**Documentación técnica - Implementación**

**NGFW & VM Series**

**SIES M**

**Versión 1.0**

Alcaldía de Medellín
Distrito de
Ciencia, Tecnología e Innovación

| | |
| --- | --- |
| **CUIDAD:** | Medellin |
| **FECHA:** | 15 Abril 2024 |
| **EMPRESA:** | Secretaría de Seguridad y Convivencia de Medellín |
| **DIRECCION:** | Calle 45 N° 55 65, Edificio Business Plaza |
| **TELEFONO:** | 315 8153441 |
| **PERSONA DE CONTACTO:** | Cristian Morales |
| **CARGO:** | Profesional Seguridad Informática |
| **RESPONSABLE BOYRA:** | Proyectos y servicios |

**LISTA DE CONTACTOS**

**Secretaria de Medellin**

| Nombre | Cargo | Teléfono | Email |
| --- | --- | --- | --- |
| Cristian Morales Garcés | Profesional Seguridad Informática | 315 8153441 | cristian.morales@medellin.gov.co |

**Boyra S.A.**

| Nombre | Cargo | Teléfono | Email |
| --- | --- | --- | --- |
| Andres Alvarez | Gerente Proyectos y servicios | +601 9156130 | helpdesk@boyra.com<br>andres.alvarez@boyra.com |

**TABLA DE CONTENIDO**

**1. OBJETIVO ..... 5**
**2. RESUMEN EJECUTIVO ..... 5**
**3. TOPOLOGÍA ..... 6**
**4. EQUIPAMIENTO NGFW ..... 6**
4.1. EQUIPAMIENTO ADQUIRIDO ..... 6
4.2. LICENCIAMIENTO ..... 7
4.3. VERSION PAN-OS ..... 8
**5. EQUIPAMIENTO PANORAMA ..... 8**
5.1. LICENCIAMIENTO ..... 9
5.2. VERSION PAN-OS ..... 9
**6. ADMINISTRACIÓN DE LA PLATAFORMA ..... 9**
**7. INTEGRACIÓN DE LA RED ..... 10**
7.1. VSYS ..... 10
7.2. VIRTUAL ROUTER ..... 11
7.3. ALTA DISPONIBILIDAD ..... 12
7.4. INTERFACES ..... 13
7.5. SECURITY ZONES ..... 17
**8. PANORAMA ..... 20**
8.1. TEMPLATE ..... 21
8.2. DEVICE GROUPS ..... 21
**9. DYNAMIC UPDATES ..... 22**
**10. SECURITY POLICIES ..... 23**
**11. NAT POLICIES ..... 28**
**12. PBF POLICIES ..... 28**
**13. DECRYPTION POLICIES ..... 28**
**14. SERVER PROFILES ..... 29**
14.1. LDAP ..... 29
**15. USER-ID ..... 30**
15.1. FUENTES DE USER-ID ..... 30
15.2. GROUP MAPPING PROFILES ..... 30
**16. RECOMENDACIONES ..... 31**
**17. CONSIDERACIONES ..... 32**

**NOTA DE PROPIEDAD**

La información y datos contenidos en todas las páginas de este documento de naturaleza comercial, técnica o financiera elaborado por *BOYRA* es información confidencial y privilegiada de *BOYRA*, y Sistema Integrado de Emergencia y Seguridad Metropolitana (SIES-M). La citada información se facilita a Sistema Integrado de Emergencia y Seguridad Metropolitana (SIES-M) bajo las más estrictas obligaciones de confidencialidad, en el bien entendido que éste no la usará sin permiso de BOYRA, para propósitos distintos al uso interno del presente proyecto.

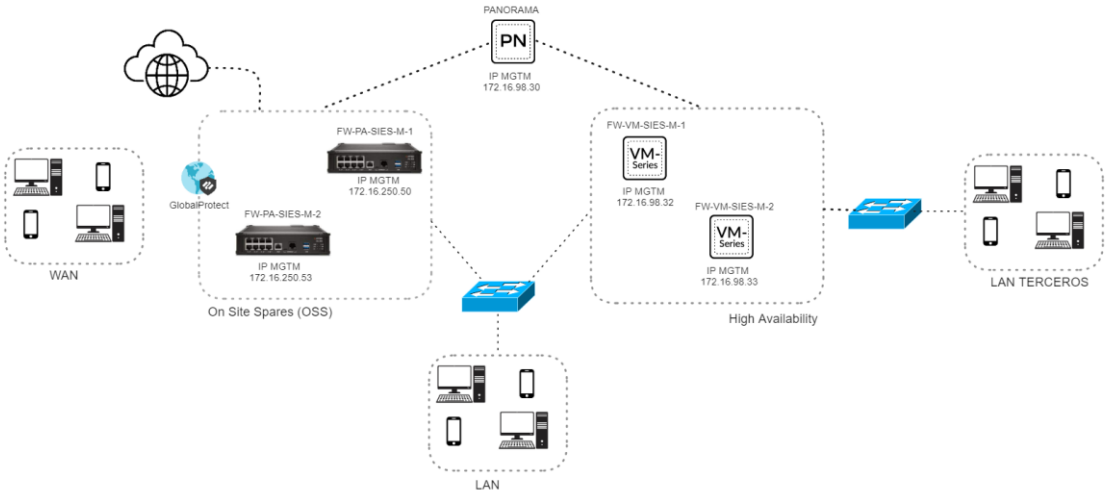
## 1. OBJETIVO

El presente documento tiene como finalidad proporcionar una visión general del requerimiento solicitado por el cliente SIES-Medellín, donde se llevó a cabo la configuración de dos Firewall PA 450, utilizando como base de configuración las VM-Series PA-VM (PA-460), adicional se detalla la infraestructura del Tenant de Cortex XDR Pro sies-m.xdr.us.paloaltonetworks.com de Palo Alto Networks, incluyendo su plataforma, componentes y configuración implementada.

## 2. RESUMEN EJECUTIVO

En este proyecto se tuvo como objetivo principal implementar soluciones de seguridad de Palo Alto Networks en el entorno de premisas y VMware ESXi del cliente SIES Medellín para garantizar una protección integral y eficaz de las cargas de trabajo y comunicaciones horizontales y laterales, así como facilitar la conectividad segura entre terceros y las redes de premisas a través de VPNs. El proyecto abarca la implementación de dos Palo Alto Networks PA-450 en modalidad standalone (el equipo secundario es de tipo On Site Spare) para proteger todo el tráfico de entrada y salida (vertical), un clusters de dos VM-Series desplegadas en VMware ESXi, para proteger todo el tráfico entre SIES M y terceros (horizontal), y un Panorama desplegado VMware ESXi.

## 3. TOPOLOGÍA




*Topología de la Solución*

## 4. EQUIPAMIENTO NGFW

Esta sección del documento provee detalle de la configuración y equipos desplegados en el ambiente de SIES MEDELLÍN.

### 4.1. EQUIPAMIENTO ADQUIRIDO

La tabla 1. Muestra el detalle de la solución adquirido con sus respectivas localidades, sistema operativo y serial:

| Device Name | Platform Model | Location | Serial Number |
|---|---|---|---|
| FW-PA-SIES-M-1 | PA-450 | Data Center SIES Medellín | 023201016643 |
| FW-PA-SIES-M-2 | PA-450 – PA Series (OSS) | Data Center SIES Medellín | 023201016639 |
| FW-VM-SIES-M-1 | PA-VM | VMware ESXi | 007951000349290 |
| FW-VM-SIES-M-2 | PA-VM | VMware ESXi | 007951000349298 |

*Tabla 1. Equipamiento Adquirido*

### 4.2. Licenciamiento

La tabla 2. muestra el detalle de las licencias, adquiridas en el palo alto:

| Nombre | Threat Prevention | PAN-DB URL Filtering | DNS Security | GlobalProtect Gateway | WildFire | Premium Support | Vsys |
|---|---|---|---|---|---|---|---|
| FW-PA-SIES-M-1 | X | X | X | X | X | X | 1 |
| FW-PA-SIES-M-2 | On Site Spare (OSS) | | | | | | 1 |
| FW-VM-SIES-M-1 | X | X | X | X | X | X | 1 |
| FW-VM-SIES-M-2 | X | X | X | X | X | X | 1 |

*Tabla 2. Licenciamiento*

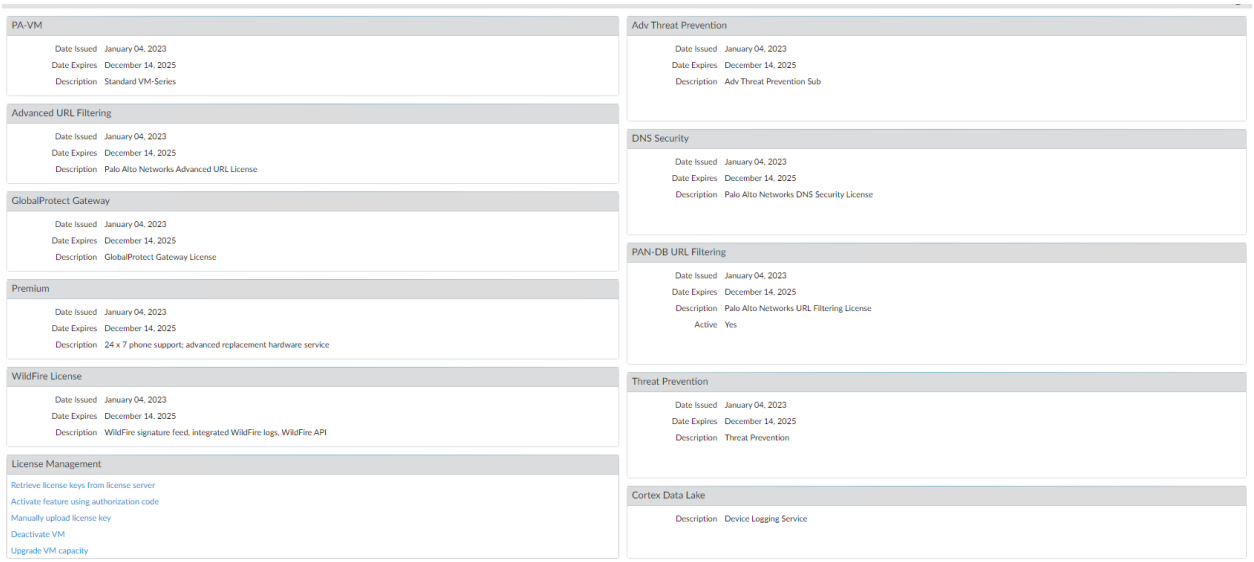



*Figura 2. Licenciamiento VM-Series*

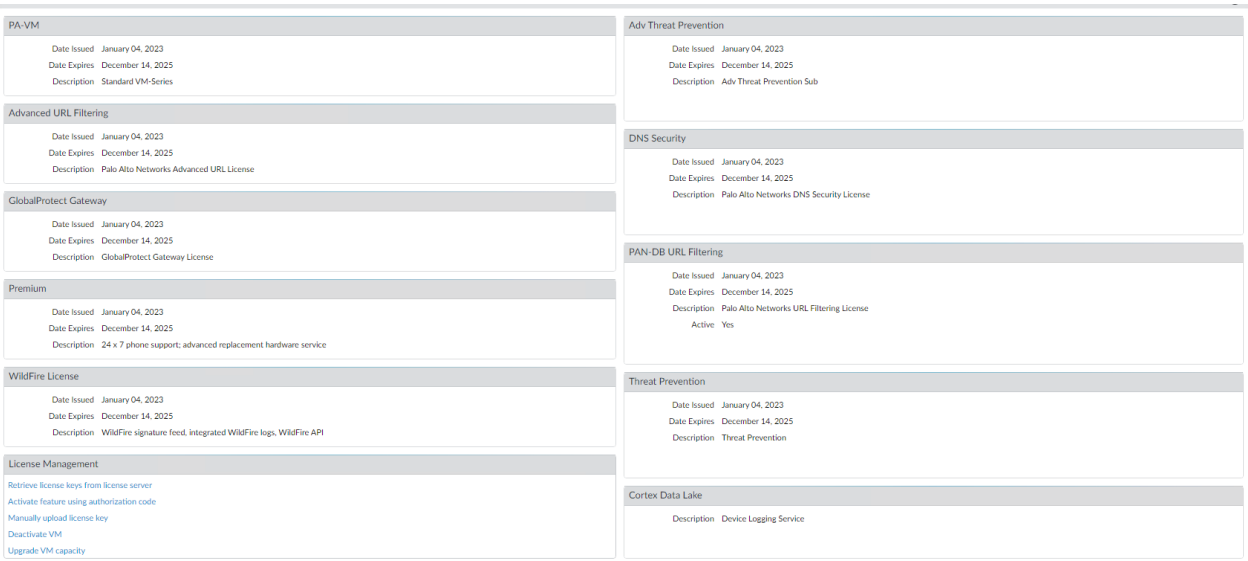



*Figura 3. Licenciamiento PA-450*

### 4.3. VERSION PAN-OS

La tabla 3. muestra el detalle de las versiones de PAN-OS, instaladas sobre cada dispositivo de seguridad, desplegada en la infraestructura del cliente SIES MEDELLÍN:

| Device Name | PanOS Deployed | Notes |
|---|---|---|
| FW-PA-SIES-M-1 | 10.1.8-h2 | PAN-OS 10.1 is end-of-life is 1 Dec 2024 |
| FW-PA-SIES-M-2 | 10.1.8-h2 | PAN-OS 10.1 is end-of-life is 1 Dec 2024 |
| FW-VM-SIES-M-1 | 10.1.8-h2 | PAN-OS 10.1 is end-of-life is 1 Dec 2024 |
| FW-VM-SIES-M-2 | 10.1.8-h2 | PAN-OS 10.1 is end-of-life is 1 Dec 2024 |

*Tabla 3. Versiones Instaladas de PAN-OS.*

## 5. EQUIPAMIENTO PANORAMA

Esta sección describe las características físicas y virtuales del sistema de gestión Panorama que fueron desplegadas en la infraestructura de SIES MEDELLÍN, la lista de dispositivos se muestra en la tabla 4.

| Device Name | Platform Model | Location to be Deployed | Serial Number(s) |
|---|---|---|---|
| Panorama | PA-VM | VMware ESXi | 000710011678 |

*Tabla 4. Panorama Server*

### 5.1. LICENCIAMIENTO

La tabla 5. muestra el detalle del licenciamiento y roles correspondiente de los equipos que conforman la infraestructura del Panorama.

| Device Name | License | Role |
|---|---|---|
| PANORAMA | VM Panorama license to manage up to 1K devices | Management-only |

*Tabla 5. Licenciamiento Panorama*

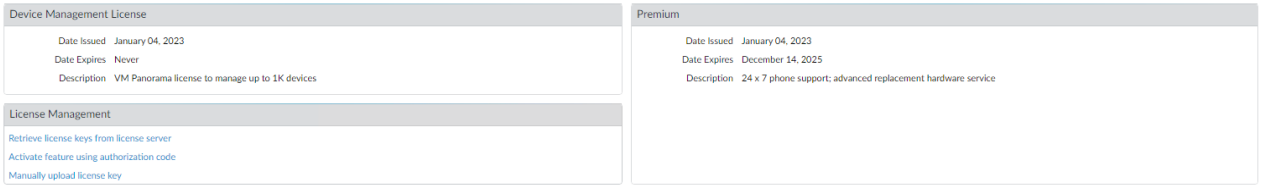



*Figura 4. Licenciamiento Panorama*

### 5.2. VERSION PAN-OS

La tabla 6. muestra el detalle de las versiones de PAN-OS, instaladas sobre cada dispositivo de seguridad, desplegada en la infraestructura del SIES MEDELLÍN:

| Device Name | PanOS Deployed | Notes |
|---|---|---|
| PANORAMA | 10.1.8-h2 | PAN-OS 10.1 is end-of-life is 1 Dec 2024 |

*Tabla 6. Versiones Instaladas de PAN-OS Panorama*

## 6. ADMINISTRACIÓN DE LA PLATAFORMA

La plataforma del cliente es administrada atreves de usuarios nombrados para cada administrador aprodado por el cliente, estos usuarios tienen permisos de administrador de la plataforma y se autentican con una base de datos externa de tipo LDAP.

La tabla 7. muestra el detalle de los usuarios de administración de la plataforma Palo Alto y Panorama.

| Name | Role | Auth Profile | Pass Profile | Role Profile |
|---|---|---|---|---|
| admin | Superuser | Auth | Pass | none |

*Tabla 6. Administrators.*

## 7. INTEGRACIÓN DE LA RED

Se muestra a continuación evidencia de la comunicación establecida entre el Panorama y los PA-450.

### 7.1. VSYS

Cada plataforma VM-Series de Palo Alto Networks, fue configurada en modo Stand alone con una sola virtual system.

| Device Name | VSYS ID | VSYS Name | interfaces | Virtual router |
|---|---|---|---|---|
| FW-PA-SIES-M-1 | vsys1 (default vsys) | Vsys1 | Ethernet 1/1<br>Ethernet 1/2<br>Ethernet 1/3<br>Ethernet 1/4<br>Ethernet1/5.733<br>Ethernet1/5.807<br>Ethernet1/5.808<br>Ethernet1/5.809<br>Ethernet1/5.810<br>Ethernet1/5.811<br>Ethernet1/5.731 | VR-SIES-M<br>VR TEL NUSE 123 |

| Device Name | VSYS ID | VSYS Name | interfaces | Virtual router |
|---|---|---|---|---|
| | | | Ethernet1/5.732 | |
| FW-PA-SIES-M-2 | vsys1 (default vsys) | Vsys1 | | |
| FW-VM-SIES-M-1 | vsys1 (default vsys) | Vsys1 | Ethernet 1/1.730<br>Ethernet 1/2.734<br>Ethernet 1/1.735<br>Ethernet 1/2.736<br>Ethernet 1/1.737<br>Ethernet 1/2.738 | VR SIES-M – JUPITER<br>VR SIES-M – UE<br>VR SIES-M - CAM |
| FW-VM-SIES-M-2 | vsys1 (default vsys) | Vsys1 | Ethernet 1/1.730<br>Ethernet 1/2.734<br>Ethernet 1/1.735<br>Ethernet 1/2.736<br>Ethernet 1/1.737<br>Ethernet 1/2.738 | VR SIES-M – JUPITER<br>VR SIES-M – UE<br>VR SIES-M - CAM |

Tabla 7. Detalle de los VSYS implementados

### 7.2. VIRTUAL ROUTER

Cada plataforma Palo Alto, fue configurada con un solo virtual system, cada interfaz está en capa 3 y es asignada a un virtual router. SIES MEDELLÍN esta utilizado enrutamiento estático, ningún protocolo de enrutamiento dinámico fue configurado.

La tabla 9. Muestra la configuración y los nombres de los virtual router.

| Device Name | Virtual System | Virtual Router | Routing Protocols |
|---|---|---|---|
| FW-PA-SIES-M-1 | VSYS1 | VR-SIES-M<br>VR TEL NUSE 123 | Static (17)<br>Static (0) |
| FW-PA-SIES-M-2 | | | |
| FW-VM-SIES-M-1 | VSYS1 | VR SIES-M – JUPITER<br>VR SIES-M – UE<br>VR SIES-M - CAM | Static (15)<br>Static (22)<br>Static (3) |
| FW-VM-SIES-M-2 | VSYS1 | VR SIES-M – JUPITER<br>VR SIES-M – UE<br>VR SIES-M - CAM | Static (15)<br>Static (22)<br>Static (3) |

*Tabla 8. Configuración General Virtual Routers.*

### 7.3. ALTA DISPONIBILIDAD

SIES Medellín ha desplego un par de VM-Series Palo Alto Networks en el ambiente de VM-Ware en alta disponibilidad de tipo activo - pasivo. Adicionalmente han adquirido un par de PA-450 que no se encuentran en alta disponibilidad, pero están en la metodología On Site Spare (OSS) para una recuperación rápida (manual) en caso de falla del hardware principal.

Se está utilizando la interfaz ethernet 1/8 para el HA1 y la interfaz ethernet 1/9 para el HA2 Todas las interfaces están directamente conectadas como se aprecia en la siguiente figura.

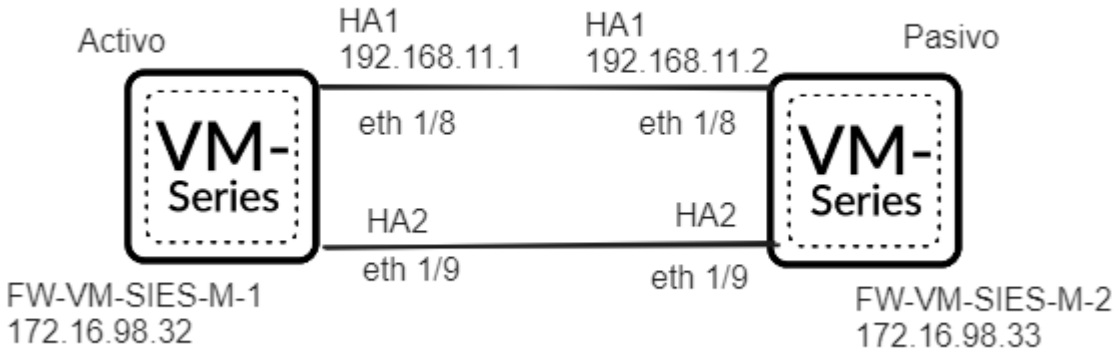



*Figura 5. Arquitectura de HA.*

La **Tabla 9.** muestra el detalle de la configuración del HA.

| Firewall Name | HA Mode | HA1 IP | HA2 IP |
|---|---|---|---|
| FW-VM-SIES-M-1 | Active/Passive | 192.168.11.1 | N/A |
| FW-VM-SIES-M-1 | Active/Passive | 192.168.11.2 | N/A |

*Tabla 9. Configuración HA.*

### 7.4. INTERFACES

Existen diferentes tipos de interfaces configurables sobre la plataforma. Esto será descrito en detalle en la próxima sección:

- Interfaces Operacionales
- Interfaces Management

#### 7.4.1. INTERFACES OPERACIONEALES

SIES-M está utilizando 5 interfaces y 8 sub-interfaces configuradas como tipo capa 3 en la configuración del FW-PA-SIES-M-1. Todas las interfaces están configuradas como auto para la negociación de la velocidad y duplex. Se le asignan su respectivo management profile. Todas las interfaces tienen configurado la IPs de forma estática.

**La Tabla 10** Muestra la configuración de interfaces del NGFW PA450 FW-PA-SIES-M-1

| Interface | Type | Mgt Profile | IP | Virtual Router | VLAN | Vsys | Zone |
|---|---|---|---|---|---|---|---|
| Ethernet1/1 | L3 | MGMT-WAN | 179.1.78.202/29 | VR-SIES-M | N/A | Vsys1 | WAN |
| Ethernet1/2 | L3 | MGMT-ICMP | 172.17.0.6/30 | VR-SIES-M | N/A | Vsys1 | LAN |
| Ethernet1/3 | L3 | MGMT-ICMP | 192.168.100.254 | VR-SIES-M | N/A | Vsys1 | WLAN |
| Ethernet1/4 | L3 | MGMT-WAN | 190.90.10.210/30 | VR-SIES-M | N/A | Vsys1 | WAN2 |
| Ethernet1/5 | L3 | MGMT-ICMP | none | none | N/A | Vsys1 | TRUNK |
| Ethernet1/5.731 | L3 | MGMT-ICMP | 192.168.202.30 | VR TEL NUSE 123 | 731 | Vsys1 | LAN TEL |
| Ethernet1/5.732 | L3 | MGMT-WAN | 190.71.244.10/29 | VR TEL NUSE 123 | 732 | Vsys1 | WAN3 |
| Ethernet1/5.733 | L3 | MGMT-ICMP | 192.168.254.6/29 | VR-SIES-M | 733 | Vsys1 | LAN SEC |
| Ethernet1/5.807 | L3 | MGMT-ICMP | 10.123.0.6/29 | VR-SIES-M | 807 | Vsys1 | DMZ |
| Ethernet1/5.808 | L3 | MGMT-ICMP | 172.18.0.38/30 | VR-SIES-M | 808 | Vsys1 | LAN SICAM |
| Ethernet1/5.809 | L3 | MGMT-WAN | 192.168.4.2/30 | VR-SIES-M | 809 | Vsys1 | WAN SIMIM |
| Ethernet1/5.810 | L3 | MGMT-ICMP | 10.200.10.6/29 | VR-SIES-M | 810 | Vsys1 | LAN SM |
| Ethernet1/5.811 | L3 | MGMT-ICMP | 192.168.254.14 | VR-SIES-M | 811 | Vsys1 | LAN MGT SW |

*Tabla 10. Configuración Interfaces Operacionales*

SIES-M está utilizando 2 interfaces y 6 sub-interfaces configuradas como tipo capa 3 en la configuración de las VM-Series FW-VM-SIES-M-1 y FW-VM-SIES-M-2. Todas las interfaces están configuradas como auto para la negociación de la velocidad y duplex. Se le asignan su respectivo management profile. Todas las interfaces tienen configurado la IPs de forma estática.

La Tabla 11 Muestra la configuración de interfaces de las VM-Series FW-VM-SIES-M-1 y FW-VM-SIES-M-2.

| Interface | Type | Mgt Profile | IP | Virtual Router | VLAN | Vsys | Zone |
|---|---|---|---|---|---|---|---|
| Ethernet1/1 | L3 | | none | none | N/A | Vsys1 | noee |
| Ethernet1/1.730 | L3 | MGMT-ICMP | 172.17.0.10/30 | VR-SIES-M - JUPITER | N/A | Vsys1 | SIES-M |
| Ethernet1/1.735 | L3 | MGMT-ICMP | 172.17.0.14/30 | VR-SIES-M - UE | N/A | Vsys1 | SIES-M UE |
| Ethernet1/1.737 | L3 | MGMT-ICMP | 172.17.0.17/30 | VR SIES-M - CAM | N/A | Vsys1 | SIES-M CAM |
| Ethernet1/2 | L3 | | none | none | N/A | Vsys1 | TRUNK |
| Ethernet1/2.734 | L3 | MGMT-WAN | 192.168.202.62 | VR-SIES-M - JUPITER | 731 | Vsys1 | VM JUPITER |
| Ethernet1/2.736 | L3 | MGMT-WAN | 192.168.201.30 | VR-SIES-M - UE | 732 | Vsys1 | SOP UE |
| Ethernet1/2.738 | L3 | MGMT-WAN | 10.10.20.1/30 | VR SIES-M - CAM | 733 | Vsys1 | SVR CAM |

*Tabla 11. Configuración Interfaces Operacionales*

### 7.4.2. INTERFACES DE GESTIÓN

El SIES Medellín configuró una (1) interfaz de administración para los dispositivos, la administración de los equipos se está realizando exclusivamente por la interfaz de MGMT de cada una de las VMs y el Panorama implementados dentro de la cuenta Networking en la VPC Security de AWS.

La interfaz de gestión se encuentra implementada en zona de seguridad protegida por el NGFW Palo Alto Networks.

La Tabla 12 Muestra las interfaces de Management configuradas para cada dispositivo.

| Device Name | MGT Port | Settings |
|---|---|---|
| *FW-PA-SIES-M-1* | IP Address | *172.16.250.50* |
| | Mask | *255.255.255.0* |
| | Gateway | *172.16.250.254* |
| | IPv6 address | *N/A* |
| | Speed | *Auto-negociate* |
| | MTU | *1500* |
| | Services | *HTTPS*<br>*SSH*<br>*Ping*<br>*SNMP*<br>*User-ID* |
| | Permitted IP's | *172.16.100.120*<br>*172.16.98.30*<br>*172.16.250.54*<br>*172.16.20.100*<br>*192.168.254.17*<br>*172.16.100.61*<br>*172.16.250.53*<br>*10.90.0.2*<br>*10.90.0.3*<br>*172.16.100.98* |
| | | |
| *FW-PA-SIES-M-2* | IP Address | *172.16.250.53* |
| | Mask | *255.255.255.0* |
| | Gateway | *172.16.250.254* |
| | IPv6 address | *N/A* |
| | Speed | *Auto-negociate* |
| | MTU | *1500* |
| | Services | *HTTPS*<br>*SSH*<br>*Ping*<br>*SNMP* |

| Device Name | MGT Port | Settings |
|---|---|---|
| | | *User-ID* |
| | Permitted IP's | *172.16.100.120*<br>*172.16.98.30*<br>*172.16.250.54*<br>*172.16.20.100*<br>*192.168.254.17*<br>*172.16.100.61*<br>*172.16.250.53*<br>*172.16.100.98* |
| | | |
| *FW-VM-SIES-M-1* | IP Address | *172.16.98.32* |
| | Mask | *255.255.254.0* |
| | Gateway | *172.16.98.10* |
| | IPv6 address | *N/A* |
| | Speed | *Auto-negociate* |
| | MTU | *1500* |
| | Services | *HTTPS*<br>*SSH*<br>*Ping*<br>*SNMP* |
| | Permitted IP's | *172.16.100.61*<br>*172.16.100.120*<br>*172.16.98.30*<br>*172.16.250.52*<br>*172.16.20.100*<br>*172.16.100.243*<br>*172.16.100.237*<br>*172.16.100.233*<br>*192.168.254.17*<br>*172.16.98.33* |
| | | |
| *FW-VM-SIES-M-2* | IP Address | *172.16.98.33* |
| | Mask | *255.255.254.0* |
| | Gateway | *172.16.98.10* |
| | IPv6 address | *N/A* |
| | Speed | *Auto-negociate* |
| | MTU | *1500* |
| | Services | *HTTPS* |

| Device Name | MGT Port | Settings |
|---|---|---|
| | | *SSH*<br>*Ping*<br>*SNMP* |
| | Permitted IP's | *172.16.100.61*<br>*172.16.100.120*<br>*172.16.98.30*<br>*172.16.250.52*<br>*172.16.20.100*<br>*172.16.100.243*<br>*172.16.100.237*<br>*172.16.100.233*<br>*192.168.254.17*<br>*172.16.98.33* |

*Tabla 12. Configuración Management Interface*

### 7.5. SECURITY ZONES

SIES-M tiene 18 zonas de seguridad configuradas tipo capa 3, en el NGFW PA450 FW-PA-SIES-M-1.

La Tabla 13. muestra las zonas de seguridad configuradas.

| Zone Name | Tipo | Zone Protection | User-ID | VSYS |
|---|---|---|---|---|
| DMZ | L3 | none | No | Vsys1 |
| LAN | L3 | none | Enable | Vsys1 |
| LAN MGT SW | L3 | none | Enable | Vsys1 |
| LAN SEC | L3 | none | No | Vsys1 |
| LAN SICAM | L3 | none | Enable | Vsys1 |
| LA SM | L3 | none | Enable | Vsys1 |
| LAN TEL | L3 | none | No | Vsys1 |
| PROXY SM | L3 | none | Enable | Vsys1 |
| TRUNK | L3 | none | No | Vsys1 |
| VPN GP | L3 | none | Enable | Vsys1 |
| VPN PONAL | L3 | none | No | Vsys1 |
| VPN SM | L3 | none | Enable | Vsys1 |
| WAN | L3 | Zone Protection Profile | No | Vsys1 |
| WAN AZURE | L3 | none | No | Vsys1 |
| WAN SIMIM | L3 | Zone Protection Profile | No | Vsys1 |
| WAN2 | L3 | ZP NO IP SPOOF | No | Vsys1 |
| WAN3 | L3 | ZP NO IP SPOOF | No | Vsys1 |
| WLAN | L3 | none | No | Vsys1 |

*Tabla 13. Configuración Zonas*

SIES-M tiene 7 zonas de seguridad configuradas tipo capa 3, en las VM-Series FW-VM-SIES-M-1 y FW-VM-SIES-M-2

La Tabla 14. muestra las zonas de seguridad configuradas.

| Zone Name | Tipo | Zone Protection | User-ID | VSYS |
|---|---|---|---|---|
| SIES-M | L3 | none | No | Vsys1 |
| SIES-M CAM | L3 | none | No | Vsys1 |
| SIES-M UE | L3 | none | No | Vsys1 |
| SO UE | L3 | none | No | Vsys1 |
| SVR CAM | L3 | none | No | Vsys1 |
| TRUNK | L3 | none | No | Vsys1 |
| VM JUPITER | L3 | Zone Protection Profile | No | Vsys1 |

*Tabla 14. Configuración Zonas*

SIES-M configuro un zone protection profile "*Zone Protection Profile*", para bloquear el escaneo de puertos TCP/UDP, host sweeps y protección contra Inundación de recursos.
Se muestra a continuación el detealle de la configuración del zone protection profile.

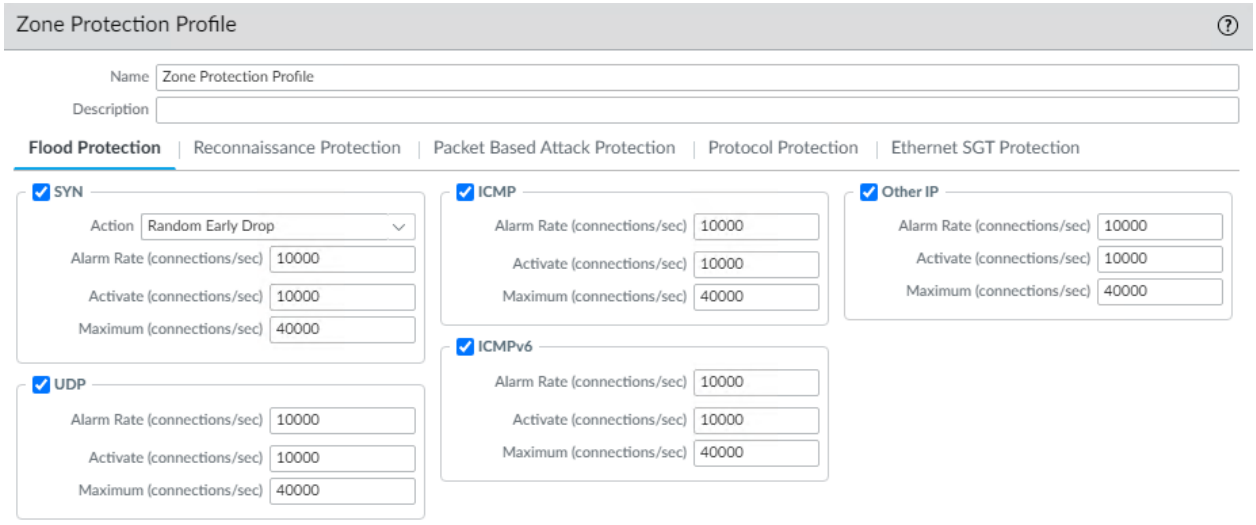



*Figura 6. Zone Protection - Flood Protection.*

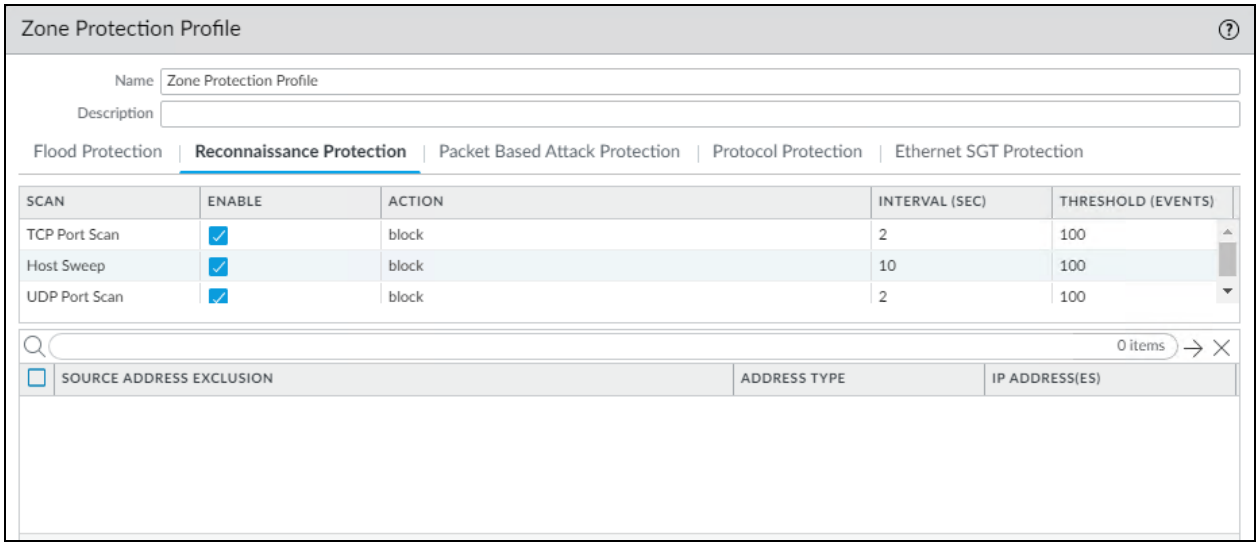



*Figura 7. Zone Protection – Reconnaissance Protection.*

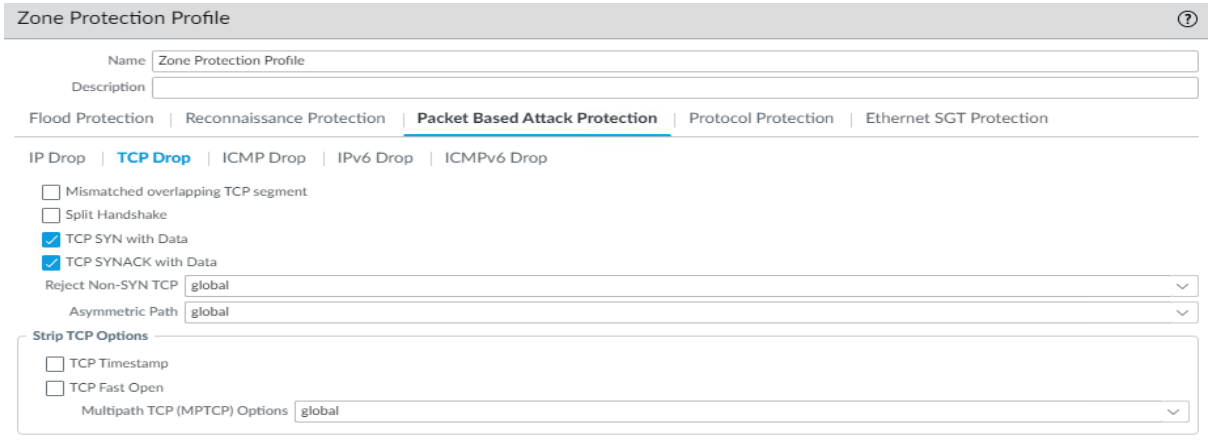



*Figura 8. Zone Protection – Packet Based Attack Protection.*

## 8. PANORAMA

Para este Proyecto de migración el cliente SIES MEDELLÍN utilizo su Panorama virtualizado en VMWare, el mismo ya se encuentra funcionando en management-only. Actualmente maneja un total de 4 dispositivos en toda la organización, todos las VMs y NGFWs son manejados con device group y templates sin configuración local.

| Device Name | MGT Port Settings | Configuracion |
|---|---|---|
| *Panorama* | IP Addres | *172.16.98.30* |
| | Mask | *255.255.254.0* |
| | Gateway | *172.16.98.10* |
| | Speed | *Auto-negotiate* |
| | MTU | *1500* |
| | Services | *HTTPS*<br>*SSH*<br>*Ping*<br>*SNMP* |
| | Permitted IP | *172.16.98.10*<br>*172.16.100.120*<br>*172.16.250.51*<br>*172.16.250.52*<br>*10.90.0.2*<br>*10.90.0.3*<br>*172.16.20.100*<br>*172.16.100.243*<br>*172.16.100.230*<br>*172.16.100.217*<br>*172.16.100.233*<br>*192.168.254.17*<br>*172.16.250.50*<br>*172.16.250.53*<br>*172.16.98.32*<br>*172.16.98.33* |
| | H/A Priority | *N/A* |

*Tabla 15. Configuración Interfaz Panorama*

### 8.1. TEMPLATE

SIES Medellín está utilizando dos Template Stacks para administrar las VM Series y los NGFW PA450, (Template_SIES-M_VMs_H y Template_SIES-M). Adicionalmente se está utilizando los siguientes Templates (Template_SIES-M y Template_SIES-M_VMs_H).

| Template Name | Stack | Stack Members |
|---|---|---|
| Template_SIES-M | Template_Stack_SIES-M | Template_SIES-M |
| | | |
| Template_SIES-M_VMs_H | Template_Stack_SIES-M_VMs_H | Template_SIES-M_VMs_H |

*Tabla 16. Esquema Template*

### 8.2. DEVICE GROUPS

SIES Medellín utiliza un par de Device Group (DG_SIES-M y DG_SIES-M_H), para las configuraciones específicas de cada VM y NGFW- se utiliza el Device Group "Shared" para las configuraciones globales. La jerarquía de los device group se muestra en la siguiente tabla

| 1st Tier | 2nd Tier | Master Device |
|---|---|---|
| Shared | | |
| | DG_SIES-M | FW-PA-SIES-M-1 |
| | | FW-PA-SIES-M-2 (OSS) |
| | | |
| | DG_SIES-M_H | FW-VM-SIES-M-1 |
| | | FW-VM-SIES-M-2 |

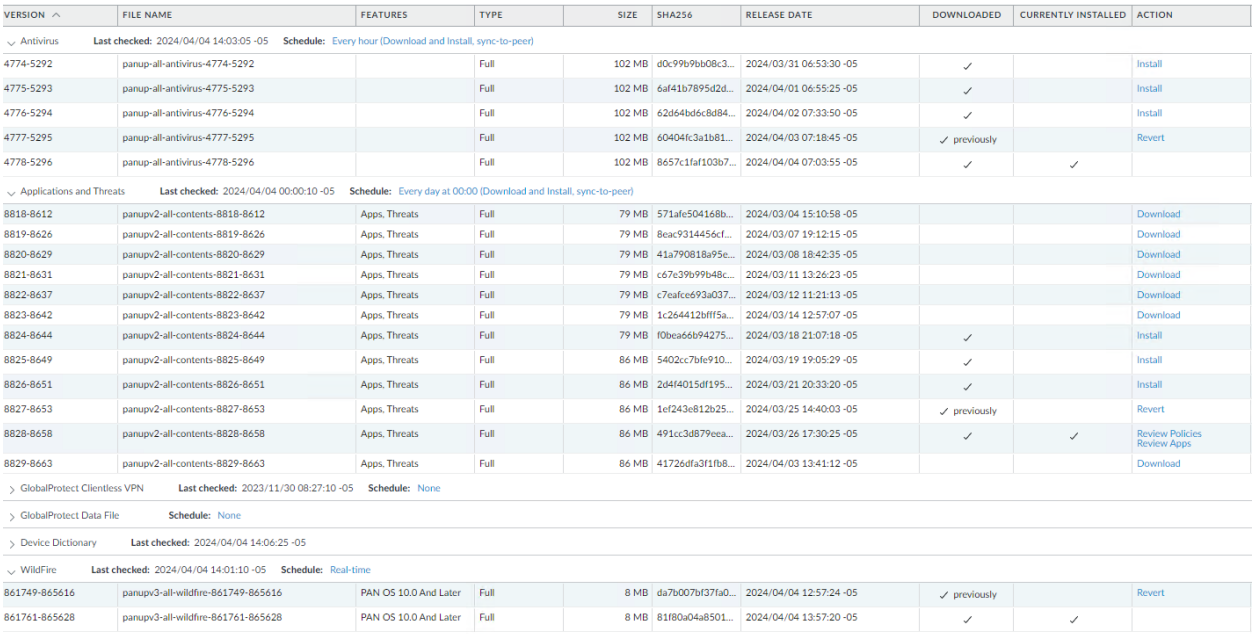
*Tabla 17. Esquema Device Group*

## 9. DYNAMIC UPDATES

La programación de la descarga e instalación de las actualizaciones dinámicas para el FW-PA-SIES-M-1son detallados en la siguiente tabla:

| Tipo | Recurrencia | Tiempo | Acción | Umbral de Horas |
|---|---|---|---|---|
| Antivirus | Every hour | n/a | Download and Install | None |
| App and Threat | Every day | 00:00 | Download and Install | None |
| WildFire | Real time | n/a | Download and Install | None |

*Tabla 18. Actualizaciones Dinámicas.*



| VERSION | FILE NAME | FEATURES | TYPE | SIZE | SHA256 | RELEASE DATE | DOWNLOADED | CURRENTLY INSTALLED | ACTION |
|---|---|---|---|---|---|---|---|---|---|
| Antivirus Last checked: 2024/04/04 14:03:05 -05 Schedule: Every hour (Download and Install, sync-to-peer) | | | | | | | | | |
| 4774-5292 | panup-all-antivirus-4774-5292 | | Full | 102 MB | d0c99b9bb08c3... | 2024/03/31 06:53:30 -05 | ✓ | | Install |
| 4775-5293 | panup-all-antivirus-4775-5293 | | Full | 102 MB | 6af41b7895d2d... | 2024/04/01 06:55:25 -05 | ✓ | | Install |
| 4776-5294 | panup-all-antivirus-4776-5294 | | Full | 102 MB | 62d64bd6c8d84... | 2024/04/02 07:33:50 -05 | ✓ | | Install |
| 4777-5295 | panup-all-antivirus-4777-5295 | | Full | 102 MB | 60404fc3a1b81... | 2024/04/03 07:18:45 -05 | ✓ previously | | Revert |
| 4778-5296 | panup-all-antivirus-4778-5296 | | Full | 102 MB | 8657c1faf103b7... | 2024/04/04 07:03:55 -05 | ✓ | ✓ | |
| Applications and Threats Last checked: 2024/04/04 00:00:10 -05 Schedule: Every day at 00:00 (Download and Install, sync-to-peer) | | | | | | | | | |
| 8818-8612 | panupv2-all-contents-8818-8612 | Apps, Threats | Full | 79 MB | 571afe504168b... | 2024/03/04 15:10:58 -05 | | | Download |
| 8819-8626 | panupv2-all-contents-8819-8626 | Apps, Threats | Full | 79 MB | 8eac9314456cf... | 2024/03/07 19:12:15 -05 | | | Download |
| 8820-8629 | panupv2-all-contents-8820-8629 | Apps, Threats | Full | 79 MB | 41a790818a95e... | 2024/03/08 18:42:35 -05 | | | Download |
| 8821-8631 | panupv2-all-contents-8821-8631 | Apps, Threats | Full | 79 MB | c67e39b99b48c... | 2024/03/11 13:26:23 -05 | | | Download |
| 8822-8637 | panupv2-all-contents-8822-8637 | Apps, Threats | Full | 79 MB | c7eafce693a037... | 2024/03/12 11:21:13 -05 | | | Download |
| 8823-8642 | panupv2-all-contents-8823-8642 | Apps, Threats | Full | 79 MB | 1c264412bff5a... | 2024/03/14 12:57:07 -05 | | | Download |
| 8824-8644 | panupv2-all-contents-8824-8644 | Apps, Threats | Full | 79 MB | f0bea66b94275... | 2024/03/18 21:07:18 -05 | ✓ | | Install |
| 8825-8649 | panupv2-all-contents-8825-8649 | Apps, Threats | Full | 86 MB | 5402cc7bfe910... | 2024/03/19 19:05:29 -05 | ✓ | | Install |
| 8826-8651 | panupv2-all-contents-8826-8651 | Apps, Threats | Full | 86 MB | 2d4f4015df195... | 2024/03/21 20:33:20 -05 | ✓ | | Install |
| 8827-8653 | panupv2-all-contents-8827-8653 | Apps, Threats | Full | 86 MB | 1ef243e812b25... | 2024/03/25 14:40:03 -05 | ✓ previously | | Revert |
| 8828-8658 | panupv2-all-contents-8828-8658 | Apps, Threats | Full | 86 MB | 491cc3d879eea... | 2024/03/26 17:30:25 -05 | ✓ | ✓ | Review Policies Review Apps |
| 8829-8663 | panupv2-all-contents-8829-8663 | Apps, Threats | Full | 86 MB | 41726dfa3f1fb8... | 2024/04/03 13:41:12 -05 | | | Download |
| GlobalProtect Clientless VPN Last checked: 2023/11/30 08:27:10 -05 Schedule: None | | | | | | | | | |
| GlobalProtect Data File Schedule: None | | | | | | | | | |
| Device Dictionary Last checked: 2024/04/04 14:06:25 -05 | | | | | | | | | |
| WildFire Last checked: 2024/04/04 14:01:10 -05 Schedule: Real-time | | | | | | | | | |
| 861749-865616 | panupv3-all-wildfire-861749-865616 | PAN OS 10.0 And Later | Full | 8 MB | da7b007bf37fa0... | 2024/04/04 12:57:24 -05 | ✓ previously | | Revert |
| 861761-865628 | panupv3-all-wildfire-861761-865628 | PAN OS 10.0 And Later | Full | 8 MB | 81f80a04a8501... | 2024/04/04 13:57:20 -05 | ✓ | ✓ | |

Figura 9. Dynamic Updates.

La programación de la descarga e instalación de las Actualizaciones dinámicas para las VMs FW-VM-SIES-M-1 y FW-VM-SIES-M-2 son detallados en la siguiente tabla:

| Tipo | Recurrencia | Tiempo | Acción | Umbral de Horas |
|---|---|---|---|---|
| Antivirus | Every hour | n/a | Download and Install | None |
| App and Threat | Every day | 01:00 | Download and Install | None |
| WildFire | Real time | n/a | Download and Install | None |

*Tabla 16. Actualizaciones Dinámicas.*

| VERSION | FILE NAME | FEATURES | TYPE | SIZE | SHA256 | RELEASE DATE | DOWNLOADED | CURRENTLY INSTALLED | ACTION |
|---|---|---|---|---|---|---|---|---|---|
| Antivirus **Last checked:** 2024/04/04 14:03:03 -05 **Schedule:** Every hour (Download and Install) | | | | | | | | | |
| 4774-5292 | panup-all-antivirus-4774-5292 | | Full | 102 MB | d0c99b9bb08c3b... | 2024/03/31 06:53:30 -05 | | | Download |
| 4775-5293 | panup-all-antivirus-4775-5293 | | Full | 102 MB | 6af41b7895d2d5... | 2024/04/01 06:55:25 -05 | | | Download |
| 4776-5294 | panup-all-antivirus-4776-5294 | | Full | 102 MB | 62d64bd6c8d847... | 2024/04/02 07:33:50 -05 | | | Download |
| 4777-5295 | panup-all-antivirus-4777-5295 | | Full | 102 MB | 60404fc3a1b814... | 2024/04/03 07:18:45 -05 | ✓ previously | | Revert |
| 4778-5296 | panup-all-antivirus-4778-5296 | | Full | 102 MB | 8657c1faf103b7... | 2024/04/04 07:03:55 -05 | ✓ | ✓ | |
| Applications and Threats **Last checked:** 2024/04/04 01:00:11 -05 **Schedule:** Every day at 01:00 (Download and Install) | | | | | | | | | |
| 8787-8442 | panupv2-all-contents-8787-8442 | Apps, Threats | Full | 76 MB | 9f8a9c56934ddb... | 2023/12/06 14:21:08 -05 | ✓ previously | | Revert |
| 8818-8612 | panupv2-all-contents-8818-8612 | Apps, Threats | Full | 79 MB | 571afe504168be... | 2024/03/04 15:10:58 -05 | | | Download |
| 8819-8626 | panupv2-all-contents-8819-8626 | Apps, Threats | Full | 79 MB | 8eac9314456cf4... | 2024/03/07 19:12:15 -05 | | | Download |
| 8820-8629 | panupv2-all-contents-8820-8629 | Apps, Threats | Full | 79 MB | 41a790818a95ed... | 2024/03/08 18:42:35 -05 | | | Download |
| 8821-8631 | panupv2-all-contents-8821-8631 | Apps, Threats | Full | 79 MB | c67e39b99b48c6... | 2024/03/11 13:26:23 -05 | | | Download |
| 8822-8637 | panupv2-all-contents-8822-8637 | Apps, Threats | Full | 79 MB | c7eafce693a0370... | 2024/03/12 11:21:13 -05 | | | Download |
| 8823-8642 | panupv2-all-contents-8823-8642 | Apps, Threats | Full | 79 MB | 1c264412bfff5a1... | 2024/03/14 12:57:07 -05 | | | Download |
| 8824-8644 | panupv2-all-contents-8824-8644 | Apps, Threats | Full | 79 MB | f0bea66b942752... | 2024/03/18 21:07:18 -05 | | | Download |
| 8825-8649 | panupv2-all-contents-8825-8649 | Apps, Threats | Full | 86 MB | 5402cc7bfe9108... | 2024/03/19 19:05:29 -05 | | | Download |
| 8826-8651 | panupv2-all-contents-8826-8651 | Apps, Threats | Full | 86 MB | 2d4f4015df1950... | 2024/03/21 20:33:20 -05 | | | Download |
| 8827-8653 | panupv2-all-contents-8827-8653 | Apps, Threats | Full | 86 MB | 1ef243e812b25e... | 2024/03/25 14:40:03 -05 | | | Download |
| 8828-8658 | panupv2-all-contents-8828-8658 | Apps, Threats | Full | 86 MB | 491cc3d879eeac... | 2024/03/26 17:30:25 -05 | ✓ | ✓ | Review Policies<br>Review Apps |
| 8829-8663 | panupv2-all-contents-8829-8663 | Apps, Threats | Full | 86 MB | 41726dfa3f1fb8c... | 2024/04/03 13:41:12 -05 | | | Download |
| GlobalProtect Clientless VPN **Last checked:** 2024/04/03 09:38:51 -05 **Schedule:** None | | | | | | | | | |
| GlobalProtect Data File **Schedule:** None | | | | | | | | | |
| Device Dictionary **Last checked:** 2024/04/04 14:06:26 -05 | | | | | | | | | |
| WildFire **Last checked:** 2024/04/04 14:00:45 -05 **Schedule:** Real-time | | | | | | | | | |
| 861749-865616 | panupv3-all-wildfire-861749-865616 | PAN OS 10.0 And Later | Full | 8 MB | da7b007bf37fa0c... | 2024/04/04 12:57:24 -05 | ✓ previously | | Revert |
| 861761-865628 | panupv3-all-wildfire-861761-865628 | PAN OS 10.0 And Later | Full | 8 MB | 81f80a04a85010... | 2024/04/04 13:57:20 -05 | ✓ | ✓ | |

*Figura 10. Dynamic Updates.*

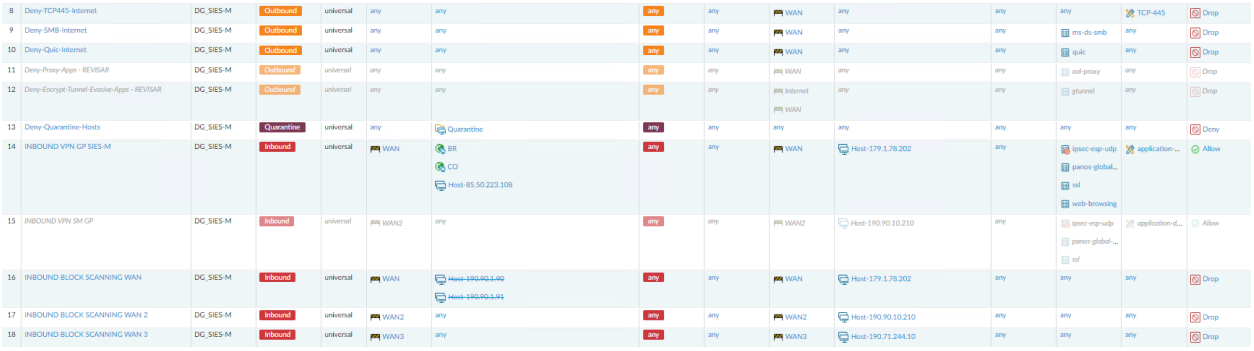
## 10. SECURITY POLICIES

En este proyecto se realizó la configuración de políticas de seguridad tipo Pre Rules, Post Rule y Default Rule.

### Security Policy Pre Rules - FW-PA-SIES-M-1

Se muestra a continuación las políticas de seguridad configuradas

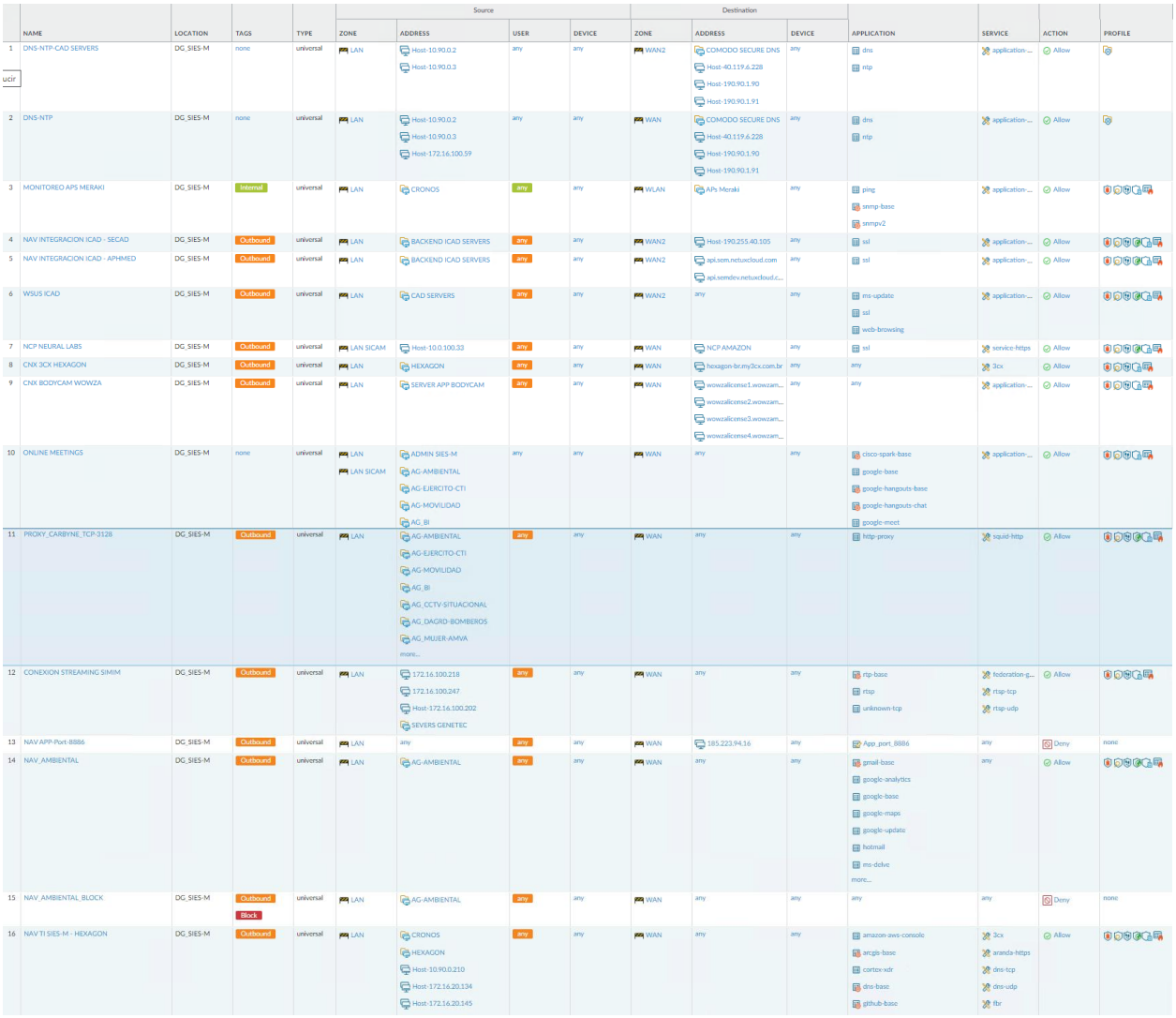
| | NAME | LOCATION | TAGS | TYPE | Source ZONE | Source ADDRESS | Source USER | Source DEVICE | Destination ZONE | Destination ADDRESS | Destination DEVICE | APPLICATION | SERVICE | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Outbound Block Rule | Shared | none | universal | any | any | any | any | any | Palo Alto Networks - Bulletproof IP addre...<br>Palo Alto Networks - High risk IP addresses<br>Palo Alto Networks - Known malicious IP ...<br>Palo Alto Networks - Tor exit IP addresses | any | any | any | Drop |
| 2 | Inbound Block Rule | Shared | none | universal | any | Palo Alto Networks - Bulletproof IP addresses<br>Palo Alto Networks - High risk IP addresses<br>Palo Alto Networks - Known malicious IP addresses<br>Palo Alto Networks - Tor exit IP addresses | any | any | any | any | any | any | any | Drop |
| 3 | Deny-Geographic-In | DG_SIES-M | Inbound | universal | any | BG<br>CN<br>CZ<br>IR<br>KP<br>KR<br>RS<br>more... | any | any | any | any | any | any | any | Drop |
| 4 | Deny-Geographic-Out | DG_SIES-M | Outbound | universal | any | any | any | any | any | BG<br>CN<br>CZ<br>IR<br>KP<br>KR<br>RS<br>more... | any | any | any | Drop |
| 5 | Deny-Malicious-IP-In | DG_SIES-M | Inbound | universal | any | Malicious-IP | any | any | any | any | any | any | any | Drop |
| 6 | Deny-Malicious-IP-Out | DG_SIES-M | Outbound | universal | any | any | any | any | any | Malicious-IP | any | any | any | Drop |
| 7 | Deny-Sinkhole-PAN | DG_SIES-M | Outbound | universal | any | any | any | any | WAN | Sinkhole-PAN | any | any | any | Drop |
| 8 | Deny-TCP445-Internet | DG_SIES-M | Outbound | universal | any | any | any | any | WAN | any | any | any | TCP-445 | Drop |



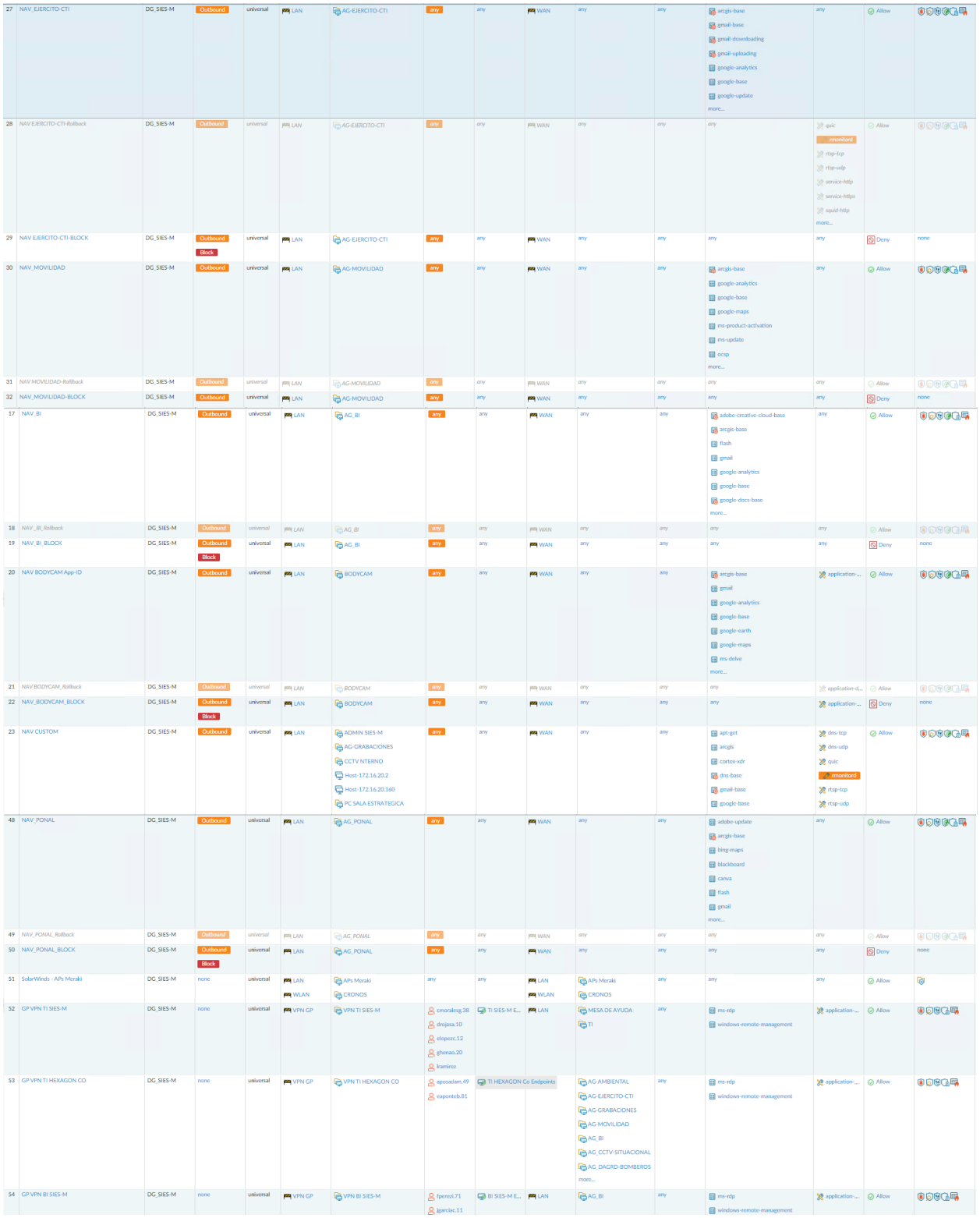
| | NAME | SOURCE ZONE | SOURCE ADDRESS | SOURCE USER | SOURCE DEVICE | DESTINATION ZONE | DESTINATION ADDRESS | DESTINATION DEVICE | APPLICATION | SERVICE | ACTION | PROFILE |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 8 | Deny-TCP445-Internet | DG_SIES-M | Outbound | universal | any | any | any | any | WAN | any | any | any | TCP-445 | Drop |
| 9 | Deny-SMB-Internet | DG_SIES-M | Outbound | universal | any | any | any | any | WAN | any | any | any | ms-ds-smb | any | Drop |
| 10 | Deny-Quic-Internet | DG_SIES-M | Outbound | universal | any | any | any | any | WAN | any | any | any | quic | any | Drop |
| 11 | Deny-Proxy-Apps - REVISAR | DG_SIES-M | Outbound | universal | any | any | any | any | WAN | any | any | any | ssl-proxy | any | Drop |
| 12 | Deny-Encrypt-Tunnel-Evasive-Apps - REVISAR | DG_SIES-M | Outbound | universal | any | any | any | any | Internet<br>WAN | any | any | any | ptunnel | any | Drop |
| 13 | Deny-Quarantine-Hosts | DG_SIES-M | Quarantine | universal | any | Quarantine | any | any | any | any | any | any | any | any | Deny |
| 14 | INBOUND VPN GP SIES-M | DG_SIES-M | Inbound | universal | WAN | BR<br>CO<br>Host-85.50.223.108 | any | any | WAN | Host-179.1.78.202 | any | ipsec-esp-udp<br>panos-global...<br>ssl<br>web-browsing | application-... | any | Allow |
| 15 | INBOUND VPN SM GP | DG_SIES-M | Inbound | universal | WAN2 | any | any | any | WAN2 | Host-190.90.10.210 | any | ipsec-esp-udp<br>panos-global-...<br>ssl | application-d... | any | Allow |
| 16 | INBOUND BLOCK SCANNING WAN | DG_SIES-M | Inbound | universal | WAN | ~~Host-190.90.1.90~~<br>~~Host-190.90.1.91~~ | any | any | WAN | Host-179.1.78.202 | any | any | any | any | Drop |
| 17 | INBOUND BLOCK SCANNING WAN 2 | DG_SIES-M | Inbound | universal | WAN2 | any | any | any | WAN2 | Host-190.90.10.210 | any | any | any | any | Drop |
| 18 | INBOUND BLOCK SCANNING WAN 3 | DG_SIES-M | Inbound | universal | WAN3 | any | any | any | WAN3 | Host-190.71.244.10 | any | any | any | any | Drop |

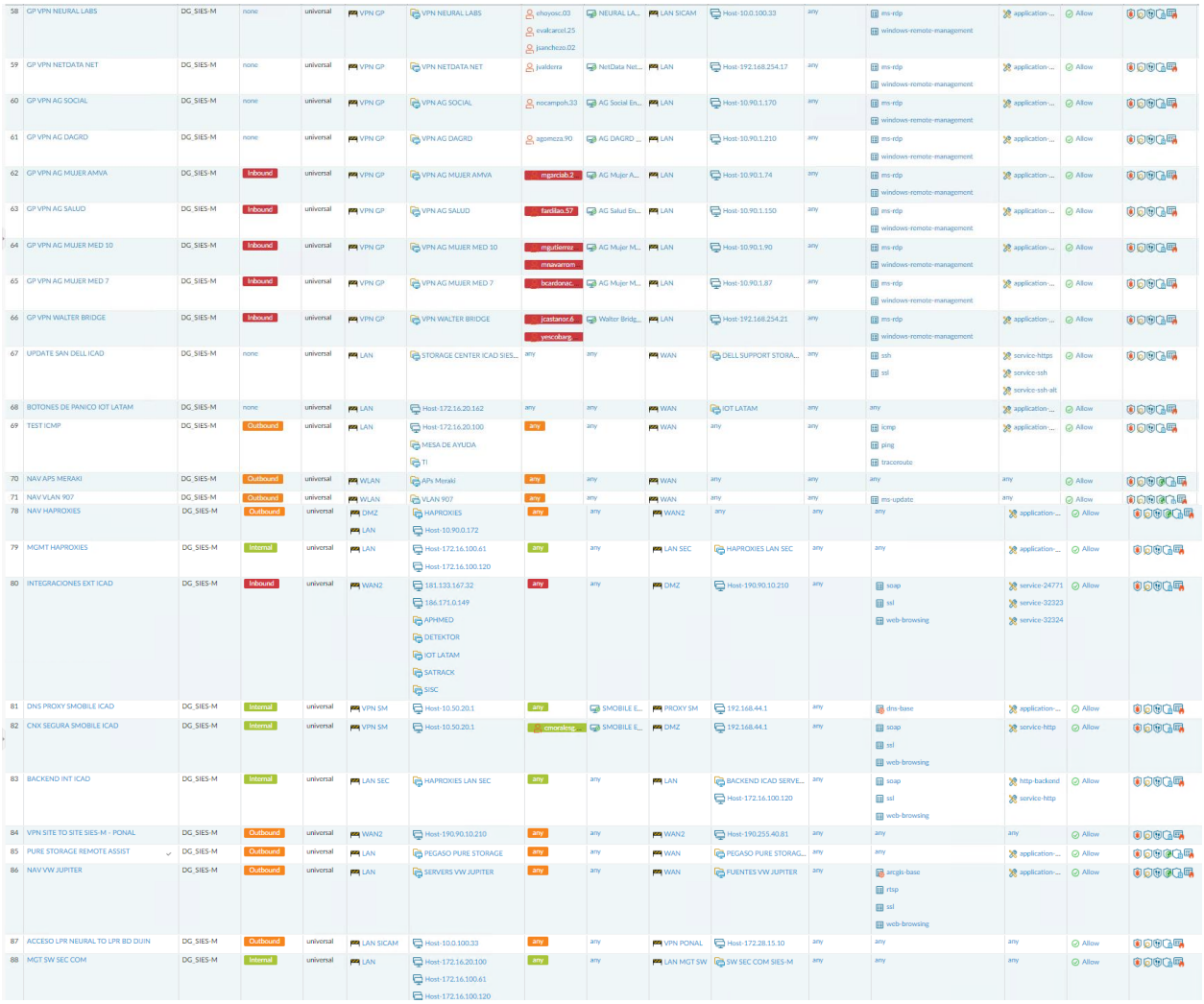
## Securtiy Policy Post Rules - FW-PA-SIES-M-1

Se muestra a continuación las políticas de seguridad configuradas:



| | NAME | LOCATION | TAGS | TYPE | SOURCE ZONE | SOURCE ADDRESS | SOURCE USER | SOURCE DEVICE | DESTINATION ZONE | DESTINATION ADDRESS | DESTINATION DEVICE | APPLICATION | SERVICE | ACTION | PROFILE |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | DNS-NTP-CAD SERVERS | DG_SIES-M | none | universal | LAN | Host-10.90.0.2<br>Host-10.90.0.3 | any | any | WAN2 | COMODO SECURE DNS<br>Host-40.119.6.228<br>Host-190.90.1.90<br>Host-190.90.1.91 | any | dns<br>ntp | application-... | Allow | |
| 2 | DNS-NTP | DG_SIES-M | none | universal | LAN | Host-10.90.0.2<br>Host-10.90.0.3<br>Host-172.16.100.59 | any | any | WAN | COMODO SECURE DNS<br>Host-40.119.6.228<br>Host-190.90.1.90<br>Host-190.90.1.91 | any | dns<br>ntp | application-... | Allow | |
| 3 | MONITOREO APS MERAKI | DG_SIES-M | Internal | universal | LAN | CRONOS | any | any | WLAN | APs Meraki | any | ping<br>snmp-base<br>snmpv2 | application-... | Allow | |
| 4 | NAV INTEGRACION ICAD - SECAD | DG_SIES-M | Outbound | universal | LAN | BACKEND ICAD SERVERS | any | any | WAN2 | Host-190.255.40.105 | any | ssl | application-... | Allow | |
| 5 | NAV INTEGRACION ICAD - APHMED | DG_SIES-M | Outbound | universal | LAN | BACKEND ICAD SERVERS | any | any | WAN2 | api.sem.netuxcloud.com<br>api.semdev.netuxcloud.c... | any | ssl | application-... | Allow | |
| 6 | WSUS ICAD | DG_SIES-M | Outbound | universal | LAN | CAD SERVERS | any | any | WAN2 | any | any | ms-update<br>ssl<br>web-browsing | application-... | Allow | |
| 7 | NCP NEURAL LABS | DG_SIES-M | Outbound | universal | LAN SICAM | Host-10.0.100.33 | any | any | WAN | NCP AMAZON | any | ssl | service-https | Allow | |
| 8 | CNX 3CX HEXAGON | DG_SIES-M | Outbound | universal | LAN | HEXAGON | any | any | WAN | hexagon-br.my3cx.com.br | any | any | 3cx | Allow | |
| 9 | CNX BODYCAM WOWZA | DG_SIES-M | Outbound | universal | LAN | SERVER APP BODYCAM | any | any | WAN | wowzalicense1.wowzam...<br>wowzalicense2.wowzam...<br>wowzalicense3.wowzam...<br>wowzalicense4.wowzam... | any | any | application-... | Allow | |
| 10 | ONLINE MEETINGS | DG_SIES-M | none | universal | LAN<br>LAN SICAM | ADMIN SIES-M<br>AG-AMBIENTAL<br>AG-EJERCITO-CTI<br>AG-MOVILIDAD<br>AG_BI | any | any | WAN | any | any | cisco-spark-base<br>google-base<br>google-hangouts-base<br>google-hangouts-chat<br>google-meet | application-... | Allow | |
| 11 | PROXY_CARBYNE_TCP-3128 | DG_SIES-M | Outbound | universal | LAN | AG-AMBIENTAL<br>AG-EJERCITO-CTI<br>AG-MOVILIDAD<br>AG_BI<br>AG_CCTV-SITUACIONAL<br>AG_DAGRD-BOMBEROS<br>AG_MUJER-AMVA<br>more... | any | any | WAN | any | any | http-proxy | squid-http | Allow | |
| 12 | CONEXION STREAMING SIMIM | DG_SIES-M | Outbound | universal | LAN | 172.16.100.218<br>172.16.100.247<br>Host-172.16.100.202<br>SEVERS GENETEC | any | any | WAN | any | any | rtp-base<br>rtsp<br>unknown-tcp | federation-g...<br>rtsp-tcp<br>rtsp-udp | Allow | |
| 13 | NAV APP-Port-8886 | DG_SIES-M | Outbound | universal | LAN | any | any | any | WAN | 185.223.94.16 | any | App_port_8886 | any | Deny | none |
| 14 | NAV_AMBIENTAL | DG_SIES-M | Outbound | universal | LAN | AG-AMBIENTAL | any | any | WAN | any | any | gmail-base<br>google-analytics<br>google-base<br>google-maps<br>google-update<br>hotmail<br>ms-delve<br>more... | any | Allow | |
| 15 | NAV_AMBIENTAL_BLOCK | DG_SIES-M | Outbound<br>Block | universal | LAN | AG-AMBIENTAL | any | any | WAN | any | any | any | any | Deny | none |
| 16 | NAV TI SIES-M - HEXAGON | DG_SIES-M | Outbound | universal | LAN | CRONOS<br>HEXAGON<br>Host-10.90.0.210<br>Host-172.16.20.134<br>Host-172.16.20.145 | any | any | WAN | any | any | amazon-aws-console<br>arcgis-base<br>cortex-xdr<br>dns-base<br>github-base | 3cx<br>aranda-https<br>dns-tcp<br>dns-udp<br>tbr | Allow | |





## Security Policy Default Rules - FW-PA-SIES-M-1

Se muestra a continuación las políticas de seguridad configuradas:

| | NAME | LOCATION | TAGS | TYPE | Source | | | | Destination | | | APPLICATION | SERVICE | ACTION |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | | | |
| 1 | intrazone-default | DG_SIES-M | none | intrazone | any | any | any | any | (intrazone) | any | any | any | any | Allow |
| 2 | interzone-default | Shared | none | interzone | any | any | any | any | any | any | any | any | any | Deny |

## Security Policy Pre Rules - FW-VM-SIES-M-1& FW-VM-SIES-M-2

| | | | | | Source | | | Destination | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | LOCATION | TAGS | TYPE | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | APPLICATION | SERVICE | ACTION |
| 1 | Outbound Block Rule | Shared | none | universal | any | any | any | any | any | Palo Alto Networks - Bulletproof IP addre...<br>Palo Alto Networks - High risk IP addresses<br>Palo Alto Networks - Known malicious IP ...<br>Palo Alto Networks - Tor exit IP addresses | any | any | any | Drop |
| 2 | Inbound Block Rule | Shared | none | universal | any | Palo Alto Networks - Bulletproof IP addresses<br>Palo Alto Networks - High risk IP addresses<br>Palo Alto Networks - Known malicious IP addresses<br>Palo Alto Networks - Tor exit IP addresses | any | any | any | any | any | any | any | Drop |
| 3 | Deny-Malicious-IP-In | DG_SIES-M_H | Inbound | universal | any | Malicious-IP | any | any | any | any | any | any | any | Drop |

## Security Policy Post Rules - FW-VM-SIES-M-1& FW-VM-SIES-M-2

| | | | | | Source | | | | Destination | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | LOCATION | TAGS | TYPE | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | APPLICATION | SERVICE | ACTION | PROFILE |
| 1 | CNX DNS PROXY | DG_SIES-M_H | Internal | universal | VW JUPITER | Host-192.168.202.62 | any | any | SIES-M | DNS ICAD | any | dns-base | application-... | Allow | |
| 2 | CNX VW JUPITER TO SIES-M APPID | DG_SIES-M_H | Inbound | universal | VW JUPITER | VW JUPITER | any | any | SIES-M | CAMS VW JUPITER<br>SEVERS GENETEC | any | ms-rdp<br>netbios-ns<br>ping<br>rtcp<br>rtp<br>rtsp<br>soap<br>more... | any | Allow | |
| 3 | CNX VW JUPITER TO SIES-M | DG_SIES-M_H | Inbound | universal | VW JUPITER | VW JUPITER | any | any | SIES-M | CAMS VW JUPITER<br>SEVERS GENETEC | any | any | any | Allow | |
| 4 | CNX VW JUPITER TO SOURCES | DG_SIES-M_H | Inbound | universal | VW JUPITER | SERVERS VW JUPITER | any | any | SIES-M | FUENTES VW JUPITER | any | rtsp<br>ssl<br>web-browsing<br>websocket | service-http<br>service-https<br>service-rtsp-...<br>service-rtsp-...<br>service-solar... | Allow | |
| 5 | CNX UE TO VW JUPITER APPID | DG_SIES-M_H | Internal | universal | SOP UE | SOPORTE UNION ELECTRICA | any | any | VW JUPITER | VW JUPITER | any | ping<br>ssh<br>web-browsing | application-... | Allow | |
| 6 | CNX UE TO VW JUPITER | DG_SIES-M_H | Internal | universal | SOP UE | SOPORTE UNION ELECTRICA | any | any | VW JUPITER | VW JUPITER | any | any | any | Allow | |
| 7 | CNX UE TO SIES-M-APPID | DG_SIES-M_H | Inbound | universal | SOP UE | SOPORTE UNION ELECTRICA | any | any | SIES-M UE | SERVICIOS UNION ELE... | any | cotp<br>ftp<br>http-audio<br>http-proxy<br>http-video<br>icmp<br>hsi-raid-mgmt_TCP_2463<br>more... | any | Allow | |
| 8 | CNX UE TO SIES-M | DG_SIES-M_H | Inbound | universal | SOP UE | SOPORTE UNION ELECTRICA | any | any | SIES-M UE | SERVICIOS UNION ELE... | any | any | any | Allow | |
| 9 | CNX MICROSTRATEGY TO ICAD-APPID | DG_SIES-M_H | Inbound | universal | SVR CAM | MICROSTRATEGY CAM | any | any | SIES-M CAM | Host-10.90.0.20 | any | any | application-... | Allow | |
| 10 | CNX MICROSTRATEGY TO ICAD | DG_SIES-M_H | Inbound | universal | SVR CAM | MICROSTRATEGY CAM | any | any | SIES-M CAM | Host-10.90.0.20 | any | any | application-... | Allow | |

## Security Policy Default Rules - FW-VM-SIES-M-1& FW-VM-SIES-M-2

| | | | | | Source | | | | Destination | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | LOCATION | TAGS | TYPE | ZONE | ADDRESS | USER | DEVICE | ZONE | ADDRESS | DEVICE | APPLICATION | SERVICE | ACTION |
| 1 | intrazone-default | DG_SIES-M | none | intrazone | any | any | any | any | (intrazone) | any | any | any | any | Allow |
| 2 | interzone-default | Shared | none | interzone | any | any | any | any | any | any | any | any | any | Deny |

## 11. NAT POLICIES

### NAT Policy Pre Rules - FW-PA-SIES-M-1

| | | | | Original Packet | | | | | | Translated Packet | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | LOCATION | TAGS | SOURCE ZONE | DESTINATION ZONE | DESTINATION INTERFACE | SOURCE ADDRESS | DESTINATION ADDRESS | SERVICE | SOURCE TRANSLATION | DESTINATION TRANSLATION |
| 1 | S-NAT | DG_SIES-M | Outbound | LAN<br>LAN SICAM<br>WLAN | WAN | ethernet1/1 | any | any | any | dynamic-ip-and-port<br>ethernet1/1<br>179.1.78.202/29 | none |
| 2 | S-NAT CAD SERVERS | DG_SIES-M | Outbound | DMZ<br>LAN | WAN2 | ethernet1/4 | 10.90.0.211<br>CAD SERVERS<br>HAPROXIES | any | any | dynamic-ip-and-port<br>ethernet1/4<br>190.90.10.210/30 | none |
| 3 | S-NAT TEL IP NUSE ... | DG_SIES-M | Outbound | LAN TEL | WAN3 | ethernet1/5.732 | TEL IP NUSE 1... | any | any | dynamic-ip-and-port<br>ethernet1/5.732<br>190.71.244.10/29 | none |
| 4 | PORT FWD INT ICA... | DG_SIES-M | Inbound | WAN2 | WAN2 | ethernet1/4 | any | Host-190.90.10.210 | service-24771 | none | destination-translation<br>address: Host-10.123.0.1<br>port: 38220 |
| 5 | PORT FWD INT ICA... | DG_SIES-M | Inbound | WAN2 | WAN2 | ethernet1/4 | any | Host-190.90.10.210 | service-32323 | none | destination-translation<br>address: Host-10.123.0.1<br>port: 10400 |
| 6 | PORT FWD INT ICA... | DG_SIES-M | Inbound | WAN2 | WAN2 | ethernet1/4 | any | Host-190.90.10.210 | service-32324 | none | destination-translation<br>address: Host-10.123.0.1<br>port: 10500 |
| 7 | PORT FWD CNX SE... | DG_SIES-M | Inbound | VPN SM | PROXY SM | loopback.1 | Host-10.50.20.1 | 192.168.44.1 | service-http | none | destination-translation<br>address: Host-10.123.0.1<br>port: 10600 |

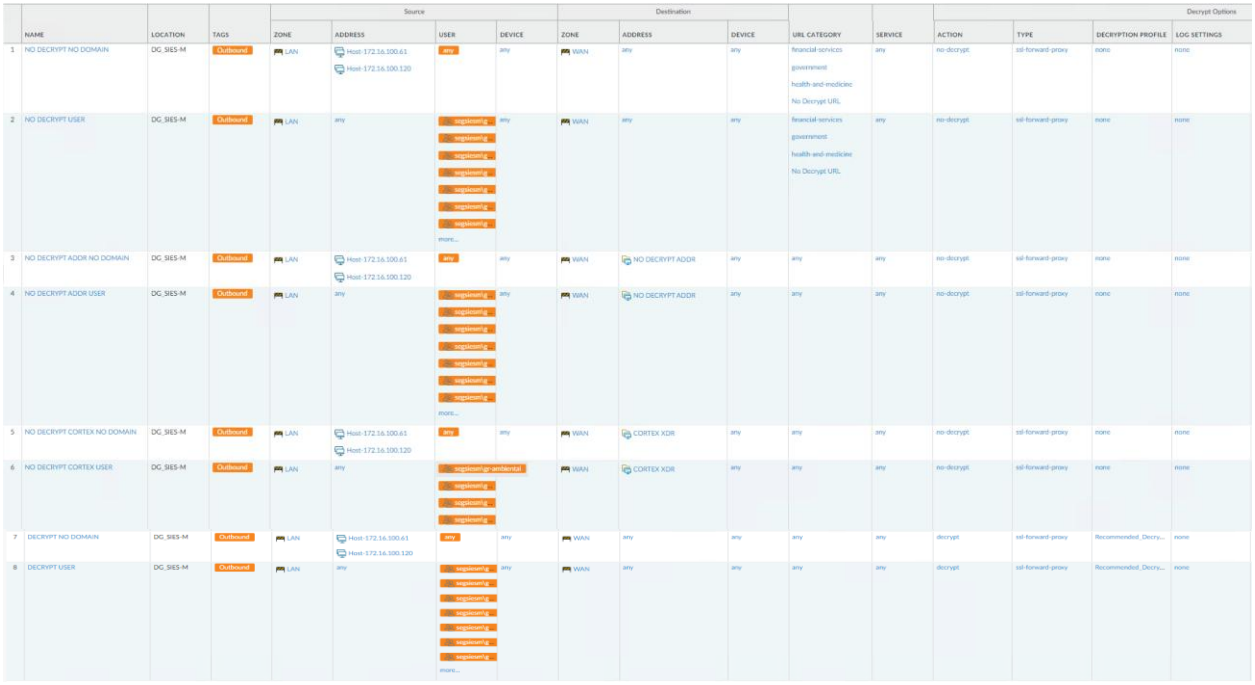
## 12. PBF POLICIES

### PBF Policy Pre Rules - FW-PA-SIES-M-1

| | | | | Source | | | Destination | | | | Forwarding | | | Monitoring | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | NAME | LOCATION | TAGS | ZONE/INTERFACE | ADDRESS | USER | ADDRESS | APPLICATION | SERVICE | ACTION | EGRESS I/F | NEXT HOP | ENFORCE SYMMETRIC RETURN | PROFILE | TARGET | DISABLE IF UNREACHABLE |
| 1 | PBF CAD SERVERS | DG_SIES-M | Outbound | DMZ<br>LAN | CAD SERVERS<br>HAPROXIES | any | HAPROXIES 1...<br>Host-10.50.20.1<br>VPN TI HEXA...<br>VPN TI HEXA... | any | any | forward | ethernet1/4 | 190.90.10.209 | true | MONITOR CAD ... | none | false |
| 2 | PBF TEL NUSE 123 | DG_SIES-M | Outbound | LAN TEL | TEL IP NUSE 1... | any | any | any | any | forward | ethernet1/5.732 | 190.71.244.9 | true | MONITOR TEL ... | none | false |

## 13. DECRYPTION POLICIES

### Decryption Policy Pre Rules - FW-PA-SIES-M-1



## 14. SERVER PROFILES

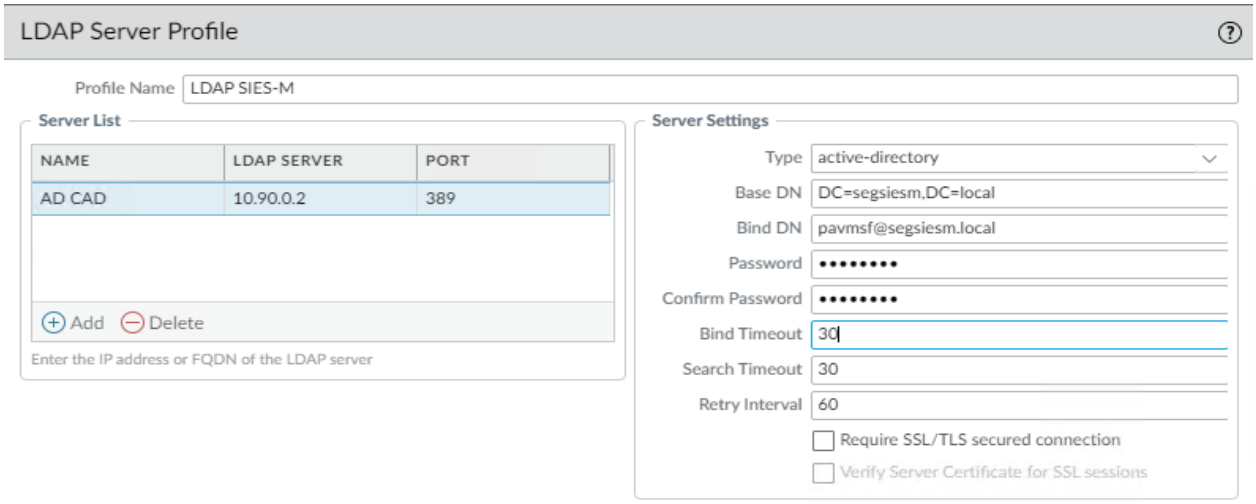
Se muestra a continuación la configuración de los Server Profiles que se implementaron en este proyecto.

### 14.1. LDAP

Se realiza la configuración del Server Profile tipo LDAP llamado LDAP SIES-M, posteriormente utilizado en la configuración de User-ID:

| Profile Name | Server List | Server Settings |
|---|---|---|
| *LDAP SIES-M* | *Name: AD CAD*<br>*LDAP Server: 10.90.0.2*<br>*Port: 389* | *Type: active-directory*<br>*Base DN: DC=segsiesm,DC=local*<br>*Bind DN: pavmsf@segsiesm.local*<br>*Bind Timeout: 30*<br>*Search Timeoput: 30*<br>*Retry Interval: 60* |

*Tabla 17. LDAP Server Profile.*




## 15. USER-ID

Para el cliente **SIES Medellín**, se han configurado un agente de user-ID agent para recolectar la información de asociación de IP's con usuario. El Group Mapping fue configurado para aprender desde el Directorio Activo. El User-ID fue configurado para hacer control en políticas seguridad basado en usuarios.

### 15.1. FUENTES DE User-ID

| User-ID Source | Type | IP Address | Port | Configured Interface |
|---|---|---|---|---|
| *LDAP* | *UID Agent* | *userid.sseguridad.sies*<br>*172.16.100.98* | *5007* | *Ethernet1/2* |

*Tabla 18. Fuente de User ID.*

### 15.2. Group Mapping Profiles

| Server Profile | Domain Setting | Group Object class | User Object Class | User and Group Attributes | Group Include List |
|---|---|---|---|---|---|
| *LDAP SIES-M* | *segsiesm* | *group* | *person* | *sAMAccountName*<br>*userPrincipalName* | |

*Tabla 19. Mapeo de Grupos de usurarios.*

## 16. RECOMENDACIONES

En esta sección se plantearán los próximos pasos y recomendaciones que se deben tomar para mejorar la administración y funcionamiento de la solución. Entre las acciones recomendadas están:

a) Se recomienda mantener la misma versión de PAN-OS en el NGFW On-Site-Spare, este debe ser cargado de forma manual para lograr realizar el up-grade con éxito. Adicionalmente, se recomienda exportar una copia de seguridad al NGFW On-Site-Spare de forma periódica del NGFW productivo.

b) Monitorear el tráfico y el número de sesiones por segundo de las VM-Series, con el fin de lograr un afinamiento en los valores definidos para los umbrales configurados en el *Zone Protection Profile*.

c) Terminar el proceso de adopción de APP-ID, con la depuración de las políticas sin tráfico, apoyándose en los resultados arrojados por el documento BPA emitido por PaloAltoNetworks.

d) Revisar periódicamente las vulnerabilidades conocidas brindas por los diferentes reportes del proveedor PaloAltoNetworks.y Unit42.

   Link de referencia: https://security.paloaltonetworks.com/

e) Revisar periódicamente los Release Notes de las nuevas versiones de PAN-OS otorgados por el proveedor, identificando los nuevos features y problemas conocidos solventados.

   Link de referencia: https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-release-notes/features-introduced-in-pan-os

## 17. CONSIDERACIONES

En esta sección se listan los puntos clave de la implementación, así como las configuraciones de NGFW que fueron descartadas, dado que no se tenía un caso de uso puntual, o no fue considerada necesaria para su despliegue en la infraestructura propuesta.

1) El NGFW On-Site-Spare ha quedado conectado con Panorama mediante su dirección IP de management, sin asignar ningún Device Group y sin asignar ningún template.
2) En caso de que se deba generar un evento de failover y deba ser migrado el tráfico del NGFW en producción al NGFW On-Site-Spare, se recomienda hacer uso de los Device Group y lo Template para transferir la configuración al NGFW On-Site-Spare
3) No se configuró políticas de DoS dado que no se encontraron casos de uso. Sin embargo, se tiene configuración de Zone Protection. Nota: esto no afecta la postura de seguridad del NGFW dentro de la infraestructura.
4) No se configuró políticas de QoS dado que no se encontraron casos de uso. Sin embargo, se tiene la configuración de Police Base Forwarding. Nota: esto no afecta la postura de seguridad del NGFW dentro de la infraestructura.

| EN CONSTANCIA SE FIRMA | |
| --- | --- |
| Firma:<br>Nombre: Andres Alvarez G.<br>Cargo: GERENTE PROYECTOS Y SERVICIOS<br>Empresa: BOYRA S.A. | Firma:<br>Nombre: Cristian Morales<br>Cargo: Profesional Seguridad Informatica<br>Empresa: secretaria de Medellín |