



SOLUZIONI

INFORMES DE SOLUCIONES DE SEGURIDAD PERIMETRAL DEL 06/07 AL 05/08

Presentado a:



Título del Servicio:	“Servicio de renovación de Soporte y licenciamiento para la Plataforma de Seguridad Perimetral y Seguridad de Correo para la Red y Sistemas del INSN”
Número de Contrato:	CONTRATO N° 054 -INSN-2022
Número de Proceso de Selección	ADJUDICACIÓN SIMPLIFICADA N° 029-2022-INSN-1
Área:	Soporte y posventa
Versión:	1.0
Fecha de Edición:	06/08/2024
Escrito por:	Soluzioni Group – Jefatura de Soporte y Postventa
Revisado por:	Luis Fernando Cieza Casanova
Aceptado por:	Miguel Sanguineti Ascencios

REGISTRO DE EDICIONES

Edición	Fecha	Información del Documento	Descripción de los cambios
1.0	06/08/2024		Primera edición del documento



SOLUZIONI

REPORTE MENSUAL DEL FIREWALL

**“Servicio de Seguridad Perimetral en Alta
Disponibilidad para el INSN”**



Project Manager Office Soluzioni

Contenido

INTRODUCCIÓN	5
1. Protección contra amenazas - Perfil de Seguridad de Antivirus	6
1.1. Top de amenazas de virus detectadas.....	7
2. Protección contra amenazas – Perfil de Seguridad de Anti-Spyware	8
2.1 Top de amenazas de spyware detectadas.....	9
3. Protección contra amenazas – Perfil de Seguridad de Protección contra Vulnerabilidades	10
3.1 Top de amenazas de vulnerabilidades detectadas	11
4. Principales fuentes y destinos.....	14
5. Otros reportes del sistema.....	15
5.1. Hosts que visitaron URLs Maliciosas	15
5.2 Actividad de Amenaza	16
5.3 Actividad de Usuario	17
5.3. Bloqueo por políticas de seguridad	18
5.4. Aplicaciones más usadas.....	19
5.5. Actividad de conexiones exitosas al GlobalProtect.....	20
6. Recomendaciones de Seguridad con el fin de Mejorar el Entorno de la Entidad.....	21



Ilustraciones

Ilustración 1: Perfil de Seguridad de Antivirus..... 6

Ilustración 2: Perfil de Seguridad de Anti-Spyware 8

Ilustración 3: Lista de amenazas de spyware detectadas..... 9

Ilustración 4: Perfil de Seguridad de Vulnerabilidades 10

Ilustración 5: Lista de amenazas de vulnerabilidades detectadas..... 11

Ilustración 6: Regiones de origen con mayor tráfico 14

Ilustración 7: Regiones de destino con mayor tráfico 14

Ilustración 8: Host con más visitas a URLs maliciosas..... 15

Ilustración 9: Actividad de Amenazas 16

Ilustración 10: Actividad de Usuario..... 17

Ilustración 11: Bloqueo por Políticas de Seguridad 18

Ilustración 12: Aplicaciones más usadas 19

Ilustración 13: Usuarios con mayor cantidad de conexiones exitosas en Global Protect..... 20



INTRODUCCIÓN

Palo Alto Firewall es una solución que permite el uso seguro de las aplicaciones a través de una identificación precisa de cada aplicación que atravesará su red, también mantiene una visibilidad y un control completo que permite proteger a la organización de las amenazas cibernéticas más recientes. Todo esto gracias a que en cada política de seguridad también se puede especificar perfiles de seguridad que ayudan a protegerse contra virus, spyware y otras amenazas.

En el presente informe perteneciente al mes de JULIO se detalla a través de diferentes reportes guías que brinda la solución que ayudan a tener una visión general de las amenazas, riesgos y vulnerabilidades, lo cual le permitirá tomar las medidas adecuadas de prevención.



1. Protección contra amenazas - Perfil de Seguridad de Antivirus

Los perfiles antivirus protegen contra virus, gusanos y troyanos, así como contra descargas de spyware. Este perfil analiza en busca de una amplia variedad de malware en ejecutables, archivos PDF, HTML y virus JavaScript, incluida la compatibilidad con el análisis de archivos comprimidos y esquemas de codificación de datos que se transfieran a través de los siguientes protocolos: HTTP, FTP, SMTP, IMAP, POP3 y SMB.

Se tiene configurado 2 perfiles aparte del perfil que viene por defecto (default), uno en estado de monitoreo que solo registra lo detectado (alert) y el otro con acción de bloqueo (reset-both).

<input type="checkbox"/>	NAME	LOCATION	PACKET CAPTURE	Decoders				Application Exceptions		WildFire Inline ML	
				PROTOCOL	SIGNATURE ACTION	WILDFIRE SIGNATURE ACTION	WILDFIRE INLINE ML ACTION	APPLICATION	ACTION	MODEL	ACTION SETTING
<input type="checkbox"/>	default	Predefined	<input type="checkbox"/>	http	default (reset-both)	default (reset-both)	default (reset-both)			Windows Executables	enable (inherit per-protocol actions)
				http2	default (reset-both)	default (reset-both)	default (reset-both)			PowerShell Script 1	enable (inherit per-protocol actions)
				smtp	default (alert)	default (alert)	default (alert)			PowerShell Script 2	enable (inherit per-protocol actions)
				imap	default (alert)	default (alert)	default (alert)			Executable Linked Format	enable (inherit per-protocol actions)
				pop3	default (alert)	default (alert)	default (alert)			MSOffice	enable (inherit per-protocol actions)
				ftp	default (reset-both)	default (reset-both)	default (reset-both)			Shell	enable (inherit per-protocol actions)
				smb	default (reset-both)	default (reset-both)	default (reset-both)				
<input type="checkbox"/>	AV		<input checked="" type="checkbox"/>	http	default (reset-both)	default (reset-both)	default (reset-both)			Windows Executables	enable (inherit per-protocol actions)
				http2	default (reset-both)	default (reset-both)	default (reset-both)			PowerShell Script 1	enable (inherit per-protocol actions)
				smtp	reset-both	reset-both	reset-both			PowerShell Script 2	enable (inherit per-protocol actions)
				imap	reset-both	reset-both	reset-both			Executable Linked Format	enable (inherit per-protocol actions)
				pop3	reset-both	reset-both	reset-both			MSOffice	enable (inherit per-protocol actions)
				ftp	default (reset-both)	default (reset-both)	default (reset-both)			Shell	enable (inherit per-protocol actions)
				smb	default (reset-both)	default (reset-both)	default (reset-both)				
<input type="checkbox"/>	Monitor_AV		<input type="checkbox"/>	http	alert	alert	alert			Windows Executables	alert-only (override more strict actions to alert)
				http2	alert	alert	alert			PowerShell Script 1	alert-only (override more strict actions to alert)
				smtp	alert	alert	alert			PowerShell Script 2	alert-only (override more strict actions to alert)
				imap	alert	alert	alert			Executable Linked Format	alert-only (override more strict actions to alert)
				pop3	alert	alert	alert			MSOffice	alert-only (override more strict actions to alert)
				ftp	alert	alert	alert			Shell	alert-only (override more strict actions to alert)
				smb	alert	alert	alert				

1.1. Top de amenazas de virus detectadas

No se ha detectado amenazas con este perfil de seguridad en estos ultimo 31 días.



2. Protección contra amenazas – Perfil de Seguridad de Anti-Spyware

Los perfiles Anti-Spyware bloquean el spyware en los hosts comprometidos para que no intenten llamar a casa o enviar balizas a los servidores externos de command-and-control (C2), lo que le permite detectar el tráfico malicioso que sale de la red desde los clientes infectados.

Se tiene configurado 2 perfiles aparte de los 2 perfiles que viene por defecto (default y strict), uno en estado de monitoreo que solo registra lo detectado (alert) y el otro con acción de bloqueo (reset-both) para severidades medias, altas y críticas, y con acción por defecto según la base de datos de amenazas para severidades baja e informacional.

<input type="checkbox"/>	NAME ▾	LOCATION	COUNT	POLICY NAME	THREAT NAME	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	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
<input type="checkbox"/>	Monitor_AntiSpyware		Policies: 1 Exceptions: 1	Monitor	any	any	alert	disable
<input type="checkbox"/>	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
<input type="checkbox"/>	AS		Policies: 3 Exceptions: 4	C-H	any	critical,high	reset-both	single-packet
				M	any	medium	reset-both	single-packet
				L-I	any	low,informational	default	disable



SOLUZIONI

2.1 Top de amenazas de spyware detectadas

En la siguiente imagen se muestra el TOP 25 de ataques tipo spyware detectados y bloqueados en los últimos 31 días.

	SOURCE ZONE	DESTINATION ZONE	THREAT TYPE	THREAT ID/NAME	ID	HOST ID	APPLICATION	APP CATEGORY	RISK	SEVERITY	ACTION	APP CONTAINER	COUNT
1	LAN	WAN-2	spyware	XMRig Miner Command and Control Traffic Detection	85886		json-rpc	networking	1	critical	reset-both	(null)	24.5k
2	LAN	WAN-1	spyware	XMRig Miner Command and Control Traffic Detection	85886		json-rpc	networking	1	critical	reset-both	(null)	24.4k
3	LAN	WAN-4	spyware	generic:letia.co.uk	653302914		dns-base	networking	3	medium	sinkhole	dns	495
4	LAN	WAN-3	spyware	generic:polyfill.io	651123048		dns-base	networking	3	medium	sinkhole	dns	336
5	LAN	WAN-3	spyware	generic:et5k413t.rest	652902156		dns-base	networking	3	medium	sinkhole	dns	172
6	WAN-3	LAN	spyware	Suspicious User-Agent Strings Detection	10004		web-browsing	general-internet	4	low	alert	(null)	93
7	LAN	WAN-3	spyware	generic:loograich.com	652673103		dns-base	networking	3	medium	sinkhole	dns	88
8	LAN	WAN-3	spyware	generic:rovno.xyz	651873258		dns-base	networking	3	medium	sinkhole	dns	60
9	LAN	WAN-3	spyware	generic:fvohyywkb.com	652215858		dns-base	networking	3	medium	sinkhole	dns	44
10	LAN	WAN-3	spyware	generic:www.augm1.com	653033781		dns-base	networking	3	medium	sinkhole	dns	19
11	WAN-3	LAN	spyware	AndroxGh0st Scanning Traffic Detection	86759		web-browsing	general-internet	4	medium	reset-server	(null)	14
12	WAN-4	LAN	spyware	AndroxGh0st Scanning Traffic Detection	86759		web-browsing	general-internet	4	medium	reset-server	(null)	11
13	LAN	WAN-3	spyware	generic:ak.oneegrou.net	651781248		dns-base	networking	3	medium	sinkhole	dns	8
14	LAN	WAN-3	spyware	generic:duckduckgogg42xjoc72x3jasowarfbgcmvfmaftt6twagswzczad	437592132		dns-base	networking	3	medium	sinkhole	dns	8
15	WAN-1	LAN	spyware	Morto RDP Request Traffic	13274		ms-rdp	networking	4	low	alert	(null)	7
16	WAN-4	LAN	spyware	AndroxGh0st Scanning Traffic Detection	86760		web-browsing	general-internet	4	medium	reset-server	(null)	6
17	WAN-3	LAN	spyware	AndroxGh0st Scanning Traffic Detection	86760		web-browsing	general-internet	4	medium	reset-server	(null)	6
18	WAN-3	LAN	spyware	OSSProxy PUP Traffic Detection	21943		web-browsing	general-internet	4	medium	reset-server	(null)	5
19	LAN	WAN-3	spyware	generic:nousupoupo.com	653726130		dns-base	networking	3	medium	sinkhole	dns	5
20	LAN	WAN-3	spyware	generic:talleres.latarumba.com	653242443		dns-base	networking	3	medium	sinkhole	dns	4
21	LAN	WAN-3	spyware	generic:letia.co.uk	653302914		dns-base	networking	3	medium	sinkhole	dns	4
22	LAN	WAN-3	spyware	generic:ompatratom.com	651492300		dns-base	networking	3	medium	sinkhole	dns	4
23	LAN	WAN-3	spyware	generic:ggwifobvx.com	652947444		dns-base	networking	3	medium	sinkhole	dns	4
24	LAN	WAN-3	spyware	generic:newsfortoday3.xyz	652143405		dns-base	networking	3	medium	sinkhole	dns	4
25	LAN	WAN-3	spyware	generic:dasikjfh2.loi	653007939		dns-base	networking	3	medium	sinkhole	dns	4

Como se puede apreciar en la imagen anterior, se aprecia gran cantidad de amenazas de tráfico C2, esto es un indicador de la presencia de máquinas violadas o comprometidas en la red. También entre las amenazas se puede apreciar que hay varias consultas DNS de amenazas tipo spyware, esto se debe a que hay consultas que buscan una resolución de DNS para dominios potencialmente asociados con el tráfico C2. Se recomienda ubicar los equipos comprometidos apoyándose de los registros de amenazas de la interfaz web del firewall ubicados en la pestaña MONITOR, también puede usar la opción **BOTNET** ubicado en la misma pestaña para identificar los equipos comprometidos por día.
























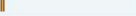

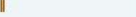
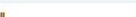
3. Protección contra amenazas – Perfil de Seguridad de Protección contra Vulnerabilidades

Los perfiles de protección contra vulnerabilidades detienen los intentos de aprovechar las fallas del sistema o de obtener acceso no autorizado a los sistemas. Mientras que los perfiles Anti-Spyware ayudan a identificar los hosts infectados a medida que el tráfico sale de la red, los perfiles de Protección contra vulnerabilidades protegen contra las amenazas que ingresan a la red. Por ejemplo, los perfiles de protección contra vulnerabilidades ayudan a proteger contra desbordamientos de búfer, ejecución de código ilegal y otros intentos de aprovechar las vulnerabilidades del sistema.

<input type="checkbox"/>	NAME	LOCATION	COUNT	RULE NAME	THREAT NAME	HOST TYPE	SEVERITY	ACTION	PACKET CAPTURE
<input type="checkbox"/>	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...					
<input type="checkbox"/>	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
<input type="checkbox"/>	VP		Rules: 6	C-H-Client	any	client	critical,high	reset-both	single-packet
			Exceptions: 16	C-H-Server	any	server	critical,high	reset-both	single-packet
				M-Client	any	client	medium	reset-both	single-packet
				M-Server	any	server	medium	reset-both	single-packet
				L-I-Client	any	client	low,informational	default	disable
				L-I-Server	any	server	low,informational	default	disable
<input type="checkbox"/>	Monitor_Vulnerability		Rules: 1	Monitor	any	any	any	alert	disable

Se recomienda ubicar los equipos comprometidos apoyándose de los registros de amenazas de la interfaz web del firewall ubicados en la pestaña MONITOR, también puede usar la opción BOTNET ubicado en la misma pestaña para identificar los equipos comprometidos por día.

En la siguiente imagen se muestra los ataques tipo vulnerabilidad detectados y bloqueados en los últimos 31 días.

	SOURCE ZONE	DESTINATION ZONE	THREAT/CONTENT TYPE	THREAT ID/NAME	ID	APPLICATION	APP CATEGORY	RISK	SEVERITY	ACTION	COUNT
1	WAN-1	LAN	vulnerability	SSH User Authentication Brute Force Attempt	40015	ssh	networking	2	high	reset-both	5.9k 
2	WAN-1	LAN	vulnerability	Non-RFC Compliant SSH Traffic on Port 22	94634	incomplete	unknown	1	informational	alert	5.8k 
3	WAN-4	LAN	vulnerability	OpenVAS Vulnerability Scanner Detection	55283	web-browsing	general-internet	4	medium	reset-both	3.8k 
4	LAN	WAN-1	vulnerability	Non-RFC Compliant SSL Traffic on Port 443	56112	ssl	networking	4	informational	alert	1.4k 
5	LAN	WAN-2	vulnerability	Non-RFC Compliant SSL Traffic on Port 443	56112	ssl	networking	4	informational	alert	1.4k 
6	WAN-3	LAN	vulnerability	ENV File Scanning Attempt	93397	web-browsing	general-internet	4	informational	alert	147 
7	VPN_GP	LAN	vulnerability	Microsoft Windows NTLMSSP Detection	92322	ms-ds-smbv3	business-systems	3	informational	alert	127 
8	WAN-4	LAN	vulnerability	ENV File Scanning Attempt	93397	web-browsing	general-internet	4	informational	alert	112 
9	WAN-3	LAN	vulnerability	ZGrab Application Layer Scanner Detection	57955	web-browsing	general-internet	4	medium	reset-both	109 
10	WAN-4	LAN	vulnerability	ZGrab Application Layer Scanner Detection	57955	web-browsing	general-internet	4	medium	reset-both	108 
11	WAN-3	LAN	vulnerability	TP-Link Archer Router Command Injection Vulnerability	93749	web-browsing	general-internet	4	high	reset-both	95 
12	WAN-4	LAN	vulnerability	TP-Link Archer Router Command Injection Vulnerability	93749	web-browsing	general-internet	4	high	reset-both	92 
13	VPN_GP	LAN	vulnerability	Microsoft Windows NTLMSSP Detection	92322	ldap	business-systems	2	informational	alert	78 
14	WAN-3	LAN	vulnerability	PNG File Chunk Length Abnormal	34243	web-browsing	general-internet	4	low	alert	71 
15	LAN	WAN-4	vulnerability	Non-RFC Compliant DNS Traffic on Port 53/5353	56505	dns-base	networking	3	informational	alert	62 
16	WAN-4	LAN	vulnerability	Non-RFC Compliant HTTP Traffic on Port 80	56391	unknown-tcp	unknown	1	informational	alert	52 
17	LAN	WAN-1	vulnerability	OpenSSL SSLv2 Man-in-the-Middle Vulnerability	59268	ssl	networking	4	informational	alert	47 
18	WAN-1	LAN	vulnerability	Non-RFC Compliant SSL Traffic	56101	ssl	networking	4	informational	alert	45 
19	WAN-1	LAN	vulnerability	HTTP Non RFC-Compliant Response Found	32880	unknown-tcp	unknown	1	informational	alert	43 
20	LAN	WAN-4	vulnerability	Non-RFC Compliant SSL Traffic on Port 443	56112	ssl	networking	4	informational	alert	42 
21	LAN	WAN-2	vulnerability	OpenSSL SSLv2 Man-in-the-Middle Vulnerability	59268	ssl	networking	4	informational	alert	42 
22	WAN-4	LAN	vulnerability	HTTP Directory Traversal Request Attempt	30844	web-browsing	general-internet	4	medium	reset-both	39 
23	LAN	WAN-2	vulnerability	Suspicious or malformed HTTP Referer field	35554	bitdefender	business-systems	3	informational	reset-both	38 
24	VPN_GP	LAN	vulnerability	Microsoft Windows NTLMSSP Detection	92322	active-directory-base	business-systems	2	informational	alert	35 
25	LAN	WAN-1	vulnerability	Suspicious or malformed HTTP Referer field	35554	bitdefender	business-systems	3	informational	reset-both	34 

Descripción de las amenazas detectadas

- **SSH User Authentication Brute Force Attempt (40015)**
Este evento indica un ataque de fuerza bruta a través de múltiples intentos de inicio de sesión en un servidor SSH.
- **Non-RFC Compliant SSH Traffic on Port 22 (94634)**
Esta firma detecta tráfico SSH sospechoso y que no cumple con RFC en el puerto 22. Esto podría estar asociado con aplicaciones que envían tráfico que no es SSH utilizando el puerto 22 indica una posible actividad maliciosa.
- **OpenVAS Vulnerability Scanner Detection (55283)**
Esta firma detecta el tráfico de OpenVAS Vulnerability Scanner.
- **Non-RFC Compliant SSL Traffic on Port 443 (56112)**
Esta firma detecta tráfico SSL sospechoso y que no cumple con RFC en el puerto 443. Esto podría estar asociado con aplicaciones que envían tráfico que no es SSL usando el puerto 443 o indicar una posible actividad maliciosa.
- **ENV File Scanning Attempt (93397)**
Esta firma detecta un intento de escanear en busca de archivos ENV (archivos de entorno).
- **Microsoft Windows NTLMSSP Detection (92322)**
Solo detecta el NTLMSSP utilizado para autenticar.
- **ZGrab Application Layer Scanner Detection (57955)**
Esta firma indica que un atacante está intentando recopilar información sobre la red utilizando el escáner ZGrab.
- **TP-Link Archer Router Command Injection Vulnerability (93749)**
El enrutador Archer de TP-Link es propenso a una vulnerabilidad de inyección de comandos al analizar ciertas solicitudes HTTP diseñadas. La vulnerabilidad se debe a la falta de controles adecuados en las solicitudes HTTP, lo que genera una vulnerabilidad de inyección de comandos explotable. Un atacante podría aprovechar la vulnerabilidad enviando solicitudes HTTP diseñadas. Un ataque exitoso podría provocar la ejecución remota de código.
- **PNG File Chunk Length Abnormal (34243)**
Esta alerta indica que la longitud de un fragmento en un archivo PNG es demasiado grande, lo que puede provocar un posible desbordamiento o ejecución de código.
- **Non-RFC Compliant DNS Traffic on Port 53/5353 (56505)**
Esta firma detecta tráfico DNS sospechoso y no conforme con RFC en el puerto 53/5353. Esto podría estar asociado con aplicaciones que envían tráfico que no es DNS a través del puerto 53/5353 o indicar una posible actividad maliciosa.
- **Non-RFC Compliant HTTP Traffic on Port 80 (56391)**
Esta firma detecta tráfico HTTP sospechoso y no compatible con RFC en el puerto 80. Esto podría estar asociado con aplicaciones que envían tráfico que no es HTTP mediante el puerto 80 o indicar una posible actividad maliciosa.
- **OpenSSL SSLv2 Man-in-the-Middle Vulnerability (59268)**
OpenSSL es propenso a sufrir una vulnerabilidad de intermediario al analizar ciertas solicitudes SSL diseñadas. La vulnerabilidad se debe a la falta de controles adecuados en las solicitudes SSL, lo que genera una vulnerabilidad de intermediario explotable. Un atacante podría aprovechar la vulnerabilidad enviando solicitudes SSL diseñadas. Un ataque exitoso podría conducir a la ejecución remota de código con los privilegios del servidor



- **Non-RFC Compliant SSL Traffic (56101)**

Esta firma detecta tráfico SSL que no cumple con RFC.

- **HTTP Non RFC-Compliant Response Found (32880)**

Esta firma detecta tráfico DNS sospechoso y que no cumple con RFC en el puerto 53/5353. Esto podría estar asociado con aplicaciones que envían tráfico no DNS utilizando el puerto 53/5353 o indicar una posible actividad maliciosa.

- **HTTP Directory Traversal Request Attempt (30844)**

Se ha descubierto una vulnerabilidad de navegación de directorios al analizar solicitudes HTTP mal formadas. Esta vulnerabilidad se debe a la falta de comprobaciones adecuadas en las solicitudes de URL HTTP. Un ataque exitoso podría dar como resultado el acceso a información confidencial que podría ayudar a otros ataques.

- **Suspicious or malformed HTTP Referer field (35554)**

Esta firma detecta un campo REFERER mal formado o no estándar dentro de un encabezado de solicitud HTTP. Este evento puede ser benigno, pero también puede indicar que se utilizan herramientas maliciosas para generar este tráfico. El campo REFERER puede ser utilizado por el tráfico de comando y control saliente de los hosts infectados y también puede estar presente dentro de los encabezados de solicitud HTTP entrantes generados por los kits de herramientas DDOS.



4. Principales fuentes y destinos

En la siguiente imagen se muestra las regiones (países) donde se ha originado la mayor cantidad de tráfico (bytes), sesiones, amenazas, contenido (carga y descarga) y consultas URL en la red de INSN durante los últimos 31 días.

También se puede ver el origen del tráfico en la red del INSN, estos son identificados como INSN y 10.0.0.0-10.255.255.255

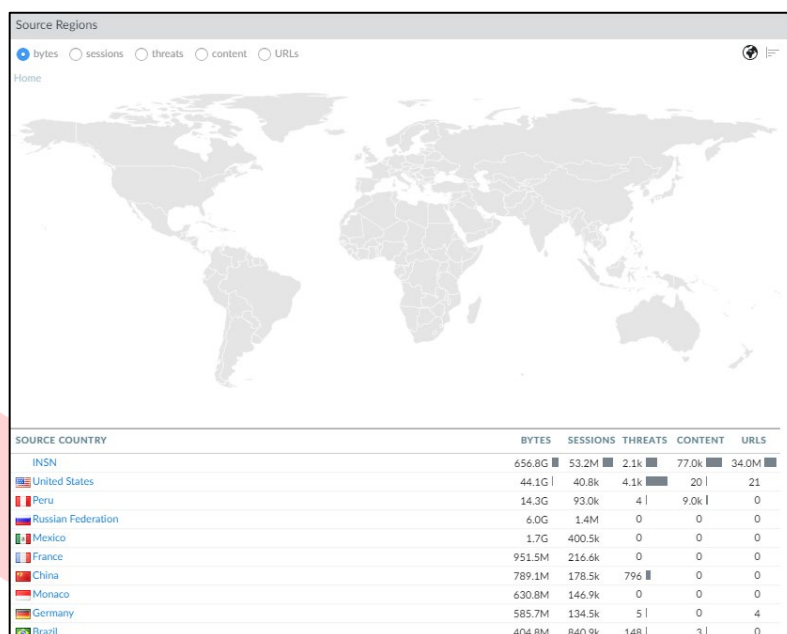


Ilustración 6: Regiones de origen con mayor tráfico

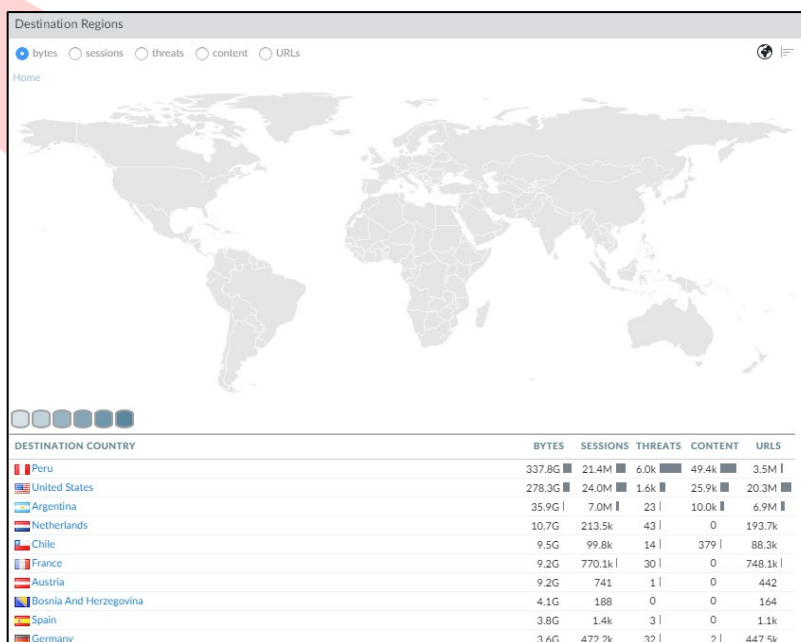


Ilustración 7: Regiones de destino con mayor tráfico



5. Otros reportes del sistema

5.1. Hosts que visitaron URLs Maliciosas

En la siguiente imagen se puede ver el top de los usuarios o hosts con la mayor cantidad de veces que intentaron ingresar a URL's maliciosas durante los últimos 31 días de servicio, estas se categorizan en dos tipos: malware y phishing. Como se aprecia, se encuentra un mayor intento de ingreso a las URLs de las cuales gran parte son categorizadas como malware y donde solo se ha identificado un mínimo registro de phishing

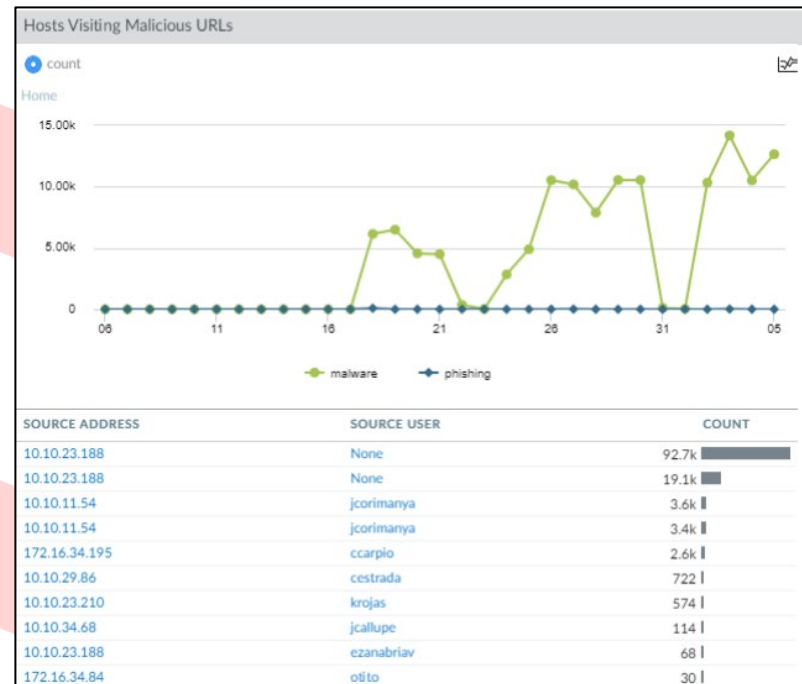


Ilustración 8: Host con más visitas a URLs maliciosas

5.2 Actividad de Amenaza

En la siguiente imagen se visualiza los tipos de amenazas detectadas durante los últimos 31 días de servicio y la cantidad de veces que fueron detectadas. Debajo de este se muestra las amenazas más relevantes, mostrando su ID, el grado de severidad, el tipo de amenaza, la categoría de la amenaza y la cantidad de veces que fueron detectadas.

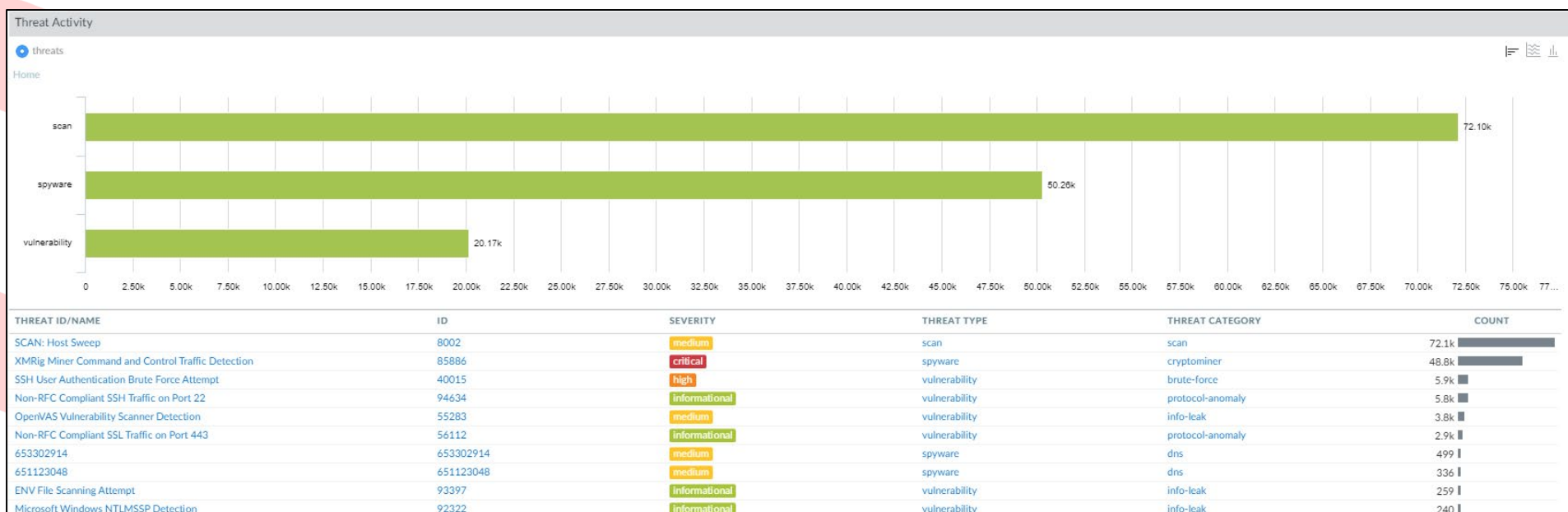


Ilustración 9: Actividad de Amenazas

5.3 Actividad de Usuario

En la siguiente imagen se visualiza la cantidad de bytes consumidos por los usuarios de la red durante los últimos 31 días de servicio. Debajo de este se visualiza a los usuarios que registraron una mayor actividad en la red, mostrando los bytes consumidos, sesiones registradas, amenazas detectadas, contenido registrado, URL's a la que intentaron acceder. o accedieron y Apps registradas.

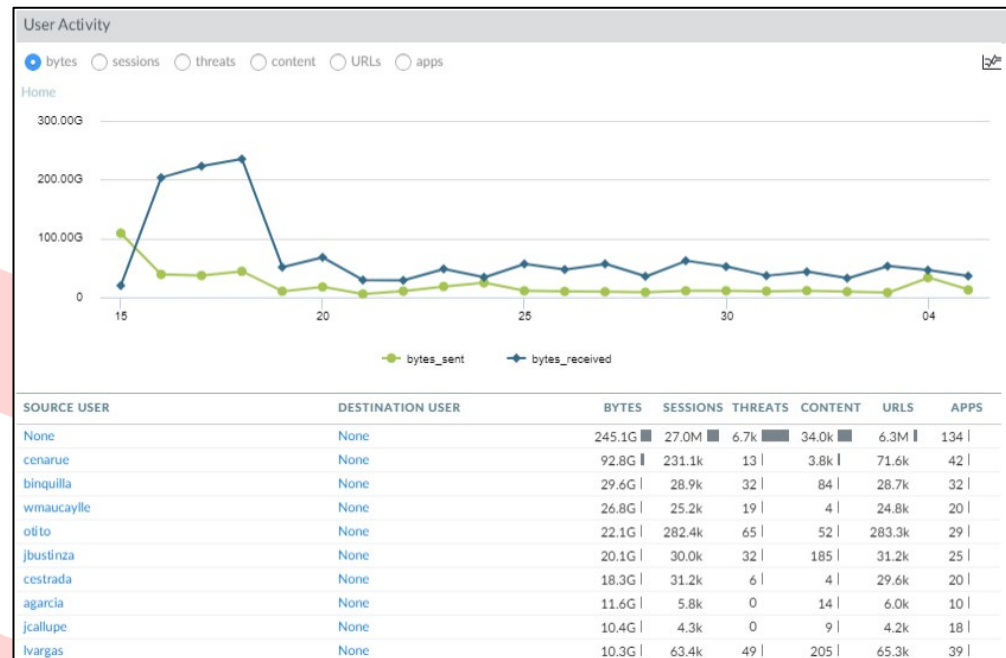


Ilustración 10: Actividad de Usuario

En algunos casos como se ve en la imagen anterior no se va a mostrar el usuario de destino ya que se trata de una comunicación de la LAN a WAN y en otros no se va a mostrar el usuario de origen ya que es una comunicación de la WAN a LAN.

5.3. Bloqueo por políticas de seguridad

En la siguiente imagen se visualiza la actividad de las políticas de seguridad al bloquear las amenazas registradas en la red durante los últimos 31 días de servicio, estas se muestran ordenadas por el tipo de amenaza y la cantidad de veces que fueron registradas. Debajo de este nos muestra las políticas de seguridad que registraron una mayor cantidad de bloqueos de amenazas.

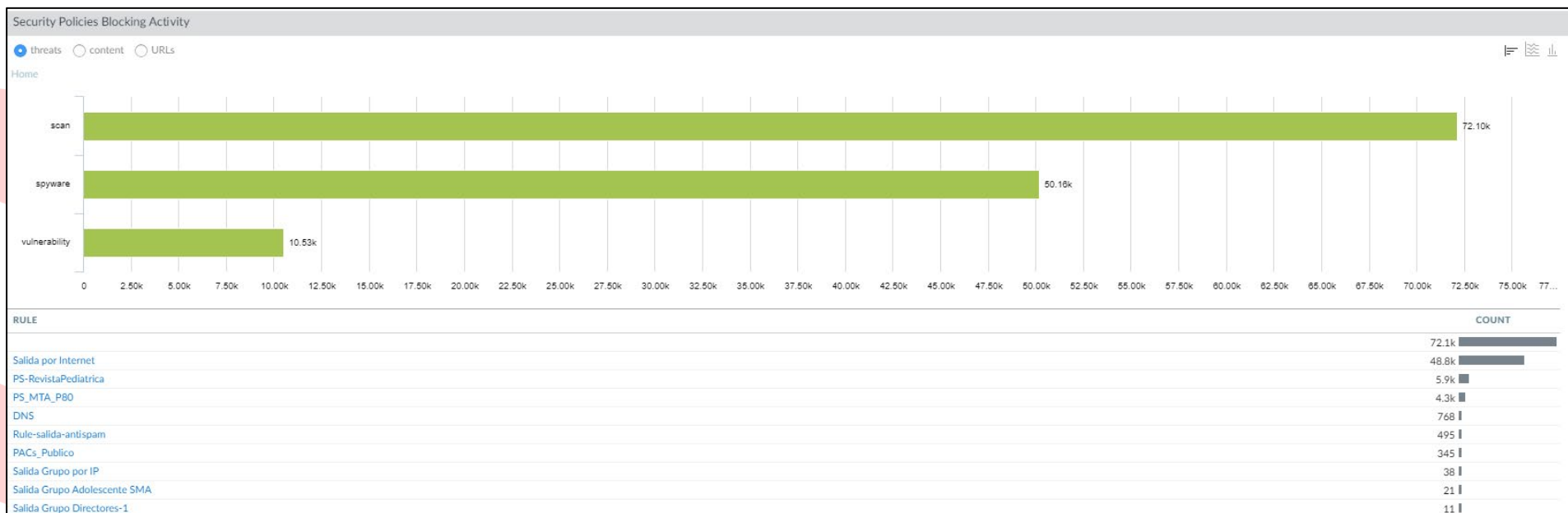


Ilustración 11: Bloqueo por Políticas de Seguridad

Estos 3 tipos de amenazas se refieren a lo siguiente:

- **Spyware:** spyware detectado a través de un perfil Anti-Spyware.
- **Vulnerability:** explotación de vulnerabilidad detectada a través de un perfil de protección de vulnerabilidad.
- **Virus:** virus detectado a través de un perfil Antivirus

Aplicaciones más usadas

En la siguiente imagen se visualiza el tráfico de las aplicaciones más usadas registradas en la red durante los últimos 31 días de servicio. Debajo de este se visualiza más detalles del top de aplicaciones más usadas, como el riesgo, la cantidad de tráfico (bytes), sesiones registradas, amenazas detectadas, contenido transferido, URLs registradas y usuarios que las usaron esas aplicaciones.

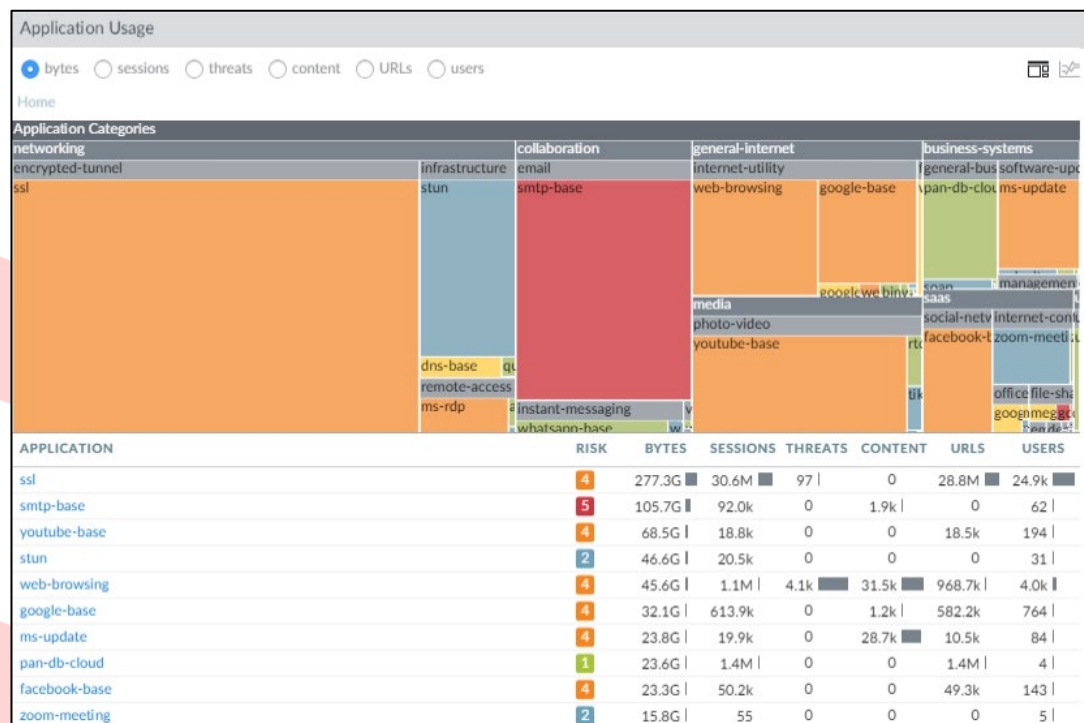


Ilustración 12: Aplicaciones más usadas

Entre estas aplicaciones se ve que la aplicación más usada es SSL, esto es porque la mayoría de tráfico es encriptado, por lo que mientras en el firewall no este configurado el desencriptamiento, este no va a poder identificar correctamente el tráfico que se lleva por ahí.

5.5. Actividad de conexiones exitosas al GlobalProtect

En la siguiente imagen se visualiza la actividad de la cantidad de conexiones exitosas por la VPN site to client con la herramienta Global Protect registradas en la red durante los últimos 31 días de servicio. Debajo de este aparte de la lista de usuarios y cantidad de conexiones, se visualizan la cantidad de asignación de IPs que obtuvieron y a cuantos portales y gateways se conectaron, este al ser único en cada caso siempre va a mostrar solo 2.



Ilustración 13: Usuarios con mayor cantidad de conexiones exitosas en Global Protect

6. Recomendaciones de Seguridad con el fin de Mejorar el Entorno de la Entidad

Para fortalecer la navegación interna y prevenir la infección de equipos por diversos métodos es necesario realizar una programación de las siguientes configuraciones:

1. Cuando se agregue una política de seguridad, colocarle los perfiles de seguridad según los privilegios de usuarios.
2. Especificar las aplicaciones y usar la acción de application-defaults en los servicios para poder usar los puertos predeterminados de las aplicaciones.
3. Especificar las Regiones permitidas (segmentos de IPs por país) con conexiones entrantes hacia los servicios publicados, esto con el fin mitigar las conexiones no deseadas a los servicios publicados.
4. Cuando se cree una nueva política colocar un nombre que haga referencia al tráfico permitido, esto con el fin de tener identificada cada política.
5. No cambiar el password del usuario INSN\PAN ya que esto afectaría el funcionamiento de la sincronización del Firewall y el Directorio Activo, de ser necesario el cambio de password favor de informar al correo soporte@soluzioniinternational.com para poder realizar los cambios respectivos en el User-ID Agent y Pa-850.
6. Realizar la inspección del tráfico saliente SSL, para poder tener una mayor visión y control sobre las aplicaciones que pasan sobre el tráfico encriptado.
7. Se recomienda habilitar la inspección del tráfico entrante para los servicios publicados, para esto se necesitaría los certificados en formato PEM, para poder importarlos en el firewall y poder realizar las respectivas configuraciones.
8. Revisión de la PCs con severidad de amenazas “altas” y “críticas”, ya que es un indicador de que estas PCs se encuentran infectadas.
9. El equipo actualmente se encuentra actualizado en la versión PAN-OS 10.2.7-h3, esta versión cuenta con nuevas funcionalidades que ayudan a proteger la red contra nuevos vectores de ataques, sería recomendable que habilitaran esas nuevas funcionalidades en el equipo.