

Guía de Seguridad de las TIC

CCN-STIC 1413

Procedimiento de empleo seguro Cortafuegos NGFW de Palo Alto Networks



Febbrero 2024



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



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

NIPO: 083-24-100-X.

Fecha de Edición: febrero 2024

Palo Alto ha participado en la elaboración y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

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

AVISO LEGAL

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

ÍNDICE

1. INTRODUCCIÓN	11
1.1 ENTORNO ACTUAL	11
1.2 ARQUITECTURA DE LOS CORTAFUEGOS DE PALO ALTO NETWORKS.....	12
1.2.1 TOPOLOGÍAS DE RED SOPORTADAS	13
1.3 SISTEMAS VIRTUALES	14
2. OBJETO Y ALCANCE	15
3. ORGANIZACIÓN DEL DOCUMENTO.....	17
4. FASE DE INSTALACIÓN	18
4.1 ENTREGA SEGURA DEL PRODUCTO.....	18
4.2 ENTORNO SEGURO DE INSTALACIÓN.....	18
5. FASE DE CONFIGURACIÓN	19
5.1 ANTES DE COMENZAR.....	19
5.1.1 INTEGRACIÓN DE LA GESTIÓN EN UNA RED PROTEGIDA.....	19
5.1.2 REGISTRO DE LOS EQUIPOS Y SUSCRIPCIONES.....	19
5.1.3 ACTUALIZACIÓN DE CONTENIDOS Y <i>FIRMWARE</i>	21
5.1.4 SEGMENTACIÓN EN ZONAS.....	22
5.2 MODO DE OPERACIÓN SEGURO	22
5.3 CONFIGURACIÓN DE LA GESTIÓN	23
5.3.1 ACCESO	23
5.3.2 BANNER DE CONEXIÓN.....	24
5.3.3 REQUISITOS MÍNIMOS DE CONTRASEÑA	24
5.3.4 CAMBIAR USUARIO Y CONTRASEÑA POR DEFECTO	25
5.3.5 CONFIGURAR OTRAS CUENTAS DE ADMINISTRACIÓN	26
5.3.6 SEGURIDAD PARA SNMP	28
5.3.7 SEGURIDAD DE ACTUALIZACIONES Y <i>UPDATES</i>	28
5.3.8 CONFIGURACIÓN NTP	30
5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS.....	31
5.4.1 IKE/IPSEC	31
5.4.2 TLS/HTTPS.....	34
5.5 CONFIGURACIÓN DE PROTOCOLOS NO SEGUROS.....	34
5.6 GESTIÓN DE CERTIFICADOS.....	35
5.6.1 CREAR UN CERTIFICADO DE CA RAÍZ AUTOFIRMADO	35
5.6.2 GENERAR UN CERTIFICADO	36
5.6.3 IMPORTAR UN CERTIFICADO Y UNA CLAVE PRIVADA	37
5.6.4 COMPROBACIÓN <i>ONLINE</i> DE VALIDEZ DE CERTIFICADOS.....	38
5.6.5 CONFIGURACIÓN DE LA CADENA DE VALIDACIÓN DE CERTIFICADOS	39
5.7 SERVIDOR DE AUTENTICACIÓN (AAA SERVER).....	40
5.8 REGISTRO DE EVENTOS (AUDITORÍA).....	42
5.8.1 GENERACIÓN DE REGISTROS	42
5.8.2 AUDITORÍA DE CAMBIOS	58
5.8.3 ALMACENAMIENTO LOCAL.....	59
5.8.4 ALMACENAMIENTO REMOTO	60
5.9 <i>BACKUPS</i>	62
5.10 AUTO-CHEQUEOS.....	62
5.11 ALTA DISPONIBILIDAD	62
5.12 CONFIGURACIÓN DE LOS SERVICIOS DE SEGURIDAD	66
5.12.1 FILTRADO DE PAQUETES CON ESTADO (STATEFUL TRAFFIC FILTERING).....	66
5.12.2 VPNS	68
5.12.2.1 <i>SITE-TO-SITE</i> VPN	69
5.12.2.2 <i>REMOTE USER-TO-SITE</i> VPN (<i>GLOBALPROTECT</i>).....	73
5.12.3 IDENTIFICACIÓN DE APLICACIONES (APP-ID)	86

5.12.3.1	COMBATIENDO LA CADENA DE CIBERATAQUE.....	88
5.12.3.2	REQUISITOS DE SEGURIDAD	88
5.12.3.3	EJEMPLO DE USO	90
5.12.3.4	OBSERVABLES	91
5.12.4	IDENTIFICACIÓN DE USUARIOS	93
5.12.4.1	MEDIDAS DE SEGURIDAD.....	94
5.12.4.2	EJEMPLO DE USO	97
5.12.4.3	OBSERVABLES	98
5.12.5	IDENTIFICACIÓN DE DISPOSITIVO (DEVICE-ID)	99
5.12.5.1	COMBATIENDO LA CADENA DE CIBERATAQUE.....	100
5.12.5.2	REQUISITOS DE SEGURIDAD	101
5.12.5.3	EJEMPLO DE USO	103
5.12.5.4	OBSERVABLES	105
5.12.6	FILTRADO DE URL (ADVANCED URL FILTERING)	105
5.12.6.1	COMBATIENDO LA CADENA DE CIBERATAQUE.....	107
5.12.6.2	REQUISITOS DE SEGURIDAD	107
5.12.6.3	EJEMPLO DE USO	111
5.12.6.4	OBSERVABLES	113
5.12.7	IPS.....	114
5.12.7.1	COMBATIENDO LA CADENA DE CIBERATAQUE.....	117
5.12.7.2	REQUISITOS DE SEGURIDAD	117
5.12.7.3	EJEMPLO DE USO	118
5.12.7.4	OBSERVABLES	119
5.12.8	ANTI-SPYWARE	121
5.12.8.1	COMBATIENDO LA CADENA DE CIBERATAQUE.....	125
5.12.8.2	REQUISITOS DE SEGURIDAD	125
5.12.8.3	EJEMPLO DE USO	126
5.12.8.4	OBSERVABLES	126
5.12.9	ANTIVIRUS	127
5.12.9.1	COMBATIENDO LA CADENA DE CIBERATAQUE.....	129
5.12.9.2	REQUISITOS DE SEGURIDAD	129
5.12.9.3	EJEMPLO DE USO	131
5.12.9.4	OBSERVABLES	131
5.12.10	BLOQUEO DE FICHEROS (FILE BLOCKING)	132
5.12.10.1	COMBATIENDO LA CADENA DE CIBERATAQUE.....	133
5.12.10.2	REQUISITOS DE SEGURIDAD	133
5.12.10.3	EJEMPLO DE USO	134
5.12.10.4	OBSERVABLES	135
5.12.11	WILDFIRE	137
5.12.11.1	COMBATIENDO LA CADENA DE CIBERATAQUE.....	138
5.12.11.2	REQUISITOS DE SEGURIDAD	138
5.12.11.3	EJEMPLO DE USO	143
5.12.11.4	OBSERVABLES	144
5.12.12	INSPECCIÓN SSL.....	146
5.12.12.1	REQUISITOS DE SEGURIDAD	148
5.12.12.2	OBSERVABLES	149
5.12.13	INSPECCIÓN DE CONTENIDO TUNELIZADO	150
5.12.13.1	EJEMPLO DE USO	152
5.12.13.2	OBSERVABLES	154
5.12.14	MOTOR DE CORRELACIÓN AUTOMATIZADO.....	155
5.12.14.1	RECOMENDACIONES.....	155
5.12.14.2	OBSERVABLES	156
5.12.15	FIRMAS DE LOS MÓDULOS DE PREVENCIÓN.....	157

5.12.15.1 RENDIMIENTO Y NÚMERO DE FIRMAS	157
5.12.15.2 ACCIÓN POR DEFECTO PARA LAS FIRMAS	158
5.13 PREVENCIÓN Y DETECCIÓN DE ATAQUES	160
5.13.1 ATAQUES DOS.....	160
5.13.1.1 COMBATIENDO LA CADENA DE CIBERATAQUE.....	161
5.13.1.2 RECOMENDACIONES.....	161
5.13.1.3 EJEMPLO DE USO	163
5.13.1.4 OBSERVABLES	164
5.13.2 INFORME DE COMPORTAMIENTO DE BOTNET	165
5.13.2.1 RECOMENDACIONES.....	166
5.13.2.2 OBSERVABLES	166
5.13.3 EVASIONES Y CONTRAMEDIDAS.....	167
6. FASE DE OPERACIÓN	168
7. CHECKLIST	169
8. REFERENCIAS.....	174

ÍNDICE DE FIGURAS

Figura 1-1: Arquitectura SP3 de Palo Alto Networks	13
Figura 5-1: Arquitectura SP3 de Palo Alto Networks	20
Figura 5-2: Configuración del acceso a la gestión	23
Figura 5-3: Configuración de un banner de acceso a la gestión	24
Figura 5-4: Configuración de la complejidad de las contraseñas de gestión	25
Figura 5-5: Cambio del usuario/contraseña de administración por defecto	26
Figura 5-6: Perfiles de autenticación de los administradores	26
Figura 5-7: Configuración de la autenticación externa de administradores	27
Figura 5-8: Configuración del acceso a la gestión de la cuenta local	28
Figura 5-9: Configuración SNMPv3	28
Figura 5-10: Validación de los servidores de actualización	29
Figura 5-11: Programación de updates de Aplicaciones y Amenazas	29
Figura 5-12: Programación de updates de Antivirus	30
Figura 5-13: Programación de updates de WildFire	30
Figura 5-14: Configuración redundada de NTP	30
Figura 5-15: Configuración IKE Crypto Profile	31
Figura 5-16: Configuración IKE Gateway (General)	32
Figura 5-17: Configuración IKE Gateway (Advanced)	33
Figura 5-18: Configuración IPSec Crypto Profile	33
Figura 5-19: Configuración SSL/TLS Service Profile	34
Figura 5-20: Configuración Perfil interfaz de gestión	35
Figura 5-21: Crear un certificado CA autofirmado	36
Figura 5-22: Generar un certificado firmado por la CA interna del cortafuegos	37
Figura 5-23: Generar una solicitud de firma de certificado (CSR)	38
Figura 5-24: Visualización de certificado pendiente de firma por la CA	38
Figura 5-25: Configuración de perfil de certificado con OSCP / CRL	39
Figura 5-26: Lista preinstalada de certificados de confianza	39
Figura 5-27: Configuración del RADIUS Server	40
Figura 5-28: Configuración del perfil de autenticación	41
Figura 5-29: Configuración del perfil de autenticación (advanced)	41
Figura 5-30: Configuración del perfil de autenticación (factors)	41
Figura 5-31: Configuración del perfil MFA	42
Figura 5-32: Habilitar el registro de logs en reglas de la política	42
Figura 5-33: Ejemplo de logs de Configuración	58
Figura 5-34: Ejemplo de salida de la herramienta Config Audit	59
Figura 5-35: Configuración general de logging e informes	60
Figura 5-36: Configuración de perfil de servidor Syslog	61
Figura 5-37: Configuración de perfil de reenvío de logs	61
Figura 5-38: Activar reenvío de logs en la configuración de la regla de seguridad	62
Figura 5-39: Widget de estado de alta disponibilidad	63
Figura 5-40: Configuración de link/path monitoring	64
Figura 5-41: Configuración recomendada de Preemption y Passive Link State	64
Figura 5-42: Configuración recomendada de ajustes de Activo/Pasivo	64
Figura 5-43: Configuración de Clúster	65
Figura 5-44: Configuración de enlaces	65
Figura 5-45: Configuración de los miembros del clúster	66
Figura 5-46: Dashboard del clúster	66
Figura 5-47: Tipos de VPNs soportadas	69
Figura 5-48: Configuración de interfaces tunnel	70
Figura 5-49: Configuración de tunnel IPSec	71

Figura 5-50: Configuración de Proxy-ID (opcional)	71
Figura 5-51: Configuración de ruta estática.....	72
Figura 5-52: Comprobación del estado del túnel IPSEC	72
Figura 5-53: Comprobación del estado del túnel IPSEC	73
Figura 5-54: Componentes de GlobalProtect	74
Figura 5-55: Configuración de interface tunnel.....	75
Figura 5-56: Importación de certificado.....	76
Figura 5-57: Generación de CA autofirmada	76
Figura 5-58: Generación de certificado autofirmado	77
Figura 5-59: Creación de perfil SSL/TLS.....	77
Figura 5-60: Creación de perfil de autenticación (Authentication)	78
Figura 5-61: Creación de perfil de autenticación (Advanced)	78
Figura 5-62: Configuración de perfil IPsec de GlobalProtect	79
Figura 5-63: Configuración de GlobalProtect Gateway (General)	79
Figura 5-64: Configuración de GlobalProtect Gateway (Authentication)	80
Figura 5-65: Configuración de GlobalProtect Gateway (Agent)	80
Figura 5-66: Configuración de GlobalProtect Gateway (Timeout Settings)	81
Figura 5-67: Configuración de GlobalProtect Gateway (Client Settings)	81
Figura 5-68: Configuración de GlobalProtect Gateway (Network Services)	81
Figura 5-69: Configuración de GlobalProtect Portal (General).....	82
Figura 5-70: Configuración de GlobalProtect Portal (Authentication)	82
Figura 5-71: Configuración de GlobalProtect Portal (Agent)	83
Figura 5-72: Configuración de GlobalProtect Portal (External)	83
Figura 5-73: Selección de agente GlobalProtect a utilizar	84
Figura 5-74: GlobalProtect Portal y descarga de agente	84
Figura 5-75: Pantalla de inicio de aplicación Globalprotect (Windows)	85
Figura 5-76: Comprobación de estado de la conexión VPN (Windows)	85
Figura 5-77: Comprobación de estado del Agente (Windows)	85
Figura 5-78: Logs de GlobalProtect	86
Figura 5-79: Algoritmo de App-ID.....	87
Figura 5-80: Ejemplo de política de aplicaciones basada en lógica positiva	89
Figura 5-81: Definición de aplicaciones propietarias	90
Figura 5-82: Política de protección de DMZ en entrada	91
Figura 5-83: Política de protección de DMZ en salida.....	91
Figura 5-84: Visibilidad de aplicaciones con AppScope	91
Figura 5-85: Ejemplo de Traffic logs	92
Figura 5-86: Ejemplo de unknown-tcp y captura en fichero pcap	92
Figura 5-87: Tecnologías User-ID disponibles.....	93
Figura 5-88: Activación de User-ID solamente en zonas internos.....	94
Figura 5-89: Deshabilitación de User-ID Agent probing.....	95
Figura 5-90: Configuración de include/exclude networks en User-ID	95
Figura 5-91: Restricción del tráfico del agente User-ID.....	96
Figura 5-92: Configuración del interfaz de User-ID	97
Figura 5-93: Ejemplo de despliegue de una política con User-ID	98
Figura 5-94: Ejemplo de página de Portal Cautivo	98
Figura 5-95: Ejemplo de logs incluyendo el atributo usuario	98
Figura 5-96: Ejemplo de bloqueo de página incluyendo el usuario.....	99
Figura 5-97: Single Pass Architecture	99
Figura 5-98: Reglas de Seguridad con Device-ID	100
Figura 5-99: Configuración de atributos	102
Figura 5-100: Uso de Device-ID en la política	102
Figura 5-101: Reglas de la Política de Seguridad con Device-ID	103
Figura 5-102: Ejemplo de políticas basadas en el ID del dispositivo (Device-ID).....	103

Figura 5-103: Restringir descargas de ficheros peligrosos para dispositivos con sistemas operativos obsoletos	103
Figura 5-104: Descifrado basado en el dispositivo.....	104
Figura 5-105: Rastreo de dispositivos en la red	104
Figura 5-106: Logs de los dispositivos.....	105
Figura 5-107: Detección en tiempo real.....	109
Figura 5-108: Activación de logging de cabeceras HTTP en URL Filtering.....	110
Figura 5-109:Desactivación de logging solamente de container pages	111
Figura 5-110: Bloqueo de sitios restringidos	112
Figura 5-111: Creación de un perfil de URL con todas las categorías en Alert.....	112
Figura 5-112: Aplicación del perfil sobre las reglas de acceso por usuario y grupo	112
Figura 5-113: Activación de análisis profundo para el filtrado avanzado de URL	113
Figura 5-114: Ejemplo de log de URL	114
Figura 5-115: Vista detallada del log de URL	114
Figura 5-116: Ejemplo de página de bloqueo de URL.....	114
Figura 5-117: Modulo Panorama para Snort	115
Figura 5-118 Perfiles de Vulnerability Protection predefinidos.....	116
Figura 5-120: Perfil de Vulnerability Protection recomendado	118
Figura 5-121: Perfiles Vulnerability Protection para clientes	118
Figura 5-122: Perfiles Vulnerability Protection para la DMZ	119
Figura 5-123: Ejemplo de log de Vulnerability Protection	119
Figura 5-124: Ejemplo de log de Vulnerability Protection detallado	120
Figura 5-125: Creación de excepciones en los perfiles de Vulnerability Protection	120
Figura 5-126: Perfiles de Anti-Spyware predefinidos.....	122
Figura 5-127: Perfiles de Anti-Spyware personalizados	122
Figura 5-128: Políticas de DNS	123
Figura 5-129: Análisis Inline en la nube	124
Figura 5-130: Perfil de Anti-spyware recomendado.....	125
Figura 5-131: Perfiles Anti-Spyware para clientes.....	126
Figura 5-132: Ejemplo de log de Anti-Spyware	126
Figura 5-133: Ejemplo de log de Anti-Spyware detallado	127
Figura 5-134: Perfil por defecto del Antivirus.....	128
Figura 5-135: Excepción en perfil de Antivirus personalizado	129
Figura 5-136: Perfil de Antivirus recomendado.....	130
Figura 5-137: Perfiles Antivirus para clientes.....	131
Figura 5-138: Perfiles Antivirus para las actualizaciones de la DMZ	131
Figura 5-139: Ejemplo de log de Antivirus.....	131
Figura 5-140: Ejemplo de log de Antivirus detallado	132
Figura 5-141: Ejemplo de página de bloqueo de Antivirus	132
Figura 5-142: Perfil de File Blocking	134
Figura 5-143: Ejemplo de Perfil de File Blocking.....	135
Figura 5-144: Aplicación de File Blocking en las reglas de seguridad.....	135
Figura 5-143: Ejemplo de log de File Blocking	135
Figura 5-146: Ejemplo de log de File Blocking detallado	136
Figura 5-147: Ejemplo de página de bloqueo y Continue de File Blocking	136
Figura 5-148: Configuración de Wildfire europeo.....	139
Figura 5-149: Configuración tamaño máx de ficheros inspeccionados WildFire	139
Figura 5-150: Configuración de información de sesión enviada a WildFire.....	140
Figura 5-151: Forwarding of Decrypted Content.....	140
Figura 5-152: Perfil de WildFire Analysis recomendado	141
Figura 5-153: Perfil de Antivirus recomendado.....	142
Figura 5-154: Configuración del perfil público de WildFire	143
Figura 5-155: Configuración del perfil híbrido de WildFire	143

Figura 5-156: Aplicación de WildFire público en las reglas de seguridad a Internet	144
Figura 5-157: Aplicación de WildFire híbrido en las reglas de datacenter.....	144
Figura 5-158: Aplicación de WildFire público en las reglas de correo electrónico	144
Figura 5-159: Ejemplo de log de File Blocking	144
Figura 5-160: Ejemplo de log de WildFire detallado	144
Figura 5-161: Ejemplo de informe de WildFire integrado en el cortafuegos.....	145
Figura 5-162: Actualizaciones de WildFire	146
Figura 5-163: Ejemplo de log generado por una firma de WildFire	146
Figura 5-164: Ejemplo de página de bloqueo de WildFire	146
Figura 5-165: Política de SSL Forward Proxy.....	148
Figura 5-166: Selección de certificados para la inspección SSL entrante.....	149
Figura 5-167: Política de SSL Inbound Inspection.....	149
Figura 5-168: Detalle de logs.....	150
Figura 5-169: Esquema cabeceras Inspección de túneles.....	151
Figura 5-170: Políticas soportadas en tráfico tunelizado.....	151
Figura 5-171: Configuración de regla de inspección de tráfico (General)	152
Figura 5-172: Configuración de regla de inspección de tráfico (Source)	153
Figura 5-173: Configuración de regla de inspección de tráfico (Destination)	153
Figura 5-174: Configuración de regla de inspección de tráfico (Inspection)	154
Figura 5-175: Monitorización de tráfico tunelizado	154
Figura 5-176: Vista de detalle de log (flag tunnel inspected).....	155
Figura 5-177: Correlation Objects predefinidos en el sistema.....	156
Figura 5-178: Logs de ejemplo del motor automático de correlación	156
Figura 5-179: Logs de ejemplo del motor automático de correlación (detalle)	157
Figura 5-180: Ejemplo de activación de DSRI.....	158
Figura 5-181: Acciones de las firmas de Anti-Spyware y Vulnerability Protection.....	159
Figura 5-182: Acciones de las firmas de Antivirus	160
Figura 5-183: Configuración por defecto perfil de protección DoS	162
Figura 5-184: Ejemplo de política DoS.....	164
Figura 5-185: Ejemplo de logs de Flood Protection	165
Figura 5-186: Ejemplo de log de Resource Protection.....	165
Figura 5-187: Ejemplo log número de eventos totales agregados	165
Figura 5-188: Personalización del Behavioral Botnet Report	166
Figura 5-189: Ejemplo de Behavioral Botnet Report	167

ÍNDICE DE TABLAS

Tabla 1: Capacidades de los diferentes despliegues de red.....	14
Tabla 2: Logs de Sistema.....	44
Tabla 3: Logs de Configuración	46
Tabla 4: Logs de tráfico.....	51
Tabla 5: Eventos Auditables	55
Tabla 6: Acciones de administración auditables	58
Tabla 7: Cadena de ciberataque – App-ID	88
Tabla 8: Requisitos de aplicaciones y grupos de usuarios de ejemplo.....	97
Tabla 9: Cadena de ciberataque – Device-ID.....	100
Tabla 10: Cadena de ciberataque: URL Filtering	107
Tabla 11: Cadena de ciberataque - Vulnerability Protection	117
Tabla 12: Cadena de ciberataque - Anti-Spyware	125
Tabla 13: Cadena de ciberataque - Antivirus.....	129
Tabla 14: Cadena de ciberataque - File Blocking	133
Tabla 15: Cadena de ciberataque - WildFire Threat Intelligence.....	138

Tabla 16: Cadena de ciberataque - DoS/Zone Protection.....	161
--	-----

1. INTRODUCCIÓN

1.1 ENTORNO ACTUAL

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.

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.

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.

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).

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.

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.

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

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

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.

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 Kubrenteses gestionados por consumidores, tales como Openshift RedHat.

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>

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.

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.

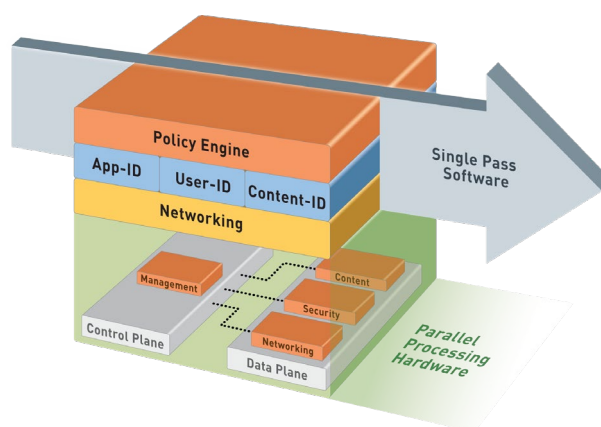


Figura 1-1: Arquitectura SP3 de Palo Alto Networks

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

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*.

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

Característica	<i>vwire</i>	<i>Layer2</i>	<i>Layer3</i>	<i>Tap</i>
VLAN tags	Sí	Sí	Sí	Sí
Tagged subinterfaces	Sí	Sí	Sí	No
Untagged subinterfaces	No	No	Sí	No
Routing	No	Sí	Sí	No
NAT	Sí	Sí	Sí	No
QoS	Sí	Sí	Sí	No

Característica	<i>vwire</i>	<i>Layer2</i>	<i>Layer3</i>	<i>Tap</i>
Descifrado SSL	Sí	Sí	Sí	Sí (<i>inbound</i>)
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/10-2/pan-os-networking-admin/configure-interfaces>

1.3 SISTEMAS VIRTUALES

Los equipos de Palo Alto Networks de las series 3000 y superiores, 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).

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/10-2/pan-os-admin/virtual-systems/virtual-systems-overview>

2. OBJETO Y ALCANCE

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

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.

Toda la documentación aquí presentada se basa en la **versión 10.2 de PAN-OS**, sistema operativo de los cortafuegos de Palo Alto Networks.

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.

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

- PA-200 Series
 - PA-220
 - PA220R
- PA-400 Series
 - PA-410
 - PA-440
 - PA-450
 - PA-460
- PA-800 Series
 - PA-820
 - PA-850
- PA-3200 Series
 - PA-3220
 - PA-3250
 - PA-3260
- PA-3400 Series
 - PA-3410
 - PA-3420
 - PA-3430
 - PA-3440
- PA-5200 Series
 - PA-5220

- PA-5250
 - PA-5260
 - PA-5280
- PA-5400 Series
 - PA-5410
 - PA-5420
 - PA-5430
 - PA-5450
- PA-7000 Series
 - PA-7050
 - PA-7080
- VM Series
 - VM-50
 - VM-100
 - VM-200
 - VM-300
 - VM-500
 - VM-700
 - VM-1000-HV

Estos productos han sido cualificados e incluidos en **el Catálogo de Productos y Servicios de Seguridad (CPSTIC)** del Centro Criptológico Nacional, en las familias de **Cortafuegos** y **VPN Ipsec**.

3. ORGANIZACIÓN DEL DOCUMENTO

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

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

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

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.

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*).

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

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.

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.

5. FASE DE CONFIGURACIÓN

5.1 ANTES DE COMENZAR

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.

5.1.1 INTEGRACIÓN DE LA GESTIÓN EN UNA RED PROTEGIDA

En primer lugar, debe integrarse el equipo en la red de gestión, que debería ser una red aislada en su organización. 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.

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, según se indica en el apartado 5.3.4.

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).

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*”.

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/10-2/pan-os-admin/getting-started/integrate-the-firewall-into-your-management-network/perform-initial-configuration>

5.1.2 REGISTRO DE LOS EQUIPOS Y SUSCRIPCIONES

Una vez que se ha configurado la gestión del dispositivo, es necesario proceder a su registro. Para ello, hay que conectarse con un navegador a:

<https://support.paloaltonetworks.com/support>

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 poder crear esta cuenta, se debe dirigir a este enlace y proceder a su creación.

<https://support.paloaltonetworks.com/Support/Index>

Una vez allí se ha de proceder a crear la cuenta, para ello se pincha sobre “Create my account” como se puede observar en la imagen.

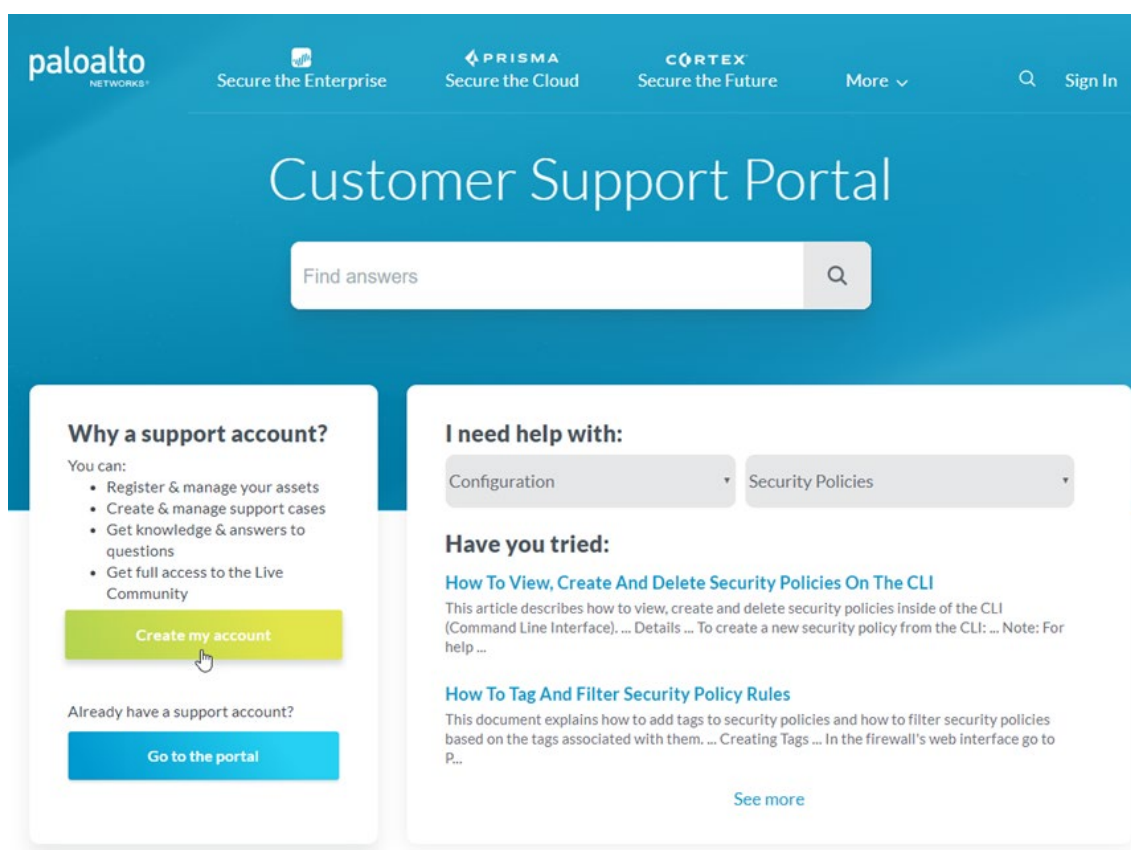


Figura 5-1: Arquitectura SP3 de Palo Alto Networks

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

Una vez conectado, seleccionar “Assets > Devices” y hacer click en “Register New Device”. Seleccionar “Register device using Serial Number or Authorization Code” y haga click en “Submit”. Después, añadir el número de serie del cortafuegos (que se puede copiar del *Dashboard* en el interfaz gráfico). 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”.

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 “*Device > 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 “*Device > 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 “*Device > 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/10-2/pan-os-admin/subscriptions/activate-subscription-licenses>

5.1.3 ACTUALIZACIÓN DE CONTENIDOS Y FIRMWARE

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.

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*”.

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.

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.

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.

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/10-2/pan-os-upgrade/software-and-content-updates/install-content-and-software-updates>

5.1.4 SEGMENTACIÓN EN ZONAS

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.

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.

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

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*.

5.2 MODO DE OPERACIÓN SEGURO

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.

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/10-2/pan-os-admin/certifications/enable-fips-and-common-criteria-support>

5.3 CONFIGURACIÓN DE LA GESTIÓN

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.

5.3.1 ACCESO

Ubicación: “Device > Setup > Management > Management Interface Settings”

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 5-2: Configuración del acceso a la gestión

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.

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”.

5.3.2 BANNER DE CONEXIÓN

Ubicación: “Device > Setup > Management > General Settings”.

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.

General Settings

Hostname: PaloAltoNetworks

Domain:

☐ Accept DHCP server provided Hostname

☐ Accept DHCP server provided Domain

Login Banner: ATENCION:Accede usted a un equipo propiedad de ...

☐ Force Admins to Acknowledge Login Banner

SSL/TLS Service Profile: None

Time Zone: Europe/Madrid

Locale: en

Date: 2022/02/01

Time: 21:41:27

Latitude:

Longitude:

☐ Automatically Acquire Commit Lock

☐ Certificate Expiration Check

☒ Tunnel Acceleration

OK Cancel

Figura 5-3: Configuración de un banner de acceso a la gestión

5.3.3 REQUISITOS MÍNIMOS DE CONTRASEÑA

Ubicación: “Device > Setup > Management > Minimum Password Complexity”

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.

Minimum Password Complexity ⓘ

☒ Enabled

Password Format Requirements

Minimum Length: 12

Minimum Uppercase Letters: 1

Minimum Lowercase Letters: 1

Minimum Numeric Letters: 1

Minimum Special Characters: 1

Block Repeated Characters: 0

☒ Block Username Inclusion (including reversed)

Functionality Requirements

New Password Differs By Characters: 3

☒ Require Password Change on First Login

Prevent Password Reuse Limit: 10

Block Password Change Period (days): 0

Required Password Change Period (days): 90

Expiration Warning Period (days): 7

Post Expiration Admin Login Count: 0

Post Expiration Grace Period (days): 2

Functionality requirements can be overridden by password profiles

OK Cancel

Figura 5-4: Configuración de la complejidad de las contraseñas de gestión

Nota: Es 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.

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*, *Minimum Lowercase Letters* y *Minimum 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*).

5.3.4 CAMBIAR USUARIO Y CONTRASEÑA POR DEFECTO

Ubicación: “*Device > Administrators*”

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

5.3.5 CONFIGURAR OTRAS CUENTAS DE ADMINISTRACIÓN

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.

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”.

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.

	NAME	ROLE	AUTHENTICATI... PROFILE	PASSWORD PROFILE	CLIENT CERTIFICATE AUTHENTICATI... (WEB)	PUBLIC KEY AUTHENTICATI... (SSH)	PROFILE	LOCKED USER
☐	admino	Superuser			☐	☐		
☐	admino	Superuser			☐	☐		
☐	jdiaz	Superuser	LDAP		☐	☐		
☒	jlgomez	Superuser	LDAP		☐	☐		

Figura 5-6: Perfiles de autenticación de los administradores

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*).

Authentication Profile

Name: LDAP

Authentication | Factors | **Advanced**

Allow List

- ☐ ALLOW LIST ^
- ☐ all

+ Add - Delete

Account Lockout

Failed Attempts: 3

Lockout Time (min): 10

OK Cancel

Figura 5-7: Configuración de la autenticación externa de administradores

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

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

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.

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

Ubicación: “*Device > Setup > Management > Authentication Settings*”

Authentication Settings

Authentication Profile: LDAP_corp

Certificate Profile: None

Idle Timeout (min): 10

API Key Lifetime (min): 0 (default)

API Keys Last Expired: [Expire All API Keys](#)

Failed Attempts: 0

Lockout Time (min): 0

Max Session Count (number): 0

Max Session Time (min): 0

OK Cancel

Figura 5-8: Configuración del acceso a la gestión de la cuenta local

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.

5.3.6 SEGURIDAD PARA SNMP

Ubicación: “*Device > Setup > Operations > SNMP Setup*”

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

Figura 5-9: Configuración SNMPv3

Nota: Puede encontrar información detallada sobre la configuración de SNMPv3 en el siguiente enlace:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000CIHOCA0>

5.3.7 SEGURIDAD DE ACTUALIZACIONES Y UPDATES

1. Updates de Servicios

Ubicación: “*Device > Setup > Services > Services*”

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 5-10: Validación de los servidores de actualización

2. Updates de aplicaciones y amenazas

Ubicación: “Device > Dynamic Updates > Schedule> Applications and Threats Update Schedule”

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)”.

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

Figura 5-11: Programación de updates de Aplicaciones y Amenazas

3. Updates de antivirus

Ubicación: “Device > Dynamic Updates > Schedule > Antivirus Update Schedule”

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 5-12: Programación de updates de Antivirus

4. Updates de Wildfire

Ubicación: “*Device > Dynamic Updates > Schedule > WildFire Update Schedule*”

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 5-13: Programación de updates de WildFire

5.3.8 CONFIGURACIÓN NTP

Ubicación: “*Device > Setup > Services > NTP*”

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

Figura 5-14: Configuración redundada de NTP

5.4 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

5.4.1 IKE/IPSEC

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).

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*).

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*.

1. Perfil criptográfico IKE

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.

Ubicación: “Network > Network Profiles > IKE Crypto”

Requisito de seguridad: Se deben seleccionar los siguientes parámetros:

IKE DH Group: Grupo 19 o Grupo 20

Encryption: AES-128 / AES-256

Authentication: SHA256 / SHA384 / SHA512

Key Lifetime: 8 horas

IKE Crypto Profile

Name: Suite-B-GCM-256-1

DH GROUP	ENCRYPTION
☐ group19	☐ aes-128-cbc
☒ group20	☒ aes-256-cbc

⊕ Add ⊖ Delete ↑ Move Up ↓ Move Down

AUTHENTICATION
☐ sha256
☐ sha384
☒ sha512

⊕ Add ⊖ Delete ↑ Move Up ↓ Move Down

Timers

Key Lifetime: Hours
8
Minimum lifetime = 3 mins

IKEv2 Authentication Multiple: 0

OK Cancel

Figura 5-15: Configuración IKE Crypto Profile

Ubicación: “Network > Network Profiles > IKE Gateways”

Requisito de seguridad: Se deben seleccionar los siguientes parámetros:

Version: IKEv2 only mode

Authentication: Certificate (no se recomienda el uso de claves precompartidas)

Advanced options:

IKE Crypto Profile: IKESecure (el perfil creado anteriormente)

IKE Gateway ⓘ

General | Advanced Options

Name: IKE_GW

Version: IKEv1 only mode

Address Type: ☒ IPv4 ☐ IPv6

Interface: ethernet1/2

Local IP Address: 172.16.24.254/24

Peer IP Address Type: ☒ IP ☐ FQDN ☐ Dynamic

Peer Address: Router Wifi IoT

Authentication: ☐ Pre-Shared Key ☒ Certificate

Local Certificate: GlobalprotectServer

Local Identification: Distinguished Name (Subject) CN=acme.com

Peer Identification: Distinguished Name (Subject) vpn.corporate.com

Peer ID Check: ☒ Exact ☐ Wildcard

☐ Permit peer identification and certificate payload identification mismatch

Certificate Profile: clients_cert

☐ Enable strict validation of peer's extended key use

Comment:

OK Cancel

Figura 5-16: Configuración IKE Gateway (General)

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

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

Por último, se asocia el *IKE peer* con el *IKE Crypto profile* creado anteriormente:

IKE Gateway ⓘ

General | **Advanced Options**

Common Options

☐ Enable Passive Mode

☐ Enable NAT Traversal

IKEv1

Exchange Mode: auto

IKE Crypto Profile: IKESecure

☐ Enable Fragmentation

☒ **Dead Peer Detection**

Interval: 5

Retry: 5

OK Cancel

Figura 5-17: Configuración IKE Gateway (Advanced)

2. Perfil criptográfico IPSEC

Ubicación: “Network > Network Profiles > IPsec Crypto”

Requisito de seguridad: Se debe seleccionar los siguientes parámetros:

IPSEC Protocol: ESP

DH Group: Grupo 19 o Grupo 20

Encryption: AES-128 / AES-256

Authentication: SHA256 / SHA384 / SHA512

Lifetime: 1 hora

IPSec Crypto Profile ⓘ

Name: Suite-B-GCM-256

IPSec Protocol: ESP

ENCRYPTION

☐ aes-256-gcm

☐ aes-256-cbc

AUTHENTICATION

☐ sha512

☐ sha384

☒ sha256

DH Group: group20

Lifetime: Hours 1

Minimum lifetime = 3 mins

☐ **Enable**

Lifesize: MB 1

Recommended lifesize is 100MB or greater

OK Cancel

Figura 5-18: Configuración IPsec Crypto Profile

En el apartado 5.12.2 se muestra un ejemplo completo de configuración de una VPN.

5.4.2 TLS/HTTPS

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*.

Ubicación: “*Device > Certificate Management > SSL/TLS Service Profile*”

Figura 5-19: Configuración SSL/TLS Service Profile

Requisito de seguridad: Se debe seleccionar la versión TLSv1.2.

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

5.5 CONFIGURACIÓN DE PROTOCOLOS NO SEGUROS

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

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*”.

Ubicación: “*Network > Network Profiles > Interface Mgmt*”

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.

Figura 5-20: Configuración Perfil interfaz de gestión

5.6 GESTIÓN DE CERTIFICADOS

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

5.6.1 CREAR UN CERTIFICADO DE CA RAÍZ AUTOFIRMADO

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.

Para generar un certificado autofirmado CA:

Ubicación: “*Device > Certificate Management > Certificates > Device Certificates > Generate*”

Requisito de seguridad: El certificado debe utilizar claves RSA o ECDSA de, al menos, la siguiente longitud:

RSA ≥ 3072 bits

ECDSA ≥ 256 bits

Generate Certificate ⓘ

Certificate Type: ☒ Local ☐ SCEP

Certificate Name: CA-ACME

Common Name: acme.com
IP or FQDN to appear on the certificate

Signed By: Certificate Authority

☐ Block Private Key Export

OCSP Responder:

Cryptographic Settings

Algorithm: RSA

Number of Bits: 4096

Digest: sha512

Expiration (days): 365

Certificate Attributes

TYPE	VALUE

+ Add - Delete

Generate Cancel

Figura 5-21: Crear un certificado CA autofirmado

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.

5.6.2 GENERAR UN CERTIFICADO

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.

Ubicación: “Device > Certificate Management > Certificate > Device Certificates > Generate”

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

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.

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

5.6.3 IMPORTAR UN CERTIFICADO Y UNA CLAVE PRIVADA

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).

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.

Ubicación: “Device > Certificate Management > Certificate > Device Certificates > Import”

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)

Una vez generado, aparece con un estado de “Pending” hasta que sea firmado por la CA.

NAME	SUBJECT	ISSUER	CA	KEY	EXPIRES	STATUS	ALGORITHM	USAGE
trust-ca	C = ES, CN = 172.16.24.254	C = ES, CN = 172.16.24.254	☒	☒	Jun 25 15:37:07 2025 GMT	valid	RSA	Forward Trust Certificate
prueba	C = ES, O = Sergio, CN = par...	C = ES, CN = 172.16.24.254	☒	☒	Dec 7 11:43:19 2025 GMT	valid	RSA	
GlobalprotectSer...	CN = acme.com	C = ES, CN = 172.16.24.254	☐	☒	Mar 14 16:58:34 2023 GMT	valid	RSA	
FW1_Management	CN = ngfw1.acme.com	CN = acme.com	☐	☒	Mar 15 16:49:23 2023 GMT	valid	RSA	
untrust-ca	CN = untrusted	CN = untrusted	☒	☒	Apr 22 15:37:49 2021 GMT	expired	RSA	Forward Untrust Certificate
CA-ACME	CN = acme.com	CN = acme.com	☒	☒	Mar 15 16:48:07 2023 GMT	valid	RSA	
MGMT_FW1	fw1.acme.com		☐	☒		pending	RSA	

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

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

5.6.4 COMPROBACIÓN ONLINE DE VALIDEZ DE CERTIFICADOS

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

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

Ubicación: “Device > Certificate Management > Certificate Profile”

Requisito de seguridad: Se deben utilizar las siguientes opciones:

Certificate Profile ⓘ

Name:

Username Field:

User Domain:

CA Certificates

☐	NAME	DEFAULT OCSP URL	OCSP VERIFY CERTIFICATE	TEMPLATE NAME/OID
☐	CA-ACME			

+ Add - Delete ↑ Move Up ↓ Move Down

Default OCSP URL (must start with http:// or https://)

☒ Use CRL CRL Receive Timeout (sec)

☒ Use OCSP OCSP Receive Timeout (sec)

OCSP takes precedence over CRL Certificate Status Timeout (sec)

☒ Block session if certificate status is unknown

☒ Block session if certificate status cannot be retrieved within timeout

☒ Block session if the certificate was not issued to the authenticating device

☒ Block sessions with expired certificates

OK Cancel

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

5.6.5 CONFIGURACIÓN DE LA CADENA DE VALIDACIÓN DE CERTIFICADOS

Ubicación: “Device > Certificate Management > Certificates > Default Trusted Certificate Authorities”

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

Device Certificates | Default Trusted Certificate Authorities

374 items

☐	NAME	SUBJECT	ISSUER	EXPIRES	STATUS
☐	00099_Eintrust_Root_Certification_Authority_-_EC1	Entrust Root Certification Authority - EC1	Entrust Root Certification Authority - EC1	Dec 18 15:55:36 2037 GMT	valid
☐	00091_thawte_Primary_Root_CA_-_G3	thawte Primary Root CA - G3	thawte Primary Root CA - G3	Dec 1 23:59:59 2037 GMT	valid
☐	00092_Certnomis_-_Root_CA	Certnomis - Root CA	Certnomis - Root CA	Oct 21 09:17:18 2033 GMT	valid
☐	00093_PosDigicert_Class_2_Root_CA_G2	PosDigicert Class 2 Root CA G2	PosDigicert Class 2 Root CA G2	Oct 17 03:02:09 2036 GMT	valid
☐	00094_SSC_Root_CA_C	SSC Root CA C	SSC Root CA C	Dec 22 12:11:30 2026 GMT	valid
☐	00095_Saudi_National_Root_CA	/C=SA/O=National Center for Digital Certification/OU=...	/C=SA/O=National Center for Digital Certification/OU=...	Nov 29 07:25:20 2029 GMT	valid
☐	00098_S-TRUST_Universal_Root_CA	S-TRUST Universal Root CA	S-TRUST Universal Root CA	Oct 21 23:59:59 2038 GMT	valid
☐	00099_Eintrust_Root_Certification_Authority_-_G2	Entrust Root Certification Authority - G2	Entrust Root Certification Authority - G2	Dec 7 17:55:54 2030 GMT	valid
☐	01000_CCA_India_2014	CCA India 2014	CCA India 2014	Mar 5 10:10:49 2024 GMT	valid
☐	01001_ISRG_Root_X1	ISRG Root X1	ISRG Root X1	Jun 4 11:04:38 2035 GMT	valid
☐	01002_AOL_Time_Warner_Root_Certification_Authority_2	AOL Time Warner Root Certification Authority 2	AOL Time Warner Root Certification Authority 2	Sep 28 23:43:00 2037 GMT	valid
☐	01004_CA_Disig_Root_R1	CA Disig Root R1	CA Disig Root R1	Jul 19 09:06:56 2042 GMT	valid
☐	01005_Tunisian_Root_Certificate_Authority_-_TunRo...	Tunisian Root Certificate Authority - TunRootCA2	Tunisian Root Certificate Authority - TunRootCA2	May 5 08:57:01 2027 GMT	valid
☐	01006_CA_DATEV_BT_03	CA DATEV BT 03	CA DATEV BT 03	Aug 2 07:40:59 2022 GMT	valid
☐	01007_Starfield_Services_Root_Certificate_Authority_-_G2	Starfield Services Root Certificate Authority - G2	Starfield Services Root Certificate Authority - G2	Dec 31 23:59:59 2037 GMT	valid
☐	01009_Microsoft_Secure_Server_CA_2011	Microsoft Secure Server CA 2011	Microsoft Root Certificate Authority 2011	Oct 18 23:05:19 2026 GMT	valid
☐	01010_Verisign_Class_3_Public_Primary_Certification...	VeriSign Class 3 Public Primary Certification Authority - ...	VeriSign Class 3 Public Primary Certification Authority - ...	Jan 18 23:59:59 2038 GMT	valid

Figura 5-26: Lista preinstalada de certificados de confianza

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.

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.

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.

5.7 SERVIDOR DE AUTENTICACIÓN (AAA SERVER)

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

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 características y, por último, asignarlo a los servicios donde se desee aplicar.

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

Ubicación: “Device > Server Profiles > RADIUS”

RADIUS Server Profile

Profile Name:

☐ Administrator Use Only

Server Settings

Timeout (sec):

Retries:

Authentication Protocol:

Servers

NAME	RADIUS SERVER	SECRET	PORT
RADIUS10	10.101.2.10	*****	1812
RADIUS11	10.101.2.11	*****	1812

Enter the IP address or FQDN of the RADIUS server

Figura 5-27: Configuración del RADIUS Server

Ubicación: “Device > Authentication Profile”

Figura 5-28: Configuración del perfil de autenticación

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)

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

5.8 REGISTRO DE EVENTOS (AUDITORÍA)

5.8.1 GENERACIÓN DE REGISTROS

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.

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

Ubicación: “*Policies > Security > Security Policy Rule > Actions*”

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

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).

1. Logs de Sistema

Formato:

FUTURE_USE, Receive Time, Serial Number, Type, Content/Threat Type, FUTURE_USE, Generated Time, Virtual System, Event ID, Object, FUTURE_USE, FUTURE_USE, Module, Severity, Description, Sequence Number, Action Flags, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name

Logs de Sistema	
Campo	Descripción
<i>Receive Time</i>	Hora en la que en log fue recibido en el plano de control.
<i>Serial Number (Serial #)</i>	Número de serie del cortafuegos que generó el log.
<i>Type</i>	Tipo de registro. Los valores son <i>traffic, threat, config, system</i> y <i>hip-match</i> .
<i>Content/Threat Type</i>	Subtipo de registro. Se refiere al proceso del sistema que genera el log. Los valores son: <i>crypto, dhcp, dnsproxy, dos, general, global-protect, ha, hw, nat, ntpd, pbf, port, pppoe, ras, routing, satd, sslmgr, sslvpn, userid, url-filtering, vpn</i> .
<i>Generated Time</i>	Hora en que se generó el registro en el plano de datos.
<i>Virtual System</i>	Sistema virtual asociado al registro.
<i>Event ID</i>	Id del evento.
<i>Object</i>	Nombre del objeto asociado al evento.

Logs de Sistema	
Campo	Descripción
<i>Module</i>	Este campo es válido solo cuando el valor del campo Subtipo es general. Proporciona información adicional sobre el subsistema que genera el log. Los valores son: <i>general, management, auth, ha, upgrade, chassis</i> .
<i>Severity</i>	Gravedad asociada al evento. Los valores son: <i>informational, low, medium, high, critical</i> .
<i>Description</i>	Descripción detallada del evento, hasta un máximo de 512 bytes.
<i>Sequence Number</i>	Identificador de entrada de registro de 64 bits, que se incrementa secuencialmente. Cada tipo de registro tiene un espacio de número único.
<i>Action Flags</i>	Campo de bits que indica si el registro se reenvió a Panorama.
<i>Device Group Hierarchy (dg_hier_level_1 to dg_hier_level_4)</i>	Secuencia de números de identificación que indican la localización del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o el sistema virtual) que genera el log, incluye el número de identificación de cada dispositivo anterior en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartido (nivel 0) no está incluido en esta estructura.
<i>Virtual System Name</i>	El nombre del sistema virtual asociado a la sesión. Sólo válido para cortafuegos habilitados para múltiples sistemas virtuales.
<i>Device Name</i>	<i>Hostname</i> del cortafuegos en el que se registró la sesión.

Tabla 2: Logs de Sistema

2. Logs de Configuración

Formato:

FUTURE_USE, Receive Time, Serial Number, Type, Subtype, FUTURE_USE, Generated Time, Host, Virtual System, Command, Admin, Client, Result, Configuration Path, Sequence Number, Action Flags, Before Change Detail, After Change Detail, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name

Logs de Configuración	
Campo	Descripción
<i>Receive Time</i>	Hora en la que en log fue recibido en el plano de control.

Logs de Configuración	
Campo	Descripción
<i>Serial Number (Serial #)</i>	Número de serie del cortafuegos que generó el log.
<i>Type</i>	Tipo de registro. Los valores son traffic, threat, config, system y hip-match.
<i>Content/Threat Type</i>	Subtipo de log de configuración. No se usa.
<i>Generated Time</i>	Hora en que se generó el registro en el plano de datos.
<i>Host</i>	Hostname o dirección IP de la máquina cliente.
<i>Virtual System</i>	Sistema virtual asociado al registro.
<i>Command (cmd)</i>	Comando ejecutado por el administrador. Los valores son: <i>add</i> , <i>clone</i> , <i>commit</i> , <i>delete</i> , <i>edit</i> , <i>move</i> , <i>rename</i> , <i>set</i> .
<i>Admin</i>	Username del administrador que realiza la configuración.
<i>Client</i>	Cliente usado por el administrador: Web o CLI.
<i>Result</i>	Resultado de la acción de configuración. Los valores son: <i>Submitted</i> , <i>Succeeded</i> , <i>Failed</i> , y <i>Unauthorized</i> .
<i>Configuration Path</i>	Path del comando de configuración.
<i>Before Change Detail</i>	Solo para logs customizados, no se encuentra en el formato por defecto. Contiene el <i>xpath</i> completo antes del cambio en la configuración.
<i>After Change Detail</i>	Solo para logs customizados, no se encuentra en el formato por defecto. Contiene el <i>xpath</i> completo después del cambio en la configuración.
<i>Sequence Number</i>	Identificador de entrada de registro de 64 bits, que se incrementa secuencialmente. Cada tipo de registro tiene un espacio de número único.
<i>Action Flags</i>	Campo de bits que indica si el registro se reenvió a Panorama.
<i>Device Group Hierarchy (dg_hier_level_1 to dg_hier_level_4)</i>	Secuencia de números de identificación que indican la localización del grupo de dispositivos dentro de una jerarquía de grupos de dispositivos. El cortafuegos (o el sistema virtual) que genera el log, incluye el número de identificación de cada dispositivo anterior en su jerarquía de grupos de dispositivos. El grupo de dispositivos compartido (nivel 0) no está incluido en esta estructura.

Logs de Configuración	
Campo	Descripción
<i>Virtual System Name</i>	El nombre del sistema virtual asociado a la sesión. Sólo válido para cortafuegos habilitados para múltiples sistemas virtuales.
<i>Device Name</i>	<i>Hostname</i> del cortafuegos en el que se registró la sesión.

Tabla 3: Logs de Configuración

3. Logs de tráfico

Formato:

FUTURE_USE, Receive Time, Serial Number, Type, Threat/Content Type, FUTURE_USE, Generated Time, Source IP, Destination IP, NAT Source IP, NAT Destination IP, Rule Name, Source User, Destination User, Application, Virtual System, Source Zone, Destination Zone, Inbound Interface, Outbound Interface, Log Forwarding Profile, FUTURE_USE, Session ID, Repeat Count, Source Port, Destination Port, NAT Source Port, NAT Destination Port, Flags, Protocol, Action, Bytes, Bytes Sent, Bytes Received, Packets, Start Time, Elapsed Time, Category, FUTURE_USE, Sequence Number, Action Flags, Source Location, Destination Location, FUTURE_USE, Packets Sent, Packets Received, Session End Reason, Device Group Hierarchy Level 1, Device Group Hierarchy Level 2, Device Group Hierarchy Level 3, Device Group Hierarchy Level 4, Virtual System Name, Device Name, Action Source, Source VM UUID, Destination VM UUID, Tunnel ID/IMSI, Monitor Tag/IMEI, Parent Session ID, Parent Start Time, Tunnel Type

Logs de Tráfico	
Campo	Descripción
<i>Receive Time</i>	Hora en la que en log fue recibido en el plano de control.
<i>Serial Number (Serial #)</i>	Número de serie del cortafuegos que generó el log.
<i>Type</i>	Tipo de log. Los valores son <i>traffic</i> , <i>threat</i> , <i>config</i> , <i>system</i> y <i>hip-match</i> .
<i>Content/Threat Type</i>	Subtipo de log. Los valores son: • <i>Start</i>—Sesión iniciada. • <i>End</i>—Sesión finalizada. • <i>Drop</i>—Sesión rechazada antes que la aplicación fuera identificada y cuando no existe regla que permita la sesión. • <i>Deny</i>— Sesión rechazada tras identificar la aplicación y cuando existe una regla que bloquea, o no existe regla que permita la sesión.
<i>Generated Time</i>	Hora en que se generó el registro en el plano de datos.

Logs de Tráfico	
Campo	Descripción
<i>Source Address</i>	IP origen original de la sesión.
<i>Destination Address</i>	IP destino original de la sesión.
<i>NAT Source IP</i>	Si existe NAT en Origen, la IP tras realizar el NAT.
<i>NAT Destination IP</i>	Si existe NAT en Destino, la IP tras realizar el NAT.
<i>Rule Name (Rule)</i>	Nombre de la regla con la que hizo match la sesión.
<i>Source User</i>	Nombre de usuario que inició la sesión
<i>Destination User</i>	Nombre de usuario destino de la sesión.
<i>Application</i>	Aplicación asociada a la sesión.
<i>Virtual System</i>	Sistema virtual asociado a la sesión.
<i>Source Zone</i>	Zona origen de la sesión.
<i>Destination Zone</i>	Zona destino de la sesión.
<i>Inbound Interface</i>	Interfaz origen de la sesión.
<i>Outbound Interface</i>	Interfaz destino de la sesión.
<i>Log Action</i>	Perfil de envío (<i>Forwarding profile</i>) aplicado a la sesión.
<i>Session ID</i>	Identificador numérico interno aplicado a la sesión.
<i>Repeat Count</i>	Solo para ICMP. Número de sesiones con la misma IP de origen, IP de destino, Aplicación, y subtipo, en el margen de 5 segundos.
<i>Source Port</i>	Puerto origen de la sesión.
<i>Destination Port</i>	Puerto destino de la sesión.
<i>NAT Source Port</i>	Puerto origen tras realizar el NAT.
<i>NAT Destination Port</i>	Puerto destino tras realizar en NAT.
Flags	Campo de 32 bits que proporciona detalles sobre la sesión. Este campo puede ser decodificado haciendo un AND a los valores con el valor registrado: 0x80000000 —La sesión tiene una captura de paquetes (PCAP). 0x02000000 —sesión IPv6.

Logs de Tráfico	
Campo	Descripción
	• <i>0x01000000</i> —La sesión SSL fué descifrada (<i>SSL Proxy</i>). • <i>0x00800000</i> —La sesión fué denegada vía filtrado URL. • <i>0x00400000</i> —Se ha realizado NAT en la sesión. • <i>0x00200000</i> —Se ha capturado información de usuario en la sesión, a través del Portal Cautivo. • <i>0x00080000</i> —En el campo origen hay un valor procedente de un proxy (<i>X-Forwarded-For value</i>). • <i>0x00040000</i> —El log corresponde a una transacción dentro de una sesión proxy http (<i>Proxy Transaction</i>). • <i>0x00008000</i> —La sesión contiene una página de acceso (<i>Container Page</i>). • <i>0x00002000</i> —La sesión tiene una coincidencia temporal con una regla con una dependencia implícita de aplicación. • <i>0x00000800</i> —Se ha utilizado un retorno simétrico para reenviar el tráfico para esta sesión.
IP Protocol	Protocolo IP asociado a esta sesión.
Action	Acción realizada para esta sesión; Los posibles valores son: • <i>Allow</i>— Sesión permitida por política. • <i>Deny</i>— Sesión denegada por política. • <i>Drop</i>— Sesión descartada. • <i>Drop ICMP</i>— Sesión descartada con un mensaje "<i>ICMP unreachable</i>" al <i>host</i> origen. • <i>Reset both</i>— Sesión terminada y se envió un TCP reset a los dos lados de la conexión. • <i>Reset client</i>— Sesión terminada y se envió un TCP reset al cliente. • <i>Reset server</i>— Sesión terminada y se envió un TCP reset al servidor.
Bytes	Número total de bytes (transmitidos y recibidos) por la sesión.
Bytes Sent	Número de bytes enviados de cliente a servidor. Disponible en todos los modelos excepto la serie PA-4000.
Bytes Received	Número de bytes enviados de servidor a cliente. Disponible en todos los modelos excepto la serie PA-4000.
Packets	Número total de paquetes (transmitidos y recibidos) por la sesión.

Logs de Tráfico	
Campo	Descripción
<i>Start Time</i>	Hora del inicio de la sesión.
<i>Elapsed Time (sec)</i>	Duración de la sesión.
<i>Category</i>	Categoría URL asociada a la sesión (si aplica).
<i>Sequence Number</i>	Identificador de entrada de registro de 64 bits, que se incrementa secuencialmente. Cada tipo de registro tiene un espacio de número único.
<i>Action Flags</i>	Campo de bits que indica si el registro se reenvió a Panorama.
<i>Source Country</i>	País de origen o región interna para direcciones privadas.
<i>Destination Country</i>	País de destino o región interna para direcciones privadas.
<i>Packets Sent</i>	Número de paquetes enviados de cliente a servidor. Disponible en todos los modelos excepto la serie PA-4000.
<i>Packets Received</i>	Número de paquetes enviados de servidor a cliente. Disponible en todos los modelos excepto la serie PA-4000.
<i>Session End Reason</i>	Razón por la que una sesión terminó. Si las causas fueron múltiples, este campo solo muestra la razón con la prioridad más alta. Los posibles valores son (ordenados en orden de prioridad): • threat— El cortafuegos ha detectado una amenaza asociada con una acción de reset, drop o block. • policy-deny— La sesión ha hecho match con una regla con una acción de deny o drop. • decrypt-cert-validation— La sesión finalizó porque el cortafuegos está configurado para bloquear el descifrado de SSL <i>forward proxy</i> o la inspección de entrada de SSL (<i>SSL inbound inspection</i>), cuando la sesión utiliza la autenticación del cliente, o cuando la sesión utiliza un certificado de servidor con alguna de las siguientes condiciones: expirado, no confiable, estado desconocido, o se produce un timeout en la verificación. Este motivo de finalización de la sesión se muestra también cuando se produce una alerta de error fatal del tipo <i>bad_certificate</i>, <i>unsupported_certificate</i>, <i>certificate_revoked</i>, <i>access_denied</i> o <i>no_certificate_RESERVED</i> (SSLv3 únicamente). • decrypt-unsupported-param— La sesión finalizó porque el cortafuegos está configurado para bloquear el descifrado de SSL

Logs de Tráfico	
Campo	Descripción
	<i>forward proxy</i> o la inspección de entrada de SSL (<i>SSL inbound inspection</i>) cuando la sesión utiliza una versión de protocolo, cifrado o algoritmo SSH no soportados. Este motivo de finalización de la sesión se muestra también cuando se produce una alerta de error fatal del tipo <i>unsupported_extension</i>, <i>unexpected_message</i> o <i>handshake_failure</i>. • decrypt-error—La sesión finalizó porque el cortafuegos está configurado para bloquear el descifrado de SSL <i>forward proxy</i> o la inspección de entrada de SSL (<i>SSL inbound inspection</i>) cuando los recursos o el módulo de seguridad de hardware (HSM) no estaba disponibles. Esta razón de finalización también se muestra cuando el cortafuegos está configurado para bloquear el tráfico SSL que tiene errores SSH o cuando se produce una alerta de error fatal distinta de las enumeradas en <i>decrypt-cert-validation</i> y <i>decrypt-unsupported-param</i>. • tcp-rst-from-client—El Cliente ha enviado un TCP reset al servidor • tcp-rst-from-server—EL servidor ha enviado un TCP reset al cliente. • resources-unavailable— La sesión se ha descartado debido a una limitación de recursos del sistema. Por ejemplo, la sesión podría haber excedido el número de paquetes out-of-order permitidos por flujo. • tcp-fin— Uno o ambos hosts en la conexión enviaron un mensaje TCP FIN para cerrar la sesión. • tcp-reuse— Se reutiliza una sesión y el cortafuegos cierra la sesión anterior. • decoder— El decodificador detecta una nueva conexión dentro del protocolo (como HTTP-Proxy) y finaliza la conexión anterior. • aged-out— La sesión ha caducado. • unknown— Este valor se aplica en las siguientes situaciones: ○ Sesiones finalizadas por algún motivo que las razones anteriores no cubren. ○ Para los registros generados en una versión de PAN-OS que no soporta el campo de <i>Session End Reason</i> (versiones anteriores a PAN-OS 6.1).

Logs de Tráfico	
Campo	Descripción
	○ En Panorama, los registros recibidos de los cortafuegos para los cuales la versión de PAN-OS no soporta el campo <i>Session End Reason</i>. ○ n/a— Este valor se aplica cuando el registro de tráfico no ha finalizado.
<i>Device Group Hierarchy (dg_hier_level_1 to dg_hier_level_4)</i>	Una secuencia de números identificativos que indican la ubicación del grupo de dispositivos dentro de una jerarquía de grupo.
<i>Virtual System Name</i>	El nombre del sistema virtual asociado a la sesión. Sólo válido para cortafuegos habilitados para múltiples sistemas virtuales.
<i>Device Name</i>	Hostname del cortafuegos en el que se registró la sesión.
<i>Action Source</i>	Especifica si la acción realizada para permitir o bloquear una aplicación, estaba definida en la aplicación o en la política. Las acciones pueden ser <i>allow</i> , <i>deny</i> , <i>drop</i> , <i>reset-server</i> , <i>reset-client</i> o <i>reset-both</i> .
<i>Source VM UUID</i>	Identifica el identificador único universal (UUID) de origen para una Máquina virtual en el entorno <i>VMware NSX</i> .
<i>Destination VM UUID</i>	Identifica el identificador único universal (UUID) de destino para una Máquina virtual en el entorno <i>VMware NSX</i> .
<i>Tunnel ID/IMSI</i>	ID del túnel que se está inspeccionando, o el International Mobile Subscriber Identity (IMSI) ID del dispositivo móvil.
<i>Monitor Tag/IMEI</i>	Nombre del monitor que configuró para la regla de la política de inspección de túneles o el ID de identidad de equipo móvil internacional (IMEI) del dispositivo móvil.
<i>Parent Session ID</i>	ID de la sesión en la que esta sesión está tunelizada. Se aplica al Túnel interno (si hay dos niveles de tunelización) o contenido interno (si hay un nivel de tunelización).
<i>Tunnel Type (Tunnel)</i>	Tipo de túnel, como IPsec o GRE.

Tabla 4: Logs de tráfico

4. Ejemplo de eventos auditable

Evento Auditable	Ejemplo	Fichero de Log
Fallo en el establecimiento de una IPSEC SA. Contenido adicional del registro de auditoría: <i>Causa del fallo</i>	<i>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</i>	<i>System</i>
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.	<i>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.</i>	<i>System</i>
Fallo de establecimiento de una sesión TLS. Contenido adicional del registro de auditoría: <i>Causa del fallo</i>	<i>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.</i>	<i>System</i>
Uso de mecanismos de identificación y autenticación. Contenido adicional del registro de auditoría: <i>Origen de la petición (p.e Dirección IP)</i>	Password Successful Login <i>11/16 06:33:06 auth informational auth- success authenticated for user 'admin'. From: 192.168.1.99</i> Certificate Successful Login <i>11/07 08:22:03 auth informational auth- success Certificate validated for user 'certAdmin'. From:192.168.1.99</i> Unsuccessful Login <i>11/07 07:03:45 auth medium auth-fail failed</i>	<i>System</i>

Evento Auditable	Ejemplo	Fichero de Log
	<i>authentication for user 'certAdmin'. Reason: Invalid username/password. From: 192.168.1.99</i>	
Intento fallido de validación de certificado. Contenido adicional del registro de auditoría: <i>Causa del fallo</i>	<i>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</i>	System
Sesión establecida con una CA. Contenido adicional del registro de auditoría: <i>Contenido completo de todos los paquetes transmitidos y recibidos durante el establecimiento de la sesión.</i>	<i>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]</i>	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.	<i>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</i>	Traffic
Indicación de paquetes descartados debido a excesivo tráfico de red (flooding). Contenido adicional del registro de auditoría: <i>Interfaz incapaz de procesar el tráfico, identificador de la</i>	<i>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</i>	Threat

Evento Auditable	Ejemplo	Fichero de Log
<i>regla que ha causado el descarte (drop).</i>		
APP-ID utilizado con el protocolo procesado. Contenido adicional del registro de auditoría: <i>Nombre del protocolo.</i>	<i>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</i>	Traffic
Modificación de la configuración de envío de registros de log a servidor de auditoría externo.	<i>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; } } }</i> <i>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; } } }</i>	Configuration
Intento de actualización manual.	<i>11/07 12:11:53 general informational general Installed panos software version 8.0.5</i>	System
Habilitación o deshabilitación de actualizaciones automáticas.	Disabling <i>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 :</i> Enabling <i>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; } }</i>	Configuration
Generación, modificación o importación de claves criptográficas.	Import/Generation <i>09/07 08:47:58 admin 192.168.1.99 Web upload config shared certificate noCRLSign noCRLSign { private-key *****;}</i> Deletion <i>11/17 05:47:44 admin 192.168.1.99 Web delete Succeeded config shared certificate lientRSA2</i>	System
Cambios en la hora del cortafuegos. Contenido adicional del registro de	<i>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</i>	Configuration

Evento Auditable	Ejemplo	Fichero de Log
auditoría: Valores antiguos y nuevos, origen del cambio (p.e dirección IP).		
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: Identificación del que inicia el canal y del objetivo del intento fallido de establecimiento del canal.	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: 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.	System

Tabla 5: Eventos Auditables

5. Ejemplo de acciones de administración auditables

Acción del Administrador	Menú GUI	Log Generado
Inicio o apagado del cortafuegos.	<i>Device->Setup->Operations->Device Operations->Shutdown Device</i>	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.	<i>Device->Setup->Management->General Settings->Time</i>	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.	<i>Device->Log Settings->System->Add->Syslog->Add</i>	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; } } }
Eliminación manual de un fichero de log.	<i>Device->Log Settings->Manage Logs</i>	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.	<i>Device->Setup->Management->Authentication Settings</i>	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.	<i>Device->Certificate Management->SSL/TLS Service Profile</i>	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... {

Acción del Administrador	Menú GUI	Log Generado
		<i>protocol-settings { min-version tls 1-1; max-v 262</i>
Creación de un usuario local.	<i>Device->Administrators</i>	<i>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</i>
Configuración de autenticación local.	<i>Device->Authentication Profile</i>	<i>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</i>
Inicio y verificación de actualizaciones software.	<i>Device->Software</i>	<i>03/20/2018 08:08:43 general informational general Installed panos software version 8.0.6</i>
Configuración del timeout de inactividad.	<i>Device->Setup->Management->Authentication Settings->Idle-timeout</i>	<i>03/20/2018 07:38:15 Web delete Succeeded deviceconfig setting management idle-timeout /config/devices /entry[@name... /deviceconfig /setting /management /idle-timeout 275</i>
Configuración del mensaje de inicio de sesión (login banner).	<i>Device->Setup->Management->Banners and Messages</i>	<i>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</i>
Configuración de IKE / IPsec.	<i>Network->IPSec Tunnels</i>	<i>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; }</i>

Acción del Administrador	Menú GUI	Log Generado
		<i>branch-vpn {auto-key { ipsec-crypto-profile default; } } 1266</i>
Configuración de reglas del cortafuegos.	<i>Policies->Security</i>	<i>03/20/2021 09:00:20 admin 192.168.1.99 Web edit Succeeded 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</i>
Configuración de certificados X.509	<i>Device->Certificate Management->Certificate Profile</i>	<i>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</i>

Tabla 6: Acciones de administración auditable

5.8.2 AUDITORÍA DE CAMBIOS

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.

Ubicación: “Monitor > Logs > Configuration > 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

Running Configuration	Candidate Configuration
...	...
7 role-based {	7 role-based {
8 superuser yes;	8 superuser yes;
9 }	9 }
10 }	10 }
11 }	11 }
12 jldiaz {	12 deleted
13 permissions {	13 deleted
14 role-based {	14 deleted
15 superuser yes;	15 deleted
16 }	16 deleted
17 }	17 deleted
18 authentication-profile LDAP;	18 deleted
19 }	19 deleted
20 jlgomez {	20 deleted
21 permissions {	21 deleted
22 role-based {	22 deleted
23 superuser yes;	23 deleted
24 }	24 deleted
25 }	25 deleted
26 authentication-profile LDAP;	26 deleted
27 }	27 deleted
28 }	28 }
29 }	29 }
30 shared {	30 shared {
31 application;	31 application;
32 application-group;	32 application-group;
...	...
81 report {	81 report {
82 topn 100;	82 topn 100;
...	...
Running config	Candidate config
Context 5	Go

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

5.8.3 ALMACENAMIENTO LOCAL

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.

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:

Ubicación: “Device > Setup > Management > Logging and Reporting Settings”

Logging and Reporting Settings

Log Storage | Log Export and Reporting | Pre-Defined Reports | Log Collector Status

Log Storage Quota

	Quota(%)	Quota(GB/MB)	Max Days			
Traffic	27	1.44 GB	[1 - 2000]	Traffic Summary	3.5	191.76 MB [1 - 2000]
Threat	11	602.69 MB	[1 - 2000]	Threat Summary	2	109.58 MB [1 - 2000]
Config	4	219.16 MB	[1 - 2000]	GTP and Tunnel Summary	1.5	82.19 MB [1 - 2000]
System	4	219.16 MB	[1 - 2000]	URL Summary	2	109.58 MB [1 - 2000]
Alarm	3	164.37 MB	[1 - 2000]	Decryption Summary	DESUM_1	0.00 MB [1 - 2000]
App Stats	4	219.16 MB	[1 - 2000]	Hourly Traffic Summary	1.5	82.19 MB [1 - 2000]
HIP Match	3	164.37 MB	[1 - 2000]	Hourly Threat Summary	1.5	82.19 MB [1 - 2000]
GlobalProtect	1.5	82.19 MB	[1 - 2000]	Hourly GTP and Tunnel Summary	1	54.79 MB [1 - 2000]
App Pcaps	1.5	82.19 MB	[1 - 2000]	Hourly URL Summary	1.5	82.19 MB [1 - 2000]
Extended Threat Pcaps	1.5	82.19 MB	[1 - 2000]	Hourly Decryption Summary	0	0.00 MB [1 - 2000]
Debug Filter Pcaps	1.5	82.19 MB	[1 - 2000]	Daily Traffic Summary	1.5	82.19 MB [1 - 2000]
IP-Tag	1.5	82.19 MB	[1 - 2000]	Daily Threat Summary	1.5	82.19 MB [1 - 2000]
User-ID	1.5	82.19 MB	[1 - 2000]	Daily GTP and Tunnel Summary	1	54.79 MB [1 - 2000]
HIP Reports	1.5	82.19 MB	[1 - 2000]	Daily URL Summary	1.5	82.19 MB [1 - 2000]
Data Filtering Captures	1.5	82.19 MB	[1 - 2000]	Daily Decryption Summary	0	0.00 MB [1 - 2000]
GTP and Tunnel	2	109.58 MB	[1 - 2000]	Weekly Traffic Summary	1.5	82.19 MB [1 - 2000]
Authentication	1.5	82.19 MB	[1 - 2000]	Weekly Threat Summary	1.5	82.19 MB [1 - 2000]
Decryption	1	54.79 MB	[1 - 2000]	Weekly GTP and Tunnel Summary	1	54.79 MB [1 - 2000]
				Weekly URL Summary	1.5	82.19 MB [1 - 2000]
				Weekly Decryption Summary	0	0.00 MB [1 - 2000]

Total Allocated: 98% (5.24 GB)
Unallocated: 2% (109.58 MB)
Max: 5.35 GB
Core Files: 0 MB

Restore Defaults

Warning: Deletion of logs based on time period may take a long time and during this time the max sustainable log rate will be degraded

OK Cancel

Figura 5-35: Configuración general de logging e informes

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

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.

5.8.4 ALMACENAMIENTO REMOTO

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.

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 v10.2, 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/10-2/pan-os-admin/monitoring/use-syslog-for-monitoring/configure-syslog-monitoring>

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

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

Ubicación: “Device > Server Profiles > Syslog > Syslog Server Profile”

Syslog Server Profile ?

Profile Name

Servers | Custom Log Format

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
default	10.101.10.2	SSL	6514	BSD	LOG_USER

[+ Add](#) [- Delete](#)

Enter the IP address or FQDN of the Syslog server

[OK](#) [Cancel](#)

Figura 5-36: Configuración de perfil de servidor Syslog

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.

Ubicación: “Objects > Log Forwarding Profile”

Log Forwarding Profile ?

Profile Name

Description

8 items → ×

☐	NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
☐	traffic	traffic	All Logs	- Panorama SysLog - default syslog	
☐	threat	threat	All Logs	- Panorama SysLog - default syslog	
☐	wildfire	wildfire	All Logs	- Panorama SysLog - default syslog	
☐	url	url	All Logs	- Panorama SysLog - default syslog	
☐	data	data	All Logs	- Panorama SysLog - default syslog	
☐	decryption	decryption	All Logs	- Panorama SysLog - default syslog	
☐	tunnel	tunnel	All Logs	- Panorama SysLog - default syslog	
☐	auth	auth	All Logs	- Panorama SysLog - default syslog	

[+ Add](#) [- Delete](#) [Clone](#)

[OK](#) [Cancel](#)

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

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

Ubicación: “Policies > Security > Security Policy Rule > Actions”

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Log Forwarding' dropdown menu is highlighted with a red rectangle, indicating the selection of 'Default-logging-profile'. Other visible settings include 'Action' set to 'Allow', 'Log at Session End' checked, and 'Log Forwarding' set to 'Default-logging-profile'.

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

5.9 BACKUPS

Ubicación: “Device > Setup > Operations”

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/10-2/pan-os-admin/firewall-administration/manage-configuration-backups>

5.10 AUTO-CHEQUEOS

Ubicación: “Device > Master Key and Diagnostics”

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

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

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.

5.11 ALTA DISPONIBILIDAD

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).

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.

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.

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.

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/10-2/pan-os-admin/high-availability>

A continuación, se indican unas recomendaciones a 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”

NAME	ENABLED	GROUP FAILURE CONDITION	INTERFACES
enlaces	☒	any	ethernet1/1 ethernet1/2

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*”

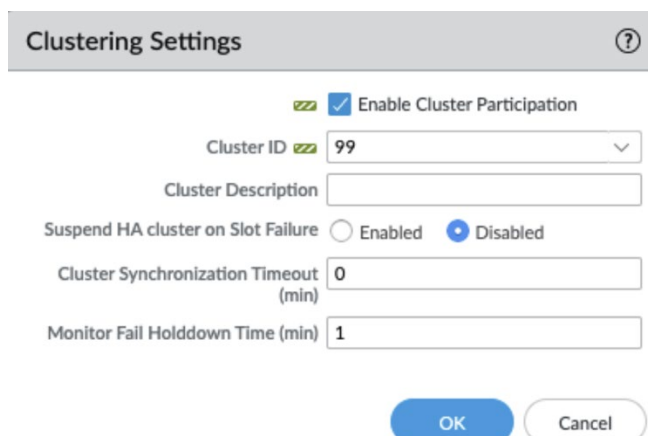
Figura 5-41: Configuración recomendada de Preemption y Passive Link State

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 el que los miembros compartan las sesiones.

Ubicación: “*Device > High Availability > General > Cluster Settings*”



Clustering Settings ⓘ

☒ Enable Cluster Participation

Cluster ID ⓘ 99 ▼

Cluster Description

Suspend HA cluster on Slot Failure ☐ Enabled ☒ Disabled

Cluster Synchronization Timeout (min)

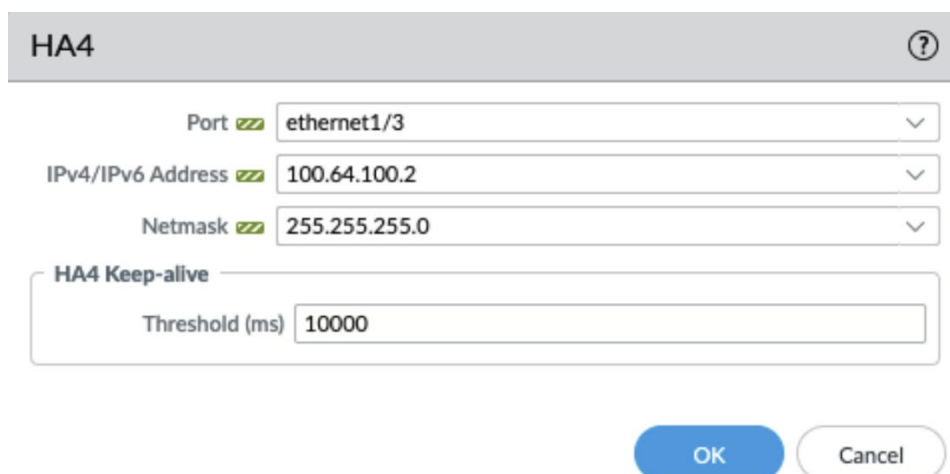
Monitor Fail Holddown Time (min)

OK Cancel

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”



HA4 ⓘ

Port ⓘ ethernet1/3 ▼

IPv4/IPv6 Address ⓘ 100.64.100.2 ▼

Netmask ⓘ 255.255.255.0 ▼

HA4 Keep-alive

Threshold (ms)

OK Cancel

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”

☐	CLUSTER DEVICE ID	DEVICE NAME	HA4 IPV4/IPV6 ADDRESS	HA4-BACKUP IPV4/IPV6 ADDRESS	SESSION SYNCHRONIZATION	DESCRIPTION
☐	007251000176614	PA-VM-HA1	100.64.100.1		enabled	
☐	007251000128671	PA-VM-HA2	100.64.100.2		enabled	
☐	007251000128713	PA-VM-HA3	100.64.100.3		enabled	

Figura 5-45: Configuración de los miembros del clúster

Monitorización del estado del *clúster*

Ubicación: “Dashboard > Widget > Settings > HA Cluster”

HA Cluster

Number of HA Cluster Members

Cluster State

State Details

HA4

HA4 Backup

2

cluster-active

Warning

Not configured or not operational

Session Statistics

Cluster Member

PA-VM-HA3

PA-VM-HA2

PA-VM-HA1

Local Table

N/A

0.012%, 100

N/A

Session Cache

0%, 0

61.983%, 2975174

0%, 0

Peer HA4 Monitoring Status

Cluster Member

PA-VM-HA3

PA-VM-HA1

HA4

0%, 0

0.1%, 10

Keepalive Missed

HA4-Backup

Figura 5-46: Dashboard del clúster

5.12 CONFIGURACIÓN DE LOS SERVICIOS DE SEGURIDAD

5.12.1 FILTRADO DE PAQUETES CON ESTADO (STATEFUL TRAFFIC FILTERING)

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

- *Internet Control Message Protocol version 4 (ICMPv4), RFC 792:*
 - *Type*
 - *Code*
- *Internet Control Message Protocol version 6 (ICMPv6), RFC 4443:*
 - *Type*
 - *Code*

- *Internet Protocol (IPv4), RFC 791:*
 - *Source address*
 - *Destination address*
 - *Transport layer protocol*
- *Internet Protocol version 6 (IPv6), RFC 2460:*
 - *Source address*
 - *Destination address*
 - *Transport layer protocol*
- *Transmission Control Protocol (TCP), RFC 793:*
 - *Source port*
 - *Destination port*
- *User Datagram Protocol (UDP), RFC 768:*
 - *Source port*
 - *Destination port*

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.

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.

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

- *Action: "Allow" o "Deny".*
- *Profiles.* Especifica cualquier chequeo adicional que debe ser realizado por los perfiles de seguridad como *IPsec crypto Security*, *IKE Network Security*. Estos perfiles permiten o requieren que el tráfico de red sea protegido.
- *Options—* Especifica las opciones adicionales de procesamiento para el tráfico que coincida con esa regla de la política de seguridad:
 - *Log Setting.* Selecciona el perfil de logs que se le aplicará a esa sesión.
 - *Schedule—* Limita los días y horas en los que la regla es efectiva.
 - *QoS Marking—* Modifica las marcas de calidad de servicio al tráfico que coincida con esta regla.

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

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).

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.

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).

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 [5.13.1. ATAQUES DOS](#)

5.12.2 VPNS

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 Protect* 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.

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

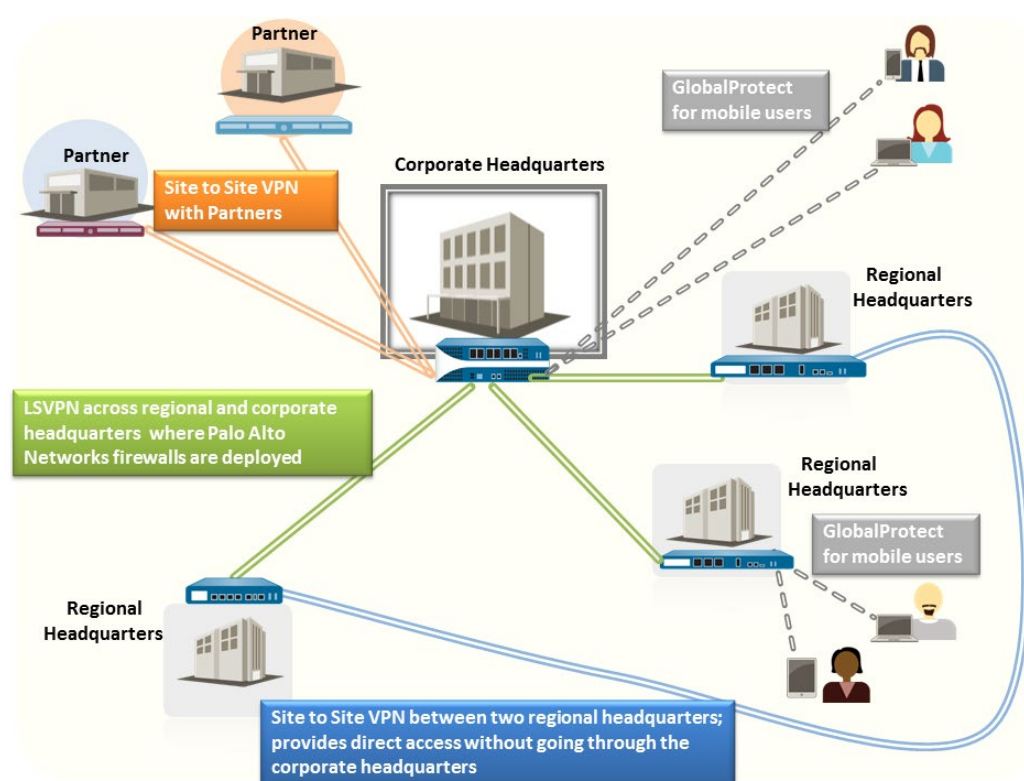


Figura 5-47: Tipos de VPNs soportadas

5.12.2.1 SITE-TO-SITE VPN

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).

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.

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

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.

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.

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.

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

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

Ubicación: “*Network > Interface > Tunnel*”

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.

The screenshot shows the 'Tunnel Interface' configuration window. At the top, there's a title bar 'Tunnel Interface' with a help icon. Below it, the 'Interface Name' is set to 'tunnel' and '1'. There's a 'Comment' field and a 'Netflow Profile' dropdown set to 'None'. Below these are tabs for 'Config', 'IPv4', 'IPv6', and 'Advanced'. The 'Config' tab is active, showing the 'Assign Interface To' section. This section has two dropdowns: 'Virtual Router' set to 'default' and 'Security Zone' set to 'corp-vpn'. At the bottom right, there are 'OK' and 'Cancel' buttons.

Figura 5-48: Configuración de interfaces tunnel

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 5.4.1. 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.

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.

Ubicación: “Network > IPsec Tunnel”

The screenshot shows the 'IPsec Tunnel' configuration window with the 'General' tab selected. The fields are as follows:

- Name: IPsec-tunnel
- Tunnel Interface: tunnel1
- Type: ☒ Auto Key, ☐ Manual Key, ☐ GlobalProtect Satellite
- Address Type: ☒ IPv4, ☐ IPv6
- IKE Gateway: IKE-Gateway
- IPsec Crypto Profile: IPsec-Crypto-Profile
- ☐ Show Advanced Options
- Comment: (empty)

Buttons: OK, Cancel

Figura 5-49: 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).

The screenshot shows the 'IPsec Tunnel' configuration window with the 'Proxy IDs' tab selected. The 'IPv4' sub-tab is active, showing a table with the following data:

PROXY ID	LOCAL	REMOTE	PROTOCOL
☒ Tunnelled-Traffic	192.168.1.0/24	192.168.2.0/24	any

Buttons: Add, Delete, OK, Cancel

Figura 5-50: Configuración de Proxy-ID (opcional)

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.

Ubicación: “Network > Virtual Routers”

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.

Virtual Router - Static Route - IPv4

Name: Remote-Network

Destination: 192.168.2.0/24

Interface: tunnel1

Next Hop: None

Admin Distance: 10 - 240

Metric: 10

Route Table: Unicast

☐ Path Monitoring

Failure Condition: ☒ Any ☐ All Preemptive Hold Time (min): 2

☐	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
Add Delete						

OK Cancel

Figura 5-51: 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>

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).

Ubicación: “Network > IPsec Tunnels”

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):

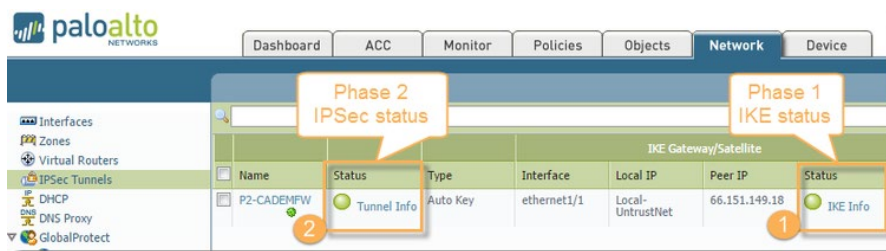


Figura 5-52: Comprobación del estado del túnel IPSEC

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.

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

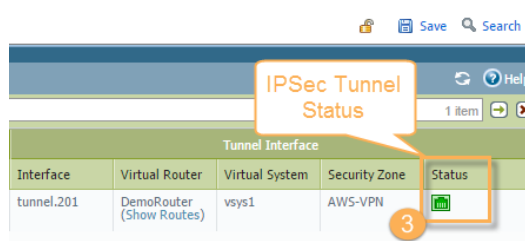


Figura 5-53: Comprobación del estado del túnel IPSEC

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).

5.12.2.2 REMOTE USER-TO-SITE VPN (GLOBALPROTECT)

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.

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:

<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 los siguientes enlaces de versiones 10.1 y posteriores:

<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>

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:

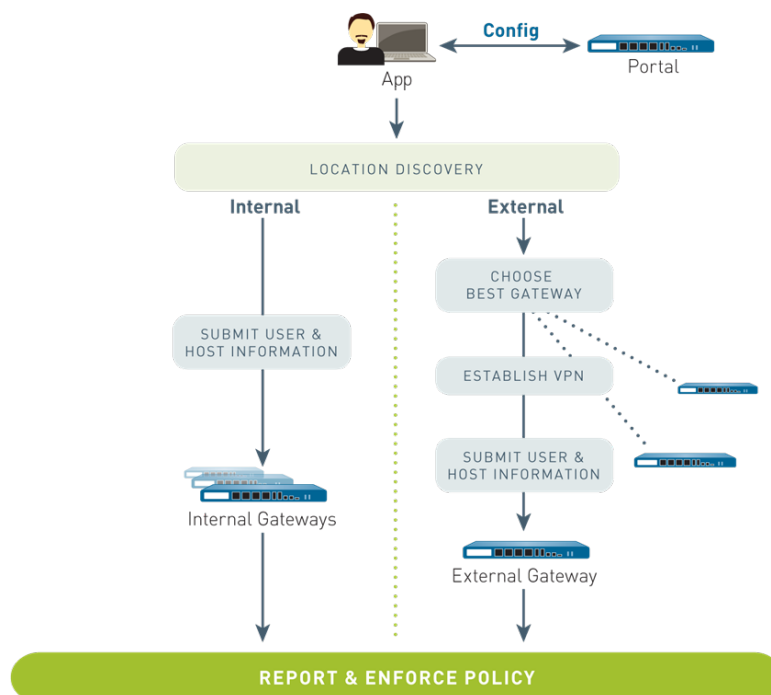


Figura 5-54: Componentes de GlobalProtect

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/10-0/globalprotect-admin.html>

1. Configuraciones previas

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

Ubicación: “*Network > IPsec Tunnels*”

The screenshot shows the 'Tunnel Interface' configuration window. The 'Interface Name' field contains 'tunnel' and the 'Comment' field contains 'GP Portal'. The 'Netflow Profile' is set to 'None'. Below these fields are tabs for 'Config', 'IPv4', 'IPv6', and 'Advanced', with 'Config' being the active tab. Under the 'Assign Interface To' section, the 'Virtual Router' is set to 'default' and the 'Security Zone' is set to 'Corp_VP'. At the bottom right, there are 'OK' and 'Cancel' buttons.

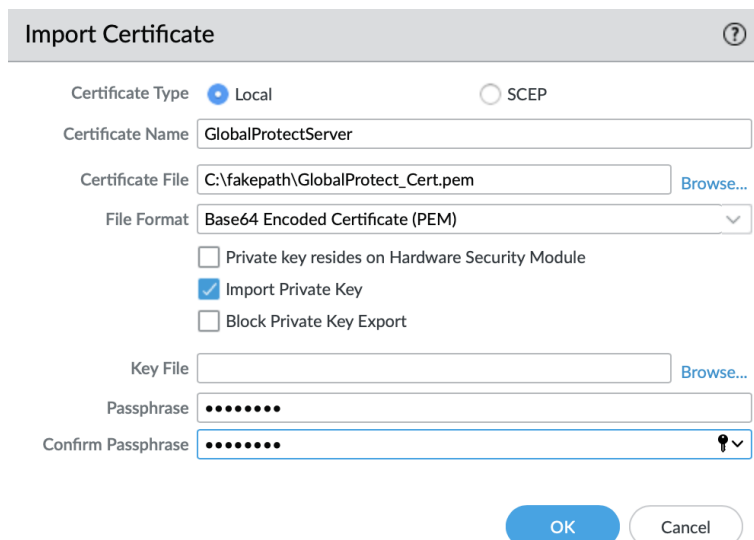
Figura 5-55: Configuración de interface tunnel

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.

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.

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:

Ubicación: “*Device > Certificate Management > Certificates*”



The 'Import Certificate' dialog box is shown with the following fields and options:

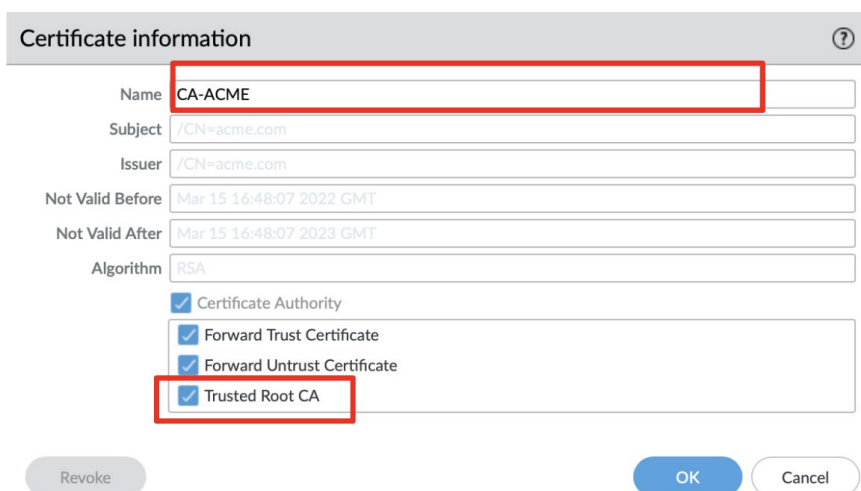
- Certificate Type:** Local (selected), SCEP
- Certificate Name:** GlobalProtectServer
- Certificate File:** C:\fakepath\GlobalProtect_Cert.pem (with a 'Browse...' button)
- File Format:** Base64 Encoded Certificate (PEM)
- Options:**
 - ☐ Private key resides on Hardware Security Module
 - ☒ Import Private Key
 - ☐ Block Private Key Export
- Key File:** (with a 'Browse...' button)
- Passphrase:** (masked with dots)
- Confirm Passphrase:** (masked with dots and a key icon)

Buttons: OK, Cancel

Figura 5-56: Importación de certificado

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

Ubicación: "Device > Certificate Management > Certificate"



The 'Certificate information' dialog box is shown with the following fields and options:

- Name:** CA-ACME (highlighted with a red box)
- Subject:** /CN=acme.com
- Issuer:** /CN=acme.com
- Not Valid Before:** Mar 15 16:48:07 2022 GMT
- Not Valid After:** Mar 15 16:48:07 2023 GMT
- Algorithm:** RSA
- Options:**
 - ☒ Certificate Authority
 - ☒ Forward Trust Certificate
 - ☒ Forward Untrust Certificate
 - ☒ Trusted Root CA (highlighted with a red box)

Buttons: Revoke, OK, Cancel

Figura 5-57: Generación de CA autofirmada

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

Figura 5-58: Generación de certificado autofirmado

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

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 5.6.

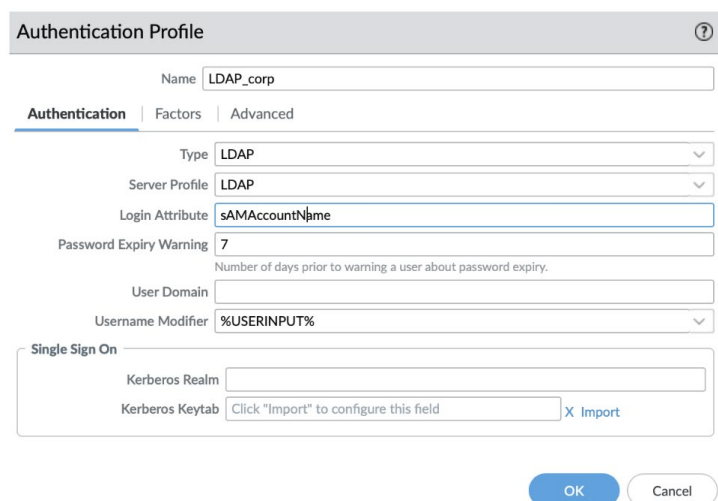
A continuación, crear el *SSL/TLS Service Profile*:

Ubicación: “*Device > Certificate Management > SSL/TLS Service Profile*”

Figura 5-59: Creación de perfil SSL/TLS

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

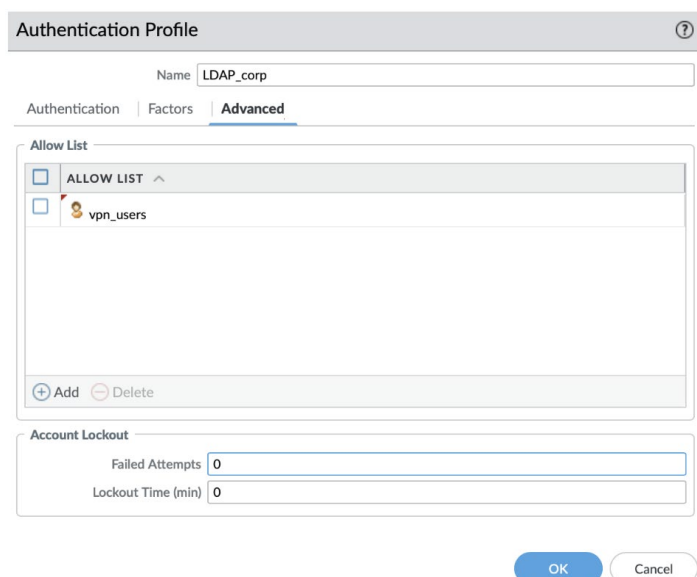
Ubicación: “Device > Authentication Profile”



The screenshot shows the 'Authentication Profile' configuration window with the 'Authentication' tab selected. The 'Name' field is set to 'LDAP_corp'. The 'Type' is 'LDAP'. The 'Server Profile' is 'LDAP'. The 'Login Attribute' is 'sAMAccountName'. The 'Password Expiry Warning' is '7'. The 'User Domain' is empty. The 'Username Modifier' is '%USERINPUT%'. The 'Single Sign On' section is expanded, showing 'Kerberos Realm' and 'Kerberos Keytab' fields. The 'Kerberos Keytab' field has a button 'X Import' next to it. At the bottom are 'OK' and 'Cancel' buttons.

Figura 5-60: Creación de perfil de autenticación (Authentication)

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):



The screenshot shows the 'Authentication Profile' configuration window with the 'Advanced' tab selected. The 'Name' field is set to 'LDAP_corp'. The 'Allow List' section is expanded, showing a list with a checkbox and the text 'ALLOW LIST' and 'vpn_users'. Below the list are 'Add' and 'Delete' buttons. The 'Account Lockout' section is expanded, showing 'Failed Attempts' and 'Lockout Time (min)' fields, both set to '0'. At the bottom are 'OK' and 'Cancel' buttons.

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

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.

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

Ubicación: “*Network > Network Profiles > GlobalProtect IPSec Crypto*”

Figura 5-62: Configuración de perfil IPSec de GlobalProtect

Requisito de seguridad: Seguir las recomendaciones realizadas en el apartado 5.4.1, respecto a los algoritmos y funciones criptográficas a utilizar en *IKE/IPsec*.

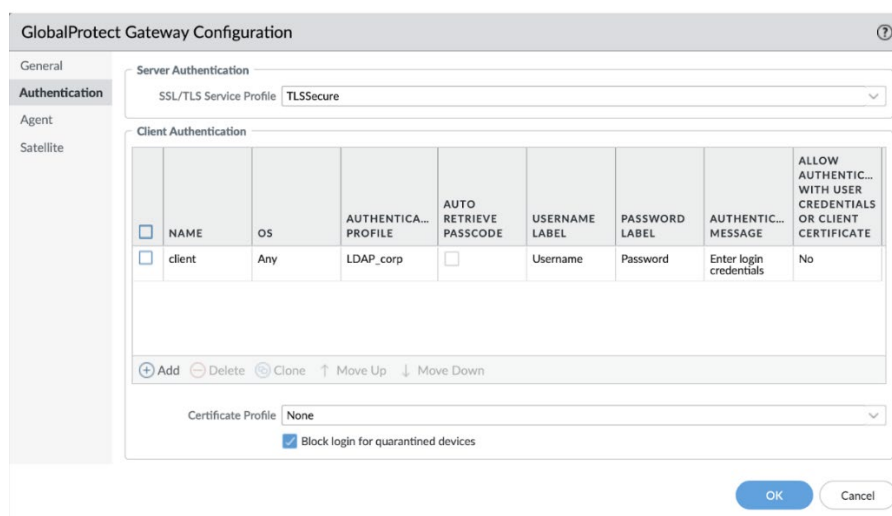
2. Configuración de *GlobalProtect Gateways*

Ubicación: “*Network > GlobalProtect > Gateways*”

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

Figura 5-63: Configuración de GlobalProtect Gateway (General)

En la pestaña Authentication, se indica el perfil SSL/TLS creado en pasos anteriores (ver apartado 5.4.2) 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).



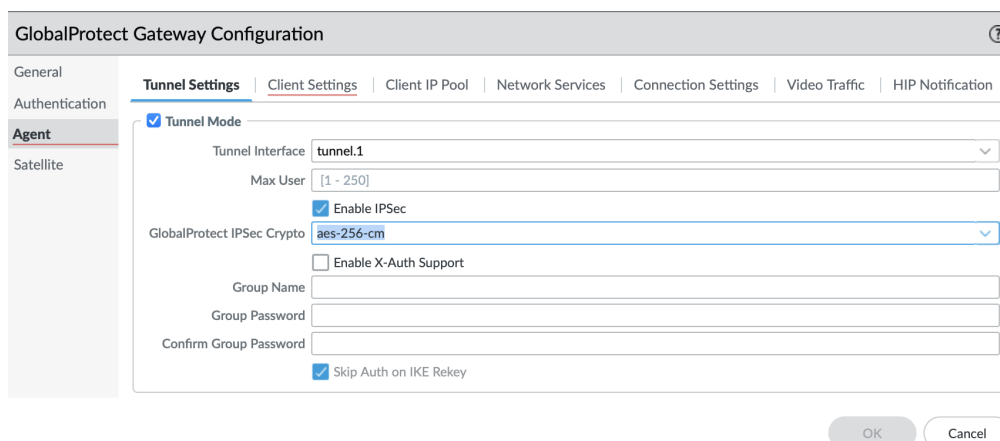
The screenshot shows the 'GlobalProtect Gateway Configuration' window with the 'Authentication' tab selected. The 'Server Authentication' section has 'SSL/TLS Service Profile' set to 'TLSSecure'. The 'Client Authentication' section contains a table with columns: NAME, OS, AUTHENTICATE PROFILE, AUTO RETRIEVE PASSCODE, USERNAME LABEL, PASSWORD LABEL, AUTHENTIC... MESSAGE, and ALLOW AUTHENTIC... WITH USER CREDENTIALS OR CLIENT CERTIFICATE. A single row is visible with 'client' as the name, 'Any' as the OS, 'LDAP_corp' as the profile, and 'No' for the last column. Below the table are buttons for '+ Add', '- Delete', 'Clone', 'Move Up', and 'Move Down'. At the bottom, 'Certificate Profile' is set to 'None' and 'Block login for quarantined devices' is checked. 'OK' and 'Cancel' buttons are at the bottom right.

NAME	OS	AUTHENTICATE PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENTIC... MESSAGE	ALLOW AUTHENTIC... WITH USER CREDENTIALS OR CLIENT CERTIFICATE
client	Any	LDAP_corp	☐	Username	Password	Enter login credentials	No

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

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

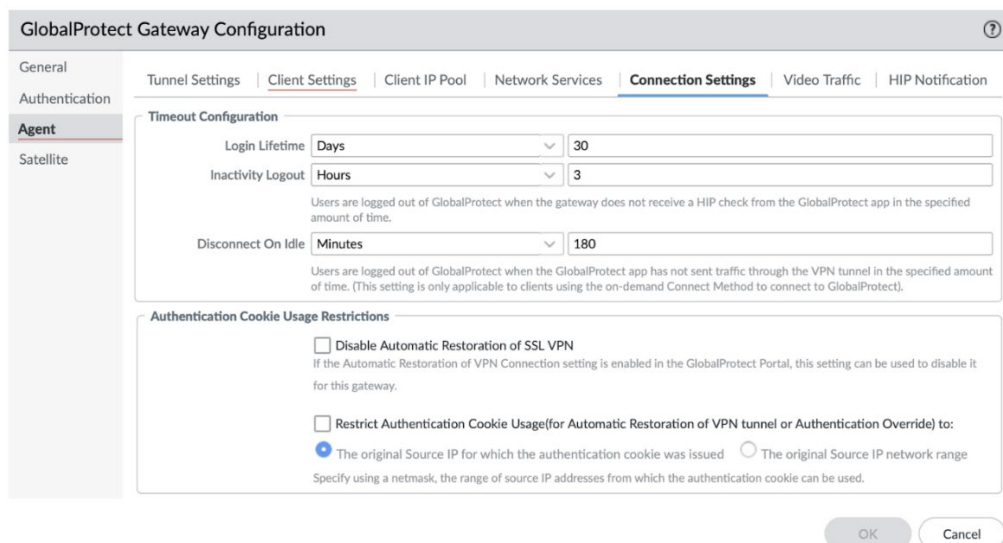
- Se asocia el túnel que va a cursar el servicio GlobalProtect, y el perfil *crypto IPsec* correspondiente.



The screenshot shows the 'GlobalProtect Gateway Configuration' window with the 'Agent' tab selected. The 'Tunnel Settings' sub-tab is active. 'Tunnel Mode' is checked. 'Tunnel Interface' is set to 'tunnel.1'. 'Max User' is set to '[1 - 250]'. 'Enable IPsec' is checked. 'GlobalProtect IPsec Crypto' is set to 'aes-256-cm'. 'Enable X-Auth Support' is unchecked. 'Group Name', 'Group Password', and 'Confirm Group Password' fields are empty. 'Skip Auth on IKE Rekey' is checked. 'OK' and 'Cancel' buttons are at the bottom right.

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

- Se configura el *timeout* de sesión:



GlobalProtect Gateway Configuration ⓘ

General | Tunnel Settings | **Client Settings** | Client IP Pool | Network Services | **Connection Settings** | Video Traffic | HIP Notification

Authentication

Agent

Satellite

Timeout Configuration

Login Lifetime: Days 30

Inactivity Logout: Hours 3

Disconnect On Idle: Minutes 180

Users are logged out of GlobalProtect when the gateway does not receive a HIP check from the GlobalProtect app in the specified amount of time.

Users are logged out of GlobalProtect when the GlobalProtect app has not sent traffic through the VPN tunnel in the specified amount of time. (This setting is only applicable to clients using the on-demand Connect Method to connect to GlobalProtect).

Authentication Cookie Usage Restrictions

☐ Disable Automatic Restoration of SSL VPN

If the Automatic Restoration of VPN Connection setting is enabled in the GlobalProtect Portal, this setting can be used to disable it for this gateway.

☐ Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override) to:

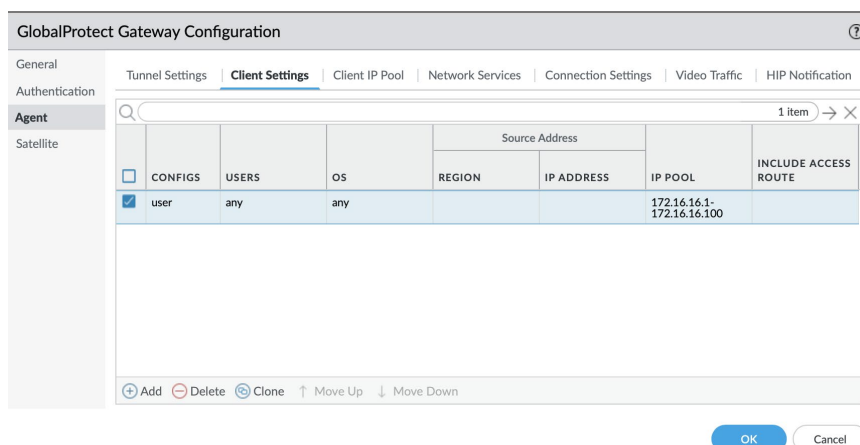
☒ The original Source IP for which the authentication cookie was issued ☐ The original Source IP network range

Specify using a netmask, the range of source IP addresses from which the authentication cookie can be used.

OK Cancel

Figura 5-66: 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):



GlobalProtect Gateway Configuration ⓘ

General | Tunnel Settings | **Client Settings** | Client IP Pool | Network Services | Connection Settings | Video Traffic | HIP Notification

Authentication

Agent

Satellite

1 item → ×

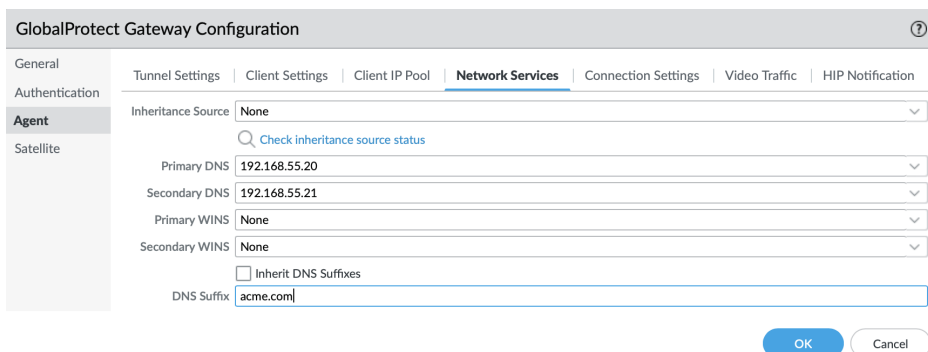
	CONFIGS	USERS	OS	Source Address		IP POOL	INCLUDE ACCESS ROUTE
				REGION	IP ADDRESS		
☒	user	any	any			172.16.16.1-172.16.16.100	

+ Add - Delete Clone ↑ Move Up ↓ Move Down

OK Cancel

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

- Se configura los servidores DNS internos:



GlobalProtect Gateway Configuration ⓘ

General | Tunnel Settings | Client Settings | Client IP Pool | **Network Services** | Connection Settings | Video Traffic | HIP Notification

Authentication

Agent

Satellite

Inheritance Source: None

[Check inheritance source status](#)

Primary DNS: 192.168.55.20

Secondary DNS: 192.168.55.21

Primary WINS: None

Secondary WINS: None

☐ Inherit DNS Suffixes

DNS Suffix: acme.com

OK Cancel

Figura 5-68: Configuración de GlobalProtect Gateway (Network Services)

3. Configuración de GlobalProtect Portal

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”:

The screenshot shows the 'GlobalProtect Portal Configuration' window with the 'General' tab selected. The configuration includes:

- Name:** GP_Portal
- Network Settings:**
 - Interface: ethernet1/1
 - IP Address Type: IPv4 Only
 - IPv4 Address: 192.168.55.20/24
- Appearance:**
 - Portal Login Page: factory-default
 - Portal Landing Page: factory-default
 - App Help Page: None
- Log Settings:**
 - ☐ Log Successful SSL Handshake
 - ☒ Log Unsuccessful SSL Handshake
 - Log Forwarding: None

Buttons at the bottom: OK, Cancel.

Figura 5-69: Configuración de GlobalProtect Portal (General)

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

The screenshot shows the 'GlobalProtect Portal Configuration' window with the 'Authentication' tab selected. The configuration includes:

- Server Authentication:**
 - SSL/TLS Service Profile: TLSSecure
- Client Authentication:**

	NAME	OS	AUTHENTI... PROFILE	AUTO RETRIEVE PASSCODE	USERNAME LABEL	PASSWORD LABEL	AUTHENT... MESSAGE	ALLOW AUTHENT... WITH USER CREDENT... OR CLIENT CERTIFIC...
☐	Client	Any	LDAP_corp	☐	Username	Password	Enter login credentials	No

Buttons: + Add, - Delete, Clone, ↑ Move Up, ↓ Move Down
- Certificate Profile:** None

Buttons at the bottom: OK, Cancel.

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

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

GlobalProtect Portal Configuration ?

General
Authentication
Portal Data Collection
Agent
Clientless VPN
Satellite

Agent

☐	CONFIGS	USER/USER GROUP	OS	EXTERNAL GATEWAYS	CLIENT CERTIFICATE
☒	agent	any	any	gw1	

+ Add - Delete Clone ↑ Move Up ↓ Move Down

☐	TRUSTED ROOT CA	INSTALL IN LOCAL ROOT CERTIFICATE STORE
☒	CA-ACME	☐

+ Add - Delete

Agent User Override Key:
Confirm Agent User Override Key:

OK Cancel

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

- 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).

Configs ?

Authentication | Config Selection Criteria | Internal | **External** | App | HIP Data Collection

Cutoff Time (sec) 5

External Gateways

☐	NAME	ADDRESS	PRIORITY RULE	MANUAL
☒	gw1	gp.acme.com	Any (Highest)	☒

+ Add - Delete

THIRD PARTY VPN

+ Add - Delete

OK Cancel

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

4. GlobalProtect APP

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

Ubicación: “*Device > GlobalProtect Client*”

VERSION	SIZE	RELEASE DATE	DOWNLOADED	CURRENTLY ACTIVATED	ACTION	
6.0.0	152 MB	2022/02/22 12:11:26			Download	Release Notes
5.2.11	99 MB	2022/03/09 11:49:56			Download	Release Notes
5.2.10	99 MB	2021/12/16 14:20:18			Download	Release Notes
5.2.9	99 MB	2021/11/30 09:57:03			Download	Release Notes
5.2.8	96 MB	2021/08/04 13:10:27			Download	Release Notes
5.2.7	94 MB	2021/06/10 14:41:40			Download	Release Notes
5.2.6	89 MB	2021/04/08 03:44:12			Download	Release Notes
5.2.5	66 MB	2021/01/13 09:07:01			Download	Release Notes
5.2.5-c84	70 MB	2021/03/24 13:53:52			Download	Release Notes
5.2.4	65 MB	2020/11/18 14:46:46			Download	Release Notes
5.2.3	65 MB	2020/10/08 12:24:26			Download	Release Notes
5.2.2	64 MB	2020/08/31 12:36:14			Download	Release Notes
5.2.1	64 MB	2020/08/13 13:08:08			Download	Release Notes
5.2.0	64 MB	2020/07/30 10:05:36			Download	Release Notes
5.1.10	61 MB	2022/02/08 15:45:41			Download	Release Notes
5.1.9	61 MB	2021/11/04 16:33:39			Download	Release Notes
5.1.8	61 MB	2020/12/28 11:08:39			Download	Release Notes

Figura 5-73: Selección de agente GlobalProtect a utilizar

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 5-74: GlobalProtect Portal y descarga de agente

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

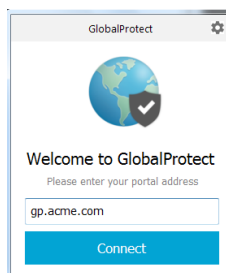


Figura 5-75: Pantalla de inicio de aplicación Globalprotect (Windows)

5. Resultado

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

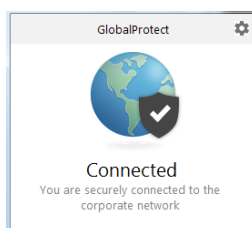


Figura 5-76: Comprobación de estado de la conexión VPN (Windows)

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

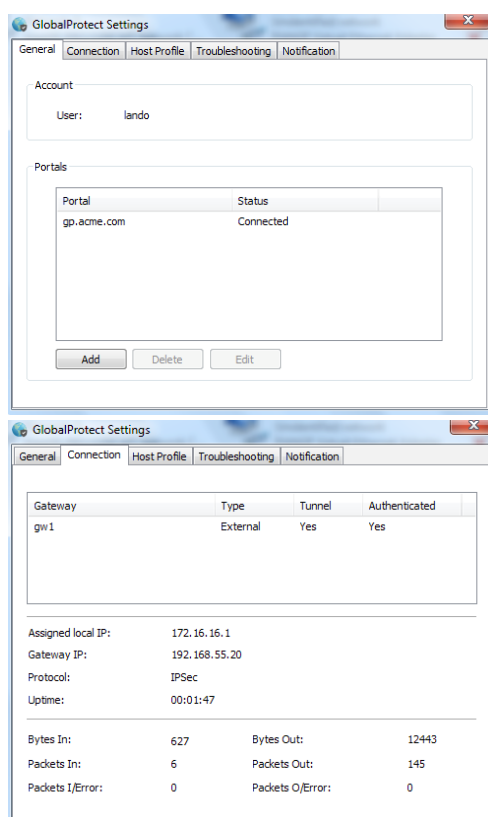


Figura 5-77: Comprobación de estado del Agente (Windows)

En los logs del cortafuegos, también se pueden consultar los eventos en “Monitor > System”:

Receive Time	Type	Severity	Event	Object	Description
02/04 09:50:56	globalprotect	Informational	globalprotectgateway-config-succ	GP_Gateway-N	GlobalProtect gateway client configuration generated. User name: lando, Private IP: 172.16.16.1, Client version: 4.1.9-7, Device name: WINDOWS7-32BIT, Client OS version: Microsoft Windows 7 Enterprise Edition Service Pack 1, 32-bit, VPN type: Device Level VPN.
02/04 09:50:56	globalprotect	Informational	globalprotectgateway-regist-succ	GP_Gateway-N	GlobalProtect gateway user login succeeded. Login from: 192.168.55.63, Source region: 192.168.0.0-192.168.255.255, User name: lando, Client OS version: Microsoft Windows 7 Enterprise Edition Service Pack 1, 32-bit.
02/04 09:50:56	globalprotect	Informational	globalprotectgateway-auth-succ	GP_Gateway-N	GlobalProtect gateway user authentication succeeded. Login from: 192.168.55.63, Source region: 192.168.0.0-192.168.255.255, User name: lando, Auth type: profile, Client OS version: Microsoft Windows 7 Enterprise Edition Service Pack 1, 32-bit.

Figura 5-78: Logs de GlobalProtect

5.12.3 IDENTIFICACIÓN DE APLICACIONES (APP-ID)

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.

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 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.

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.

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.

En el caso de los cortafuegos de Palo Alto Networks, el módulo encargado de realizar la identificación de la aplicación se denomina **App-ID**. 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*).

Además, la inteligencia de este mecanismo es heredada por el resto de 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 5-79: Algoritmo de App-ID

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.

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*, ...).

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/products/technologies/app-id.html>

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/app-id>

5.12.3.1 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 7: Cadena de ciberataque – App-ID

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.

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*.

En relación a 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.

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.

5.12.3.2 REQUISITOS DE SEGURIDAD

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 implica que selectivamente se permite sólo lo estrictamente necesario.** Por el contrario, una aproximación basada en lógica negativa se fundamenta en denegar todo aquello que no está permitido, práctica muy poco recomendable por su difícil gestión (requiere estar monitorizando constantemente las nuevas aplicaciones) y porque deja una superficie de ataque mucho mayor.

Una aproximación fundamentada sobre lógica positiva simplemente requiere que se habilite la lista 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.

	Name	Tags	Type	Source			Destination		Application	Service	URL Category	Action
				Zone	Address	User	Zone	Address				
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 5-80: Ejemplo de política de aplicaciones basada en lógica positiva

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.

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

Ubicación: “Policies > Security”

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

Ubicación: “Policies > Security”

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

Ubicación: “Policies > Security”

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

Ubicación: “Objects > Applications”; “Policies > Security”; “Policies > Application Override”

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*.

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/10-2/pan-os-admin/app-id/manage-custom-or-unknown-applications>

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

Figura 5-81: Definición de aplicaciones propietarias

5.12.3.3 EJEMPLO DE USO

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.

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):

	Name	Tags	Type	Source			Destination		Application	Service	URL Category	Action
				Zone	Address	User	Zone	Address				
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 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 5-82: Política de protección de DMZ en entrada

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 5-83: Política de protección de DMZ en salida

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.

5.12.3.4 OBSERVABLES

Logs

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)*.

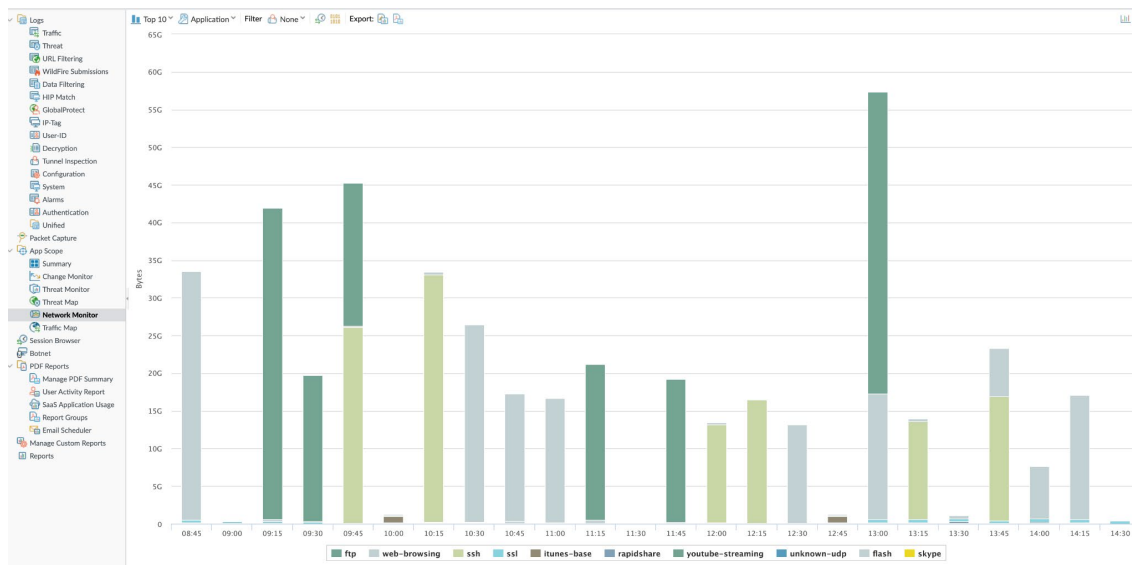


Figura 5-84: Visibilidad de aplicaciones con AppScope

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 la misma.

	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 5-85: Ejemplo de Traffic logs

Aplicaciones desconocidas

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 5-86: Ejemplo de unknown-tcp y captura en fichero pcap

Dependencia de aplicaciones

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*.

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 equipo 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*.

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*.

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.

5.12.4 IDENTIFICACIÓN DE USUARIOS

El objetivo fundamental de este módulo 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*

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.).

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*.

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

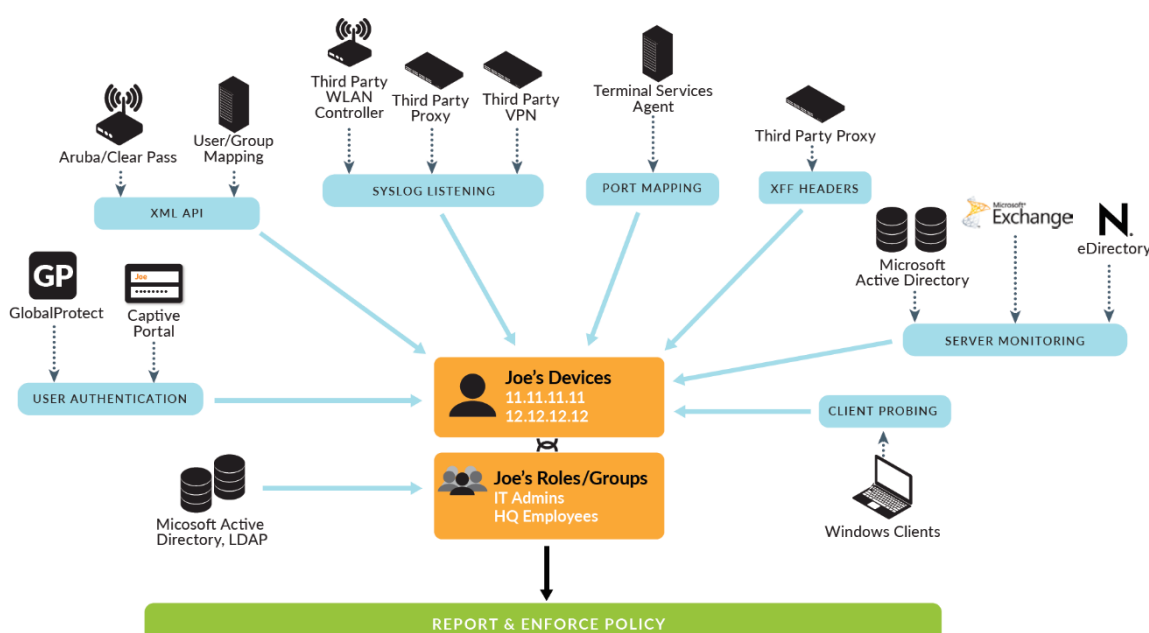


Figura 5-87: Tecnologías User-ID disponibles

Nota: Si se desea obtener más información sobre User-ID visitar:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/user-id>

5.12.4.1 MEDIDAS DE SEGURIDAD

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.

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

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

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 disparando 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.

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

Ubicación: “Network > Zones”

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.

Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	Enabled	User ID	
						Included Networks	Excluded Networks
Internet	layer3	ethernet1/1			☐	any	none
LAN	layer3	ethernet1/2			☒	10.10.0.0/16	none
DMZ	layer3	ethernet1/3			☐	any	none
Datacenter	layer3	ethernet1/4			☐	any	none

Figura 5-88: Activación de User-ID solamente en zonas internos

3. Deshabilitar WMI si no se utiliza

Ubicación: “Device > User Identification > User Mapping > Palo Alto Networks User ID Agent Setup > Client Probing”

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*.

Palo Alto Networks User-ID Agent Setup

Server Monitor Account | Server Monitor | **Client Probing** | Cache | Syslog Filters | Ignore User List

☐ Enable Probing

Probe Interval (min) 20

OK Cancel

Figura 5-89: Deshabilitación de User-ID Agent probing

4. Configurar include/exclude networks

Ubicación: “Network > Zones”; “Device > User Identification > User Mapping > Include/Exclude Networks”

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.

Name	Type	Interfaces / Virtual Systems	Zone Protection Profile	Log Setting	Enabled	User ID	
						Included Networks	Excluded Networks
☐ Internet	layer3	ethernet1/1			☐	any	none
☒ LAN	layer3	ethernet1/2			☒	10.10.0.0/16	none
☐ DMZ	layer3	ethernet1/3			☐	any	none
☐ Datacenter	layer3	ethernet1/4			☐	any	none

Include/Exclude Networks				
☐	NAME	ENABLED	TYPE	NETWORK ADDRESS
☐	Internas	☒	Include	10.10.0.0/16
(+) Add (-) Delete Custom Include/Exclude Network Sequence				

Figura 5-90: Configuración de include/exclude networks en User-ID

5. Configurar una cuenta dedicada para user-id

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.

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.

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/10-2/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

Ubicación: “Device > Setup > Services > Service Route Configuration”; “Policies > Security”

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.

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

Bloqueo-User-ID	IT	universal	LAN	IP-Gestion-FW	any	Internet	any	ms-wmi	application-default	any	msrpc	Deny
-----------------	----	-----------	-----	---------------	-----	----------	-----	--------	---------------------	-----	-------	------

Figura 5-91: Restricción del tráfico del agente User-ID

Service Route Configuration ?

☐ Use Management Interface for all
 ☒ Customize

IPv4 | IPv6 | Destination

SERVICE	SOURCE INTERFACE	SOURCE ADDRESS
☐ Palo Alto Networks Services	Use default	Use default
☐ Panorama	Use default	Use default
☐ Proxy	Use default	Use default
☐ RADIUS	Use default	Use default
☐ SCEP	Use default	Use default
☐ SNMP Trap	Use default	Use default
☐ Syslog	Use default	Use default
☐ TACACS+	Use default	Use default
☐ UID Agent	Use default	Use default
☐ URL Updates	Use default	Use default
☐ VM Monitor	Use default	Use default
☐ WildFire Private	Use default	Use default
☐ Ztp	Use default	Use default

Set Selected Service Routes

OK Cancel

Figura 5-92: Configuración del interfaz de User-ID

5.12.4.2 EJEMPLO DE USO

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			✓		
ms-update			✓		

Tabla 8: Requisitos de aplicaciones y grupos de usuarios de ejemplo

Name	Tags	Type	Source			Destination		Application	Service	URL Category	Action
			Zone	Address	User	Zone	Address				
5 Ventas	LAN Ventas	universal	LAN	any	acme\ventas	Internet	any	Aplicaciones-Streaming Aplicaciones-Ventas web-browsing Webmail	application-default	any	Allow
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 IT	LAN Gestión	universal	LAN	any	acme\IT	Internet	any	adobe-update facebook-base ms-update paloalto-updates ssl symantec-av-update web-browsing more...	application-default	any	Allow

Figura 5-93: Ejemplo de despliegue de una política con User-ID

5.12.4.3 OBSERVABLES

Identificación del usuario

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 el que ninguno de los mecanismos transparentes apliquen, es posible presentar una página de Portal Cautivo al usuario que se puede personalizar en “*Device > Response Pages*”:

Figura 5-94: Ejemplo de página de Portal Cautivo

Logs

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 5-95: Ejemplo de logs incluyendo el atributo usuario

Notificación al usuario

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*”:

Application Blocked

Access to the application you were trying to use has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: labs\bob

Application: twitter-base

Figura 5-96: Ejemplo de bloqueo de página incluyendo el usuario

5.12.5 IDENTIFICACIÓN DE DISPOSITIVO (Device-ID)

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.

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.

Desde la versión PAN-OS 10.0, en la que se introduce Device-ID, que permite crear políticas que acompañan a un dispositivo sin importar en qué parte de la red esté conectado. 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 DeviceID en los logs proporciona contexto adicional que combinado con AppID y UserID, permite obtener información detallada sobre el comportamiento en la red.

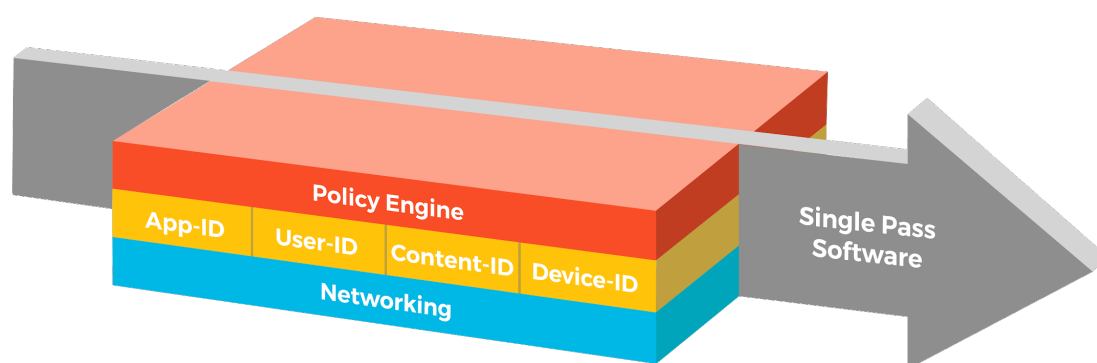


Figura 5-97: Single Pass Architecture

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, 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.

Device-ID está disponible en Panorama y todos los NGFW con tecnología ML, excepto las series VM-50 y CN, que ejecutan PAN-OS 10.0 o posterior.

NAME	TAGS	Source			Destination	APPLICATION	SERVICE	ACTION	PROFILE	Rule Usage	
		ZONE	USER	DEVICE						RULE USAGE	APPS SEEN
Sanctioned SaaS App...	Allowed	Trust	acme/finance	any	Untrust	boxnet concur docusign ms-office365 slack	application...	Allow		-	0
Tolerated SaaS Appl...	Acceptable	Trust	acme/all_em...	any	Untrust	gmail-base gmail-downl... google-base linkedin-base twitter-base	application...	Allow		-	0
Access Points	wirelessinfra	Trust	any	Aruba_APs	any	any	application...	Allow		-	0
RaspberryPi	wirelessinfra	Trust	any	RaspberryPi	any	any	application...	Allow		-	0

Users Devices Applications All Security Subscriptions (WF, TP, UF, DNS, ...)

Figura 5-98: Reglas de Seguridad con Device-ID

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/10-2/pan-os-admin/device-id/device-id-overview>

5.12.5.1 COMBATIENDO LA CADENA DE CIBERATAQUE

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

Tabla 9: Cadena de ciberataque – Device-ID

Device-ID proporciona los siguientes beneficios:

Visibilidad completa:

- Los administradores pueden rastrear un dispositivo a medida que se mueve a través de la red.
- Permite la evaluación de la superficie de ataque.

- Los analistas de SOC pueden rastrear amenazas específicas a dispositivos individuales.
- Personal de respuesta a incidentes para reaccionar más rápidamente.
- Remediación más rápida.

Reducir la superficie de ataque:

- Elimina la dependencia de la configuración del dispositivo.
- No importa si un dispositivo se conecta a la red o a una VLAN incorrecta.

Prevención de amenazas:

- Utiliza las mismas capacidades de prevención de amenazas proporcionadas a través de ContentID.
- 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.

Forense:

- Reducción del tiempo de remediación. Cuando ocurre un incidente, los clientes actualmente necesitan correlacionar la dirección IP del registro del firewall 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.

5.12.5.2 REQUISITOS DE SEGURIDAD

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 al diseño de red definido.
- Ningún actor malicioso puede conectar dispositivos a redes restringidas.
- Intentar resolver el problema de identificación integrando 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 donde hay un NAC disponible y puede realizar clasificación de dispositivos, el cliente tiene que realizar la implementación y mantener una integración con el firewall 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.

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

Ubicación: “Objects > Devices”; “Add”; “Browse”

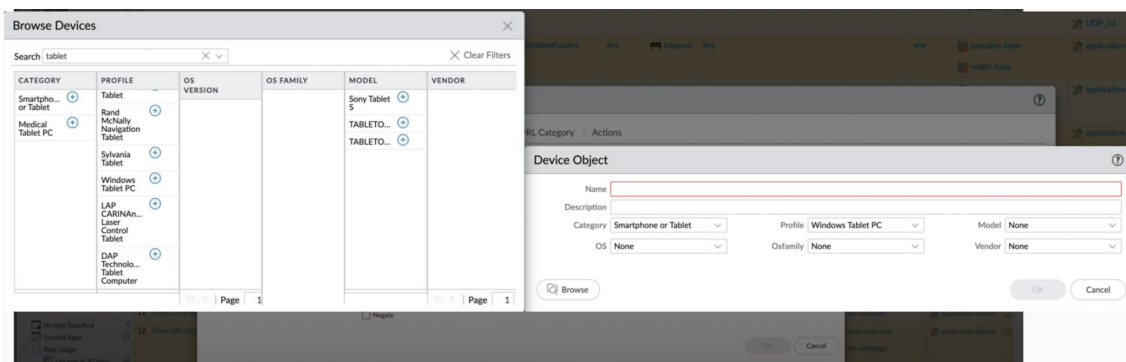


Figura 5-99: Configuración de atributos

Añadir un dispositivo de origen a una regla

Ubicación: “Policies > Security”; “Source > Source Device”; “Add”

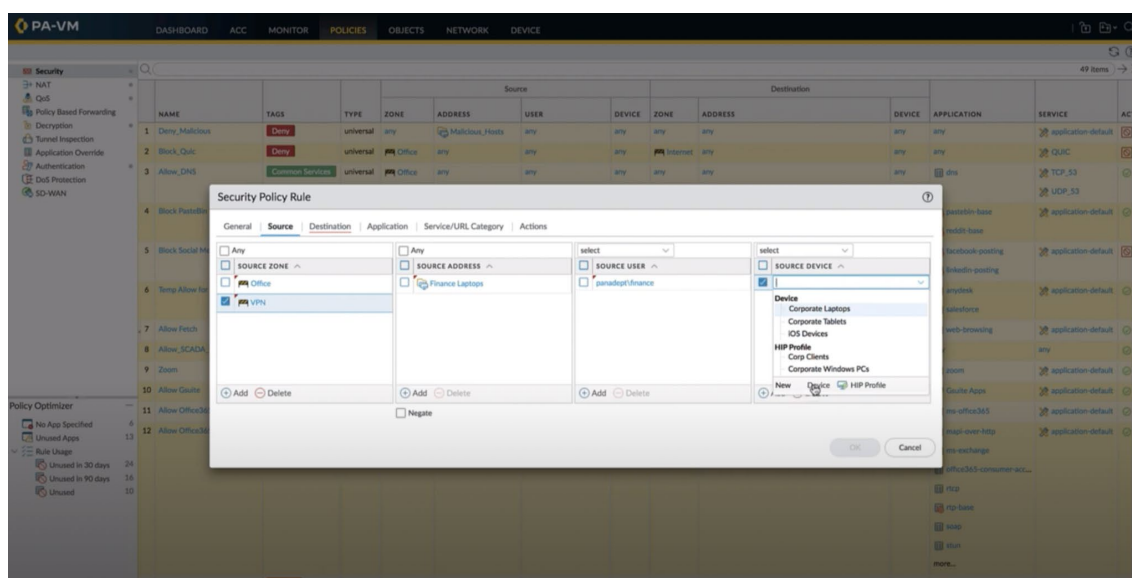


Figura 5-100: Uso de Device-ID en la política

Resultado

Ubicación: “Policies > Security”

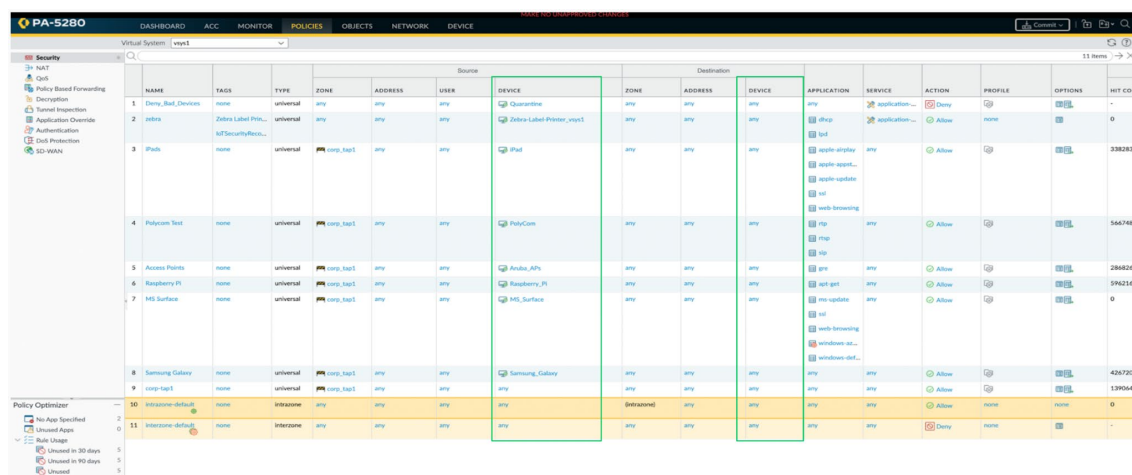


Figura 5-101: Reglas de la Política de Seguridad con Device-ID

5.12.5.3 EJEMPLO DE USO

Permitir acceso basado en el dispositivo

Ubicación: “*Policies > Security*”

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

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.

Service	Users	Source	Destination	Protocol	Port	Action	Comments
Infrastructure_Services	IP Users	any	any	any	any	allow	any
IP_Phones	IP Users	any	any	Cisco_VoIP...	any	allow	any
IP_Phones_Deny	IP Users	any	any	Cisco_VoIP...	any	deny	any

Figura 5-102: Ejemplo de políticas basadas en el ID del dispositivo (Device-ID)

Reducción de la superficie de ataque

Ubicación: “*Policies > Security*”

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

DeviceID 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.

The screenshot displays the Windows Defender application interface. At the top, a navigation bar shows 'Kiosk_Web_Browsing' and 'Kiosk_Deny' tabs. Below this, a table lists various settings, including 'Windows XP Hosts' and 'Internet'. The 'Device Object' section is expanded, showing 'Windows XP Hosts' as the selected device object. The 'File Blocking Profile' section is also expanded, showing 'End of Support File Blocking' as the selected profile. This profile restricts devices with outdated OS from downloading risky files. A table titled 'Risky Files' lists various file types, including .asp, .aspx, .deflated4-zip, .dll, .encrypted-7z, .encrypted-docx, .encrypted-pdf, and .PE. The 'Direction' column indicates 'both' for all entries, and the 'Action' column indicates 'block' for all entries. The 'Add' and 'Delete' buttons are visible at the bottom of the table.

Figura 5-103: Restringir descargas de ficheros peligrosos para dispositivos con sistemas operativos obsoletos

Descifrado basado en el dispositivo

Ubicación: “Policies > Decryption”

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

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.

	NAME	TAGS	Source			Destination			URL CATEGORY	SERVICE	ACTION
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS			
1	No-decrypt-for-WhatsApp-mobile-app	none	L3-trust	any	any	Smartphones and tablets	L3-untrust	any	any	whatsapp	no-decrypt
2	Decrypt-whatsapp	none	L3-trust	any	any	any	L3-untrust	any	any	internet-commu...	decrypt

Figura 5-104: Descifrado basado en el dispositivo

Rastrear un dispositivo en la red

Ubicación: “ACC”

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

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.

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.

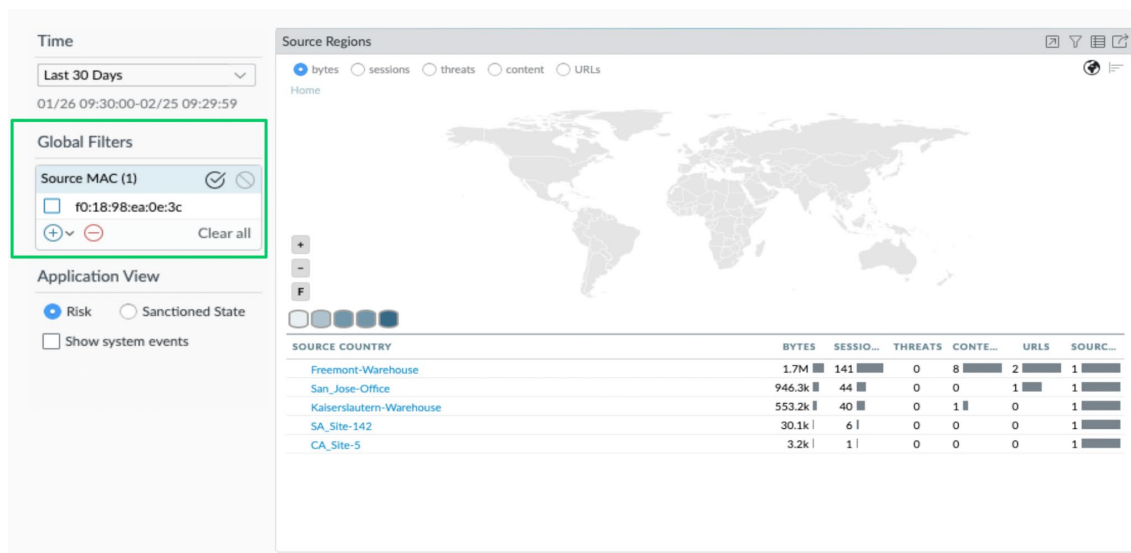


Figura 5-105: Rastreo de dispositivos en la red

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.

5.12.5.4 OBSERVABLES

Ubicación: “Monitor > Traffic”

Es posible ver la actividad de los dispositivos consultando “Monitor > Traffic”.

RECEIVE TIME	TYPE	FROM ZONE	TO ZONE	SOURCE	SOURCE DEVICE CATEGORY	SOURCE DEVICE VENDOR	SOURCE DEVICE PROFILE	SOURCE DEVICE OS VERSION	SOURCE DEVICE OS FAMILY	SOURCE DEVICE MODEL	SOURCE DEVICE MAC	SOURCE USER	DESTINATION	DESTINATION DEVICE PROFILE	TO PORT	APPLICATION	ACTION
12/16 11:26:52	end	corp_tapi	corp_tapi	10.57.101.211		Apple Inc.	Macintosh	MacOS					10.55.2.10		53	dns	allow
12/16 11:26:51	end	corp_tapi	corp_tapi	10.55.82.99		Apple Inc.	Macintosh	MacOS			a8:80:36:39:c4:c1		44.240.64.157		443	ssl	allow
12/16 11:26:51	end	corp_tapi	corp_tapi	10.55.40.99		Apple Inc.	Polycom IP Phone			VVX801	64:16:79:37:26:c3		10.55.2.10		53	dns	allow
12/16 11:26:51	end	corp_tapi	corp_tapi	10.54.101.66		Apple Inc.	Macintosh	MacOS			6:c4:c0:a1:50:94		10.55.66.10		53	dns	allow
12/16 11:26:51	end	corp_tapi	corp_tapi	10.55.20.79	Network Security Equipment	Palo Alto Networks, Inc.	Palo Alto Networks Device		PAN-OS		e4:a7:49:7c:94:30		10.55.2.10		53	dns	allow
12/16 11:26:51	end	corp_tapi	corp_tapi	10.55.20.79	Network Security Equipment	Palo Alto Networks, Inc.	Palo Alto Networks Device		PAN-OS		e4:a7:49:7c:94:30		10.55.2.10		53	dns	allow
12/16 11:26:51	end	corp_tapi	corp_tapi	10.55.76.58	Network Security Equipment	Palo Alto Networks, Inc.	Palo Alto Networks Device		PAN-OS		84:08:12:a7:9c:00		10.55.66.10		53	dns	allow
12/16 11:26:51	end	corp_tapi	corp_tapi	10.54.100.131	Network Security Equipment	Apple Inc.	Macintosh	MacOS			6:c4:c0:a1:50:94		10.55.2.70		4282	incomplete	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.55.21.46	Network Security Equipment	Palo Alto Networks, Inc.	Palo Alto Networks Device		PAN-OS		b4:0c:25:8f:3e:13		4.2.2.2		53	dns	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.55.48.45	Network Security Equipment	Raspberry Pi Foundation	Raspberry Pi Device				b8:27:ad:30:87:54		10.46.6.159		80	incomplete	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.55.21.46	Network Security Equipment	Palo Alto Networks, Inc.	Palo Alto Networks Device		PAN-OS		b4:0c:25:8f:3e:13		4.2.2.2		53	dns	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.50.8.20	Network Security Equipment	Palo Alto Networks, Inc.	PC Linux	Linux					91.189.89.198		123	ntp	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.55.21.46	Network Security Equipment	Palo Alto Networks, Inc.	Palo Alto Networks Device		PAN-OS		b4:0c:25:8f:3e:13		4.2.2.2		53	dns	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.55.20.79	Network Security Equipment	Palo Alto Networks, Inc.	Palo Alto Networks Device		PAN-OS		e4:a7:49:7c:94:30		10.55.2.10		53	dns	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.47.110.137	Network Security Equipment	Apple Inc.	PC Windows	Windows					10.101.3.88		443	no-ds-emb3	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.55.21.46	Network Security Equipment	Palo Alto Networks, Inc.	Palo Alto Networks Device		PAN-OS		b4:0c:25:8f:3e:13		4.2.2.2		53	dns	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.55.21.46	Network Security Equipment	Palo Alto Networks, Inc.	Palo Alto Networks Device		PAN-OS		b4:0c:25:8f:3e:13		4.2.2.2		53	dns	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.55.20.79	Network Security Equipment	Palo Alto Networks, Inc.	Palo Alto Networks Device		PAN-OS		e4:a7:49:7c:94:30		10.55.2.10		53	dns	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.57.101.211	Network Security Equipment	Apple Inc.	Macintosh	MacOS					10.55.2.10		53	dns	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.55.20.79	Network Security Equipment	Palo Alto Networks, Inc.	Palo Alto Networks Device		PAN-OS		e4:a7:49:7c:94:30		104.199.115.54		443	passive-ssl-tls-enc	allow
12/16 11:26:50	end	corp_tapi	corp_tapi	10.57.101.211	Network Security Equipment	Apple Inc.	Macintosh	MacOS					10.55.2.10		53	dns	allow

Figura 5-106: Logs de los dispositivos

5.12.6 FILTRADO DE URL (ADVANCED URL FILTERING)

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.

La solución de filtrado de URL de Palo Alto Networks, 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 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 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.

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.

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.

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.

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.

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.

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*

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>

5.12.6.1 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 10: Cadena de ciberataque: URL Filtering

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).

5.12.6.2 REQUISITOS DE SEGURIDAD

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.

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

Ubicación: "Objects > Security Profiles > URL Filtering"; "Policies > Security"

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

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>

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

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

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

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

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

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.

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.

URL Filtering Profile (Read Only)

Name: default

Description:

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | Inline ML

73 items → X

☐	CATEGORY	SITE ACCESS	USER CREDENTIAL SUBMISSION
☐	private-ip-addresses	allow	allow
☐	proxy-avoidance-and-anonymizers	allow	allow
☐	questionable	block	block
☐	real-estate	allow	allow
☒	real-time-detection	alert	allow
☐	recreation-and-hobbies	allow	allow
☐	reference-and-research	allow	allow
☐	religion	allow	allow

* indicates a custom URL category, + indicates external dynamic list

[Check URL Category](#)

OK Cancel

Figura 5-107: Detección en tiempo real

Ubicación: “Objects > Security Profiles > URL Filtering > URL Filtering Profile > Categories”

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

Ubicación: “Objects > Security Profiles > URL Filtering > URL Filtering Profile > URL Filtering Settings”

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.

URL Filtering Profile

Name:

Description:

Categories: **URL Filtering Settings** | User Credential Detection | HTTP Header Insertion | Inline ML

☐ Log container page only

☐ Safe Search Enforcement

HTTP Header Logging

- ☒ User-Agent
- ☒ Referer
- ☒ X-Forwarded-For

OK Cancel

Figura 5-108: Activación de logging de cabeceras HTTP en URL Filtering

6. Desactivar el logging solo de container pages

Ubicación: “Objects > Security Profiles > URL Filtering > URL Filtering Profile > URL Filtering Settings”

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*

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”.

URL Filtering Profile ⓘ

Name

Description

Categories | **URL Filtering Settings** | User Credential Detection | HTTP Header Insertion | Inline ML

☐ Log container page only

☐ Safe Search Enforcement

HTTP Header Logging

☒ User-Agent

☒ Referer

☒ X-Forwarded-For

OK Cancel

Figura 5-109: Desactivación de logging solamente de container pages

5.12.6.3 EJEMPLO DE USO

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.

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:

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	URL CATEGORY	ACTION
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE				
1	Sitios-Restringidos	none	universal	 LAN	any	any	any	 Internet	any	any	 ssl  web-browsing	 application-default	 hacking malware peer-to-peer phishing proxy-avoidance... questionable web-advertisem...	 Deny

Figura 5-110: Bloqueo de sitios restringidos

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 5-111: Creación de un perfil de URL con todas las categorías en Alert

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE
9	Otros Usuarios Conocidos	none	universal	LAN	any	known-user	any	Internet	any	any	application-default	any	Allow	

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE
61	pan-soc Non-Standard Port Access	none	universal	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	application-default	any	Deny	

Figura 5-112: Aplicación del perfil sobre las reglas de acceso por usuario y grupo

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

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.

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

Recomendación: Activar los check “Enable local inline categorization” y “Enable cloud inline categorization”

The screenshot shows the 'URL Filtering Profile' configuration window. The 'Name' field contains 'Default'. The 'Description' field is empty. The 'Inline Categorization' tab is selected, showing two checked options: 'Enable local inline categorization' and 'Enable cloud inline categorization'. Below these is an 'Exceptions' section with a table header 'CUSTOM URL CATEGORY/EDL' and an empty table body. At the bottom of the exceptions section are 'Add' and 'Delete' buttons. The main configuration area has 'OK' and 'Cancel' buttons at the bottom right.

Figura 5-113: 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>

5.12.6.4 OBSERVABLES

Logs

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:

RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	APPLICATION	ACTION
02/08 14:26:13	proxy-avoidance-and-anonymizers	proxy-avoidance-and-anonymizers,low-risk	anonymizer.com...	Users	Public	192.168.45.200			52.204.10.149			web-browsing	block-url

Figura 5-114: Ejemplo de log de URL

Detailed Log View													
General				Source				Destination					
Session ID 46451				Source User				Destination User					
Action block-url				Source 192.168.45.200				Destination 52.204.10.149					
Application web-browsing				Source DAG				Destination DAG					
Rule allow-all				Country 192.168.0.0-192.168.255.255				Country United States					
Rule UUID 399b9b2f-30fb-4b26-84e9-b9e462ea84b2				Port 57687				Port 80					
Device SN				Zone Users				Zone Public					
IP Protocol tcp				Interface ethernet1/2				Interface ethernet1/1					
Log Action				NAT IP 192.168.55.20				NAT IP 52.204.10.149					
Category proxy-avoidance-and-anonymizers				NAT Port 5904				NAT Port 80					
PCAP	RECEIVE TIME	TYPE	APPLICA...	ACTI...	RULE	RULE UUID	BY...	SEVERI...	CATE...	URL CATE... LIST	VERDI...	URL	FILE NAME
	2022/02/08 14:26:24	end	web-browsing	allow	allow-all	399b9...	716		proxy-avoida... and-anony...				
	2022/02/08 14:26:13	url	web-browsing	block-url	allow-all	399b9...		inform...	proxy-avoida... and-	proxy-avoida... and-		anonymizer.com/L...	

Close

Figura 5-115: Vista detallada del log de URL

Notificación al usuario

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:

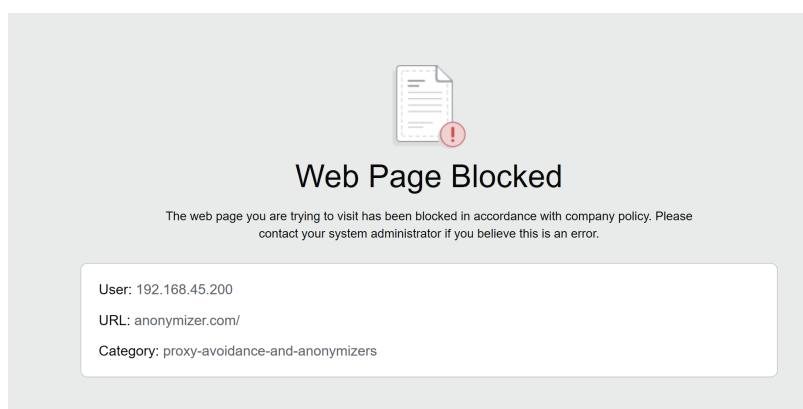


Figura 5-116: Ejemplo de página de bloqueo de URL

5.12.7 IPS

La funcionalidad de *Vulnerability Protection* 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.

El módulo tiene capacidad de convertir firmas IPS en Snort y Suricata de forma automática en firmas de vulnerabilidades de Palo Alto 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.

Ubicación: “Panorama > IPS Converter > Manage > Upload Signatures”

Figura 5-117: Modulo Panorama para Snort

Éste 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

Por defecto se ofrecen dos perfiles de *Vulnerability Protection* predefinidos:

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 informativas.

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 informativas, 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 5-118 Perfiles de Vulnerability Protection predefinidos

B. Perfiles Personalizados

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.

Vulnerability Protection Rule

Rule Name: R1

Threat Name: any

Used to match any signature containing the entered text as part of the signature name

Action: Reset Both

Packet Capture: disable

Host Type: any

Category: any

Severity:

- ☐ any (All severities)
- ☒ critical
- ☒ high
- ☒ medium
- ☐ low
- ☐ informational

Used to match any signature containing the entered text as part of the signature CVE or Vendor ID

OK Cancel

Figura 5-119: Perfiles de Vulnerability Protection personalizados

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/threat-prevention> <https://docs.paloaltonetworks.com/advanced-threat-prevention>

5.12.7.1 COMBATIENDO LA CADENA DE CIBERATAQUE

	Entrega	Explotación	Instalación	Mando y Control	Acciones en el Objetivo
Vulnerability Protection		Bloquear <i>exploits</i>			Prevenir el movimiento lateral

Tabla 11: Cadena de ciberataque - Vulnerability Protection

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.

5.12.7.2 REQUISITOS DE SEGURIDAD

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 tests 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.

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

Ubicación: “Objects > Security Profiles > Vulnerability Protection”

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 a aplicar una vez transcurrida la fase inicial de análisis.

Vulnerability Protection Profile

Name: best-practice-vuln-profile-pcap

Description:

Rules Exceptions

☐	RULE NAME	THREAT NAME	CVE	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
☐	simple-client-critical	any	any	client	critical	reset-both	single-packet
☐	simple-client-high	any	any	client	high	reset-both	single-packet
☐	simple-client-medium	any	any	client	medium	reset-both	single-packet
☐	simple-client-informational	any	any	client	informational	default	disable
☐	simple-client-low	any	any	client	low	default	single-packet
☐	simple-server-critical	any	any	server	critical	reset-both	single-packet
☐	simple-server-high	any	any	server	high	reset-both	single-packet
☐	simple-server-medium	any	any	server	medium	reset-both	single-packet
☐	simple-server-informational	any	any	server	informational	default	disable
☐	simple-server-low	any	any	server	low	default	single-packet

Figura 5-119: Perfil de Vulnerability Protection recomendado

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

Ubicación: “Policies > Security”

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.

5.12.7.3 EJEMPLO DE USO

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.

	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 Marketi... 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	

Figura 5-120: Perfiles Vulnerability Protection para clientes

	Name	Tags	Type	Source			Destination		Application	Service	URL Category	Action	Profile
				Zone	Address	User	Zone	Address					
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 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 5-121: Perfiles Vulnerability Protection para la DMZ

5.12.7.4 OBSERVABLES

Logs

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 5-122: Ejemplo de log de Vulnerability Protection

Detailed Log View

General

Session ID 3471
 Action drop
 Host ID
 Application ypserv
 Rule Unexpected Traffic
 Rule UID f0ebfc60-bf3f-4f89-a060-f059dc110bc9
 Device SN 007058000117547
 IP Protocol udp
 Log Action ToUS1RAMA
 Generated Time 2022/02/19 10:04:32
 Receive Time 2022/02/19 10:04:33
 Tunnel Type N/A

Source

Source User
 Source 66.1.1.9
 Source DAG
 Country United States
 Port 8406
 Zone L3-TAP
 Interface ethernet1/4
 X-Forwarded-For IP 0.0.0.0

Destination

Destination User pancademo\angela.bordelon
 Destination 10.154.10.181
 Destination DAG
 Country 10.0.0.0-10.255.255.255
 Port 59016
 Zone L3-TAP
 Interface ethernet1/4

Details

Threat Type vulnerability
 Threat ID/Name SunRPC rpc.yupdated Remote Command Execution Vulnerability
 ID 33789 (View in Threat Vault)
 Category code-execution
 Content Version AppThreat-8528-7235
 Severity high
 Repeat Count 1
 File Name
 URL
 Partial Hash 0
 Pcap ID 1207673900171222377
 Source UUID
 Destination UUID
 Dynamic User Group
 Network Slice ID SST
 Network Slice ID SD
 App Category networking

Flags

Captive Portal ☐
 Proxy Transaction ☐
 Decrypted ☐
 Packet Capture ☒
 Client to Server ☒
 Server to Client ☐
 Tunnel Inspected ☐

DeviceID

Source Device Category
 Source Device Profile
 Source Device Model
 Source Device Vendor
 Source Device OS Family
 Source Device OS Version
 Source Device Host
 Source Device MAC

PCAP	RECEIVE TIME	TYPE	APPLICATI...	ACTION	RULE	RULE UID	BYT...	SEVERITY	CATEG...	URL CATEG... LIST	VERDICT	URL	FILE NAME
...	2022/02/19 10:04:33	vulnerabil...	ypserv	drop	Unexpect... Traffic	f0ebfc6...		high	any				
...	2022/02/19 10:04:33	vulnerabil...	ypserv	drop	Unexpect... Traffic	f0ebfc6...		high	any				
...	2022/02/19 10:04:33	vulnerabil...	ypserv	drop	Unexpect... Traffic	f0ebfc6...		high	any				

Close

Figura 5-123: Ejemplo de log de Vulnerability Protection detallado

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.

Threat Details

Name SunRPC rpc.yupdated Remote Command Execution Vulnerability
 ID 33789 (View in Threat Vault)
 Description Sun Solaris rpc.yupdated service is prone to a command injection vulnerability while handling certain crafted RPC requests. The vulnerability is due to improper user input validation when processing RPC requests. A remote unauthenticated attacker can leverage this vulnerability by sending crafted RPC message to the target host, potentially injecting and executing arbitrary commands with System level privileges.
 Severity HIGH
 CVE CVE-1999-0209
 Bugtraq ID 1749
 Vendor ID
 Reference

EXEMPT PROFILES

3 items → ×

EXEMPT PROFILES	USED IN CURRENT SECURITY RULE
☒ Alert-ALL-Panorama (shared)	
☐ Alert-All-Panorama1 (shared)	
☐ strict-pcap (shared)	

EXEMPT IP ADDRESSES

1 item → ×

EXEMPT IP ADDRESSES
☒ 10.0.0.1

+ Add - Delete

OK Cancel

Figura 5-124: Creación de excepciones en los perfiles de Vulnerability Protection

5.12.8 ANTI-SPYWARE

La funcionalidad de *Anti-Spyware* 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*.

El servicio de seguridad de DNS (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.

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.

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

A. Perfiles Predefinidos

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

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.

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 5-125: Perfiles de Anti-Spyware predefinidos

B. Perfiles Personalizados

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.

Anti-Spyware Profile (Read Only) ⓘ

Name: default

Description:

Signature Policies | Signature Exceptions | DNS Policies | DNS Exceptions

☐	POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
☐	simple-critical	critical	default	disable
☐	simple-high	high	default	disable
☐	simple-medium	medium	default	disable
☐	simple-low	low	default	disable

OK Cancel

Figura 5-126: Perfiles de Anti-Spyware personalizados

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

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#tabs-id066476b2-c4dd-4fc0-b7e4-f4ba32e19f60&id=16e04f-38c2-4f07-ab94-84dd30669553>

Anti-Spyware Profile (Read Only) ?

Name: default

Description:

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions

DNS Policies

☐	Command and Control Domains	default (high)	default (block)	disable
☐	Dynamic DNS Hosted Domains	default (informational)	default (allow)	disable
☐	Grayware Domains	default (low)	default (block)	disable
☐	Malware Domains	default (medium)	default (block)	disable
☐	Parked Domains	default (informational)	default (allow)	disable
☐	Phishing Domains	default (low)	default (block)	disable
☐	Proxy Avoidance and Anonymizers	default (low)	default (block)	disable
☐	Newly Registered Domains	default (informational)	default (allow)	disable

DNS Sinkhole Settings

Sinkhole IPv4: Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)

Sinkhole IPv6: IPv6 Loopback IP (::1)

OK Cancel

Figura 5-127: Políticas de DNS

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).

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*.

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>

Palo Alto Networks utiliza una serie de motores de detección basados en 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 antispayware y requiere una licencia activa de Advanced Threat Prevention.

Ubicación: “Objects > Security Profiles > Anti-spyware > Inline Cloud Analysis”

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.

Anti-Spyware Profile

Name: Default

Description:

Signature Policies | Signature Exceptions | DNS Policies | DNS Exceptions | **Inline Cloud Analysis**

☒ Enable cloud inline analysis

Available Analysis Engines

MODEL	DESCRIPTION	ACTION
HTTP Command and Control detector	Machine Learning engine to detect HTTP based command and control traffic	alert
HTTP2 Command and Control detector	Machine Learning engine to detect HTTP2 based command and control traffic	alert

Figura 5-128: Análisis Inline en la nube

5.12.8.1 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 12: Cadena de ciberataque - Anti-Spyware

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.

5.12.8.2 REQUISITOS DE SEGURIDAD

1. Configurar perfil de *Anti-spyware*

Ubicación: “Objects > Security Profiles > Anti-spyware”

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.

Anti-Spyware Profile

Name

best-practices anti-spyware

Description

Signature Policies

Signature Exceptions

DNS Policies

DNS Exceptions

☐	POLICY NAME	SEVERITY	ACTION	PACKET CAPTURE
☐	high	high	reset-both	single-packet
☐	critical	critical	reset-both	single-packet
☐	medium	medium	reset-both	single-packet
☐	low	low	default	disable
☐	info	informational	default	disable

+ Add

- Delete

↑ Move Up

↓ Move Down

🔄 Clone

🔍 Find Matching Signatures

OK

Cancel

Figura 5-129: Perfil de Anti-spyware recomendado

2. Configurar DNS Sinkholing

Ubicación: “Objects > Security Profiles > Anti-spyware”

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

Ubicación: “Policies > Security”

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.

5.12.8.3 EJEMPLO DE USO

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:

	NAME	TAGS	TYPE	Source			Destination		APPLICATION	SERVICE	URL CATEG...	ACTION	PROFILE
				ZONE	ADDRESS	USER	ZONE	ADDRESS					
13	Users Out Web	Outbo... Outbo...	universal	Users	any	diab\domain u...	Public	any	ssl web-browsing	appl...	any	Allow	

Figura 5-130: Perfiles Anti-Spyware para clientes

5.12.8.4 OBSERVABLES

Logs

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*:

(action eq sinkhole)												
TYPE	THREAT ID/NAME	FROM ZONE	TO ZONE	SOURCE ADDRESS	SOURCE USER	SOURCE DYNAMIC ADDRESS GROUP	DESTINATION ADDRESS	DESTINATION DYNAMIC ADDRESS GROUP	DYNAMIC USER GROUP	TO PORT	APPLICATION	ACTION
spyware	Suspicious DNS Query (generic:0.187.94.bad.spky...	Users	Critical Infrastruc...	192.168.45.200	diab\yoda		192.168.25.65			53	dns	sinkhole

Figura 5-131: Ejemplo de log de Anti-Spyware

Detailed Log View

General

Session ID 60099

Action sinkhole

Host ID

Application dns

Rule Active Directory Users to Corporate

Rule UUID b88dbaf4-e19e-4929-962c-f2ca4dc506a4

Device SN 015351000059152

IP Protocol udp

Log Action Default Logging Profile

Source

Source User diablyoda

Source 192.168.45.200

Source DAG

Country 192.168.0.0-192.168.255.255

Port 63334

Zone Users

Interface ethernet1/2

X-Forwarded-For IP 0.0.0.0

Destination

Destination User

Destination 192.168.25.65

Destination DAG

Country 192.168.0.0-192.168.255.255

Port 53

Zone Critical Infrastructure

Interface ethernet1/4

Flags

PCAP	RECEIVE TIME	TYPE	APPLICAT...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG... LIST	VERDI...	URL	FILE NAME
	2021/01/27 04:51:13	spyware	dns	sinkhole	Active Direct... Users to Corpor...	b88db...		medium	any				
	2021/01/27 04:51:13	spyware	dns	sinkhole	Active Direct... Users to	b88db...		medium	any				

Close

Figura 5-132: Ejemplo de log de Anti-Spyware detallado

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.

5.12.9 ANTIVIRUS

La funcionalidad de Antivirus detecta y previene la transmisión de virus sobre los siguientes protocolos:

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

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

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:

Antivirus Profile (Read Only)

Name: default

Description:

Tab: Action | Signature Exceptions | WildFire Inline ML

☐ Enable Packet Capture

Decoders

PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
http	default (reset-both)	default (reset-both)	default (reset-both)
http2	default (reset-both)	default (reset-both)	default (reset-both)
smtp	default (alert)	default (alert)	default (alert)
imap	default (alert)	default (alert)	default (alert)
pop3	default (alert)	default (alert)	default (alert)
ftp	default (reset-both)	default (reset-both)	default (reset-both)
smb	default (reset-both)	default (reset-both)	default (reset-both)

Application Exceptions

0 items → ×

APPLICATION	ACTION
-------------	--------

+ Add - Delete

OK Cancel

Figura 5-133: 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

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:

The screenshot shows the 'Antivirus Profile' configuration window. The 'Name' field is 'AV-SN' and the 'Description' field is empty. The 'Action' tab is selected, showing 'Signature Exceptions' and 'WildFire Inline ML'. A table lists one exception:

THREAT ID	THREAT NAME	
1000001	Virus/Android.VGeneric.aghwhm	☒

At the bottom, there is a 'Threat ID' input field, 'Add', 'PDF/CSV' buttons, and 'OK' and 'Cancel' buttons.

Figura 5-134: 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>

5.12.9.1 COMBATIENDO LA CADENA DE CIBERATAQUE

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

Tabla 13: Cadena de ciberataque - Antivirus

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.

5.12.9.2 REQUISITOS DE SEGURIDAD

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.

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.

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

Ubicación: “Objects > Security Profiles > Antivirus”

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 de *WildFire*.

Antivirus Profile ⓘ

Name: AV-SN

Description:

Action | Signature Exceptions | WildFire Inline ML

☒ Enable Packet Capture

Decoders

PROTOCOL ^	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
ftp	default (reset-both)	default (reset-both)	default (reset-both)
http	default (reset-both)	default (reset-both)	default (reset-both)
http2	default (reset-both)	default (reset-both)	default (reset-both)
imap	default (alert)	default (alert)	default (alert)
pop3	default (alert)	default (alert)	default (alert)
smb	default (reset-both)	default (reset-both)	default (reset-both)
smtp	default (alert)	default (alert)	default (alert)

Application Exceptions

0 items → ×

APPLICATION	ACTION
-------------	--------

+ Add - Delete

OK Cancel

Figura 5-135: Perfil de Antivirus recomendado

2. Utilizar antivirus en todas las reglas que permitan tráfico

Ubicación: “Policies > Security”

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*.

5.12.9.3 EJEMPLO DE USO

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 usos auten	LAN	universal	LAN	any	known-user	Internet	any	facebook-base flash gmail-base ssl web-browsing	application-default	any	Allow	

Figura 5-136: Perfiles Antivirus para clientes

Name	Tags	Type	Source			Destination		Application	Service	URL Category	Action	Profile
			Zone	Address	User	Zone	Address					
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 5-137: Perfiles Antivirus para las actualizaciones de la DMZ

5.12.9.4 OBSERVABLES

Logs

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.

	Receive Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	Victim Name	To Port	Application	Action	Severity
	04/27 16:33:56	virus	Eicar Test File	Internet	LAN	188.40.238.252		192.168.45.64	acme\user1	50420	web-browsing	reset-both	medium

Figura 5-138: Ejemplo de log de Antivirus

Detailed Log View

General

Session ID

156883

Action

alert

Host ID

Application

web-browsing

Rule

DailyTransfer-BranchTrust2Hub-egress

Rule UUID

70c50fda-ee15-4ba8-a1d8-4dfe5edbf58

Device SN

IP Protocol

tcp

Log Action

ToUS1RAMA

Generated Time

2022/01/12 07:24:53

Receive Time

2022/01/12 07:24:53

Tunnel Type

N/A

Source

Source User

Source

192.168.160.51

Source DAG

Country

192.168.0.0-192.168.255.255

Port

40761

Zone

L3-Trust

Interface

ethernet1/5

X-Forwarded-For IP

Destination

Destination User

Destination

192.168.162.21

Destination DAG

Country

192.168.0.0-192.168.255.255

Port

443

Zone

zone-to-hub

Interface

tunnel903

Details

Threat Type

virus

Threat ID/Name

Trojan/Win32.hisboarder.fv

ID

219127317 (View in Threat Vault)

Category

pe

Content Version

Antivirus-3959-4470

Severity

medium

Repeat Count

1

File Name

192.168.162.21/malware/Oc9...

URL

Partial Hash

0

Pcap ID

0

Source UUID

Destination UUID

Dynamic User Group

Network Slice ID

SST

Network Slice ID SD

App Category

general-internet

App Subcategory

internet-utility

Flags

Captive Portal

☐

Proxy Transaction

☐

Decrypted

☒

Packet Capture

☐

Client to Server

☐

Server to Client

☒

Tunnel Inspected

☐

DeviceID

Source Device

Category

Source Device

Profile

Source Device

Model

Source Device

Vendor

Source Device

OS

Family

Source Device

OS

Version

PCAP	RECEIVE TIME	TYPE	APPLICATI...	ACTION	RULE	RULE UUID	BYT...	SEVERITY	CATEGO...	URL CATEGO... LIST	VERDICT	URL	FILE NAME
	2022/01/12 07:25:12	end	web-browsing	allow	DailyTra... BranchTr... egress	70c50fd...	175...		private-ip-addresses				
	2022/01/12 07:24:58	url	web-browsing	alert	DailyTra... BranchTr... egress	70c50fd...		informati...	private-ip-addresses	private-ip-addresses		192.168...	

Close

Figura 5-139: Ejemplo de log de Antivirus detallado

Notificación al usuario

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*”:

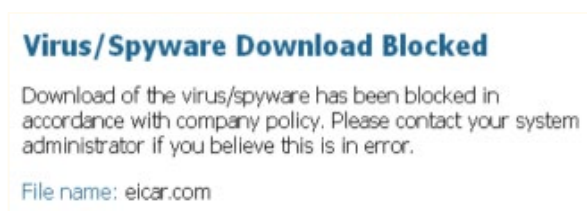


Figura 5-140: Ejemplo de página de bloqueo de Antivirus

5.12.10 BLOQUEO DE FICHEROS (FILE BLOCKING)

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.

5.12.10.1 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 <i>drive-by downloads</i>		Prevenir la exfiltración de datos y el movimiento lateral

Tabla 14: Cadena de ciberataque - File Blocking

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.

5.12.10.2 REQUISITOS DE SEGURIDAD

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

Ubicación: “*Objects > Security Profiles > File Blocking*”

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*.

File Blocking Profile

Name: Ficheros-SN

Description:

NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
☒ R1	any	any	both	alert

1 item

+ Add - Delete

OK Cancel

Figura 5-141: Perfil de File Blocking

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

Ubicación: “Policies > Security”

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.

5.12.10.3 EJEMPLO DE USO

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.

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:

File Blocking Profile ?

Name:

Description:

3 items → ×

☐	NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
☐	Ejecutables	any	dll exe msi ocx	both	alert
☐	Torrent	any	torrent	both	alert
☐	Cifrados	any	encrypted-doc encrypted-docx encrypted-office2007	both	alert

+ Add - Delete

OK Cancel

Figura 5-142: Ejemplo de Perfil de File Blocking

Name	Tags	Type	Zone	Address	User	Zone	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 usos auten	LAN	universal	LAN	any	known-user	Internet	any	facebook-base flash gmail-base ssl web-browsing	application-default	any	Allow	

Figura 5-143: Aplicación de File Blocking en las reglas de seguridad

5.12.10.4 OBSERVABLES

Logs

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 5-144: Ejemplo de log de File Blocking

Detailed Log View

General	Source	Destination
Session ID 46016	Source User pancademolaura.hale	Destination User
Action block-continue	Source 10.154.9.178	Destination 72.14.213.136
Application google-base	Source DAG	Destination DAG
Rule General Web Infrastructure	Country 10.0.0.0-10.255.255.255	Country United States
Rule UUID af55edec-9335-4979-b955-fc0c6749fe31	Port 3573	Port 80
Device SN 007058000117547	Zone L3-TAP	Zone L3-TAP
IP Protocol tcp	Interface ethernet1/4	Interface ethernet1/4
Log Action ToUS1RAMA	X-Forwarded-For IP 0.0.0.0	
Category search-engines		
Generated Time 2022/02/19 09:03:12		
Receive Time 2022/02/19 09:03:21		
Tunnel Type N/A		

Details
Content Type file
Threat ID/Name Microsoft PE File
ID 52060 (View in Threat Vault)
Severity low
Repeat Count 1
File Name GoogleEarthSetup.exe
File URL
File Digest
Dynamic User Group
Network Slice ID SD
Network Slice ID SST
App Category general-Internet
App Subcategory internet-utility
App Technology browser-based
App Characteristic used-by-malware,able-to-transfer-file,has-known-vulnerability,tunnel-other-application,pervasive-use

Flags
Captive Portal ☐
Proxy Transaction ☐
Decrypted ☐
Packet Capture ☐
Client to Server ☐
Server to Client ☒
Tunnel Inspected ☐

DeviceID
Source Device Category Personal Computer
Source Device Profile PC-Windows
Source Device Model
Source Device Vendor
Source Device OS Family Windows
Source Device OS Version
Source Device Host
Source Device MAC

PCAP	RECEIVE TIME	TYPE	APPLICATI...	ACTION	RULE	RULE UUID	BYT...	SEVERITY	CATEG...	URL CATEG... LIST	VERDICT	URL	FILE NAME
	2022/02/19 09:03:21	file	google-base	block-continue	General Web Infrastru...	af55ede...		low	search-engines				GoogleE...
	2022/02/19 09:04:42	end	google-base	allow	General Web Infrastru...	af55ede...	27563		search-engines				

Close

Figura 5-145: Ejemplo de log de File Blocking detallado

Notificación al usuario

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”:

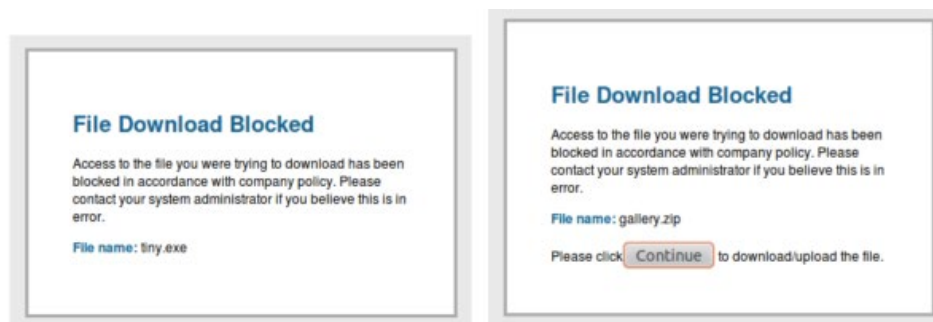


Figura 5-146: Ejemplo de página de bloqueo y Continue de File Blocking

5.12.11 WILDFIRE

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.

El motor de *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.

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.

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 procedentes 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.

Además, y tal y como se comentó en el apartado [5.12.9 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.

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.

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).

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>

5.12.11.1 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 15: Cadena de ciberataque - WildFire Threat Intelligence

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.

5.12.11.2 REQUISITOS DE SEGURIDAD

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*.

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

Ubicación: “*Device > Setup > Wildfire > General Settings*”

Recomendación: Cambie la configuración de la nube pública por defecto, para utilizar solamente la ubicada dentro de la Unión Europea, “*eu.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).

General Settings

WildFire Public Cloud

WildFire Private Cloud

☐ Use Proxy Settings for Private Cloud

File Size Limits

FILE TYPE	SIZE LIMIT
pe (MB)	16 (default)
apk (MB)	10 (default)
pdf (KB)	3072 (default)
ms-office (KB)	16384 (default)
jar (MB)	5 (default)
flash (MB)	5 (default)
MacOSX (MB)	10 (default)
archive (MB)	50 (default)
linux (MB)	50 (default)
script (KB)	20 (default)

☐ Report Benign Files

☐ Report Grayware Files

OK Cancel

Figura 5-147: Configuración de Wildfire europeo

2. Incrementar el tamaño de archivo en Wildfire

Ubicación: “Device > Setup > Wildfire > General Settings”

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.

General Settings

WildFire Public Cloud

WildFire Private Cloud

☐ Use Proxy Settings for Private Cloud

File Size Limits

FILE TYPE	SIZE LIMIT
pe (MB)	16 (default)
apk (MB)	10 (default)
pdf (KB)	3072 (default)
ms-office (KB)	16384 (default)
jar (MB)	5 (default)
flash (MB)	5 (default)
MacOSX (MB)	10 (default)
archive (MB)	50 (default)
linux (MB)	50 (default)
script (KB)	20 (default)

☐ Report Benign Files

☐ Report Grayware Files

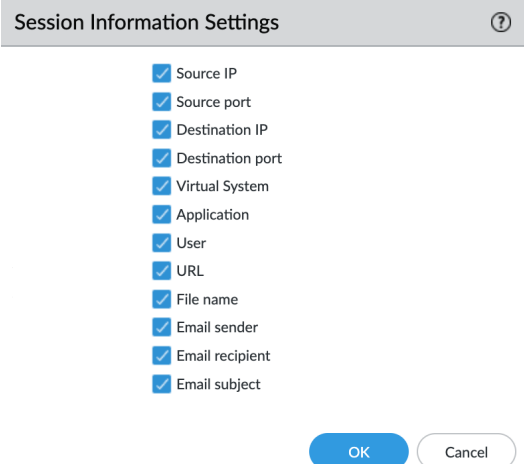
OK Cancel

Figura 5-148: Configuración tamaño máx de ficheros inspeccionados WildFire

3. Envío de la información de sesión a Wildfire

Ubicación: “Device > Setup > Wildfire > Session Information Settings”

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.

A dialog box titled "Session Information Settings" with a help icon. It contains a list of 13 items, each with a checked checkbox: Source IP, Source port, Destination IP, Destination port, Virtual System, Application, User, URL, File name, Email sender, Email recipient, and Email subject. At the bottom are "OK" and "Cancel" buttons.

Session Information Settings
☒ Source IP
☒ Source port
☒ Destination IP
☒ Destination port
☒ Virtual System
☒ Application
☒ User
☒ URL
☒ File name
☒ Email sender
☒ Email recipient
☒ Email subject

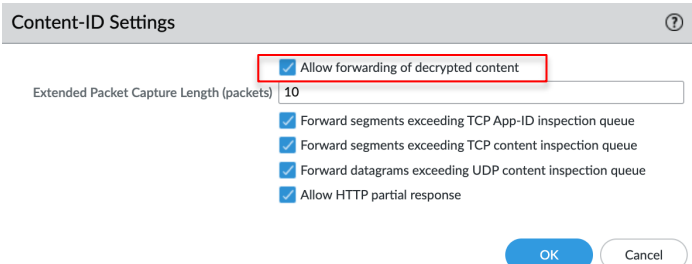
OK Cancel

Figura 5-149: Configuración de información de sesión enviada a WildFire

4. Configurar *forwarding* para el tráfico SSL descifrado

Ubicación: “Device > Setup > Content-ID > Content-ID Settings”

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

A dialog box titled "Content-ID Settings" with a help icon. It contains a checkbox "Allow forwarding of decrypted content" which is checked and highlighted with a red rectangle. Below it is a text field "Extended Packet Capture Length (packets)" with the value "10". At the bottom are "OK" and "Cancel" buttons.

Content-ID Settings
☒ Allow forwarding of decrypted content
Extended Packet Capture Length (packets) 10
☒ Forward segments exceeding TCP App-ID inspection queue
☒ Forward segments exceeding TCP content inspection queue
☒ Forward datagrams exceeding UDP content inspection queue
☒ Allow HTTP partial response

OK Cancel

Figura 5-150: Forwarding of Decrypted Content

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

Ubicación: “Objects > Security Profiles > WildFire Analysis”

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.

WildFire Analysis Profile

Name: WF-SN

Description:

NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
R1	any	any	both	public-cloud

1 item

+ Add - Delete

OK Cancel

Figura 5-151: Perfil de WildFire Analysis recomendado

6. Configurar perfil de antivirus

Ubicación: “Objects > Security Profiles > Antivirus”

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.

Antivirus Profile

Name: AV-SN

Description:

Action | Signature Exceptions | WildFire Inline ML

☒ Enable Packet Capture

Decoders

PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
smtp	reset-both	reset-both	reset-both
smb	default (reset-both)	default (reset-both)	default (reset-both)
pop3	reset-both	reset-both	reset-both
imap	reset-both	reset-both	reset-both
http2	default (reset-both)	default (reset-both)	default (reset-both)
http	default (reset-both)	default (reset-both)	default (reset-both)
ftp	default (reset-both)	default (reset-both)	default (reset-both)

Application Exceptions

0 items

APPLICATION	ACTION
-------------	--------

+ Add - Delete

OK Cancel

Figura 5-152: Perfil de Antivirus recomendado

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

Ubicación: “Policies > Security”

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

Ubicación: “CLI”; “Monitor > Logs > WildFire Submissions”

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-VM> test wildfire registration
This test may take a few minutes to finish. Do you want to continue? (y or n)
Test wildfire Public Cloud
Testing cloud server eu.wildfire.paloaltonetworks.com ...
wildfire registration:    successful
download server list:    successful
select the best server:   eu-panos.wildfire.paloaltonetworks.com
Test wildfire Private Cloud
Cloud server is empty
admin@PA-VM>
```

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.

5.12.11.3 EJEMPLO DE USO

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.

WildFire Analysis Profile

Name: Wildfire-Publico

Description:

NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
☒ Todos	any	any	both	public-cloud

+ Add - Delete

OK Cancel

Figura 5-153: Configuración del perfil público de WildFire

WildFire Analysis Profile

Name: Wildfire-Hibrido

Description:

NAME	APPLICATIONS	FILE TYPES	DIRECTION	ANALYSIS
☐ Publicos	any	apk archive email-link flash jar linux MacOSX pe	both	public-cloud
☐ Privados	any	script ms-office pdf	both	private-cloud

+ Add - Delete

OK Cancel

Figura 5-154: Configuración del perfil híbrido de WildFire

7	Recursos Humanos	LAN	universal	LAN	any	acme/recursos humanos	Internet	any	facebook-base linkedin web-browsing	application-default	any	Allow	
8	Gestión	LAN	universal	LAN	any	acme/gestion	Internet	any	linkedin salesforce web-browsing webex	application-default	any	Allow	
9	Otros usos auten	LAN	universal	LAN	any	known-user	Internet	any	facebook-base flash gmail-base ssl web-browsing	application-default	any	Allow	

Figura 5-155: Aplicación de WildFire público en las reglas de seguridad a Internet

11	Acceso Datacenter	LAN	universal	LAN	any	acme/gestion acme/marketing acme/recursos humanos acme/ventas	Datacenter	any	active-directory activesync ms-ds-smb msrpc netbios-dg netbios-ns netbios-ss more...	application-default	any	Allow	
----	-------------------	-----	-----------	-----	-----	--	------------	-----	---	---------------------	-----	-------	--

Figura 5-156: Aplicación de WildFire híbrido en las reglas de datacenter

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):

2	Acceso-mail-externo	DMZ	universal	Inte	any		DMZ	Serv...	activesync icmp imap pop3 smtp ssl web-browsing	application-default	any	Allow	
3	Salida-mail-externo	DMZ	universal	DMZ	Serv...		Internet	any	dns smtp	application-default	any	Allow	

Figura 5-157: Aplicación de WildFire público en las reglas de correo electrónico

5.12.11.4 OBSERVABLES

Logs

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 5-158: Ejemplo de log de File Blocking

Detailed Log View

Log Info

WildFire Analysis Report

General

Session ID 65540

Action block

Application pop3

Rule Unexpected Traffic

Rule UUID f0ebfc60-bf3f-4f89-a060-f059dc110ac9

Verdict malicious

Device SN 007058000116936

IP Protocol tcp

Source

Source User

Source 66.1.1.8

Source DAG

Port 38691

Zone L3-TAP

Interface ethernet1/4

Destination

Destination User

Destination 10.154.10.167

Destination DAG

Port 110

Zone L3-TAP

Interface ethernet1/4

Details

PCAP	RECEIVE TIME	TYPE	APPLICA...	ACTION	RULE	RULE UUID	BY...	SEVERI...	CATEG...	URL CATEG...	VERDI...	URL	FILE NAME
	2022/02/19 07:21:14	wildfire	pop3	block	Unexp... Traffic	f0ebfc...		informa...			malicio...		Id9uv1...
	2022/02/19 07:21:14	wildfire	pop3	block	Unexp... Traffic	f0ebfc...		informa...			malicio...		Id9uv1...
	2022/02/19 07:21:14	wildfire	pop3	block	Unexp... Traffic	f0ebfc...		informa...			malicio...		Id9uv1...

Close

Figura 5-159: Ejemplo de log de WildFire detallado

Detailed Log View

Log Info | **WildFire Analysis Report**

WildFire Analysis Summary [Download PDF](#)

File Information

File Type	RTF
File Signer	
SHA-256	1d6a6ad6ce3bf3e924135ae56a017e60bc8f80fa3ebaf159336f4a024a3e6a
MD5	7734c34c6a9656a4d6bf682a85742d76
File Size	23 bytes
First Seen Timestamp	2014-01-26 06:54:43 UTC
Verdict	malware (Updated on 2019-01-03)
Sample File	Download File

Coverage Status

For endpoint anti-virus coverage information for this sample, visit [Virus Total](#)

Dynamic Analysis

Virtual Machine 1 **Virtual Machine 2**

This virtual machine is configured with the following software: Windows XP, Adobe Reader 9.4.0, Flash 10, Office 2007.

Behavior Summary

The file was found to be suspicious on this virtual machine.

Behavior

- Created a file in the Windows folder
- Created or modified files
- Modified Windows registries

Network Activity

No network data available

Host Activity (by process)

Select a process below to view detailed forensics on the activities performed on the host by individual processes.

[C:\Program Files\Microsoft Office\Office12\WINWORD.EXE](#)

PCAP	RECEIVE TIME	TYPE	APPLICATION	ACTION	RULE	RULE UUID	BYT...	SEVERITY	CATEGOR...	URL CATEGOR...	VERDICT	URL	FILE NAME
------	--------------	------	-------------	--------	------	-----------	--------	----------	------------	----------------	---------	-----	-----------

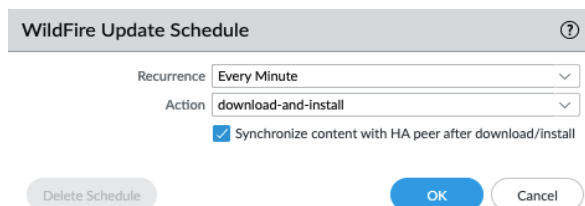
[Close](#)

Figura 5-160: Ejemplo de informe de WildFire integrado en el cortafuegos

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

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.



The image shows the 'WildFire Update Schedule' configuration window. It has a title bar with a question mark icon. Inside, there are two dropdown menus: 'Recurrence' set to 'Every Minute' and 'Action' set to 'download-and-install'. Below these is a checked checkbox labeled 'Synchronize content with HA peer after download/install'. At the bottom, there are three buttons: 'Delete Schedule', 'OK', and 'Cancel'.

Figura 5-161: Actualizaciones de WildFire

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.

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:

	Generate Time	Type	Name	From Zone	To Zone	Attacker	Attacker Name	Victim	Victim Name	To Port	Application	Action	Severity
	08/05 10:16:46	wildfire-virus	Virus/Win32.VGeneric.fqmy	untrust	LAN	54.155.123.115		192.168.3.102	labeibob	2831	web-browsing	reset-both	medium

Figura 5-162: Ejemplo de log generado por una firma de WildFire

Notificación al usuario

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 5-163: Ejemplo de página de bloqueo de WildFire

5.12.12 INSPECCIÓN SSL

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.

El descifrado del cortafuegos de Palo Alto Networks se basa en políticas, y puede usarse para descifrar, examinar y controlar las conexiones SSL 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 a texto plano, y después aplica App-ID y los ajustes de seguridad en el tráfico de texto plano, incluidos los ajustes de las funciones de Descifrado, Antivirus, *Vulnerability Protection*, *Antispyware*, Filtrado de URL y perfiles de bloqueo de archivos. Cuando el tráfico se haya descifrado y examinado en el cortafuegos, el tráfico de texto sin cifrar se volverá a cifrar al salir del cortafuegos para asegurar su privacidad y seguridad.

Los cortafuegos de Palo Alto Networks ofrecen los siguientes tipos de descifrado:

- Descifrado SSL en salida (*SSL Forward Proxy*).
- Descifrado SSL 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/pan-os/10-2/pan-os-admin/decryption>

Los cortafuegos de Palo Alto Networks permiten descifrar, obtener visibilidad, e impedir amenazas conocidas como desconocidas sobre el protocolo TLSv1.3. 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).

Se pueden solucionar los problemas relacionados con el descifrado de SSL 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 TLS, tráfico no TLS, tráfico descifrado y tráfico 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.

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.

5.12.12.1 REQUISITOS DE SEGURIDAD

Se debe configurar el descifrado SSL 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*).

Opcionalmente, puede también establecer criterios para el control de los protocolos que se utilizan vía SSL, 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

Ubicación: “*Policies > Decryption*”

Requisito de seguridad: Se debe configurar el descifrado SSL 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*).

	Name	Tags	Source			Destination		URL Category	Service	Action	Type	Decryption Profile
			Zone	Address	User	Zone	Address					
1	Excepciones-Descifrado...	none	LAN	any	any	Internet	any	financial-services	any	no-decrypt	ssl-forward-proxy	none
2	Descifrad-Salida	none	LAN	any	any	Internet	any	health-and-med...	any	decrypt	ssl-forward-proxy	none

Figura 5-164: Política de SSL Forward Proxy

2. Configurar la inspección SSL en entrada

Ubicación: “*Policies > Decryption*”

Requisito de seguridad: Se debe configurar el descifrado SSL en entrada para todo el tráfico de servicios que preste al exterior, típicamente aquellos ubicados en DMZs o Datacenter.

Se pueden configurar reglas de política de inspección de entrada SSL 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.

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 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.

En la pestaña “*Options*” en “*Type*” elegir “*SSL Inbound Inspection*” y bajo “*Certificates*” se añaden los certificados.

Decryption Policy Rule ?

General | Source | Destination | Service/URL Category | **Options**

Action ☐ No Decrypt ☒ Decrypt

Type **SSL Inbound Inspection**

Certificates

☒	CERTIFICATES ^
☐	cert_9
☐	fwd-proxy
☐	inbound-cert
☐	leaf-cert
☐	new-inbound

+ Add - Delete

Decryption Profile **default**

Log Settings

☒ Log Successful SSL Handshake

☒ Log Unsuccessful SSL Handshake

Log Forwarding **None**

OK Cancel

Figura 5-165: Selección de certificados para la inspección SSL entrante

Name	Tags	Source			Destination		URL Category	Service	Action	Type	Decryption Profile
		Zone	Address	User	Zone	Address					
3 Descifrado-DMZ	none	Internet	any	any	DMZ	Servidor-web-externo	any	any	decrypt	ssl-inbound-inspection Servidor Web Externo	none

Figura 5-166: Política de SSL Inbound Inspection

5.12.12.2 OBSERVABLES

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.

Detailed Log View		
Session ID 33736 Action allow Action Source from-policy Host ID Application ssl Rule Unknown User SSL and Web Rule UUID 39388395-1f90-4e9c-aeaa-ca99af636ce1 Session End Reason tcp-fin Category educational-institutions Device SN IP Protocol tcp Log Action Generated Time 2022/03/15 15:20:32 Start Time 2022/03/15 15:20:27 Receive Time 2022/03/15 15:20:32 Elapsed Time(sec) 0 Tunnel Type N/A	Source User Source 70.143.78.216 Source DAG Country United States Port 63756 Zone L3-TAP Interface ethernet1/4 X-Forwarded-For IP	Destination User Destination 10.154.1.46 Destination DAG Country 10.0.0.0-10.255.255.255 Port 443 Zone L3-TAP Interface ethernet1/4
	Details Type end Bytes 11565 Bytes Received 9238 Bytes Sent 2327 Repeat Count 1 Packets 23 Packets Received 13 Packets Sent 10 Source UUID Destination UUID Dynamic User Group	Flags Captive Portal ☐ Proxy Transaction ☐ Decrypted ☐ Packet Capture ☐ Client to Server ☐ Server to Client ☐ Symmetric Return ☐ Mirrored ☐ Tunnel Inspected ☐ MPTCP Options ☐ Recon excluded ☐

Figura 5-167: Detalle de logs

5.12.13 INSPECCIÓN DE CONTENIDO TUNELIZADO

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*)

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.

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.

La inspección de túneles está soportada si el cortafuegos está funcionando en modo nivel 3, nivel 2, *virtual wire* y TAP.

En la siguiente figura se muestran los dos niveles de inspección de túneles que el cortafuegos puede inspeccionar:

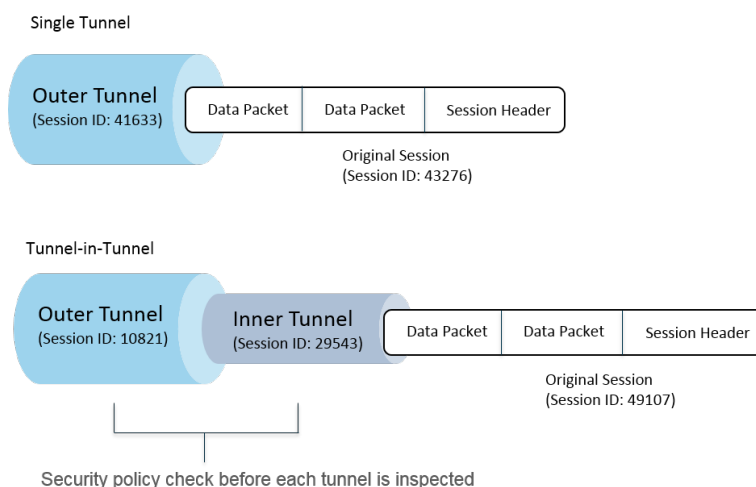


Figura 5-168: Esquema cabeceras Inspección de túneles

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 5-169: Políticas soportadas en tráfico tunelizado

- 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).

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.

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/10-2/pan-os-networking-admin/tunnel-content-inspection/view-tunnel-information-in-logs>

5.12.13.1 EJEMPLO DE USO

En el ejemplo, se configura la inspección del tráfico encapsulado en un túnel GRE:

Ubicación: “Policies > Tunnel Inspection > Add”

The screenshot shows the 'Tunnel Inspection Policy Rule' configuration window. The 'General' tab is active, displaying the following fields:

- Name:** GRETunnelinsp
- Description:** (empty text area)
- Tags:** (dropdown menu)
- Group Rules By Tag:** None
- Audit Comment:** (empty text area)

At the bottom right, there are 'OK' and 'Cancel' buttons. A link for 'Audit Comment Archive' is visible below the audit comment field.

Figura 5-170: Configuración de regla de inspección de tráfico (General)

En la pestaña *Source* se indica la zona, dirección y usuario origen:

The screenshot shows the 'Tunnel Inspection Policy Rule' configuration window with the 'Source' tab selected. The window has four tabs: General, Source, Destination, and Tunnel ID. The 'Source' tab contains three columns: 'SOURCE ZONE', 'SOURCE ADDRESS', and 'SOURCE USER'. Each column has a list of items with checkboxes. In the 'SOURCE ZONE' column, 'Any' is unchecked and 'GRE_Tunnel' is checked. In the 'SOURCE ADDRESS' column, 'Any' is checked. In the 'SOURCE USER' column, 'any' is selected in the dropdown. At the bottom of each column are '+ Add' and '- Delete' buttons. A 'Negate' checkbox is at the bottom center. 'OK' and 'Cancel' buttons are at the bottom right.

Figura 5-171: Configuración de regla de inspección de tráfico (Source)

En la pestaña *Destination* se indica la zona/dirección destino:

The screenshot shows the 'Tunnel Inspection Policy Rule' configuration window with the 'Destination' tab selected. The window has four tabs: General, Source, Destination, and Tunnel ID. The 'Destination' tab contains two columns: 'DESTINATION ZONE' and 'DESTINATION ADDRESS'. Each column has a list of items with checkboxes. In the 'DESTINATION ZONE' column, 'Any' is unchecked and 'GRE_tunnel' is checked. In the 'DESTINATION ADDRESS' column, 'Any' is checked. At the bottom of each column are '+ Add' and '- Delete' buttons. A 'Negate' checkbox is at the bottom center. 'OK' and 'Cancel' buttons are at the bottom right.

Figura 5-172: Configuración de regla de inspección de tráfico (Destination)

En la pestaña *Inspection* se indica el tipo de túnel, máximo número de niveles de inspección, dirección y usuario origen:

Tunnel Inspection Policy Rule

General | Source | Destination | **Inspection** | Tunnel ID

Protocols

- ☐ TUNNEL PROTOCOL
- ☒ GRE
- GRE
- Non-encrypted IPSec
- VXLAN

Inspect Options | Security Options | Monitor Options

Maximum Tunnel Inspection Levels: ☒ One Level ☐ Two Levels (Tunnel In Tunnel)

- ☐ Drop packet if over maximum tunnel inspection level
- ☐ Drop packet if unknown protocol inside tunnel
- ☐ Drop packet if tunnel protocol fails strict header check
- ☐ Return scanned VXLAN tunnel to source

Select optional protocol inspection and enforcement items.

OK Cancel

Inspect Options | **Security Options** | Monitor Options

☒ Enable Security Options

Tunnel Source Zone: [Dropdown]

Tunnel Destination Zone: [Dropdown]

Assign optional security zones for separate security policy treatment of tunnel content.

OK Cancel

Figura 5-173: Configuración de regla de inspección de tráfico (Inspection)

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.

5.12.13.2 OBSERVABLES

Ubicación: "ACC > Virtual System/All > Tunnel Activity"

Export

Time: [Dropdown: Last 30 Calendar Days]

02/13 00:00:00-03/14 23:59:59

Global Filters: [Clear all]

Network Activity | Threat Activity | Blocked Activity | **Tunnel Activity** | GlobalProtect Activity | SSL Activity | +

Tunnel ID Usage

- ☒ bytes
- ☐ sessions
- ☐ threats
- ☐ content
- ☐ URLs

Home

Tunnel Monitor Tag Usage

- ☒ bytes
- ☐ sessions
- ☐ threats
- ☐ content
- ☐ URLs

Home

Figura 5-174: Monitorización de tráfico tunelizado

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"):

Detailed Log View		
General Session ID 228638 Action allow Action Source from-policy Host ID Application ssl Rule Unknown User SSL and Web Rule UUID 8938395-1190-4e9c-a0ca- ca99a1636cc1 Session End Reason aged-out Category educational-institutions Device SN IP Protocol tcp Log Action Generated Time 2023/03/15 15:35:28 Start Time 2023/03/15 15:26:40 Receive Time 2023/03/15 15:35:28 Elapsed Time(us) 468 Tunnel Type N/A	Source Source User Source 24.5.247.169 Source DAG Country United States Port 51287 Zone L3-TAP Interface ethernet1/4 X-Forwarded-For IP Details Type end Bytes 5724 Bytes Received 3112 Bytes Sent 2612 Repeat Count 1 Packets 17 Packets Received 9 Packets Sent 8 Source UUID Destination UUID Dynamic User Group Network Slice ID SD Network Slice ID SST	Destination Destination User Destination 10.154.7.4 Destination DAG Country 10.0.0.0-10.255.255.255 Port 443 Zone L3-TAP Interface ethernet1/4 Flags Captive Portal ☐ Proxy Transaction ☐ Decrypted ☐ Packet Capture ☐ Client to Server ☐ Server to Client ☐ Symmetric Return ☐ Mirrored ☐ Tunnel Inspected ☐ Not for Inspection ☐ Recon excluded ☐ Forwarded in Security Chain ☐

Figura 5-175: Vista de detalle de log (flag tunnel inspected)

5.12.14 MOTOR DE CORRELACIÓN AUTOMATIZADO

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, a partir de la versión 7.0 de PAN-OS. 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.

Nota: Si se desea obtener más información sobre el motor de correlación automatizado, consultar el siguiente enlace:

<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/monitor/monitor-automated-correlation-engine>

5.12.14.1 RECOMENDACIONES

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”.

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.

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 5-176: Correlation Objects predefinidos en el sistema

5.12.14.2 OBSERVABLES

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 5-177: Logs de ejemplo del motor automático de correlación

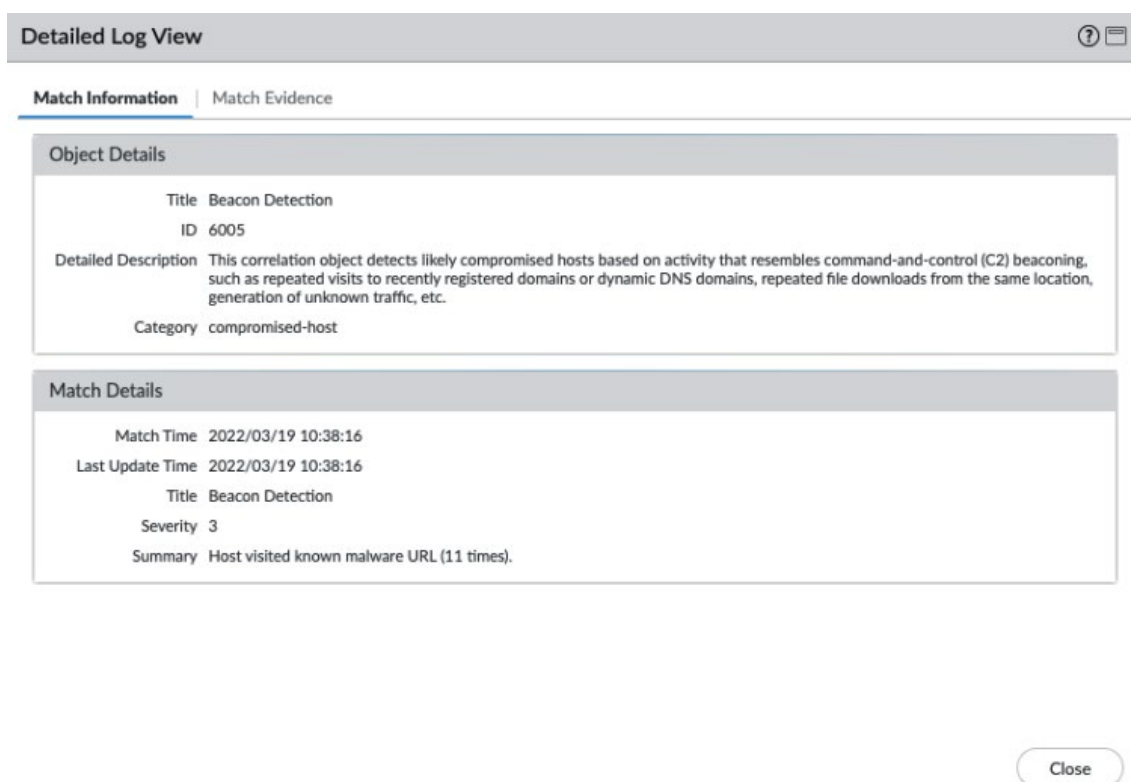


Figura 5-178: Logs de ejemplo del motor automático de correlación (detalle)

5.12.15 FIRMAS DE LOS MÓDULOS DE PREVENCIÓN

5.12.15.1 RENDIMIENTO Y NÚMERO DE FIRMAS

El rendimiento de los módulos de *Threat Prevention* no se ve impactado 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.

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.

La siguiente figura muestra un ejemplo de configuración con DSRI habilitado para los servidores de una DMZ:

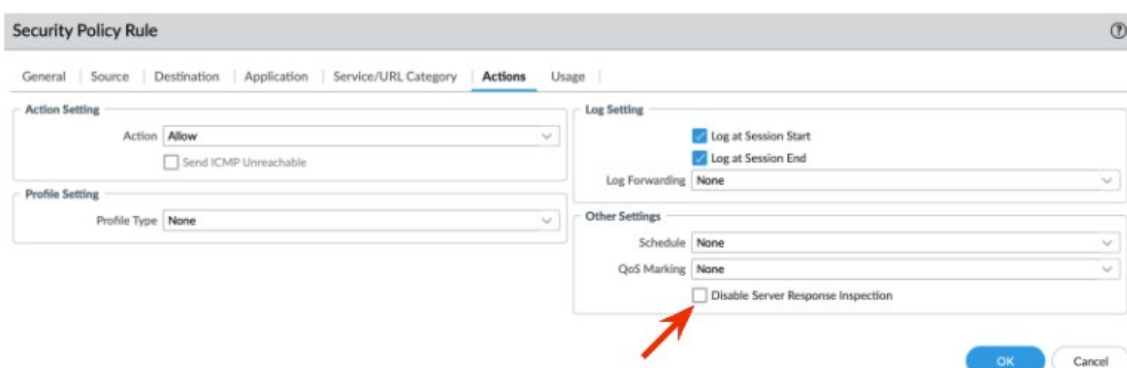


Figura 5-179: Ejemplo de activación de DSRI

5.12.15.2 ACCIÓN POR DEFECTO PARA LAS FIRMAS

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*.

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.

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*

Vulnerability Protection Rule ⓘ

Rule Name:

Threat Name:
Used to match any signature containing the entered text as part of the signature name

Action: Packet Capture:

Host Type: Category:

☒ Any
☐ CVE ^

Used to match any signature containing the entered text as part of the signature CVE or Vendor ID

Figura 5-180: Acciones de las firmas de Anti-Spyware y Vulnerability Protection

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*

Antivirus Profile ⓘ

Name: default-1

Description:

Action | Signature Exceptions | WildFire Inline ML

☐ Enable Packet Capture

Decoders

PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION
ftp	default (reset-both)	default (reset-both)	default (reset-both)
http	default (reset-both)	default (reset-both)	default (reset-both)
http2	default (reset-both)	default (reset-both)	default (reset-both)
imap	default (alert)	default (alert)	default (alert)
pop3	default (alert)	default (alert)	default (alert)
smb	allow	default (reset-both)	default (reset-both)
smtp	alert	default (alert)	default (alert)
	drop		
	reset-client		
	reset-server		
	reset-both		

Application Exceptions

APPLICATION

0 items → ×

OK Cancel

Figura 5-181: Acciones de las firmas de Antivirus

5.13 PREVENCIÓN Y DETECCIÓN DE ATAQUES

5.13.1 ATAQUES DOS

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.

Es importante señalar que es posible emplear ambos mecanismos en el mismo perfil de DoS.

5.13.1.1 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 16: Cadena de ciberataque - DoS/Zone Protection

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.

5.13.1.2 RECOMENDACIONES

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*.

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

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/10-2/pan-os-admin/monitoring/netflow-monitoring>

Las siguientes figuras muestran un ejemplo de protección con los valores por defecto.

The image displays two side-by-side screenshots of the 'DoS Protection Profile' configuration window in the Palo Alto Networks management interface. Both windows show a profile named 'Mi-DOS' with the 'Classified' type selected.

Left Screenshot (Flood Protection tab):

- Name:** Mi-DOS
- Description:** (empty)
- Type:** ☐ Aggregate, ☒ Classified
- Tab:** Flood Protection (selected)
- Sub-tab:** SYN Flood (selected)
- Action:** Random Early Drop
- Alarm Rate (connections/s):** 10000
- Activate Rate (connections/s):** 10000
- Max Rate (connections/s):** 40000
- Block Duration (s):** 300

Right Screenshot (Resources Protection tab):

- Name:** Mi-DOS
- Description:** (empty)
- Type:** ☐ Aggregate, ☒ Classified
- Tab:** Resources Protection (selected)
- Sub-tab:** Sessions (selected)
- Maximum Concurrent Sessions:** 32768

Both windows have 'OK' and 'Cancel' buttons at the bottom.

Figura 5-182: Configuración por defecto perfil de protección DoS

2. Ratios Máximos

Cuando se exceden los umbrales establecidos en los “*Maximal Rate*”, cualquier paquete que haga *match* con la política de protection 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

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.

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

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*.

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.

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.

5.13.1.3 EJEMPLO DE USO

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

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 geo-localizada 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

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:

	NAME	TAGS	Source			Destination		SERVICE	ACTION	Protection		SCHEDULE	LOG FORWARDING
			ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS			AGGREGATE	CLASSIFIED		
1	Protection_Web	none	IPs seguras	any	any	Internet	any	any	deny	none	profile: Mi-DoS src-dest-ip-both	none	none

Figura 5-183: Ejemplo de política DoS

5.13.1.4 OBSERVABLES

Flood Protection

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”.

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:

	Receive Time	Type	Name	From Zone	To Zone	Attacker	Victim	To Port	Application	Action	Severity
	11/17 19:35:44	flood	UDP Flood	LAN	Internet	192.168.3.25	0.0.0.0	0	not-applicable	random-drop	critical
	11/17 19:31:05	flood	UDP Flood			0.0.0.0	0.0.0.0	0	not-applicable	random-drop	critical

Figura 5-184: Ejemplo de logs de Flood Protection

Resource Protection

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 5-185: Ejemplo de log de Resource Protection

Es importante tener en cuenta que los equipos de Palo Alto Networks agregan 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:

Detailed Log View		
General	Source	Destination
Session ID 0 Action drop Application not-applicable Rule Proteger DMZ Virtual System Device SN IP Protocol hopopt Log Action Generated Time 2016/11/17 19:42:33 Receive Time 2016/11/17 19:42:33	Attacker Name Attacker 192.168.3.25 Country 192.168.0.0-192.168.255.255 Port 0 Zone Interface	Victim Name Victim 0.0.0.0 Country 0.0.0.0-0.255.255.255 Port 0 Zone Interface
	Details	Flags
	Threat Type: flood Threat Name: Session Limit Event ID 8801 Severity: critical Repeat Count: 2062 File Name URL Pcap ID 0	Captive Portal ☐ Proxy Transaction ☐ Decrypted ☐ Packet Capture ☐ Client to Server ☒ Server to Client ☐

Figura 5-186: 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>

5.13.2 INFORME DE COMPORTAMIENTO DE BOTNET

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.

5.13.2.1 RECOMENDACIONES

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.

Es posible personalizar el módulo para adecuarlo a las características de cada entorno tal y como muestra la siguiente imagen:

The screenshot shows the 'Botnet Configuration' window with a help icon. It contains three main sections:

- HTTP Traffic:** A table with columns ENAB..., COUNT, EVENT, and DESCRIPTION.

ENAB...	COUNT	EVENT	DESCRIPTION
☒	5	Malware URL visit	Identifies users communicating with known malware URLs based on Malware and Botnet URL filtering categories
☒	5	Use of dynamic DNS	Looks for dynamic DNS query traffic which could be indicative of botnet communication
☒	10	Browsing to IP domains	Identifies users that browse to IP domains instead of URLs
☒	5	Browsing to recently registered domains	Looks for traffic to domains that have been registered within the last 30 days
☒	5	Executable files from unknown sites	Identifies executable files downloaded from unknown URLs
- Unknown Applications:** Two sub-tables for TCP and UDP.

Unknown TCP		Unknown UDP	
Sessions Per Hour	10 [1 - 3600]	Sessions Per Hour	10 [1 - 3600]
Destinations Per Hour	10 [1 - 3600]	Destinations Per Hour	10 [1 - 3600]
Minimum Bytes	50 [1 - 200]	Minimum Bytes	50 [1 - 200]
Maximum Bytes	100 [1 - 200]	Maximum Bytes	100 [1 - 200]
- Other Applications:** A list with one item, IRC, which is checked.

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

Figura 5-187: Personalización del Behavioral Botnet Report

5.13.2.2 OBSERVABLES

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/4GBrd6
3	4	172.16.33.231	pancademo\alex.bell	Repeatedly visited (22) the same malicious URL antonello.messina.it/4GBrd6
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 5-188: Ejemplo de Behavioral Botnet Report

5.13.3 EVASIONES Y CONTRAMEDIDAS

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 es un mecanismo simple y efectivo de hacer *bypass* de un cortafuegos cuando no se realiza descifrado SSL, porque simplemente no podrá inspeccionar el tráfico.

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

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 auditoria. 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.
- 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

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	☐	☐	
Instalación en un entorno seguro	☐	☐	
CONFIGURACIÓN			
ANTES DE COMENZAR			
Integración de la gestión en una red protegida	☐	☐	
Registro de los equipos	☐	☐	
Registro de las licencias	☐	☐	
Actualización de contenidos	☐	☐	
Actualización de firmware	☐	☐	
Segmentación con zonas	☐	☐	
MODO DE OPERACIÓN SEGURO			
Modo de Operación seguro activado (FIPS-CC)	☐	☐	
GESTIÓN DEL EQUIPO			
Métodos de acceso	☐	☐	
Banner de conexión	☐	☐	
Requisitos mínimos de contraseña	☐	☐	
Cambiar usuario y contraseña por defecto	☐	☐	
Configurar otras cuentas de administración	☐	☐	
Configurar <i>timeouts</i> de sesión	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Configurar comportamiento de intentos fallidos de autenticación	☐	☐	
Securización SNMP	☐	☐	
Securización de los updates	☐	☐	
Frecuencia y planificación de updates de aplicaciones y amenazas	☐	☐	
Frecuencia y planificación de updates de Antivirus	☐	☐	
Frecuencia y planificación de updates de WildFire	☐	☐	
Configuración NTP	☐	☐	
PROTOCOLOS SEGUROS			
Configurar IKE / IPsec	☐	☐	
Configurar de HTTPS / TLS	☐	☐	
PROTOCOLOS NO SEGUROS			
Deshabilitar protocolos no seguros	☐	☐	
CERTIFICADOS			
Instalar certificados	☐	☐	
Instalar certificados de CA raíz (<i>root CA certificates</i>)	☐	☐	
Configurar validación de certificados	☐	☐	
SERVIDORES DE AUTENTICACIÓN			
Configurar perfiles de autenticación	☐	☐	
Restringir usuarios que se puedan autenticar	☐	☐	
Configurar doble factor de autenticación	☐	☐	
AUDITORÍA			
Configurar logging de todo el tráfico relevante	☐	☐	
Habilitar <i>FIPS-CC Specific Logging</i>	☐	☐	
Habilitar <i>Packet Drop Logging</i>	☐	☐	
Habilitar <i>TLS Session Logging</i>	☐	☐	
Habilitar CA (OCSP/CRL) <i>Session Establishment Logging</i>	☐	☐	
Habilitar <i>IKE Session Establishment Logging</i>	☐	☐	
Política de auditoría de cambios	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Configurar los parámetros para almacenamiento local	☐	☐	
Configurar el envío a servidor <i>syslog</i>	☐	☐	
BACKUPS			
Backups automáticos programados	☐	☐	
CONFIGURACIÓN DE HA			
HA sincronizado	☐	☐	
Configuración de <i>link/path monitoring</i>	☐	☐	
Exclusión entre <i>Preemption</i> y <i>Passive Link State</i>	☐	☐	
VPNs			
Configuración de VPNs <i>site-to-site</i>	☐	☐	
Configuración de VPNs acceso remoto (<i>GlobalProtect</i>)	☐	☐	
APP-ID Y POLÍTICAS			
Usar aplicaciones en las políticas de seguridad	☐	☐	
Evitar el uso de Service “Any”	☐	☐	
Configurar regla de “Deny” explícita	☐	☐	
Aplicaciones específicas para tráfico propietario	☐	☐	
IDENTIFICACIÓN DE LOS USUARIOS			
Mapeo de Usuario-IP para todo el tráfico de usuarios	☐	☐	
Deshabilitar User-ID en los interfaces externos	☐	☐	
Deshabilitar WMI si no se utiliza	☐	☐	
Configurar <i>Include/Exclude networks</i>	☐	☐	
Configurar una cuenta dedicada para User-ID	☐	☐	
Restringir el tráfico de User-ID hacia zonas inseguras	☐	☐	
FILTRADO DE URLS			
Utilizar URL <i>Filtering</i> en todas las reglas hacia internet	☐	☐	
Activar el <i>logging</i> de cabeceras HTTP	☐	☐	
Desactivar el <i>logging</i> solo de <i>Container Pages</i>	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
IPS (VULNERABILITY PROTECTION)			
Configurar perfil de <i>Vulnerability Protection</i>	☐	☐	
Utilizar <i>Vulnerability Protection</i> en todas las reglas que permitan tráfico	☐	☐	
ANTI-SPYWARE			
Configurar perfil de <i>Anti-Spyware</i>	☐	☐	
Configurar <i>DNS Sinkholing</i>	☐	☐	
Utilizar <i>Anti-Spyware</i> en todas las reglas que permitan tráfico hacia Internet	☐	☐	
ANTIVIRUS			
Configurar perfil de Antivirus	☐	☐	
Utilizar Antivirus en todas las reglas que permitan tráfico	☐	☐	
BLOQUEO DE FICHEROS			
Configurar perfil de <i>File Blocking</i>	☐	☐	
Utilizar <i>File Blocking</i> en todas las reglas que permitan tráfico	☐	☐	
WILDFIRE			
Configurar el uso de la nube pública europea	☐	☐	
Incrementar el tamaño de archivo en <i>WildFire</i>	☐	☐	
Envío de la información de sesión a <i>WildFire</i>	☐	☐	
Configurar <i>forwarding</i> para el tráfico SSL descifrado	☐	☐	
Configurar perfil de <i>WildFire Analysis</i> para todos los ficheros	☐	☐	
Configurar perfil de Antivirus	☐	☐	
Utilizar <i>WildFire Analysis</i> y Antivirus en todas las reglas que permitan tráfico	☐	☐	
Verificar que el servicio de <i>WildFire</i> funciona	☐	☐	
INSPECCIÓN SSL			
Configurar la inspección SSL en salida	☐	☐	
Configurar la inspección SSL en entrada	☐	☐	
INSPECCIÓN DE CONTENIDO TUNELIZADO			
Configurar la inspección de contenido tunelizado	☐	☐	

ACCIONES	SÍ	NO	OBSERVACIONES
Incluir la revisión periódica de los logs generados, en los procedimientos operativos	☐	☐	
CORRELATION ENGINE			
Activar todos los <i>Correlation Objects</i>	☐	☐	
PREVENCIÓN DE ATAQUES DE DOS			
Configurar <i>Flood Protection</i>	☐	☐	
Configurar <i>Resources Protection</i>	☐	☐	
Ajustar valores por defecto y ratios máximos	☐	☐	
INFORMES DE COMPORTAMIENTO BOTNET			
Incluir la revisión diaria de los informes generados, en los procedimientos operativos	☐	☐	
OPERACIÓN			
Comprobaciones periódicas del <i>hardware</i> y el <i>software</i>	☐	☐	
Comprobaciones periódicas de la integridad del <i>firmware</i>	☐	☐	
Comprobaciones periódicas de la operación de los algoritmos y funciones criptográficas	☐	☐	
Actualizaciones periódicas y parches de seguridad	☐	☐	
Realización de <i>backups</i> automáticos	☐	☐	
Mantenimiento de los registros de auditoría	☐	☐	
Revisión periódica de los cambios de configuración del sistema	☐	☐	
Revisión periódica de los registros de auditoría	☐	☐	
Revisión diaria del comportamiento de <i>botnets</i>	☐	☐	
Revisión periódica de logs de <i>Correlations Objects</i>	☐	☐	

8. REFERENCIAS

- Palo Alto Networks official documentation for PAN-OS 10.2:
<https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-admin/getting-started>
- *Advanced Threat Prevention*:
<https://docs.paloaltonetworks.com/advanced-threat-prevention/administration/threat-prevention>
- *Palo Alto Firewall Security Configuration Benchmark*
<https://www.sans.org/reading-room/whitepapers/auditing/palo-alto-firewall-security-configuration-benchmark-35777>
- *CIS Palo Alto Firewall 6 Benchmark V1.0.0*:
<https://benchmarks.cisecurity.org/downloads/show-single/?file=palofirewall.100>
- *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>

