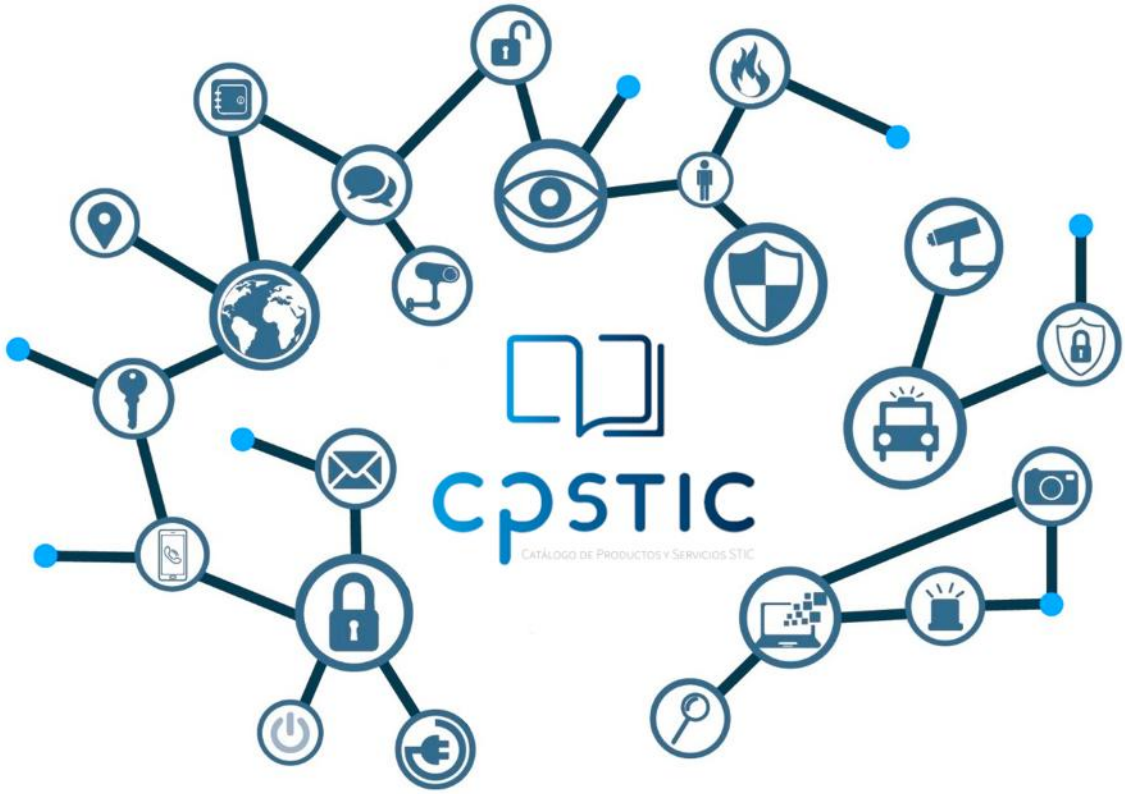
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1413

Procedimiento de Empleo Seguro
Cortafuegos NGFW de Palo Alto Networks



Junio 2026

Edita:

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.06.11 13:27:38 +02'00'

Centro Criptológico Nacional, 2026

ÍNDICE

1 INTRODUCCIÓN

1.1 ENTORNO ACTUAL

1. En los últimos años las amenazas cibernéticas han evolucionado desde vectores de ataque simples hasta sujetos capaces de construir *malware* persistente, muy sofisticado, con capacidades de infección en múltiples áreas. Para poder ofrecer una prevención eficiente, las soluciones actuales de seguridad necesitan comprender y gestionar todas las fases en la cadena de ataque.

2. Además, hoy día los departamentos TI se enfrentan a una problemática creciente con usuarios –tanto externos como internos- que utilizan una nueva generación de aplicaciones, capaces de evadir la detección que ofrecen los firewalls o cortafuegos tradicionales, que permitían establecer políticas de seguridad basadas fundamentalmente en puertos y protocolos.

3. Hasta hace no mucho, esta aproximación era válida, pues lo normal era que por el puerto 80 pasara sólo la navegación web y por el puerto 443, el tráfico SSL. Sin embargo, las nuevas aplicaciones de la Web 2.0 tales como *Facebook, YouSendIt, SalesForce, Messenger, Skype*, etc., se han convertido en un verdadero fenómeno social y su uso se ha extendido tanto en ámbitos privados como profesionales. Muchas de estas aplicaciones utilizan técnicas evasivas como *port hopping*, tunelización/emulación de otras aplicaciones, etc., para burlarse de las reglas de los cortafuegos tradicionales, basadas en puertos y protocolos. Muchas de ellas se esconden incluso bajo tráfico cifrado para ocultar su identidad.

4. Como resultado de todo ello, los responsables de TI no pueden identificar o controlar las aplicaciones que están corriendo realmente en la red, y esta falta de visibilidad y control impacta negativamente en el negocio, generando:
    - Incumplimiento de regulaciones y políticas internas.
    - Fuga de datos.
    - Incremento del consumo de ancho de banda.
    - Aumento de las amenazas (virus, *spyware*, gusanos y otras vulnerabilidades).
    - Desaprovechamiento de los recursos (tanto humanos como de equipamiento).
5. Los responsables de TI necesitan por tanto una nueva aproximación, que les permita identificar con precisión las aplicaciones, y no solamente los puertos que usan, a través de una inspección completa del tráfico. Esto implica una transición de la seguridad tradicional, basada en puertos/protocolos (*Stateful Inspection*), a otra en base a la clasificación de tráfico por aplicación y contenidos. Los departamentos de explotación y operación de seguridad tienen que abordar esta transición con los mismos recursos, por lo que el reto es grande y debe abordarse por tanto con garantías de solvencia tecnológica.

6. Un ***NGFW*** (*Next Generation Firewall* - firewall de nueva generación) es un cortafuegos cuya principal misión es ofrecer visibilidad y control sobre las aplicaciones modernas, qué

usuarios las emplean y asegurar que los contenidos que circulan por ellas son los adecuados y lo hacen de forma segura.

7. Los cortafuegos de Palo Alto Networks fueron concebidos desde su inicio para dar respuesta a todos estos retos, como NGFW, trabajando fundamentados en un motor capaz de identificar la aplicación, el usuario y el contenido, en vez de solamente el puerto y el protocolo. Asimismo, también han incorporado capacidades para la detección y prevención del *malware* desconocido. Así, ofrecen identificación de la aplicación, filtrado URL, protección frente a vulnerabilidades, antivirus, anti-*Spyware*, sandboxing (*WildFire*) y tecnologías de prevención DoS, capaces de detectar y prevenir un gran rango de amenazas y comunicaciones maliciosas en la red.

1.2 ARQUITECTURA DE LOS CORTAFUEGOS DE PALO ALTO NETWORKS

8. Palo Alto Networks cuenta con cortafuegos de nueva generación, tanto *hardware* como *software,* en forma de máquinas virtuales (VM) y contenedores para este último.

9. Actualmente se soportan los siguientes hipervisores para máquinas virtuales: VMware ESXi, VMware NSX-V/T, Nutanix, KVM, Hyper-V, Openstack. Para entornos en la nube, se soportan plataformas Microsoft Azure, Google Cloud Platform (GCP), Amazon Web Services (AWS), Alibaba Cloud y Oracle Cloud.

10. En el caso de contenedores, se soporta el despliegue en entornos Kubernetes gestionados por proveedores cloud (AWS EKS, GCP GKE, Azure AKS), y en entornos Kubernetes gestionados por consumidores, tales como Openshift RedHat.

Nota: En los siguientes enlaces se puede encontrar información detallada sobre los hipervisores (Serie-VM) y sobre los entornos de soportados basados en contenedores respectivamente:
https://docs.paloaltonetworks.com/compatibility-matrix/reference/vm-series-firewalls/vms-series-hypervisor-support
https://docs.paloaltonetworks.com/compatibility-matrix/reference/cn-series-firewalls

11. Una de las grandes ventajas de las plataformas de Palo Alto Networks es que, en general, las funcionalidades son homogéneas entre todas las plataformas, tanto físicas como virtuales.

Nota: En el siguiente enlace puede encontrar información detallada sobre las diferentes plataformas, así como sus capacidades y comparativa:
https://www.paloaltonetworks.com/products/product-selection.html

12. Más concretamente, Palo Alto Networks diseñó desde sus orígenes una arquitectura completamente nueva, específicamente diseñada para trabajar con una aproximación a la seguridad multidisciplinar, denominada **SP3 (*Single Pass Parallel Processing*)**, que comparten todos sus cortafuegos.

13. La arquitectura SP3 representa un concepto revolucionario a la hora de diseñar equipamiento dedicado a realizar tareas de seguridad. Ha sido concebida para cumplir (2) funciones clave dentro del cortafuegos de nueva generación de Palo Alto Networks. En primer lugar, la arquitectura *Single Pass* realiza todas las operaciones **una vez por paquete**. Según se procesa un paquete, el *routing* se realiza una vez, la búsqueda en la política se

realiza una vez, la identificación de la aplicación y la decodificación se realiza una vez, y el análisis de las amenazas y los contenidos se realiza una vez. Esto reduce significativamente la cantidad de sobrecarga de procesamiento necesaria para realizar múltiples funciones. En segundo lugar, la arquitectura *Single Pass* utiliza firmas basadas en **patrones uniformes**. En lugar de utilizar motores y conjuntos de firmas por separado (lo que requiere múltiples análisis en la exploración) y en lugar de utilizar servidores *proxy* (lo que requiere la descarga completa de los archivos antes de analizarlos), la arquitectura *Single Pass* escanea el tráfico de todas las firmas una única vez y en forma de *stream*, para evitar introducir latencias innecesarias.

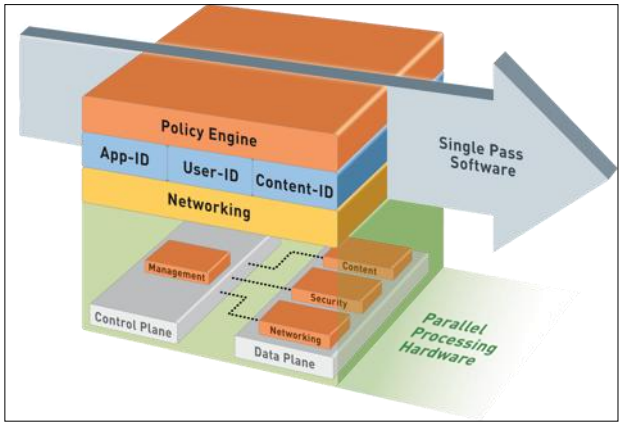


Figura 2-1: Arquitectura SP3 de Palo Alto Networks

14. Tal y como muestra la imagen anterior, cada equipo dispone de un *backplane* de control separado del de datos. Esta dualidad permite que la sobrecarga en uno de los *backplanes* no afecte al otro, lo que garantiza la capacidad de gestión aun cuando el equipo está saturado, así como la capacidad de procesar el tráfico independientemente de las tareas de gestión que se estén llevando a cabo.

1.2.1 TOPOLOGÍAS DE RED SOPORTADAS

15. Una de las grandes ventajas de las plataformas de Palo Alto Networks es que permiten trabajar con diferentes topologías de red; topologías que además se pueden utilizar simultáneamente dentro de un mismo equipo, lo que flexibiliza enormemente su uso e inclusión en las redes ya existentes. En concreto se soportan los siguientes modos de despliegue:

    - Monitor o modo visibilidad (*tap* o *span*).
    - Modo transparente en línea (*virtual wire*).
    - Modo L2 *Bridging*.
    - Modo L3 *Routing*.

16. La siguiente tabla muestra un resumen de las capacidades de cada tipo de despliegue:

Característica	*vwire*	*Layer2*	*Layer3*	*Tap*
VLAN tags	Sí	Sí	Sí	Sí
Tagged subinterfaces	Sí	Sí	Sí	No
Untagged subinterfaces	No	No	Sí	No

Característica	*vwire*	*Layer2*	*Layer3*	*Tap*
Routing	No	Sí	Sí	No
NAT	Sí	Sí	Sí	No
QoS	Sí	Sí	Sí	No
Descifrado SSL	Sí	Sí	Sí	Sí (*inbound*)
Portal Cautivo	Sí	Sí	Sí	No
Policy Based Forwarding	No	Sí	Sí	No

Tabla 1: Capacidades de los diferentes despliegues de red

Nota: En el siguiente enlace puede encontrar información detallada sobre los diferentes despliegues de red, incluyendo ejemplos de configuración, para que seleccione el más adecuado:
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-networking-admin/configure-interfaces

1.3 SISTEMAS VIRTUALES

17. Los equipos de Palo Alto Networks, soportan la capacidad de ser virtualizados para ofrecer entornos de administración independientes allí donde se requiere tener gestión diferenciada (por ejemplo, en entornos *multi-tenant*, donde el mismo equipo es compartido por diferentes clientes, que cuentan además con diferentes administradores).

18. Durante la definición de la virtualización, el administrador asigna los interfaces que desea a cada cortafuegos virtual, que pasa a comportarse a partir de este momento como un sistema independiente del resto de sistemas virtuales. De esta forma es posible administrar independientemente los sistemas virtuales, o generar informes para cada uno de ellos.

Nota: En el siguiente enlace encontrará información detallada sobre los sistemas virtuales y sus capacidades:
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/virtual-systems/virtual-systems-overview

2 OBJETO Y ALCANCE

19. El objeto del presente documento es servir como guía para realizar una in**stalación y configuración segura** de los cortafuegos NGFW de Palo Alto Networks, siguiendo como criterio fundamental la **securización del entorno en el que se despliega.**

20. Así, se ofrecen recomendaciones sobre la configuración y casos de uso respecto al despliegue de políticas y perfiles de seguridad, con el fin de maximizar el beneficio de una aproximación integral y multidisciplinar a la prevención de amenazas.

21. Toda la documentación aquí presentada se basa en la **versión 11.1 y superior de PAN-OS**, sistema operativo de los cortafuegos de Palo Alto Networks.

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

23. Los modelos *hardware* y versiones *software* del producto, a los que aplica esta guía son los siguientes:

Serie	*Modelos Hardware*
PA-400	• PA-410, PA-410R y PA-410R-5G • PA-415 y PA-415-5G • PA-440, PA-450 y PA-460 • PA-445 • PA-450R y PA-450R-5G • PA-455 y PA-455-5G
PA-800	• PA-820 • PA-850
PA-1400	• PA-1410 • PA-1420
PA-3200	• PA-3220 • PA-3250 • PA-3260
PA-3400	• PA-3410 • PA-3420 • PA-3430 • PA-3440
PA-5200	• PA-5220 • PA-5250 • PA-5260 • PA-5280

Serie	*Modelos Hardware*
PA-5400	• PA-5410, PA-5420 y PA-5430 • PA-5440 • PA-5445 • PA-5450
PA-7000	• PA-7050 • PA-7080 • PA-7500

Tabla 2: Modelos hardware

24. Y los modelos *software* y versiones del producto, a los que aplica esta guía son los siguientes:

Serie	*Modelos Software (VM)*
VM-Series	• VM-50 • VM-100 • VM-300 • VM-500 • VM-700

Tabla 3: Modelos software (VM)

Notas Serie-VM:

- Todos los modelos se pueden implementar como máquinas virtuales en los siguientes hipervisores: VMware ESXi y vCloud Air, KVM, Microsoft Hyper-V, Cisco ACI, Cisco ENCS y Cisco CSP.
- En entornos de nube pública (Amazon Web Services, Azure, Google Cloud Platform, Oracle Cloud Infrastructure y Alibaba Cloud), se admiten todos los modelos excepto el VM-50.
- Para VMware NSX, solo se admiten los modelos VM-100, VM-300, VM-500 y VM-700.
- En el siguiente enlace encontrará información detallada de los requisitos para los modelos VM:

https://docs.paloaltonetworks.com/vm-series/11-1/vm-series-deployment/license-the-vm-series-firewall/vm-series-models

25. Para conocer el listado, categoría o nivel y familia de los productos descritos en la presente guía consulte el catálogo de productos y servicios STIC (CPSTIC): https://cpstic.ccn.cni.es/es/catalogo-productos-servicios-stic.

3 ORGANIZACIÓN DEL DOCUMENTO

26. El documento está dividido en varios capítulos que cubren los siguientes contenidos:

- Capítulo 1: Incluye una introducción sobre del producto descrito en el documento y una visión acerca de la seguridad actual.
- Capítulo 2: Describe el objeto y alcance del documento y los productos y modelos a los que hace referencia.
- Capítulo 4: Indica los puntos a tener en cuenta en la fase de despliegue e instalación segura de los cortafuegos Palo Alto Networks.
- Capítulo 5: Indica todas las recomendaciones y pasos necesarios para configurar el producto con el objetivo de lograr una configuración segura.
- Capítulo 6: Describe las tareas necesarias para la operación segura de los cortafuegos, que deberán ser incluidas en los procedimientos operativos.
- Capítulo 7: Checklist a rellenar para asegurar el cumplimiento de todas las recomendaciones incluidas en este documento.

4 FASE DE INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

27. Tras la entrega de los dispositivos, es necesario asegurarse que no han sido manipulados, lo que podría suponer un problema de seguridad.

28. Para asegurarse de la autenticidad e integridad de los productos, se siguen estos pasos:

    1. El número de seguimiento, número de pedido y número de serie obtenidos al realizar el pedido, deben coincidir con los incluidos en el producto recibido.

    2. Verificar que el paquete no ha sido dañado durante el transporte y que no tiene signos de haber sido abierto y/o manipulado.

    3. Los productos deben venir debidamente embalados, con su envoltorio sellado.

    4. Si el producto es *software*, se debe descargar únicamente de la página web del portal de cliente de Palo Alto Networks (siguiendo las instrucciones del correo donde se incluyen los códigos de autorización). También se tiene que confirmar el código de integridad (SHA-256) que viene incluido en todas las descargas.

29. Posteriormente, se debe confirmar que el *hardware* y/o versión *software* coinciden con los acordados. Esto se debe confirmar en las etiquetas del producto y/o en la interfaz gráfica del producto (en la pantalla del *dashboard*).

30. Si el producto no tiene instalada la versión de *software* deseada, se puede descargar manualmente desde el portal de cliente de Palo Alto Networks (en este caso se tiene que comprobar manualmente el código SHA-256 de integridad), o se puede arrancar con la versión que tenga y desde la propia interfaz gráfica, descargarla e instalarla, en cuyo caso, el *software* ya realizará automáticamente la comprobación de integridad del *software* descargado.

4.2 ENTORNO SEGURO DE INSTALACIÓN

31. Como norma general, los NGFW de Palo Alto Networks deberán instalarse en un Centro de Proceso de Datos, el cual tendrá un acceso limitado y restringido al conjunto de personas expresamente autorizadas.

32. Se deberá cumplir con las medidas de seguridad física y de seguridad del personal determinadas por la normativa que sea aplicables al sistema en el que se despliegan los equipos.

4.3 REGISTRO Y LICENCIAS

33. Una vez que se ha configurado la gestión del dispositivo, es necesario proceder a su registro a través de la cuenta correspondiente en el portal de soporte (*Customer Support Portal, CSP*). Para ello hay que conectarse al portal de soporte en el siguiente enlace e introducir las credenciales de acceso a la cuenta:

    https://support.paloaltonetworks.com/Support

34. Se puede utilizar una cuenta de soporte en Palo Alto Networks ya existente para acceder al portal. Si no dispone de una cuenta de soporte activa, debería de crear una para poder registrar estos equipos. Para crear una cuenta de soporte, se debe pinchar sobre "*Create Account*", dentro del enlace del portal de soporte, tal y como se puede observar en la imagen.

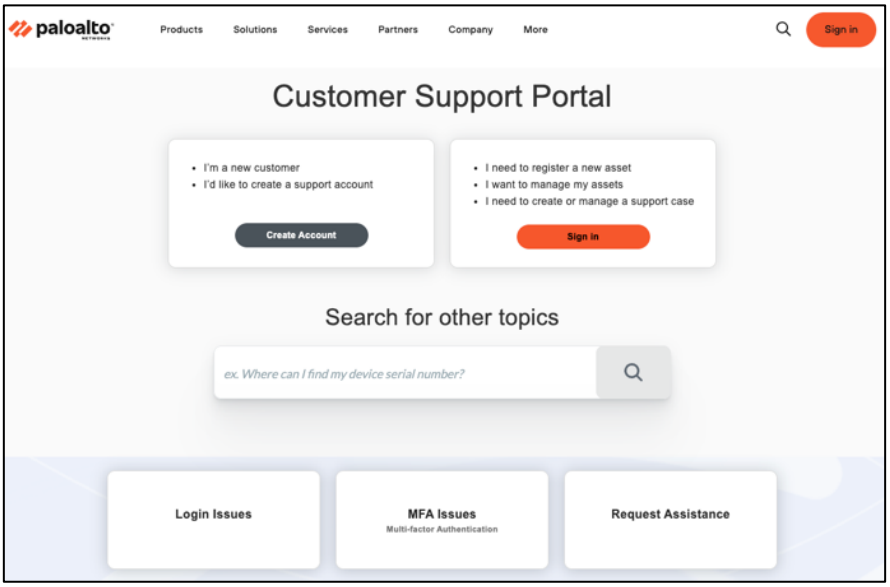


Figura 4-1: Página del portal de soporte (*Customer Support Portal*, CSP)

35. Se ha de rellenar el formulario que nos aparecerá con los datos que nos soliciten.

36. Una vez conectado, seleccionar "*Products > Devices*" y hacer click en "*Register New Device*". Seleccionar "*Register device using Serial Number*" y haga click en "*Next*". Después, añadir el número de serie del cortafuegos (que se puede copiar del *Dashboard* en el interfaz gráfico).

37. Opcionalmente, introducir el "*Device Name*" y el "*Device Tag*", junto con la información de despliegue (Ciudad, Código Postal y País), leer el "*end-user license agreement (EULA)*" y posteriormente hacer click en "*Agree*" y "*Submit*".

38. Una vez que el equipo ha sido registrado, se puede añadir las licencias que hayan sido adquiridas. Para ello, se deben localizar los códigos de licencia que deben haberle llegado vía email. Si no es así, puede contactar con el proveedor para reclamarlas. Puede registrar las licencias siguiendo tres (3) procedimientos diferentes:

1. Registro en el propio portal de soporte. Es el método recomendado porque es el más sencillo. Para ello, hay que añadir los "*Authorization Code*" en la página web donde se registró el equipo. Cuando la gestión del equipo tenga conexión a Internet basta con ir a "*Products > Devices > Licenses*" y hacer click en "*Retrieve license keys from license server*" para que las licencias aparezcan.

2. Activar la funcionalidad usando el "*authorization code*". Solamente se utiliza para los códigos que no hayan sido registrados a través del portal de soporte. Una vez configurada la gestión del equipo para que tenga conexión a Internet, hay que ir a "*Products > Devices > Licenses*" y hacer click en "*Activate feature using authorization code*". Posteriormente se introduce el código de autorización que automáticamente se registrará.

3. Manualmente. Pensada para aquellos equipos que no tienen conexión a Internet. En este caso hay que descargarse un fichero con la clave de la licencia del portal de soporte y después cargarlo en el cortafuegos desde "Products > *Devices > Licenses*" y haciendo click en "*Manually upload license key*".

Nota: En el siguiente enlace encontrará información detallada sobre el registro de equipos: *https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/subscriptions/activate-subscription-licenses*

4.4 CONSIDERACIONES PREVIAS

39. En este apartado se enumeran las tareas básicas que se han de realizar para la puesta en marcha inicial de un dispositivo de Palo Alto Networks.

4.4.1 MODO DE OPERACIÓN SEGURO

40. El dispositivo debe operar en lo que se denominará **modo de operación seguro**. Al habilitarse este modo, se borrarán todas las configuraciones existentes y se establecerán una serie de parámetros de configuración fijos, que cumplen con un nivel base de seguridad.

41. Para habilitar el modo de operación seguro, inicie el cortafuegos en modo de mantenimiento y luego seleccione **Modo FIPS-CC** en el menú principal. El modo de operación seguro (FIPS-CC) proporciona las siguientes características:

    - Restricción de los mecanismos criptográficos a los algoritmos autorizados por la CCN-STIC-807.
    - Roles de usuario Administrador de seguridad, Administrador de auditoría y Administrador criptográfico.
    - Prueba de integridad del *software* y funciones de *auto-test* criptográficas en *Dispositivo> Clave maestra y Diagnóstico*.

Nota: Cuando se habilita el modo de operación seguro (FIPS-CC) el equipo restablece los valores por defecto de fábrica. Toda la configuración previa será borrada.
Para más detalles de cómo habilitar el modo de operación seguro en el equipo, acceder a:

https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/certifications/enable-fips-and-common-criteria-support

4.4.2 INTEGRACIÓN DE LA GESTIÓN EN UNA RED PROTEGIDA

42. En primer lugar, el equipo debe estar integrado en la red de gestión. Esta red debería ser una red fuera de banda de la red de servicio y dedicada exclusivamente a tareas de gestión del equipo.Para ello, tanto los equipos físicos como los virtuales cuentan con recursos de gestión dedicados conectados al *management plane,* diferentes a los de producción, con el fin de evitar que una saturación del plano de datos pueda afectar al de control o viceversa.

Nota: Aunque es posible utilizar un puerto del *dataplane* para realizar la gestión del equipo, se debe utilizar el puerto de gestión dedicado para garantizar la separación de recursos.

43. Toda la configuración puede realizarse a través del interfaz gráfico, por lo que basta con conectarse a la IP de gestión por defecto que traen todos los equipos, 192.168.1.1, a través de un navegador y por HTTPS. El usuario y contraseña por defecto es "admin". La contraseña del usuario "admin" debe ser actualizada en el primer uso, según se indica en el apartado 5.2.3.

44. Una vez conectado, ir a "*Device > Setup > Management*" y configurar los parámetros requeridos. Típicamente se necesitará como mínimo configurar la dirección IP de gestión definitiva, el *gateway*, los DNS y la hora (NTP).

45. Si es posible, la configuración de red debe permitir el acceso a Internet para los servicios de actualización de Palo Alto Networks, que puede realizarse opcionalmente a través de *proxy*. Si no es posible ofrecer conectividad con Internet desde la red de gestión, es posible configurar aquellos servicios que lo requieren a través de un puerto del plano de datos desde "*Device > Setup > Services > Service Route Configuration*".

46. No se debe activar Telnet y HTTP, por no ser protocolos seguros. Asimismo, también es recomendable añadir las IPs desde las que se puede gestionar el equipo a la lista "*Permitted IP Addresses*" para evitar accesos no deseados.

Nota: En el siguiente enlace encontrará información detallada sobre las tareas de configuración inicial:
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/getting-started/integrate-the-firewall-into-your-management-network/perform-initial-configuration

4.4.3 SEGMENTACIÓN EN ZONAS

47. En los cortafuegos de Palo Alto Networks las políticas de seguridad se aplican entre zonas. Una zona es un grupo de interfaces (físicos o virtuales) que representan un segmento de la red a la que se conecta el cortafuegos. Las zonas representan la primera línea de defensa puesto que el tráfico solamente puede fluir entre ellas si hay una regla del cortafuegos que lo permita.

48. Cuanto más granular sea el diseño de las zonas, mayor control se tendrá sobre el tráfico y mejor se evitará el movimiento lateral del *malware*. Es importante tener en cuenta que una zona puede contener un único interfaz o varios, por lo que resultan una agrupación lógica muy interesante para facilitar el control del tráfico.

49. Se **debe, por tanto, planificar cuidadosamente la segmentación en zonas que va a realizar en su red, intentando utilizar como criterio la granularidad**.

50. A modo de ejemplo, el diseño en el que se basa este documento cuenta con cuatro zonas de seguridad, asociadas a cuatro interfaces distintos del cortafuegos: Internet, DMZ, LAN y *Datacenter*.

5 FASE DE CONFIGURACIÓN

5.1 CONFIGURACIÓN DE LA GESTIÓN

51. En este apartado se realizan las recomendaciones para configurar adecuadamente la gestión de los cortafuegos de *Palo Alto Networks*, teniendo siempre como premisa la securización del sistema.

5.1.1 ACCESO

52. **Ubicación**: "*Device > Setup > Management > Management Interface Settings*"

53. **Requisito de seguridad:** Se deben habilitar exclusivamente los protocolos seguros, evitando especialmente Telnet y HTTP. Esta configuración es la que el sistema ofrece por defecto, así que, si no la modifica, la configuración es segura en origen.

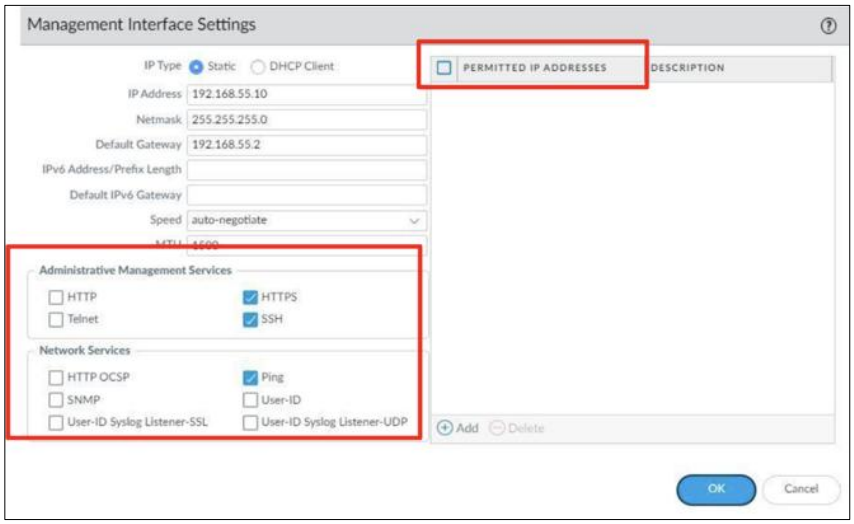


Figura 5-1: Configuración del acceso a la gestión

54. Se debe configurar, del mismo modo, la lista de direcciones IP permitidas, de modo que solamente las IPs o redes de administradores válidos puedan tener acceso al sistema.

55. Esta configuración debe hacerse extensible si se habilita la gestión en el plano de datos (*dataplane*), dentro de *"Network Interface Mgmt"*. En este sentido, es importante señalar que se debe utilizar la gestión dedicada del *management plane,* siempre que sea posible. Si se necesita cambiar algún servicio de gestión a un interfaz del dataplane puede hacerlo desde "*Device > Setup > Services > Service Route Configuration".*

5.1.2 BANNER DE CONEXIÓN

56. **Ubicación**: "*Device > Setup > Management > General Settings*"

57. **Requisito de seguridad:** Se debe configurar un *banner* de conexión a la gestión, idealmente proporcionado por el departamento legal, que informe a usuarios de que acceden a un sistema sobre el que no tienen permisos de gestión y que se podrán tomar las oportunas medidas legales en caso de acceso no autorizado.

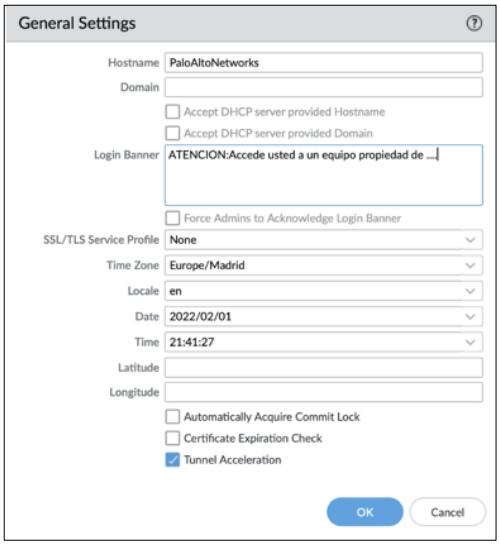


Figura 5-2: Configuración de un banner de acceso a la gestión

5.1.3 REQUISITOS MÍNIMOS DE CONTRASEÑA

58. **Ubicación**: "*Device > Setup > Management > Minimum Password Complexity*"

59. **Requisito de seguridad:** Se debe habilitar la utilización de una política de contraseñas con una complejidad mínima. La siguiente figura muestra una configuración tipo, que se puede ajustar a los requisitos de su organización.

Figura 5-3: Configuración de la complejidad de las contraseñas de gestión

Nota: preferible utilizar "*Minimum Password Complexity*" a "*Password Profiles*" porque es más seguro. No obstante, si utiliza ambos, verifique que los datos comunes de ambas configuraciones están en consonancia.

60. Se deberán seguirse las siguientes directrices y opciones de configuración:

- No deberá permitirse la repetición de al menos las 5 últimas contraseñas utilizadas (parámetro *Prevent Password Reused Limit*).

- No deberá realizarse un nuevo cambio de contraseña en los 4 días posteriores al último cambio (parámetro *Block Password Change Period*).

- Deberán ser de 12 caracteres como mínimo, aunque se recomienda una longitud de 15 caracteres (parámetro *Minimum Length*).

- Deberán incluir caracteres alfanuméricos y caracteres especiales como "!","@", "#", "$", "%", "^", "&", "*", "(" y ")", al menos una letra en mayúscula y otra en minúscula, un número o más, y un signo de puntuación o más (parámetro *Minimum Uppercase Letters, Minimun Lowercase Letters* y *Minimun Special Characters*).

- Deberán contener un número mínimo de juegos de caracteres o de cambios en el juego de caracteres (parámetro *New Password Differs By Characters*).

- El valor recomendado para la vigencia y expiración de contraseñas es de 30 días (parámetro *Required Password Change Period*).

5.1.4 CAMBIAR USUARIO Y CONTRASEÑA POR DEFECTO

61. **Ubicación**: "*Device > Administrators*"

62. **Requisito de seguridad:** Cambiar el nombre de usuario y la contraseña del usuario por defecto del equipo, "admin/admin". Como se verá en el siguiente punto, este usuario es recomendable mantenerlo en local, como backup de otros administradores y se debe seleccionar una contraseña con una fortaleza adecuada, que cumpla, como mínimo, con los requisitos establecidos en el punto anterior.

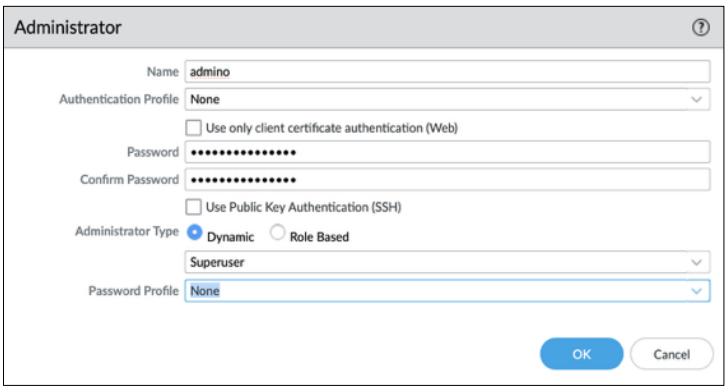


Figura 5-4: Cambio del usuario/contraseña de administración por defecto

5.1.5 CONFIGURAR OTRAS CUENTAS DE ADMINISTRACIÓN

63. Se recomienda crear usuarios de administración que tengan perfiles de autenticación basados en sistemas externos, como LDAP o Radius, para todas las cuentas salvo una, que se mantendrá local y que tendrá una configuración de contraseña especialmente segura, para garantizar el acceso al equipo si los sistemas externos de autenticación fallan.

64. Si se desea restringir los permisos que un determinado administrador tiene, es posible utilizar un rol entre los predefinidos, con menor nivel de privilegios, o configurar un rol personalizado con las capacidades específicas que se quieren otorgar desde "*Device > Admin Roles*".

Nota: En el siguiente enlace encontrará información detallada sobre la configuración de roles:
https://docs.paloaltonetworks.com/ngfw/administration/firewall-administration/manage-firewall-administrators/configure-an-admin-role-profile

65. La siguiente imagen muestra un ejemplo en el que el usuario "*admino*", creado en el punto anterior, es local, mientras que "*jdiaz*" y "*jlgomez*" utilizan perfiles de autenticación basados en LDAP. El usuario "admino" ha de intentar no utilizarse salvo en ocasiones en las que el acceso vía LDAP no sea posible.

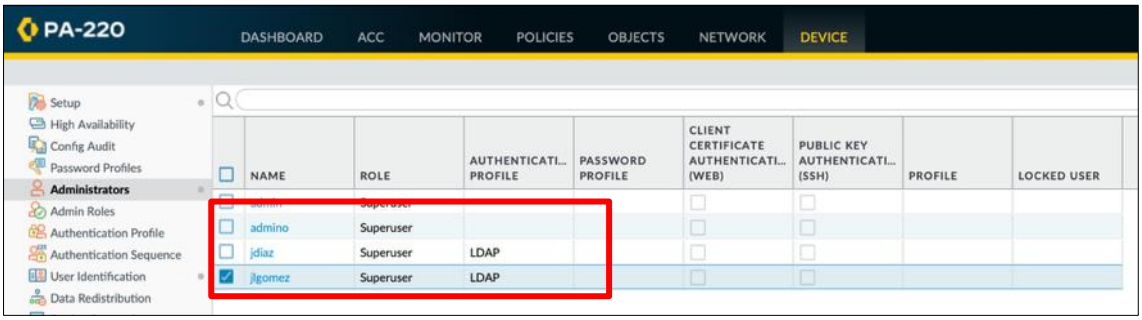


Figura 5-5: Perfiles de autenticación de los administradores

66. Para los perfiles de autenticación externa se debe configurar, desde *Device > Authentication Profile*, el umbral de intentos fallidos de autenticación, tras lo cual, el usuario quedará bloqueado un tiempo (*lockout time*).

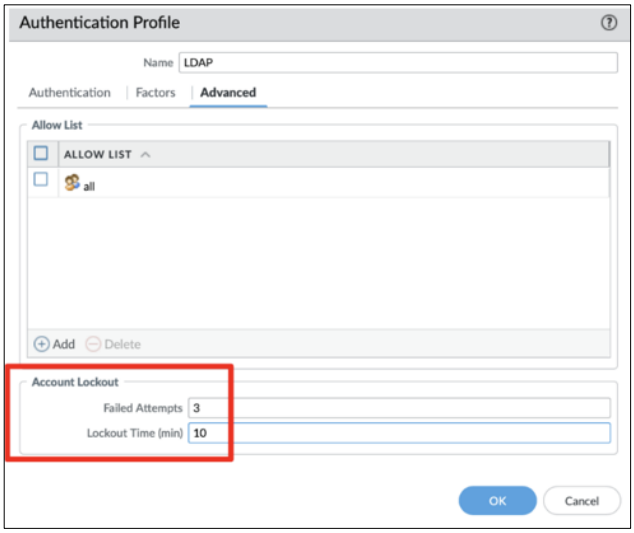


Figura 5-6: Configuración de la autenticación externa de administradores

67. No se recomienda configurar estos parámetros para el administrador local, con objeto de evitar que la cuenta local pueda bloquearse.

68. Finalmente, en todos los casos debe configurarse el *timeout* de inactividad, transcurrido el cual, la sesión será automáticamente desconectada.

69. El tiempo máximo (en minutos) sin actividad puede ser configurado en un rango de 0 a 1440 minutos (por defecto está configurado el valor de 60). Si se configura a 0, esta funcionalidad se deshabilita.

70. El número máximo de intentos fallidos de autenticación (*Failed attempts*) no debería ser superior a 5 intentos.

71. **Ubicación**: "*Device > Setup > Management > Authentication Settings*"

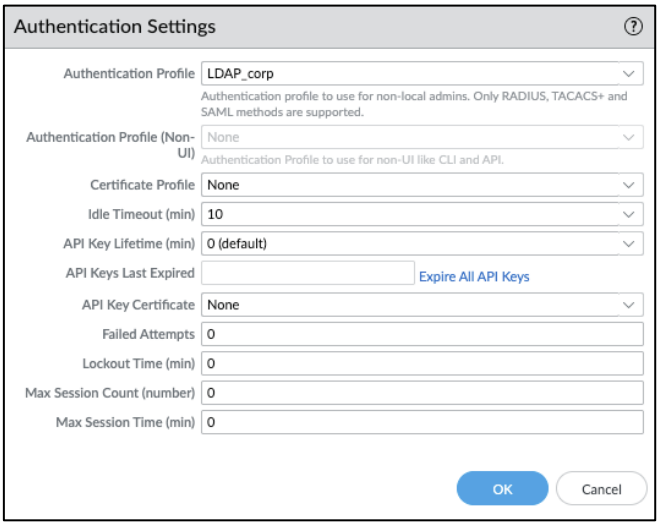


Figura 5-7: Configuración del acceso a la gestión de la cuenta local

72. El Administrador de seguridad puede revocar los privilegios de administrador de cualquiera de las siguientes maneras:

    - Eliminar la cuenta del usuario completamente, navegando a "*Device > Administrators*", seleccionando el usuario administrador y haciendo clic en "Eliminar".

    - Cambiar la función del administrador, navegando a "*Device > Administrators*", seleccionando el usuario administrador y seleccionando un perfil con menos privilegios.

5.1.6 SEGURIDAD PARA SNMP

73. **Ubicación**: "*Device > Setup > Operations > SNMP Setup*"

74. **Requisito de seguridad:** Si es requerido, se debe utilizar SNMPv3, que es significativamente más seguro que SNMPv2c.

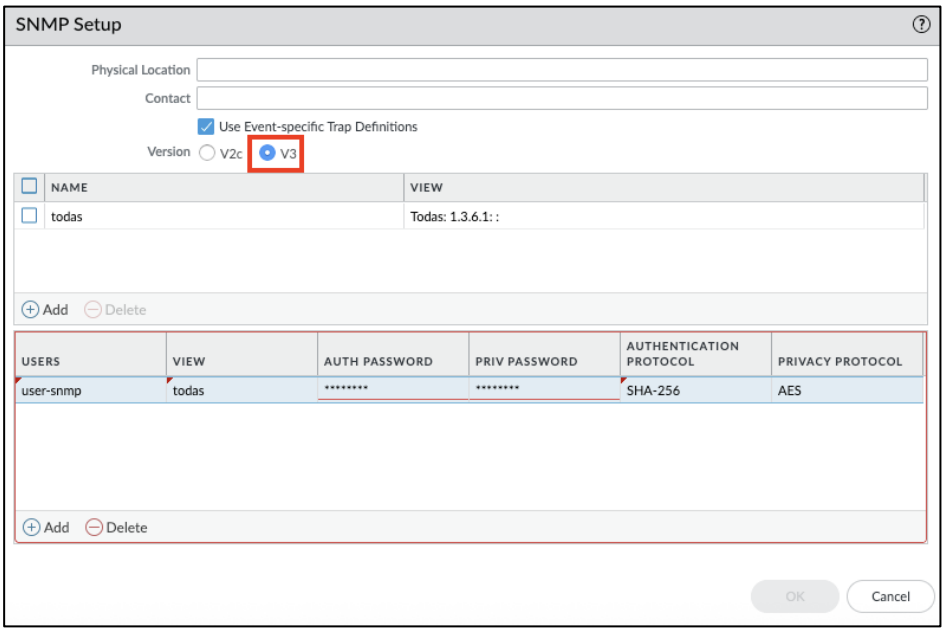


Figura 5-8: Configuración SNMPv3

Nota: Puede encontrar información detallada sobre la configuración de SNMPv3 en el siguiente enlace:
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClHOCA0

5.1.7 SEGURIDAD DE ACTUALIZACIONES Y UPDATES

5.1.7.1 UPDATES DE SERVICIOS

75. **Ubicación**: "*Device > Setup > Services > Services*"

76. **Recomendación:** Active la verificación de los servicios de actualización para evitar contenidos fraudulentos. Tenga en cuenta que, si la conexión es a través de un proxy para SSL, es posible que tenga que deshabilitar esta opción para que el servicio funcione adecuadamente.

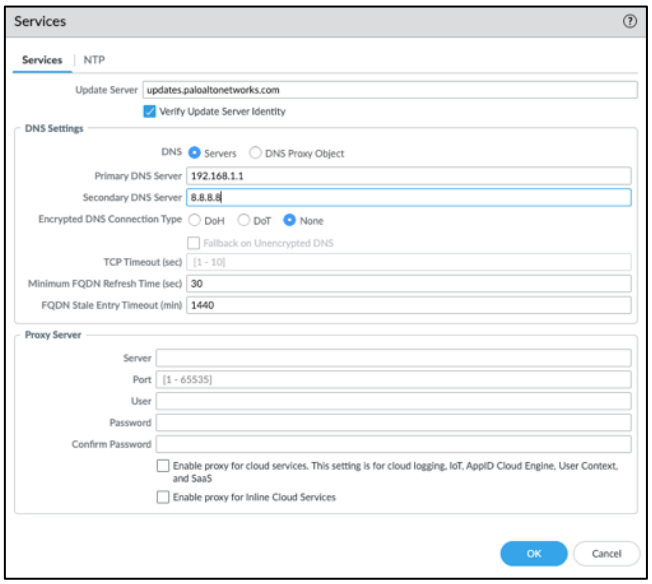


Figura 5-9: Validación de los servidores de actualización

5.1.7.2 UPDATES DE APLICACIONES Y AMENAZAS

77. **Ubicación:** "*Device > Dynamic Updates > Applications and Threats > Update Schedule*"

78. **Recomendación:** Programar las actualizaciones para que se descarguen e instalen diariamente, para estar seguro de que cuenta con las últimas definiciones. Si se desea minimizar el impacto de un posible error en alguna firma, se puede forzar a que la instalación de cualquier contenido tenga una determinada antigüedad, a través del campo "*Threshold* (*hours*)".

79. Como prevención adicional, es posible retrasar la instalación de las nuevas actualizaciones de contenidos que contienen nuevos APP-IDs:

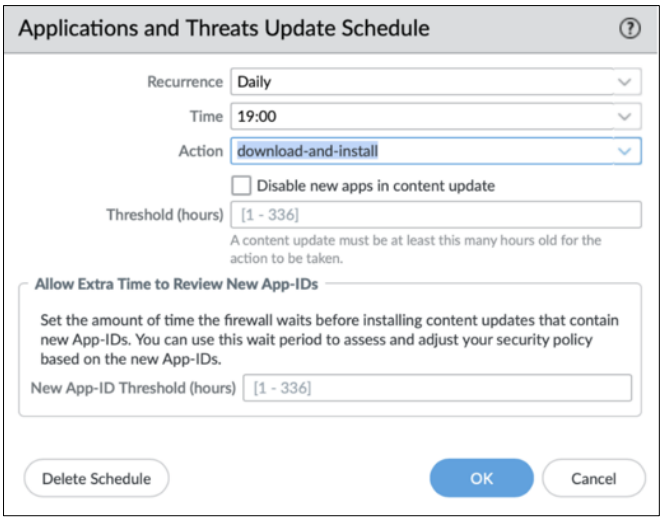


Figura 5-10: Programación de updates de Aplicaciones y Amenazas

5.1.7.3 UPDATES DE ANTIVIRUS

80. **Ubicación**: "*Device > Dynamic Updates > Antivirus > Antivirus Update Schedule*"

81. **Recomendación**: Programar las actualizaciones para que se descarguen e instalen cada hora para estar seguro de que cuenta con las últimas definiciones. Si se desea minimizar el impacto de un posible error en alguna firma, se puede forzar a que la instalación de cualquier contenido tenga una determinada antigüedad, a través del campo "*Threshold (hours)*".

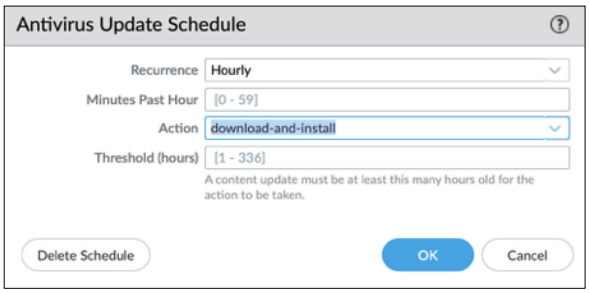


Figura 5-11: Programación de updates de Antivirus

5.1.7.4 UPDATES DE WILDFIRE

82. **Ubicación:** "*Device > Dynamic Updates > WildFire > WildFire Update Schedule*"

83. **Recomendación:** Programar las actualizaciones para que se descarguen e instalen en tiempo real para estar seguro de que cuenta con las últimas definiciones, recibiendo estas de manera inmediatas.

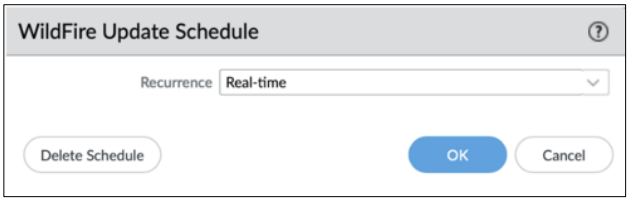


Figura 5-12: Programación de updates de WildFire

5.1.8 CONFIGURACIÓN NTP

84. **Ubicación**: "*Device > Setup > Services > NTP*"

85. **Recomendación**: Configurar dos servidores NTP para garantizar la disponibilidad del servicio. En caso de usar autenticación con clave simétrica utilice SHA1.

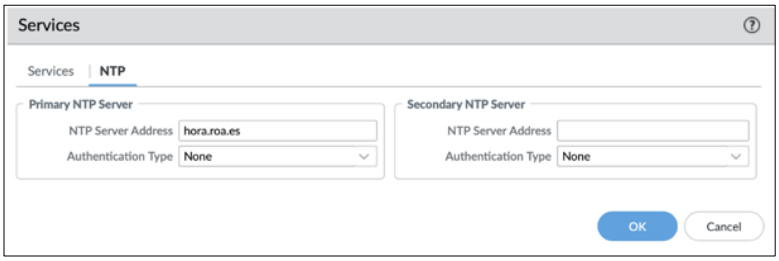


Figura 5-13: Configuración redundada de NTP

5.2 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

5.2.1 IKE/IPSEC

86. IPsec (*Internet Protocol security*) es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado (IKE).

87. En esta guía, los protocolos IKE/IPSEC se utilizan para establecer VPNs entre dos puntos, los cuales podrían ser dos dispositivos de red (*site to site*) o un dispositivo final y un equipo de red (*client to site*).

88. Los parámetros recomendados en este apartado cumplen con los requisitos establecidos en la guía *CCN-STIC-807 Criptología de empleo en el Esquema Nacional de Seguridad.*

5.2.1.1 PERFIL CRIPTOGRÁFICO IKE

89. En primer lugar, es necesario configurar los parámetros en el perfil IKE y posteriormente, crear el IKE *peer*, en el cual se indica la versión del protocolo a usar, la IP del equipo con el que se establecerá el túnel y la forma de autenticar esta fase.

90. **Ubicación**: "*Network > Network Profiles > IKE Crypto*"

91. **Requisito de seguridad**: **Se deben seleccionar los siguientes parámetros:**

- ***IKE DH Group*: Grupo 19 / Grupo 20**
- ***Encryption*: AES-128-cbc / AES-256-cbc**
- ***Authentication:* SHA256 / SHA384 / SHA512**
- Key Lifetime: 8 horas

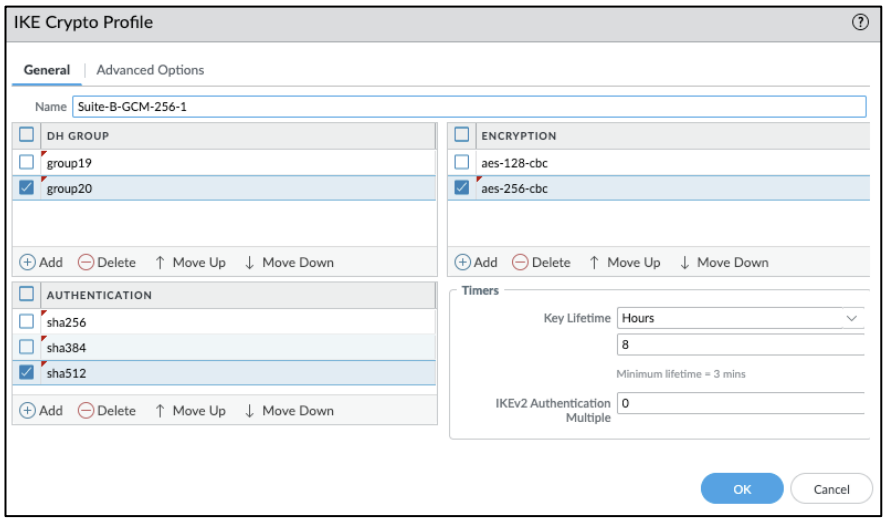


Figura 5-14: Configuración IKE Crypto Profile

92. **Ubicación**: "*Network > Network Profiles > IKE Gateways*"

93. **Requisito de seguridad**: Se deben seleccionar los siguientes parámetros:

    - *Vesion*: IKEv2 only mode
    - *Authentication*: Certificate (no se recomienda el uso de claves pre-compartidas)
    - Advanced options:
        i. *IKE Crypto Profile*: IKESecure (el perfil creado anteriormente)

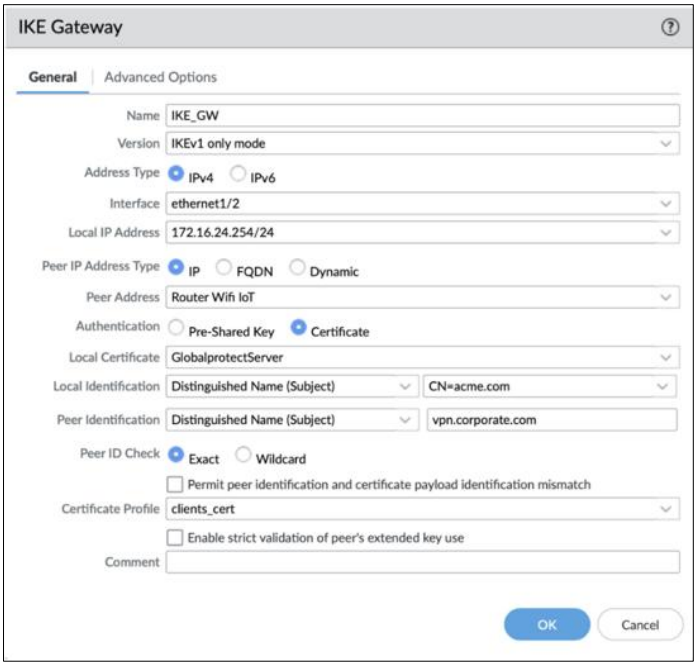


Figura 5-15: Configuración IKE Gateway (General)

94. Para la autenticación con certificado, se recomienda utilizar el campo CN en ambos extremos y habilitar la extensión "*Extended Key Use*".

95. El certificado a utilizar en este punto (importándolo o generándolo directamente en la CA integrada) debe utilizar claves RSA o ECDSA de, al menos, la siguiente longitud:

    - RSA ≥ 3072 bits
    - ECDSA ≥ 256 bits

96. Por último, se asocia el *IKE peer* con el *IKE Crypto profile* creado anteriormente en la pestaña de "*Advanced Options*":

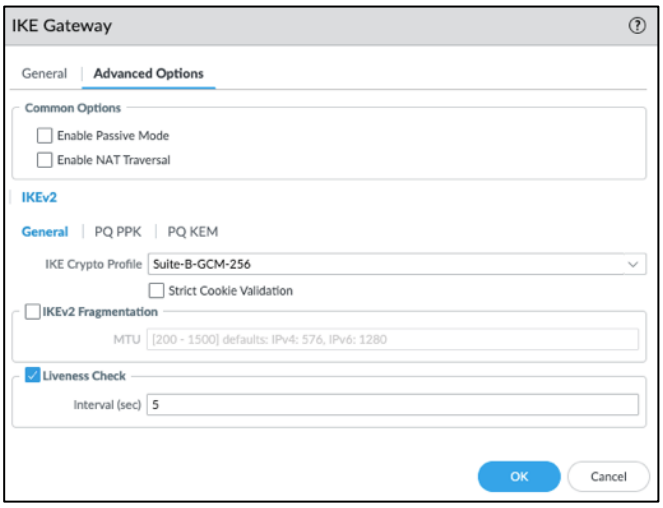


Figura 5-16: Configuración IKE Gateway (Advanced)

97. Opcionalmente se puede configurar el perfil IKE para soportar ataques basados en computación cuántica (*Quantum Computing*) o *QC*. Para ello, los cortafuegos de Palo Alto Networks, a partir de su version PAN-OS 11.1 soportan algoritmos de criptografía post-cuántica (*Post-Quantum Cryptography*) o también conocido por su siglas *PQC*.

98. Esta configuración se puede establecer en la pestaña de "*Advanced Options > PQ PPK*"

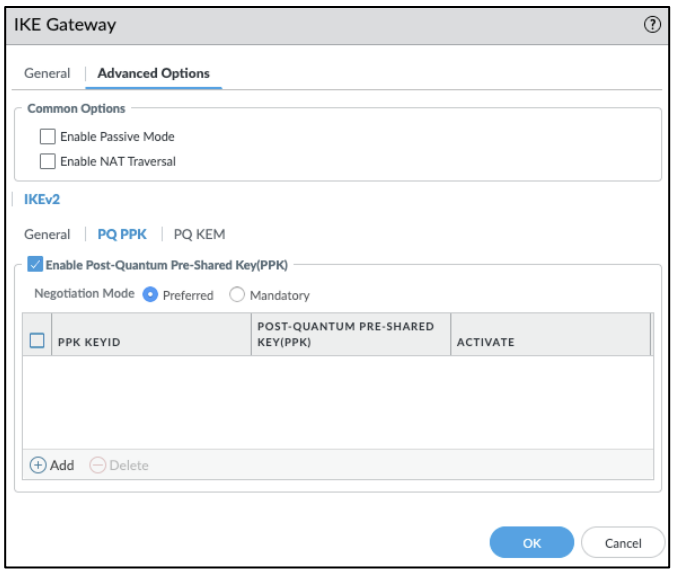


Figura 5-17: Configuración IKE Gateway (*Post-Quantum Cryptography*)

5.2.1.2 PERFIL CRIPTOGRÁFICO IPSEC

99. **Ubicación**: "*Network > Network Profiles > IPSec Crypto*"

100. Requisito de seguridad: Se debe seleccionar los siguientes parámetros:

- **IPSEC Protocol: ESP**
- **DH *Group*: Grupo 19 o Grupo 20**
- ***Encryption*: AES-256-gcm / AES-256-cbc**

- ***Authentication*: SHA256 / SHA384 / SHA512**
- *Lifetime*: 1 hora

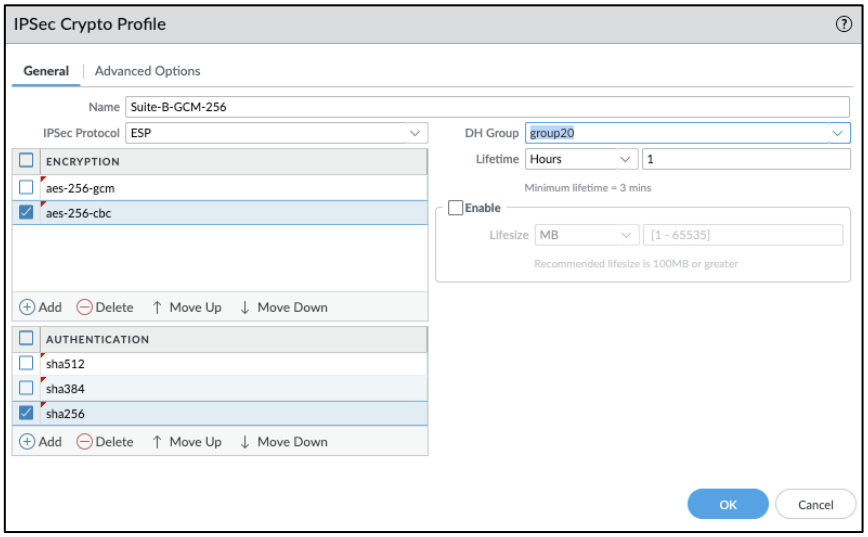


Figura 5-18: Configuración IPSec Crypto Profile

101. En el apartado 5.11.2 se muestra un ejemplo completo de configuración de una VPN.

5.2.2 TLS/HTTPS

102. Los cortafuegos Palo Alto Networks utilizan TLS para las siguientes funciones:

- Administración del equipo.
- Gestión de actualizaciones (contenido, versión).
- Comunicación con Palo Alto *Cloud services* (como, por ejemplo, *WildFire*).
- Comunicación con la consola de gestión Panorama.
- Reenvío de logs a equipos externos.
- Servicios de autenticación.
- VPNs GlobalProtect.

103. **Ubicación**: "*Device > Certificate Management > SSL/TLS Service Profile*"

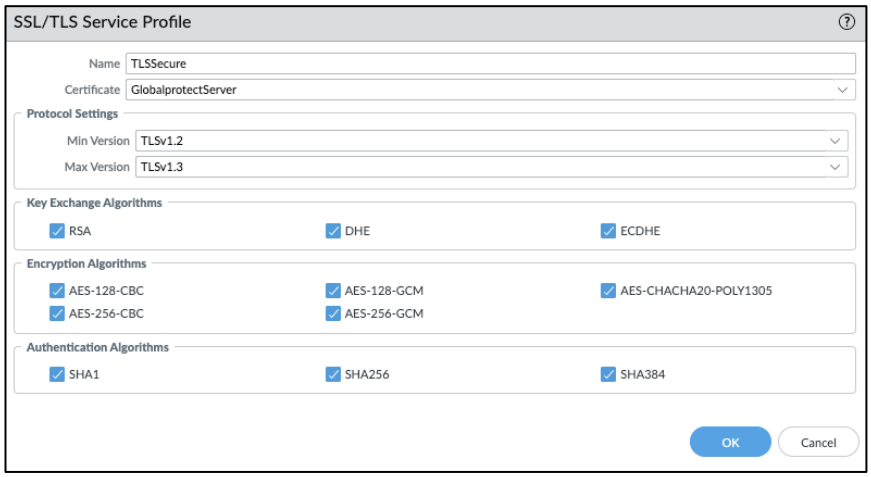


Figura 5-19: Configuración SSL/TLS Service Profile

104. **Requisito de seguridad**: Se debe seleccionar la versión mínima TLSv1.2 o TLSv1.3. Con relación al uso de SHA1 y DHE como algoritmos de autenticación e intercambio de clave respectivamente, el sistema permite su uso, aunque se recomienda la desactivación de éstos y configurar algoritmos más robustos como ECDHE o SHA256 respectivamente, o en su defecto las recomendaciones de la guía CCN STIC 807.

105. El certificado a utilizar en este punto (importándolo o generándolo directamente en la CA integrada) debe utilizar claves RSA o ECDSA de, al menos, la siguiente longitud (ver apartado 5.4):
    - **RSA ≥3072 bits**
    - **ECDSA ≥256 bits**

5.3 CONFIGURACIÓN DE PROTOCOLOS NO SEGUROS

106. Los protocolos no seguros como pueden ser Telnet, HTTP, FTP, etc., deben ser deshabilitados para evitar su uso.

107. La configuración de los protocolos de gestión se realiza desde los perfiles de gestión, los cuales se asignan a los interfaces que están en modo "*Layer 3*".

108. **Ubicación**: "*Network > Network Profiles > Interface Mgmt*"

109. **Requisito de seguridad**: Se deben deshabilitar todos los protocolos no seguros. Estos perfiles de interfaces de gestión solo se recomienda configurarlos en zonas de confianza. En el caso de SNMP, habilitarlo sólo si es necesario.

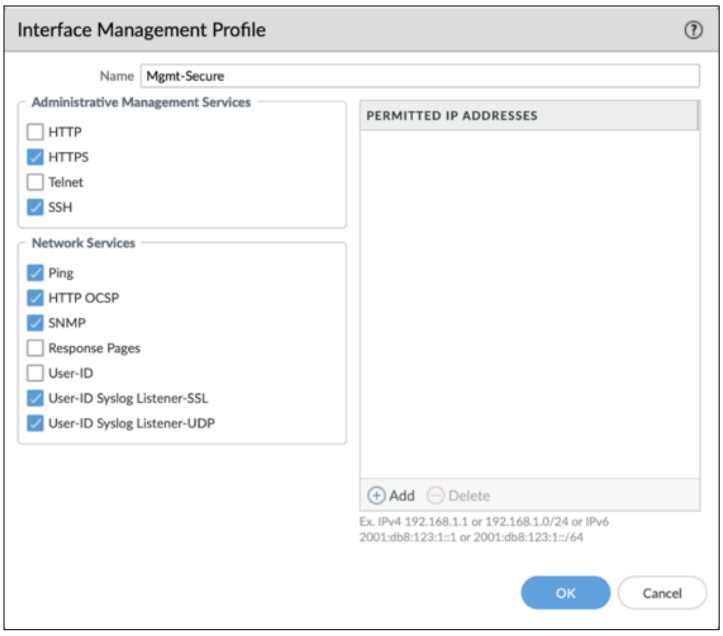


Figura 5-20: Configuración Perfil interfaz de gestión

5.4 GESTIÓN DE CERTIFICADOS

110. Los cortafuegos de Palo Alto Networks emplean diferentes métodos para obtener certificados.

5.4.1 CREAR UN CERTIFICADO DE CA RAÍZ AUTOFIRMADO

111. Un certificado de CA (*Certificate Authority*) autofirmado, es el certificado más importante en una cadena de certificados. Un cortafuegos puede usar este certificado para emitir automáticamente certificados para otros usos. Por ejemplo, el cortafuegos emite certificados para el descifrado SSL/TLS y para satélites en una VPN a gran escala GlobalProtect.

112. Para generar un certificado autofirmado CA:

113. **Ubicación**: "*Device > Certificate Management > Certificates > Device Certificates > Generate*"

114. **Requisito de seguridad**: El certificado debe utilizar claves RSA o ECDSA de, al menos, la siguiente longitud:
    - RSA ≥3072 bits
    - ECDSA ≥256 bits

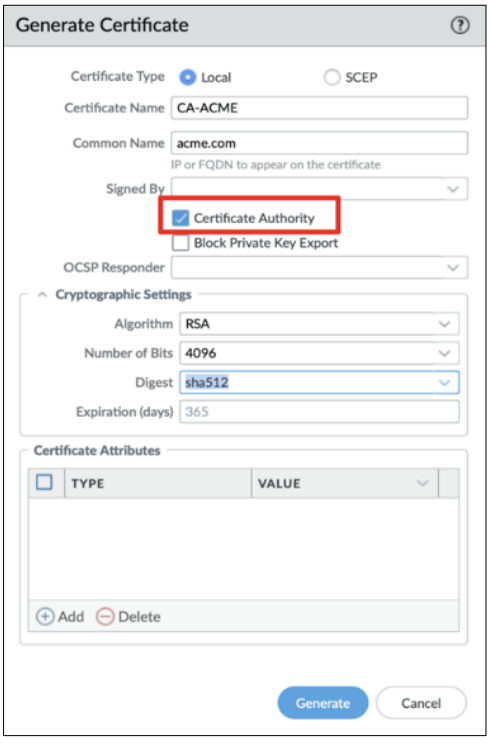


Figura 5-21: Crear un certificado CA autofirmado

115. La opción *Agregar (Add)* en los atributos del certificado, puede seleccionarse para identificar con mayor detalle características del cortafuegos, como Organización, Unidad organizativa o País.

5.4.2 GENERAR UN CERTIFICADO

116. Los cortafuegos de Palo Alto Networks usan certificados para autenticar clientes, servidores, usuarios y dispositivos en varias aplicaciones, incluyendo *Captive Portal, GlobalProtect, VPN IPSec* de *site to site* y acceso de interfaz web al cortafuegos / Panorama.

117. **Ubicación**: "*Device > Certificate Management > Certificate > Device Certificates > Generate*"

118. **Requisito de seguridad**: El certificado debe utilizar claves RSA o ECDSA de, al menos, la siguiente longitud:
    - RSA ≥3072 bits
    - ECDSA ≥256 bits

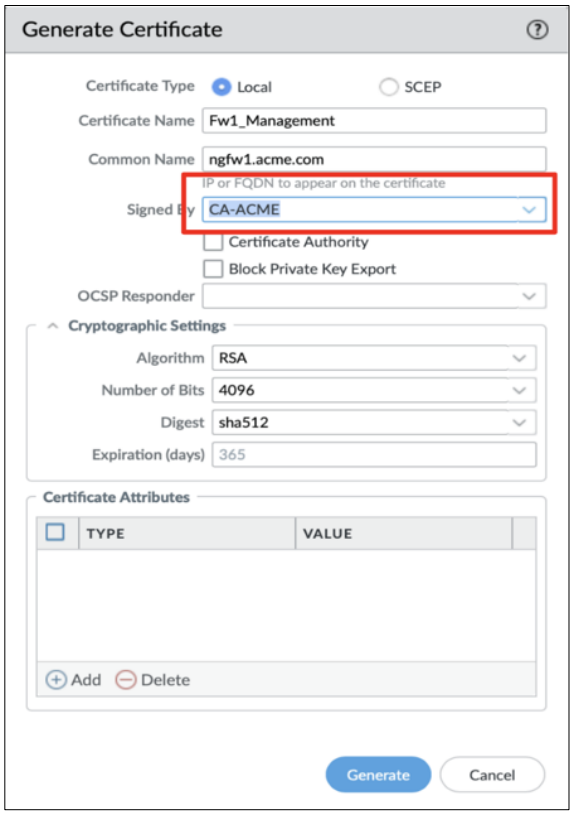


Figura 5-22: Generar un certificado firmado por la CA interna del cortafuegos

119. En el campo Nombre común, se ingresa el FQDN (recomendado) o la dirección IP de la interfaz, donde se configura el servicio que usará este certificado. La opción *Agregar (Add)* en los atributos del certificado puede seleccionarse para identificar con mayor detalle las características cortafuegos, como Organización, Unidad organizativa o País.

120. El certificado se genera y la clave privada se almacena cifrada utilizando AES.

5.4.3 IMPORTAR UN CERTIFICADO Y UNA CLAVE PRIVADA

121. Si la empresa tiene su propia infraestructura de clave pública (PKI), lo ideal es importar un certificado y una clave privada al cortafuegos, desde la autoridad de certificación de la empresa (CA).

122. Para obtener un certificado de una CA externa, se debe generar una solicitud de firma de certificado (CSR) y enviar a la CA. Después de que la CA emita un certificado con los atributos especificados, se debe importar en el cortafuegos. La CA puede ser una CA pública o una CA de empresa.

123. **Ubicación**: "*Device > Certificate Management > Certificate > Device Certificates > Import*"

124. **Requisito de seguridad**: El certificado debe utilizar claves RSA o ECDSA de, al menos, la siguiente longitud:
    - RSA ≥3072 bits
    - ECDSA ≥256 bits

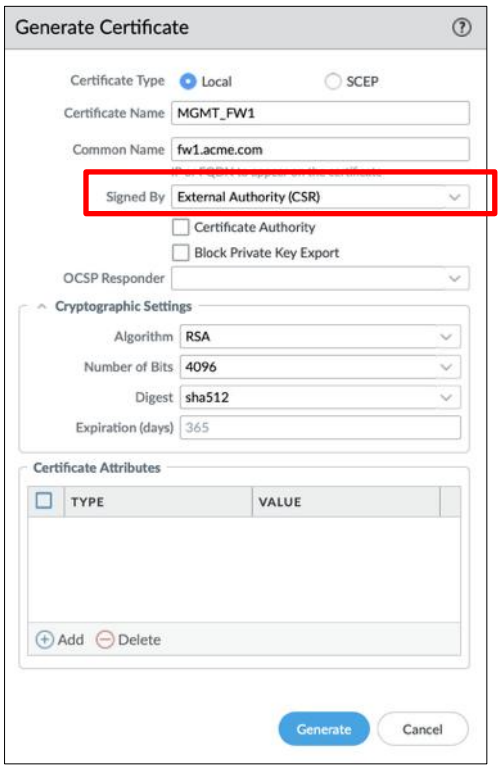


Figura 5-23: Generar una solicitud de firma de certificado (CSR)

125. Una vez generado, aparece con un estado de "*Pending*" hasta que sea firmado por la CA.

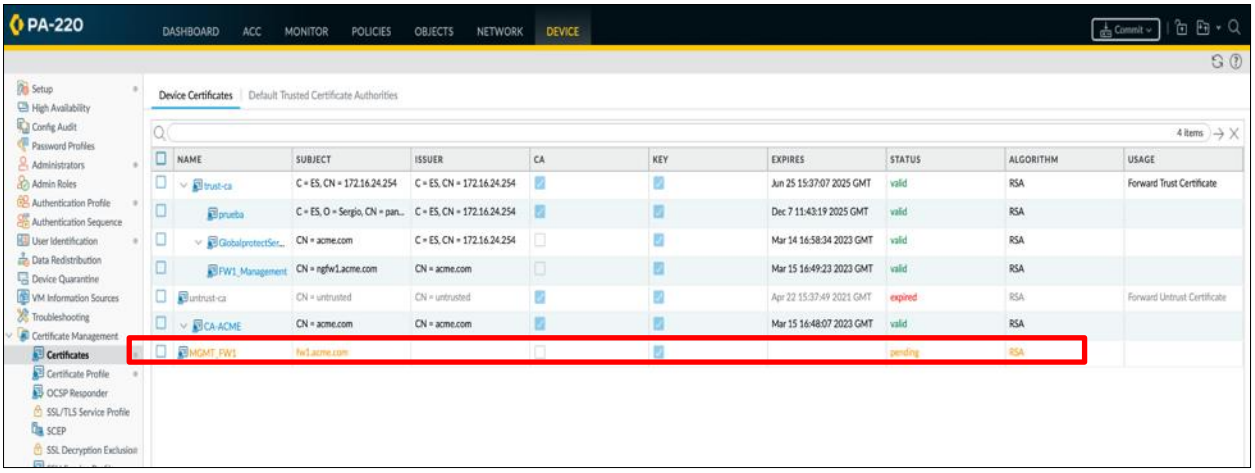


Figura 5-24: Visualización de certificado pendiente de firma por la CA

126. Para ello, se exporta en formato CSR y una vez firmado por la CA, se volvería a importar indicando la contraseña definida.

5.4.4 COMPROBACIÓN *ONLINE* DE VALIDEZ DE CERTIFICADOS

127. Los cortafuegos Palo Alto Networks soportan validación online de la validez de los certificados mediante el uso de CRL y OSCP.

128. La configuración de estas opciones se realizará desde los perfiles de certificados:

129. **Ubicación**: "*Device > Certificate Management > Certificate Profile*"

130. **Requisito de seguridad**: Se deben utilizar las siguientes opciones:

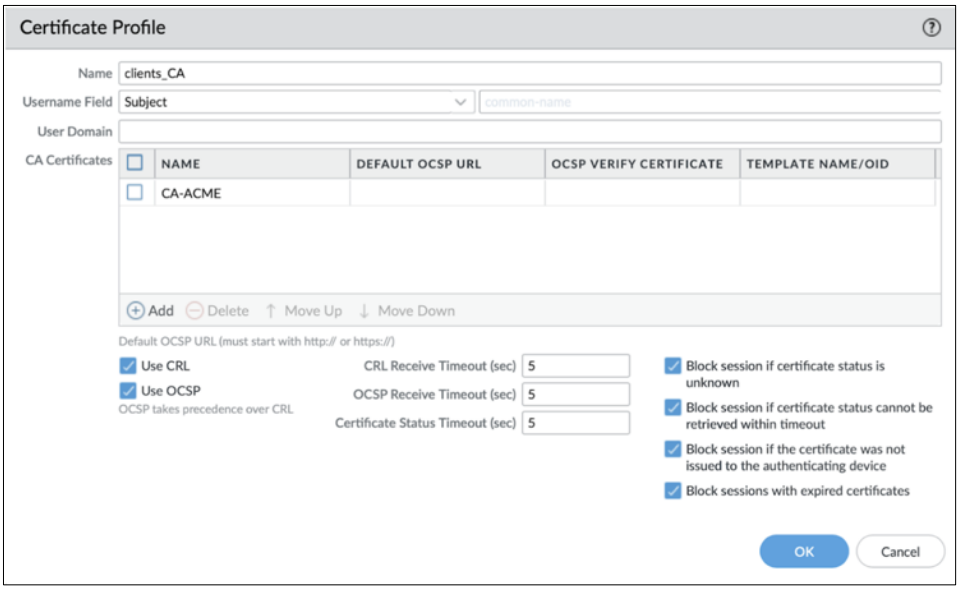


Figura 5-25: Configuración de perfil de certificado con OSCP / CRL

5.4.5 CONFIGURACIÓN DE LA CADENA DE VALIDACIÓN DE CERTIFICADOS

131. **Ubicación**: "*Device > Certificate Management > Certificates > Default Trusted Certificate Authorities*"

132. Use esta página para ver, deshabilitar o exportar las autoridades de certificación (CA) en las que confía el cortafuegos.

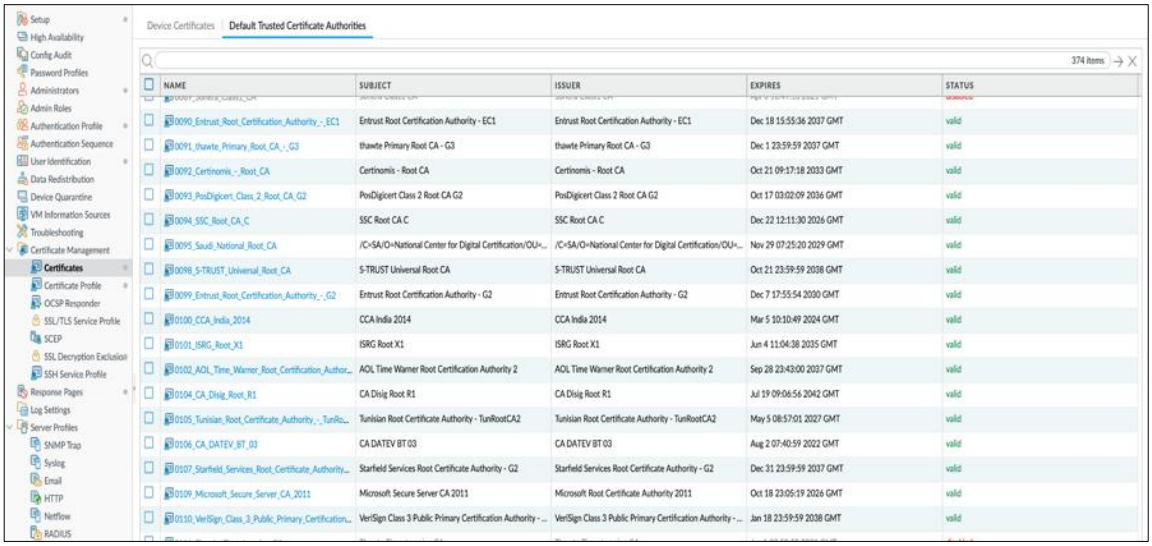


Figura 5-26: Lista preinstalada de certificados de confianza

133. La lista preinstalada de CAs, incluye a los proveedores de certificados más comunes y confiables, responsables de emitir los certificados que el cortafuegos requiere para asegurar las conexiones a Internet. Para cada CA raíz de confianza, se muestra el nombre, el asunto, el emisor, la fecha de vencimiento y el estado de validez.

134. El cortafuegos no confía en las CA intermedias de forma predeterminada, porque las CA intermedias no forman parte de la cadena de confianza entre el cortafuegos y la CA raíz de confianza.

135. Debe agregar manualmente las CA intermedias en las que desea que confíe el cortafuegos, junto con las CA empresariales de confianza adicionales que su organización requiera.

5.5 SERVIDOR DE AUTENTICACIÓN (*AAA SERVER*)

136. Los cortafuegos Palo Alto Networks permiten autenticar usuarios con servidores externos como RADIUS, LDAP, SAML, Kerberos, etc.

137. Para realizar la configuración se debe crear un servidor de autenticación con los datos de conexión, posteriormente un perfil de autenticación donde se definen el resto de las características y, por último, asignarlo a los servicios donde se desee aplicar.

138. Como ejemplo, se muestra cómo configurar un servidor RADIUS para autenticar la administración del equipo.

139. **Ubicación**: *"Device > Server Profiles > RADIUS"*

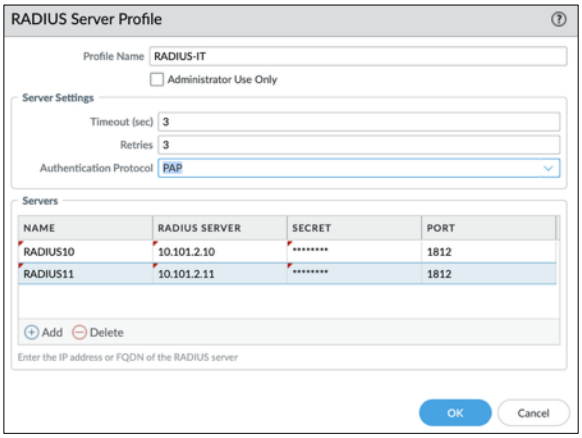


Figura 5-27: Configuración del RADIUS Server

140. **Ubicación**: "*Device > Authentication Profile*"

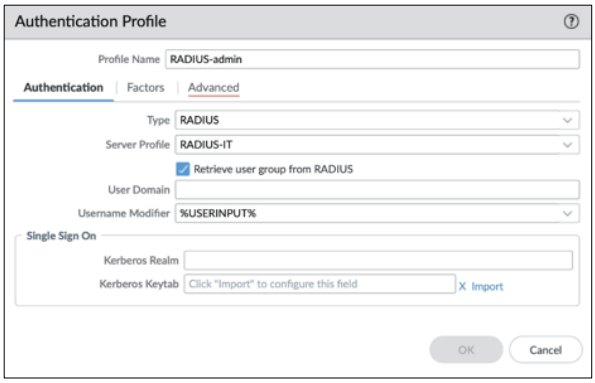


Figura 5-28: Configuración del perfil de autenticación

141. **Requisito de seguridad**: Siempre que sea posible, se deben restringir los usuarios que se pueden autenticar (*Allow List*).

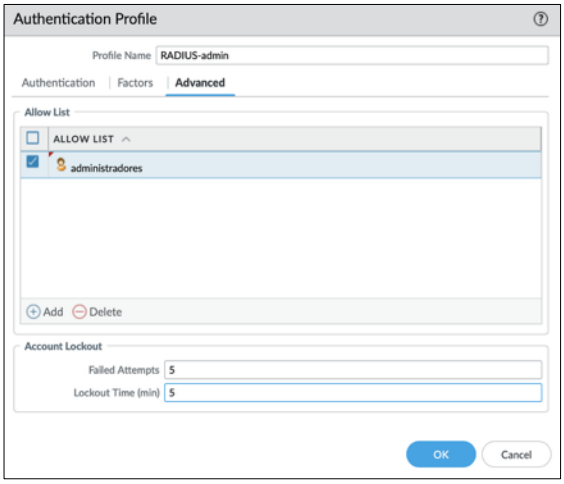


Figura 5-29: Configuración del perfil de autenticación (*advanced*)

142. **Recomendación**: Siempre que sea posible, se debe utilizar doble factor de autenticación.

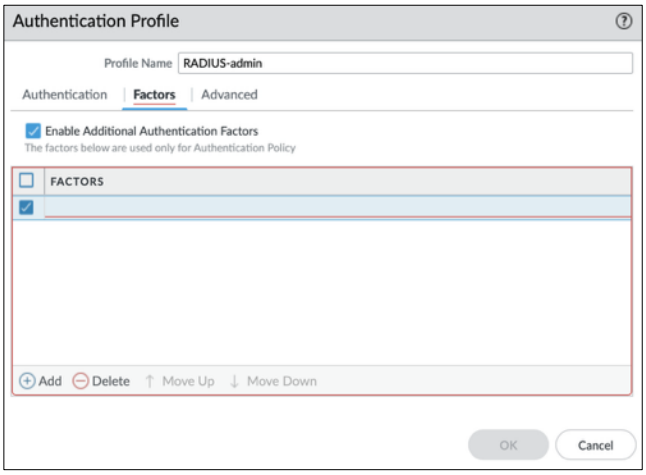


Figura 5-30: Configuración del perfil de autenticación (*factors*)

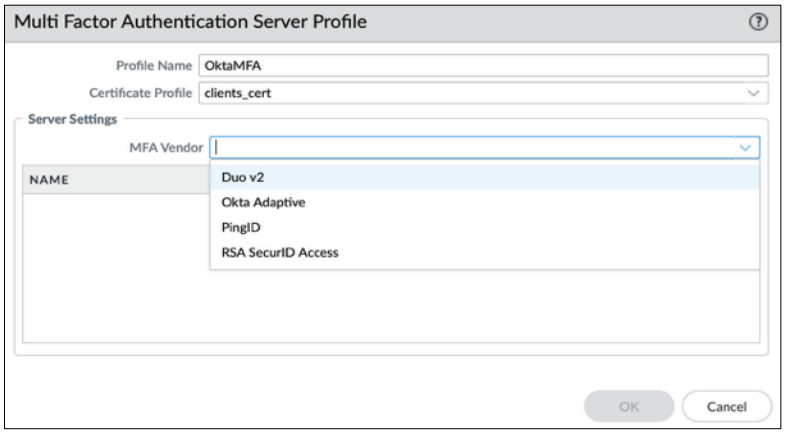


Figura 5-31: Configuración del perfil MFA

5.6 ACTUALIZACIONES

143. Para garantizar que los equipos están al día, tanto en las capacidades de reconocimiento de aplicaciones, como en la de prevención de amenazas, es importante que se encuentren actualizados.

144. Antes de actualizar el *firmware* es recomendable actualizar primero el contenido. Por defecto el cortafuegos accede a *https://updates.paloaltonetworks.com*, que se sirve desde una infraestructura CDN. Si es necesario ofrecer acceso a un host o una IP estática, entonces puede utilizarse *https://staticupdates.paloaltonetworks.com* o la IP 199.167.52.15. Esta configuración se encuentra en "*Device > Setup > Services*".

145. Para descargar manualmente las últimas actualizaciones disponibles, seleccionar "*Device > Dynamic Updates*" y haga click en "*Check Now*". En primer lugar, se debe instalar las actualizaciones de las aplicaciones y posteriormente el resto.

146. Una vez que los contenidos ya han sido actualizados, se puede proceder a la actualización del *firmware* a la versión recomendable que le aconseje su integrador en el momento de despliegue de los equipos.

147. Las actualizaciones están firmadas digitalmente por Palo Alto Networks. Durante el proceso de carga de la actualización, y antes de comenzar la instalación, el *software* que lo realiza utiliza un certificado incorporado para verificar la firma digital de la nueva versión, con el objetivo de confirmar la integridad del paquete.

148. Si la firma digital es válida, el *software* notificará al administrador que la actualización está lista para instalarse. En cambio, si se determina que la firma digital no es válida, el *software* mostrará un mensaje de error que indica que la actualización no es válida y no estará disponible para la instalación.

Nota: En el siguiente enlace encontrará información detallada sobre las tareas de actualización: *https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-upgrade/software-and-content-updates/install-content-and-software-updates*

5.7 REGISTRO DE EVENTOS (AUDITORÍA)

5.7.1 GENERACIÓN DE REGISTROS

149. La auditoría generada por el cortafuegos comprende varios tipos de registros que se almacenan localmente en el disco duro en el sistema de archivos PAN-OS:

- **Logs de sistema**: Incluyen eventos en el inicio y cierre de sesión del usuario.
- **Logs de configuración**: incluyen eventos relacionados con la configuración de políticas de seguridad, así como otros eventos seleccionados como auditables por el administrador.
- **Logs de tráfico**: Incluyen todos los eventos de flujo de tráfico.
- **Logs de amenazas**: Incluyen los eventos relacionados con la detección y el bloqueo de amenazas.

150. **Requisito de seguridad**: Se debe habilitar *logging* de todo el tráfico relevante. Únicamente se debe dejar sin registrar el tráfico totalmente confiable.

151. **Ubicación**: "*Policies > Security > Security Policy Rule > Actions*"

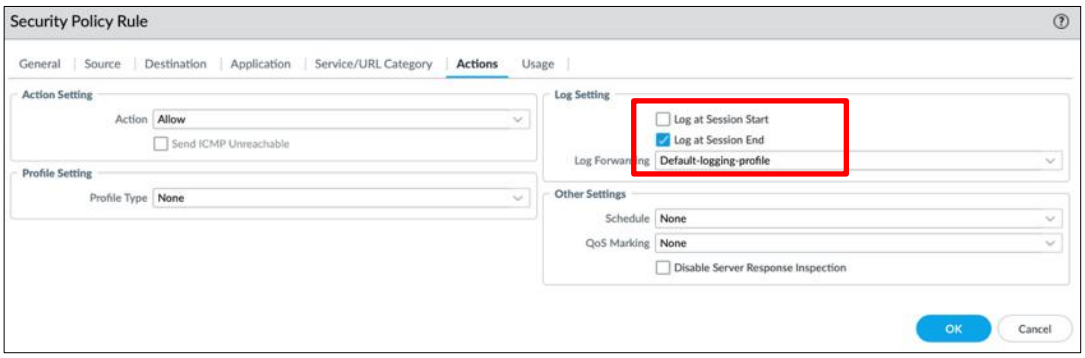


Figura 5-32: Habilitar el registro de logs en reglas de la política

152. **Requisito de seguridad:** Se debe habilitar, además, las siguientes opciones:

- ***FIPS-CC Specific Logging***— Habilita *logs* más detallados, especificados en el estándar de *Common Criteria* (CC).

- ***Packet Drop Logging***— Habilita el *login* para todos los paquetes rechazados por política.

- ***TLS Session Logging***— Habilita el *logging* para el establecimiento de sesiones TLS.

- ***CA (OCSP/CRL) Session Establishment Logging***— Habilita el *logging* cuando el servidor de seguridad envía una solicitud a la CA para verificar el estado de revocación del certificado mediante el Protocolo OSCP o una solicitud del servidor de la Lista de revocación de certificados (deshabilitado por defecto).

- ***IKE Session Establishment Logging***— Habilita el *logging* para el establecimiento de sesiones IPSEC IKE cuando el VPN *gateway* se autentica con el peer (habilitado por defecto).

5.7.1.1 LOGS DEL SISTEMA

153. En el siguiente enlace encontrará información detallada sobre los logs del sistema:

https://docs.paloaltonetworks.com/ngfw/administration/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/system-log-fields

5.7.1.2 LOGS DE CONFIGURACIÓN

154. En el siguiente enlace encontrará información detallada sobre los logs de configuración:
https://docs.paloaltonetworks.com/ngfw/administration/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/config-log-fields

5.7.1.3 LOGS DE TRÁFICO

155. En el siguiente enlace encontrará información detallada sobre los logs de tráfico:
https://docs.paloaltonetworks.com/ngfw/administration/monitoring/use-syslog-for-monitoring/syslog-field-descriptions/traffic-log-fields

5.7.1.4 EJEMPLO DE EVENTOS AUDITABLES

Evento Auditable	Ejemplo	Fichero de Log
Fallo en el establecimiento de una IPSEC SA. Contenido adicional del registro de auditoría*: Causa del fallo*	*11/10 01:54:51 vpn critical ikev2-nego-fail-cert IKEv2 certificate authentication failed. Peer certificate revocation status couldn't be checked due to end-entity certificate 'CN=20.1.1.20, O=Internet Widgits Pty Ltd, ST=Some State, C=AU*	*System*

Evento Auditable	Ejemplo	Fichero de Log
Sesión establecida con el peer. Contenido adicional del registro de auditoría: Contenido completo de todos los paquetes transmitidos y recibidos durante el establecimiento de la sesión.	11/15/2021 6:27 *vpn ikev2-nego-child-start branchgw IKEv2 child SA negotiation is started as initiator, rekey. Initiated SA: 20.1.1.40[500]-20.1.1.20[500] message id:0x00000000* 11/15/2021 *vpn ipsec-key-install branchgw IPSec key installed. Installed SA: 20.1.1.40[500]-20.1.1.20[500] SPI:0xF768489C/0x82109BCC lifetime 3600 Sec lifesize unlimited* 11/15/2021 6:27 *vpn ikev2-nego-child-succ branchgw IKEv2 child SA negotiation is succeeded as initiator, rekey. Established SA: 20.1.1.40[500]-20.1.1.20[500] message id:0x00000002, SPI:0xF768489C/0x82109BCC*	*System*
Fallo de establecimiento de una sesión TLS. Contenido adicional del registro de auditoría*: Causa del fallo*	11/15/2021 6:27 *vpn ikev2-nego-child-start branchgw IKEv2 child SA negotiation is started as initiator, rekey. Initiated SA: 20.1.1.40[500]-20.1.1.20[500] message id:0x00000000* 11/15/2021 *vpn ipsec-key-install branchgw IPSec key installed. Installed SA: 20.1.1.40[500]-20.1.1.20[500] SPI:0xF768489C/0x82109BCC lifetime 3600 Sec lifesize unlimited* 11/15/2021 6:27 *vpn ikev2-nego-child-succ branchgw IKEv2 child SA negotiation is succeeded as initiator, rekey. Established SA: 20.1.1.40[500]-20.1.1.20[500] message id:0x00000002, SPI:0xF768489C/0x82109BCC*	*System*
Uso de mecanismos de identificación y autenticación. Contenido adicional del registro de auditoría*:* *Origen de la petición (p.e Dirección IP)*	***Password Successful Login*** 11/16 06:33:06 *auth informational auth- success authenticated for user 'admin'. From: 192.168.1.99* ***Certificate Successful Login*** 11/07 08:22:03 *auth informational auth- success Certificate validated for user 'certAdmin'. From:192.168.1.99* ***Unsuccessful Login*** 11/07 07:03:45 *auth medium auth-fail failed authentication for user 'certAdmin'. Reason: Invalid username/password. From: 192.168.1.99*	*System*
Intento fallido de validación de certificado. Contenido adicional del registro de auditoría: *Causa del fallo*	11/10 01:54:51 *vpn critical ikev2-nego-fail- cert IKEv2 certificate authentication failed. Peer certificate revocation status couldn't be checked due to end-entity certificate 'CN=20.1.1.20, O=Internet Widgits Pty Ltd, ST=Some State, C=AU*	*System*

Evento Auditable	Ejemplo	Fichero de Log
Sesión establecida con una CA. Contenido adicional del registro de auditoría: *Contenido completo de todos los paquetes transmitidos y recibidos durante el establecimiento de la sesión.*	*09/06 13:41:50 sslmgr informational ca- session-establishment-success 192.168.1.00 CRL request to 192.168.1.100 succeeded. Destination address 192.168.1.100, Destination port 80. Source address 192.168.1.60, Source port 43416* *09/06 13:41:50 general informational general Sucessfully get CRL http://192.168.1.100/ca- crl.cer]*	*System*
Aplicación de las reglas configuradas con opción de log. Contenido adicional del registro de auditoría: Direcciones origen y destino, Puertos origen y destino, protocolo TLS, interfaz.	11/10/2021 1:08 *10108000519 TRAFFIC end 20.1.1.40 20.1.1.20 VPNRule ike vsys1 ISP ISP ethernet3/2 ethernet3/2 1 500 500* *0 0 0x19 udp allow 8198 6734 1464 37 11/10/2021 0:50 452 any 0 6.48E+18 0x0 United States United States 0 33 4 aged-out aged-out 0 0 0 0 PA-7050 from-policy*	*Traffic*
Indicación de paquetes descartados debido a excesivo tráfico de red (flooding). Contenido adicional del registro de auditoría: *Interfaz incapaz de procesar el tráfico, identificador de la regla que ha causado el descarte (drop).*	9/25/2021 18:45 *10108000519 THREAT flood 0.0.0.0 0.0.0.0 not-applicable vsys1 untrust untrust 1 0 0 0 0 0x2000 tcp drop TCP Flood(8501) any critical client-to-server 6.4699E+18 0x0* *0.0.0.0-0.255.255.255 0.0.0.0-0.255.255.255 0 0 0 0 0 0 0 0 PA-7050 0 0 N/A flood AppThreat-0-0 0x0*	*Threat*
APP-ID utilizado con el protocolo procesado. Contenido adicional del registro de auditoría: *Nombre del protocolo.*	9/25/2021 15:36 *10108000519 TRAFFIC end 1 7.7.7.7 8.8.8.8 rule2 ftp vsys1 untrust trust ethernet3/6 ethernet3/5 570425425 1 54425 21 0 0 0x1c tcp allow 2506 1018 1488 31 6 any 0 6.46871E+18 0x0 United States United States 0 16 15 tcp-fin 0 0 0 0 PA-7050 from-policy 0 0 N/A*	*Traffic*
Modificación de la configuración de envío de registros de log a servidor de auditoría externo.	11/16/2021 9:33 *192.168.1.99 edit admin Web Succeeded config shared log-settings syslog syslog syslog { server { syslog {transport TCP; port 514; format BSD; } } } syslog { server { syslog { transport SSL; port 6514; format IETF; } } }*	*Configuration*

Evento Auditable	Ejemplo	Fichero de Log
	11/16/2021 9:33 192.168.1.99 edit admin Web Succeeded config shared log-settings syslog syslog syslog { server { syslog { server 192.168.1.77; } } } syslog { server { syslog { server 192.168.1.78; } } }	
Intento de actualización manual.	*11/07 12:11:53 general informational general Installed panos software version 8.0.5*	*System*
Habilitación o deshabilitación de actualizaciones automáticas.	***Disabling*** *11/17 04:07:06 admin 192.168.1.99 Web edit Succeeded deviceconfig system update-schedule threats recurring recurring { weekly{ action download-only; } } recurring:* ***Enabling*** 11/17 04:13:17 *admin 192.168.1.99 Web edit succeeded deviceconfig system update-schedule threats recurring recurring: recurring{ weekly { action download-only; } }*	*Configuration*
Generación, modificación o importación de claves criptográficas.	***Import/Generation*** 09/07 08:47:58 *admin 192.168.1.99 Web upload config shared certificate noCRLSign noCRLSign { private-key ********;}* ***Deletion*** *11/17 05:47:44 admin 192.168.1.99 Web delete Succeeded config shared certificate lientRSA2*	*System*
Cambios en la hora del cortafuegos. Contenido adicional del registro de auditoría: *Valores antiguos y nuevos, origen del cambio (p.e dirección IP).*	11/17 06:05:52 *general medium general System time changed from 2021/11/17 06:02:04 to 2021/11/17 06:05:52*	*Configuration*
Intento de desbloqueo de una sesión.	11/07 12:23:18 *general medium auth-fail failed authentication for user 'admin'. Reason: User is in locked users list From: 192.168.1.99*	*System*
Terminación de una sesión remota debido a time-out de sesión.	11/07 12:31:45 *general informational general Session for user admin via Web from 192.168.1.99 timed out*	*System*
Terminación de una sesión remota.	11/07 12:41:27 *general informational general User admin logged out via Web from 192.168.1.99*	*System*
Inicio/finalización/fallo de un canal confiable. Contenido adicional del registro de auditoría:	*11/10 15:12:36 syslog high syslog-conn-status Syslog connection established to server['AF_INET.192.168.1.99:443.']* 11/17 06:34:50 *general informational general Connection to Update server:*	*System*

Evento Auditable	Ejemplo	Fichero de Log
Identificación del que inicia el canal y del objetivo del intento fallido de establecimiento del canal.	*updates.paloaltonetworks.com completed successfully, initiated by 192.168.1.99* 11/15/2021 6:27 *vpn ikev2-nego-child-start branchgw IKEv2 child SA negotiation is started as initiator, rekey. Initiated SA: 20.1.1.40[500]-20.1.1.20[500] message id:0x00000000.* *11/15/2021 vpn ipsec-key-install branchgw IPSec key installed. Installed SA: 20.1.1.40[500]-20.1.1.20[500] SPI:0xF768489C/0x82109BCC lifetime 3600 Sec lifesize unlimited.* 11/15/2021 6:27 *vpn ikev2-nego-child-succ branchgw IKEv2 child SA negotiation is succeeded as initiator, rekey. Established SA: 20.1.1.40[500]-20.1.1.20[500] message id:0x00000002, SPI:0xF768489C/0x82109BCC.*	

Tabla 4: Eventos Auditables

5.7.1.5 EJEMPLO DE ACCIONES DE ADMINISTRACIÓN AUDITABLES

Acción del Administrador	Menú GUI	Log Generado
Inicio o apagado del cortafuegos.	*Device->Setup->Operations->Device Operations->Shutdown Device*	***Startup*** *03/21 03:21:12 general high system-start The system is starting up.* ***Shutdown*** *03/21 04:29:50 general high system-shutdown The system is shutting down.*
Establecimiento de hora del sistema.	*Device->Setup->Management->General Settings->Time*	*04/04 07:18:08 general medium general System time changed from 2018/04/04 07:18:12 to 2018/04/04 07:18:08 by admin*
Configuración de reenvío de logs a Sistema externo.	*Device->Log Settings->System->Add->Syslog->Add*	*11/16/2021 9:33 192.168.1.99 edit admin Web Succeeded config shared log-settings syslog syslog syslog {server { syslog { transport TCP; port 514; format BSD; } } } syslog { server { syslog { transport SSL; port 6514; format IETF; } } }* *11/16/2021 9:33 192.168.1.99 edit admin Web Succeeded config shared log-settings syslog syslog syslog {server { syslog { server 192.168.1.77; } } } syslog { server { syslog { server 192.168.1.78; } } }*

Acción del Administrador	Menú GUI	Log Generado
Eliminación manual de un fichero de log.	*Device->Log Settings->Manage Logs*	*03/20/2018 07:42:38 general informational general log type config cleared by user admin*
Configuración del comportamiento del mecanismo de bloqueo para fallos de autenticación.	*Device->Setup->Management->Authentication Settings*	*04/04 07:48:26 admin 192.168.1.99 Web set Succeeded deviceconfig setting management 04/04 07:48:26 /config/devices/entry[@name='localhost.localdomain']/deviceconfig/setting/management management { admin-lockout {failed-attempts 5; lockout-time 1; }}*
Configuración de HTTPS / TLS.	*Device->Certificate Management->SSL/TLS Service Profile*	*03/20/2018 07:31:01 admin 192.168.1.99 Web set Succeeded config shared ssl-tls-service-profile Test_TLS_Provile /config/shared /ssl-tls-service-profile /entry [@name… Test_TLS_Pro… { protocol-settings { min-version tls 1-1; max-v 262*
Creación de un usuario local.	*Device->Administrators*	*03/20/2018 08:07:28 admin 192.168.1.99 Web set Succeeded config mgt-config users newuser2 /config/mgt-config/users /entry[@name… newuser2 { permissions { role-based { superuser yes; } } phash * 1*
Configuración de autenticación local.	*Device->Authentication Profile*	*03/20/2018 07:27:19 Web set Succeeded config shared authentication-profile TestAuthenticationProfile /config/shared /authentication-profile /entry[@name… authentication-profile { TestAuthentica… { multi-facto 261*
Inicio y verificación de actualizaciones software.	*Device->Software*	*03/20/2018 08:08:43 general informational general Installed panos software version 8.0.6*
Configuración del timeout de inactividad.	*Device->Setup->Management->Authentication Settings->Idle-timeout*	*03/20/2018 07:38:15 Web delete Succeeded deviceconfig setting management idle-timeout /config/devices /entry[@name… /deviceconfig /setting /management /idle-timeout 275*

Acción del Administrador	Menú GUI	Log Generado
Configuración del mensaje de inicio de sesión (login banner).	*Device->Setup->Management->Banners and Messages*	*03/20/2018 07:34:07 Web set Succeeded deviceconfig system motd-and-banner /config/devices/entry[@name…/deviceconfig/system/motd-and-banner motd-and-banner {banner-header "Test Banner2";} 268*
Configuración de IKE / IPsec.	*Network->IPSec Tunnels*	*03/20/2018 07:58:21 admin 192.168.1.99 Web edit Succeeded network tunnel ipsec branch-vpn /config/devices /entry[@name…/network/tunnel /ipsec /entry[@name… vpn'] branch-vpn {auto-key { ipsec-crypto-profile Suite-B-GCM-128; } branch-vpn {auto-key { ipsec-crypto-profile default; } } 1266*
Configuración de reglas del cortafuegos.	*Policies->Security*	*03/20/2021 09:00:20 admin 192.168.1.99 Web edit Succeded vsys vsys 1 rulebase security rules VPNRule1 application /config/devices/entry[@name…/vsys/entry[@... /rulebase /security/rules /entry[@name… /application application [any]; application [ssh]; 1269*
Configuración de certificados X.509	*Device->Certificate Management->Certificate Profile*	*03/20/2018 07:37:56 admin 192.168.1.99 Web set Succeeded config shared certificate-profile Test_Certificate_Profile /config/shared/certificate-profile/entry[@name…] Test_Certificat… { CA { TestCA { } } } 271*

Tabla 5: Acciones de administración auditables

5.7.2 AUDITORÍA DE CAMBIOS

156. Los cortafuegos de Palo Alto Networks permiten auditar los cambios realizados en el sistema. Para ello cuentan con dos herramientas fundamentales: el log de configuración, que registra todos los eventos asociados a cambios, y el sistema de auditoría de configuraciones, que compara dos configuraciones diferentes y muestra las diferencias entre ambas.

157. **Ubicación**: "*Monitor > Logs > Configuration" y "Device > Config Audit*"

Receive Time	Administrator	Host	Client	Command	Result	Configuration Path	Before Change	After Change	Sequence Number
01/03 16:13:29	admin	192.168.55.1	Web	edit	Succeed...	vsys vsys1 rulebase decryption rules Descifrado-DMZ type	type { ssl-inbound-inspection CA-LABMADRID; }	type { ssl-inbound-inspection "Servidor Web Externo"; }	955
01/03 16:13:25	admin	192.168.55.1	Web	move	Succeed...	vsys vsys1 rulebase decryption rules Descifrado-DMZ			954
01/03 16:13:10	admin	192.168.55.1	Web	request	Succeed...	config shared certificate		certificate { Servidor Web Externo { subject-hash 41c1d0d7; issu	953
01/03 16:12:29	admin	192.168.55.1	Web	move	Succeed...	vsys vsys1 rulebase decryption rules Descifrado-DMZ			952
01/03 16:12:28	admin	192.168.55.1	Web	set	Succeed...	vsys vsys1 rulebase decryption rules Descifrado-DMZ		Descifrado-DMZ { category [any]; service [any]; type { ssl-i	951

Figura 5-33: Ejemplo de logs de Configuración

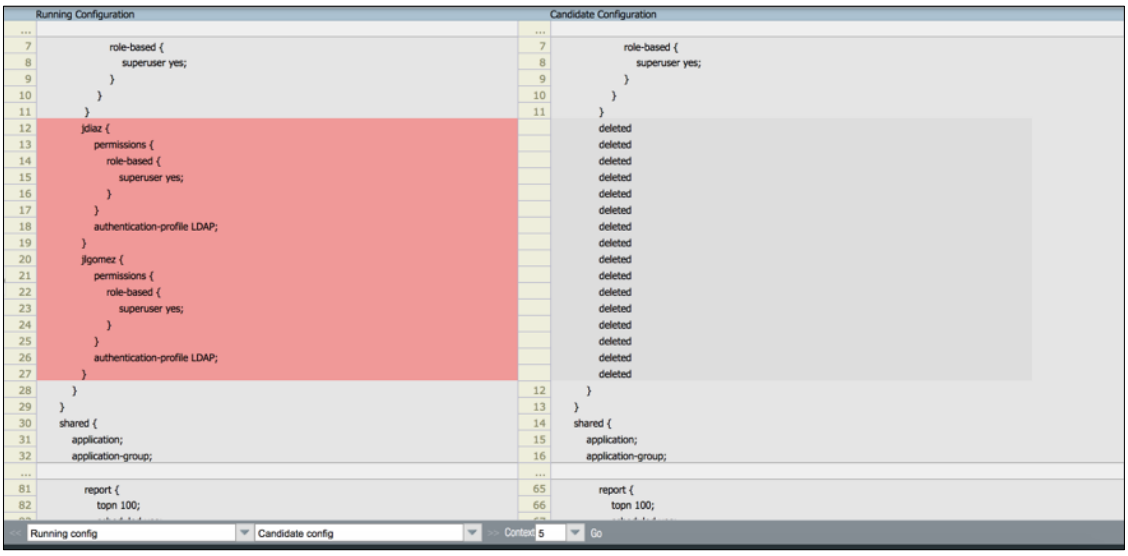


Figura 5-34: Ejemplo de salida de la herramienta Config Audit

5.7.3 ALMACENAMIENTO LOCAL

158. El cortafuegos almacena los registros de auditoría localmente y los protege de la eliminación no autorizada, al permitir que solo administradores de seguridad con la función de administrador de auditoría, puedan acceder a los registros con permisos de eliminación. Por otro lado, no existe ningún interfaz que permita a un usuario modificar los registros de auditoría.

159. El espacio para log en local se divide por tipo de logs, los cuales tienen asignado una cuota total del total destinada a este uso. Si se desea modificar esas cuotas:

160. **Ubicación**: "*Device > Setup > Management > Logging and Reporting Settings*"

161. Los archivos de log suelen almacenarse en el directorio */var/log* del disco duro del dispositivo. Este directorio contiene varios subdirectorios con archivos de registro relacionados con eventos del sistema, tráfico, amenazas y otras funciones.

- Registros de tráfico: */var/log/pan/vault*
- Registros de amenazas: */var/log/pan*
- Registros del sistema: */var/log/sistema*

162. Tenga en cuenta que la visualización y gestión de estos registros suele requerir permisos administrativos adecuados y conocimientos de la interfaz de línea de comandos (CLI) o la interfaz web del dispositivo.

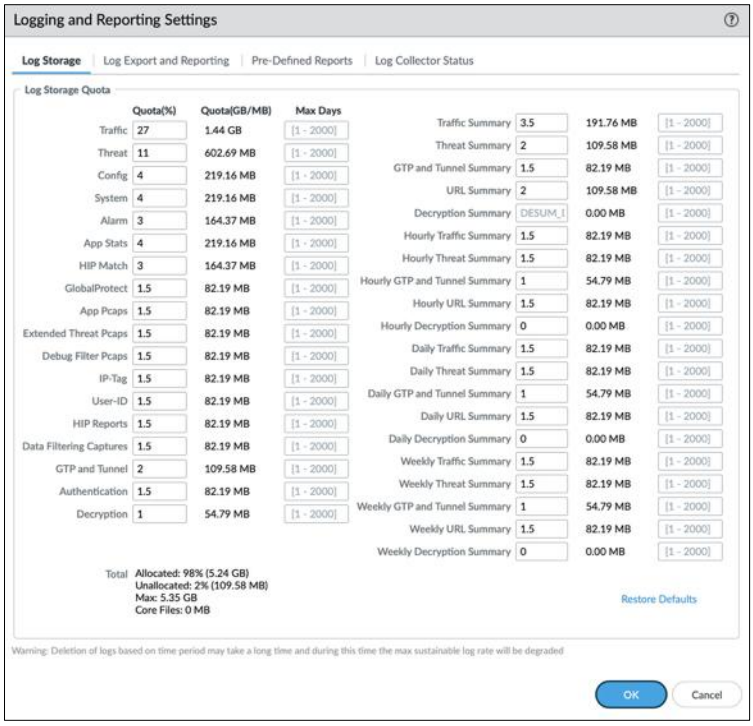


Figura 5-35: Configuración general de logging e informes

163. Cuando la capacidad asignada está llena, se comienza a sobrescribir los logs (empezando por los más antiguos).

164. **Recomendación**: Se recomienda la exportación de los logs a un sistema externo para poder retener los logs el tiempo determinado por la normativa de aplicación.

5.7.4 ALMACENAMIENTO REMOTO

165. El cortafuegos se puede configurar para reenviar los registros de auditoría generados, a un servidor de *syslog* externo. Cuando se configura así, el cortafuegos convierte automáticamente los registros de auditoría al formato *syslog*, antes de enviarlos al servidor de externo.

166. El cortafuegos intenta automáticamente volver a conectarse al servidor de *syslog* externo si el canal protegido por TLS se rompe involuntariamente.

Nota: En el manual de administración de PAN-OS v11, en la sección *Monitoring*, subsección *Use Syslog for Monitoring*, apartado *Configure Syslog Monitoring*, se proporciona información adicional sobre cómo configurar el equipo para exportar registros de auditoría a un servidor de *syslog*.
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/monitoring/use-syslog-for-monitoring/configure-syslog-monitoring

167. En primer lugar, se deberán configurar los datos del servidor Syslog para el envío de logs (*Syslog Server Profile*).

168. **Requisito de seguridad**: Se debe utilizar un canal protegido por **TLS** (versión 1.2 o superior).

169. **Ubicación**: "*Device > Server Profiles > Syslog > Syslog Server Profile*"

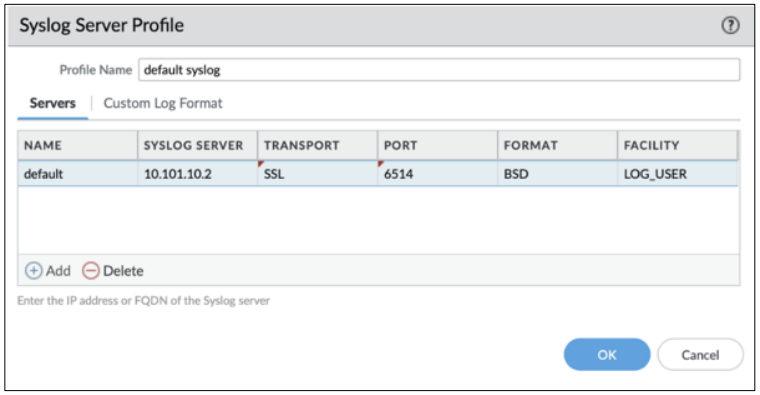


Figura 5-36: Configuración de perfil de servidor Syslog

170. Después, se deberá crear un perfil de reenvío de logs en el que se indicarán qué tipo de registros se van a enviar al servidor syslog externo.

171. **Ubicación**: "*Objects > Log Forwarding*"

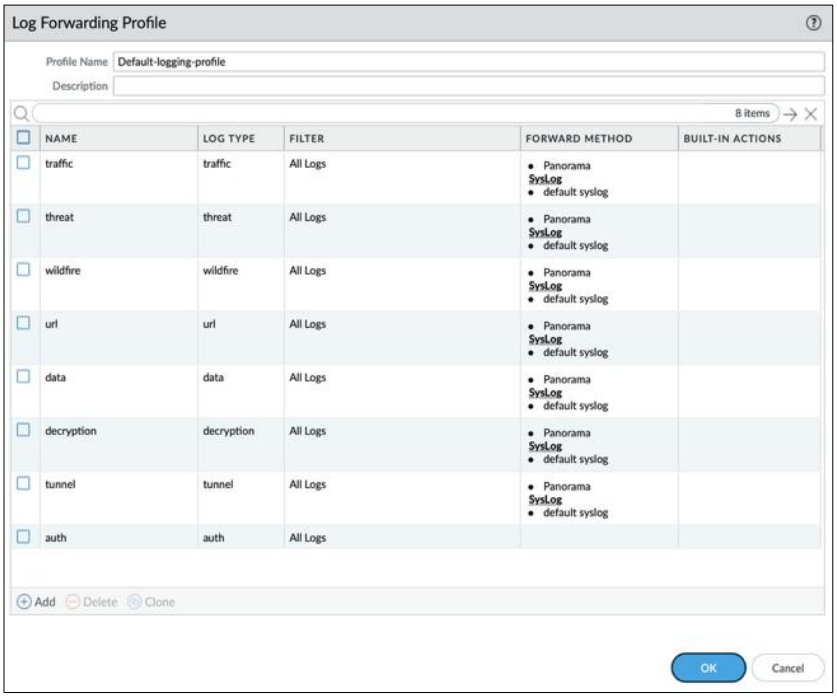


Figura 5-37: Configuración de perfil de reenvío de logs

172. Por último, se debe habilitar el reenvío de logs en las reglas de la política de seguridad.

173. **Ubicación**: "*Policies > Security > Security Policy Rule > Actions*"

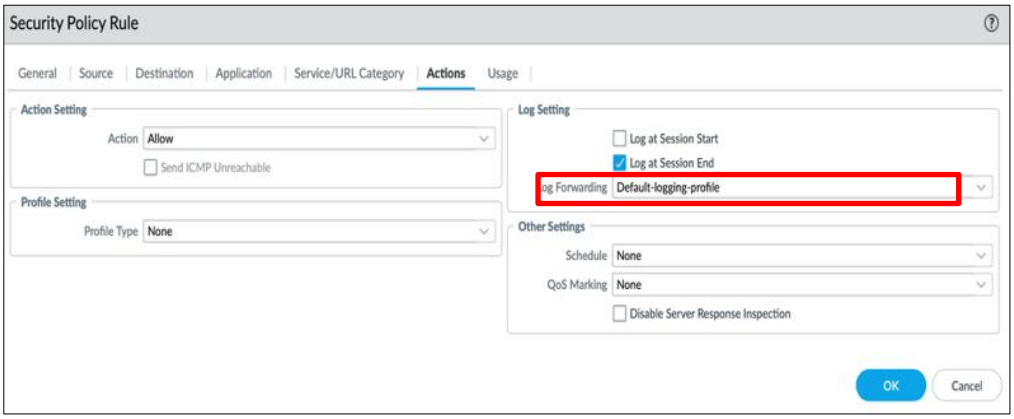


Figura 5-38: Activar reenvío de logs en la configuración de la regla de seguridad

5.8 BACKUPS

174. **Ubicación**: "*Device > Setup > Operations*"

175. **Recomendación**: La configuración *running*, incluye todos los ajustes que se han compilado y que, por tanto, están activos, como las reglas de las políticas o los objetos usados. La configuración *candidate* es una copia de la configuración *running*, más cualquier cambio inactivo que se ha realizado tras el último *commit*. La realización de backups de la configuración running o candidate permitirá restaurar posteriormente versiones previas del cortafuegos.

Nota: Puede encontrar información detallada sobre la gestión de los *backups* en: *https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/firewall-administration/manage-configuration-backups*

5.9 AUTO-CHEQUEOS

176. **Ubicación**: "*Device > Master Key and Diagnostics*"

177. Cuando el cortafuegos funciona en el **modo de operación seguro**, los administradores tienen la capacidad de ejecutar los siguientes auto-chequeos (*self-tests*):

    - Auto-chequeos de algoritmos y funciones criptográficas.
    - Auto-chequeos de Integridad del *software*.

178. Para ello, el administrador debe seleccionar la acción de "Ejecutar autoprueba de algoritmos criptográficos" para la primera opción, o "Ejecutar autoprueba de integridad del *software*" para la segunda opción. Si uno de los tests falla, el equipo entrará en estado de error. Durante el tiempo en que el equipo está en estado de error, no es posible realizar ninguna operación criptográfica ni sacar ningún dato del equipo.

5.10 ALTA DISPONIBILIDAD

179. Para garantizar que el servicio se presta de manera continuada, cuando un equipo falla o se ve sometido a una operación de actualización o mantenimiento, es recomendable configurar la solución de seguridad en alta disponibilidad (*High Availability*, HA).

180. El despliegue de alta disponibilidad se puede realizar mediante dos firewalls colocados en un grupo de HA o hasta 16 firewalls formando un clúster HA cuya configuración está sincronizada para evitar un único punto de fallo en la red y proporcionar redundancia.

181. Es importante tener en cuenta que un grupo de HA no está diseñado para aumentar el rendimiento de la solución, sino para garantizar su disponibilidad, por lo que es necesario dimensionar adecuadamente cada miembro del *grupo* para garantizar que cada uno es capaz de soportar la carga de trabajo requerida en cualquier momento por sí solo.

182. En cambio, la configuración en clúster permite el escalado horizontal del número de firewalls y así aumentar el rendimiento. Un *cluster* sincroniza las sesiones entre todos los miembros del clúster. Ante una caída de la red, o de un firewall, las sesiones conmutan a otro miembro del clúster garantizando la disponibilidad del servicio.

183. El clúster se puede desplegar en nivel 3 o en modo *virtual-wire*, y los miembros pueden ser firewalls independientes o grupos de HA tanto activo-pasivo como activo-activo.

Nota: Puede encontrar información detallada sobre la configuración de HA en el enlace: *https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/high-availability*

184. A continuación, se indican unas recomendaciones para tener en cuenta en la configuración de la alta disponibilidad:

- Configuración Sincronizada.

Una vez que la configuración de HA se ha realizado, es importante comprobar que ambos miembros mantienen la configuración sincronizada. La forma más sencilla de verificarlo es a través de los *widgets* del Dashboard principal.

Ubicación: "*Dashboard > Widgets > System > High Availability*"

Figura 5-39: Widget de estado de alta disponibilidad

- Monitorización de *links* y *paths*.

Debe habilitarse la monitorización de enlaces (*links*) y, opcionalmente, también la del camino (*path*), para asegurar que en caso de fallo de un enlace se produce la conmutación entre los miembros del *cluster*.

Ubicación: "*Device > High Availability > Link and Path Monitoring*"

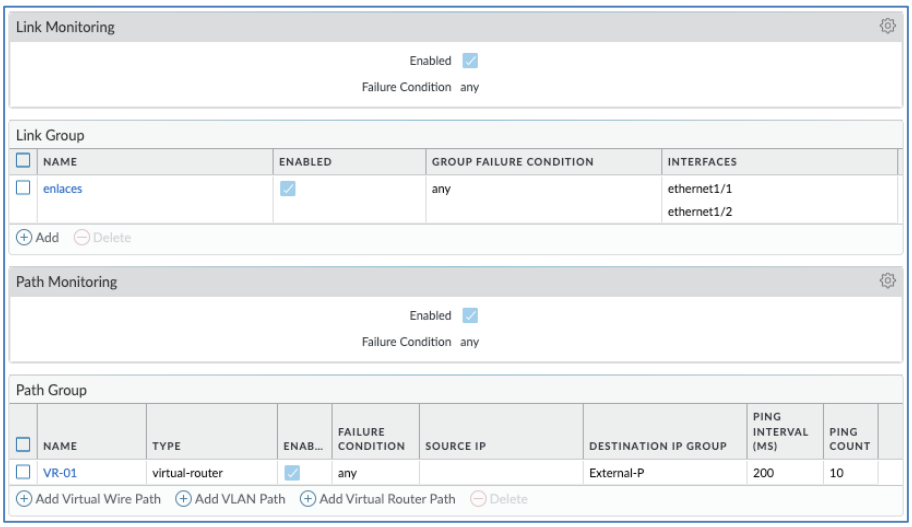


Figura 5-40: Configuración de link/path monitoring

- *Preemptive*.

Si se activa la opción "*Preemptive*" junto con la opción de "*Passive Link State*" a *Shutdown*, podría causarse una condición de *loop* en el equipo respaldo del *cluster*, cuando también está activado el *link monitoring*. Por ello, la mejor práctica es configurar "*Passive Link State*" a *Shutdown* y no activar "*Preemption*".

Ubicación: "*Device > High Availability > General > Election Settings*"

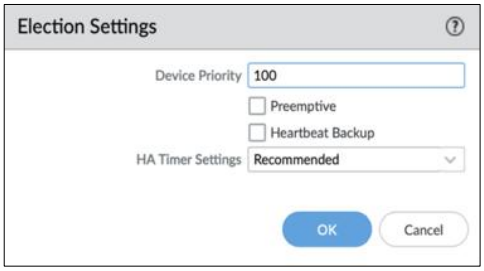


Figura 5-41: Configuración recomendada de Preemption y Passive Link State

Ubicación: "*Device > High Availability > General > Active/Passive Settings*"

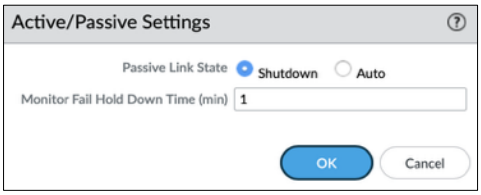


Figura 5-42: Configuración recomendada de ajustes de Activo/Pasivo

- Configuración Clúster.

Habilitar la participación en el *clúster* e indicar un identificador de *clúster* para que los miembros compartan las sesiones.

Ubicación: "*Device > High Availability > General > Cluster Settings"*

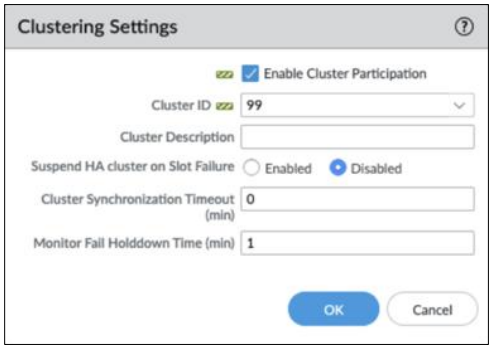


Figura 5-43: Configuración de Clúster

Configurar las interfaces que participan en el *clúster*. Elegir la interfaz dedicada al *clúster*, asignar la IP, la máscara y el umbral para considerar que un equipo está vivo y sigue perteneciendo al *clúster*.

Ubicación: "*Device > High Availability > HA Communications > Clustering Links"*

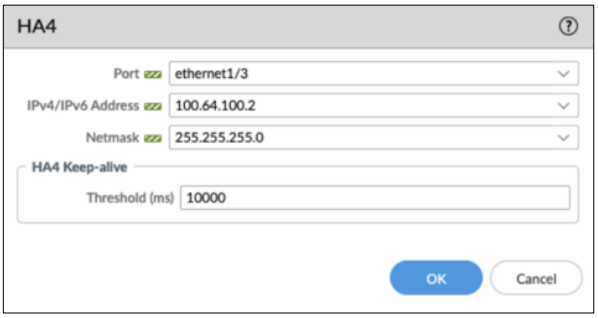


Figura 5-44: Configuración de enlaces

Para añadir miembros al *clúster* hay que añadir el firewall local. En caso de añadir un grupo de HA, hay que añadir ambos miembros al cluster.

Ubicación: "*Device > High Availability > Cluster Config"*

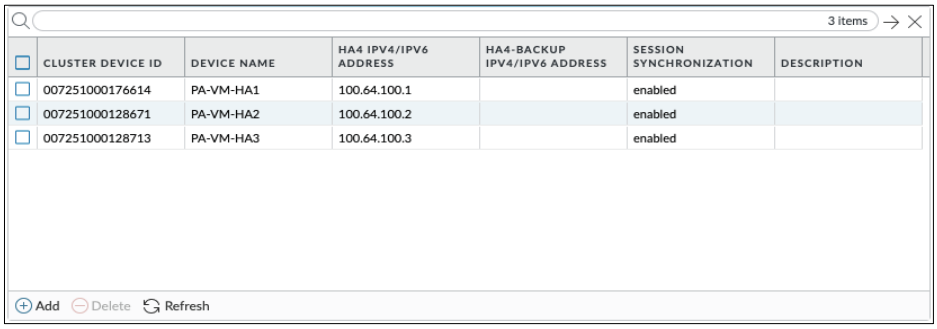


Figura 5-45: Configuración de los miembros del clúster

Monitorización del estado del *clúster*

Ubicación: "*Dashboard > Widget > Settings > HA Cluster"*

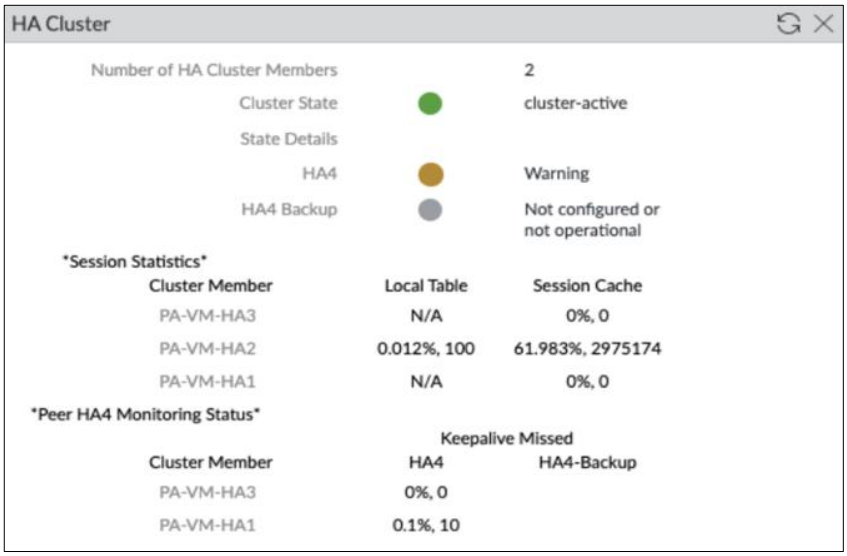


Figura 5-46: Dashboard del clúster

5.11 CONFIGURACIÓN DE LOS SERVICIOS DE SEGURIDAD

5.11.1 FILTRADO DE PAQUETES CON ESTADO (*STATEFUL TRAFFIC FILTERING*)

185. Los cortafuegos Palo Alto Networks pueden configurarse para realizar "*Stateful traffic filtering*" en los siguientes protocolos, con los siguientes atributos.

a) *Internet Control Message Protocol version 4 (ICMPv4), RFC 792*:

   i. Type

   ii. Code

b) *Internet Control Message Protocol version 6 (ICMPv6), RFC 4443*:

   i. Type

   ii. Code

c) *Internet Protocol (IPv4), RFC 791*:

i. *Source address*

ii. *Destination address*

iii. *Transport layer protocol*

d) *Internet* Protocol version 6 (IPv6), RFC 2460:

i. *Source address*

ii. *Destination address*

iii. *Transport layer protocol*

e) *Transmission Control Protocol (TCP), RFC 793*:

i. *Source port*

ii. *Destination port*

f) *User Datagram Protocol (UDP), RFC 768*:

i. *Source port*

ii. *Destination port*

186. Los cortafuegos agrupan los interfaces en zonas de seguridad. Cada zona identifica uno o varios interfaces del cortafuegos. Se deben crear zonas separadas para cada tipo de interfaz (capa 2, capa 3 o *virtual wire*) y cada interface tiene que ser asignado a una zona para poder procesar tráfico.

187. La política de seguridad se usa para determinar si bloquear o permitir una sesión específica basándose en los atributos de la misma, como la zona origen/destino, IP origen/destino y puerto origen/destino.

188. Adicionalmente, una política de seguridad incluye atributos que indican qué hacer con los paquetes de red:

a) *Action* – "*Allow*", "*Deny*", "Drop", "*Reset client*", *Reset server*", "*Reset both client and server*".

b) *Profile Settings* – Especifica cualquier chequeo adicional que debe ser realizado por los perfiles de seguridad como *Antivirus*, *Vulnerability Protection, Anti-Spyware, etc*. Estos perfiles permiten o requieren que el tráfico de red sea protegido.

c) *Log Setting* – Selecciona el perfil de logs que se le aplicará a esa sesión.

d) *Other Settings:*

i. *Schedule*— Limita los días y horas en los que la regla es efectiva.

ii. *QoS Marking*—Modifica las marcas de calidad de servicio al tráfico que coincida con esta regla.

iii. *Disable Server Response Inspection*— Deshabilita la inspección de paquetes desde el servidor al cliente, esto puede ser útil en momentos de alga carga de los equipos

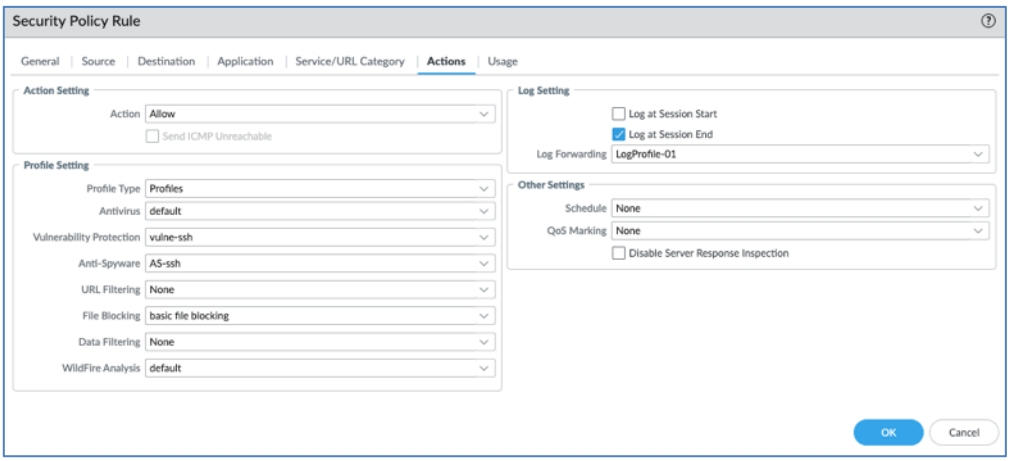


Figura 5-47: Acciones sobre una política de seguridad

189. Todo el tráfico que pasa a través del cortafuegos se compara con una sesión, y cada sesión se compara con una política de seguridad. Cuando se produce una coincidencia de sesión, la política de seguridad se aplica al tráfico bidireccional (de cliente a servidor y de servidor a cliente) en esa sesión. Para el tráfico que no coincide con ninguna regla definida, se aplican las reglas predeterminadas. Las reglas predeterminadas permiten todo el tráfico *intrazone* (dentro de la zona) y bloquean todo el tráfico *interzone* (entre zonas).

190. Las políticas de seguridad se evalúan de izquierda a derecha y de arriba a abajo. Un paquete se compara con la primera regla que cumple con los criterios definidos; después de que se produce una coincidencia, las reglas posteriores no se evalúan.

191. Por lo tanto, las reglas más específicas deben preceder a las más genéricas para imponer los mejores criterios de coincidencia. El tráfico que coincide con una regla genera una entrada de log al final de la sesión en el log de tráfico, si el log está habilitado para esa regla. Las opciones de log son configurables para cada regla y, por ejemplo, pueden configurarse para iniciar el registro de log al inicio de una sesión, al final de la sesión, o en ambos casos. El tráfico se descarta en los siguientes casos:

- Si la dirección de origen del tráfico entrante corresponde a la dirección IP de una red de transmisión externa o *loopback*.
- Si el tráfico entrante se recibe de la red externa, pero tiene una dirección de origen que corresponde a la red interna.
- Si el tráfico se recibe de la red interna, pero tiene una dirección de origen que corresponde a la red externa.
- Si la dirección de origen es igual a la dirección de la interface de red donde se recibió el paquete de red.

- Si son paquetes IPv4 con las opciones strict source routing, loose source routing, and record route packets

- Paquetes con direcciones en el rango 100.64.0.0/10 (RFC 6598).

192. El administrador debe limitar el número de conexiones TCP *Half-open* y definir umbrales que puedan constituir un *flooding*. Para más información, consultar el apartado 5.12.1 ATAQUES DOS.

5.11.2 VPNS

193. Los cortafuegos de Palo Alto Networks incluidos en esta guía soportan varios despliegues de VPNs (Red Privada Virtual):

    - ***Site-to-site VPN***: Una VPN que conecta una sede central con una sede remota o una "*Hub and Spoke VPN"* que conecta una sede central con múltiples sedes remotas.

      El NGFW utiliza el set de protocolos IPSec para establecer un túnel seguro para asegurar confidencialidad, autenticación e integridad en el tráfico transmitido entre las dos sedes.

    - ***Remote User-to-Site VPN****:* Es una solución basada en el agente *Global Protec*t para permitir a un usuario remoto establecer una conexión segura a través del NGFW. Esta solución utiliza SSL e IPSec para securizar el tráfico entre el usuario remoto y la sede central.

    - ***Large Scale VPN***: Palo Alto Networks *Global Protect Large Scale VPN* (LSVPN) provee un mecanismo simple para el despliegue escalable de una topología "*hub and spoke VPN*" de hasta 1024 sedes remotas. Esta solución requiere Palo Alto Networks NGFW desplegados en la sede central y en cada sede remota. Se basa en certificados para la autenticación de los dispositivos, SSL para securizar la comunicación entre todos los componentes e IPSec para securizar el tráfico.

194. En la siguiente figura se ven los distintos tipos de VPNs que se soportan:

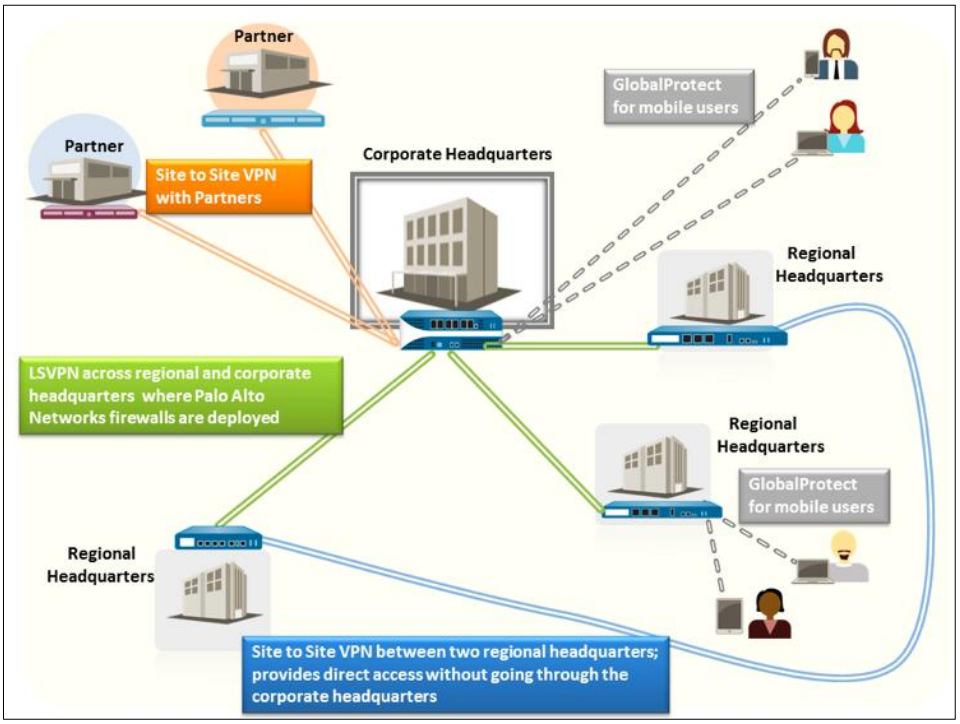


Figura 5-48: Tipos de VPNs soportadas

5.11.2.1 *SITE-TO-SITE* VPN

195. Una VPN *Site-to-Site* permite conectar dos redes LAN (dos sedes remotas con Palo Alto Networks NGFW o una sede con Palo Alto Networks NGFW y la otra con un equipo de un fabricante distinto que soporte los estándares IPSec).

196. El NGFW Palo Alto Networks establece una *route-based* VPN. El cortafuegos realiza una decisión de *routing* basado en la dirección IP destino y si esa decisión resulta en un envío del tráfico por una *interface* túnel, se gestionaría como tráfico VPN y se le aplicarían los protocolos configurados para securizar el tráfico y hacerlo llegar a través del túnel al extremo remoto.

197. El cortafuegos es interoperable con equipos que implementen VPNs en modo *route-based* o *policy-based.*

198. El conjunto de protocolos de seguridad IP (IPSec) se usa para establecer un túnel seguro para intercambiar el tráfico VPN, y la información en el paquete IP está protegido (y cifrado si el tipo de túnel es ESP). El paquete IP (encabezado y *payload*) está embebido en otro *payload* al que se aplica un nuevo encabezado antes de enviar a través del túnel IPSec.

199. La dirección IP origen en el nuevo encabezado es la del extremo VPN local y la dirección IP destino es la del extremo VPN en la sede remota. Cuando el paquete llega al extremo VPN remoto, el encabezado externo se elimina y el paquete original se envía a su destino.

200. Para configurar el túnel VPN, primero deben autenticarse los dos extremos que van a establecer el túnel. Una vez autenticados, los extremos negocian el mecanismo de cifrado

y los algoritmos para proteger la comunicación. El proceso de intercambio de claves de Internet (IKE) se utiliza para autenticar a los interlocutores de VPN, y las Asociaciones de seguridad IPSec (SA) se definen en cada extremo del túnel para proteger la comunicación de VPN.

201. A continuación, se describe como se configura un túnel IPSec en el extremo en el que se sitúe el cortafuegos de Palo Alto Networks.

202. En primer lugar, se debe crear un nuevo interface túnel que será en el encargado de gestionar el tráfico de la VPN.

203. **Ubicación**: "*Network > Interface > Tunnel*"

204. **Recomendación:** Asigne la zona de seguridad acorde a la arquitectura de red. Como norma general, se recomienda utilizar una zona específica para las VPNs para simplificar la gestión de las mismas y separarlas del resto de redes locales.

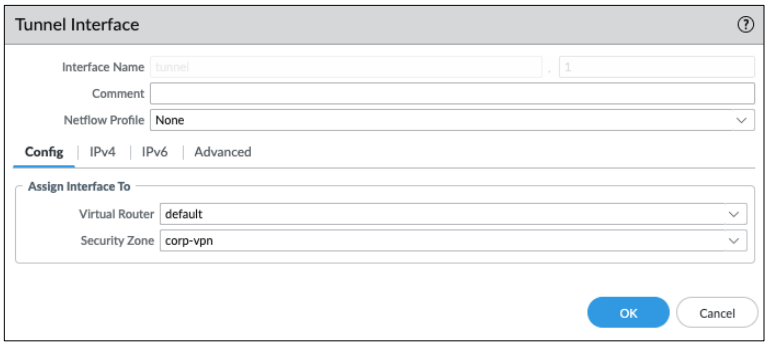


Figura 5-49: Configuración de interfaces tunnel

205. A continuación, se debe crear el perfil criptográfico que se utilizará con el protocolo IKE (*IKE Crypto Profile*), configurar el nodo (*IKE Gateway*), y crear el perfil criptográfico para el protocolo IPsec (*IPsec Crypto Profile*), según las indicaciones y recomendaciones detalladas en el apartado 5.2.1 IKE/IPSEC. Indicar, que en este apartado se especifican las opciones más seguras que se recomienda seleccionar. Sin embargo, el otro extremo remoto debe soportar esas opciones. En caso de que no estén disponibles, seleccione las más seguras soportadas por los dos.

206. Finalmente, agregue un nuevo túnel IPSec. En la ventana General, seleccione la interface túnel, el *IKE Gateway* y el *IPsec Crypto Profile* creados anteriormente, para establecer los parámetros de los túneles IPSec entre los dos extremos.

207. **Ubicación**: "*Network > IPSec Tunnel*"

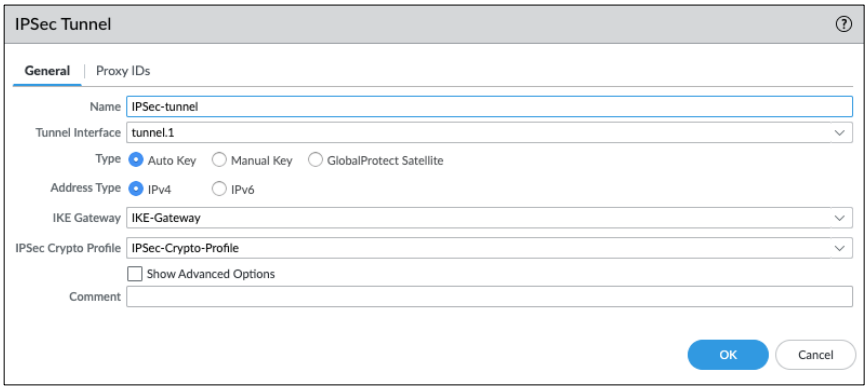


Figura 5-50: Configuración de tunnel IPSec

Nota: Si el otro extremo del túnel es un dispositivo VPN de terceros configurado como VPN *route-based*, escriba el ID de proxy local y el ID de proxy remoto, que deberán coincidir con la configuración en el otro extremo (normalmente serán las subredes LAN locales y remotas).

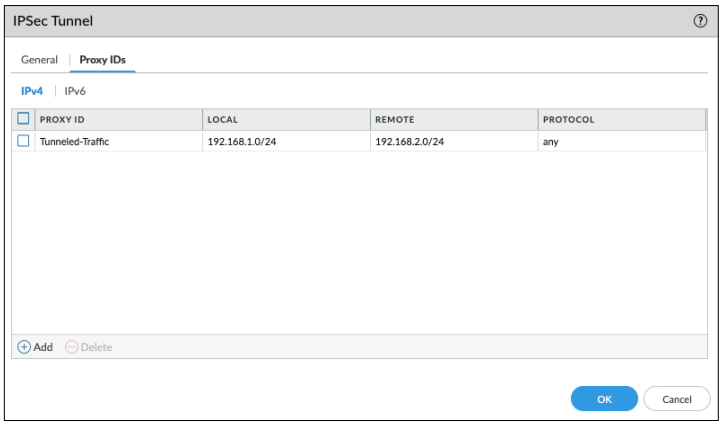


Figura 5-51: Configuración de Proxy-ID (opcional)

208. Al establecer una configuración de ID de *proxy* de túnel IPSec, para identificar redes IP locales y remotas para el tráfico que se ha establecido, los datos del ID de proxy para el túnel IPSec deben configurarse con la información de red IP posterior a NAT, ya que en el ID de *proxy* la información define las redes que se permitirán a través del túnel en ambos lados para la configuración IPSec.

209. **Ubicación**: "*Network > Virtual Routers*"

210. Añada una ruta estática en el *virtual router* correspondiente, que será la que haga posible que el tráfico sea gestionado por el interfaz túnel creado.

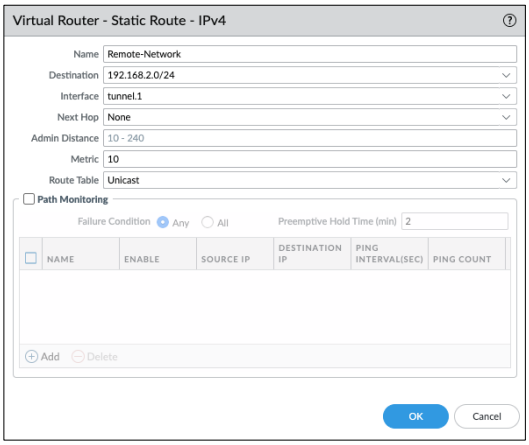


Figura 5-52: Configuración de ruta estática

Nota: Para más información de las opciones configurables en los túneles VPN *site-to-site*, consulte el siguiente enlace: *https://docs.paloaltonetworks.com/network-security/ipsec-vpn/administration/get-started-with-ipsec-vpn-site-to-site/site-to-site-vpn-overview*

211. Una vez configurados los dos extremos del cortafuegos, el túnel se establecerá cuando el cortafuegos detecte tráfico que deba ser enviado por el túnel (o cuando el otro extremo intente establecerlo).

212. **Ubicación**: "*Network > IPSec Tunnels*"

213. En la siguiente figura se puede ver cuál es el estado de las distintas fases del túnel IPSec (estado de la fase 1 y 2):

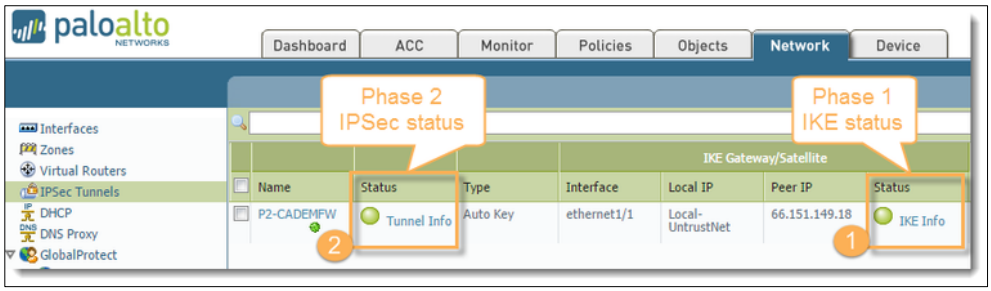


Figura 5-53: Comprobación del estado del túnel IPSEC

214. Para establecer el túnel se debe establecer primero la fase 1 y posteriormente la fase 2. Debido a que las opciones y algoritmos son diferentes, podría darse el caso que la fase 1 sí estuviese establecida y la fase 2 no. Revisando estos estados se puede tener más información acerca de los posibles fallos de negociación de los parámetros de seguridad que existan.

215. Por último, si el túnel IPSec está activo, en la misma pantalla se verá de la siguiente manera:

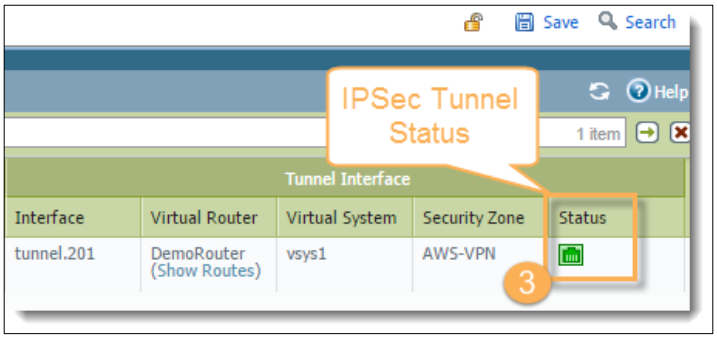


Figura 5-54: Comprobación del estado del túnel IPSEC

216. En todos estos estados, si el indicador es verde significa que está correctamente establecido y si está en rojo significa que no lo está actualmente (podría haber sido válido previamente, pero en este momento estaría expirado).

5.11.2.2 REMOTE *USER-TO-SITE* VPN (*GLOBALPROTECT™*)

217. *GlobalProtect* proporciona una completa infraestructura para gestionar sus usuarios móviles y permitir su acceso seguro independientemente del tipo de dispositivo y de la localización del mismo.

218. La infraestructura de *GlobalProtect* tiene tres componentes:

- ***GlobalProtect Portal:*** El portal *GlobalProtect* proporciona las funciones de administración para su infraestructura de *GlobalProtect*. Es el punto de entrada al servicio para los dispositivos móviles y es el encargado de enviar a los mismos la información del portal, los *GlobalProtect Gateways* disponibles, así como los certificados de cliente que puedan ser necesarios para conectarse con estos *Gateways*.

  El portal también es el encargado de la distribución de la aplicación *GlobalProtect* a los dispositivos finales con sistemas operativos Windows y MacOS (para IOS y Android, se distribuye directamente desde las tiendas de aplicaciones correspondientes).

  Si se está utilizando la funcionalidad HIP (*Host Information Profile*), el portal define la información a recopilar de los dispositivos acorde a su política de seguridad.

- ***GlobalProtect Gateways*:** Los *gateways* de *GlobalProtect* son los dispositivos que realmente realizan el túnel seguro y proporcionan la seguridad al tráfico de las aplicaciones *GlobalProtect*.

  Si la función HIP está habilitada, la puerta de enlace genera un informe HIP a partir de los datos del dispositivo relacionado con las aplicaciones que está usando y con esta información, se podría usar para asegurar el cumplimiento de la política de seguridad.

  Se pueden configurar varios *GlobalProtect Gateways* en función de la localización (cada usuario se conectaría al más cercano), del tipo de usuario (separando los *gateways* de usuarios internos de los de colaboradores/usuarios externos) o para permitir un despliegue masivo y poder tener una solución escalable.

Se podría configurar el portal y el *Gateway* sobre el mismo NGFW o distribuirlo en varios.

- ***GlobalProtect APP*:** Se refiere al *software* que se instala en los dispositivos finales y que permite el acceso a los recursos de red a través de los portales y *gateways* desplegados.

  La aplicación para Windows y MacOS se puede obtener desde el propio Portal y a través del mismo, se pueden configurar las características de dicha aplicación.

Nota: Para ver las opciones disponibles de configuración de la aplicación, consulte los siguientes enlaces de versiones 10.1 y posteriores:
https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-portals/define-the-globalprotect-app-configurations
https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-portals/customize-the-globalprotect-app

La aplicación para dispositivos IOS y Android está disponible en la Apple Store y Google Play.

Nota: Para ver el listado completo de los dispositivos compatibles con GlobalProtect APP y la forma de distribuirlo, consulte:
https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-overview/what-os-versions-are-supported-with-globalprotect
https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-apps/deploy-the-globalprotect-app-software

219. En la siguiente figura se muestra como los componentes de GlobalProtect trabajan de forma coordinada para permitir el acceso de todos los tipos de usuarios:

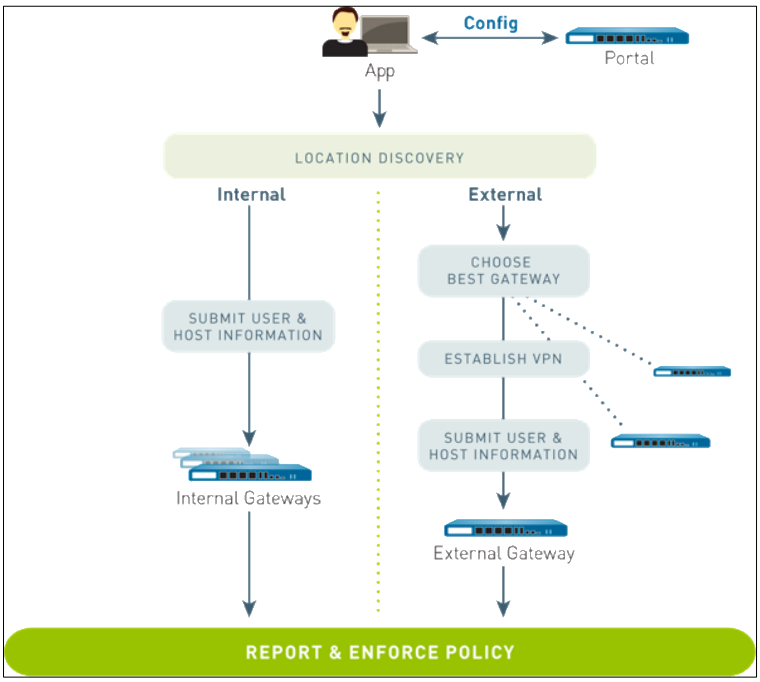


Figura 5-55: Componentes de GlobalProtect

220. Para configurar *Global Protect*, se deben realizar varias acciones:

- Configuraciones previas: Se deben realizar unas configuraciones previas a nivel de red, certificados digitales y autenticación que, posteriormente, se aplicarán a los componentes de GlobalProtect.

- Configuración de GlobalProtect Gateway.

- Configuración de GlobalProtect Portal.

- Instalación y configuración de *GlobalProtect APP.*

Nota: En el siguiente apartado de la documentación encontrará información detallada de GlobalProtect:
https://docs.paloaltonetworks.com/globalprotect

1. Configuraciones previas

221. En primer lugar, se debe configurar un interface túnel, que será en el que se configure *GlobalProtect*.

222. **Ubicación:** "*Network > IPSec Tunnels*"

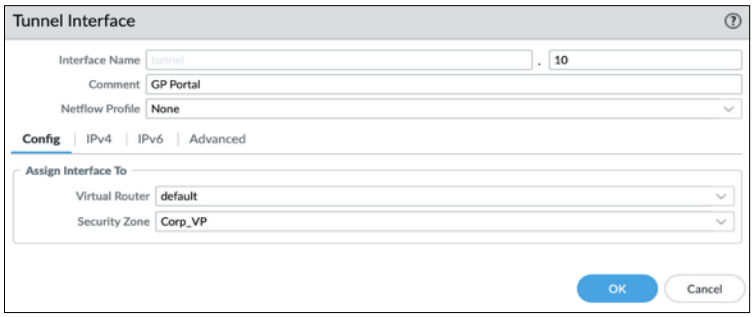


Figura 5-56: Configuración de interface tunnel

223. **Recomendación:** Asigne la zona de seguridad acorde a la arquitectura de red. Como norma general, se recomienda utilizar una zona específica para las VPNs para simplificar la gestión de estas y separarlas del resto de redes locales.

224. En segundo lugar, importar/generar el certificado digital a utilizar por el Portal. *GlobalProtect* utiliza certificados digitales para autenticar al servidor y, de forma opcional, a los dispositivos finales.

225. Para poder gestionar estos certificados es necesario tener un certificado para autenticar al servidor. Para ello, se importa el certificado emitido para este servicio por la CA de confianza de la organización:

226. **Ubicación:** "*Device > Certificate Management > Certificates*"

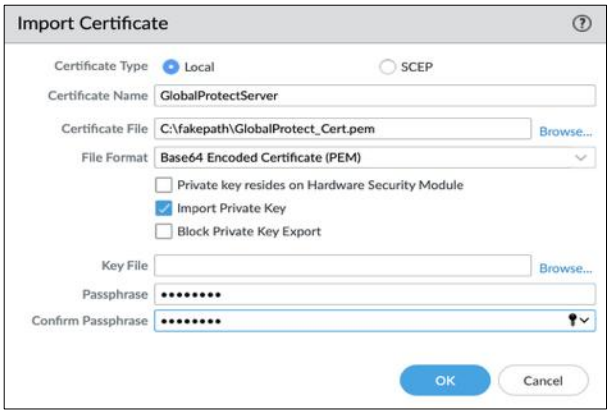


Figura 5-57: Importación de certificado

227. En el caso que no exista una CA disponible, se podría generar un certificado raíz autofirmado por la CA que lleva el cortafuegos integrado, y posteriormente un certificado para el servidor:

228. **Ubicación:** *"Device > Certificate Management > Certificate"*

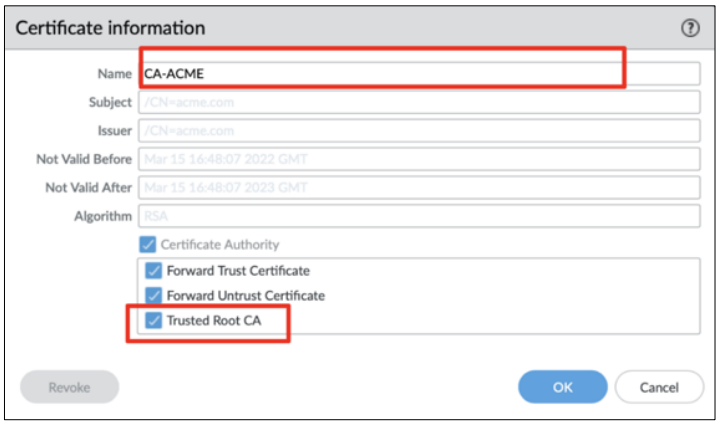


Figura 5-58: Generación de CA autofirmada

229. Para generar el certificado del servicio, generar uno nuevo y, esta vez, seleccionar la CA previamente generada como entidad firmante.

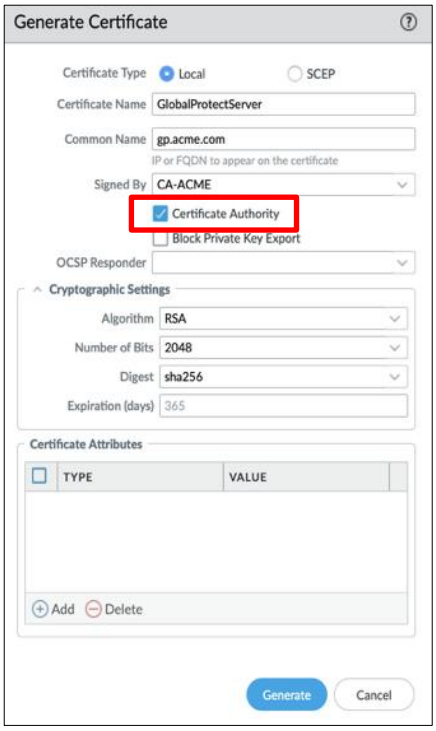


Figura 5-59: Generación de certificado autofirmado

230. Recomendación**:** Utilizar una CA externa para gestionar los certificados acordes a la política de seguridad corporativa.

231. El *Common Name* debe coincidir con el dominio al que se conectarán los dispositivos finales. A la hora de generar certificados, seguir las recomendaciones indicadas en el apartado 5.4.
232. A continuación, crear el SSL/TLS *Service Profile:*

233. **Ubicación:** "*Device > Certificate Management > SSL/TLS Service Profile*"

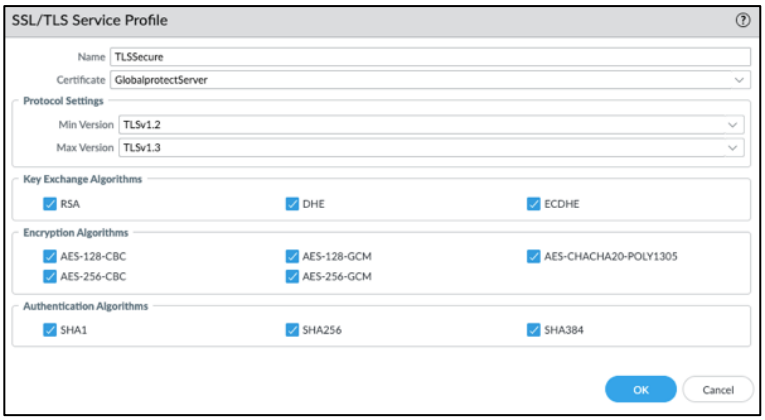


Figura 5-60: Creación de perfil SSL/TLS

234. Crear perfil de autenticación a utilizar por los usuarios del servicio:

235. **Ubicación**: *"Device > Authentication Profile"*

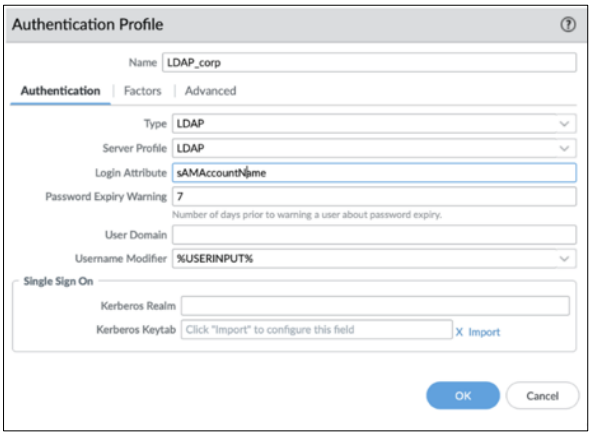


Figura 5-61: Creación de perfil de autenticación (Authentication)

236. Es posible seleccionar los usuarios a los que se les permite acceder a este servicio desde la pestaña "*Advanced*" (si la base de datos es LDAP y está integrado el equipo en *User-ID*, visto en anteriores apartados de la guía, es posible seleccionar grupos a los que se les permite acceder a este servicio):

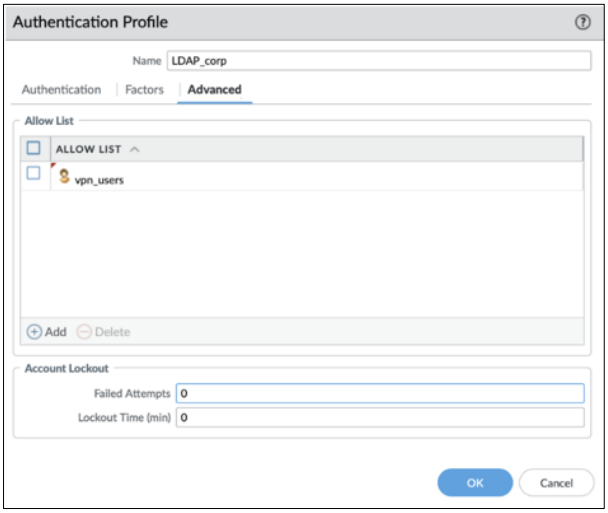


Figura 5-62: Creación de perfil de autenticación (Advanced)

237. **Recomendación:** Se recomienda utilizar un servicio externo de autenticación como LDAP o RADIUS. En caso de que no sea posible, también se puede crear una base de datos local para autenticar a los usuarios.

238. A continuación, crear perfil de autenticación a utilizar por los usuarios del servicio:

239. **Ubicación:** "*Network > Network Profiles > GlobalProtect IPSec Crypto*"

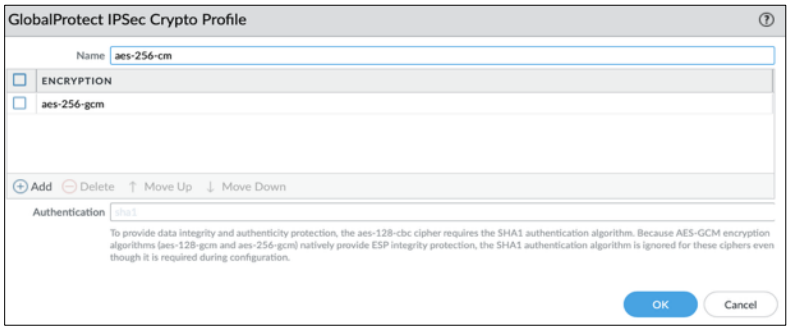


Figura 5-63: Configuración de perfil IPSec de GlobalProtect

240. **Requisito de seguridad:** Seguir las recomendaciones realizadas en el apartado 5.2.1, respecto a los algoritmos y funciones criptográficas a utilizar en *IKE/IPsec*.

2. Configuración de *GlobalProtect Gateways*

241. **Ubicación:** "*Network > GlobalProtect > Gateways*"

242. En la pestaña General, se indica el interface y la IP a la que se conectarán los dispositivos:

Figura 5-64: Configuración de GlobalProtect Gateway (General)

243. En la pestaña Authentication, se indica el perfil SSL/TLS creado en pasos anteriores (ver apartado 5.2.2) y se asocia a los clientes con el perfil de autenticación correspondiente (se podría asociar un perfil de autenticación para cada tipo de cliente en función del sistema operativo).

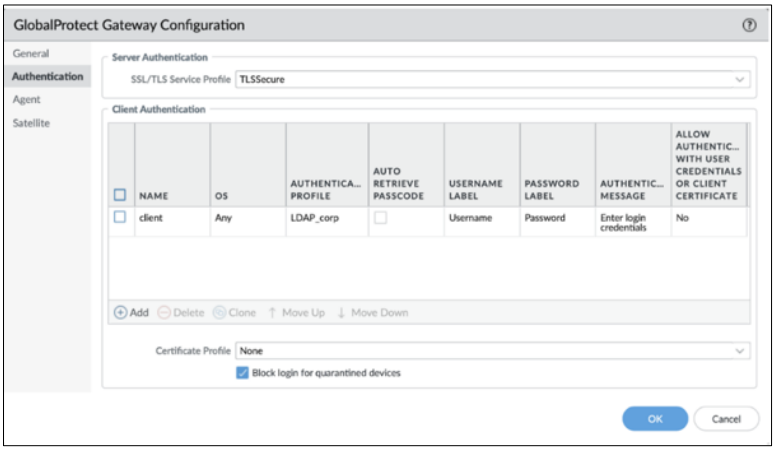


Figura 5-65: Configuración de GlobalProtect Gateway (Authentication)

244. En la pestaña *Agent*, se realizan configuraciones correspondientes a los agentes:

- Se asocia el túnel que va a cursar el servicio GlobalProtect, y el perfil *crypto IPsec* correspondiente.

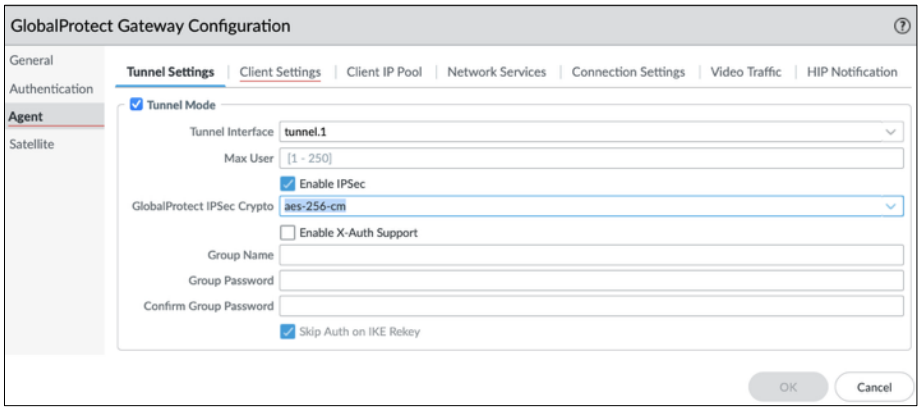


Figura 5-66: Configuración de GlobalProtect Gateway (Agent)

- Se configura el *timeout* de sesión:

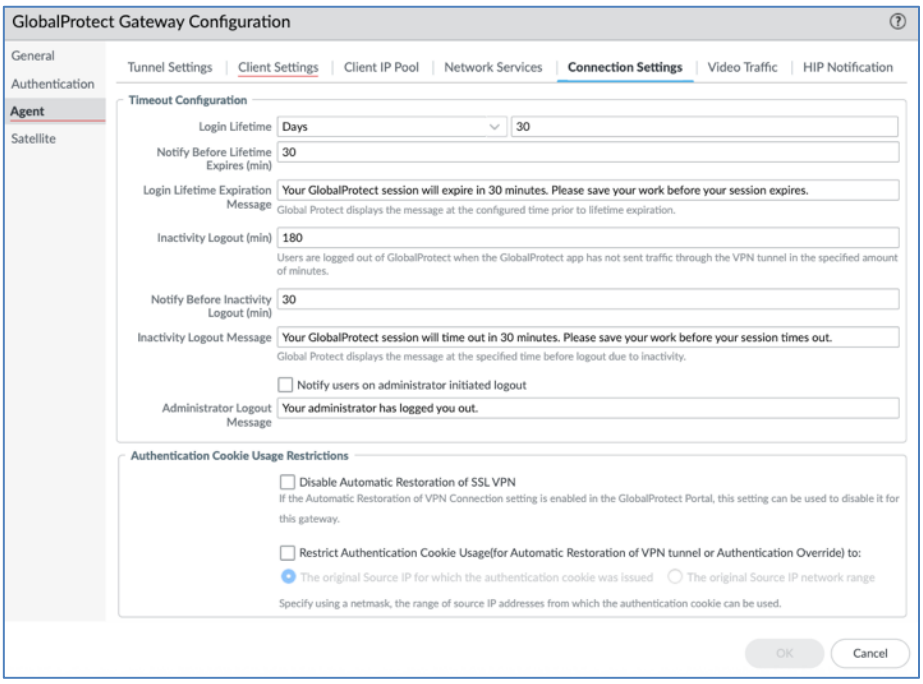


Figura 5-67: Configuración de GlobalProtect Gateway (Timeout Settings)

- Se configuran las IPs locales a asignar a los dispositivos, y ruta distribuida que dará acceso a los recursos internos de red (en este punto se podrían asignar rangos distintos en función del usuario/grupo de usuario o del sistema operativo):

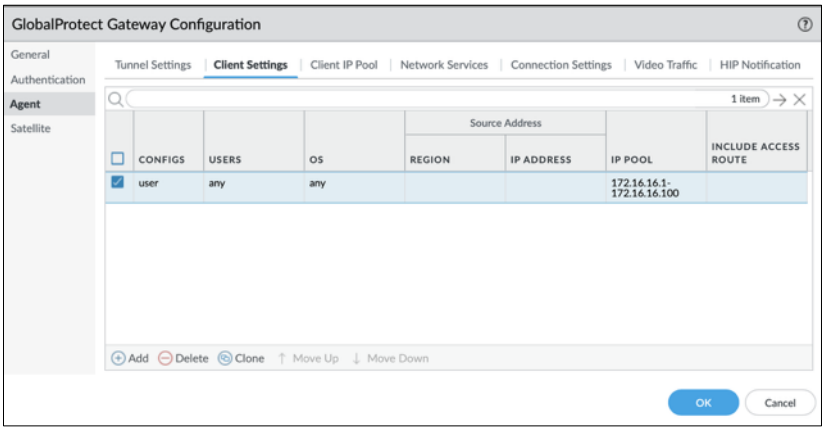


Figura 5-68: Configuración de GlobalProtect Gateway (Client Settings)

- Se configura los servidores DNS internos:

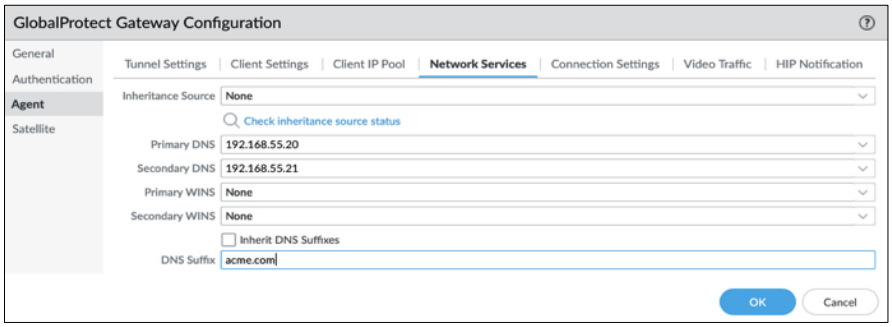


Figura 5-69: Configuración de GlobalProtect Gateway (Network Services)

3. Configuración de GlobalProtect Portal

245. **Ubicación**: "*Network > GlobalProtect > Portals*"

- En la pestaña General, se indica el interface y la IP a la que se conectarán los dispositivos, así como la apariencia de la web del portal, que puede ser personalizada desde "*Device > Response Pages":*

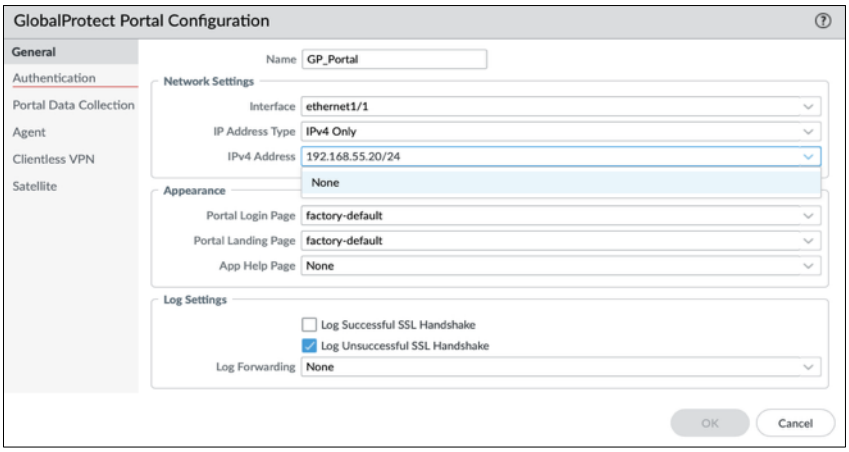


Figura 5-70: Configuración de GlobalProtect Portal (General)

- En la pestaña *Authentication*, se configuran los parámetros de autenticación, similar a los configurados previamente en el *Gateway*:

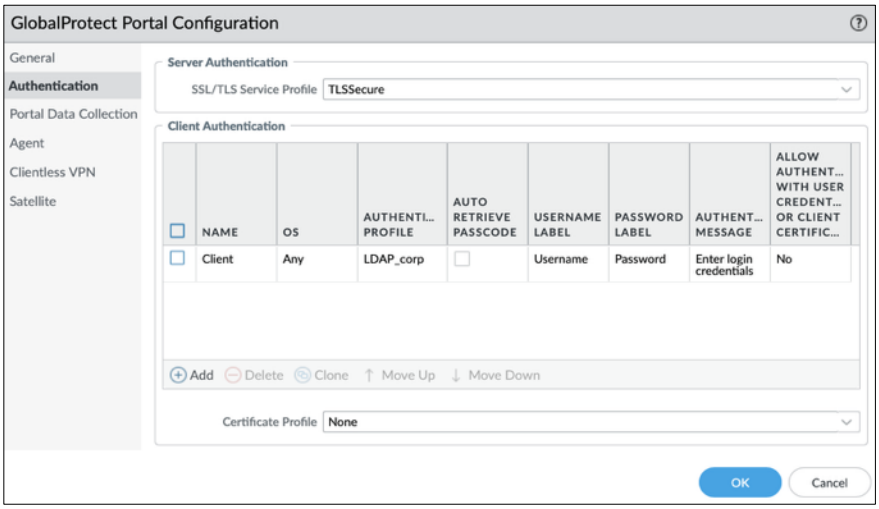


Figura 5-71: Configuración de GlobalProtect Portal (Authentication)

- En la pestaña *Agent*, se configuran los parámetros de los agentes, y se asocian al gateway creado anteriormente:

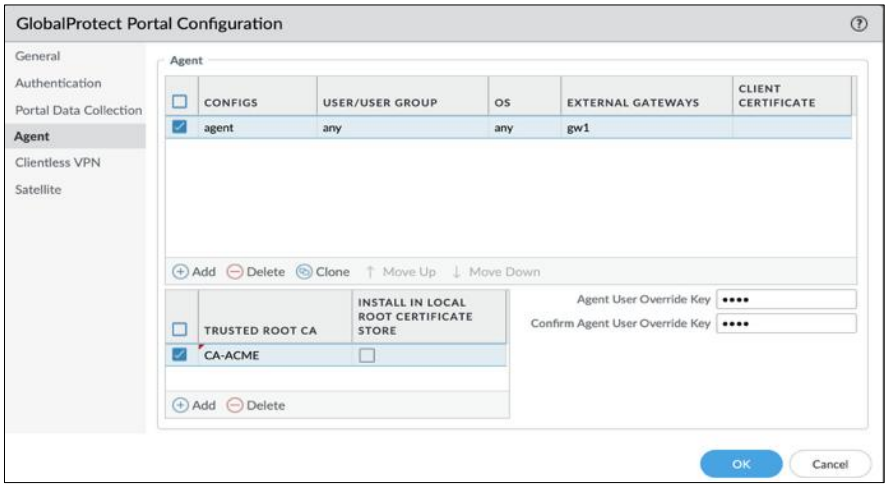


Figura 5-72: Configuración de GlobalProtect Portal (Agent)

246. Como ya se ha comentado, se podrían asignar diferentes *gateways* (internos y/o externos) en función del usuario/grupo de usuario o el sistema operativo de los dispositivos (añadiendo tantos tipos de agentes como sean necesarios).

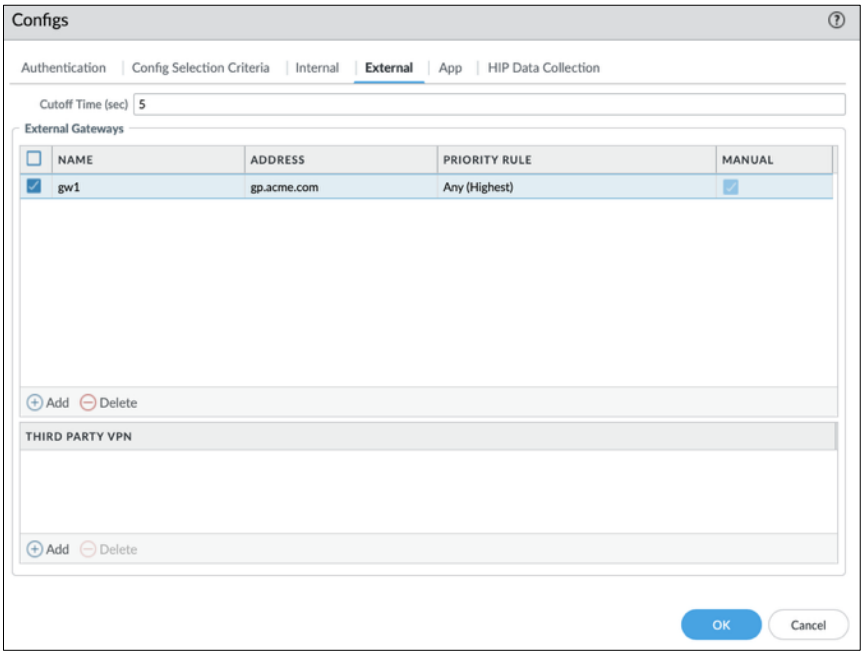


Figura 5-73: Configuración de GlobalProtect Portal (*External*)

4. GlobalProtect APP

247. El agente a utilizar en el portal se gestiona desde el cortafuegos. Para ello:

248. **Ubicación: "***Device > GlobalProtect Client*"

Figura 5-74: Selección de agente GlobalProtect a utilizar

249. Por último, faltaría instalar *GlobalProtect* APP en los dispositivos finales:

- Windows/MacOS: El *software* está disponible en la web del Portal. Acceder a la misma mediante HTTPS, introducir unas credenciales válidas y descargar el agente correspondiente al sistema operativo.

Figura 5-75: GlobalProtect Portal y descarga de agente

- Dispositivos móviles IOS / Android: Obtener la aplicación correspondiente desde *Apple Store* o *Google P*lay. Una vez descargado el agente, será necesario introducir el nombre del Portal (FQDN) y las credenciales.

Figura 5-76: Pantalla de inicio de aplicación GlobalProtect (Windows / MacOS)

Figura 5-77: Pantalla de inicio de aplicación GlobalProtect (MacOS)

5. Resultado

250. Una vez conectado, se muestra un mensaje por defecto como el siguiente:

Figura 5-78: Comprobación de estado de la conexión VPN (Windows / MacOS)

251. Si se desea ver más información en el agente, se abrirían las opciones:

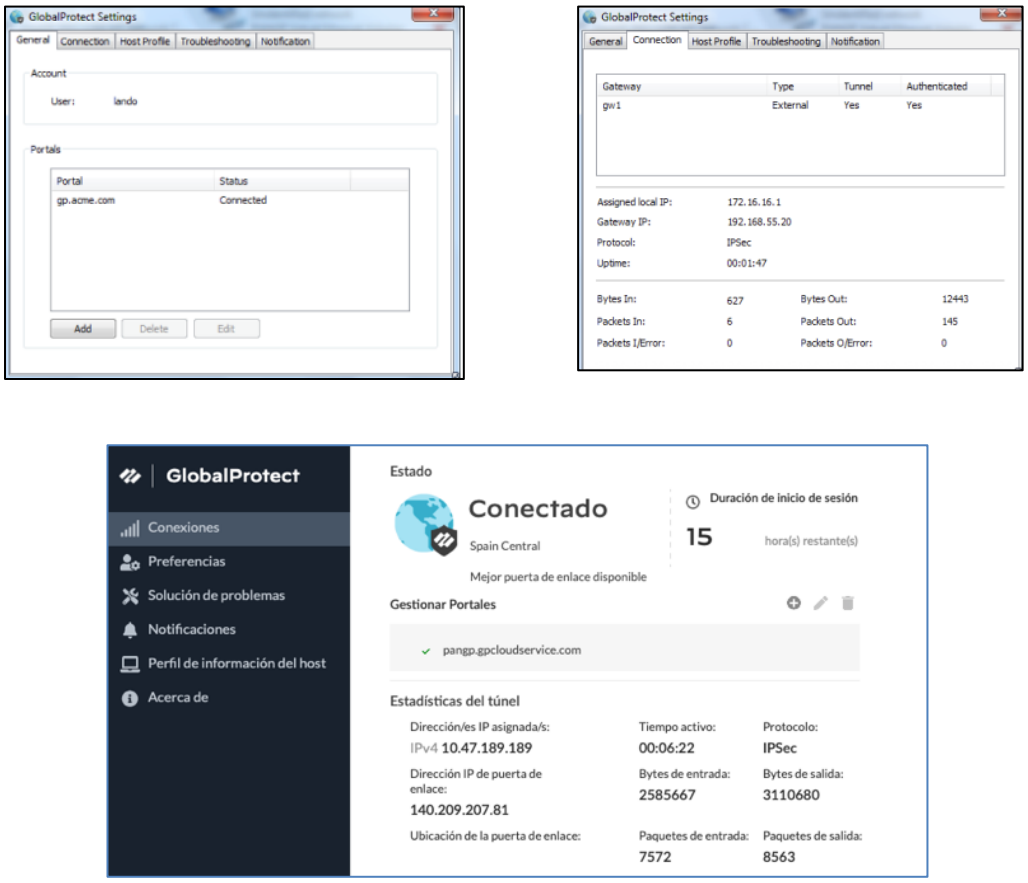


Figura 5-79: Comprobación de estado del Agente (Windows / MacOS)

252. En los logs del cortafuegos, también se pueden consultar los eventos en "*Monitor > System*":

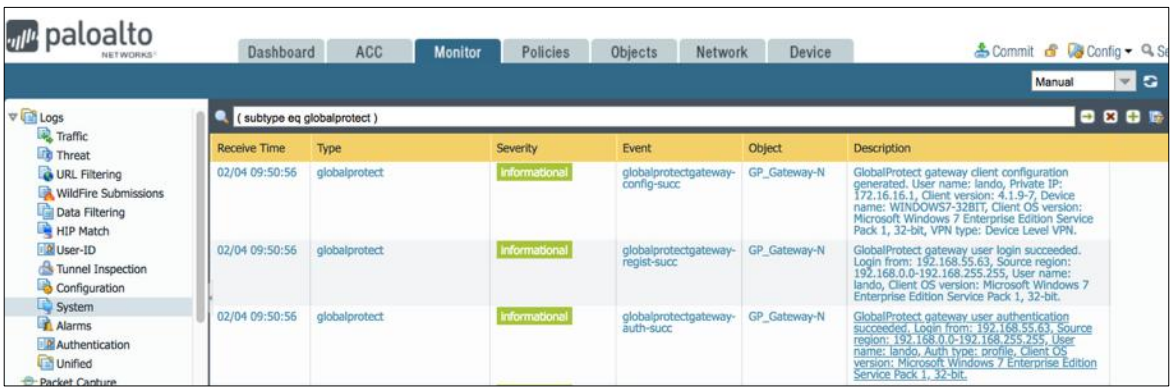


Figura 5-80: Logs de GlobalProtect

5.11.3 IDENTIFICACIÓN DE APLICACIONES (*APP-ID™*)

253. En los entornos de red modernos la identificación de la aplicación es un componente crítico para poder construir una política de seguridad efectiva. Durante los últimos años, el uso tanto de Internet, como de las redes internas, se ha incrementado de manera importante, lo que ha resultado en una gran cantidad de aplicaciones que ahora acceden a los servicios de red.

254. En general, se observan las siguientes tendencias cuando se analiza el comportamiento de las aplicaciones en la red:

- Muchas aplicaciones están diseñadas para acceder a Internet sobre el puerto 80, utilizando el protocolo HTTP, o utilizan el puerto 80 en caso de que su puerto regular esté bloqueado.

- El cifrado SSL/TLS es cada vez más utilizado con la intención de tunelizar las aplicaciones y que no sean visibles en su camino.

- Las aplicaciones internas, con frecuencia utilizan muchos puertos o puertos dinámicos para facilitar la comunicación entre los extremos.

- El uso de cortafuegos tradicionales que no son capaces de diferenciar las aplicaciones basándose solamente en el puerto y el protocolo.

255. Las propias aplicaciones pueden utilizarse como plataforma para lanzar los ataques y, en muchas ocasiones, transportan las amenazas al interior de la red. La identificación y el control de la aplicación ayudan en la reducción de la superficie de ataque.

256. Todos los sistemas, servicios, aplicaciones y usuarios de la red son un objetivo potencial para los cibercriminales. Al crear políticas de seguridad que realmente se basen en la identificación de la aplicación, en lugar de solamente en el puerto o protocolo, es posible reducir el riesgo al que se encuentran expuestos los sistemas y redes. Esto se consigue permitiendo solamente aquellas aplicaciones que son necesarias y, por tanto, bloqueando todas las demás.

257. En el caso de los cortafuegos de Palo Alto Networks, el módulo encargado de realizar la identificación de la aplicación se denomina ***App-ID™***. App-ID es un sistema patentado de clasificación de tráfico disponible exclusivamente en los cortafuegos de Palo Alto Networks.

258. Su objetivo es identificar la aplicación real que el usuario está empleando, así como la función concreta en cada momento (por ej. no solamente *facebook*, sino el *chat* de *facebook*), independientemente del puerto, protocolo, cifrado (SSH o SSL). Aplica múltiples mecanismos de clasificación (firmas de aplicación, decodificación de protocolo de aplicación y heurística) al flujo de tráfico de red para identificar las aplicaciones con precisión.

259. Además, la inteligencia de este mecanismo es heredada por el resto de los módulos de manera que la aplicación, y sus características, se tienen en cuenta a la hora de buscar

posibles ataques, realizar controles de ancho de banda, etc. La siguiente figura muestra el detalle del algoritmo que se utiliza en la identificación de las aplicaciones.

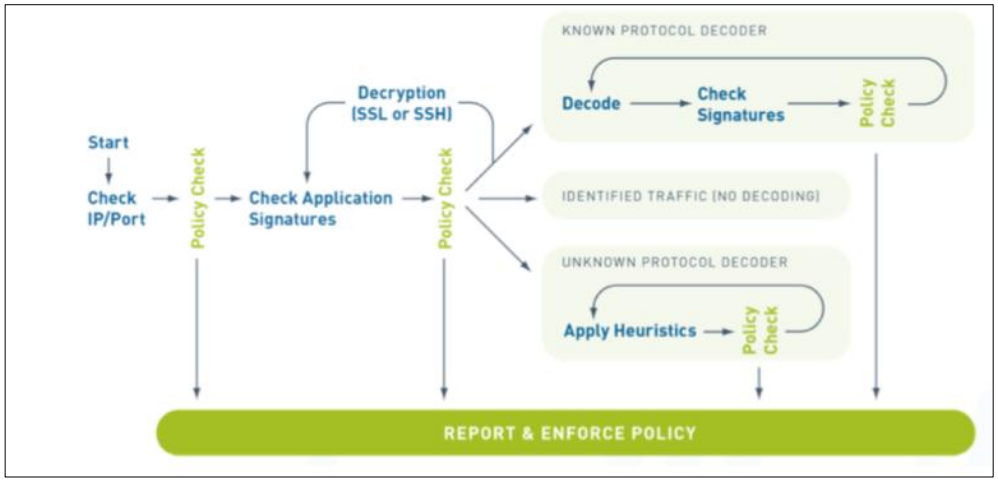


Figura 5-81: Algoritmo de *App-ID*

260. La identificación de la aplicación permite también detectar tácticas evasivas o ataques de manera genérica, lo que supone una cobertura superior, especialmente frente a sitios o técnicas nuevas. Por ejemplo, si se quiere evitar que los usuarios utilicen técnica de evasión (sistemas que encapsulan nuestras peticiones de navegación, para que parezcan legítimas cuando realmente no lo son) se puede, por supuesto, utilizar el filtrado de URL, que será efectivo para los sitios conocidos.

261. Ahora bien, surgen nuevos sitios a diario, por lo que no es complicado encontrar alguno nuevo aún no categorizado por el motor de filtrado. En este supuesto el mecanismo basado en URL no sirve, porque el sitio es desconocido; sin embargo, el mecanismo de identificación de la aplicación sí sería capaz de detectarlo, en base a identificar qué tecnología utiliza el sitio y bloquearla si así lo establece la política de seguridad corporativa (algunos ejemplos de este tipo de aplicaciones serían: *glype-proxies, cgi-proxies, php-proxies,* ...).

262. Asimismo, es muy importante señalar que, puesto que el equipo no actúa como proxy, todo el proceso de identificación y control de aplicaciones es transparente para los usuarios, independientemente de la aplicación que estén utilizando. Es decir, no hay aplicaciones "*proxificables*" o no "*proxificables*", todas se controlan de igual modo.

Nota: Se puede obtener una vista detallada de todas las aplicaciones soportadas entrando en la pestaña *Objects* de cualquier cortafuegos, o visitando:
https://applipedia.paloaltonetworks.com/
En los siguientes enlaces encontrará información complementaria sobre App-ID:
https://www.paloaltonetworks.com/technologies/app-id
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/app-id

5.11.3.1 COMBATIENDO LA CADENA DE CIBERATAQUE

	Entrega	Explotación	Instalación	Mando y Control	Acciones en el Objetivo
APP ID	Bloquear aplicaciones de alto riesgo Descifrar SSL			Bloquear C2 sobre puertos no estándar	Prevenir la exfiltración de datos y el movimiento lateral

Tabla 46: Cadena de ciberataque – App-ID

263. App-ID juega un rol muy importante en diferentes fases de la cadena de ataque. Puede controlar la fase de entrega si se bloquea o controla el acceso de los usuarios a las aplicaciones que se utilizan normalmente para el envío del código dañino, como pueden ser las redes sociales, correos electrónicos personales y las aplicaciones de compartición de archivos. Durante el proceso de identificación de la aplicación, App-ID también puede realizar el descifrado SSL, para evitar que las aplicaciones cifradas no sean inspeccionadas.

264. Un caso de uso específico de la identificación de la aplicación es la capacidad del motor App-ID para identificar y controlar las aplicaciones desconocidas. Estas aplicaciones no forman parte de la base de datos de aplicaciones y se representan como *unknown-udp, unknown-tcp* o *unknown-p2p.*

265. En relación con utilizar App-ID como mecanismo de prevención de amenazas, la capacidad de identificar y controlar las aplicaciones desconocidas permite bloquear las comunicaciones del código dañino. El motivo es que el código dañino muchas veces utiliza protocolos propietarios para comunicarse con los servidores externos de mando y control a través de puertos estándar y, en muchas ocasiones, este tráfico se identificará como "*unknown*". Obviamente una política de seguridad configurada adecuadamente no debería permitir el tráfico desconocido o debería al menos controlarlo de manera muy precisa.

266. Por último, App-ID puede reforzar la arquitectura "*Zero Trust"* al limitar el uso de las aplicaciones en función de los grupos de usuarios. Esto puede limitar las capacidades de movimiento lateral y exfiltración de datos a través de aplicaciones específicas.

5.11.3.2 REQUISITOS DE SEGURIDAD

267. El principio clave a aplicar cuando se define una política de cortafuegos basada en aplicaciones, es seguir una aproximación basada en lógica positiva. **La lógica positiva (*Default Deny*) implica que selectivamente se permite sólo lo estrictamente necesario**, generalmente aplicado a sistemas basados en "listas blancas"Por el contrario, una aproximación basada en lógica negativa (*Default Allow*) se fundamenta en permitir todo aquello que no está expresamente prohibido. De la misma forma, es un principio generalmente aplicado a sistemas basados en "listas negras". Esta última es una práctica muy poco recomendable por su difícil gestión (requiere estar monitorizando

constantemente las nuevas aplicaciones) y porque deja una superficie de ataque mucho mayor.

268. Una aproximación fundamentada sobre lógica positiva simplemente requiere que se habilite la lista "blanca" de aplicaciones permitidas y que el cortafuegos bloquee todo lo demás a través de la regla de fin de política, tal y como muestra la siguiente figura de manera simplificada.

				Source			Destination					
	Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	URL Category	Action
1	Aplicaciones-Permitidas	none	universal	LAN	any	any	Internet	any	dns flash ssl web-browsing	application-default	any	Allow
2	Deny-All	none	universal	any	any	any	any	any	any	any	any	Deny

Figura 5-82: Ejemplo de política de aplicaciones basada en lógica positiva

269. Cuando se migra de una política de cortafuegos basado en puertos a una basada en aplicaciones, la tarea más importante es determinar qué aplicaciones deberían permitirse en la operativa diaria. Si no existe una lista bien definida de aplicaciones, entonces la recomendación es configurar primero el equipo de Palo Alto Networks como un cortafuegos tradicional, basado en puertos, o desplegarlo en modo monitorización para obtener primero la lista de las aplicaciones que hay en la red.

270. Después, esta lista debería examinarse para seleccionar solamente las que estén permitidas por la política de seguridad. En este sentido Palo Alto Networks cuenta con una herramienta de migración de políticas de seguridad, para facilitar la transición, denominada *Expedition*.

1. Usar aplicaciones en las políticas de seguridad

271. **Ubicación**: "*Policies* > *Security*"

272. **Requisito de seguridad :** Hacer uso del criterio por aplicación en tantas reglas como sea posible, idealmente en todas, porque ayuda a reducir sustancialmente la superficie de ataque y controlar los vectores de propagación de las amenazas.

2. Evitar el uso del *service any*

273. **Ubicación**: "*Policies* > *Security*"

274. **Requisito de seguridad:** La columna Service regula el puerto por el que se permite que circule el tráfico. Se debe evitar el uso de la opción any (cualquier puerto), para minimizar la superficie de ataque. En su lugar, debe utilizarse application-default, que solamente permite los puertos por defecto de las aplicaciones especificadas en la regla o, en su lugar, una lista de puertos personalizados.

3. Configurar un *deny* explícito como última regla

275. **Ubicación**: "*Policies* > *Security*"

276. **Requisito de seguridad :** Se debe configurar una regla explícita de tipo Deny como última regla de la política de seguridad, para que el sistema registre en los logs, cualquier tráfico denegado y puedan ser revisados posteriormente.

Nota: Cuando se añade la regla que bloquea todo lo demás, "*Deny-All*" en nuestro ejemplo, se sobrescriben las reglas por defecto *intrazone* e *interzone*, por lo que se puede bloquear sin querer conexiones intrazona. Asegúrese de añadir las reglas intrazona que requiera antes de la regla de bloqueo general.

4. Crear aplicaciones específicas para el tráfico propietario

277. **Ubicación**: "*Objects* > *Applications*"; "*Policies* > *Security*"; "*Policies* > *Application Override*"

278. **Requisito de seguridad**: Según se mencionó anteriormente, se debe minimizar el tráfico desconocido. Para ello, es necesario caracterizar las aplicaciones propietarias que, por defecto, el sistema identifique como *unknown*.

279. Si es necesario trabajar a nivel 4, es posible utilizar *Application Override*, dentro de *Policies*.

Nota: Puede encontrar información detallada sobre cómo crear aplicaciones propietarias en: *https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/app-id/manage-custom-or-unknown-applications*

280. A modo de ejemplo, las siguientes imágenes muestran cómo crear una aplicación propietaria, basada en la identificación de una *Cookie* de sesión particular:

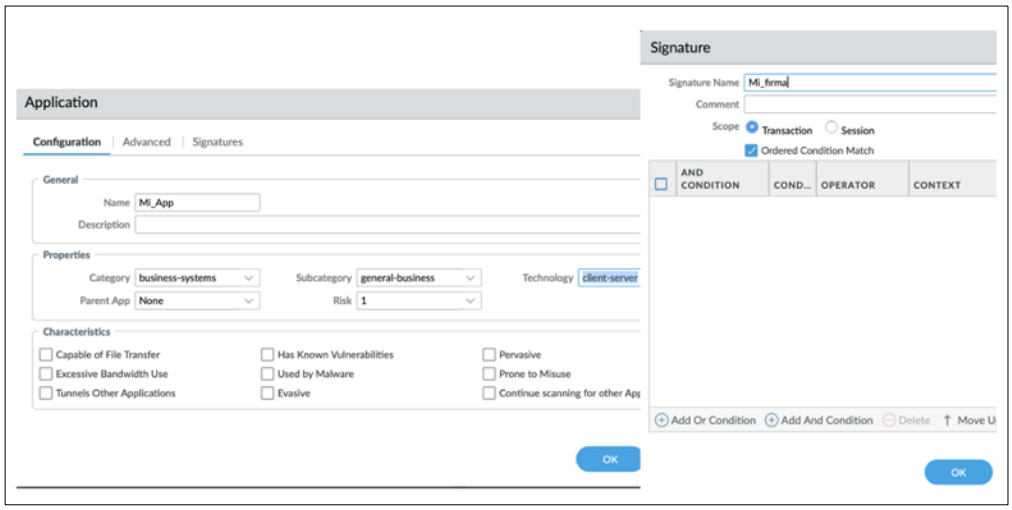


Figura 5-83: Definición de aplicaciones propietarias

5.11.3.3 EJEMPLO DE USO

281. En el apartado de ejemplo de uso de cada sección, se creará una configuración que describa cómo habilitar y desplegar cada función concreta en la política de seguridad. Se recuerda que, para el ejemplo, se trabaja en una instalación en la que hay cuatro zonas diferentes de seguridad: Internet, DMZ, LAN y Datacenter.

282. La primera parte de este ejemplo de uso se centrará en controlar el acceso a las aplicaciones desde equipos externos hacia los servicios que se publican, como por

ejemplo servidores web o de correo. En este caso, se crean dos (2) políticas de acceso para estos servicios (web y correo):

				Source			Destination					
	Name	Tags	Type	Zone	Address	User	Zone	Address	Application	Service	URL Category	Action
1	Acceso web externo	DMZ	universal	Internet	any	any	DMZ	Servidor-web-externo	flash icmp ssl web-browsing	application-default	any	Allow
2	Acceso mail externo	DMZ	universal	Internet	any	any	DMZ	Servidor-correo-externo	activesync icmp imap pop3 smtp ssl web-browsing	application-default	any	Allow
3	Salida mail externo	DMZ	universal	DMZ	Servidor-correo-externo	any	Internet	any	dns smtp	application-default	any	Allow

Figura 5-84: Política de protección de DMZ en entrada

283. Para permitir la salida desde la DMZ, se añade una regla extra:

4	Updates DMZ	DMZ	universal	DMZ	any	any	Internet	any	apt-get dns ms-update ssl symantec-av... web-browsing	application-default	any	Allow

Figura 5-85: Política de protección de DMZ en salida

284. Al definir el acceso en base a la aplicación, en vez de el puerto o el protocolo, cualquier tráfico hacia servicios públicos que no cuadre con la aplicación será denegado. Esta aproximación permite reducir la superficie de ataque al deshabilitar el acceso de cualquier aplicación que pudiera haberse configurado sin querer en los servidores pero que no es necesaria realmente.

5.11.3.4 OBSERVABLES

Logs

285. Es posible ver la actividad de las aplicaciones consultando "*Monitor > App Scope > Network Monitor*". También es posible hacer un análisis en profundidad utilizando el *Application Command Center (ACC).*

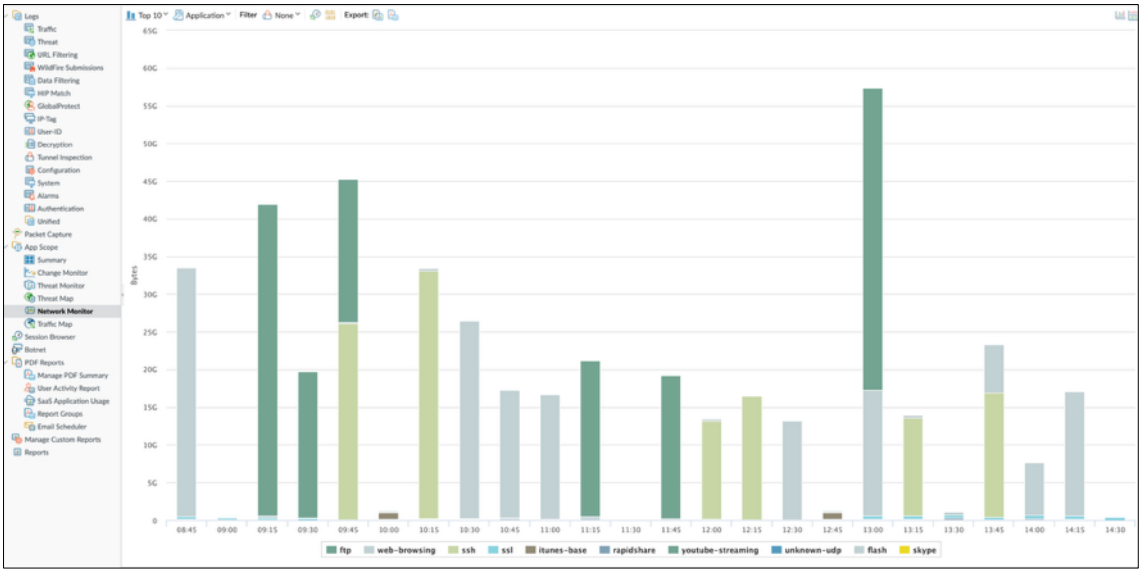


Figura 5-86: Visibilidad de aplicaciones con AppScope

286. El tráfico que haga *match* con una regla, generará una entrada en el log de tráfico si el *logging* está habilitado para esa regla. Cualquier regla puede tener el *logging* activado al finalizar la sesión (acción por defecto), pero también al comienzo de esta.

		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
		09/13 18:59:22	end	LAN	LAN	192.168.45.142	acme\user2	192.168.45.255	138	netbios-dg	allow	LAN-LAN	unknown	249
		09/13 18:59:22	end	LAN	Internet	192.168.45.142	acme\user2	216.58.211.206	443	google-base	allow	LAN-Internet	unknown	3.8G
		09/13 18:59:22	end	LAN	LAN	192.168.45.142	acme\user2	192.168.45.255	137	netbios-ns	allow	LAN-LAN	unknown	2.6k

Figura 5-87: Ejemplo de Traffic logs

Aplicaciones desconocidas

287. Cualquier instancia de tráfico identificado como *unknown-udp, unknown-tcp o unknown-p2p*, generará por defecto una captura de paquete en el log correspondiente. Estas capturas pueden proporcionar una indicación inicial sobre el tipo de tráfico que ha generado la aplicación desconocida, para que se caracterice posteriormente.

		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
		10/04 10:27:23	end	LAN	Internet	192.168.45.142		192.168.55.1	80	unknown-tcp	allow	LAN-Internet	tcp-fin	3.0k
		10/04 09:48:59	end	LAN	Internet	192.168.45.142		192.168.55.1	80	unknown-tcp	allow	LAN-Internet	tcp-fin	3.0k

Figura 5-88: Ejemplo de unknown-tcp y captura en fichero pcap

Dependencia de aplicaciones

288. Ciertas aplicaciones tienen dependencias de otras aplicaciones para operar de manera correcta. Para poder permitir una aplicación, es necesario permitir también las aplicaciones padre. El ejemplo más común de este tipo de dependencia es el caso de las aplicaciones tipo web que dependen de SSL y *web-browsing.* También es posible que, dentro de una misma aplicación, algunas funciones dependan de otras. Por ejemplo, *facebook-posting* depende de la aplicación padre *facebook-base*.

289. La aplicación *web-browsing* es muy genérica y comprende cualquier tráfico basado en HTTP que no se reconoce como otra aplicación más específica. Si el cortafuegos de Palo

Alto Networks se ubica entre los clientes y un *proxy web*, entonces cualquier tráfico proxificado se clasificará como la aplicación *http-proxy* en vez de *web-browsing.*

290. Desde la versión de PAN-OS 5.0 en adelante, las aplicaciones de dependencia se han eliminado de todas aquellas aplicaciones que pueden ser identificadas en un punto predeterminado de la sesión, y que utilizan cualquiera de los siguientes protocolos: HTTP, SSL, MS-RPC, RPC, t.120, RTSP, RTMP y NETBIOS-SS. Las aplicaciones personalizadas que se basan en HTTP, SSL, MS-RPC o RTSP pueden también permitirse en la política de seguridad sin necesidad de habilitar las aplicaciones padre. Por ejemplo, si se quieren permitir los *updates software* de Java, que utilizan HTTP, no se necesita habilitar *web-browsing.*

291. Para permitir aplicaciones concretas que tienen una dependencia explícita sobre *web-browsing*, y cuando no se desea habilitar todo el *web-browsing* al mismo tiempo, se puede configurar un perfil de *URL Filtering* que limita el ámbito de uso a las categorías que se desean permitir.

5.11.4 IDENTIFICACIÓN DE USUARIOS (*USER-ID™*)

292. La identificación de usuarios es una tarea esencial en la definición de las políticas de seguridad del cortafuegos. No es válido únicamente con conocer la dirección IP del origen de la conexión, si no el usuario y/o grupo que la inicia, ya que dicha dirección IP puede ser asignada a diferentes usuarios o lo que es peor podría ser suplantada

293. En el caso de los cortafuegos de Palo Alto Networks, el módulo encargado de realizar la identificación de usuarios se denomina ***User-ID™***.

294. El objetivo fundamental del módulo de User-ID es averiguar quién es el usuario, independientemente de la dirección IP que tenga, así como el rol que desempeña en la organización. Para ello, el equipo se integra, de modo transparente, con los directorios corporativos ya existentes de los que extrae tanto la tupla Usuario-DirecciónIP, como los grupos del directorio LDAP a los que el usuario pertenece. Una vez que esta información es obtenida, se utiliza tanto para la generación de políticas de seguridad como para la de visibilidad (informes, logs, estadísticas, etc.). Se soportan los siguientes directorios:
    - Active Directory
    - LDAP
    - eDirectory

295. Además, existe un agente de User-ID para los entornos Citrix y Terminal Services y el sistema también cuenta con una API XML y un *listener* de *syslog* que permite inyectar usuarios desde otro tipo de sistemas de información (como un servidor Radius, una solución de autenticación 802.1x, etc.).

296. Finalmente, también se cuenta con sistemas activos de autenticación de usuarios, como los barridos WMI, el portal cautivo o la solución SSL-VPN, denominada *GlobalProtect*.

297. La siguiente imagen muestra el resumen de todas las tecnologías disponibles para User-ID:

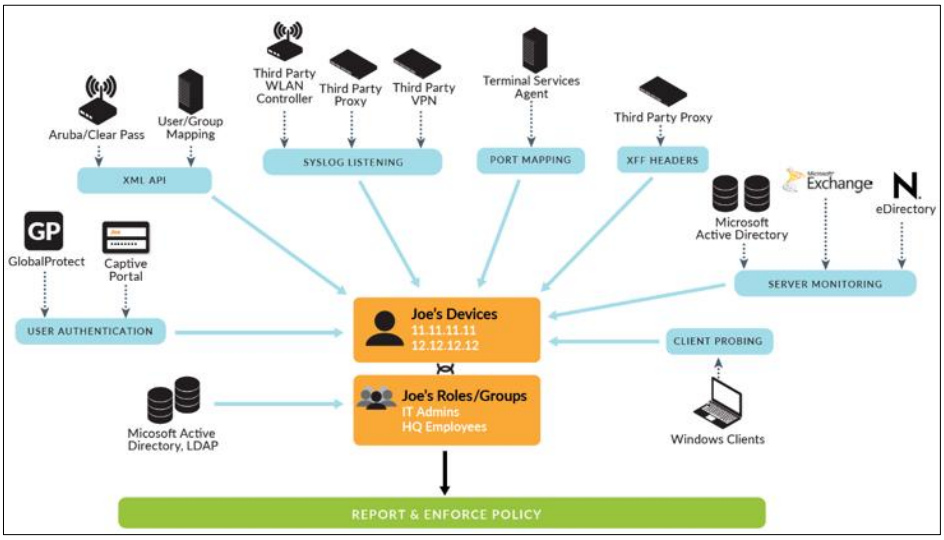


Figura 5-89: Tecnologías User-ID disponibles

Nota: Si se desea obtener más información sobre User-ID visitar: *https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/user-id*

5.11.4.1 MEDIDAS DE SEGURIDAD

298. Cuando se crean políticas basadas en usuarios y grupos, se recomienda que se creen reglas diferentes por usuario o grupo de usuarios en vez de combinar múltiples usuarios o grupos en una misma regla, incluso si requieren los mismos privilegios de acceso. Esta aproximación conseguirá que la gestión del acceso sea más sencilla para cada grupo. Ofrecerá, asimismo, mayores posibilidades de filtrado cuando se deseen crear informes personalizados, en función de las reglas.

299. Cuando se utiliza el agente software de User-ID para obtener los mapeos usuario-ip, se recomienda desplegar múltiples instancias para redundar el servicio. Además, es posible utilizar el portal cautivo conjuntamente para integrar todos los usuarios de los que no ha sido posible aprender su IP, por ejemplo, aquellos cuyas máquinas no forman parte del dominio de Active Directory.

1. Mapeo de usuario-ip para todo el tráfico de usuarios

300. **Ubicación**: “Device > User Identification”; “Monitor > Logs > URL Filtering”; “Monitor > Logs > Traffic”

301. **Recomendación**: Se recomienda configurar adecuadamente el User-ID para obtener, al menos, el mapeo usuario-IP, lo que le permitirá obtener rápidamente información sobre qué usuario está generando qué tipo de evento. Opcionalmente se puede configurar también la integración con los grupos del directorio LDAP corporativo, para poder crear reglas por grupo de usuarios en vez de por dirección IP. En este caso es importante tener en cuenta que los grupos y los contenidos han de estar bien alineados con la política de seguridad, para evitar desviaciones.

302. La integración final de User-ID dependerá en gran medida del tipo de entorno. Una vez configurado, puede comprobar fácilmente si el mapeo se está produciendo según se espera observando la columna *Source User* o *Destination User* de los logs de Tráfico o URL.

2. Deshabilitar *user-id* en los interfaces externos

303. **Ubicación**: "*Network > Zones*"

304. **Recomendación**: Se recomienda configurar el User-ID solamente en las zonas internas, donde se encuentran los usuarios confiables. Si se configura la identificación de usuarios en interfaces externos, se enviará información sensible sobre la red al exterior.

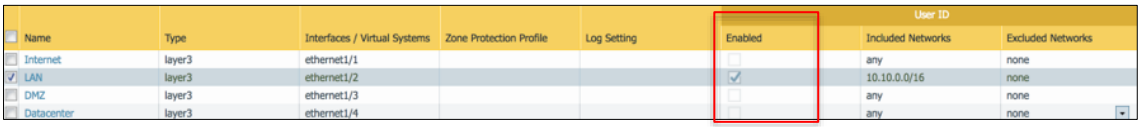


Figura 5-90: Activación de User-ID solamente en zonas internos

3. Deshabilitar WMI si no se utiliza

305. **Ubicación**: "*Device > User Identification > User Mapping > Palo Alto Networks User ID Agent Setup > Client Probing*"

306. **Recomendación**: Para poder ejecutar barridos WMI es necesario contar con una cuenta con permisos de administración en el directorio. Si no se utiliza este mecanismo para mapear usuarios, es mejor deshabilitarlo para evitar que un atacante interno pudiera lanzar ataques tipo *pass-the-hash.*

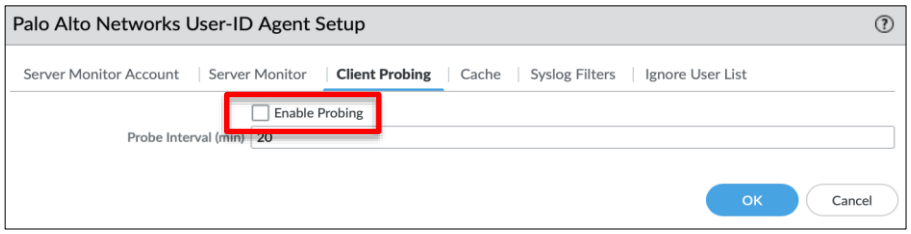
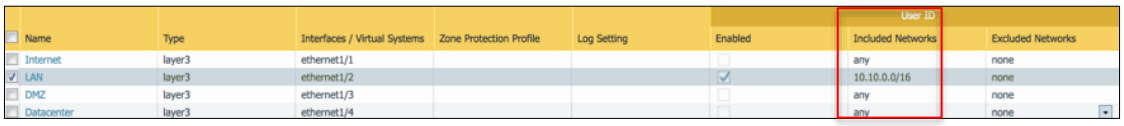


Figura 5-91: Deshabilitación de User-ID Agent probing

4. Configurar *include/exclude networks*

307. **Ubicación**: "*Network > Zones*"; "*Device > User Identification > User Mapping > Include/Exclude Networks*"

308. **Recomendación:** Para evitar aprender usuarios sobre redes no confiables, se debe añadir exclusivamente aquellas redes IP donde se encuentren usuarios confiables. Es recomendable hacer la configuración tanto en la parte de Zona como en la parte de configuración del agente.



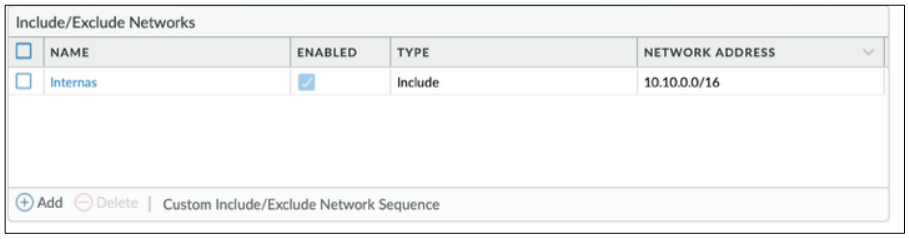


Figura 5-92: Configuración de include/exclude networks en User-ID

5. Configurar una cuenta dedicada para user-id

309. Requisito de seguridad: Se debe configurar una cuenta dedicada para User-ID, con los privilegios mínimos requeridos. A continuación, se listan los grupos a los que debe pertenecer el usuario, en función de si se utiliza el agente embebido o el agente *software*:

- Agente User-ID embebido: Distributed COM Users y Event Log Readers.
- Agente User-ID software: Domain Users y Event Log Readers.
- *Grupo Server Operators*. Este grupo es necesario en ambos casos si se desea monitorizar las sesiones abiertas (como, por ejemplo, las carpetas compartidas o las impresoras de red). Puesto que los miembros de este grupo tienen también privilegios para apagar o reiniciar servidores, se debe utilizar exclusivamente si va a monitorizar estas sesiones.

310. Se deben eliminar los siguientes privilegios de cuenta dedicada:

- Eliminar el logon interactivo. Aunque la cuenta necesita acceder a determinados logs, no requiere hacer login interactivo en el dominio o servidores. Se puede eliminar este privilegio desde las *Group Policies* o utilizando una cuenta de servicio gestionada.

- Eliminar el acceso remoto. Para evitar que un atacante pueda utilizar esta cuenta de manera remota si se viera comprometida.

311. Si va a utilizar la autenticación basada en Portal Cautivo transparente con el agente embebido, la recomendación es que utilice Kerberos en lugar de NTLM. NTLM es un protocolo menos seguro y requiere que el cortafuegos se una al dominio, mientras que Kerberos es más seguro, ofrece autenticación más fuerte y no requiere que el cortafuegos se una al dominio.

Nota: Puede encontrar información detallada sobre la configuración de las cuentas de usuario en:
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/user-id/map-ip-addresses-to-users/create-a-dedicated-service-account-for-the-user-id-agent

6. Restringir el tráfico de user-id hacia zonas inseguras

312. **Ubicación**: "*Device > Setup > Services > Service Route Configuration*"; "*Policies > Security*"

313. **Recomendación:** Controlar el tráfico que el agente de User-ID -*software* o embebido- genera, para evitar que circule hacia redes no confiables. Para ello, es necesario bloquear la aplicación *msrpc* y *ms-wmi* a través de una regla específica en la política de seguridad.

314. Para el agente embebido, este tráfico se genera por defecto desde la IP de gestión, asignada en el *Management Plane.*

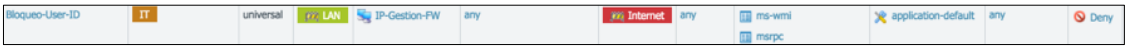


Figura 5-93: Restricción del tráfico del agente User-ID

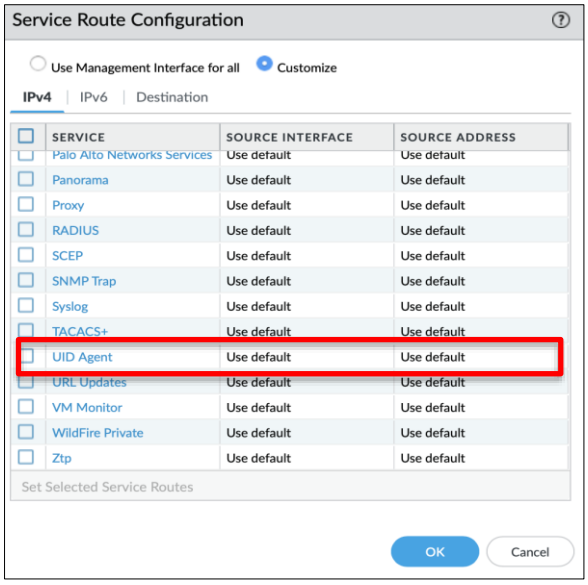


Figura 5-94: Configuración del interfaz de User-ID

5.11.4.2 EJEMPLO DE USO

315. Para construir la política de seguridad del ejemplo se ha determinado que se requieren las siguientes aplicaciones para cada uno de los departamentos, según se muestra en la siguiente tabla:

	Ventas	Marketing	IT	Recursos Humanos	Gestión
web-browsing	√	√	√	√	√
linkedin	√	√		√	√
facebook-base		√		√	
facebook-posting		√			
twitter		√			
google-analytics		√			
salesforce	√				√
webex	√				√
google-maps	√				
adobe-update			√		
paloalto-update			√		

	Ventas	Marketing	IT	Recursos Humanos	Gestión
ms-update			√		

Tabla7: Requisitos de aplicaciones y grupos de usuarios de ejemplo

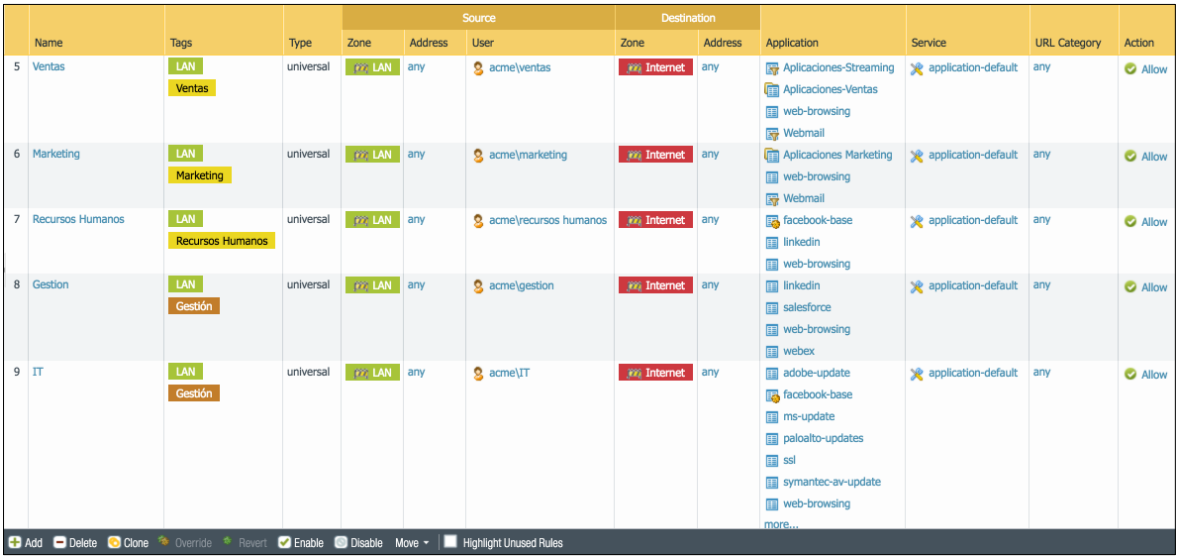


Figura 5-95: Ejemplo de despliegue de una política con User-ID

5.11.4.3 OBSERVABLES

Identificación del usuario

316. La mayoría de los mecanismos de User-ID permiten identificar a un usuario de manera transparente, lo que significa que el usuario no tendrá que autenticarse explícitamente contra el cortafuegos. Para aquellos casos en los que ninguno de los mecanismos transparentes aplique, es posible presentar una página de Portal Cautivo al usuario que se puede personalizar en "*Device > Response Pages*":

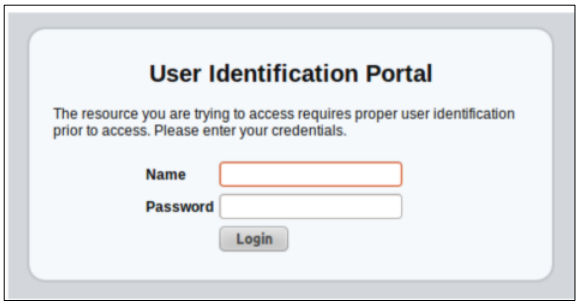


Figura 5-96: Ejemplo de página de Portal Cautivo

Logs

317. Todas las entradas de los logs pueden consultarse desde la pestaña "*Monitor > Logs*". Tal y como puede verse en la siguiente imagen el nombre de usuario aparece en las entradas de los logs:

		Receive Time	Type	From Zone	To Zone	Source	Source User	Destination	To Port	Application	Action	Rule	Session End Reason	Bytes
		09/13 18:59:22	end	LAN	Internet	192.168.45.142	acme\user2	8.8.8.8	53	dns	allow	LAN-Internet	unknown	448
		09/13 18:59:22	end	LAN	LAN	192.168.45.142	acme\user2	192.168.45.255	138	netbios-dg	allow	LAN-LAN	unknown	249

Figura 5-97: Ejemplo de logs incluyendo el atributo usuario

Notificación al usuario

318. Cuando un usuario intenta acceder a un recurso que está bloqueado, y es de tipo web, como por ejemplo una aplicación no permitida, o una URL bloqueada, es posible mostrarle una página personalizada indicándole que el acceso no está permitido. La personalización de la página puede hacerse en *"Device > Response Pages":*

Figura 5-98: Ejemplo de bloqueo de página incluyendo el usuario

5.11.5 IDENTIFICACIÓN DE DISPOSITIVO (*DEVICE-ID™*)

319. En los entornos de red modernos es necesaria la identificación de los dispositivos conectados para crear una política de seguridad efectiva. Los clientes tienen una visibilidad limitada o nula y necesitan saber qué dispositivos están conectados en la red. Para ello confían en múltiples herramientas de terceros aumentando los gastos operativos.

320. Los controles para permitir o bloquear dispositivos basados en la dirección IP resultan inapropiados y provocan agujeros de seguridad. Incapaces de prevenir las amenazas del dispositivo, no hay forma de aplicar los servicios de seguridad según los dispositivos. El seguimiento de las actividades de la red a dispositivos requiere la correlación de información de múltiples sistemas haciendo que la remediación se dilate en el tiempo.

321. Desde la versión PAN-OS 10.0, se introduce el módulo Device-IDTM. De forma similar a cómo User-ID proporciona reglas de políticas basadas en usuarios y App-ID proporciona reglas de políticas basadas en aplicaciones, Device-ID proporciona reglas de políticas basadas en un dispositivo, independientemente de los cambios en su dirección IP o ubicación.

322. La aplicación de políticas basada en los atributos del dispositivo, como la versión del sistema operativo, permite a los equipos de seguridad controlar más estrictamente la superficie de ataque. La información de Device-ID en los logs proporciona contexto adicional que combinado con App-ID y User-ID, permite obtener información detallada sobre el comportamiento en la red.

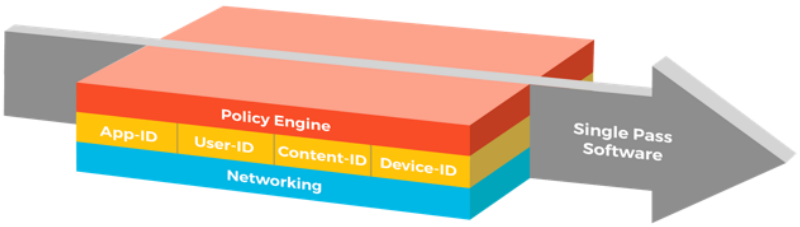


Figura 5-99: *Single Pass Architecture*

323. Device-ID es un nuevo campo en la política que permite a los administradores escribir políticas basadas en las características del dispositivo. Permite a los equipos de seguridad comprender cómo se relacionan los eventos con los dispositivos y crear políticas asociadas con los dispositivos en lugar de sus direcciones IP o ubicación, que pueden cambiar con el tiempo. Con Device-ID, los firewalls de nueva generación pueden aplicar el control de políticas y el servicio de seguridad en función de la identidad del dispositivo (impresoras, cámaras, equipos médicos, industriales, etc), bloquear dispositivos en la red con un sistema operativo desactualizado, rastrear rápidamente las amenazas hasta dispositivos individuales. Device-ID se puede utilizar en políticas de seguridad, descifrado, calidad de servicio (QoS) y autenticación.

324. De manera opcional, los cortafuegos se pueden suscribir al servicio de IoT Security de Palo alto Networks. A través de esta suscripción los cortafuegos envían los registros de tráfico al servicio de IoT Security para su análisis. Mediante técnicas de inteligencia artificial y aprendizaje automático IoT Security descubre e identificar automáticamente los dispositivos conectados a la red y, a continuación, crea un inventario de datos sobre los dispositivos, que se actualiza dinámicamente. A partir de PAN-OS 11.1, los administradores pueden ver este inventario directamente en la interfaz web del cortafuegos.

325. Device-ID está disponible en Panorama y todos los NGFW con tecnología ML (*Machine Learning*), excepto las series VM-50, y CN-Series.

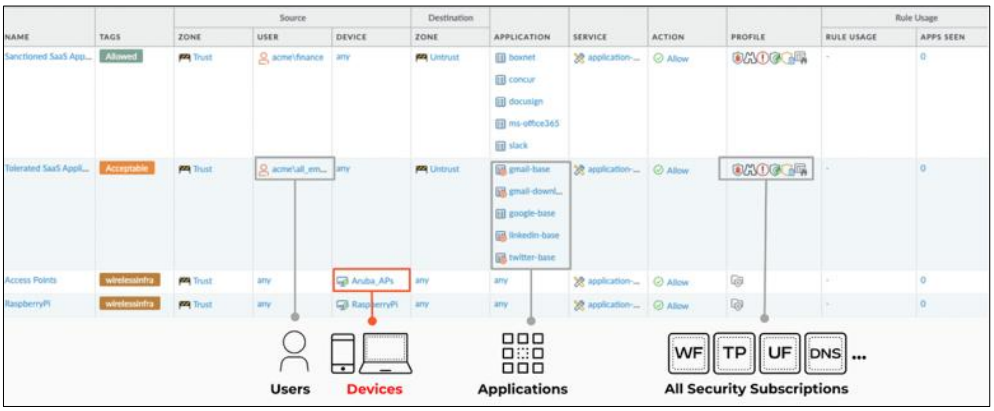


Figura 5-100: Reglas de Seguridad con Device-ID

326. Device-ID es una característica de PAN-OS que ofrece contexto de dispositivo a la red, con la suscripción de *IoT Security* como primera fuente de datos.

Nota: En los siguientes enlaces encontrará información complementaria sobre Device-ID: *https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/device-id/device-id-overview*

5.11.5.1 COMBATIENDO LA CADENA DE CIBERATAQUE

	Entrega	Explotación	Instalación	Mando y Control	Acciones en el Objetivo
Device-ID					Políticas de Seguridad basadas en el tipo de dispositivo

Tabla8: Cadena de ciberataque – Device-ID

327. Device-ID proporciona los siguientes beneficios:

a) Visibilidad completa:
   i. Los administradores pueden rastrear un dispositivo a medida que se mueve a través de la red.
   ii. Permite la evaluación de la superficie de ataque.
   iii. Los analistas del SOC pueden rastrear amenazas específicas a dispositivos individuales.
   iv. Personal de respuesta a incidentes para reaccionar más rápidamente.
   v. Remediación más rápida.

b) Reducir la superficie de ataque:
   i. Elimina la dependencia de la configuración del dispositivo.
   ii. No importa si un dispositivo se conecta a la red o a una VLAN incorrecta.

c) Prevención de amenazas:
   i. Utiliza las mismas capacidades de prevención de amenazas proporcionadas a través de Content-ID.
   ii. La información de identidad del dispositivo en los registros de amenazas permite aumentar la eficiencia de los flujos de trabajo existentes y habilitar otros nuevos.

d) Forense:
   i. Reducción del tiempo de remediación. Cuando ocurre un incidente, los clientes actualmente necesitan correlacionar la dirección IP del registro del cortafuegos con la información de logs de un servidor DHCP o un sistema de administración de activos, lo que aumenta el tiempo que lleva identificar qué dispositivo o dispositivos en la red están afectados.

5.11.5.2 REQUISITOS DE SEGURIDAD

328. Hasta ahora los administradores de seguridad para securizar el comportamiento de un dispositivo, tienen que escribir políticas basadas en la dirección IP donde, basados en el

diseño, se dedican subredes al dispositivo según el tipo o la función. Esto implica confiar en:

- Que los dispositivos tienen las IPs deseadas y están conectados de acuerdo con el diseño de red definido.

- Ningún actor malicioso puede conectar dispositivos a redes restringidas.

329. Intentar resolver el problema de identificación integrándose con sistemas de control de acceso a la red (NAC) o sistemas de gestión de activos. Los sistemas de NAC presentan varios problemas:

    - La complejidad y dificultad del despliegue se traslada en una carencia de cobertura. La mayoría de las implementaciones casi siempre quedan incompletas.

    - En casos dónde hay un NAC disponible y puede realizar clasificación de dispositivos, el cliente tiene que realizar la implementación y mantener una integración con el cortafuegos para usar la información en las reglas de las políticas de seguridad. El desarrollo de estas integraciones incrementa los costes de operación para el cliente.

330. Por tanto, se necesita que la identidad del dispositivo esté disponible para usar directamente dentro de la política. Que la aplicación de políticas sea coherente, independientemente de dónde esté conectado el dispositivo o cómo esté configurado. La suscripción de IoT Security es la primera fuente de datos confiable que alimenta directamente Device-ID, eliminando la necesidad de integraciones dispares.

Configurar un nuevo objeto de dispositivo basado en múltiples atributos

331. **Ubicación**: "*Objects > Devices > Add > Browse*"

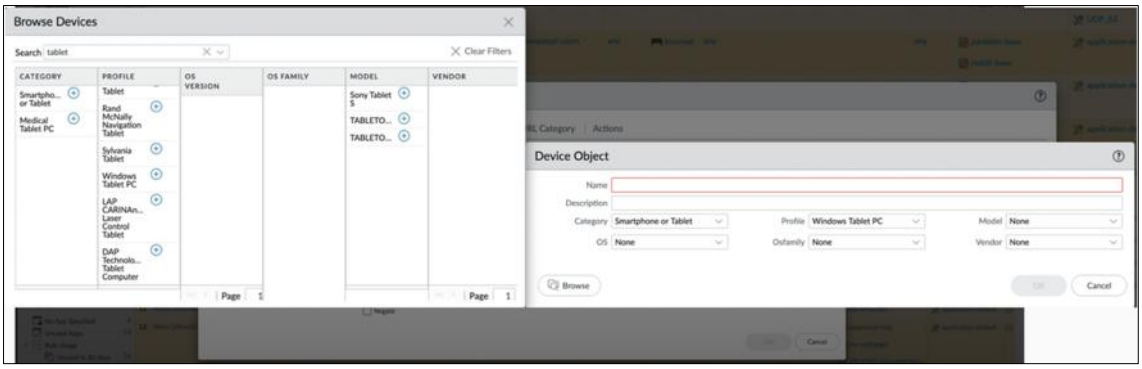


Figura 5-101: Configuración de atributos

Añadir un dispositivo de origen a una regla

332. **Ubicación**: "*Policies > Security > Source > Source Device > Add*"

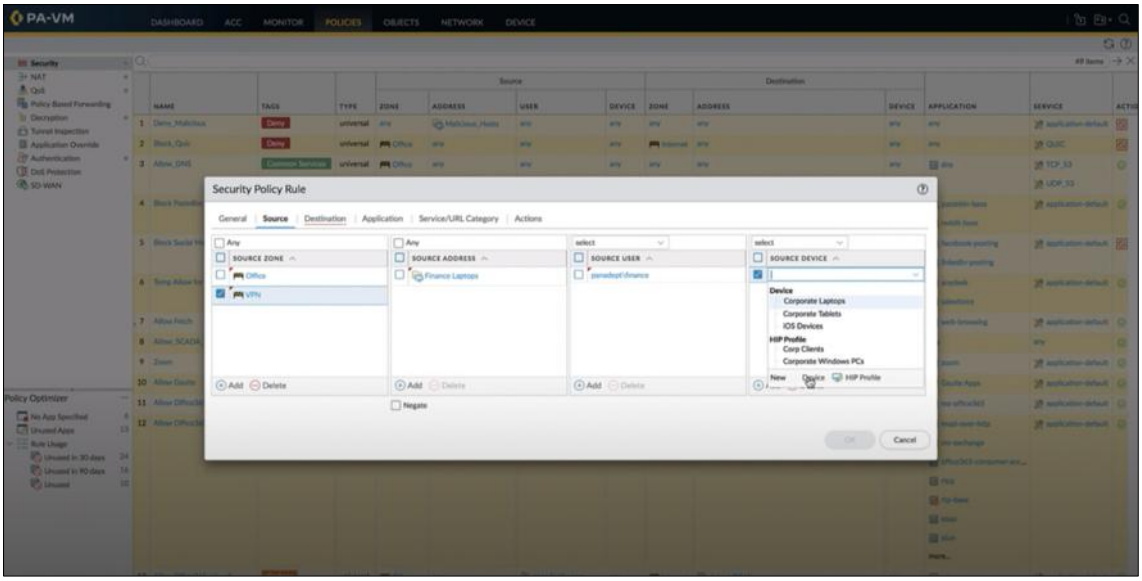


Figura 5-102: Uso de Device-ID en la política

Resultado

333. **Ubicación**: "*Policies > Security*"

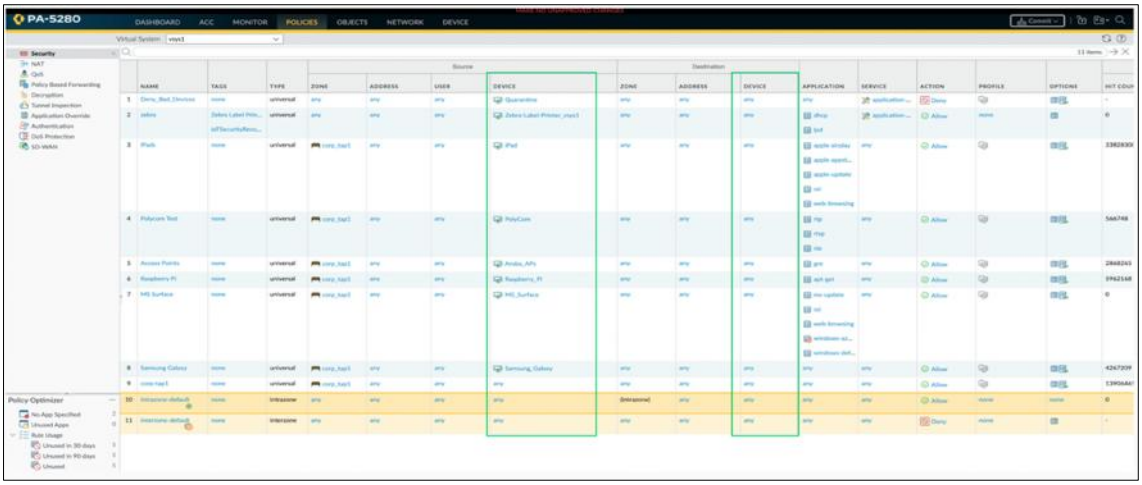


Figura 5-103: Reglas de la Política de Seguridad con Device-ID

5.11.5.3 EJEMPLO DE USO

Permitir acceso basado en el dispositivo

334. **Ubicación**: "*Policies > Security*"

335. **Requisito de seguridad**: es necesario poder controlar el acceso según el tipo de dispositivo desde el que se realiza la conexión.

336. En las políticas mostradas a continuación, Device-ID permite que el administrador permita que los dispositivos VoIP accedan sólo a las aplicaciones que deberían,

independientemente de dónde estén conectados, mientras se restringe la actividad de otras aplicaciones.

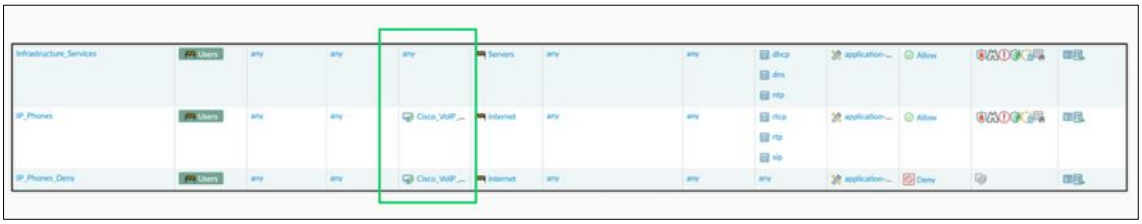


Figura 5-104: Ejemplo de políticas basadas en el ID del dispositivo (Device-ID)

Reducción de la superficie de ataque

337. **Ubicación**: "*Policies > Security*"

338. **Requisito de seguridad**: es necesario limitar la superficie del ataque.

339. Device-ID permite a los administradores controlar de forma más granular la superficie de ataque. En este ejemplo, un objeto de dispositivo se define usando solo el atributo del sistema operativo. Este objeto de dispositivo coincidirá con "cualquier" dispositivo que ejecute *Windows XP Embedded*, ya que el riesgo en este caso es el sistema operativo obsoleto. El administrador puede combinar esto con perfiles de seguridad personalizados para limitar el riesgo de manera más estricta. En este ejemplo, se aplica un perfil de bloqueo de archivos que no permite las descargas de tipos de archivos peligrosos a la regla utilizada por los dispositivos con Windows XP.

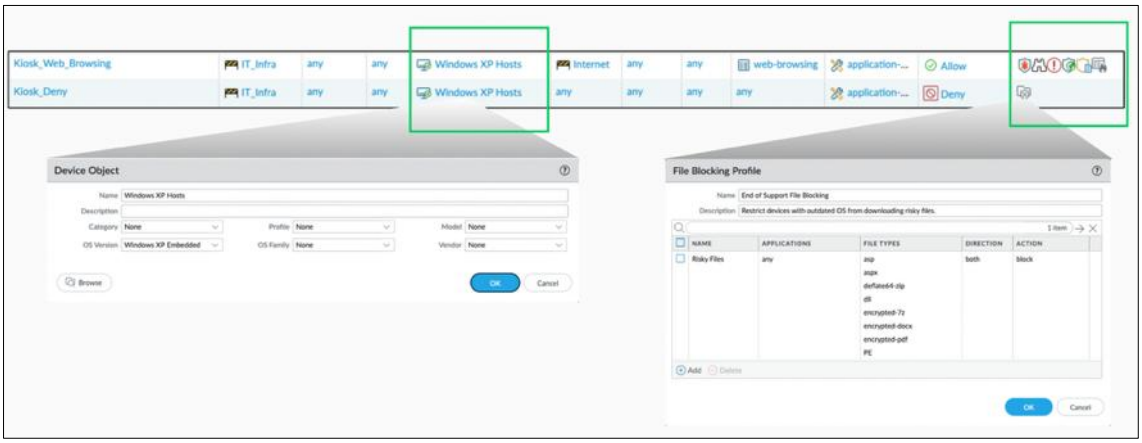


Figura 5-105: Restringir descargas de ficheros peligrosos para dispositivos con sistemas operativos obsoletos

Descifrado basado en el dispositivo

340. **Ubicación**: "*Policies > Decryption*"

341. **Requisito de seguridad**: es necesario poder descifrar tráfico según el tipo de dispositivo.

342. Ciertas aplicaciones como WhatsApp se rompen cuando se descifran sus aplicaciones móviles nativas. En este ejemplo, omitimos el descifrado de WhatsApp en dispositivos móviles, pero lo habilitamos en todos los demás dispositivos.

Figura 5-106: Descifrado basado en el dispositivo

Rastrear un dispositivo en la red

343. **Ubicación**: *"ACC"*

344. **Requisito de seguridad**: se debe poder rastrear un equipo conectado a la red independientemente de su ubicación de conexión.

345. Debido a que los datos de identidad del dispositivo están integrados con los registros de firewall de próxima generación, los nuevos flujos de trabajo están disponibles a través de las herramientas existentes, como ACC. En este ejemplo, una dirección MAC (o dirección física) se usa como un filtro global para mostrar en qué parte de la red se ha conectado un dispositivo. Vemos que la dirección MAC enumerada se ha conectado a varias ubicaciones diferentes durante los últimos 30 días.

346. Esta capacidad puede ser parte de un flujo de trabajo de respuesta a incidentes para ver dónde se ha conectado un host infectado dentro de la red para ayudar en las actividades de contención y remediación.

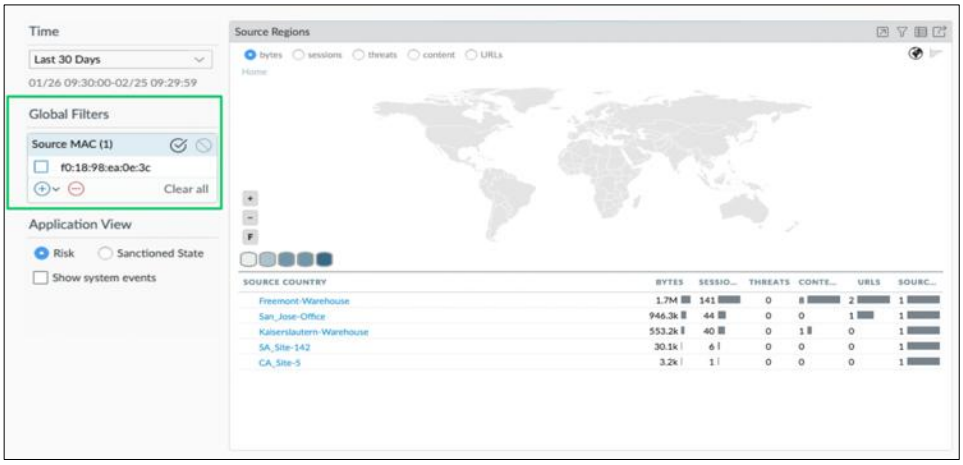


Figura 5-107: Rastreo de dispositivos en la red

347. Plataforma todo en uno con App-ID, User-ID, Content-ID y Device-ID. Device-ID es un elemento central de PAN-OS, se puede utilizar con la prevención de amenaza, App-ID y User-ID del NGFW para proteger los dispositivos en la red. Los clientes pueden mantener una red funcional y segura y no necesitan depender de múltiples proveedores.

5.11.5.4 OBSERVABLES

348. **Ubicación**: "Monitor > Traffic"

349. Es posible ver la actividad de los dispositivos consultando "Monitor > Traffic".

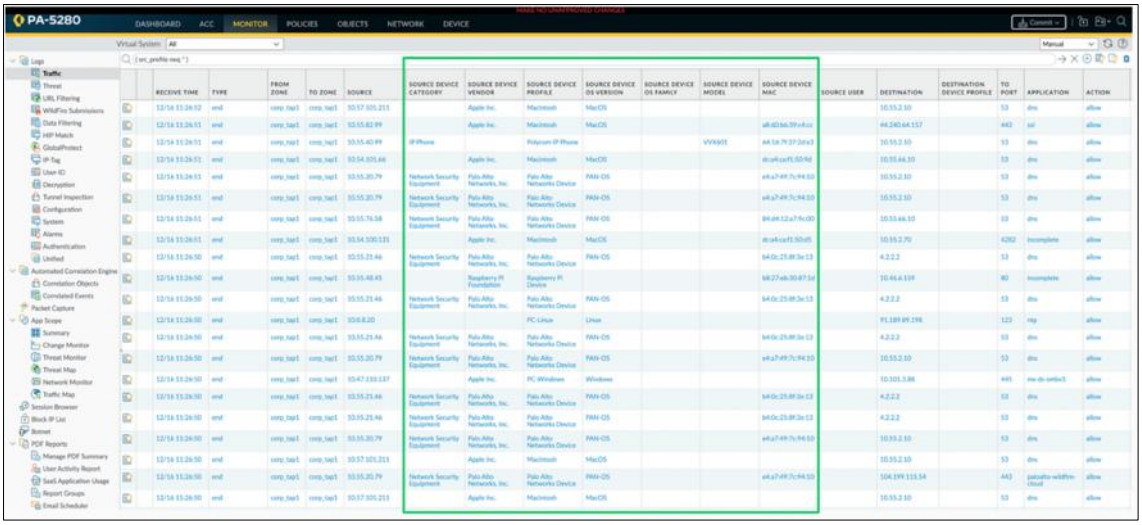


Figura 5-108: Logs de los dispositivos

5.11.6 FILTRADO DE URL (*ADVANCED URL FILTERING*)

350. La naturaleza de los patrones de tráfico web es única para cada cliente, en función de los usuarios y necesidades de cada negocio. Para ello, la solución de Palo Alto Networks permite la personalización automática de la base de datos de filtrado, en función del comportamiento del tráfico web observado.

351. La solución de filtrado de URL de Palo Alto Networks, incluida dentro del servicio de seguridad de *Advanced URL Filtering*, protege contra las amenazas web permitiendo habilitar el acceso web de manera segura mientras controla cómo interactúan sus usuarios con el contenido en línea. La suscripción al servicio de Filtrado de URL Avanzado proporciona toda la funcionalidad que ofrece la suscripción de Filtrado de URL heredada, al mismo tiempo que proporciona el beneficio adicional del análisis de URL en tiempo real. El filtrado de URL avanzado proporciona una respuesta ante las brechas de cobertura inherentes a las soluciones de bases de datos al proporcionar un análisis de URL en tiempo real por solicitud. De esta forma, la solución ofrece protección contra las URL maliciosas de nueva creación, antes de que las bases de datos de filtrado de URL tengan la oportunidad de analizar y agregar su contenido, lo cual tradicionalmente ha brindado a los atacantes un período abierto desde el cual pueden lanzar campañas de ataque. Los modelos basados en *Machine Learning* (ML) utilizados por el filtrado de URL avanzado han sido entrenados y se actualizan continuamente para detectar varias URL maliciosas, páginas web de phishing y C2.

352. Cuando un usuario solicita una página web, el cortafuegos consulta las excepciones agregadas por el usuario, así como la base de datos PAN-DB para la categoría de riesgo de la página web destino. PAN-DB utiliza información de Unit 42, *WildFire*, base de datos DNS y datos de telemetría de Palo Alto Networks, así como datos de *Cyber Threat Alliance*, y aplica varios analizadores para determinar la categoría. Si la URL muestra características maliciosas, también se envía a un filtrado de URL avanzado en la nube para un análisis en tiempo real, y genera datos de análisis adicionales. El cortafuegos recupera la categoría de riesgo resultante y la utiliza para hacer cumplir la política de acceso web configurada. Además, el cortafuegos almacena en caché la información de categorización del sitio, para

permitir una recuperación rápida para solicitudes posteriores, mientras elimina las URL a las que los usuarios no han accedido recientemente para que refleje con precisión el tráfico de la red. Además, las comprobaciones integradas en las consultas en la nube de PAN-DB garantizan que el cortafuegos reciba la información de categorización de URL más reciente.

353. Los cortafuegos configurados para analizar las URL en tiempo real mediante el aprendizaje automático en el plano de datos (URL Filtering Inline ML) proporcionan una capa adicional de seguridad contra los sitios web de phishing y las vulnerabilidades de JavaScript. Los modelos de aprendizaje automático en línea utilizados para identificar estas amenazas basadas en URL se extienden a variantes actualmente desconocidas que coinciden con características que Palo Alto Networks ha identificado como maliciosas.

354. La funcionalidad de filtrado URL puede bloquear el acceso a URLs específicas, sitios web y categorías de sitios web, o generar una alerta cuando se produce el acceso. También es posible definir listas personalizadas de acceso blancas y negras.

355. Una vez que las reglas de acceso del cortafuegos han sido creadas, pueden aplicarse los perfiles de URL filtering para aquellas reglas que permiten el acceso web, con el fin de reducir la superficie de ataque. En su caso de uso más básico, esto es posible conseguirlo bloqueando el acceso a aquellos sitios clasificados como maliciosos. Otras posibilidades incluyen el bloqueo del acceso a aquellas categorías web o sitios que incluyen un riesgo potencial porque dan servicio a un gran número de usuarios y, como tales, pueden ser fuente preferente de propagación de malware, como por ejemplo los sites de file sharing, foros o redes sociales.

356. El URL Filtering puede habilitarse incluyendo las categorías directamente en las reglas de seguridad, o bien a través de la definición de un perfil de URL Filtering por regla, según convenga. Hay muchas maneras de hacer cumplir el acceso a la página web, más allá de bloquear y permitir ciertos sitios. Por ejemplo, se pueden usar varias categorías por URL para permitir que los usuarios accedan a un sitio web, pero bloquear funciones particulares como enviar credenciales corporativas o descargar archivos. También se pueden usar categorías de URL para aplicar diferentes tipos de políticas, como autenticación, descifrado, QoS y seguridad.

357. Existe un perfil *default* disponible para el *URL Filtering* que bloquea el acceso a las siguientes categorías:
    - *Abused-drugs*
    - *Adult*
    - *Gambling*
    - *Hacking*
    - *Malware*
    - *Phishing*
    - *Command-and-control*
    - *Questionable*

- *Weapons*

358. También se pueden crear perfiles personalizados para filtrar las categorías acordes a las reglas aceptadas de uso de la organización.

Nota: Si se desea obtener más información sobre *URL Filtering*:
https://www.paloaltonetworks.com/network-security/advanced-url-filtering
https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-basics
También se puede consultar en línea la categoría y el nivel de riesgo asociado a una URL a través del siguiente enlace:
https://urlfiltering.paloaltonetworks.com/

5.11.6.1 COMBATIENDO LA CADENA DE CIBERATAQUE

	Entrega	Explotación	Instalación	Mando y Control	Acciones en el Objetivo
URL Filtering	Bloquear URLs de sitios malos conocidos			Bloquear malware y dominios *fast-flux*	

Tabla 9: Cadena de ciberataque: URL Filtering

359. El *URL Filtering* puede utilizarse para reducir la superficie de ataque de los empleados, así como para romper la cadena de ataque en la fase de Entrega, al bloquear el acceso a los sitios web maliciosos y los enlaces que apuntan hacia los entregables del malware. Adicionalmente, el *URL Filtering* puede también prevenir el acceso a los sitios, páginas y dominios, que se emplean como servidores C2 (mando y control).

5.11.6.2 REQUISITOS DE SEGURIDAD

360. Dependiendo del perfil de riesgo de la organización y de la política de seguridad, deberían considerarse las acciones *Block* o *Continue* para las categorías problemáticas, en lugar de *Allow* o *Alert*. La ventaja de la opción *Continue* es que aún se permite el acceso a los empleados si pulsan sobre el botón *Continue*, a la vez que se conseguirá bloquear el acceso no deseado u ofuscado a categorías particulares o desconocidas de URLs. Este mecanismo ofrece gran protección frente a los *exploits drive-by*, en los que se visita un enlace sin que el usuario sea consciente.

361. Las categorías más obvias para bloquear son *adult, malware, phishing y proxy-avoidance-and-anonymizers,* aunque hay otras que también deberían considerarse si no son necesarias. Además, la categoría *Unknown* también debería recibir una acción diferente a *Allow* o *Alert* para reducir el riesgo potencial de los sitios desconocidos.

1. Utilizar *URL filtering* en todas las reglas hacia internet

362. **Ubicación**: "*Objects > Security Profiles > URL Filtering*"; "*Policies > Security*"

363. **Requisito de seguridad:** Se debe aplicar un perfil de *URL Filtering* en todas las reglas que permitan el tráfico hacia Internet. Como mínimo, la acción del perfil debe incluir la acción

alert, para garantizar que se deja un log en el sistema. Se debe considerar, además, bloquear las categorías más peligrosas, mencionadas en el punto anterior.

2. Prevenir phishing de credenciales

364. El cortafuegos utiliza distintos métodos para detectar credenciales corporativas introducidas en una página web. Estos métodos requieren de User-ID, permitiendo al cortafuegos comparar los envíos de nombre de usuario y contraseña a páginas web con credenciales corporativas válidas.

Nota: Métodos de detección de credenciales:
https://docs.paloaltonetworks.com/advanced-url-filtering/administration/url-filtering-features/credential-phishing-prevention

365. **Ubicación**: "*Objects > Security Profiles > URL Filtering > URL Filtering Profile > User Credential Detection*"

366. **Recomendación**: Se recomienda alertar sobre cualquier introducción de credenciales a las categorías permitidas.

3. Detectar phishing y Java Scripts maliciosos en tiempo real mediante *URL Filtering Inline ML*

367. **Ubicación:** "*Objects > Security Profiles > URL Filtering > URL Filtering Profile > Inline ML*"

368. **Recomendación:** *El perfil por defecto bloquea la detección de exploits de tipo JavaScript, y alerta sobre páginas URL de phishing de credenciales.*

Nota: URL Filtering Inline ML:
https://docs.paloaltonetworks.com/advanced-url-filtering

4. Activar Advanced URL filtering para análisis de URLs en tiempo real

369. Se ha introducido una nueva categoría "real-time-detection" con la versión de contenido 8390-xxxx y posteriores.

370. Esta nueva categoría será utilizada por las funciones de Advanced URL Filtering para indicar una detección en tiempo real de URL maliciosas. A su vez, estas direcciones URL maliciosas se clasifican además en sus respectivas categorías maliciosas, como C2, phishing, malware y grayware.

371. El cortafuegos aplica la acción más severa de las acciones configuradas para las categorías de URL detectadas de una URL determinada. Por ejemplo, supongamos que example.com está categorizado como *real-time-detection*, *command-and-control* y *shopping*: categorías con una acción de *alert*, *block* y *allow* configurada, respectivamente. El cortafuegos bloqueará la URL porque el bloqueo es la acción más grave de las categorías detectadas.

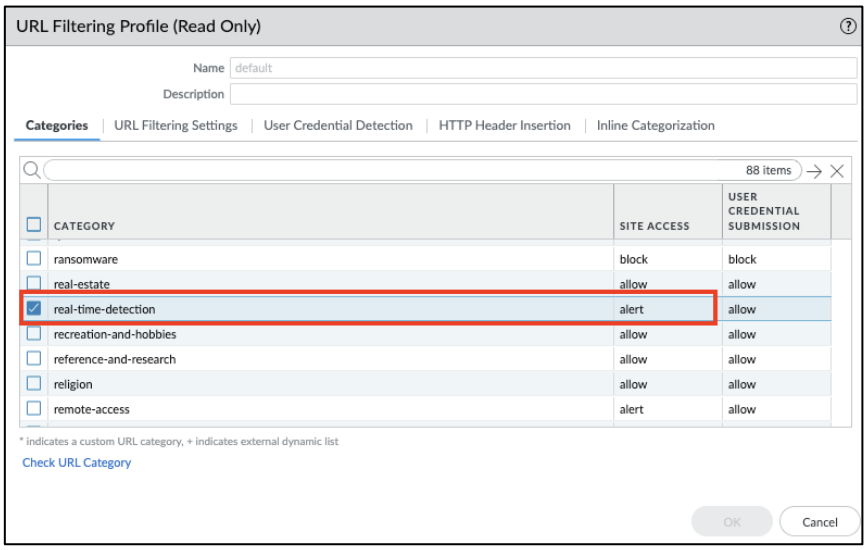


Figura 5-109: Detección en tiempo real

372. **Ubicación**: "*Objects > Security Profiles > URL Filtering > URL Filtering Profile > Categories*"

373. **Recomendación:** Palo Alto Networks recomienda establecer la categoría *real-time-detection* en modo alerta. Esto proporciona visibilidad de las URL analizadas en tiempo real y bloqueará (o permitirá, según la configuración de su política) según la configuración de categoría configurada para amenazas web específicas.

5. Activar el *logging* de cabeceras HTTP

374. **Ubicación**: "*Objects > Security Profiles > URL Filtering > URL Filtering Profile > URL Filtering Settings*"

375. **Recomendación:** Se recomiendan activar las opciones de logging para *User-Agent*, *Referer*, y *X-Forwarded* en *HTTP Header Logging*, porque ofrecen información útil en caso de necesitar hacer un análisis posterior.

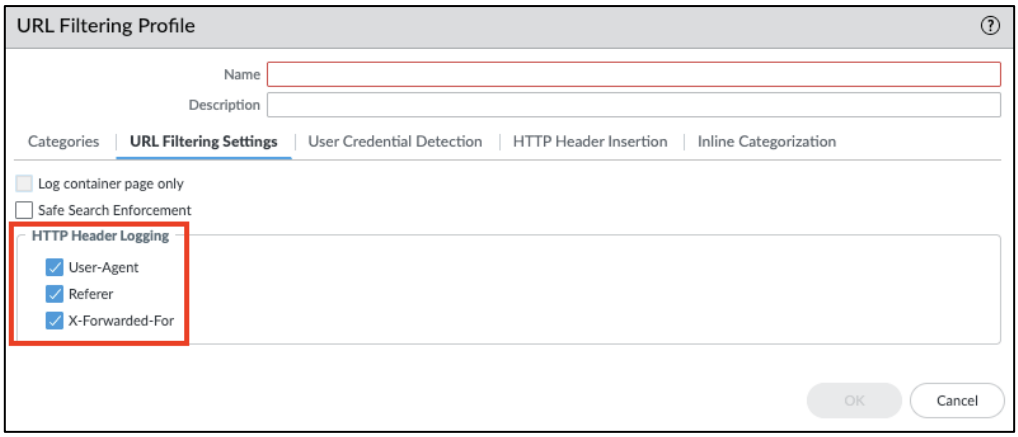


Figura 5-110: Activación de logging de cabeceras HTTP en *URL Filtering*

6. Desactivar el *logging* solo de *container pages*

376. **Ubicación**: "*Objects > Security Profiles > URL Filtering > URL Filtering Profile > URL Filtering Settings*"

377. **Recomendación:** Por defecto, el sistema registra solamente las páginas contenedoras. Esto permite reducir el tamaño del log ya que solamente se registrarán aquellas URIs en las que la página o fichero solicitado, se correspondan con determinados tipos *MIME*. La configuración por defecto incluye:

- *application/pdf*
- *application/soap+xml*
- *application/xhtml+xml*
- *text/html*
- *text/plain*
- *text/xml*

378. Cuando esta función está habilitada, puede que no haya siempre un evento de URL correlado para las amenazas detectadas por los módulos de Antivirus o Protección de Vulnerabilidades. Si se desea mantener el *logging* completo para cualquier URL solicitada, se recomienda deshabilitar los *container page.* También es posible definir qué *mime-types* se quiere registrar en *"Device > Setup > Content-ID > Content-ID features > Container Pages".*

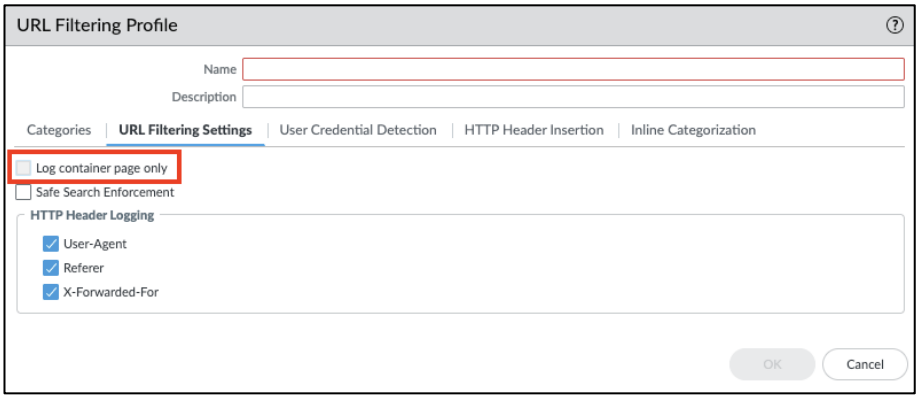


Figura 5-111:Desactivación de logging solamente de container pages

5.11.6.3 EJEMPLO DE USO

379. En el ejemplo se requiere una política de filtrado URL que cumpla con los siguientes requisitos:

1. El acceso a los siguientes sites debe estar bloqueado para todo el mundo que utilice la conexión a Internet corporativa, tanto empleados como invitados:

    - *Hacking*
    - *Malware*
    - *Peer-to-peer*
    - *Phishing*

- *Proxy-avoidance-and-anonymizers*
- *Questionable*

2. El acceso a cualquier otro site externo debe ser monitorizado y alertado para los usuarios conocidos, pero no bloqueado.

3. El acceso a cualquier otro site externo debe ser bloqueado para cualquier sistema no identificado.

4. El acceso al sitio web corporativo debe estar permitido para todo el mundo, tanto usuarios internos como externos. No hace falta realizar filtrado URL sobre este tráfico.

380. El primer requisito puede conseguirse creando una regla en el cortafuegos que bloquee estas categorías. Es importante ubicar esta regla antes que cualquier otra para garantizar que ningún usuario o sistema no pase por ella:

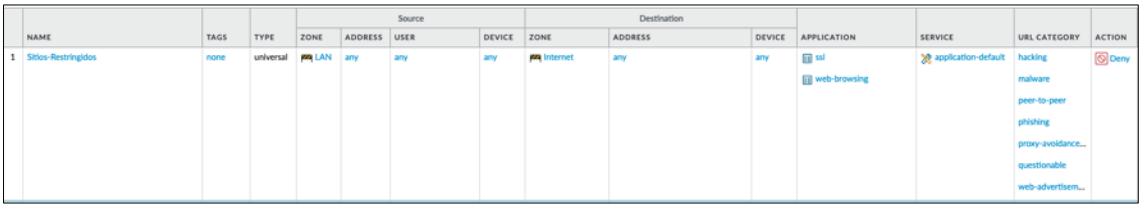


Figura 5-112: Bloqueo de sitios restringidos

381. El segundo requisito puede conseguirse creando un perfil de URL Filtering que alerte en todas las categorías y aplicando este perfil sobre las reglas ya existentes, para cada grupo de usuarios:

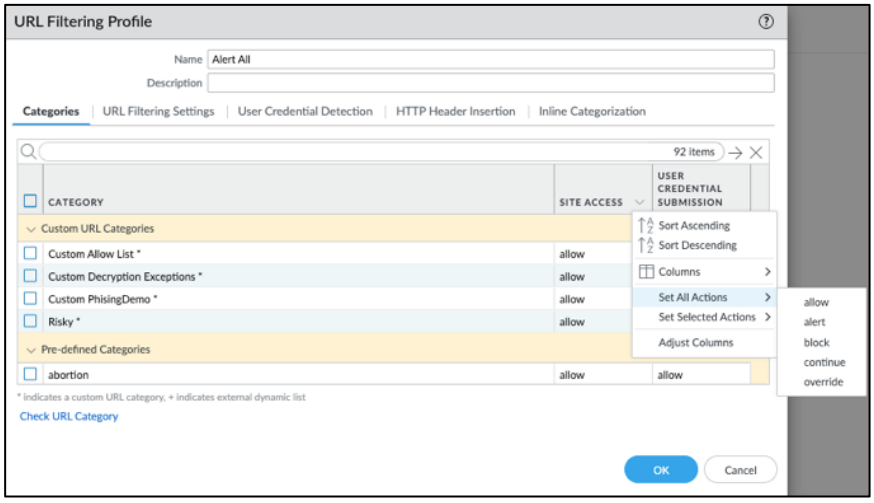
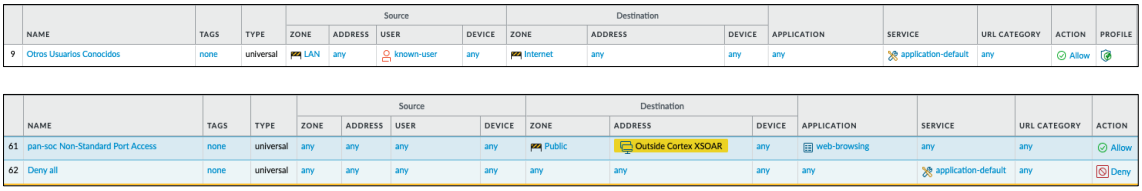


Figura 5-113: Creación de un perfil de URL con todas las categorías en Alert



	NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE
9	Otros Usuarios Conocidos	none	universal	LAN	any	known-user	any	Internet	any	any	any	application-default	any	Allow	
61	pan-soc Non-Standard Port Access	none	universal	any	any	any	any	Public	Outside Cortex XSOAR	any	web-browsing	any	any	Allow	
62	Deny all	none	universal	any	any	any	any	any	any	any	any	application-default	any	Deny	

Figura 5-114: Aplicación del perfil sobre las reglas de acceso por usuario y grupo

382. El tercer requisito se consigue con la regla de bloqueo general mostrada antes, última en la política, denominada “Deny All”.

383. El filtrado de URL avanzado de Palo Alto Networks ahora opera una serie de detectores de aprendizaje profundo en línea basados en la nube, “*deep learning*”, que evalúan contenidos de páginas web sospechosas en tiempo real para proteger a los usuarios frente a amenazas de día cero. Esto incluye sitios web camuflados, ataques multinivel, desafíos CAPTCHA y URL de un solo uso no vistas anteriormente. Cuando el NGFW procesa una solicitud de URL con contenido de página web sospechoso, reenvía los datos de respuesta HTTP a la nube y analiza el contenido de la página web que se considera sospechoso y se categoriza en consecuencia. Los detectores y analizadores de aprendizaje profundo utilizados para categorizar los sitios web se actualizan e implementan automáticamente a medida que los investigadores de amenazas de Palo Alto Networks mejoran la lógica de detección, y no requiere que el administrador descargue e implemente paquetes de actualización. La categorización en línea en la nube se habilita y configura a través del perfil de filtrado de URL y requiere una licencia activa de filtrado avanzado de URL.

384. **Ubicación**: *“Objects > Security Profiles > URL Filtering > URL Filtering Profile > Inline Categorization”*

385. **Recomendación:** Activar los checks “*Enable local inline categorization*” y “*Enable cloud inline categorization*”

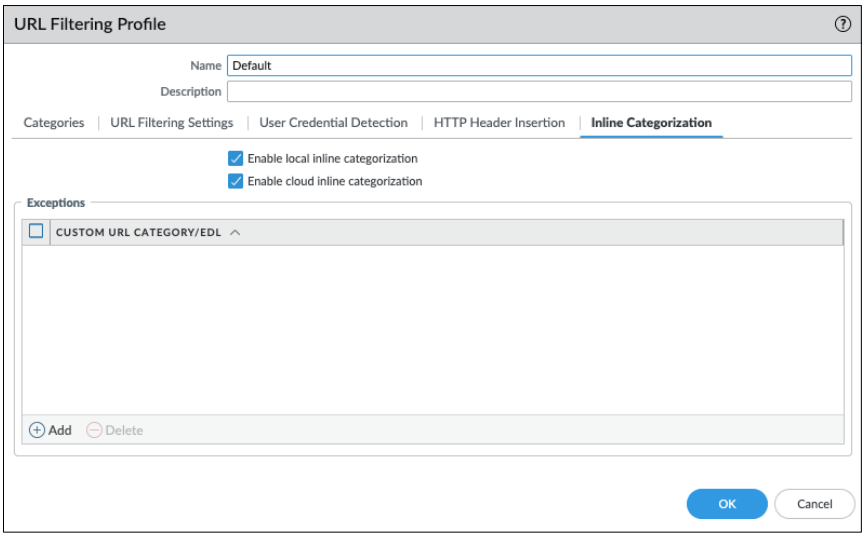


Figura 5-115: Activación de análisis profundo para el filtrado avanzado de URL

Nota: Para garantizar la disponibilidad de aplicaciones críticas para el negocio, Palo Alto networks recomienda seguir los consejos de “Transición de perfiles de filtrado de URL de forma segura a Mejores prácticas”:

https://docs.paloaltonetworks.com/best-practices/internet-gateway-best-practices/best-practice-internet-gateway-security-policy/transition-safely-to-best-practice-security-profiles/transition-url-filtering-profiles-safely-to-best-practices

5.11.6.4 OBSERVABLES

Logs

386. Los logs de *URL Filtering* pueden consultarse a través de la vista "*Monitor > Logs > URL Filtering*". La vista detallada de un log particular también referencia los logs relacionados asociados con esa entrada de log de URL:

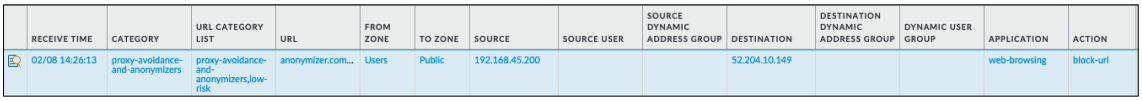


Figura 5-116: Ejemplo de log de URL

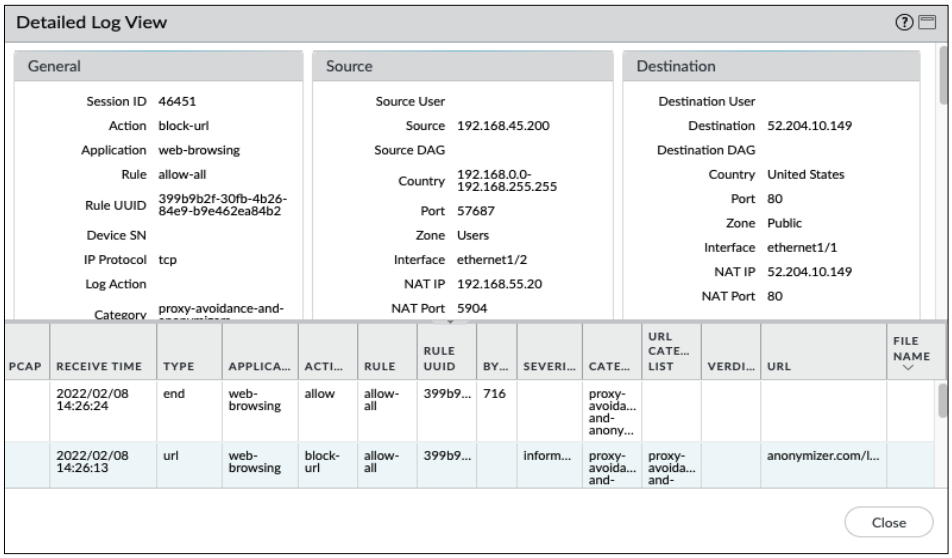


Figura 5-117: Vista detallada del log de URL

Notificación al usuario

387. Cuando un usuario intenta acceder a una URL que está bloqueada o que requiere la acción de continuación u *override*, se le muestra una página personalizada indicándoselo:

Figura 5-118: Ejemplo de página de bloqueo de URL

5.11.7 IPS

388. La funcionalidad de Vulnerability Protection, incluida dentro del servicio de seguridad de Advanced Threat Prevention, detecta y previene los ataques de red contra vulnerabilidades, tanto en sistemas cliente como servidor. El módulo hereda la inteligencia de la identificación de App-ID para buscar amenazas que sean relevantes en el contexto de cada aplicación, lo que minimiza los falsos positivos.

389. El módulo tiene capacidad de convertir firmas de *Snort* y *Suricata* de forma automática en firmas de vulnerabilidades de Palo Alto Networks mediante un complemento o *plugin* instalado en Panorama, aumentando inmediatamente la cobertura existente de prevención de amenazas con otras fuentes de inteligencia o mediante firmas creadas específicamente para su entorno de red.

390. **Ubicación**: "*Panorama > IPS Converter > Manage > Upload Signatures*"

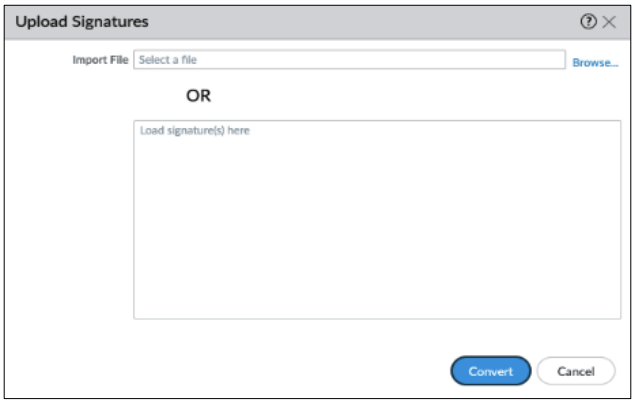


Figura 5-119: Modulo Panorama para Snort

391. Este módulo también dispone de protección contra los ataques de evasión, con el que los atacantes intentan acceder a su red sin pasar por la inspección de seguridad. Las medidas de seguridad mejoradas cubren las técnicas de evasión que hacen un mal uso de las URL y el contenido codificado en Base64.

A. Perfiles Predefinidos

392. Por defecto se ofrecen dos perfiles de Vulnerability Protection predefinidos:

393. El perfil "default" aplica la acción por defecto a todas las vulnerabilidades de cliente y servidor con severidad crítica, alta y media. No registra las catalogadas como bajas o informacionales.

394. El perfil "*strict*" aplica la acción de bloqueo a todas las vulnerabilidades de cliente y servidor clasificadas con severidad crítica, alta y media. Para las bajas e informacionales, aplica la acción por defecto.

NAME	LOCATION	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
strict	Predefined	Rules: 10	simple-client-critical	any	client	critical	reset-both	disable
			simple-client-high	any	client	high	reset-both	disable
			simple-client-medium	any	client	medium	reset-both	disable
			simple-client-informational	any	client	informational	default	disable
			simple-client-low	any	client	low	default	disable
			simple-server-critical	any	server	critical	reset-both	disable
			simple-server-high	any	server	high	reset-both	disable
			more...					
default	Predefined	Rules: 6	simple-client-critical	any	client	critical	default	disable
			simple-client-high	any	client	high	default	disable
			simple-client-medium	any	client	medium	default	disable
			simple-server-critical	any	server	critical	default	disable
			simple-server-high	any	server	high	default	disable
			simple-server-medium	any	server	medium	default	disable

Figura 5-120: Perfiles de Vulnerability Protection predefinidos

B. Perfiles Personalizados

395. Además de los perfiles predefinidos es posible crear perfiles personalizados. Un perfil personalizado puede contener una o más reglas y excepciones que definen qué firmas de *Vulnerability Protection* han de incluirse. Para cada regla es posible seleccionar qué tipo de acción se desea que se aplique, el tipo de *host* (cliente o servidor), la categoría de firmas a activar y la severidad.

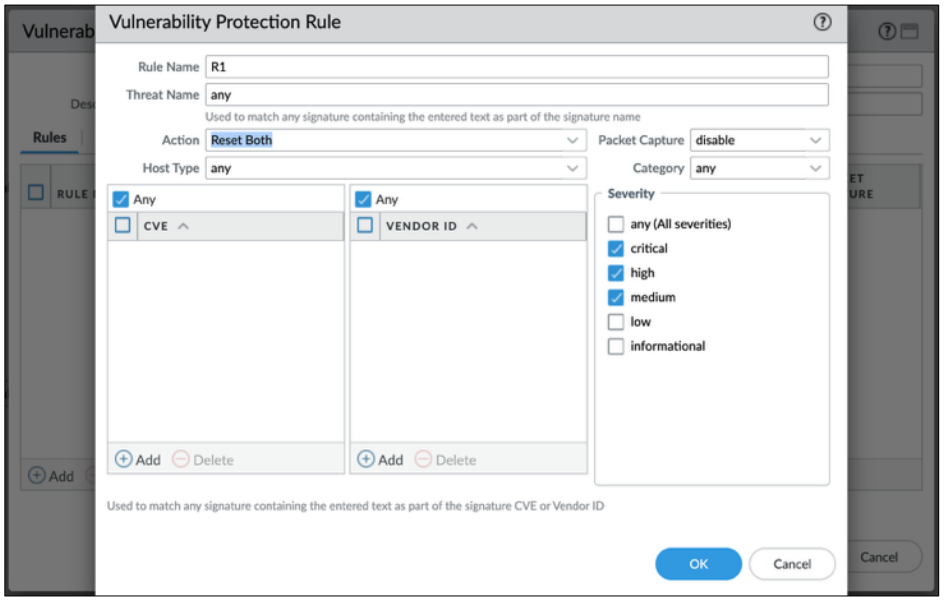


Figura 5-121: Perfiles de Vulnerability Protection personalizados

396. Los perfiles personalizados permiten también la configuración de la captura de paquetes sobre el tráfico que hace *match*. Estas capturas pueden utilizarse para obtener evidencia de los ataques o para propósitos de depuración.

Nota: Si se desea obtener más información sobre *Vulnerability Protection* visitar:
https://www.paloaltonetworks.com/network-security/advanced-threat-prevention
https://docs.paloaltonetworks.com/advanced-threat-prevention

5.11.7.1 COMBATIENDO LA CADENA DE CIBERATAQUE

	Entrega	Explotación	Instalación	Mando y Control	Acciones en el Objetivo
Vulnerability Protection		Bloquear *exploits*			Prevenir el movimiento lateral

Tabla 10: Cadena de ciberataque - Vulnerability Protection

397. El módulo de *Vulnerability Protection* puede ayudar en la rotura de la cadena de ataque en la fase de Explotación, gracias a la prevención de las vulnerabilidades de cliente y servidor para que no sean explotadas. También es de ayuda ofreciendo una protección similar durante los intentos de movimiento lateral, cuando el atacante intenta explotar vulnerabilidades en los hosts internos.

5.11.7.2 REQUISITOS DE SEGURIDAD

398. Cuando se despliegan perfiles de Vulnerability Protection es importante revisar que no afectan al tráfico legítimo. Aunque las firmas se desarrollan cuidadosamente, trabajan en el contexto de la aplicación –lo que minimiza los falsos positivos- y se ven sometidas a test de regresión. Hay algunas que son de naturaleza genérica y que, por tanto, pueden dispararse sobre tráfico proveniente de servicios o aplicaciones legítimos. Especialmente deben revisarse aquellas aplicaciones que se han construido de manera personalizada.

399. En general, se recomienda comenzar con un perfil que utilice la acción por defecto para cada firma o crear un perfil en modo alerta, para obtener una foto clara de qué se va a bloquear. Posteriormente, y una vez finalizado el ajuste inicial, es recomendable configurar el perfil por defecto *strict*, que bloquea las vulnerabilidades clasificadas como *critical, high y medium*, o definir uno con estas características.

1. Configurar perfil de *Vulnerability Protection*

400. **Ubicación**: "*Objects > Security Profiles > Vulnerability Protection*"

401. **Recomendación:** Configurar un perfil con todas las firmas de tipo *critical*, *high* y *medium* en modo *reset-both* (denegación) y con la captura de paquetes activada, y el resto con su acción por defecto. Este es el perfil para aplicar una vez transcurrida la fase inicial de análisis.

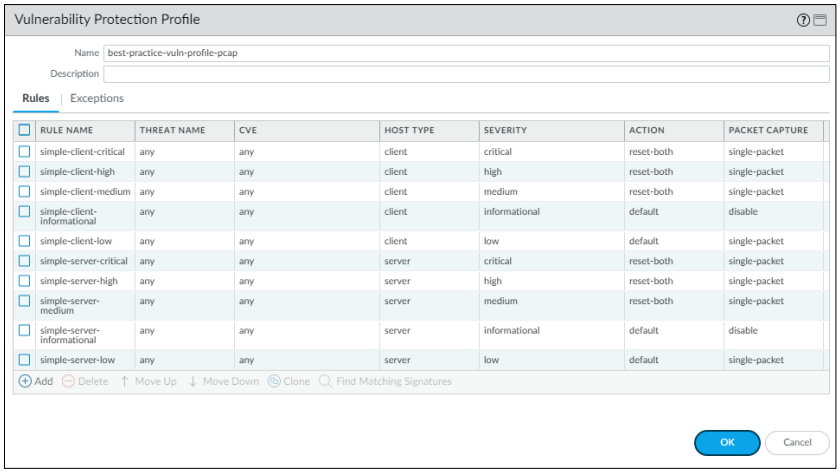


Figura 5-122: Perfil de Vulnerability Protection recomendado

2. Utilizar *Vulnerability Protection* en todas las reglas que permitan tráfico

402. **Ubicación**: "*Policies > Security*"

403. **Recomendación:** Aplicar el perfil de *Vulnerability Protection* configurado, antes en todas las reglas que permitan tráfico para detectar intentos de explotación de vulnerabilidades, tanto de cliente como de servidor.

5.11.7.3 EJEMPLO DE USO

404. En el ejemplo se activarán perfiles de tipo *Vulnerability Protection*, para todo el tráfico que generan los usuarios internos y, también, para el de las DMZs, tanto en entrada como en salida.

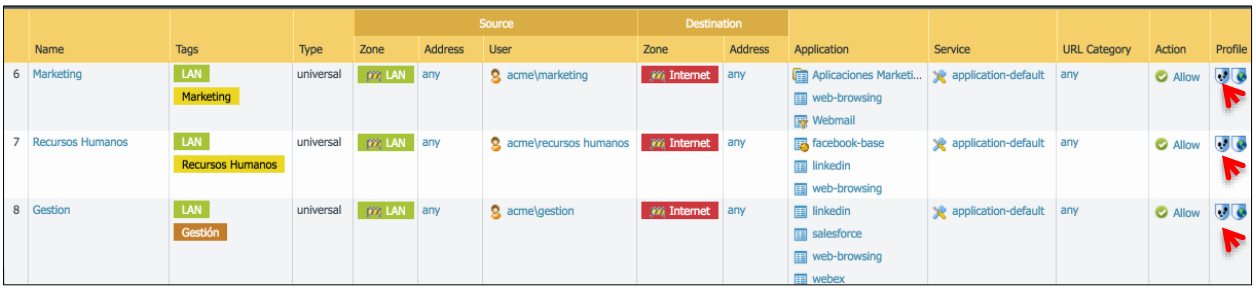


Figura 5-123: Perfiles Vulnerability Protection para clientes

	Name	Tags	Type	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Application	Service	URL Category	Action	Profile
1	Acceso-web-externo	DMZ	universal	Internet	any	any	DMZ	Servidor-web-externo	flash icmp ssl web-browsing	application-default	any	Allow	
2	Acceso-mail-externo	DMZ	universal	Internet	any	any	DMZ	Servidor-correo-externo	activesync icmp imap pop3 smtp ssl web-browsing	application-default	any	Allow	
3	Salida-mail-externo	DMZ	universal	DMZ	Servidor-correo-externo	any	Internet	any	dns smtp	application-default	any	Allow	
4	Updates DMZ	DMZ	universal	DMZ	any	any	Internet	any	apt-get dns ms-update ssl symantec-av-update web-browsing	application-default	any	Allow	

Figura 5-124: Perfiles Vulnerability Protection para la DMZ

5.11.7.4 OBSERVABLES

Logs

405. Los detalles de las alertas de *Vulnerability Protection* pueden consultarse en "*Monitor > Logs > Threat*". La vista detallada de una amenaza particular también referenciará los logs asociados con la entrada.

Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity
09/12 21:25:35	vulnerability	Apache Wicket Unspecified XSS Vulnerability	LAN	Internet	192.168.45.64	acme\user1	204.79.197.203	80	web-browsing	drop	critical
04/27 13:27:23	vulnerability	Windows Command Shell Access	Internet	LAN	192.168.55.90		192.168.45.142	4444	unknown-tcp	alert	critical

Figura 5-125: Ejemplo de log de Vulnerability Protection

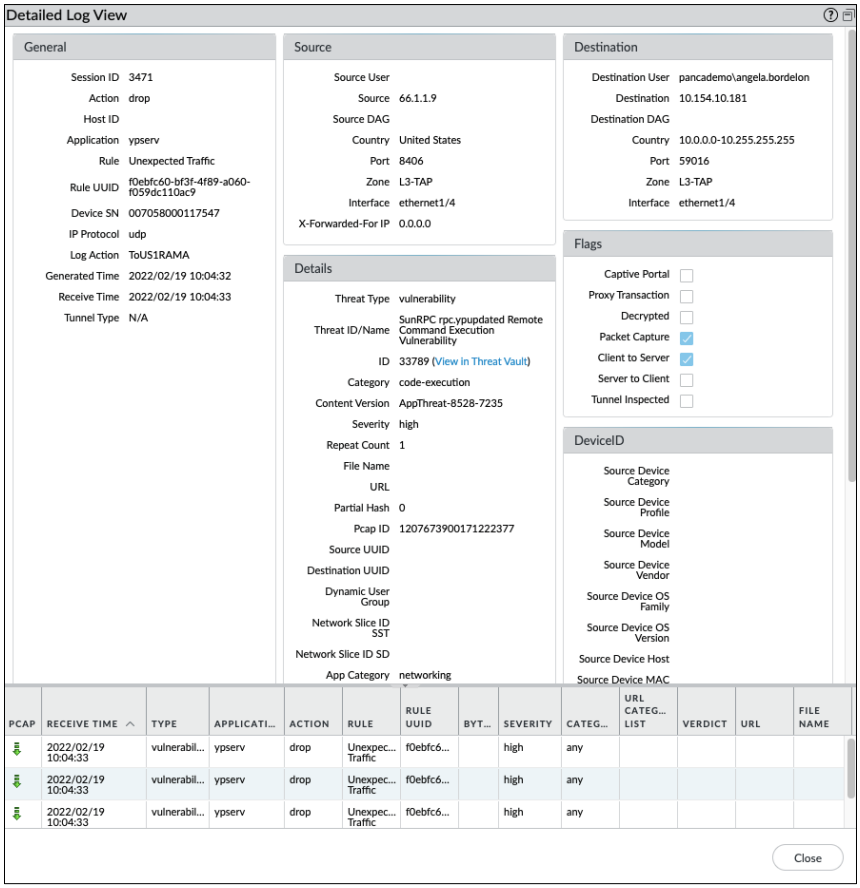


Figura 5-126: Ejemplo de log de Vulnerability Protection detallado

406. Desde la versión 5.0 de PAN-OS es posible crear excepciones de IPs. Esto se consigue haciendo click en el nombre de la amenaza en la vista del log y añadiendo la dirección IP a excluir en los perfiles en los que sea necesario.

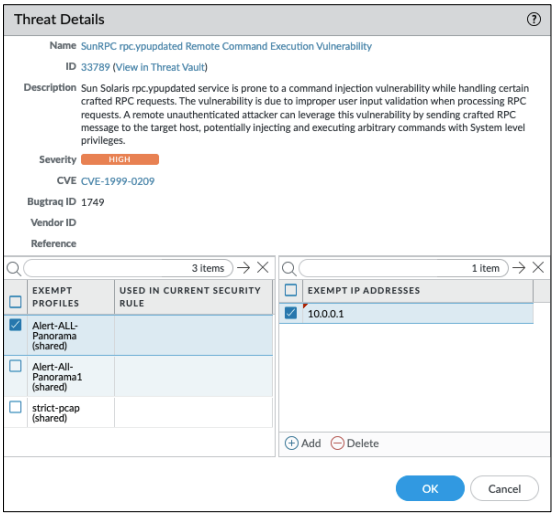


Figura 5-127: Creación de excepciones en los perfiles de Vulnerability Protection

5.11.8 ANTI-SPYWARE

407. La funcionalidad de Anti-Spyware, incluida dentro del servicio de seguridad de Advanced Threat Prevention, detecta y previene el spyware y las comunicaciones de red que realiza el malware. A diferencia del antivirus, la funcionalidad de Anti-Spyware no está limitada a protocolos específicos y puede detectar cualquier tipo de comunicación tipo phone-home.

408. El servicio de seguridad de DNS, incluido dentro del servicio de seguridad de Advanced DNS Security, realiza análisis de solicitudes de DNS en tiempo real utilizando análisis predictivos y aprendizaje automático en múltiples fuentes de datos de DNS. Esto se utiliza para generar protecciones frente a amenazas basadas en DNS, a las que se puede acceder en tiempo real mediante la configuración del perfil de seguridad antispyware adjunto a una regla de política de seguridad. Como servicio basado en la nube, DNS Security permite acceder a una fuente de firmas y protecciones de DNS infinitamente escalable para defender frente a dominios maliciosos. Las firmas de dominio y las protecciones generadas por Palo Alto Networks se derivan de una multitud de fuentes, incluyendo WildFire, DNS pasivo, rastreo web activo y análisis de contenido web malicioso, análisis de sandbox de URL, Honeynet, ingeniería inversa DGA, datos de telemetría, whois, investigación de la Unit 42 y fuentes de datos de terceros, como Cyber Threat Alliance.

409. El servicio *DNS Security* incluye protección frente a las siguientes categorías de ataques DNS:

- Dominios *command-and-control*: Esta categoría incluye direcciones URL y dominios utilizados por malware y/o sistemas comprometidos para comunicarse con el servidor remoto de un atacante para recibir comandos maliciosos o extraer datos. Esta protección incluye detectores de DNS tunneling, DGA (algoritmos de generación de dominio), *NXNSAttack*, *DNS Rebinding* y *DNS Infiltration*.

- Dynamic DNS (DDNS): Al utilizar dominios DDNS los adversarios pueden cambiar la dirección IP asociada con registros DNS determinados y evitar la detección más fácilmente. *DNS Security* detecta servicios de DDNS al filtrar y hacer referencias cruzadas de datos de DNS de varias fuentes para generar listas de candidatos que luego se validan para maximizar la precisión.

- Dominios de malware: Los dominios maliciosos alojan y distribuyen malware, y pueden incluir sitios web que intentan instalar varios tipos de amenazas en sus víctimas.

- Nuevos dominios: Si bien se pueden crear nuevos dominios con fines legítimos, la gran mayoría a menudo se utilizan para facilitar actividades maliciosas.

- Dominios de *Phishing*: Dominios utilizados para engañar a sus víctimas con el fin de obtener información privilegiada.

- Dominios *Grayware*: Su objetivo es facilitar vectores de ataque, producir varios comportamientos indeseables, o simplemente pueden mostrar contenido ofensivo.

Dominios *Parked*: Sitios webs inactivos que ofrecen contenido limitado con fines lucrativos.

- Proxy Avoidance & *Anonymizers*: Ofrecen servicios para evitar restricción de contenido, permitiendo hacer bypass de la política de seguridad establecida en una organización.

410. Para habilitar la protección de la seguridad DNS, se debe activar la suscripción del servicio *Advanced DNS Security*, y crear un perfil Anti-Spyware para hacer referencia al servicio, para posteriormente referenciar el perfil en una política de seguridad.

A. Perfiles Predefinidos

411. Por defecto se ofrecen dos perfiles de Anti-Spyware predefinidos:

412. El perfil "*default*" aplica la acción por defecto a todas las firmas con severidad crítica, alta, media y baja. No registra las catalogadas como informacionales.

413. El perfil "*strict*" aplica la acción de bloqueo a todas las firmas con severidad crítica, alta y media. Para las bajas e informacionales aplica la acción por defecto.

NAME	LOCATION	COUNT	POLICY NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
default	Predefined	Policies: 4	simple-critical	any	critical	default	disable
			simple-high	any	high	default	disable
			simple-medium	any	medium	default	disable
			simple-low	any	low	default	disable
strict	Predefined	Policies: 5	simple-critical	any	critical	reset-both	disable
			simple-high	any	high	reset-both	disable
			simple-medium	any	medium	reset-both	disable
			simple-informational	any	informational	default	disable
			simple-low	any	low	default	disable

Figura 5-128: Perfiles de Anti-Spyware predefinidos

B. Perfiles Personalizados

414. Además de los perfiles predefinidos es posible crear perfiles personalizados. Un perfil personalizado puede contener una o más reglas y excepciones que definen qué firmas de *Anti-Spyware* han de incluirse. Para cada regla es posible seleccionar qué tipo de acción se desea que se aplique, la categoría de firmas a activar y la severidad.

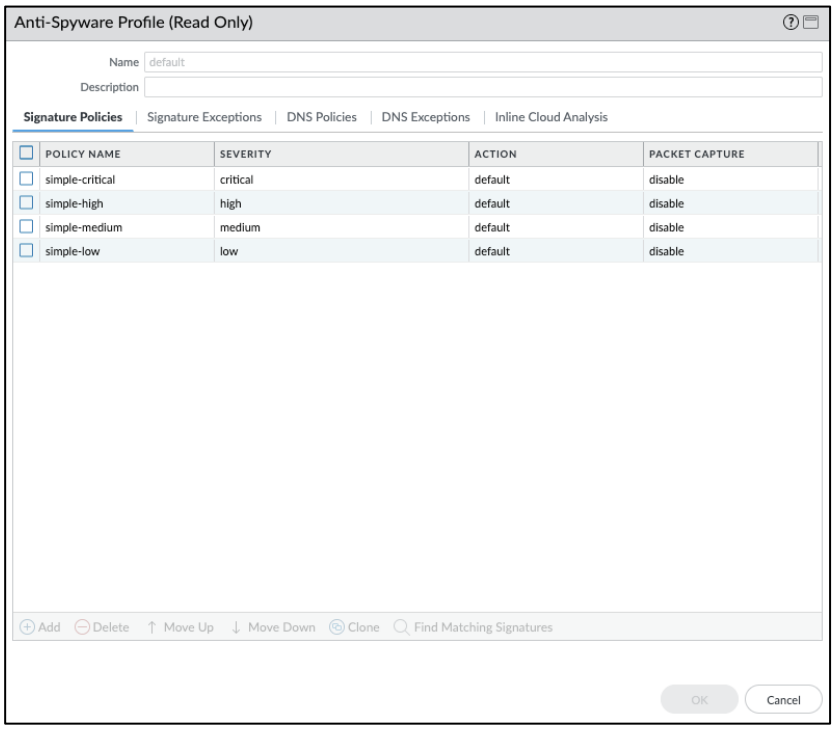


Figura 5-129: Perfiles de Anti-Spyware personalizados

415. Los perfiles personalizados permiten, también, la configuración de la captura de paquetes sobre el tráfico que hace match. Estas capturas pueden utilizarse para obtener evidencia de los ataques o para propósitos de depuración.

A. DNS Policies

416. Bajo la pestaña *DNS Policies* en el perfil *Anti-Spyware*, se configuran los ajustes de la política de seguridad DNS, pudiendo definir distintas acciones en función de la categoría de la amenaza DNS.

Nota: Si se desea obtener más información sobre la configuración del servicio DNS: *https://docs.paloaltonetworks.com/dns-security/administration/configure-dns-security/enable-dns-security*

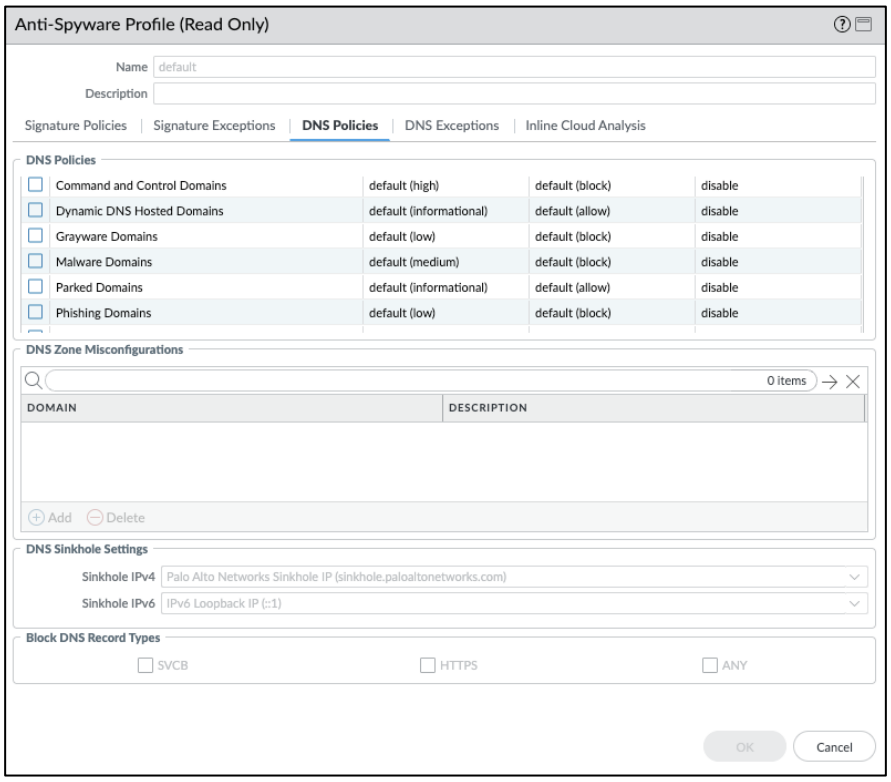


Figura 5-130: Políticas de DNS

417. La función de sinkholing permite que los administradores puedan identificar los equipos de la red que están infectados a través del análisis del tráfico DNS, incluso cuando el cortafuegos está al norte de un DNS local (por ej., en una configuración de Active Directory donde el cortafuegos no está entre los clientes y los DC, que actúan como servidores DNS internos).

418. En una configuración sin sinkhole, el log de threat identificará la IP del DNS resolver local, como el origen del tráfico en lugar del equipo que realmente está infectado. Con sinkholing configurado, los clientes reciben una respuesta DNS con una IP configurada por el administrador. Los equipos infectados pueden posteriormente identificarse fácilmente en los logs de traffic, porque mostrarán intentos de conexión contra la IP de sinkhole.

419. Si se desea que las peticiones de *sinkhole* alcancen un servidor de Palo Alto Networks que actúa como *honeypot*, con el fin de mejorar las capacidades de detección, hay que seleccionar la IP de Palo Alto Networks en la configuración.

Nota: Si se desea obtener más información sobre DNS Sinkholing visitar: *https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/configure-threat-prevention/use-dns-queries-to-identify-infected-hosts-on-the-network/how-dns-sinkholing-works*

420. Palo Alto Networks utiliza una serie de motores de detección basados en *Machine Learning* (ML) en la nube de *Advanced Threat Prevention* para analizar el tráfico en busca de amenazas avanzadas C2 (comando y control) y *spyware* en tiempo real para proteger a los usuarios frente a las amenazas de día cero. Al utilizar motores de detección basados en la nube, puede acceder a una amplia gama de mecanismos de detección que se

actualizan y despliegan automáticamente sin necesidad de que el usuario descargue paquetes de actualización ni utilice analizadores en el NGFW que requieren mucho proceso y pueden mermar los recursos. La lógica del motor de detección basado en la nube se supervisa y actualiza continuamente mediante con datos de tráfico C2 de *WildFire*, y con actualizaciones manuales por parte de investigadores de amenazas de Palo Alto Networks para detecciones más precisas. El análisis en línea en la nube admite cinco motores de análisis para amenazas basadas en C2 a través de HTTP, HTTP2, SSL, UDP desconocido y TCP desconocido. Los modelos de análisis adicionales se suministran a través de actualizaciones de contenido; sin embargo, las mejoras de los modelos existentes se realizan como una actualización desde la nube, y no requiere actualización del cortafuegos. El análisis en línea en la nube se activa y configura mediante el perfil antispyware y requiere una licencia activa de *Advanced Threat Prevention*.

421. **Ubicación**: "*Objects > Security Profiles > Anti-spyware > Inline Cloud Analysis*"

422. **Requisito de seguridad:** Se debe habilitar "*Enable cloud inline analysis*". Especificar la acción a realizar cuando se detecte una amenaza utilizando el motor de análisis correspondiente. Las opciones disponibles son:

- *Allow* – La solicitud se permite y no se genera entrada de log.
- *Alert* – La petición se permite y se genera entrada de log.
- *Drop* – Se tira la petición, no se envía acción de reset al host/aplicación.
- *Reset-Client* – Se resetea la conexión del lado del cliente.
- *Reset-Server* – Se resetea la conexión del lado del servidor.
- *Reset-Both* – Se resetea la conexión en ambos lados cliente y servidor.

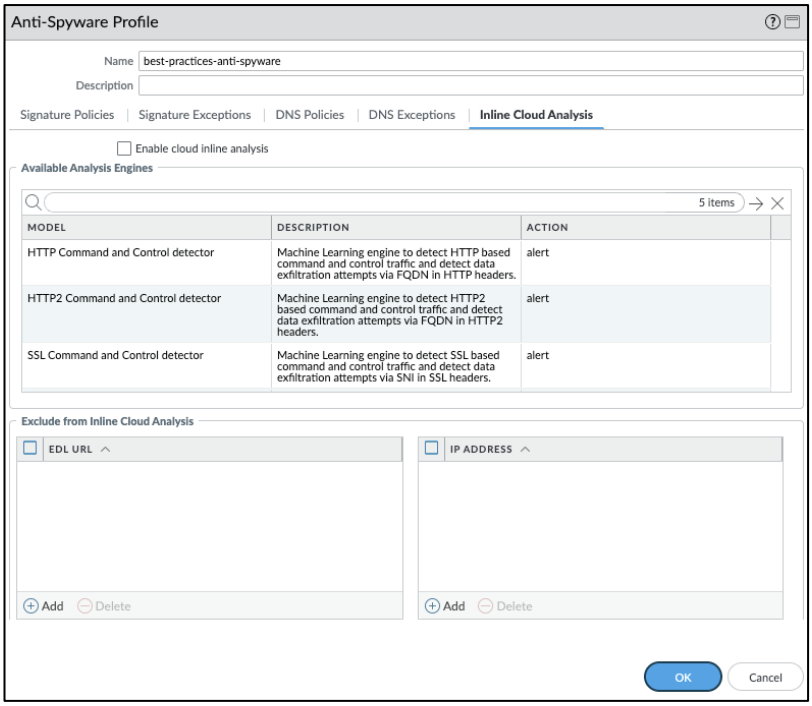


Figura 5-131: Análisis Inline en la nube

5.11.8.1 COMBATIENDO LA CADENA DE CIBERATAQUE

	Entrega	Explotación	Instalación	Mando y Control	Acciones en el Objetivo
Anti-Spyware				Bloquear el *spyware* y el tráfico C2	Bloquear la extracción de datos mediante DNS

Tabla 11: Cadena de ciberataque - Anti-Spyware

423. El módulo de *Anti-Spyware* puede ayudar en la rotura de la cadena de ataque en la fase de Mando y Control, evitando que los equipos comprometidos puedan conectarse contra los servidores C2.

5.11.8.2 REQUISITOS DE SEGURIDAD

1. Configurar perfil de *Anti-spyware*

424. **Ubicación**: "*Objects > Security Profiles > Anti-spyware*"

425. **Requisito de seguridad:** Se debe configurar un perfil con todas las firmas de tipo *critical*, *high* y *medium* en modo *reset-both* (denegación), y con la captura de paquetes activada, y el resto con su acción por defecto.

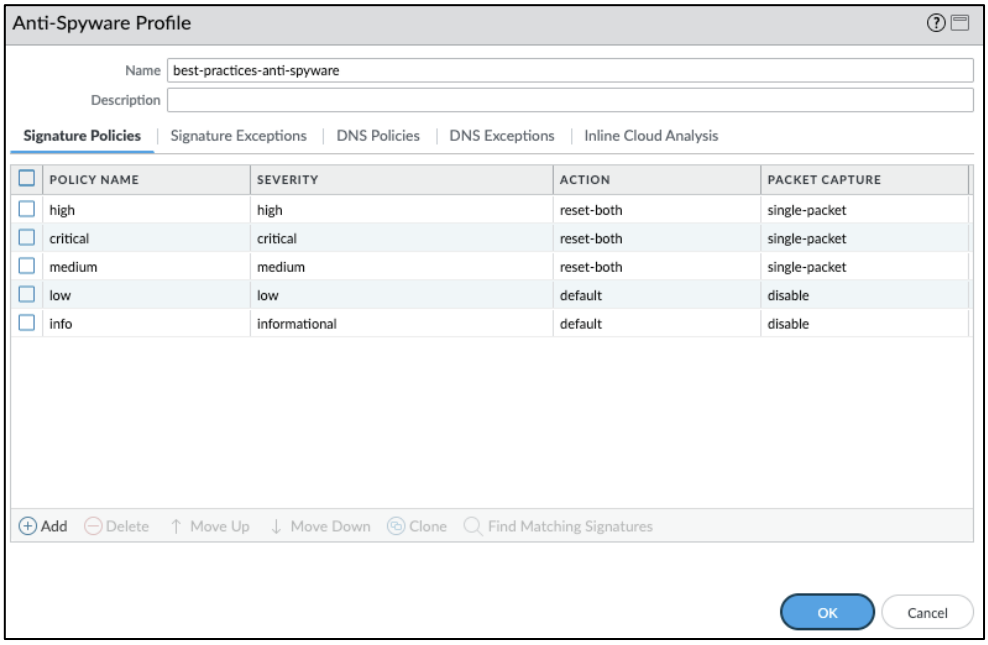


Figura 5-132: Perfil de Anti-spyware recomendado

2. Configurar DNS *Sinkholing*

426. **Ubicación**: "*Objects > Security Profiles > Anti-spyware*"

427. **Recomendación:** Se debe activar la configuración de *DNS-Sinkholing* mostrada anteriormente sobre el mismo perfil de Anti-spyware, utilizando la IP de *Sinkholing* de

Palo Alto Networks o, en su defecto, una propia. Opcionalmente, se puede activar *Passive DNS Monitoring* para contribuir a mejorar la inteligencia de amenazas.

3. Utilizar *anti-spyware* en todas las reglas que permitan tráfico hacia internet

428. **Ubicación**: "*Policies > Security*"

429. **Requisito de seguridad:** Se debe aplicar el perfil de Anti-spyware configurado antes, en todas las reglas que permitan tráfico hacia internet, para detectar tanto los intentos de infección como las conexiones hacia servidores de mando y control de equipos infectados.

5.11.8.3 EJEMPLO DE USO

430. En el ejemplo, se activan perfiles de tipo *Anti-Spyware* para todo el tráfico que generan los usuarios y las actualizaciones de la DMZ. Para ello, se clonan los perfiles por defecto tal y como se especificó en el punto anterior, y se aplica a las reglas en cuestión:

Figura 5-133: Perfiles Anti-Spyware para clientes

5.11.8.4 OBSERVABLES

Logs

431. Los detalles de las alertas de Anti-*Spyware* pueden consultarse en "*Monitor > Logs > Threat*". La vista detallada de una amenaza particular también referenciará los logs asociados con la entrada. Obsérvese que la siguiente imagen muestra un ejemplo de *spyware* y otro de *sinkhole*:

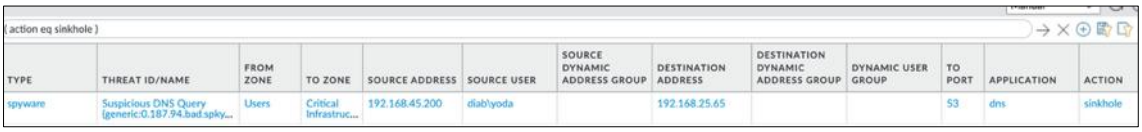


Figura 5-134: Ejemplo de log de Anti-Spyware

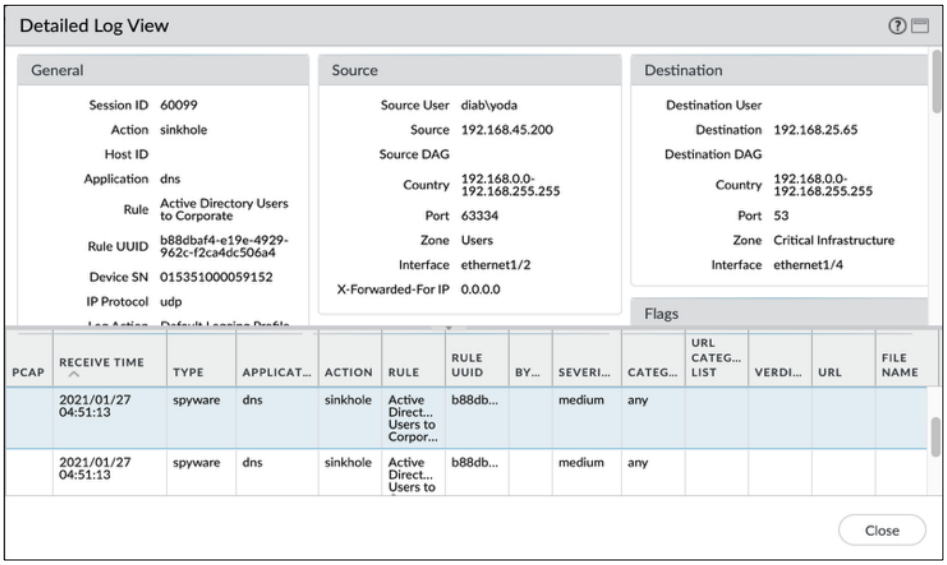


Figura 5-135: Ejemplo de log de Anti-Spyware detallado

432. Al igual que los perfiles de *Vulnerability Protection*, es posible crear excepciones de IPs para los perfiles de *Anti-Spyware*. Esto se consigue haciendo click en el nombre de la amenaza en la vista del log y añadiendo la dirección IP a excluir en los perfiles en los que sea necesario.

5.11.9 ANTIVIRUS

433. La funcionalidad de Antivirus, incluida dentro del servicio de seguridad de *Advanced Threat Prevention*, detecta y previene la transmisión de virus sobre los siguientes protocolos:

- HTTP
- FTP
- SMTP
- IMAP
- POP3
- SMB

434. Los ficheros transmitidos por cualquier aplicación que use cualquiera de los protocolos anteriores, será inspeccionado por la funcionalidad de Antivirus. La inspección tiene lugar siguiendo un motor de análisis tipo *streaming*, lo que significa que los ficheros no son cacheados ni almacenados al completo en el cortafuegos, sino analizados en tiempo real según circulan por el equipo. Esto implica que la experiencia del usuario es buena puesto que recibe los contenidos según se inspeccionan, sin dilación.

A. Perfil Predefinido

435. Hay un perfil predeterminado denominado *default* disponible para el perfil de Antivirus. Este perfil tiene la acción por defecto configurada para cada protocolo y difiere de unos a otros, tal y como puede verse en la siguiente figura:

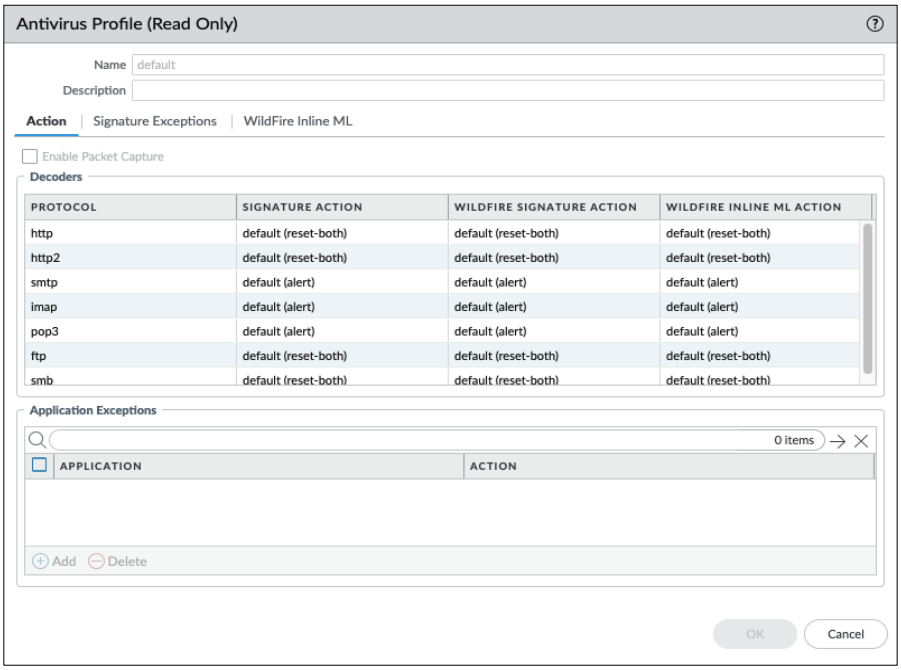


Figura 5-136: Perfil por defecto del Antivirus

Nota: La razón por la que los protocolos SMTP, IMAP y POP3 tienen la acción por defecto configurada como *Alert*, es porque en la mayoría de las ocasiones ya existen *gateways* de Antivirus dedicados para estos protocolos. No obstante, para el protocolo SMTP sí que es posible configurar una acción de bloqueo.
Para POP3 e IMAP no se recomienda configurar la acción en bloqueo porque, debido a limitaciones de los propios protocolos, no es posible eliminar un fichero en modo *streaming* sin afectar a toda la sesión.

B. Perfiles Personalizados

436. Al igual que con los módulos de *Vulnerability Protection* y *Anti-Spyware*, el módulo de Antivirus permite crear perfiles personalizados y también excepciones. La siguiente figura muestra un ejemplo de ello:

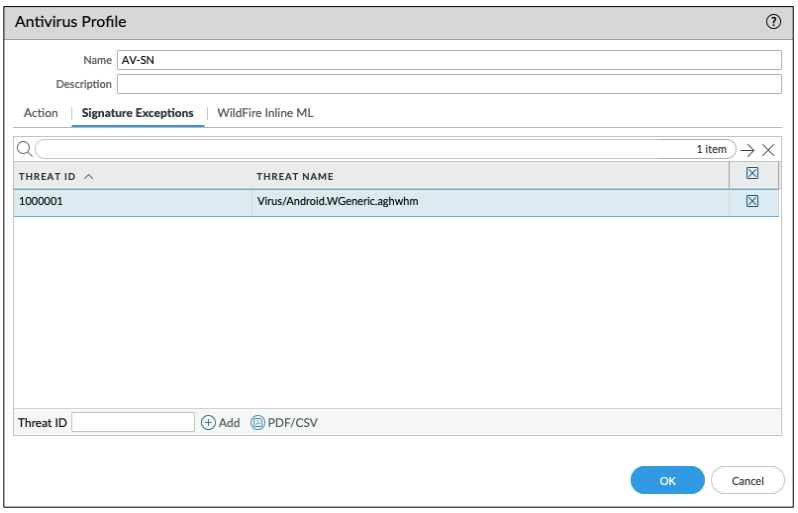


Figura 5-137: Excepción en perfil de Antivirus personalizado

Nota: Si se desea obtener más información sobre el módulo de Antivirus visitar: *https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/threat-prevention*

5.11.9.1 COMBATIENDO LA CADENA DE CIBERATAQUE

	Entrega	Explotación	Instalación	Mando y Control	Acciones en el Objetivo
Antivirus			Bloquear ficheros maliciosos		Prevenir el movimiento lateral

Tabla 12: Cadena de ciberataque - Antivirus

437. El módulo de Antivirus puede ayudar en la rotura de la cadena de ataque en la fase de Instalación, bloqueando los ficheros maliciosos y las herramientas de *exploiting* cuando circulan por la red. También puede ofrecer el mismo tipo de protección frente a los intentos de movimiento lateral cuando los *exploit kits*, u otras herramientas, se copian hacia otros equipos comprometidos.

5.11.9.2 REQUISITOS DE SEGURIDAD

438. La configuración del perfil por defecto del módulo de Antivirus puede utilizarse en la mayoría de los casos, cuando existen otras soluciones de análisis para los protocolos SMTP, POP3 e IMAP. Puesto que los perfiles predefinidos son solamente de lectura, se recomienda copiarlos para que se puedan definir excepciones si son necesarias, además de configurar la captura de paquetes por si es necesario hacer un análisis posterior.

439. Si no existe un gateway de antivirus dedicado para el protocolo SMTP, entonces es posible configurar un perfil personalizado en el que la acción para SMTP se cambia de alert a reset-both. En este caso, el cortafuegos enviará un mensaje de respuesta con código 541 al servidor SMTP remitente, para informarle de que se ha detectado un virus y evitar así que siga reenviando el mismo mensaje.

440. Las firmas de Antivirus se generan en función del *payload* de cada tipo de fichero, lo que significa que una misma firma puede cubrir muchas variantes del mismo *malware*. Normalmente presentan, además, una ratio de falsos positivos muy pequeño. Si, no obstante, se encontrara uno, es posible excluirlo de un perfil personalizado tal y como se mostró anteriormente.

1. Configurar perfil de antivirus

441. **Ubicación**: "*Objects > Security Profiles > Antivirus*"

442. **Recomendación**: Se recomienda configurar un perfil con los *decoders* http, ftp, smb y smtp en modo *reset-both* y pop3 e imap en *alert*, con la captura de paquetes activada, tanto para la columna del Antivirus (*Action*) como para la columna de *WildFire* (*WildFire Action*). La columna *Action* regula las firmas de la suscripción de Antivirus, mientras que la columna *WildFire Action*, regula las firmas que se reciben a través de la suscripción del servicio de *WildFire*.

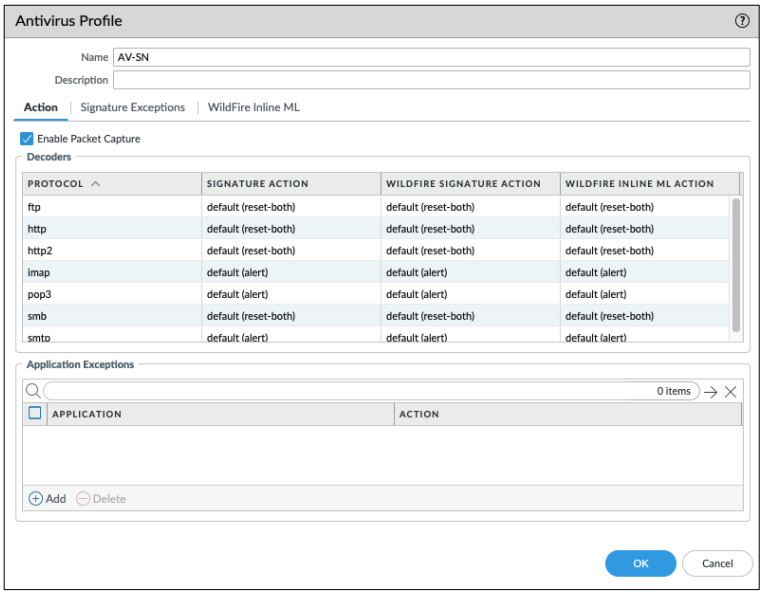


Figura 5-138: Perfil de Antivirus recomendado

2. Utilizar antivirus en todas las reglas que permitan tráfico

443. **Ubicación:** "*Policies > Security*"

444. **Requisito de seguridad:** Se debe aplicar el perfil de Antivirus configurado antes, en todas las reglas de seguridad que permitan el tráfico, para detectar tanto el malware conocido como el nuevo que se registra y actualiza a través de *WildFire*.

5.11.9.3 EJEMPLO DE USO

445. En el ejemplo, se van a activar perfiles de tipo Antivirus para todo el tráfico que generan los usuarios y las actualizaciones de la DMZ. Para ello, se clonan los perfiles por defecto, tal y como se especificó en el punto anterior, y se aplicarán a las reglas en cuestión:

	Name	Tags	Type	Source			Destination		Application	Service	URL Category	Action	Profile
				Zone	Address	User	Zone	Address					
6	Marketing	LAN Marketing	universal	LAN	any	acme\marketing	Internet	any	Aplicaciones Marketing web-browsing Webmail	application-default	any	Allow	
7	Recursos Humanos	LAN Recursos Humanos	universal	LAN	any	acme\recursos humanos	Internet	any	facebook-base linkedin web-browsing	application-default	any	Allow	
8	Gestion	LAN Gestión	universal	LAN	any	acme\gestion	Internet	any	linkedin salesforce web-browsing webex	application-default	any	Allow	
9	Otros usus auten	LAN	universal	LAN	any	known-user	Internet	any	facebook-base flash gmail-base ssl web-browsing	application-default	any	Allow	

Figura 5-139: Perfiles Antivirus para clientes

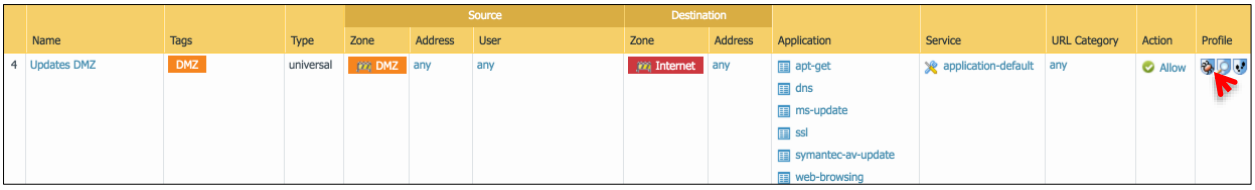


Figura 5-140: Perfiles Antivirus para las actualizaciones de la DMZ

5.11.9.4 OBSERVABLES

Logs

446. Los detalles de las alertas de Antivirus pueden consultarse en *Monitor > Logs > Threat*. La vista detallada de una amenaza particular también referenciará los logs asociados con la entrada.

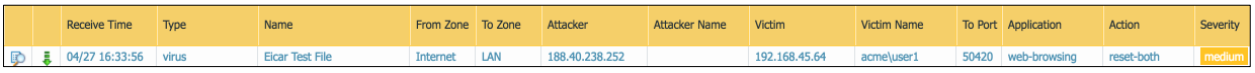


Figura 5-141: Ejemplo de log de Antivirus

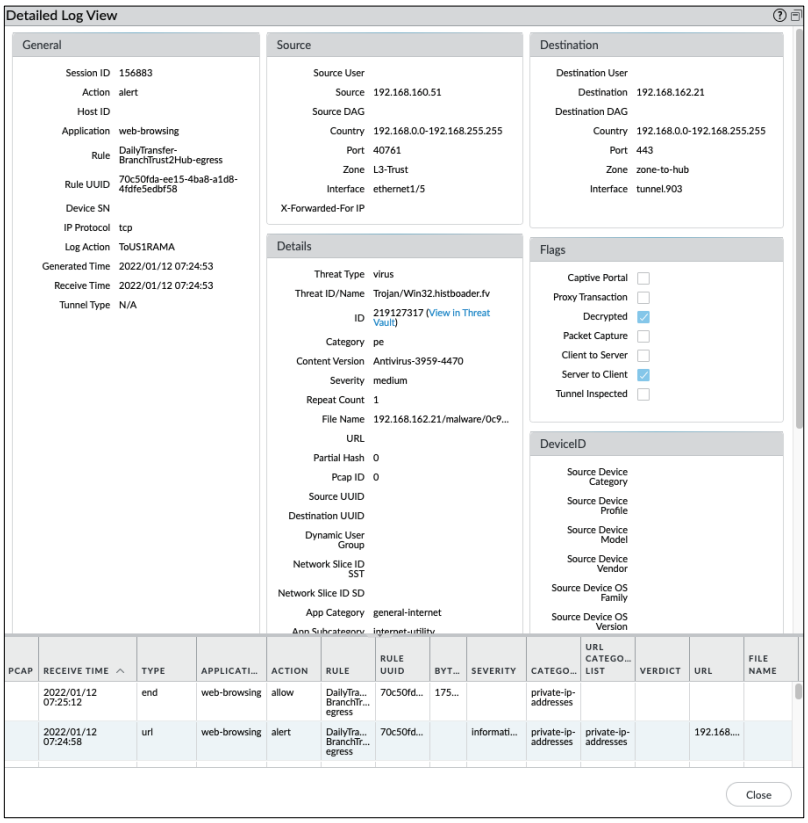


Figura 5-142: Ejemplo de log de Antivirus detallado

Notificación al usuario

447. Cuando un usuario intenta descargar un virus a través de alguna aplicación de tipo web, se le informa a través de una página en el navegador que es posible personalizar en *"Device > Response Pages":*

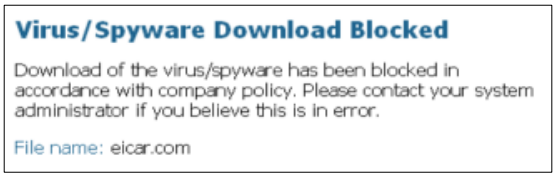


Figura 5-143: Ejemplo de página de bloqueo de Antivirus

5.11.10 BLOQUEO DE FICHEROS (*FILE BLOCKING*)

448. Cuando se usan los perfiles de *File Blocking* es posible detectar y prevenir las descargas y *uploads* de diferentes tipos de archivos. Como ocurre con otros perfiles de seguridad, los perfiles de *File Blocking* pueden habilitarse por regla de seguridad, por lo que es posible crear controles muy granulares para segmentos de red, usuarios y grupos de usuarios específicos.

5.11.10.1 COMBATIENDO LA CADENA DE CIBERATAQUE

	Entrega	Explotación	Instalación	Mando y Control	Acciones en el Objetivo
File Blocking			Bloquear los ficheros no necesarios y prevenir los *drive-by downloads*		Prevenir la exfiltración de datos y el movimiento lateral

Tabla 13: Cadena de ciberataque - File Blocking

449. El módulo de *File Blocking* puede usarse para romper la cadena de ataque en la fase de Instalación, al evitar la descarga o *upload* de determinados tipos de ficheros, como por ejemplo los ejecutables. Esta funcionalidad es especialmente útil para bloquear los *drive-by downloads*, en los que un fichero es descargado en el sistema sin que el usuario se dé cuenta. Los perfiles de *File Blocking* también son útiles para evitar la fuga de datos al prevenir el envío de ficheros a servicios públicos diferentes a los que aprueba la organización.

5.11.10.2 REQUISITOS DE SEGURIDAD

450. La funcionalidad de *File Blocking* es especialmente útil, ya que evita que los usuarios se descarguen e instalen *software* no verificado sobre equipos de la compañía y también previniendo los *drive-by download.* No existen perfiles predefinidos, pero son fáciles de crear. Si bloquear ficheros es demasiado estricto, debería considerarse el uso de la acción "*Continue*" al menos para los tipos de fichero más peligrosos. Esto requerirá que el usuario tenga que confirmar explícitamente la descarga de este tipo de ficheros, lo que resulta ser un mecanismo simple pero muy efectivo contra los *drive-by download.*

1. Configurar perfil de *File Blocking*

451. **Ubicación**: "*Objects > Security Profiles > File Blocking*"

452. **Requisito de seguridad**: Los perfiles que habrá que crear, serán diferentes en función de los usuarios y los privilegios de gestión de archivos que tengan, por lo que es complicado

señalar en esta guía una recomendación válida para todos los escenarios. En cualquier caso, y como mínimo, se debe configurar un perfil que audite todos los archivos intercambiados, a través de una acción de tipo *alert*.

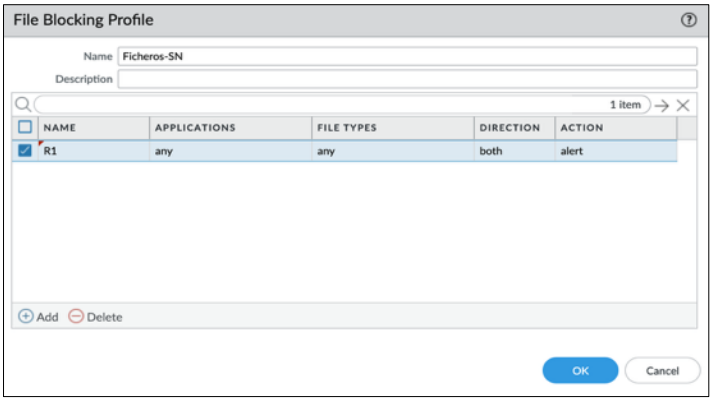


Figura 5-144: Perfil de File Blocking

2. Utilizar *file blocking* en todas las reglas que permitan tráfico

453. **Ubicación:** "*Policies > Security*"

454. Requisito de seguridad: Se debe aplicar el perfil o perfiles de *File Blocking* configurados antes, en todas las reglas de seguridad que permitan el tráfico. Si se dispone de varios perfiles de *File Blocking*, estos pueden aplicarse en función de los tipos de usuarios y tráfico para cada regla.

5.11.10.3 EJEMPLO DE USO

455. En el ejemplo se va a aplicar la siguiente política:
    - Avisar al usuario de la descarga de los ficheros ejecutables.
    - Avisar al usuario de la descarga y el upload de los ficheros *torrent*.
    - Avisar al usuario de la descarga de ficheros cifrados.

456. En las siguientes figuras se muestra cómo se configura el perfil y cómo se aplica para las reglas de usuarios, a excepción del grupo IT:

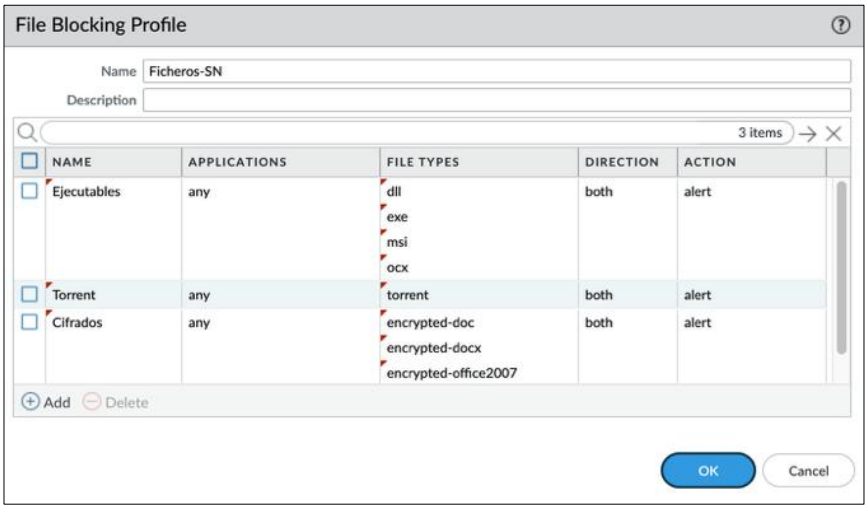
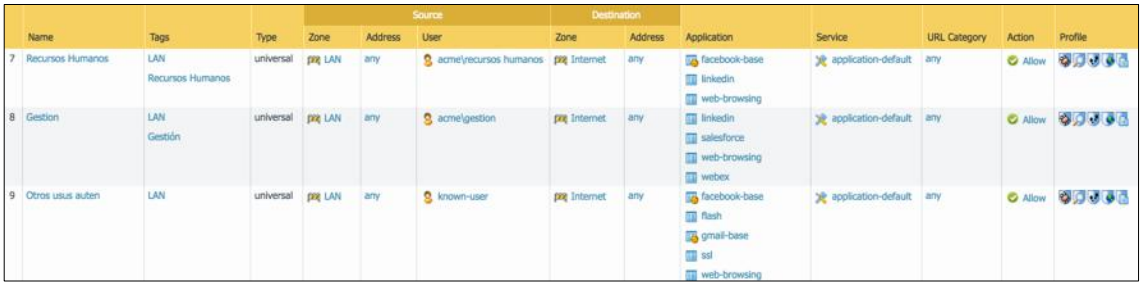


Figura 5-145: Ejemplo de Perfil de File Blocking



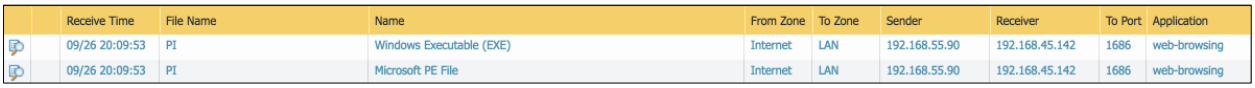
	Name	Tags	Type	Source Zone	Source Address	Source User	Destination Zone	Destination Address	Application	Service	URL Category	Action	Profile
7	Recursos Humanos	LAN Recursos Humanos	universal	LAN	any	acme\recursos humanos	Internet	any	facebook-base linkedin web-browsing	application-default	any	Allow	
8	Gestion	LAN Gestión	universal	LAN	any	acme\gestion	Internet	any	linkedin salesforce web-browsing webex	application-default	any	Allow	
9	Otros usus auten	LAN	universal	LAN	any	known-user	Internet	any	facebook-base flash gmail-base ssl web-browsing	application-default	any	Allow	

Figura 5-146: Aplicación de File Blocking en las reglas de seguridad

5.11.10.4 OBSERVABLES

Logs

457. Los detalles de las alertas de *File Blocking* pueden consultarse en "*Monitor > Logs > Data Filtering*". La vista detallada de un fichero particular también referenciará los logs asociados con esa entrada.



	Receive Time	File Name	Name	From Zone	To Zone	Sender	Receiver	To Port	Application
	09/26 20:09:53	PI	Windows Executable (EXE)	Internet	LAN	192.168.55.90	192.168.45.142	1686	web-browsing
	09/26 20:09:53	PI	Microsoft PE File	Internet	LAN	192.168.55.90	192.168.45.142	1686	web-browsing

Figura 5-147: Ejemplo de log de File Blocking

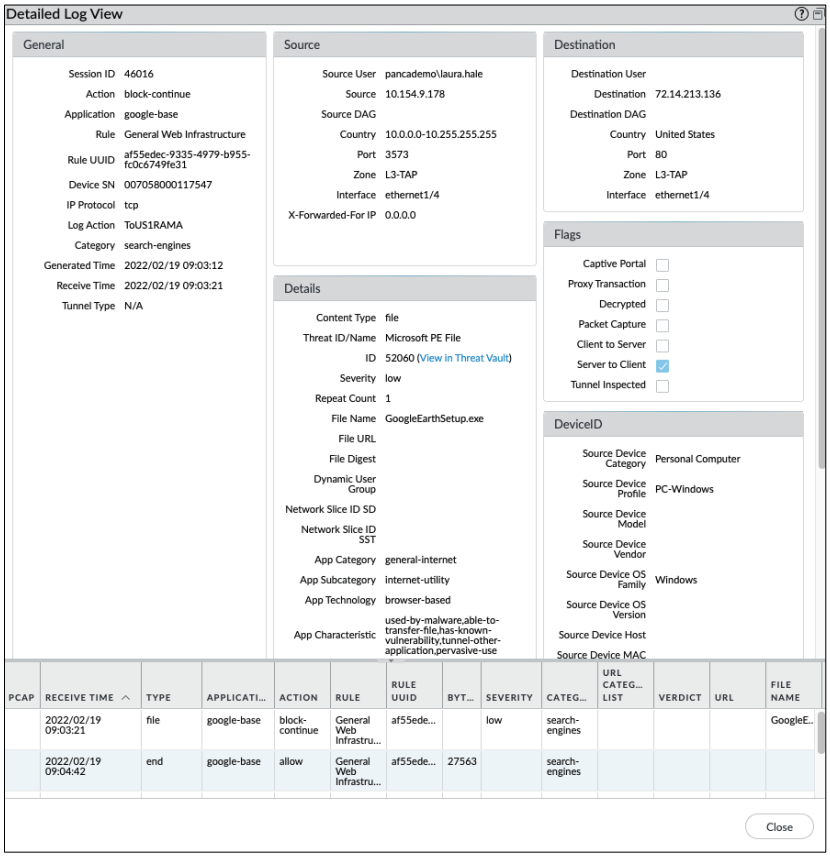


Figura 5-148: Ejemplo de log de File Blocking detallado

Notificación al usuario

458. Cuando un usuario intenta descargar un fichero bloqueado o configurado con la acción "*Continue*" a través de alguna aplicación de tipo web, se le informa a través de una página en el navegador que es posible personalizar en "*Device > Response Pages":*

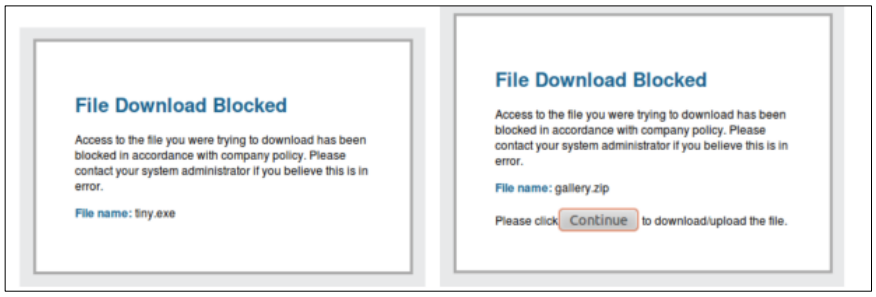


Figura 5-149: Ejemplo de página de bloqueo y Continue de File Blocking

5.11.11 WILDFIRE

459. El *malware* moderno es el corazón de muchos de los ataques más sofisticados a las redes hoy día. Cada vez se personaliza más para intentar evadir las medidas de seguridad tradicionales. Palo Alto Networks ha desarrollado una aproximación integral que es capaz de trabajar en el ciclo de vida completo del malware, lo que incluye la prevención de la infección, la identificación del *malware zero-day* (es decir, *malware* nunca antes identificado) o el *malware* dirigido, además de identificar y bloquear las infecciones activas.

460. El motor de *WildFire*, incluido dentro del servicio de seguridad de *Advanced WildFire*, descubre el *malware zero-day*, así como el dirigido a través de la observación directa de su comportamiento en un entorno virtual y seguro, fuera de la red del cliente (*sandbox*). La funcionalidad de *WildFire* también se aprovecha del contexto de la aplicación que ofrece App-ID, y gracias a ella, es capaz de identificar las transferencias de archivos en múltiples aplicaciones y no solamente en los adjuntos de email o las descargas web.

461. Además de identificar el *malware* nunca antes visto, *WildFire* es capaz de generar firmas rápidamente para prevenir infecciones futuras del *malware* descubierto. Desde la versión PAN-OS 10.0 se pueden analizar ejecutables de Windows y scripts de *PowerShell* mediante *machine learning* en el plano de datos detectando el malware antes de que pueda infiltrarse en la red al proporcionar capacidades de análisis en tiempo real en el firewall, lo que reduce la posibilidad de proliferación de variantes de malware desconocidas.

462. Se ofrece una distribución global de firmas de antivirus de WildFire en tiempo real tan pronto haya nuevos veredictos disponibles, proporcionando acceso instantáneo a la inteligencia global de Palo Alto Networks procedente de multitud de fuentes, previniendo el éxito de los ataques, minimizando el tiempo de exposición a actividades maliciosas, la superficie del ataque y el daño resultante que el malware puede realizar dentro de la red.

463. Además, y tal y como se comentó en el apartado 5.11.9 ANTIVIRUS, las firmas están basadas en el payload, por lo que una misma firma puede identificar múltiples variantes de la misma familia de malware, incluso las que aún no se han visto.

464. El cortafuegos puede ofrecer alertas instantáneas cuando se detecta malware nuevo en la red, gracias al envío de alertas, mensajes de syslog o traps SNMP. Además, todas las firmas que WildFire genera son automáticamente propagadas a todos los cortafuegos y endpoints de Palo Alto Networks que tengan las suscripciones correspondientes.

465. Finalmente, el servicio *sandbox* de *WildFire* se comercializa tanto en formato de nube pública, como en formato de nube privada (*appliance* WF-500), para aquellos clientes que no quieren enviar archivos fuera de la organización. También se soporta un entorno mixto, en el que el administrador determina qué ficheros envía a la nube pública y cuáles a la privada (por ej. los binarios a la nube pública y los documentos a la privada).

466. Con el fin de garantizar el cumplimiento de las leyes europeas y nacionales, es importante señalar que la nube pública de *WildFire* cuenta con una instancia dentro de la Unión Europea, más concretamente en Amsterdam, de tal manera que los archivos no abandonen las fronteras europeas.

Nota: Si se desea obtener más información sobre *WildFire* visitar:
https://docs.paloaltonetworks.com/advanced-wildfire
Información sobre la derogación de la ley "*Safe Harbor*":
http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117es.pdf

5.11.11.1 COMBATIENDO LA CADENA DE CIBERATAQUE

	Entrega	Explotación	Instalación	Mando y Control	Acciones en el Objetivo
WildFire Threat Intelligence	Detectar nuevos sites maliciosos		Detectar malware desconocido	Detectar nuevo tráfico C2	

Tabla 14: Cadena de ciberataque - *WildFire Threat Intelligence*

467. Los resultados de los análisis de *WildFire* se utilizan para generar firmas para diferentes mecanismos de protección. Actualmente, *WildFire* puede generar firmas contra ficheros y nombres DNS maliciosos, así como alimentar las categorías de *malware* y *phishing* del filtrado URL PAN-DB. Por todo ello, se ha convertido en una herramienta crítica para conseguir romper la cadena de ataque, especialmente frente al malware desconocido.

5.11.11.2 REQUISITOS DE SEGURIDAD

468. Dada la proliferación del malware desconocido, es altamente recomendable habilitar el análisis de *WildFire* para todos los ficheros nuevos. Como se comentó anteriormente, se soporta tanto la nube pública, como la privada e híbrida. Los ficheros que actualmente *WildFire* es capaz de inspeccionar son: .exe, .dll, .scr, .ocx, .sys, .drv, Adobe (.pdf), documentos Microsoft Office (.doc, .docx., .xls, .xlsx, .ppt, y .pptx), .rtf, Java (.jar y ficheros class), Adobe Flash .swf, Android. apk y OS-X (Mach-O, DMG*, PKG y application bundle).*

Nota: Desde la versión PAN-OS 7.0 ya no es necesario configurar un perfil de *File Blocking* con la acción configurada como "*forward*" o "*continue-and-forward*" para enviar los ficheros a *WildFire*.

469. Además de enviar los ficheros para su análisis, las transferencias maliciosas también pueden ser bloqueadas inmediatamente si una firma de *WildFire* está disponible de antemano. Para conseguir este objetivo es necesario configurar un perfil de Antivirus con la acción configurada a *"reset-both"* en la columna de "*WildFire Action"* para los protocolos correspondientes.

1. Configurar el uso de la nube pública *WildFire* europea o España

470. **Ubicación**: "Device > Setup > Wildfire > General Settings"

471. **Recomendación**: Cambie la configuración de la nube pública por defecto, para utilizar solamente la ubicada dentro de la Unión Europea, "*eu.wildfire.paloaltonetworks.com*" o más específicamente la región de España *"es.wildfire.paloaltonetworks.com"*. Esta configuración es importante para cumplir con las normativas que imponen limitaciones en la ubicación de los datos fuera de territorio europeo. Se destaca que, en función de la normativa que sea de aplicación al sistema, el uso del servicio en modalidad nube pública podría no estar permitido y el uso de *WildFire* se limitaría al despliegue en modalidad de nube privada (WF-500).

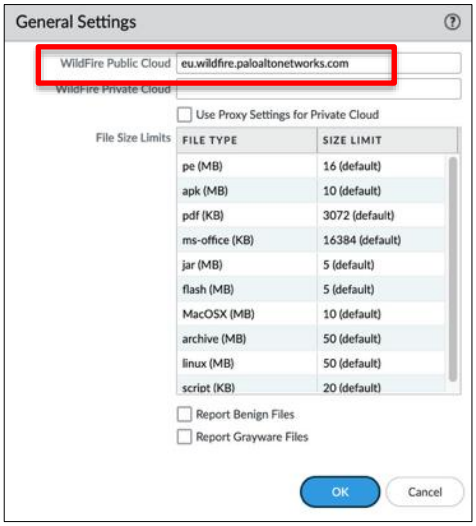


Figura 5-150: Configuración de Wildfire europeo

2. Incrementar el tamaño de archivo en *Wildfire*

472. **Ubicación:** "*Device > Setup > Wildfire > General Settings*"

473. **Recomendación:** Se recomienda incrementar los tamaños de archivo que *WildFire* inspecciona, hasta el máximo para cada tipo. En caso de clientes que no cuenten con la suscripción de *WildFire*, el sistema solo enviará automáticamente los archivos de tipo PE.

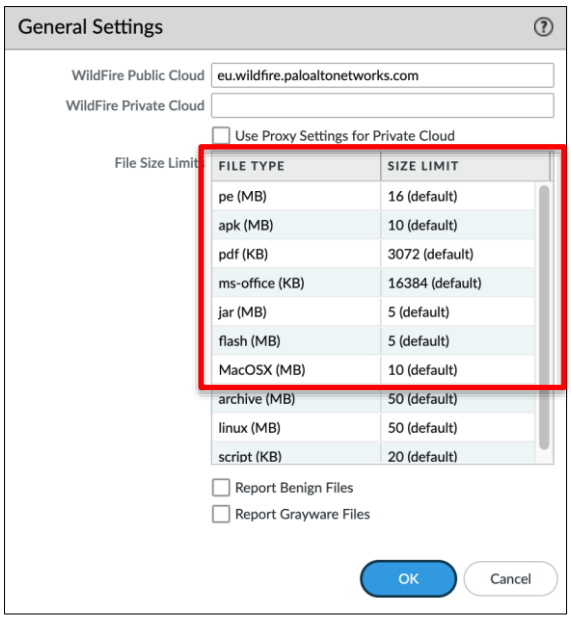


Figura 5-151: Configuración tamaño máximo de ficheros inspeccionados WildFire

3. Envío de la información de sesión a *Wildfire*

474. **Ubicación:** "*Device > Setup > Wildfire > Session Information Settings*"

475. **Recomendación:** Se recomienda activar el envío de toda la información de la sesión, para obtener *reports* con información más detallada y precisa, y minimizar el tiempo necesario para identificar a una estación que pueda estar potencialmente infectada.

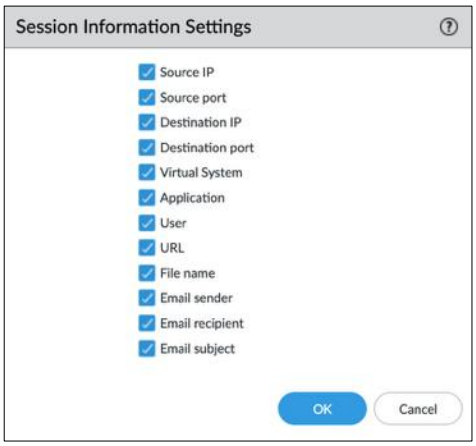


Figura 5-152: Configuración de información de sesión enviada a WildFire

4. Configurar *Forwarding* para el tráfico SSL descifrado

476. **Ubicación:** "*Device > Setup > Content-ID > Content-ID Settings*"

477. **Recomendación:** Se recomienda activar este flag para permitir que el sistema envíe a *WildFire*, también los archivos que se reciben vía SSL/TLS. Es importante tener en cuenta que para que esta configuración se aplique es necesario contar, además, con una política de descifrado SSL/TLS en salida, que se describe posteriormente.

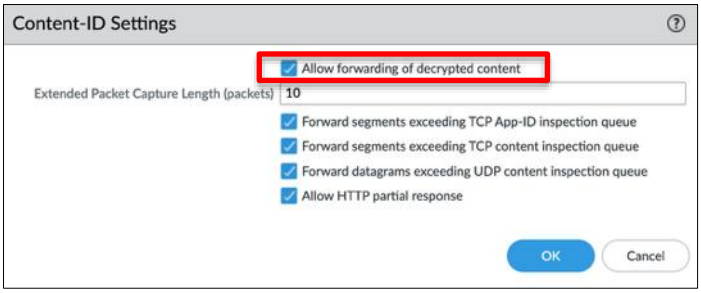


Figura 5-153: Forwarding of Decrypted Content

5. Configurar perfil de *Wildfire* analysis para todos los ficheros

478. **Ubicación:** "*Objects > Security Profiles > WildFire Analysis*"

479. **Recomendación:** Se recomienda configurar un perfil en el que se envíen todos los ficheros para su análisis en *WildFire*. Si se dispone de una nube privada, WF-500, la recomendación es enviar los ficheros más sensibles a la nube privada.

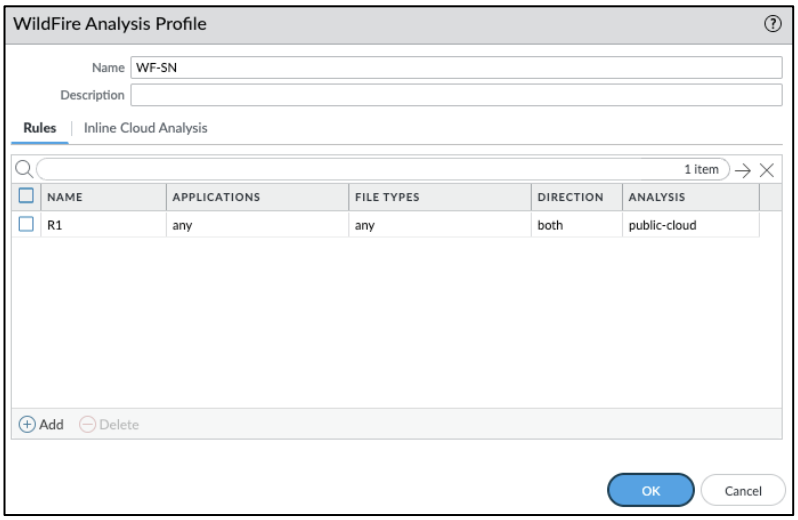


Figura 5-154: Perfil de WildFire Analysis recomendado

6. Configurar perfil de antivirus

480. **Ubicación**: "*Objects > Security Profiles > Antivirus*"

481. **Recomendación:** Clonar el perfil de Antivirus por defecto y modificarlo como se muestra para aplicarlo a todas las políticas de seguridad que permiten tráfico. La recomendación es configurar "*reset-both*" para los siete protocol decoders: FTP, HTTP, HTTP2, IMAP, POP3, SMB y SMTP), con la captura de paquetes activada. La columna *Signature Action* regula las firmas de la suscripción de Antivirus, *WildFire Signature Action*, regula las firmas que se reciben a través de la suscripción de *WildFire*, *Wildfire Inline ML Action* actúa sobre el motor de aprendizaje automático.

Nota: Esta configuración ya se realizó anteriormente en el módulo de Antivirus y no es necesario repetirla aquí, por tanto. Aparece nuevamente en este punto, solamente para recordar que la configuración de las firmas de *WildFire* se realiza dentro del módulo de Antivirus.

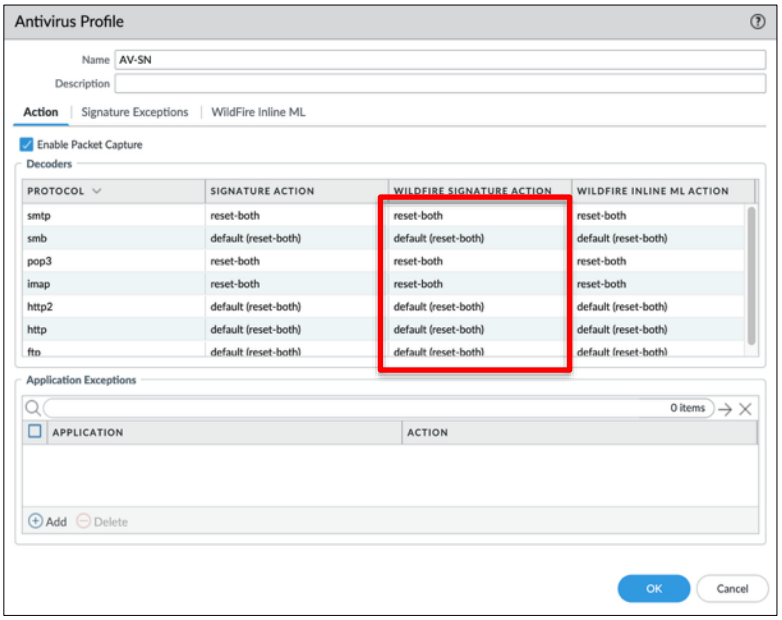


Figura 5-155: Perfil de Antivirus recomendado

7. Utilizar *Wildfire analysis* y antivirus en todas las reglas que permitan tráfico

482. **Ubicación:** "*Policies > Security*"

483. **Recomendación:** Se recomienda aplicar los perfiles de *WildFire Analysis* y Antivirus configurados antes, en todas las reglas de seguridad que permitan el tráfico.

8. Verificar que el servicio de Wildfire funciona

484. **Ubicación**: "*CLI*"; "*Monitor > Logs > WildFire Submissions*"

485. **Recomendación:** Una vez que la configuración de *WildFire* ha sido completada, se recomienda verificar que el sistema puede comunicarse adecuadamente con la nube. Para ello, y vía CLI, se puede ejecutar el comando "*test wildfire registration*", que debe mostrar una salida similar a la indicada a continuación:

```
admin@PA-440> test wildfire registration channel public
This test may take a few minutes to finish. Do you want to continue? (y or n)

WildFire registration for Public Cloud is triggered

WildFire Public Cloud:
  Server address:                 eu.wildfire.paloaltonetworks.com
  Best server:                    eu.wildfire.paloaltonetworks.com
  Device registered:              yes
  Through a proxy:                no
  Valid wildfire license:         yes
  Service route IP address:       192.168.1.254
  Global status:                  Idle
  Count of available workers:     20
  Available worker indices:       0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
  Upload status Usage: 'I': Idle, 'U': Uploading, 'Q': Querying
    Upload worker index:           0   1   2   3   4   5   6   7   8   9
    Upload status:                 I   I   I   I   I   I   I   I   I   I
    Status time (seconds):         4   4   4   4   4   4   4   4   4   4
    Upload worker index:           10  11  12  13  14  15  16  17  18  19
    Upload status:                 I   I   I   I   I   I   I   I   I   I
    Status time (seconds):         4   4   4   4   4   4   4   4   4   4


admin@PA-440>
```

486. Opcionalmente, también se puede descargar un archivo de *test* que Palo Alto Networks ofrece, desde *http://wildfire.paloaltonetworks.com/publicapi/test/pe*. Una vez que la descarga y el análisis se haya producido, se reciben los logs correspondientes dentro *de "Monitor > Logs > Submissions"* tal y como se muestran posteriormente.

5.11.11.3 EJEMPLO DE USO

487. En el ejemplo, se habilita el envío de ficheros a la nube pública de *WildFire* en ambas direcciones para todas las comunicaciones entre los usuarios e Internet, dado que no suele ser problemático el envío a la nube pública de ficheros con origen o destino público. Además, toda la comunicación entre los usuarios y el *datacenter*, será enviada a la nube privada de *WildFire* (WF-500). Finalmente, todo el tráfico entrante hacia el *relay* de correo de la DMZ, también será inspeccionado.

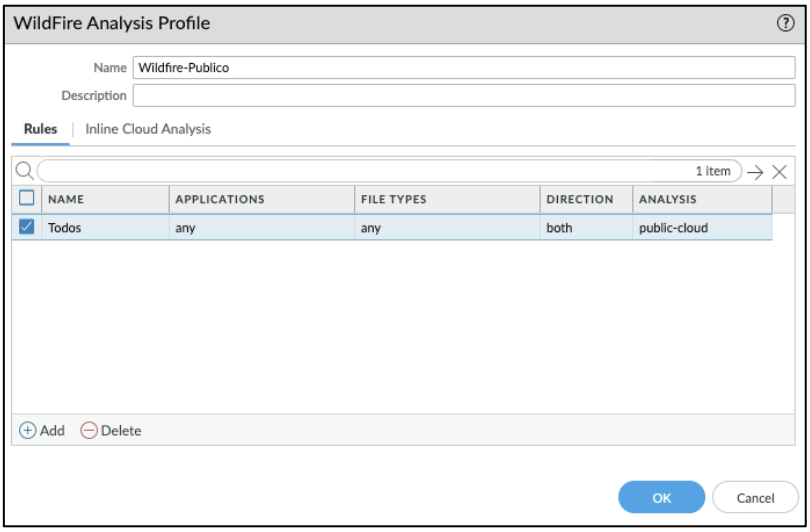


Figura 5-156: Configuración del perfil público de WildFire

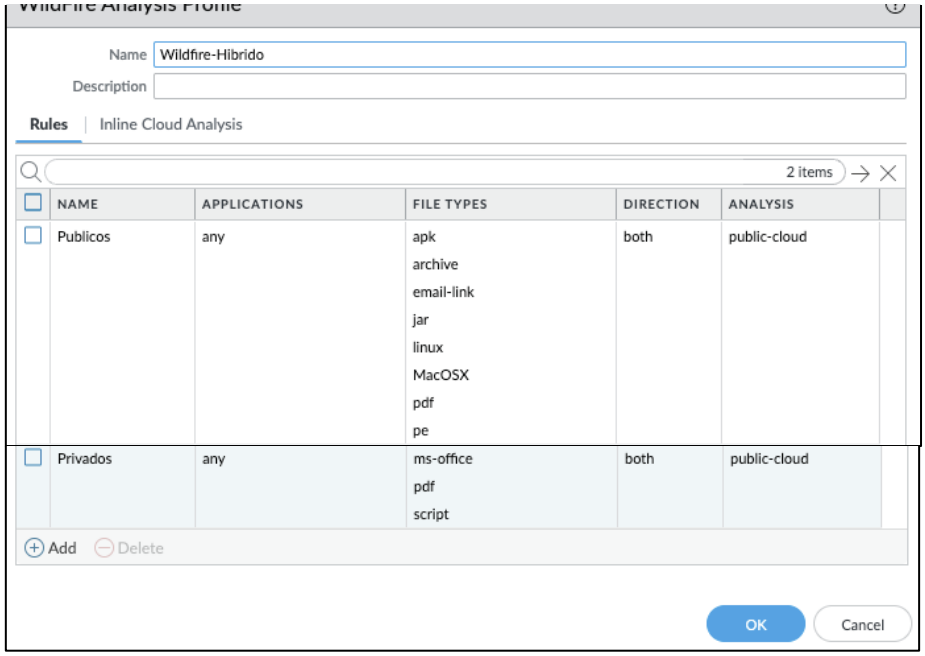


Figura 5-157: Configuración del perfil híbrido de WildFire

Figura 5-158: Aplicación de WildFire público en las reglas de seguridad a Internet

Figura 5-159: Aplicación de WildFire híbrido en las reglas de datacenter

488. También se aplicará el perfil público en las reglas relativas al correo electrónico, para que se inspeccionen, tanto los archivos adjuntos, como los enlaces de correo (archivos tipo *email-link*):

Figura 5-160: Aplicación de WildFire público en las reglas de correo electrónico

5.11.11.4 OBSERVABLES

Logs

489. Los detalles de las alertas de *WildFire* pueden consultarse en *Monitor > Logs > WildFire Submissions.* Se pueden registrar tanto los ficheros maliciosos (acción por defecto) como los ficheros benignos y los catalogados como "*grayware*". La vista detallada de un fichero particular también referenciará los logs asociados con esa entrada, y muestra el informe que *WildFire* ha generado en la pestaña *WildFire Analysis Report*:

	Receive Time	File Name	URL	Source Zone	Destination Zone	Attacker	Attacker Name	Victim	Desti... Port	Application	Rule	Verdict
	10/15 09:57:40	cwall.doc		Internet	LAN	74.112.185.96		192.168.3.25	59195	boxnet-base	LAN-Internet	malicious
	10/15 09:49:40	cwall.exe		Internet	LAN	74.112.185.96		192.168.3.25	59195	boxnet-base	LAN-Internet	malicious

Figura 5-161: Ejemplo de log de File Blocking

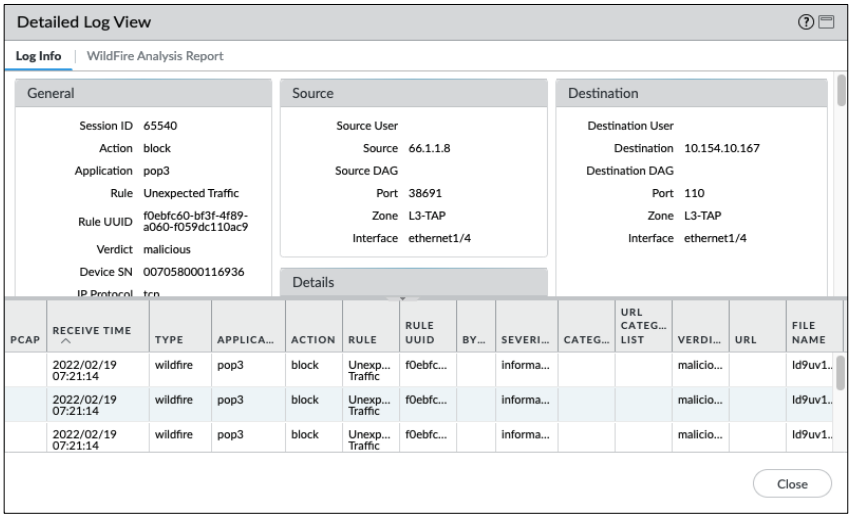


Figura 5-162: Ejemplo de log de WildFire detallado

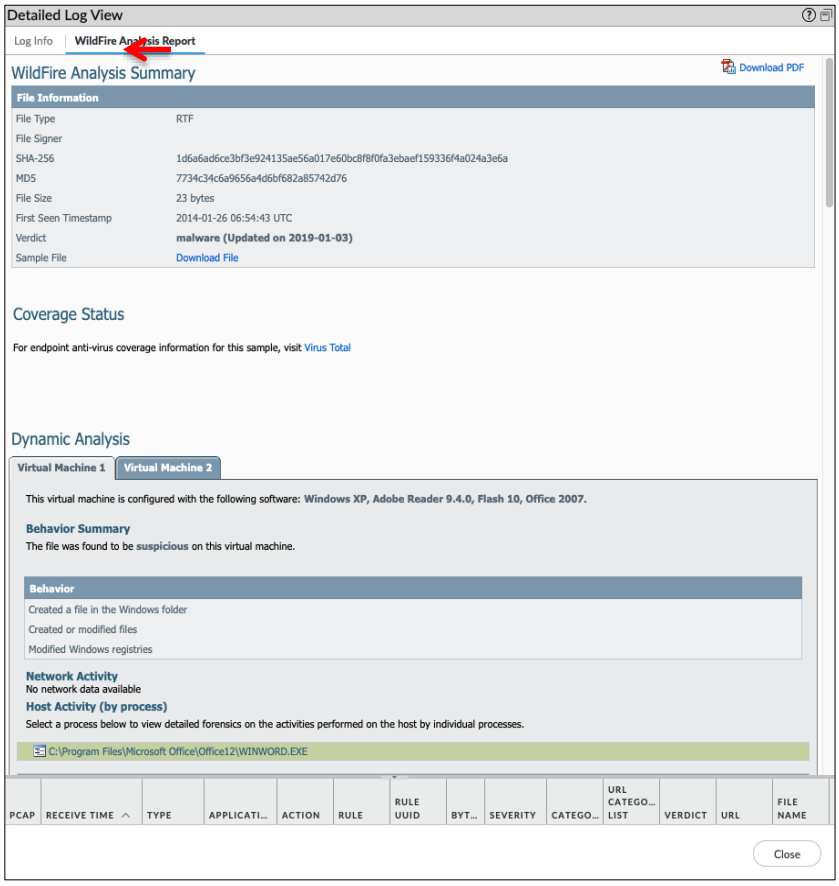


Figura 5-163: Ejemplo de informe de WildFire integrado en el cortafuegos

490. El informe de análisis de *WildFire* puede descargarse como fichero PDF desde esta vista, siendo también posible descargar el fichero original y un fichero pcap con el tráfico de red que la muestra genera, tal y como lo ve *WildFire*. Además, el informe incluye la información del análisis estático y dinámico para todos los entornos virtuales en los que la muestra ha sido ejecutada. Finalmente, el informe también incorpora un enlace para que se pueda reportar directamente un veredicto incorrecto al soporte de Palo Alto Networks.

Generación de firmas

491. Si se encuentra un fichero malicioso durante el análisis de *WildFire*, se generarán firmas de protección que estarán disponibles para todos los clientes con la suscripción de *WildFire* en la siguiente actualización dinámica. A fecha de escritura de este documento, las actualizaciones de las firmas de Antivirus de *WildFire* se distribuyen de manera global en tiempo real tan pronto como están disponibles los nuevos veredictos. Se recomienda configurar la comprobación de disponibilidad actualizaciones cada minuto.

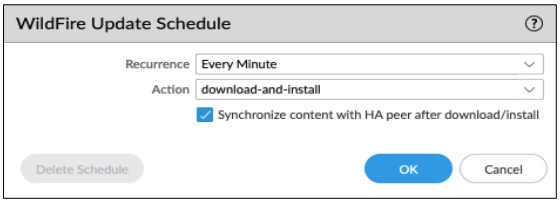


Figura 5-164: Actualizaciones de WildFire

492. Es importante señalar que las firmas de Palo Alto Networks se basan en el payload del fichero y no en su hash o nombre, lo que permite que una misma firma pueda detectar múltiples variantes polimórficas de una misma muestra.

493. Si un fichero es malicioso, y hay disponible una firma de *WildFire* ya instalada, el fichero puede ser bloqueado por la funcionalidad de Antivirus, y el cortafuegos generará una entrada de log de tipo *wildfire-virus* en el *Threat log*, tal y como muestra la siguiente imagen:

Figura 5-165: Ejemplo de log generado por una firma de WildFire

Notificación al usuario

494. Cuando un usuario intenta descargar un fichero a través de alguna aplicación de tipo web para el que existe una firma de *WildFire*, y la acción se configura como bloqueo, se le informa a través de una página en el navegador que es posible personalizar en "*Device > Response Pages*":

Figura 5-166: Ejemplo de página de bloqueo de WildFire

5.11.12 INSPECCIÓN SSL/TLS

495. Los cortafuegos de Palo Alto Networks ofrecen la posibilidad de descifrar y examinar el tráfico para ofrecer visibilidad, control y seguridad granular. El descifrado de un cortafuegos de Palo Alto Networks ofrece la capacidad de aplicar políticas de seguridad al tráfico cifrado, que de otra manera no podría bloquearse ni moldearse de acuerdo con los ajustes de seguridad que ha configurado. Se debe usar el descifrado del cortafuegos, para evitar que entre en la red contenido malicioso o que salga de ella contenido sensible no percibido como tal por estar cifrado.

496. El descifrado del cortafuegos de Palo Alto Networks se basa en políticas, y puede usarse para descifrar, examinar y controlar las conexiones SSL/TLS y SSH entrantes y salientes. Las políticas de descifrado le permiten especificar el tráfico que se desea descifrar en función de la categoría de URL, destino u origen, para poder bloquear o restringir el tráfico especificado según sus ajustes de seguridad. El cortafuegos usa certificados y claves para descifrar el tráfico especificado por la política, y después aplica App-ID y los ajustes de seguridad en el tráfico de descifrado. Entre los ajustes de seguridad sobre el tráfico descifrado se incluyen las funciones de Antivirus, *Vulnerability Protection, Antispyware*, Filtrado de URL y perfiles de bloqueo de archivos. Cuando el tráfico se haya descifrado y examinado en el cortafuegos, dicho tráfico se volverá a cifrar al salir del cortafuegos para asegurar su privacidad y confidencialidad.

497. Los cortafuegos de Palo Alto Networks ofrecen los siguientes tipos de descifrado:

- Descifrado SSL/TLS en salida (SSL *Forward Proxy*)
- Descifrado SSL/TLS en entrada (SSL *Inbound Inspection*)
- Descifrado SSH

Nota: Si se desea obtener más información sobre las capacidades y configuración del descifrado SSL visite: *https://docs.paloaltonetworks.com/network-security/decryption/administration/decryption-overview*

498. Los cortafuegos de Palo Alto Networks permiten descifrar, obtener visibilidad, e impedir amenazas conocidas como desconocidas sobre el protocolo TLSv1.3 y anteriores. TLSv1.3 es la última versión del protocolo TLS, que proporciona seguridad y mejoras en el rendimiento para aplicaciones. El soporte de TLSv1.3 permite el descifrado en todos modos: SSL Forward Proxy, SSL Inbound Inspection, SSL Decryption Broker, y SSL Decryption Port Mirroring incluyendo GlobalProtect Clientless VPN (navegador a portal de GlobalProtect).

499. Se pueden solucionar los problemas relacionados con el descifrado de SSL/TLS y evaluar la política de seguridad de manera sencilla con las funciones del Centro de comando de aplicaciones (ACC) y los registros de descifrado consolidados. Las nuevas funciones en ACC permiten identificar el tráfico con problemas en el descifrado, utilizar los nuevos registros de descifrado para profundizar en los detalles y resolver el problema. Con las nuevas funciones de ACC se identifica la cantidad de tráfico SSL/TLS, tráfico no SSL/TLS, tráfico descifrado y tráfico SSL/TLS no descifrado. Además, ACC identifica el tráfico que usa algoritmos y protocolos débiles para mitigar el riesgo asociado con aplicaciones, servidores y dispositivos que usan protocolos o algoritmos más antiguos e inseguros.

500. Los cortafuegos de Palo Alto Networks permiten bloquear la exportación de claves privadas cuando se generan en el propio cortafuegos o cuando se importan en el propio PAN-OS. El bloqueo de exportación de claves fortalece la política de seguridad porque impide que los administradores fraudulentos puedan realizar un mal uso de las claves. Se puede saber qué claves están bloqueadas y cuáles no. Sin embargo, un administrador con el role de Superusuario no puede exportar las claves privadas.

501. Asimismo, los cortafuegos de Palo Alto Networks se pueden integrar con dispositivos HSM (*Hardware Security Module*). Los clientes HSM integrados con los cortafuegos de Palo Alto Networks ofrecen mayor seguridad para las claves privadas utilizadas en el descifrado SSL/TLS (tanto en el modo *SSL Forward Proxy* como en *SSL Inbound Inspection*). Además, se puede usar el HSM para cifrar claves maestras.

5.11.12.1 REQUISITOS DE SEGURIDAD

502. Se debe configurar el descifrado SSL/TLS tanto en salida, para toda la navegación de usuarios con la excepción de algunas categorías de URL (SSL Forward Proxy), como en entrada para proteger los servicios que se prestan al exterior (SSL Inbound Inspection).

503. Opcionalmente, puede también establecer criterios para el control de los protocolos que se utilizan vía SSL/TLS, incluso para el tráfico que no descifre, con el fin de garantizar que no se utilizan protocolos obsoletos o inseguros en "*Objects > Decryption Profile*".

1. Configurar la inspección SSL en salida

504. **Ubicación**: "*Policies > Decryption*"

505. **Requisito de seguridad**: Se debe configurar el descifrado SSL/TLS en salida para toda la navegación excepto para las categorías URL que sean consideradas (en el ejemplo de la siguiente figura: *financial-services* y *health-and-medicine*).

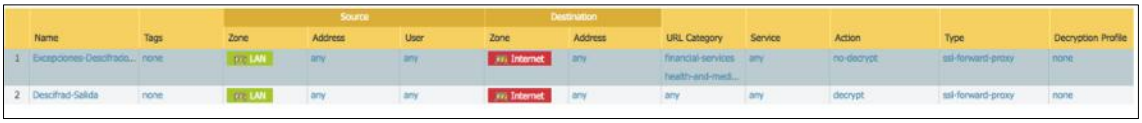


Figura 5-167: Política de SSL Forward Proxy

2. Configurar la inspección SSL en entrada

506. **Ubicación: "***Policies > Decryption*"

507. **Requisito de seguridad:** Se debe configurar el descifrado SSL/TLS en entrada para todo el tráfico de servicios que preste al exterior, típicamente aquellos ubicados en DMZs o Datacenter.

508. Se pueden configurar reglas de política de inspección de entrada SSL/TLS con hasta 12 certificados de servidor. Permite actualizar los certificados de los servidores protegidos sin que se produzca un tiempo de inactividad por descifrado. Se pueden configurar reglas para descifrar e inspeccionar el tráfico a servidores que alojan varios dominios, cada uno con un certificado diferente.

509. Para garantizar que siempre haya un certificado válido disponible, se importa el nuevo certificado y clave del servidor en su cortafuegos y se añade a su regla de política de descifrado antes de actualizar al servidor web. El NGFW utiliza el certificado de servidor antiguo pero válido como proxy de la conexión entre el cliente y el servidor interno para descifrar e inspeccionar el tráfico SSL/TLS entrante. Después de instalar el nuevo certificado en su servidor, el cortafuegos lo utilizará para las nuevas conexiones SSL/TLS siempre que el certificado de la regla de política de inspección entrante SSL/TLS coincida con el certificado del servidor. Si se produce una discrepancia en el certificado, la sesión finaliza y la entrada del registro de descifrado indica que el motivo de finalización de la sesión es una discrepancia entre el cortafuegos y el certificado del servidor.

510. En la pestaña "*Options*" en "*Type*" elegir "*SSL Inbound Inspection*" y bajo "*Certificates*" se añaden los certificados.

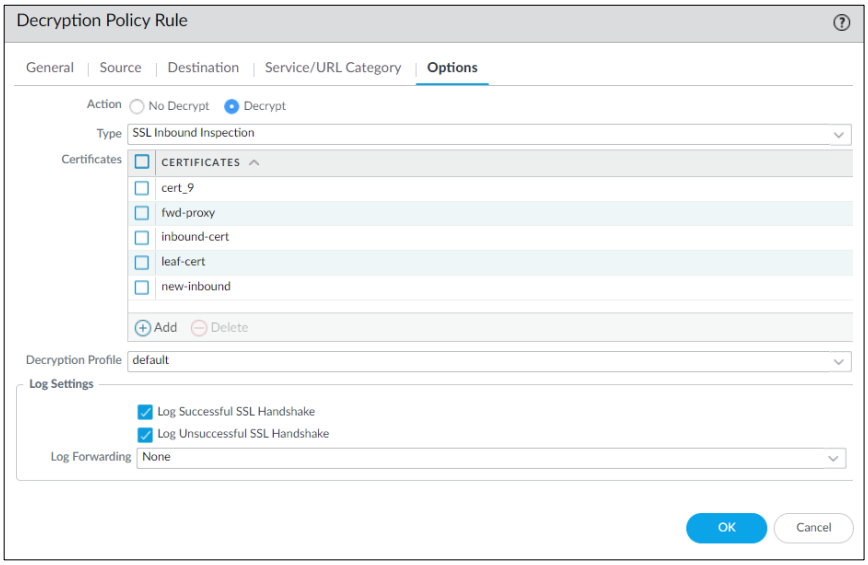


Figura 5-168: Selección de certificados para la inspección SSL entrante

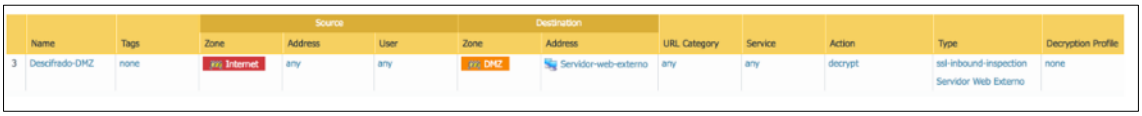


Figura 5-169: Política de SSL Inbound Inspection

5.11.12.2 OBSERVABLES

511. En todos los logs que se generan en el cortafuegos, se puede consultar si el tráfico ha sido descifrado. Para ello, se puede acceder al detalle de la sesión y se puede confirmar si el flag "*Decrypted*" está activado o no.

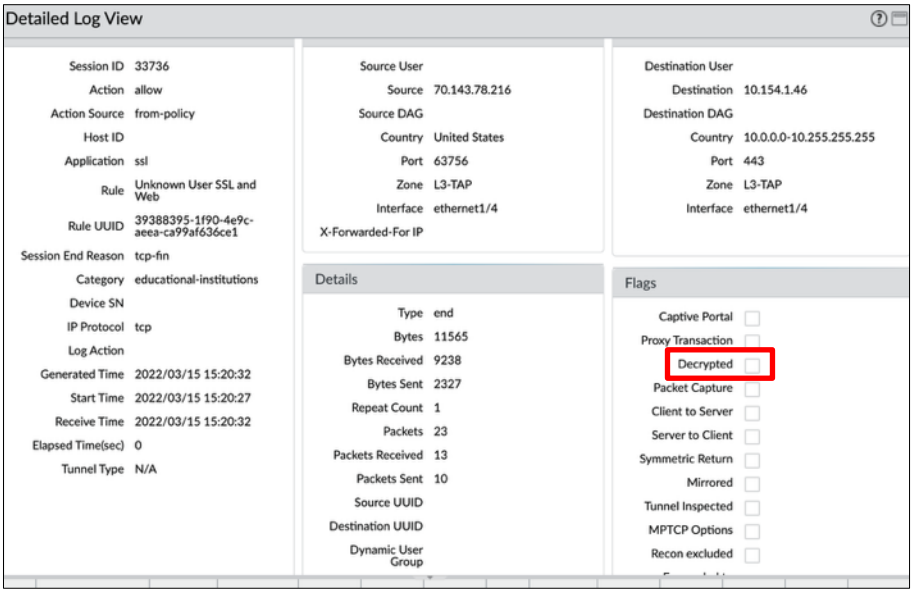


Figura 5-170: Detalle de logs

5.11.13 INSPECCIÓN DE CONTENIDO TUNELIZADO

512. El cortafuegos es capaz inspeccionar el contenido del tráfico tunelizado de los protocolos no cifrados:

- GRE (*Generic Routing Encapsulation* – RFC 2784)
- Tráfico IPSec no cifrado (*Null encryption Algorithm for IPSec-RFC-2410* y modo transporte AH IPsec)
- GTU-U (*GPRS Tunneling Protocol* for user data)
- VXLAN (*Virtual Extensible Local Area Network* - RFC 7348)

513. Se recomienda utilizar esta funcionalidad para reforzar la seguridad, protección frente a DoS y gestión de ancho de banda en estos tipos de túneles. Asimismo, con esta inspección sería posible tener visibilidad de la actividad de los túneles en los logs y en el Centro de Control de Aplicaciones (ACC) para verificar que este tráfico cumple con la normativa de seguridad corporativa.

514. Para poder inspeccionar el tráfico de los túneles indicados anteriormente, tan solo es necesario que el cortafuegos esté en el camino de dicho túnel. Dos casos de uso típicos serían:

- *Organizaciones que desean inspeccionar el tráfico de túneles GRE o IPSEC sin cifrado con objetivo de tener visibilidad del tráfico, aplicar QoS o crear informes de tráfico.*
- *Operadores que* usan GTP-U para enviar tunelizado el tráfico de datos de los dispositivos móviles.

515. La inspección de túneles está soportada si el cortafuegos está funcionando en modo nivel 3, nivel 2*, virtual wire* y TAP.

516. En la siguiente figura se muestran los dos niveles de inspección de túneles que el cortafuegos puede inspeccionar:

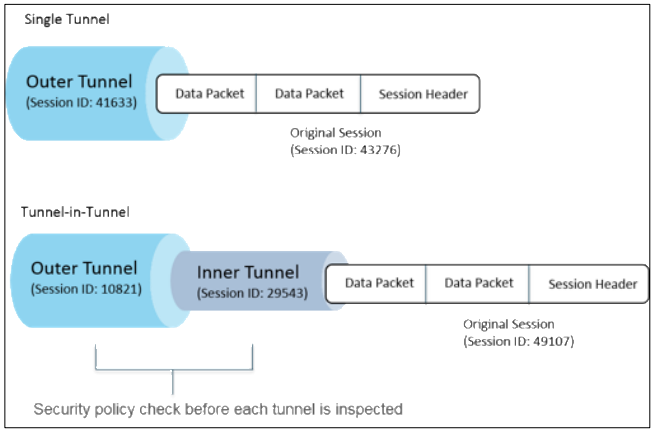


Figura 5-171: Esquema cabeceras Inspección de túneles

517. Las siguientes acciones se realizarían cuando se recibe un paquete en este escenario:

- El cortafuegos realiza un chequeo de la política de seguridad, para determinar si el protocolo túnel (en concreto, la aplicación) está permitido o denegado.

- Si la política de seguridad permite el tráfico, el cortafuegos selecciona una regla de política de inspección de túneles, en función de la zona origen/destino, IP origen/destino y usuario. La regla de política de inspección de túnel determina los protocolos de túnel que inspecciona el cortafuegos, el nivel máximo de encapsulación permitido (un solo túnel, o un túnel dentro de un túnel), y decide si permite los paquetes que contengan un protocolo de túnel que no pase una inspección de encabezado definida estrictamente por la RFC 2780, y si permite paquetes que contienen protocolos desconocidos.

- Si el tráfico pasa los chequeos de seguridad indicados, el cortafuegos inspecciona el contenido del túnel que está sujeto a la política de seguridad. Las políticas de seguridad soportadas para este tipo de tráfico se muestran en la siguiente tabla:

POLICY	OUTER TUNNEL SESSION	INNER TUNNEL SESSION	INSIDE ORIGINAL SESSION
App-Override	–	–	✓
DoS Protection	✓	✓	✓
NAT	✓	–	–
Policy-Based Forwarding (PBF) and Symmetric Return	✓	–	–
QoS	–	–	✓
Security (required)	✓	✓	✓
User-ID	✓	✓	✓
Zone Protection	✓	✓	✓

Figura 5-172: Políticas soportadas en tráfico tunelizado

518. Si el cortafuegos encuentra un segundo túnel, realiza las mismas acciones anteriormente indicadas de forma recursiva, para ver el contenido de este segundo nivel (para realizarlo sería necesario que la segunda regla de la política de inspección de túneles permitiera dos niveles de inspección para que se realice esta recursividad).

519. Por defecto, el contenido encapsulado en un túnel pertenece a la misma zona de seguridad que el túnel (por lo que aplica la misma política de seguridad que protege esa zona). Si se desea modificar esa zona de seguridad para el tráfico encapsulado se debe configurar *Tunnel Zone.*

Nota: Cuando se habilita o edita una política de inspección de túneles, el tráfico que la esté utilizando en ese momento se verá afectado, ya que las sesiones TCP internas al túnel se procesan como flujos *non-SYN TCP*. Si se desea modificar este comportamiento, se podría deshabilitar esta funcionalidad en la *Zone Protection*, en cuyo caso, si la zona está compartida con más servicios, se deshabilitaría para todos los servicios originados en esa zona.

520. Hay que destacar que, si el túnel se finaliza en el propio cortafuegos, no es necesario crear una política de inspección de túneles ya que, por defecto, una vez finalizado se tiene visibilidad completa de todo el tráfico.

Nota: Para más información sobre esta funcionalidad:

https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-networking-admin/tunnel-content-inspection/view-tunnel-information-in-logs

5.11.13.1 EJEMPLO DE USO

521. En el ejemplo, se configura la inspección del tráfico encapsulado en un túnel GRE:

522. **Ubicación**: "*Policies > Tunnel Inspection > Add*"

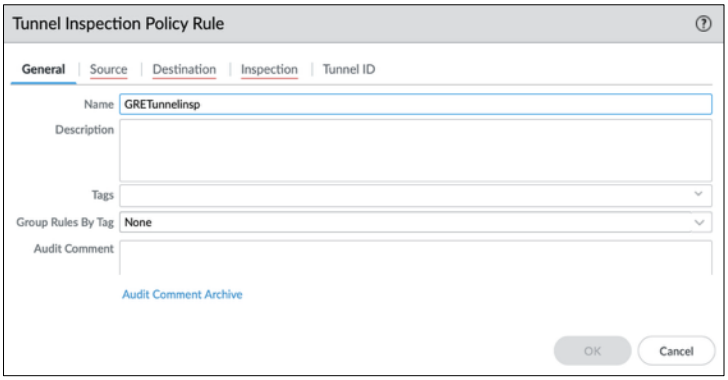


Figura 5-173: Configuración de regla de inspección de tráfico (General)

523. En la pestaña *Source* se indica la zona, dirección y usuario origen:

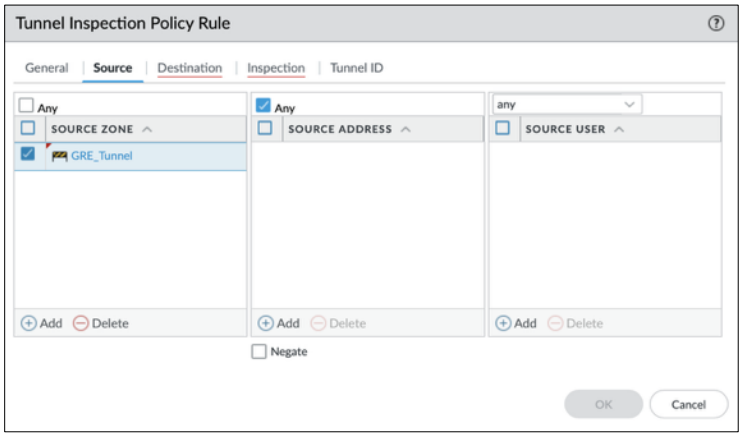


Figura 5-174: Configuración de regla de inspección de tráfico (Source)

524. En la pestaña *Destination* se indica la zona/dirección destino:

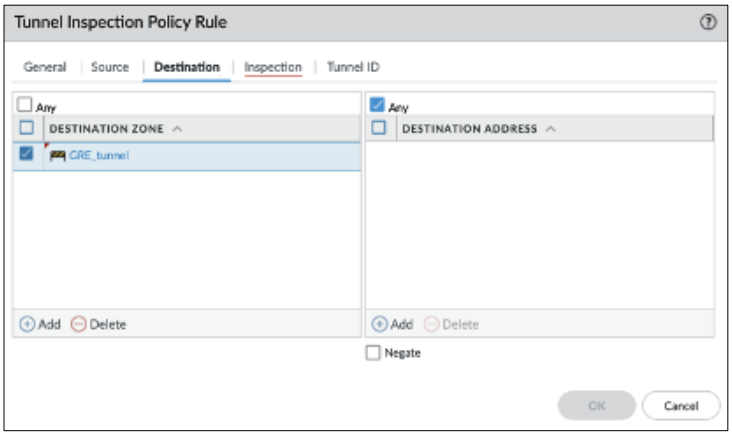


Figura 5-175: Configuración de regla de inspección de tráfico (Destination)

525. En la pestaña *Inspection* se indica el tipo de túnel, máximo número de niveles de inspección, dirección y usuario origen:

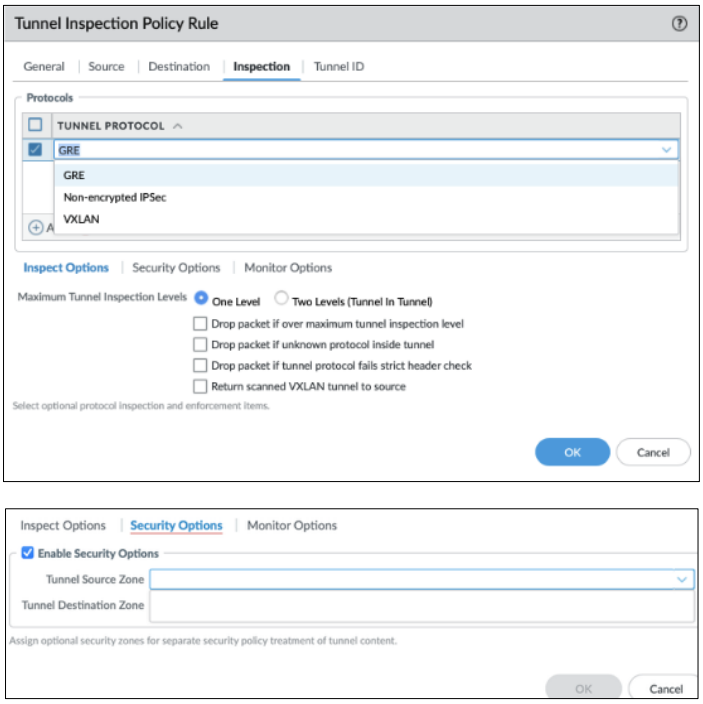


Figura 5-176: Configuración de regla de inspección de tráfico (Inspection)

526. **Recomendación:** Se recomienda configurar una zona específica para el tráfico tunelizado, con el objetivo de poder ajustar los parámetros especiales de *Zone Protection* sin afectar al resto de zonas. Asimismo, tener este tipo de tráfico en zonas independientes permite un reporting más sencillo.

5.11.13.2 OBSERVABLES

527. **Ubicación**: "*ACC > Virtual System/All > Tunnel Activity*"

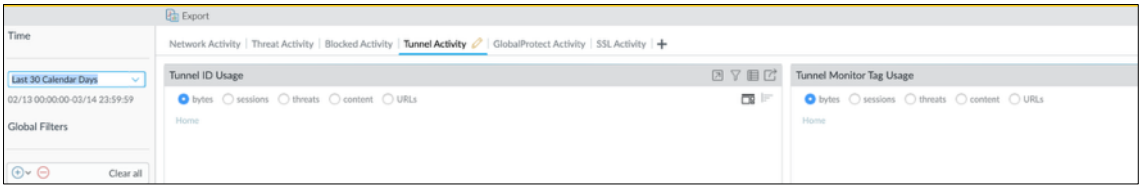


Figura 5-177: Monitorización de tráfico tunelizado

528. Adicionalmente, en los logs del cortafuegos se puede comprobar si el log en cuestión corresponde con un tráfico tunelizado (*detailed log view, Flag "Tunneled Inspected*"):

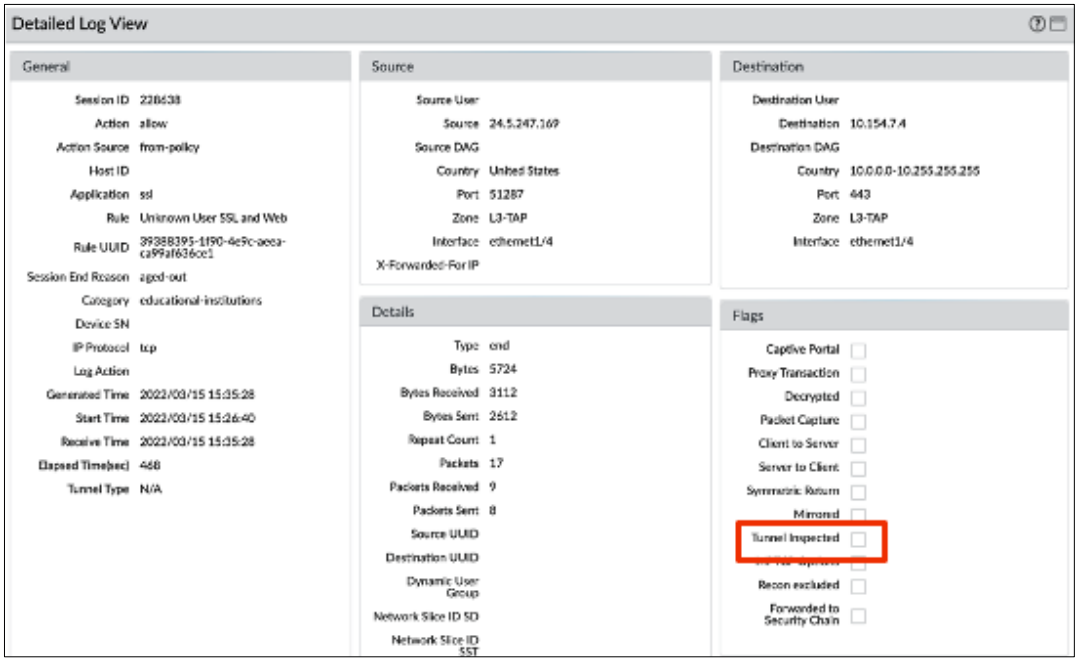


Figura 5-178: Vista de detalle de log (flag *Tunnel Inspected*)

5.11.14 MOTOR DE CORRELACIÓN AUTOMATIZADO

529. A partir de la versión 7.0 de PAN-OS, el motor de correlación automatizado es un mecanismo añadido a las capacidades de alerta y reporting de los cortafuegos de Palo Alto Networks y la consola Panorama. Es una herramienta de análisis que utiliza los logs del cortafuegos para detectar eventos especialmente importantes en la red. El motor correla una serie de eventos de amenazas relacionados que, cuando se combinan, indican con alta probabilidad que ha tenido lugar un ataque. Resalta los elementos más críticos, como por ejemplo los *hosts* comprometidos, permitiendo identificar el riesgo y tomar acciones para prevenir la explotación de los recursos de red. El motor utiliza objetos de correlación para analizar los logs en busca de patrones, de manera que cuando encuentra un *match*, genera un evento correlado. Esta funcionalidad está soportada en los siguientes modelos de NGFW:

- PA-3200 Series
- PA-3400 Series
- PA-5200 Series

- PA-5400 Series
- PA-7000 Series

Nota: Si se desea obtener más información sobre el motor de correlación automatizado, consultar el siguiente enlace: *https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-web-interface-help/monitor/monitor-automated-correlation-engine*

5.11.14.1 RECOMENDACIONES

530. El motor utiliza los Correlation Objects, estando todos ellos habilitados por defecto. Los Correlation Objects pueden revisarse, así como activarse/desactivarse a través de "Monitor > Automated Correlation Engine > Correlation Objects".

531. La recomendación es mantener todos activos y revisar los logs que se generan desde ellos, puesto que suelen confirmar que alguna estación se encuentra comprometida. Para ello, se recomienda incluir la revisión periódica de los logs de este módulo dentro de la política de operativa de la plataforma. Si se cuenta con un sistema de alarma, se aconseja asimismo configurarlo.

532. Respecto a su actualización, estos objetos se actualizan automáticamente a través de los *"content updates":*

TITLE	CATEGORY	STATE	DESCRIPTION
Multiple User from One Endpoint MFA Credential Theft	credential-theft-abuse	active	This correlation object detects multiple account abuse from a possibly compromised endpoint
WildFire C2	compromised-host	active	This correlation object detects hosts that have exhibited command-and-control (C2) network behavior corresponding to malware detected by WildFire elsewhere on your network.
WildFire and Traps ESM Correlated C2	compromised-host	active	This correlation object detects hosts that have received malware detected by WildFire or executed malware as seen by Traps, and have also exhibited command- and-control (C2) network behavior corresponding to the detected malware.
Single Account and Endpoint MFA Credential Theft	credential-theft-abuse	active	This correlation object detects activity from a possibly compromised user account from a single endpoint
Compromise Activity Sequence	compromised-host	active	This correlation object detects a host involved in a sequence of activity indicating remote compromise, starting with scanning or probing activity, progressing to exploitation, and concluding with network contact to a known malicious domain.
Exploit Kit Activity	compromised-host	active	This object detects probable exploit kit activity targeted at a host on the network. Exploit kits are identified by a vulnerability exploit or exploit kit landing page signature, combined with either a malware download signature or a known command-and-control signature.
Single Account 1 FA Multiple Endpoints Credential Timeouts	credential-theft-abuse	active	This correlation object detects timed out attempts of first factor authentications from multiple endpoints using a single user account
Beacon Detection	compromised-host	active	This correlation object detects likely compromised hosts based on activity that resembles command-and-control (C2) beaconing, such as repeated visits to recently registered domains or dynamic DNS domains, repeated file downloads from the same location, generation of unknown traffic, etc.
Single Account and Endpoint MFA Credential Timeout	credential-theft-abuse	active	This correlation object detects timedout MFA authentication attempts from a single endpoint using single account
Multiple Endpoint MFA Credential Timeout Abuse	credential-theft-abuse	active	This correlation object detects timed out second factor authentications from multiple endpoints using a single user account
Multiple Endpoint MFA Credential Abuse	credential-theft-abuse	active	This correlation object detects activity from multiple endpoints using a single user account
Exploit Kit Delivering XOR obfuscated malware	compromised-host	active	This correlation object detects exclusive-or (XOR) obfuscated malware downloaded to a host. XOR obfuscation is a technique to evade detection by encrypting portions of a file in order to hide malicious code. This correlation object specifically identifies XOR obfuscated malware that is delivered to the host by an exploit kit. While the Exploit Kit Activity object detects exploit kits combined with either a malware download signature or a known command-and-control signature, this object is provided to specifically detect an event where XOR obfuscation malware inserted on a host by an exploit kit and to distinguish such an event from other exploit kit activities.
Single Account 1 FA Credential Abuse	credential-theft-abuse	active	This correlation object detects timed out first factor authentications from an endpoint using a single user account

Figura 5-179: Correlation Objects predefinidos en el sistema

5.11.14.2 OBSERVABLES

533. Los logs generados pueden verse en *Monitor > Automated Correlation Engine > Correlated Events.* Si se hace click en la lupa se puede ver el detalle que generó la entrada:

	MATCH TIME	DYNAMIC ADDRESS GROUP	UPDATE TIME	OBJECT NAME	SOURCE ADDRESS	SOURCE USER	SEVERITY	SUMMARY
	2022/03/19 10:38:16		2022/03/19 10:38:16	Beacon Detection	10.154.9.207	pancademo\april...	medium	Host visited known malware URL (11 times).
	2022/03/18 17:05:11		2022/03/19 10:05:00	Beacon Detection	10.154.229.157	pancademo\ejoh...	medium	Host visited known malware URL (100 times).
	2022/03/18 17:16:20		2022/03/19 10:05:00	Beacon Detection	10.154.239.17	pancademo\pet...	medium	Host visited known malware URL (100 times).
	2022/03/18 17:13:44		2022/03/19 10:02:00	Beacon Detection	10.154.239.17	pancademo\pet...	medium	Host visited known malware URL (100 times).
	2022/03/18 17:03:14		2022/03/19 10:02:00	Beacon Detection	10.154.229.157	pancademo\ejoh...	medium	Host visited known malware URL (100 times).
	2022/03/18 17:05:32		2022/03/19 10:00:30	Beacon Detection	10.154.229.157	pancademo\ejoh...	medium	Host visited known malware URL (100 times).
	2022/03/18 17:12:12		2022/03/19 10:00:30	Beacon Detection	10.154.239.17	pancademo\pet...	medium	Host visited known malware URL (100 times).
	2022/03/18 19:34:05		2022/03/19 09:41:00	Beacon Detection	10.154.227.16	pancademo\rlam...	medium	Host visited known malware URL (100 times).
	2022/03/18 19:32:47		2022/03/19 09:39:30	Beacon Detection	10.154.227.16	pancademo\rlam...	medium	Host visited known malware URL (100 times).
	2022/03/18 19:31:59		2022/03/19 09:36:30	Beacon Detection	10.154.227.16	pancademo\rlam...	medium	Host visited known malware URL (100 times).
	2022/03/19 09:16:23		2022/03/19 09:16:23	Beacon Detection	10.154.228.67	pancademo\alan...	medium	Host visited known malware URL (12 times).
	2022/03/19 08:32:35		2022/03/19 08:32:35	Beacon Detection	10.154.14.123	pancademo\fran...	medium	Host visited known malware URL (12 times).
	2022/03/19 08:28:20		2022/03/19 08:28:20	Beacon Detection	10.154.9.151	pancademo\carl...	medium	Host visited known malware URL (13 times).
	2022/03/19 08:07:06		2022/03/19 08:07:06	Beacon Detection	10.154.10.176	pancademo\jose...	medium	Host visited known malware URL (12 times).
	2022/03/19 07:51:12		2022/03/19 07:51:12	Beacon Detection	10.154.9.207	pancademo\april...	medium	Host visited known malware URL (12 times).
	2022/03/19 07:17:47		2022/03/19 07:17:47	Beacon Detection	10.154.221.76	pancademo\stev...	medium	Host visited known malware URL (14 times).
	2022/03/19 07:15:55		2022/03/19 07:15:55	Beacon Detection	10.154.221.76	pancademo\stev...	medium	Host visited known malware URL (14 times).
	2022/03/19 07:14:22		2022/03/19 07:14:22	Beacon Detection	10.154.221.76	pancademo\stev...	medium	Host visited known malware URL (14 times).
	2022/03/19 07:12:09		2022/03/19 07:12:09	Beacon Detection	10.154.254.178	pancademo\dan...	medium	Host visited known malware URL (13 times).
	2022/03/19 07:10:05		2022/03/19 07:10:05	Beacon Detection	10.154.254.178	pancademo\dan...	medium	Host visited known malware URL (12 times).

Figura 5-180: Logs de ejemplo del motor automático de correlación

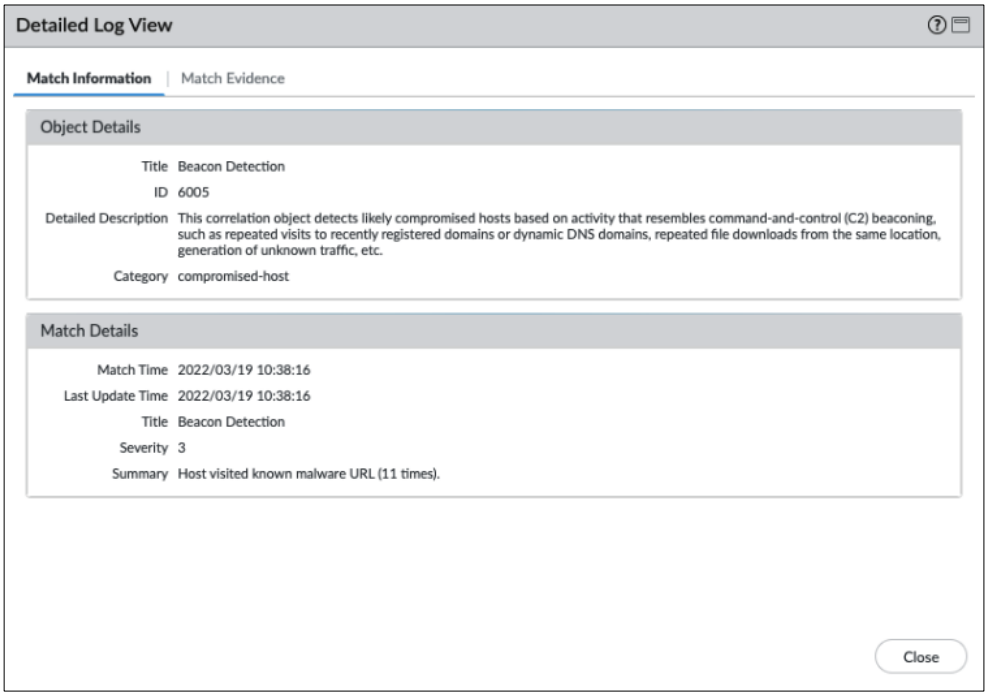


Figura 5-181: Logs de ejemplo del motor automático de correlación (detalle)

5.11.15 FIRMAS DE LOS MÓDULOS DE PREVENCIÓN

5.11.15.1 RENDIMIENTO Y NÚMERO DE FIRMAS

534. El rendimiento de los módulos de Advanced Threat Prevention no se ven impactados por el número de perfiles o firmas que se habilitan, gracias a la arquitectura Single Pass Parallel Processing (SP3). El contenido de cualquier sesión es inspeccionado en paralelo por el Antivirus, el Anti-Spyware y los perfiles de Vulnerability Protection. Así pues, la

recomendación es activar todas las firmas en los perfiles, sin preocuparse por el rendimiento.

535. Una configuración que sí tendrá impacto positivo en el rendimiento, es DSRI o Disable Server Response Inspection. Con DSRI habilitado, el tráfico de respuesta de los servidores no se inspecciona, lo que incrementará la capacidad de proceso. Por supuesto, esta funcionalidad solamente es recomendable si los servidores de destino son de confianza, por lo que normalmente solo se configura en las reglas que protegen los servidores que están bajo control y que, por tanto, son de confianza.

536. La siguiente figura muestra un ejemplo de configuración con DSRI habilitado para los servidores de una DMZ:

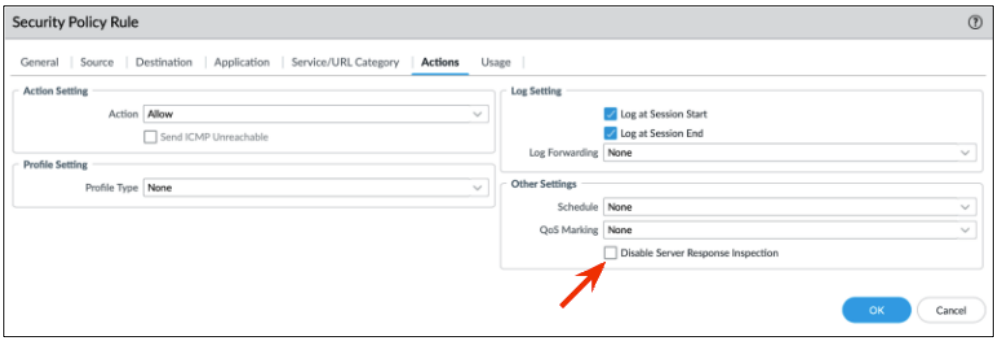


Figura 5-182: Ejemplo de activación de DSRI

5.11.15.2 ACCIÓN POR DEFECTO PARA LAS FIRMAS

537. Cada firma de amenaza presente en los perfiles de Anti-Spyware o Vulnerability Protection, tiene una acción por defecto asignada. Esta acción por defecto es la acción que se ejecutará, cuando se selecciona para el campo acción la opción default.

538. Con cada actualización de contenidos la acción por defecto de cada firma es configurada por los ingenieros de investigación de Palo Alto Networks, a su valor más recomendable, pudiendo evolucionar con el tiempo. Esta acción por defecto también puede ser modificada por los administradores, tal y como se ha detallado anteriormente.

539. A continuación, se listan las acciones disponibles que pueden aplicarse a los perfiles de *Anti-Spyware* y *Vulnerability Protection:*

- *Default*
- *Allow*
- *Alert*
- *Drop*
- *Reset-both*
- *Reset-client*
- *Reset-server*

- *Block-IP*

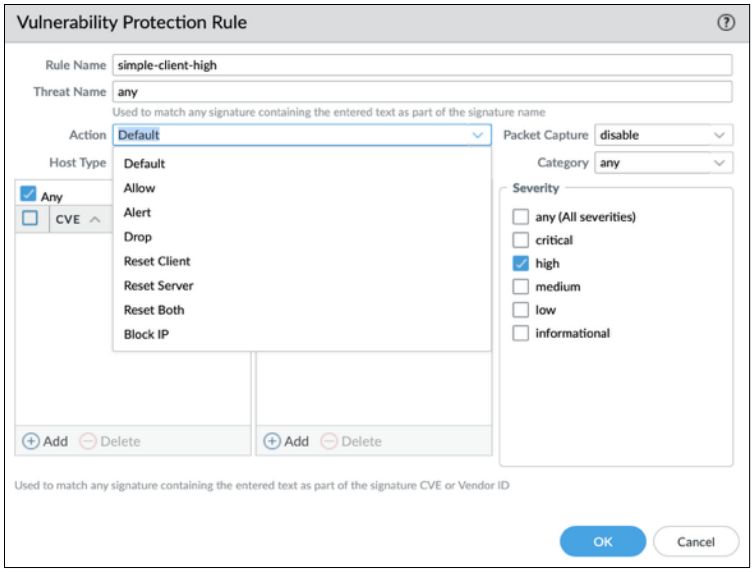


Figura 5-183: Acciones de las firmas de Anti-Spyware y Vulnerability Protection

540. Para los perfiles de Antivirus, la acción por defecto no se configura en base a las firmas, sino por protocolo. A continuación, se listan las acciones disponibles que pueden aplicarse a los protocolos para el Antivirus:

- *Allow*
- *Alert*
- *Drop*
- *Reset-client*
- *Reset-server*
- *Reset-both*

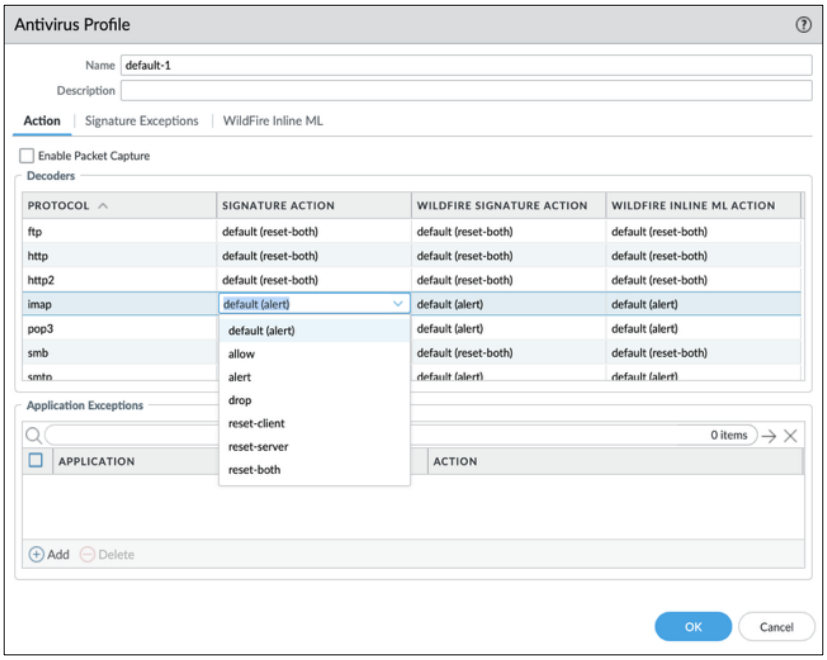


Figura 5-184: Acciones de las firmas de Antivirus

5.12 PREVENCIÓN Y DETECCIÓN DE ATAQUES

5.12.1 ATAQUES DOS

541. El módulo de DoS Protection es un complemento al de *Zone Protection*, y ofrece políticas de prevención de ataques DoS de red, destinadas a la protección de hosts específicos. En concreto, se ofrecen los siguientes mecanismos de prevención dentro de este módulo:

    - ***Flood Protection***. Detecta y previene los intentos de inundación con paquetes que típicamente terminan creando demasiadas sesiones a medio completar, o consumiendo todos los recursos de algún servicio concreto. En este tipo de ataque, la dirección IP origen suele estar "*spoofeada*" (es decir, falseada). Este mecanismo puede comenzar a bloquear paquetes en base a perfiles agregados o clasificados, tan pronto como los umbrales configurados se exceden.

    - ***Resources Protection***. Detecta y previene los intentos de consumir las sesiones de algún servicio. Este tipo de ataque se realiza normalmente utilizando una gran cantidad de hosts origen (denominados *bots*) para crear tantas sesiones completas como sea posible. Es más complicado de detectar que el anterior, porque las sesiones pueden utilizarse para enviar tráfico que parezca legítimo a los *hosts* objetivo. El módulo puede limitar la cantidad de sesiones disponibles, de nuevo en base a un perfil agregado o clasificado.

542. Es importante señalar que es posible emplear ambos mecanismos en el mismo perfil de DoS.

5.12.1.1 COMBATIENDO LA CADENA DE CIBERATAQUE

	Entrega	Explotación	Instalación	Mando y Control	Acciones en el Objetivo
DoS/Zone Protection		Prevenir las evasiones L3/L4			Prevenir los ataques DoS y el movimiento lateral

Tabla 15: Cadena de ciberataque - DoS/Zone Protection

543. Aunque el DoS Protection no ofrece ningún mecanismo como tal para romper la cadena de ciberataque, puede ser de ayuda reduciendo el impacto de cualquier acción destinada a impactar a los servicios públicos o privados de la organización, a través del consumo de los recursos legítimos.

5.12.1.2 RECOMENDACIONES

544. La definición de los perfiles de protección DoS Protection, depende en gran medida de qué tipo de servicios se quiere proteger, y los usuarios que lo utilizarán. Puesto que cada entorno es diferente es necesario, en general, hacer un análisis previo, al igual que ocurría con Zone Protection.

545. Independientemente del entorno, es importante poner especial atención a los siguientes factores:

- Valores por defecto
- Ratio Máximo
- Perfiles Agregados vs Clasificados
- SYN-cookie vs Random Early Drop Default threshold values.

1. Valores por defecto

546. Los valores por defecto no representan valores que se deban considerar como buenas prácticas. Los umbrales deben ser configurados en base a la información real de sesiones, para el entorno en cuestión en el que se desean aplicar. Un mecanismo adecuado para obtener esta información, es configurar el *reporting* a través de *Netflow* en el cortafuegos y enviarlo a un analizador que lo interprete.

Nota: Para obtener información detallada sobre cómo configurar *Netflow* en los cortafuegos de Palo Alto Networks consultar:
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/monitoring/netflow-monitoring

547. Las siguientes figuras muestran un ejemplo de protección con los valores por defecto:

548. **Ubicación**: "*Objects > Security Profiles > DoS Protection*"

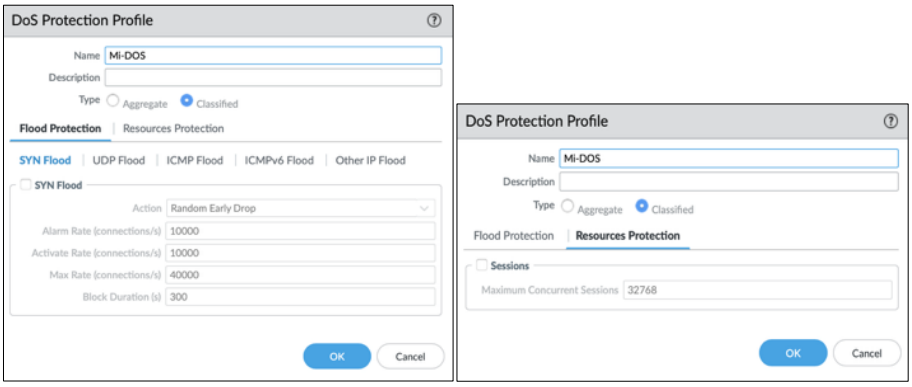


Figura 5-185: Configuración por defecto perfil de protección DoS

2. Ratios Máximos

549. Cuando se exceden los umbrales establecidos en los "*Maximal Rate*", cualquier paquete que haga *match* con la política de protección de DoS y el criterio de clasificación, si se utiliza un perfil de tipo "*Classified*", será descartado. El valor por defecto para *SYN-cookie* es 1.000.000, lo que hará que, en la mayoría de los entornos, no se dispare y, por tanto, es necesario ajustar los valores adecuados para los siguientes escenarios:

- Para ofrecer protección frente a inundaciones de tipo *TCP SYN*, cuando se utiliza como mecanismo de defensa RED (*Random Early Drop*).

- Para ofrecer protección frente a inundaciones de tipo UDP, ICMP u otras.

Nota: Cuando se utiliza *SYN* Cookies como mecanismo de prevención frente a ataques de tipo *SYN Flood*, en lugar de *RED*, el mecanismo ya ofrece protección en sí mismo y por ese motivo el valor "*Maximal Rate*" no ofrece protección adicional a ningún servicio, excepto al propio servicio de SYN-Cookie del cortafuegos.

3. Perfiles agregados vs clasificados

550. Cuando se configuran los umbrales DoS para *Flood Protection* y *Resource Protection*, es importante comprender la diferencia entre perfiles de tipo agregado y clasificado:

- **Agregado**: Los umbrales DoS definidos en el perfil, se aplican a todos los paquetes que hagan *match* con el criterio definido en la regla DoS en cuestión. Por ejemplo, una regla agregada con una protección frente a *floods* UDP de 10000 paquetes por segundo (pps), cuenta todos los paquetes que hagan *match* con esa regla particular.

- **Clasificado**: Los umbrales DoS definidos en el perfil, se aplican a todos los paquetes que hagan *match* con la regla y también con el criterio de clasificación, que puede ser "*source IP*", "*destination IP*" o "*source-and-destination IP*". Por ejemplo, una regla clasificada con una protección frente a floods UDP de 10000 pps y un criterio de clasificación de tipo "*source-ip*", comienza a descartar paquetes cuando una IP origen en concreto alcanza ese umbral, y solamente descartará paquetes para ese origen.

551. A partir de estas definiciones se puede inferir que los perfiles agregados son la mejor opción para protegerse frente ataques que vengan desde Internet. Un perfil clasificado

para Internet es menos apropiado, porque puede haber múltiples clientes detrás una dirección de NAT, y porque además es posible saturar la tabla de sesiones dada la cantidad potencial diferente de direcciones IPv4 e IPv6. Por el contrario, para clientes internos que no estén detrás de una IP de NAT, una clasificación basada en *"source-ip"* es probablemente la mejor opción para controlar el uso de los recursos. Por ejemplo, en los entornos educativos, donde los usuarios internos pueden en muchas ocasiones utilizar cualquier *software*, como p2p que consume muchos recursos, se puede utilizar un perfil clasificado para limitar el número de sesiones concurrentes por cliente y prevenir la saturación.

4. SYN-cookie vs Random Early Drop

552. El mecanismo de SYN-cookie es superior para contrarrestar los ataques de tipo SYN flood y, por tanto, es preferible frente a Random Early Drop.

553. Para cualquier otro tipo de inundación, Random Early Drop es la única opción. Este algoritmo comienza a descartar paquetes de manera aleatoria si la ratio de paquetes por segundo se encuentra entre los valores "Activate Rate" y "Maximal Rate". La probabilidad de descarte se incrementa linealmente con la ratio de paquetes. Si la ratio de paquetes excede el "Maximal Rate", entonces todos los paquetes en exceso son descartados.

554. Cuando se usan *SYN Cookies*, y desde la versión de PAN-OS 4.0 y posteriores, la ratio de activación, "*Activate Rate*", se configura por defecto a "0" porque el mecanismo es determinista y, por tanto, no introduce falsos positivos.

5.12.1.3 EJEMPLO DE USO

555. En el ejemplo se va a suponer que se tiene un servidor web en una DMZ para el que configuraremos un perfil de DoS, que proteja el servidor frente a ataques de tipo SYN *Flood*, y también frente al uso excesivo de sesiones.

Perfil de DoS Protection

556. Para la protección frente a ataques de tipo SYN Flood, se recomienda utilizar el mecanismo de SYN-*Cookies*, mejor que el de *Random Early Drop*, ya que ofrece mejor cobertura. Para evitar el abuso de las sesiones, deben considerarse las ventajas y desventajas de las siguientes técnicas, y elegir la más apropiada o una combinación de varias:

- Usar un perfil clasificado que limite las conexiones concurrentes usando como clasificador *"source-destination-ip"*. Esta medida reducirá el impacto que puede crear el ataque desde una *botnet* y mantendrá el servicio disponible para los usuarios legítimos. Si el límite es demasiado bajo puede afectar a los clientes que accedan al servicio web detrás de una IP de NAT. Si por el contrario es muy alto, es fácil para una botnet poder llegar a consumir todas las sesiones disponibles.

- Usar un perfil agregado en combinación con información de IP geolocalizada en la regla de protección DoS. Un perfil agregado en sí mismo no es suficiente para prevenir un ataque que agote las sesiones, pero combinado con información geo-IP puede reducir el impacto de un ataque DDoS global. Esta aproximación es válida si la audiencia del servicio web reside en un conjunto determinado de países.

- Usar un perfil clasificado incluyendo límite de sesiones concurrentes usando como criterio *"source-destination-ip"* junto con datos de localización geo-IP. Esta aproximación requerirá algún tiempo de ajuste, pero puede ser muy efectiva una vez implantada.

Reglas de *DoS Protection*

557. Una vez que los perfiles de protección DoS necesarios han sido definidos, hay que configurarlos sobre una o varias reglas de protección DoS para activarlos. Las reglas DoS definen los parámetros de origen y destino sobre los que el perfil se aplicará. Es recomendable intentar que las reglas sean lo más específicas posibles. En este ejemplo particular, se definirá una regla para cada servicio a proteger. De esta manera, los umbrales aplicarán solamente al servidor definido en la regla y no a los demás. La siguiente figura muestra un ejemplo de regla de DoS en combinación con información geo-IP. En concreto, se trata de un perfil clasificado por dirección IP origen y destino, que se aplica para todos aquellos orígenes que no vengan desde IPs españolas:

Figura 5-186: Ejemplo de política DoS

5.12.1.4 OBSERVABLES

Flood Protection

558. Cuando se dispara el mecanismo, se envían los logs de alerta al log de amenazas (Threat Log). Los logs mostrarán entradas diferentes para el origen y destino del ataque, en función del tipo de protección configurada. Así, cuando se utilizan perfiles agregados, tanto el origen como el destino mostrarán la dirección 0.0.0.0 y no se ofrece información de zona. Cuando, por el contrario, se utilizan perfiles clasificados, el log mostrará la información de origen y destino siempre y cuando forme parte del criterio de clasificación. El puerto de destino siempre se muestra como "0".

559. En la siguiente imagen se puede ver un log de cada tipo. El primero es de un perfil agregado, mientras que el segundo es de un perfil clasificado por origen y, como tal, en el log se muestra la IP origen que creó la entrada:

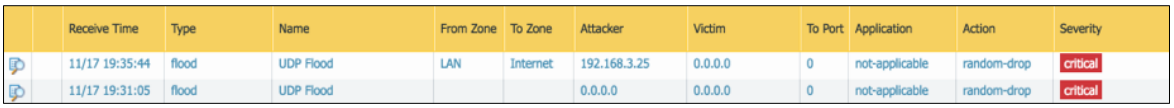


Figura 5-187: Ejemplo de logs de Flood Protection

Resource Protection

560. Cuando se dispara el mecanismo, se envían los logs de alerta al log de amenazas (*Threat Log*) generándose un log de nombre "*Session Limit Event*". Los logs mostrarán entradas diferentes para el origen y destino del ataque en función del tipo de protección configurada, siguiendo la misma lógica descrita en el punto anterior.

Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	Severity
11/17 19:42:33	flood	Session Limit Event			192.168.3.25	0.0.0.0	0	not-applicable	drop	critical

Figura 5-188: Ejemplo de log de Resource Protection

561. Es importante tener en cuenta que los equipos de Palo Alto Networks agrupan por defecto los logs que son idénticos cada 5 segundos, con el fin de evitar inundar el sistema de *logging*. No obstante, almacenan en un campo del log extendido, denominado "*Repeat Count*", el volumen total de eventos recibidos para esa entrada, tal y como puede verse en la siguiente imagen:

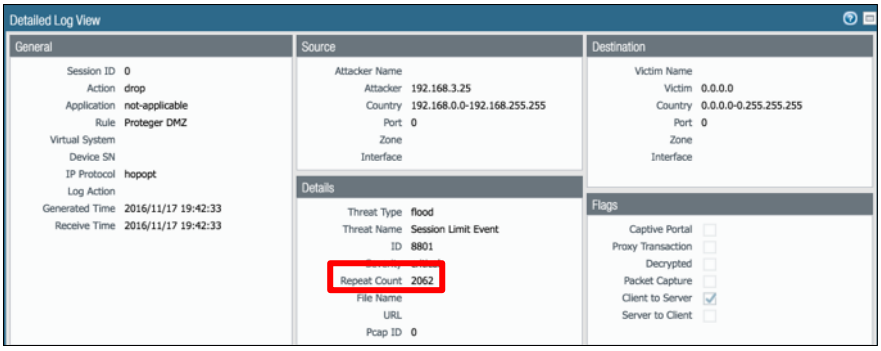


Figura 5-189: Ejemplo log número de eventos totales agregados

Nota: Las buenas prácticas para la configuración del DoS se encuentran en el siguiente enlace: *https://docs.paloaltonetworks.com/best-practices/dos-and-zone-protection-best-practices/dos-and-zone-protection-best-practices/deploy-dos-and-zone-protection-using-best-practices*

5.12.2 INFORME DE COMPORTAMIENTO DE *BOTNET*

562. El informe de comportamiento de *botnets*, automatiza el proceso de identificar y correlar aquellos comportamientos que indican la presencia probable de un *bot*, de modo similar a como se realiza un análisis de reputación. Para ello, este sistema de análisis busca diferentes características o patrones de comportamiento en los logs de las últimas 24 horas, según se resumen a continuación:

- Tráfico TCP/UDP desconocido
- Existencia de DNS dinámico
- Actividad sobre sitios de malware conocidos
- Visitas a dominios de reciente registro
- Navegación por direcciones IP en vez de URLs
- Descarga de ejecutables desde sites desconocidos
- Tráfico IRC

5.12.2.1 RECOMENDACIONES

563. El *report* de comportamiento de *botnets* está habilitado por defecto. Se ejecuta todos los días, y genera un informe con los *hosts* sospechosos del día anterior. Se recomienda incluir

la revisión diaria de los logs de este módulo dentro de la política de operativa de la plataforma.

564. Es posible personalizar el módulo para adecuarlo a las características de cada entorno tal y como muestra la siguiente imagen:

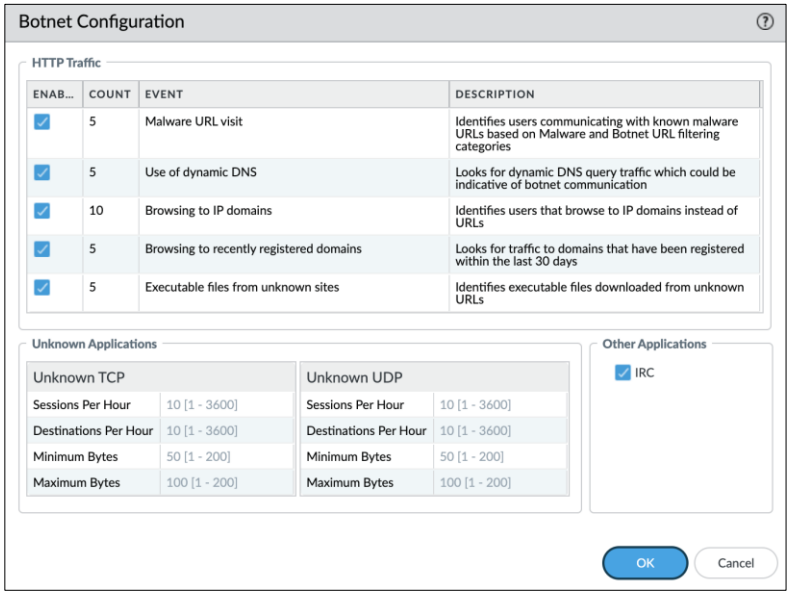


Figura 5-190: Personalización del *Behavioral Botnet Report*

5.12.2.2 OBSERVABLES

565. Cada día se genera un informe con la actividad y *hosts* sospechosos del día anterior, que incluye un grado de confianza para indicar la probabilidad de infección, siendo 5 el mayor grado de confianza de que el host tiene problemas y 1 el menor:

	Confidence	Source Address	Source User	Description
1	5	10.154.10.58	pancademo\marsha.wirth	Downloads executable(s) from malicious URL colombiantravelservices.com/fei6 . Repeatedly visited (8) the same malicious URL networksecurityx.hopto.org/ . IRC traffic
2	4	10.154.131.240	pancademo\clint.hill	Repeatedly visited (21) the same malicious URL antonello.messina.it/4GBrdf6
3	4	172.16.33.231	pancademo\alex.bell	Repeatedly visited (22) the same malicious URL antonello.messina.it/4GBrdf6
4	2	10.154.1.108	pancademo\robert.loomis	Repeatedly visited (85) the same URL 94.158.198.142/
5	2	10.154.5.33	pancademo\jason.gaughan	Repeatedly visited (82) the same URL 208.76.71.252/
6	2	10.154.14.176	pancademo\justin.pugh	Repeatedly visited (85) the same URL 198.173.5.23/
7	2	10.154.1.223	pancademo\eddie.brand	Repeatedly visited (85) the same URL 120.50.176.106/
8	2	10.154.213.142	pancademo\jason.waters	Repeatedly visited (84) the same URL 82.131.218.0/
9	2	10.154.228.8	pancademo\jordan.bowery	Repeatedly visited (83) the same URL 71.175.58.228/

Figura 5-191: Ejemplo de *Behavioral Botnet Report*

5.12.3 EVASIONES Y CONTRAMEDIDAS

566. Las evasiones son mecanismos que los atacantes emplean para intentar evadir la capacidad de inspección de un cortafuegos, como por ejemplo la fragmentación o el *overlapping* de segmentos TCP. Además de las evasiones de L4, también existen evasiones en L7, siendo éstas últimas muy populares por su gran simplicidad. Por ejemplo, el cifrado SSL/TLS es un mecanismo simple y efectivo de hacer *bypass* de un cortafuegos cuando no se realiza descifrado SSL/TLS, porque simplemente no podrá inspeccionar el tráfico.

567. Los equipos de Palo Alto Networks vienen preconfigurados para gestionar un gran número de tácticas evasivas. Además, es posible realizar algunos ajustes para personalizar esta configuración según se describe en la nota de este mismo apartado.

Nota: En el siguiente apartado de la documentación encontrará las prácticas recomendadas para evitar las evasiones:
https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/threat-prevention/best-practices-for-securing-your-network-from-layer-4-and-layer-7-evasions

6 FASE DE OPERACIÓN

568. La operación correcta de un sistema ya desplegado debe incluir los procedimientos necesarios para realizar:

- Comprobaciones periódicas del *hardware* y *software* para asegurar que no se ha introducido *hardware* o *software* no autorizado. El *firmware* activo y su integridad deberán verificarse periódicamente para comprobar que está libre de software malicioso.

- Comprobaciones periódicas de la correcta operación de los algoritmos y funciones criptográficas, a través de la ejecución de los correspondientes auto-chequeos (*self-tests*).

- Actualizaciones periódicas del *software* de los equipos, para garantizar que están al día, tanto en las capacidades de reconocimiento de aplicaciones, como en la prevención de amenazas.

- Realización de backups automáticos de forma periódica y, a poder ser, de forma centralizada.

- Mantenimiento de los registros de auditoría. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos. La información de auditoria se guardará en las condiciones y por el periodo establecido en la normativa de seguridad.

- Auditar, al menos, los eventos especificados en la normativa de referencia y aquellos otros extraídos del análisis de riesgos.

569. Es recomendable, en concreto, llevar a cabo revisiones de los cambios en la configuración del sistema, de los logs generados por los *Correlation Objects*, y del report de comportamiento de *botnets*.

7 CHECKLIST

570. A continuación, se presenta una lista rápida para comprobar si las recomendaciones de seguridad descritas anteriormente, han sido implantadas o no en cada entorno.

INFORMACIÓN DEL DISPOSITIVO	
Nombre	
Nº de Serie	
Ubicación	
Fecha	

ACCIONES	SÍ	NO	OBSERVACIONES
INSTALACIÓN			
Verificación de la entrega segura del producto	ϒ	ϒ	
Instalación en un entorno seguro	ϒ	ϒ	
CONFIGURACIÓN			
ANTES DE COMENZAR			
Integración de la gestión en una red protegida	ϒ	ϒ	
Registro de los equipos	ϒ	ϒ	
Registro de las licencias	ϒ	ϒ	
Actualización de contenidos	ϒ	ϒ	
Actualización de firmware	ϒ	ϒ	
Segmentación con zonas	ϒ	ϒ	
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (FIPS-CC)	ϒ	ϒ	
GESTIÓN DEL EQUIPO			
Métodos de acceso	ϒ	ϒ	
Banner de conexión	ϒ	ϒ	
Requisitos mínimos de contraseña	ϒ	ϒ	
Cambiar usuario y contraseña por defecto	ϒ	ϒ	
Configurar otras cuentas de administración	ϒ	ϒ	
Configurar *timeouts* de sesión	ϒ	ϒ	
Configurar comportamiento de intentos fallidos de autenticación	ϒ	ϒ	
Securización SNMP	ϒ	ϒ	

ACCIONES	SÍ	NO	OBSERVACIONES
Securización de los updates	ϒ	ϒ	
Frecuencia y planificación de updates de aplicaciones y amenazas	ϒ	ϒ	
Frecuencia y planificación de updates de Antivirus	ϒ	ϒ	
Frecuencia y planificación de updates de WildFire	ϒ	ϒ	
Configuración NTP	ϒ	ϒ	
PROTOCOLOS SEGUROS			
Configurar IKE / IPsec	ϒ	ϒ	
Configurar de HTTPS / TLS	ϒ	ϒ	
PROTOCOLOS NO SEGUROS			
Deshabilitar protocolos no seguros	ϒ	ϒ	
CERTIFICADOS			
Instalar certificados	ϒ	ϒ	
Instalar certificados de CA raíz (*root CA certificates)*	ϒ	ϒ	
Configurar validación de certificados	ϒ	ϒ	
SERVIDORES DE AUTENTICACIÓN			
Configurar profiles de autenticación	ϒ	ϒ	
Restringir usuarios que se puedan autenticar	ϒ	ϒ	
Configurar doble factor de autenticación	ϒ	ϒ	
AUDITORÍA			
Configurar logging de todo el tráfico relevante	ϒ	ϒ	
Habilitar *FIPS-CC Specific Logging*	ϒ	ϒ	
Habilitar *Packet Drop Logging*	ϒ	ϒ	
Habilitar *TLS Session Logging*	ϒ	ϒ	
Habilitar CA (OCSP/CRL) *Session Establishment Logging*	ϒ	ϒ	
Habilitar IKE *Session Establishment Logging*	ϒ	ϒ	
Política de auditoría de cambios	ϒ	ϒ	
Configurar los parámetros para almacenamiento local	ϒ	ϒ	
Configurar el envío a servidor *syslog*	ϒ	ϒ	
BACKUPS			

ACCIONES	SÍ	NO	OBSERVACIONES
Backups automáticos programados	ϒ	ϒ	
CONFIGURACIÓN DE HA			
HA sincronizado	ϒ	ϒ	
Configuración de *link/path monitoring*	ϒ	ϒ	
Exclusión entre *Preemption* y *Passive Link State*	ϒ	ϒ	
VPNs			
Configuración de VPNs *site-to-site*	ϒ	ϒ	
Configuración de VPNs acceso remoto (Gl*obalProt*ect)	ϒ	ϒ	
APP-ID Y POLÍTICAS			
Usar aplicaciones en las políticas de seguridad	ϒ	ϒ	
Evitar el uso de Service "*Any*"	ϒ	ϒ	
Configurar regla de "*Deny*" explícita	ϒ	ϒ	
Aplicaciones específicas para tráfico propietario	ϒ	ϒ	
IDENTIFICACIÓN DE LOS USUARIOS			
Mapeo de Usuario-IP para todo el tráfico de usuarios	ϒ	ϒ	
Deshabilitar User-ID en los interfaces externos	ϒ	ϒ	
Deshabilitar WMI si no se utiliza	ϒ	ϒ	
Configurar *Include/Exclude* networks	ϒ	ϒ	
Configurar una cuenta dedicada para User-ID	ϒ	ϒ	
Restringir el tráfico de User-ID hacia zonas inseguras	ϒ	ϒ	
FILTRADO DE URLS			
Utilizar URL *Filtering* en todas las reglas hacia internet	ϒ	ϒ	
Activar el *logging* de cabeceras HTTP	ϒ	ϒ	
Desactivar el *logging* solo de *Container Pages*	ϒ	ϒ	
IPS (*VULNERABILITY PROTECTION*)			
Configurar perfil de *Vulnerability Protection*	ϒ	ϒ	
Utilizar *Vulnerability Protection* en todas las reglas que permitan tráfico	ϒ	ϒ	
ANTI-SPYWARE			

ACCIONES	SÍ	NO	OBSERVACIONES
Configurar perfil de *Anti-Spyware*	ϒ	ϒ	
Configurar *DNS Sinkholing*	ϒ	ϒ	
Utilizar *Anti-Spyware* en todas las reglas que permitan tráfico hacia Internet	ϒ	ϒ	
ANTIVIRUS			
Configurar perfil de Antivirus	ϒ	ϒ	
Utilizar Antivirus en todas las reglas que permitan tráfico	ϒ	ϒ	
BLOQUEO DE FICHEROS			
Configurar perfil de *File Blocking*	ϒ	ϒ	
Utilizar *File Blocking* en todas las reglas que permitan tráfico	ϒ	ϒ	
WILDFIRE			
Configurar el uso de la nube pública europea	ϒ	ϒ	
Incrementar el tamaño de archivo en *WildFire*	ϒ	ϒ	
Envío de la información de sesión a *WildFire*	ϒ	ϒ	
Configurar *forwarding* para el tráfico SSL descifrado	ϒ	ϒ	
Configurar perfil de *WildFire Analysis* para todos los ficheros	ϒ	ϒ	
Configurar perfil de Antivirus	ϒ	ϒ	
Utilizar *WildFire Analysis* y Antivirus en todas las reglas que permitan tráfico	ϒ	ϒ	
Verificar que el servicio de *WildFire* funciona	ϒ	ϒ	
INSPECCIÓN SSL			
Configurar la inspección SSL en salida	ϒ	ϒ	
Configurar la inspección SSL en entrada	ϒ	ϒ	
INSPECCIÓN DE CONTENIDO TUNELIZADO			
Configurar la inspección de contenido tunelizado	ϒ	ϒ	
Incluir la revisión periódica de los logs generados, en los procedimientos operativos	ϒ	ϒ	
CORRELATION ENGINE			
Activar todos los *Correlation Objects*	ϒ	ϒ	
PREVENCIÓN DE ATAQUES DE DOS			
Configurar *Flood Protection*	ϒ	ϒ	

ACCIONES	SÍ	NO	OBSERVACIONES
Configurar *Resources Protection*	ϒ	ϒ	
Ajustar valores por defecto y ratios máximos	ϒ	ϒ	
INFORMES DE COMPORTAMIENTO *BOTNET*			
Incluir la revisión diaria de los informes generados, en los procedimientos operativos	ϒ	ϒ	
OPERACIÓN			
Comprobaciones periódicas del *hardware* y el *software*	ϒ	ϒ	
Comprobaciones periódicas de la integridad del *firmware*	ϒ	ϒ	
Comprobaciones periódicas de la operación de los algoritmos y funciones criptográficas	ϒ	ϒ	
Actualizaciones periódicas y parches de seguridad	ϒ	ϒ	
Realización de *backups* automáticos	ϒ	ϒ	
Mantenimiento de los registros de auditoría	ϒ	ϒ	
Revisión periódica de los cambios de configuración del sistema	ϒ	ϒ	
Revisión periódica de los registros de auditoría	ϒ	ϒ	
Revisión diaria del comportamiento de *botnets*	ϒ	ϒ	
Revisión periódica de logs de *Correlations Objects*	ϒ	ϒ	

8 REFERENCIAS

[REF1] Hipervisores VM-Series:
https://docs.paloaltonetworks.com/compatibility-matrix/reference/vm-series-firewalls/vms-series-hypervisor-support
https://docs.paloaltonetworks.com/compatibility-matrix/reference/cn-series-firewalls

[REF2] Palo Alto Networks official documentation for PAN-OS 11:
https://docs.paloaltonetworks.com/pan-os/11-1/pan-os-admin/getting-started

[REF3] *Advanced Threat Prevention:*
https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/threat-prevention

[REF4] *Palo Alto Firewall Security Configuration Benchmark*
https://www.sans.org/reading-room/whitepapers/auditing/palo-alto-firewall-security-configuration-benchmark-35777

[REF5] *CIS Palo Alto Firewall 6 Benchmark V1.0.0:*
https://benchmarks.cisecurity.org/downloads/show-single/?file=palofirewall.100

[REF6] *Security Best Practices Checklist for Palo Alto Networks Next-Generation Firewalls:* http://www.consigas.com/blog/security-best-practices-checklist-for-palo-alto-networks-next-generation-firewalls
https://docs.paloaltonetworks.com/best-practices

9 ABREVIATURAS

AAA	Authentication, Authorization, and Accounting
ACC	Application Command Center
API	Application Programming Interface
App-ID	Application Identification
AWS	Amazon Web Services
C2	Command and Control
CA	Certificate Authority
CC	Common Criteria
CCN-STIC	Centro Criptológico Nacional - Guía de Seguridad de las TIC
CDN	Content Delivery Network
CLI	Command Line Interface
CPSTIC	Catálogo de Productos y Servicios de Seguridad de CCN
CRL	Certificate Revocation List
DCOM	Distributed Component Object Model
DDoS	Distributed Denial of Service
Device-ID	Device Identification
DGA	Domain Generation Algorithm
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DSRI	Disable Server Response Inspection
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
ESP	Encapsulating Security Payload
EULA	End-User License Agreement
FIPS	Federal Information Processing Standards
FIPS-CC	Federal Information Processing Standards - Common Criteria
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
GCP	Google Cloud Platform
GRE	Generic Routing Encapsulation
GTP-U	GPRS Tunneling Protocol for User Data
GUI	Graphical User Interface

HA	High Availability
HIP	Host Information Profile
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ICMPv4	Internet Control Message Protocol version 4
ICMPv6	Internet Control Message Protocol version 6
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
KVM	Kernel-based Virtual Machine
L3	Layer 3 (Capa 3 del modelo OSI - Red)
L4	Layer 4 (Capa 4 del modelo OSI - Transporte)
L7	Layer 7 (Capa 7 del modelo OSI - Aplicación)
LDAP	Lightweight Directory Access Protocol
LSVPN	Large Scale Virtual Private Network
MFA	Multi-Factor Authentication
ML	Machine Learning
NAC	Network Access Control
NAT	Network Address Translation
NGFW	Next Generation Firewall
NTLM	NT LAN Manager
NTP	Network Time Protocol
NXNSAttack	NXNS Attack (amplification attack on DNS resolvers)
OCSP	Online Certificate Status Protocol
P2P	Peer-to-Peer
PAN-DB	Palo Alto Networks Database

PAN-OS	Palo Alto Networks Operating System
PCAP	Packet Capture
POP3	Post Office Protocol 3
PQC	Post-Quantum Computing
QC	Quantum Computing
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RED	Random Early Drop
RSA	Rivest-Shamir-Adleman (algoritmo de cifrado)
SA	Security Association
SAML	Security Assertion Markup Language
SMB	Server Message Block
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SP3	Single Pass Parallel Processing
SSL	Secure Sockets Layer
SYN	Synchronize (bandera en el encabezado TCP utilizada en el establecimiento de conexiones)
Syslog	System Logging Protocol
TCP	Transmission Control Protocol
TI	Tecnología de la Información
TLS	Transport Layer Security
TTP	Hypertext Transfer Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
User-ID	User Identification
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VXLAN	Virtual Extensible Local Area Network
WAF	Web Application Firewall
WF-500	WildFire Private Cloud Appliance
WildFire	Servicio de análisis de amenazas de Palo Alto Networks
WMI	Windows Management Instrumentation
X.509	Public Key Infrastructure Standard