer de información en tiempo real de atacantes.



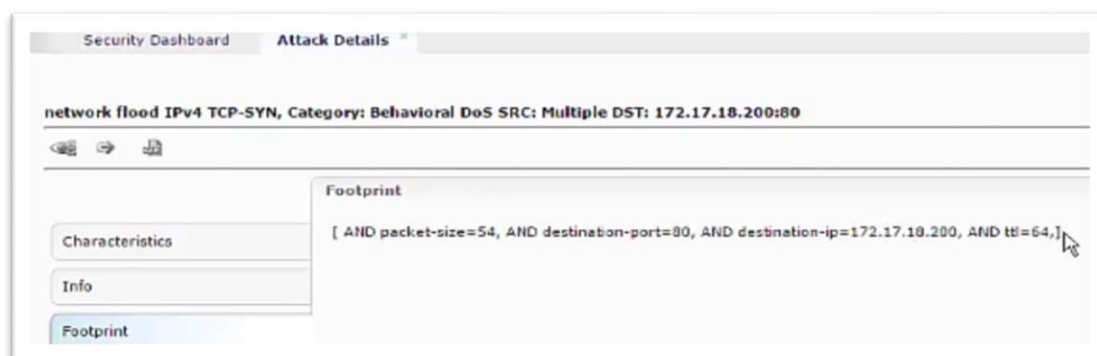
La solución requiere el uso del sistema APSolute Vision Manager, que puede ser comprado como dispositivo o instalado en virtual. El APSolute es el gestor de los dispositivos de Radware. Accediendo a él pueden verse los ataques detectados en tiempo real y los detalles.



Start Time	Attack Category	Status	Risk	Attack Name	Source Address	Destination Address	Policy	Radware ID	Direction
Oct 29, 2014 3:45:33 PM	Behavioral DoS	Started	High	network flood IPv4 TCP-SYN	0.0.0.0	0.0.0.0	AppWallXPF	73	
Oct 29, 2014 3:43:58 PM	Anomalies	Occurred	Medium	L4 Source or Dest Port Zero	Multiple	Multiple	Packet Anomalies	125	



El sistema, ante la detección de un ataque, permite aplicar automáticamente reglas para mitigar y bloquear a los atacantes, mientras deja las conexiones “buenas” atravesar el bloqueo filtrando, efectivamente, los ataques.



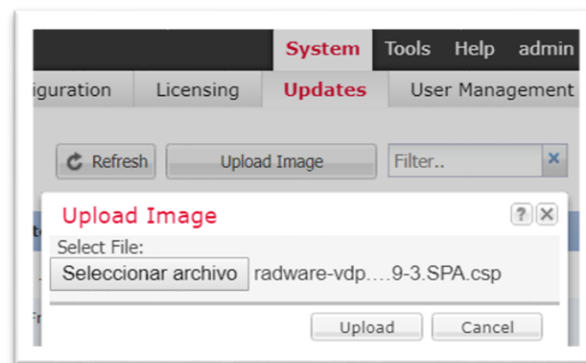
Las instalaciones de “service-changing” del vDP están soportadas en todos los montajes Firepower salvo en Cluster Inter-chassis. Sí está soportado en Cluster Intra-chassis.

En los modelos Firepower 4110 y 4120 la instalación del vDP se debe realizar a la vez que la instalación inicial del Logical Device, por lo que, si existe uno ya creado, deberá eliminarse y volverse a crear, reiniciando de este modo la configuración del cortafuegos.

En el siguiente ejemplo, en cambio, vamos a instalar un vDP en un Logical Device pre-existente en un Firepower 4150. La instalación supone un rearranque del cortafuegos, pero no una pérdida de configuración del cortafuegos.

Le asignaremos una dirección IP de gestión dentro del rango de gestión del Firepower FTD para utilizar así el mismo interfaz.

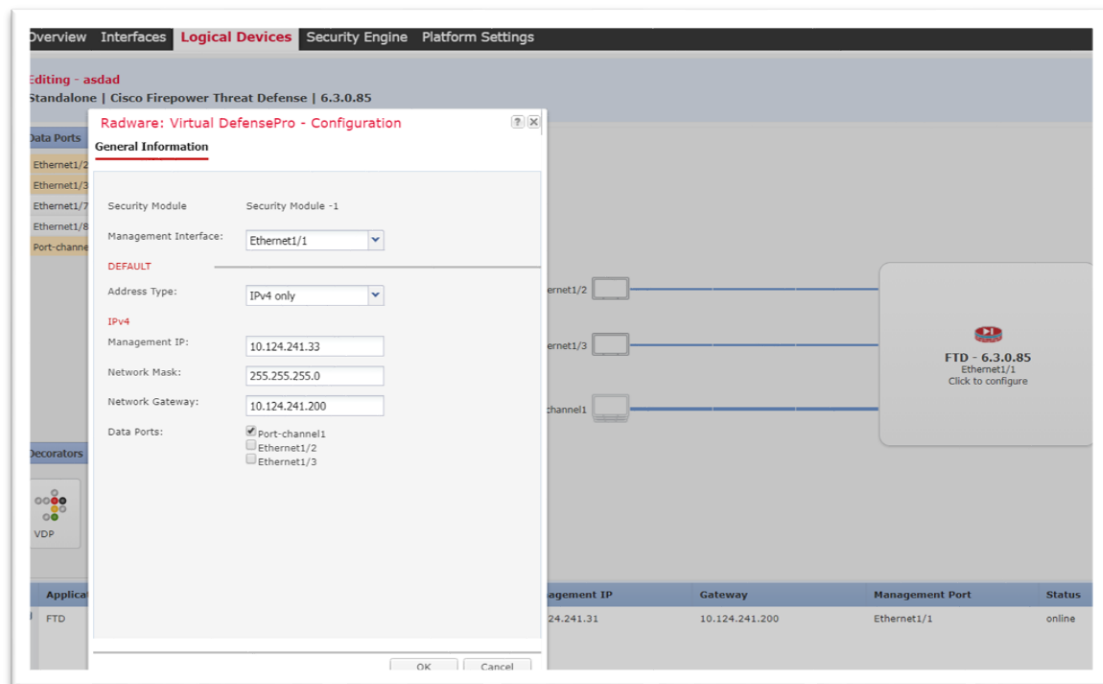
El primer paso es descargar la imagen software desde la web de Cisco, dentro del modelo del cortafuegos FTD, sección “Radware Virtual Defense Pro (vDP)”. Usando conexión web al FXOS Chassis Manager debemos subir la imagen al cortafuegos.



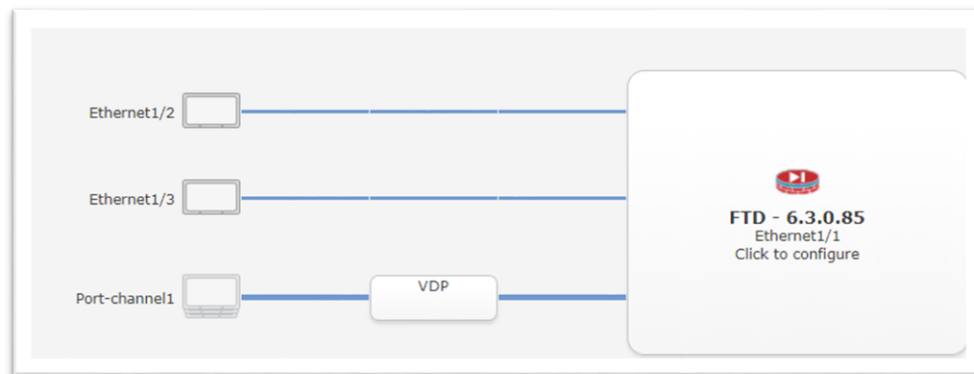
Con el Logical Device de FTD ya creado y online. En este ejemplo, el Port-Channel 1 es el interfaz con conexión a Internet.

Overview Interfaces Logical Devices Security Engine Platform Settings						
Logical Device List (1 instances) 0% (0 of 86) Cores Available						
asdad	Standalone	Status:ok				
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.3.0.85		10.124.241.31	10.124.241.200	Ethernet1/1	online
Interface Name Type Attributes Ethernet1/2 data Cluster Operational Status : not-applicable Ethernet1/3 data FIREPOWER-MGMT-IP : 10.124.241.31 Port-channel1 data MGMT-URL : https://10.124.241.64/ HA-ROLE : standalone UUID : 4e6d1bfc-6874-11e9-baf5-b8de9255d3ee						

Al editarlo aparecerá una nueva ventana del “Decorator” que pedirá los datos de gestión, dirección IP y que interfaz de datos usará para el “Service-Chaining”.



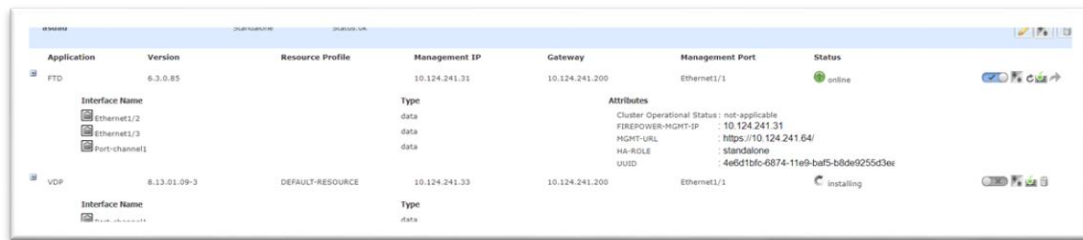
En el dibujo debe aparecer el vDP como entrada del interfaz y, a su vez, dando la entrada al cortafuegos, “Service-Chaining”.



En la parte de abajo aparecen las características de FTD y VDP que se instalarán/modificarán.

Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.3.0.85		10.124.241.31	10.124.241.200	Ethernet1/1	online
Interface Name						
Ethernet1/2			Type		data	
Ethernet1/3			Type		data	
Port-channel1			Type		data	
VDP	8.13.01.09-3		10.124.241.33	10.124.241.200	Ethernet1/1	online
Interface Name						
Port-channel1			Type		data	

Una vez realizados los cambios, aparecerá el vDP en estado “instalándose”.



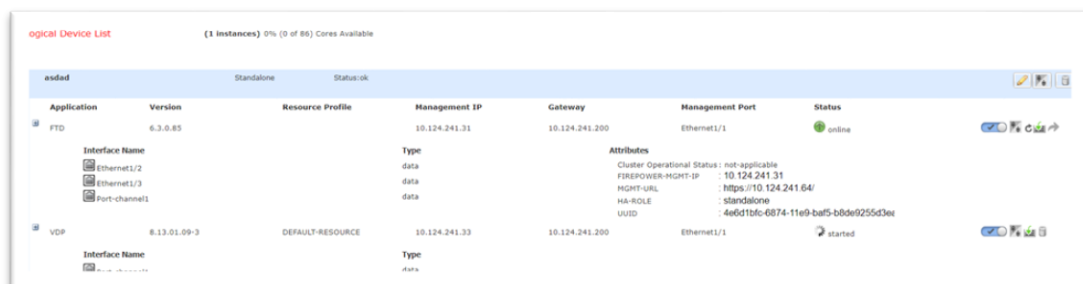
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.3.0.85		10.124.241.31	10.124.241.200	Ethernet1/1	online
Interface Name Ethernet1/2 Ethernet1/3 Port-channel1						
		Type				
		data				
		data				
		data				
Attributes Cluster Operational Status : not-applicable FIREPOWER-MGMT-IP : 10.124.241.31 MGMT-URL : https://10.124.241.64/ HA-ROLE : standalone UUID : 4e6d1bfc-6874-11e9-baf5-b8de9255d3ee						
vDP	8.13.01.09-3	DEFAULT-RESOURCE	10.124.241.33	10.124.241.200	Ethernet1/1	installing
Interface Name Port-channel1						
		Type				
		data				

El sistema parará el “Logical Device” y lo volverá a arrancar con las 2 apps “encadenadas” en la interfaz Port-Channel1.



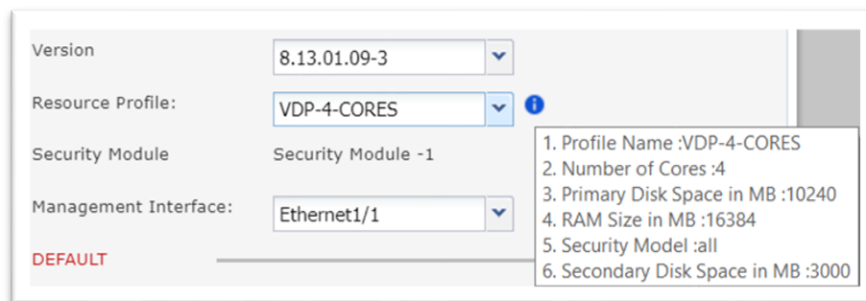
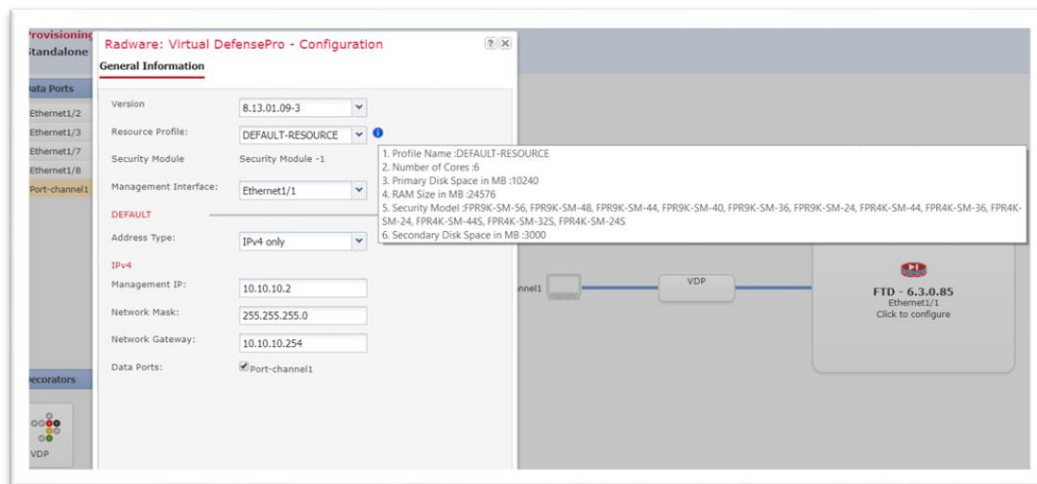
Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.3.0.85		10.124.241.31	10.124.241.200	Ethernet1/1	stopping
Interface Name Ethernet1/2 Ethernet1/3 Port-channel1						
		Type				
		data				
		data				
		data				
Attributes Cluster Operational Status : not-applicable FIREPOWER-MGMT-IP : 10.124.241.31 MGMT-URL : https://10.124.241.64/ HA-ROLE : standalone UUID : 4e6d1bfc-6874-11e9-baf5-b8de9255d3ee						
vDP	8.13.01.09-3	DEFAULT-RESOURCE	10.124.241.33	10.124.241.200	Ethernet1/1	starting
Interface Name Port-channel1						
		Type				
		data				

Una vez concluido el proceso, la aplicación FTD debe aparecer “online” y la VDP “started”, lista para ser configurada con el APSolute Vision Manager.



Application	Version	Resource Profile	Management IP	Gateway	Management Port	Status
FTD	6.3.0.85		10.124.241.31	10.124.241.200	Ethernet1/1	online
Interface Name Ethernet1/2 Ethernet1/3 Port-channel1						
		Type				
		data				
		data				
		data				
Attributes Cluster Operational Status : not-applicable FIREPOWER-MGMT-IP : 10.124.241.31 MGMT-URL : https://10.124.241.64/ HA-ROLE : standalone UUID : 4e6d1bfc-6874-11e9-baf5-b8de9255d3ee						
vDP	8.13.01.09-3	DEFAULT-RESOURCE	10.124.241.33	10.124.241.200	Ethernet1/1	started
Interface Name Port-channel1						
		Type				
		data				

Si se realiza una instalación simultánea del Logical Device FTD y el vDP, se puede seleccionar el “Resource Profile”, es decir, los recursos asignados al vDP desde la instancia nativa FTD. Existen diferentes perfiles con diferentes consumos. La selección del perfil depende de las necesidades de la instalación.



16. UTILIDAD DE MIGRACIÓN A FIREPOWER

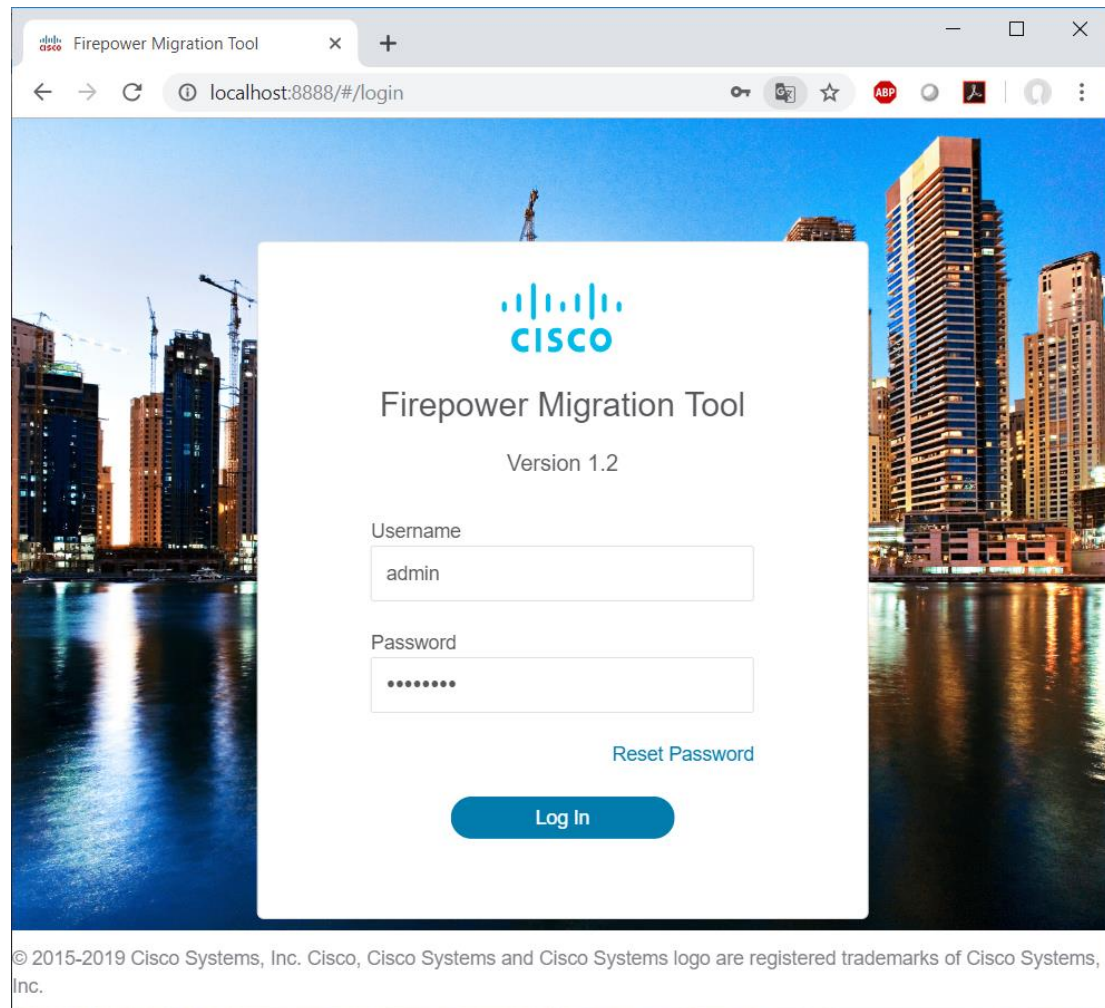
La herramienta “Firepower Migration Tool” es una utilidad que se puede descargar de la web de Cisco, siguiendo cualquier modelo FTD, que permite migrar las configuraciones de Cisco ASA y Checkpoint a Firepower.

La utilidad corre en equipos Windows y Mac. Se recomienda crear un directorio y ejecutarla dentro de él, puesto que la herramienta es solo un ejecutable auto-contenido que al arrancar crea directorios de trabajo y ficheros en el mismo directorio de ejecución.

La ejecución corre en segundo plano en una ventana de logs y abre un navegador a la aplicación. El navegador Firefox no está soportado. Se recomienda usar Chrome.

La utilidad soporta la migración de las siguientes características de una configuración ASA a Firepower:

- Objetos de red y grupos.
- Objetos de servicio y grupos (no anidados).
- ACLs de entrada (reglas in inbound en interfaces).
- NATs, tanto manuales como auto.
- Rutas estáticas (excepto con tracking).
- Interfaces, incluyendo físicos, Subinterfaces y EtherChannels.
- Bridge Groups, solo para el modo transparente.



Las credenciales de login son:

- Usuario: admin
- Contraseña: Admin123

En el primer arranque se pide resetear la contraseña.

La herramienta mostrará una pantalla de “checklist” con los requisitos necesarios para realizar la migración.

Pre-Migration Checklist

Before you begin your Adaptive Security Appliance (ASA) to Firepower Threat Defense migration, you must have the following items:

1. **Stable IP Connection:** Make sure that the Firepower Migration Tool has a stable IP connection to the Firepower Management Center throughout the migration process. Do not perform any changes on the Firepower Migration Center during migration.
2. **Firepower Management Center Version:** Make sure that the Firepower Management Center that manages the Firepower Threat Defense device is version 6.2.3 or above.
3. **Firepower Management Center Account:** Create a dedicated user account with administrative privileges for the Firepower Migration Tool and use those credentials during the migration.
4. **Firepower Threat Defense Device (Optional):** Add the target Firepower Threat Defense device to Firepower Management Center.
5. **ASA Configuration Requirements:** If you are manually uploading a configuration, export the file from a supported Adaptive Security Appliance (ASA) device for one or more contexts in .cfg or .txt format / Connect to a live ASA to export Configuration file for one or more contexts.
6. **Interface Requirements:** If your source ASA has Port Channel interfaces, you must create Port Channel Interfaces on the Firepower Management Center; sub interfaces will be automatically created.
7. **Power Options:** On this Windows/Mac machine, configure the Plan Settings in Power Options to Never Put the Computer to Sleep, so the system doesn't go to sleep during a large migration push.
8. **Default Browser:** Configure the system default browser as Google Chrome.



This migration may take a while. Do not make any changes to the Firepower Management Center (FMC) when migration is in progress.

New Migration

La utilidad permite hacer un “Resume” de una migración ya iniciada si se cierra, voluntaria o involuntariamente.

Seleccionando “New Migration” se inicia un nuevo proceso de migración.

El comienzo es obtener la configuración del ASA. La última versión de la aplicación permite subir el fichero de configuración manualmente o conectase directamente a un equipo ASA proporcionando credenciales.

The screenshot shows the Cisco Firepower Migration Tool interface. At the top, there's a progress bar with six steps: 1. Extract ASA Information (active), 2. Select Target, 3. Map FTD Interface, 4. Map Security Zones & Interface Groups, 5. Review & Validate, and 6. Complete Migration. Below the progress bar, the 'Extract ASA Information' section is displayed. It has a dropdown menu for 'Extraction Methods'. Under this menu, there are two main options: 'Manual Upload' and 'Connect to ASA'. The 'Manual Upload' section includes instructions: 'File format is '.cfg' or '.txt'.', 'For Multi-context upload a show tech.', and 'For Single-context upload show running.'. It has an 'Upload' button. The 'Connect to ASA' section includes instructions: 'Single-context : Enter the management IP address and connect using admin credentials.' and 'Multi-context : Enter the IP address of the admin context and connect using admin credentials.'. It has a text input field for 'ASA IP Address/Hostname:' and a 'Connect' button. At the bottom right, there is a 'Next' button.

Una vez obtenida la configuración, se muestra un resumen de los datos obtenidos y errores de parsing, si los hubiera.

Upload the ASA Configuration File		
UPLOAD SUMMARY		
Upload Status: Completed Upload		
Filename: Config-1.txt		
0 parsing errors found. Refer to the log file for more details		
652	215	78
Access Control List Lines	Used Network Objects	Used Port Objects
30	29	46
Logical Interfaces	Static Routes	Network Address Translation
Please download the Pre-Migration report for a detailed summary of the parsed configuration. Download Report		

Seleccionando “Download Report” se puede visualizar un informe detallado las líneas migradas, las no soportadas y las parcialmente migradas. Se debe estudiar el informe con detalle para tratar de solucionar los problemas después de la migración y lograr la migración completa.

Si todo está correcto, pulsando Next nos pedirá los datos de conexión al gestor Firepower Management Center (FMC).

Connect to FMC

IP Address [Connect](#)

Se detectarán los dispositivos FTD y se pedirá la selección de uno, pasando a la selección de mapeo de interfaces.

Select FTD Device and Map Interfaces

Select FTD Device: 192.168.115.17 : FTD_1 [Get Interfaces](#)

Warning: Please ensure that the firewall mode configured on the target FTD device is the same as in the uploaded ASA configuration file. The existing configuration of the FTD device on the FMC is erased when you push the migrated configuration to the FMC.

Partiendo de las interfaces del ASA, se deben asignar los nuevos del FTD.

Select FTD Device and Map Interfaces i

Select FTD Device: 192.168.115.17 : FTD_1 Get Interfaces

ASA Interface Name	FTD Interface Name
GigabitEthernet0/0	GigabitEthernet0/0
TenGigabitEthernet0/8	GigabitEthernet0/1
TenGigabitEthernet0/9	GigabitEthernet0/2

10 per page 1 to 3 of 3 Page 1 of 1

En la siguiente fase, se debe realizar el mapping de zonas de seguridad.

Map Security Zones and Interface Groups i

Auto-Create

ASA Logical Interface Name	FTD Interface	FMC Security Zones	FMC Interface Groups
OUTSIDE	GigabitEthernet0/0	Select Security Zone	Select Interface Groups
VM-INFRA	GigabitEthernet0/1.602	Select Security Zone	Select Interface Groups
VMOTION_BACKUP	GigabitEthernet0/1.603	Select Security Zone	Select Interface Groups
PROD-FW-WEB-LB	GigabitEthernet0/1.610	Select Security Zone	Select Interface Groups
PROD-FW-DB-LB	GigabitEthernet0/1.612	Select Security Zone	Select Interface Groups
PROD-FW-MT-LB	GigabitEthernet0/1.613	Select Security Zone	Select Interface Groups
PROD-UTILITY	GigabitEthernet0/1.614	Select Security Zone	Select Interface Groups
PROD-DB	GigabitEthernet0/1.650	Select Security Zone	Select Interface Groups

Si se usa “Auto-Create”, la herramienta hará una asignación que, normalmente, suele ser correcta y ahorra mucho tiempo en la migración.

En la siguiente pantalla se muestra un resumen para revisión y validación del proceso de migración.

Review and Validate Configuration 

[Access Control](#) [NAT](#) [Network Objects](#) [Port Objects](#) [Interfaces](#) [Routes](#)

Actions 

Save 

		SOURCE				DESTINATION					
☐	#	Name	Zone	Network	Port	Zone	Network	Port	State	Action	
☐	1	FROM-OUTSIDE_R1	outside	RAXGEN_v1_NET_NEST	ANY	ANY	any	ANY	  	Permit	
☐	2	FROM-OUTSIDE_R2	outside	ABC-NEST	ANY	ANY	any	ANY	  	Permit	
☐	3	FROM-OUTSIDE_R3	outside	any	ANY	ANY	any	ICMP-ALLOWED	  	Permit	
☐	4	FROM-OUTSIDE_R4	outside	SHUN-IP-DENY	ANY	ANY	any	ANY	  	Deny	
☐	5	FROM-OUTSIDE_R5	outside	SHUN-IP-DENY	ANY	ANY	any	icmp	  	Deny	
☐	6	FROM-OUTSIDE_R6	outside	MYRACK-SERVERS	ANY	ANY	10.185.2.128	tcp:443	  	Permit	

Se deben revisar todas las pestañas, Access Control, NAT, Objetos, Interfaces y Rutas.

Review and Validate Configuration 1

Access Control NAT Network Objects Port Objects Interfaces Routes

Actions Save

ORIGINAL PACKET						TRANSLATED PACKET					
NAT Ty...	Source...	Destin...	Type	Source Add...	Destination ...	Source Port	Destination...	Source Add...	Destination ...	Source Port	Destination...
MANUAL		outside_jg	static	FW-SEGMENTS	CLIENT-VPN-IPPOOL			FW-SEGMENTS	CLIENT-VPN-IPPOOL		
MANUAL	MANAGEMENT_NT_jg	outside_jg	dynamic	EQ_RS-DC	EQ_RS-DNS				EQ_RS-DNS		
MANUAL		outside_jg	dynamic	RS-DR-NET	RS-KMS-SERVERS		KMS-PROT-DST		RS-KMS-SERVERS		KMS-PROT-DST
MANUAL		outside_jg	dynamic	PROD_SERVERS-INET				PROD-INET_PAT			
MANUAL		outside_jg	dynamic	NON-PROD_SERVERS-				NON-PROD-INET_PAT			

Las reglas de Access Control se pueden seleccionar (una o varias) y, en “Actions”, decidir que no se migren.

El siguiente paso realiza una validación interna, donde, en ocasiones, puede reportar errores.

Validation Status

⚠ Conflicts Detected

The following object conflicts need to be resolved

3

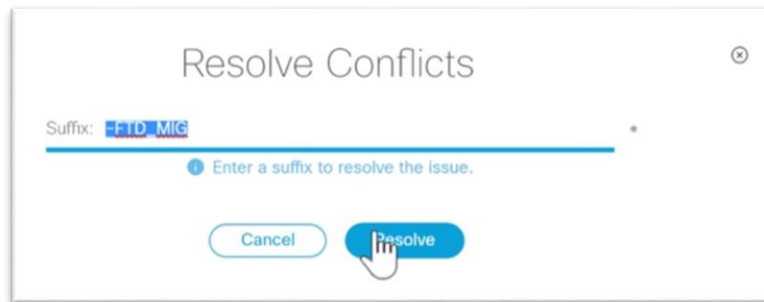
Network Object Conflicts

2

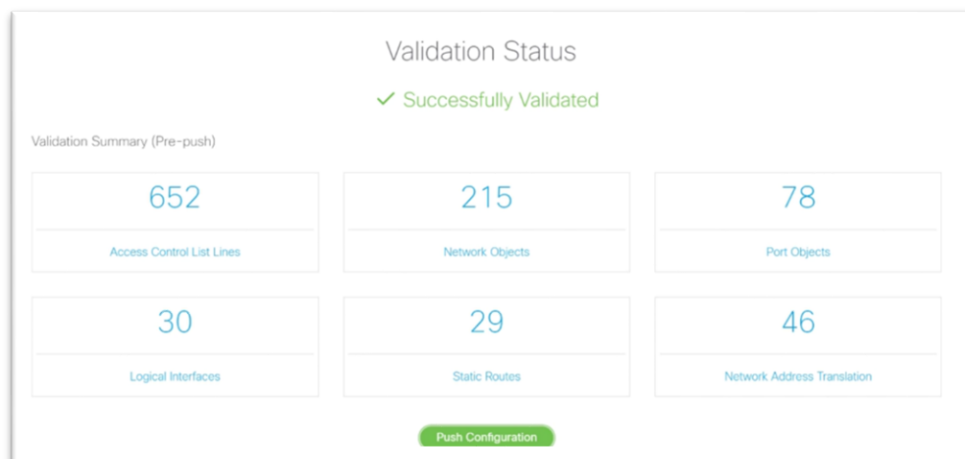
Port Object Conflicts

Resolve Conflicts

Normalmente estos son por conflictos de nombres repetidos por la diferencia de objetos entre ASA y FTD. Pulsando en “Resolve Conflicts” y luego seleccionando y pulsando sobre Actions->Resolve Conflicts se puede arreglar fácilmente añadiendo un sufijo nuevo.

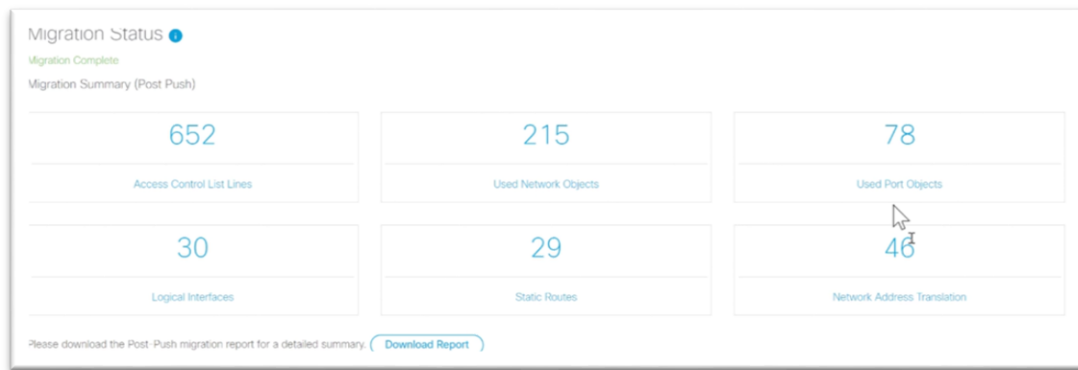


Una vez resueltos todos los problemas, la validación debe ser correcta.



Presionando en “Push Configuration” se iniciará el proceso que puede tardar varios minutos.

Una vez finalizado se mostrará un resumen y se genera un informe.



Es importante estudiar este informe para detectar algún fallo o problema que pudiera afectar a la migración.

Una vez terminada la migración, en el FMC aparecerá la ACP con las reglas. Se debe comprobar que es correcta.

15-Mig-1529576762

Policy: Default:Profile:Policy

SSM Policy: SSM

Identity Policy: SSM

Filter by Device

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Source Ports	Dest Ports	URLs	SSE/SST Attr...	Action
1. CORP-Shared_F14	CORP-Shared	Any	any	RS-PROD-VIPS	Any	Any	Any	Any	TCP (S):443	Any	Any	Allow
2. CORP-Shared_F15	CORP-Shared	Any	any	RS-PROD-VIPS	Any	Any	Any	Any	TCP (S):80	Any	Any	Allow
3. CORP-Shared_F16	CORP-Shared	Any	any	RS-NONPROD-VIPS	Any	Any	Any	Any	TCP (S):443	Any	Any	Allow
4. CORP-Shared_F17	CORP-Shared	Any	any	RS-NONPROD-VIPS	Any	Any	Any	Any	TCP (S):80	Any	Any	Allow
5. CORP-Shared_F18	CORP-Shared	Any	any	10.185.10.13	Any	Any	Any	Any	TCP (S):25	Any	Any	Allow
6. CORP-Shared_F19	CORP-Shared	Any	any	10.185.60.237	Any	Any	Any	Any	TCP (S):80	Any	Any	Allow
7. CORP-Shared_F20	CORP-Shared	Any	any	RS-PERF-VIPS	Any	Any	Any	Any	TCP (S):443	Any	Any	Allow
8. CORP-Shared_F21	CORP-Shared	Any	any	RS-PERF-VIPS	Any	Any	Any	Any	TCP (S):80	Any	Any	Allow
9. NONPROD-DB-Trainee	NONPROD-DB-T	Any	any	10.185.10.13	Any	Any	Any	Any	TCP (S):443	Any	Any	Allow

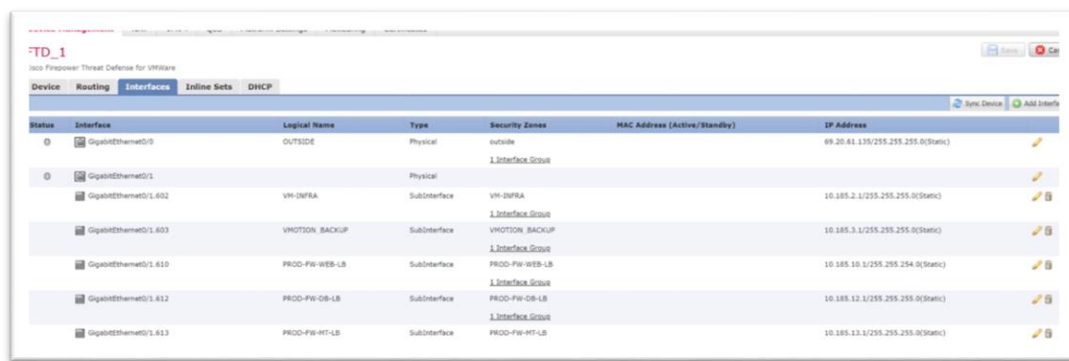
También se debe revisar la política de NAT y las interfaces del dispositivo destino de la migración.

15-Mig-1529576762

Policy: Default:Profile:Policy

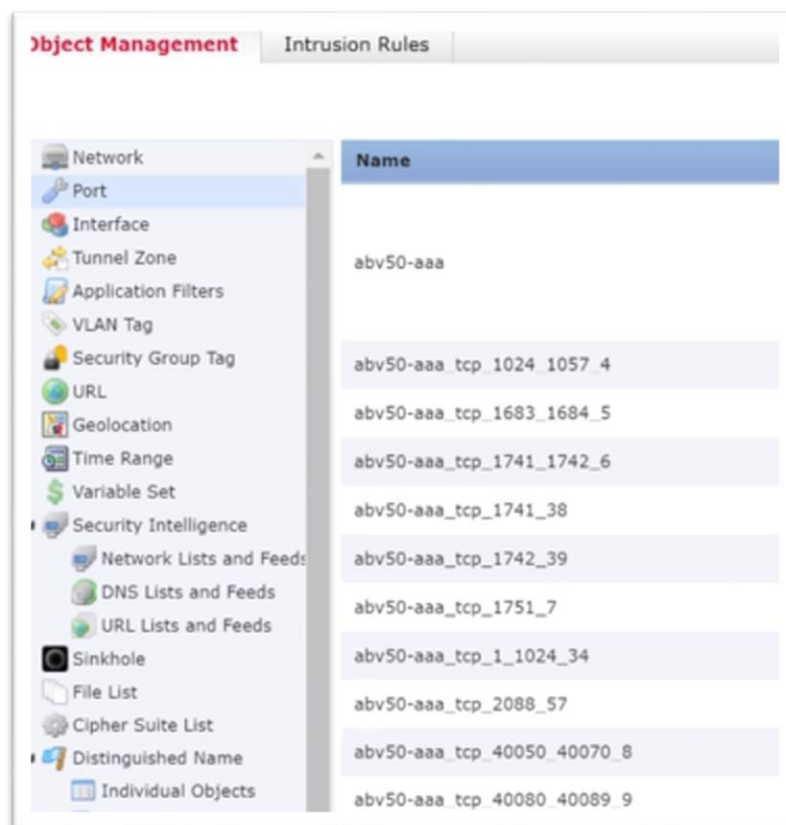
Filter by Device

Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
Dynamic	MANAGEMENT_Ig	outside_Ig	EQ_RS-OC	EQ_RS-ONS	Interface	EQ_RS-ONS	Original	RS-KMS-SERVERS	Original	KMS-PROT-DST
Dynamic	any	outside_Ig	RS-DR-NET	RS-KMS-SERVERS	Interface	RS-KMS-SERVERS	Original	KMS-PROT-DST	Original	KMS-PROT-DST
Static	PROD-UTILITY_Ig	outside_Ig	FM-ODS	104.130.83.194	104.130.83.194	104.130.83.194	104.130.83.194	104.130.83.194	104.130.83.194	Ons: false
Static	STORAGE_Ig	outside_Ig	OB-10.185.70.8	104.205.12.86	104.205.12.86	104.205.12.86	104.205.12.86	104.205.12.86	104.205.12.86	Ons: true
Static	STORAGE_Ig	outside_Ig	OB-10.185.70.7	104.205.12.87	104.205.12.87	104.205.12.87	104.205.12.87	104.205.12.87	104.205.12.87	Ons: true
Static	VM-INFRA_Ig	outside_Ig	104.10.185.2.81	104.205.12.81	104.205.12.81	104.205.12.81	104.205.12.81	104.205.12.81	104.205.12.81	Ons: false
Static	VM-INFRA_Ig	outside_Ig	104.10.185.2.80	104.205.12.80	104.205.12.80	104.205.12.80	104.205.12.80	104.205.12.80	104.205.12.80	Ons: false



Status	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
0	GigabitEthernet0/0	OUTSIDE	Physical	outside	1.Interface Group	69.20.41.175/255.255.255.0(Static)
0	GigabitEthernet0/1		Physical			
	GigabitEthernet0/1.602	VN-INFRA	SubInterface	VN-INFRA	1.Interface Group	10.185.2.1/255.255.255.0(Static)
	GigabitEthernet0/1.603	VNOTION_BACKUP	SubInterface	VNOTION_BACKUP	1.Interface Group	10.185.3.1/255.255.255.0(Static)
	GigabitEthernet0/1.610	PROD-FW-WEB-LB	SubInterface	PROD-FW-WEB-LB	1.Interface Group	10.185.10.1/255.255.254.0(Static)
	GigabitEthernet0/1.612	PROD-FW-DB-LB	SubInterface	PROD-FW-DB-LB	1.Interface Group	10.185.12.1/255.255.255.0(Static)
	GigabitEthernet0/1.613	PROD-FW-RT-LB	SubInterface	PROD-FW-RT-LB	1.Interface Group	10.185.13.1/255.255.255.0(Static)

Resaltar que los Service Objects de ASA son transformados a Port Objects.



17. ANEXO A. LISTA DE COMPROBACIÓN – CHECKLIST

En la siguiente lista se resumen puntos concretos que deben ser analizados conforme a los puntos de esta guía para verificar que se han seguido las guías de seguridad en la instalación del equipo.

En cada nueva integración se deben seguir y analizar las acciones de esta guía a fin de comprobar que las medidas de seguridad se han implementado correctamente.

La lista está dividida en secciones, que pueden ser de aplicación o no, dependiendo de la integración específica que se deba realizar. La columna de apartado indica el apartado relevante dentro de esta guía en relación con el punto.

INFORMACIÓN DEL DISPOSITIVO	
Nombre	
Nº de Serie	
Ubicación	
Fecha	

ACCIÓN	SÍ	NO	OBSERVACIONES	APARTADO
BÁSICO				
Estudiar el diseño a implementar	☐	☐		7
Configuración inicial y conexión a Red de Gestión	☐	☐		8
Modo de funcionamiento	☐	☐		9
CONFIGURACIÓN DEL CHASSIS (Firepower 4100/9300)				
Establecimiento del modo Common Criteria	☐	☐		10.1
Sincronización horaria (NTP)	☐	☐		10.2
Instalación de certificado confiable HTTPS	☐	☐		10.4
Gestión y política de usuarios del chassis	☐	☐		10.5
Establecer política de copia de seguridad	☐	☐		10.6
Configuración de Interfaces	☐	☐		10.7
Instalación cortafuegos FTD	☐	☐		10.8

ACCIÓN	SÍ	NO	OBSERVACIONES	APARTADO
Establecer procedimiento de actualizaciones	☐	☐		10.9
GESTIÓN A TRAVÉS DE FIREPOWER MANAGEMENT CENTER				
Configuración inicial y conexión a Red de Gestión	☐	☐		13.1 y 13.2
Establecimiento del modo Common Criteria para el gestor	☐	☐		13.3
Sincronización horaria (NTP) para el gestor	☐	☐		13.4
Instalación de certificado confiable HTTPS	☐	☐		13.6
Configuración de “banner”, gestión y política de usuarios	☐	☐		13.7 y 13.8
Licenciamiento del sistema	☐	☐		13.9
Añadir los dispositivos al gestor	☐	☐		13.11.1
Configuración de conexiones, interfaces	☐	☐		13.11.3
Configuración del routing (dinámico/estático)	☐	☐		13.11.4
Configuración DHCP	☐	☐		13.11.5 y 13.11.6
Establecimiento del modo Common Criteria en los dispositivos	☐	☐		13.12.1
Sincronización horaria (NTP) en los dispositivos	☐	☐		13.12.2
Configuración de “banner” y usuarios de los dispositivos	☐	☐		13.12.4
Establecer política de copia de seguridad	☐	☐		13.24

ACCIÓN	SÍ	NO	OBSERVACIONES	APARTADO
Establecer procedimientos de actualizaciones	☐	☐		13.25, 13.26, 13.27, 13.28, 13.29
ALTA DISPONIBILIDAD				
Instalación Failover (Activo/Pasivo)	☐	☐		13.13.1
Instalación Cluster (Activo/Activo)	☐	☐		13.13.2
NAT				
Creación de las políticas de NAT en los dispositivos	☐	☐		13.14
REGLAS DE ACCESO (ACP)				
Creación de reglas y políticas de acceso en los dispositivos	☐	☐		13.15
NGIPS				
Configurar filtro Security Intelligence	☐	☐		13.15.4
Configurar el descubrimiento de red (Network Discovery)	☐	☐		13.16
Creación de reglas y política de intrusión (Intrusion Policy)	☐	☐		13.17
DESCUBRIMIENTO DE IDENTIDADES				
Configuración de política de identidad e instalación de agente	☐	☐		13.18

PROTECCIÓN DE MALWARE				
Configuración de política anti-malware	☐	☐		13.19
INTERCEPCIÓN SSL/TLS				
Creación y configuración de la política SSL	☐	☐		13.20
REDES PRIVADAS VIRTUALES (VPN)				
Configuración redes privadas site to site	☐	☐		13.22
Configuración redes privadas de acceso remoto	☐	☐		13.23
GESTIÓN A TRAVÉS DE FIREPOWER DEVICE MANAGER				
Completar asistente de configuración	☐	☐		14.1
Configuración de conexiones, interfaces	☐	☐		14.2 y 14.3
Configuración del routing (dinámico/estático)	☐	☐		14.4
Desactivación de gestión por Red de Datos	☐	☐		14.5
Creación de la política de NAT	☐	☐		14.10
Establecer procedimientos de actualizaciones	☐	☐		14.13 y 14.14
ALTA DISPONIBILIDAD				
Instalación Failover (Activo/Pasivo)	☐	☐		14.12
PROTECCIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO				
Instalación Radware Defense Pro (vDP)	☐	☐		15
BORRADO SEGURO DEL SISTEMA				
Aplicación procedimiento de borrado	☐	☐		11

18. ANEXO B. ADECUACIÓN AL ESQUEMA NACIONAL DE SEGURIDAD

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) en el ámbito de la Administración Electrónica, establece la política de seguridad en la utilización de medios electrónicos por las Administraciones Públicas.

Está constituido por principios básicos y requisitos mínimos a cumplir que permiten una protección adecuada de la información.

Todos los organismos superiores de las Administraciones Públicas deben disponer de su política de seguridad que garantice el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos.

En su Anexo II el ENS establece una serie de medidas de seguridad que están condicionadas a la valoración (Anexo I) del nivel de seguridad en cada dimensión, y a la categoría (artículo 40) del sistema de información de que se trate. A su vez, la categoría del sistema se calcula en función del nivel de seguridad en cada dimensión.

Estas medidas constituyen un mínimo que se debe implementar, o justificar los motivos por los cuales no se implementan o se sustituyen por otras medidas de seguridad que alcancen los mismos efectos protectores sobre la información y los servicios.

Las medidas de seguridad se dividen en tres grupos:

- **Marco organizativo (org)**
Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.
- **Marco operacional (op)**
Formado por las medidas a tomar para proteger la operación la operación del sistema como conjunto integral de componentes para un fin.
- **Medidas de protección (mp)**
Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

La siguiente tabla muestra un resumen de los diversos módulos del ENS en que los equipos Cisco Firepower ayudan a su cumplimiento y que han sido revisados en detalle en esta guía.

MARCO ORGANIZATIVO		
Medidas de seguridad		Componente Firepower
org.1	Política de seguridad	Visibilidad
org.2	Normativa de seguridad	
org.3	Procedimientos de seguridad	

org.4	Proceso de autorización	
MARCO OPERACIONAL		
Medidas de seguridad		Componente Firepower
op.pl.2	Arquitectura de Seguridad	Cortafuegos, AVC, NGIPS, DLP, User Agent
op.pl.5	Componentes Certificados	Certificaciones de terceros
op.acc.1	Identificación	User Agent, portal cautivo
op.acc.2	Requisitos de Acceso	User Agent, portal cautivo
op.acc.3.r3.1		
op.acc.4	Proceso de gestión de derechos de acceso	User Agent, portal cautivo
Op.acc.4.5	Política de acceso remoto	
op.acc.5	Mecanismo de autenticación (usuarios externos)	User Agent, portal cautivo
op.acc.6	Mecanismos de autenticación (usuarios de la organización)	NGIPS, User Agent
op.acc.3.r3.1 op.acc.4.5 op.acc.6.r9	Acceso Remoto	VPN site to site, VPN acceso remoto, User Agent
op.exp.3	Gestión de la configuración de seguridad	REST API, NGIPS, AMP
op.exp.4	Mantenimiento y actualizaciones de seguridad	Procedimientos y configuración de actualizaciones.
op.exp.5	Gestión de cambios	Auditoria, copias de seguridad
op.exp.6	Protección frente a código dañino	NGIPS, AMP, URL-Filtering
op.exp.7	Gestión de incidencias	NGIPS, FMC, REST API
op.exp.8	Registro de actividad. Protección de los registros de actividad	User Agent, FMC (Connection Events), DLP FMC, copias de seguridad
op.exp.9	Registro de la gestión de incidentes	FMC
op.cont.2	Plan de continuidad	Alta disponibilidad
op.cont.4	Medios alternativos	Alta disponibilidad

	Instalaciones alternativas	
op.mon.1	Detección de intrusión	NGIPS, AMP, URL-Filtering
op.mon.2	Sistema de métricas	FMC, REST API
MEDIDAS DE PROTECCIÓN		
Medidas de seguridad		Componente Firepower
mp.com.1	Perímetro seguro	Cortafuegos, AVC, NGIPS, User Agent, AMP
mp.com.2	Protección de la confidencialidad	VPN site to site, VPN acceso remoto
mp.com.3	Protección de la autenticidad y la integridad	VPN site to site, VPN acceso remoto, NGIPS
mp.com.4	Segregación de flujos de información en la red	Cortafuegos
mp.info.1	Datos de carácter personal	Autenticación basada en roles
mp.info.2	Calificación de la información	Master key, VPN site so site, VPN acceso remoto
mp.info.6	Copias de seguridad (backup)	FMC, FXOS
mp.s.1	Protección del correo electrónico	NGIPS, AVC, AMP
mp.s.2	Protección de servicios y aplicaciones web	NGIPS, AVC, User Agent, interceptación SSL
mp.s.4	Protección frente a la denegación de servicio	Radware Defense Pro (vDP)

