Manual de usuario servicio FortiPortal

euskaltel telecable

Grupo Euskaltel

Contenido

1 Introducción a FortiPortal 3
2 División por tipo de cliente 4
3 Portal web 5
4 Dashboard 9
5 Política Firewall 12
5.1 Instalación de políticas 16
5.2 Regla de acceso 19
6 Objetos Firewall 28
6.1 Zone/Interface 29
6.2 Firewall Objects 29
6.3 Security Profiles 35
6.3.1 Antivirus 35
6.3.2 Control de Aplicaciones 37
6.3.3 Data Leak Prevention 38
6.3.4 Email Filter 39
6.3.5 IPS 39
6.3.6 Web Filter 40
6.4 User & Device 43
7 View 44
7.1 Application View 46
7.2 Attack 48
7.3 Sandbox 48
8 Reports 49
9 Audit 50
10 Recursos adicionales 51
11 Wifi 52
11.1 Managed AP 52
11.2 WiFi Monitor 52
11.3 WiFi Profile 55

12 SDWAN 57
12.1 SD-WAN status y opciones avanzadas 58
12.2 Configuración SD-WAN 59
12.2.1 Configuración de interfaces 59
12.2.2 Configuración de SLA 61
12.2.3 Reglas SD-WAN 63
12.3 Monitorización SD-WAN 65
12.4 Plantillas SD-WAN 65

1 Introducción a FortiPortal

Este documento es un manual detallado de las operativas que puede realizar autónomamente un usuario final en la política de seguridad de su firewall virtual en la plataforma ofrecida por Euskaltel, a través de la nueva herramienta Fortiportal.

Fortiportal refleja a través de un portal web interactivo, todas las características de la política de seguridad y aporta visibilidad de los flujos que gestiona dicha política a través de cuadros de mando, gráficos de tráfico, análisis de logs y reportes de datos agregados.

Dispone de acciones tanto de análisis como de cambios en la política que pueden realizarse de forma sencilla.

2 División por tipo de cliente

No todos los clientes tienen los mismos privilegios para realizar los cambios en los diferentes componentes de la política de seguridad de su firewall virtual.

Estos componentes principalmente son:

- **Política Firewall** (reglas de acceso)
- **NAT**
- **Control de aplicaciones**
- **Web filter (navegación)**
- **Antispam**
- **Antivirus**
- **IPS**
- **ATP (Advanced Threat Prevention)**
- **Wifi y FortiAP**
- **SDWAN**

Para organizar dichos privilegios se han seleccionado 3 tipos de clientes, que mostramos a continuación, por orden de menor a mayor número de funcionalidades adquiridas:

- **Cliente Avanzado:** Además de los permisos de acceso y modificación de la política firewall, también maneja los perfiles de Control de Aplicaciones.
- **Cliente con Navegación:** Posee los mismos permisos que el cliente avanzado, a los que añade los de definición de filtrado web (URL Web Filtering) y antivirus para navegación.
- **Cliente Premium:** el perfil más avanzado incluye todos los permisos anteriores, más el control sobre la política de IPS (Intrusion Prevention) y ATP o sandboxing en cloud.

Además existen dos tipos de cliente centrados en dos características concretas de la política de seguridad:

- **Cliente administrador FortiAPs**
- **Cliente administrador SDWAN**

Estos dos perfiles de cliente se pueden asignar como único perfil para ese cliente o añadir a los perfiles de administración de política generales, vistos más arriba.

La siguiente tabla recoge la comparativa de los perfiles según sus privilegios de administración y cambios en cada una de las características de su política de seguridad:

Tabla 1

	Lectura y Escritura				
	Avanzado	Navegación	Premium	FortiAPs	SDWAN
Dashboards	✓	✓	✓	✓	✓
Reportes	✓	✓	✓	✓	✓
Logs View	✓	✓	✓	✓	✓
Auditoria	✓	✓	✓	✓	✓
FW Policy	✓	✓	✓		
Control APP	✓	✓	✓		
URL web filter		✓	✓		
Antivirus		✓	✓		
IPS			✓		
ATP			✓		
WIFI y FortiAP				✓	
SDWAN					✓

3 Portal web

El servicio de FortiPortal es accesible a través de la URL:

https://fwvirtualportal.com

La página de acceso presenta la siguiente apariencia:

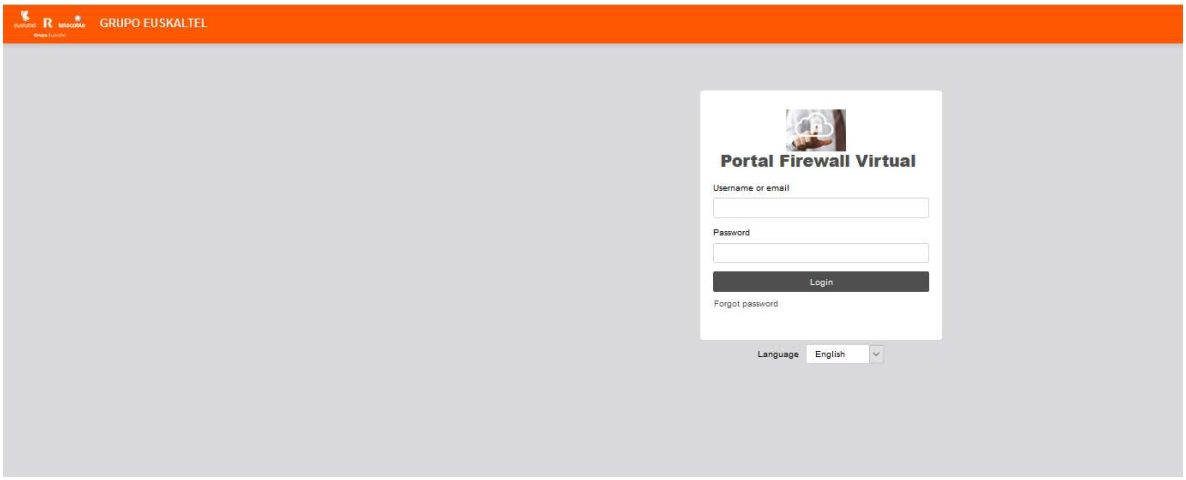


Ilustración 1

En la misma podemos elegir el idioma en el que se mostrarán los diferentes menús:

- Inglés
- Español
- Italiano
- Rumano
- Portugués
- Francés
- Alemán

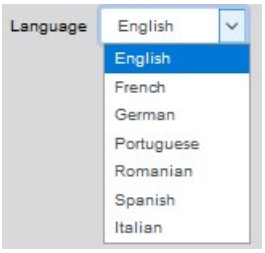


Ilustración 2

Tras rellenar los datos de usuario y contraseña, podemos acceder a los menús del portal:

Si no recordamos la contraseña, existe la posibilidad de recuperarla mediante correo electrónico, de modo temporal, pulsando sobre "Forgot password":

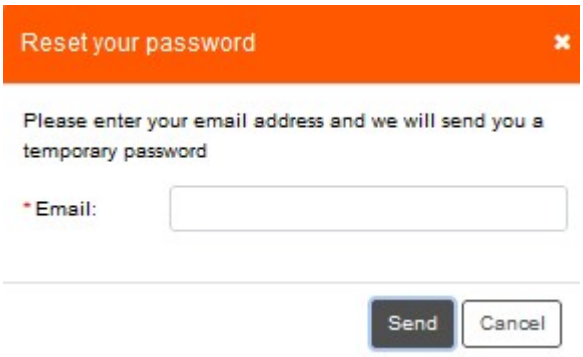


Ilustración 3

Una vez autenticados, accedemos a la información sobre el firewall virtual, en una ventana como la siguiente:

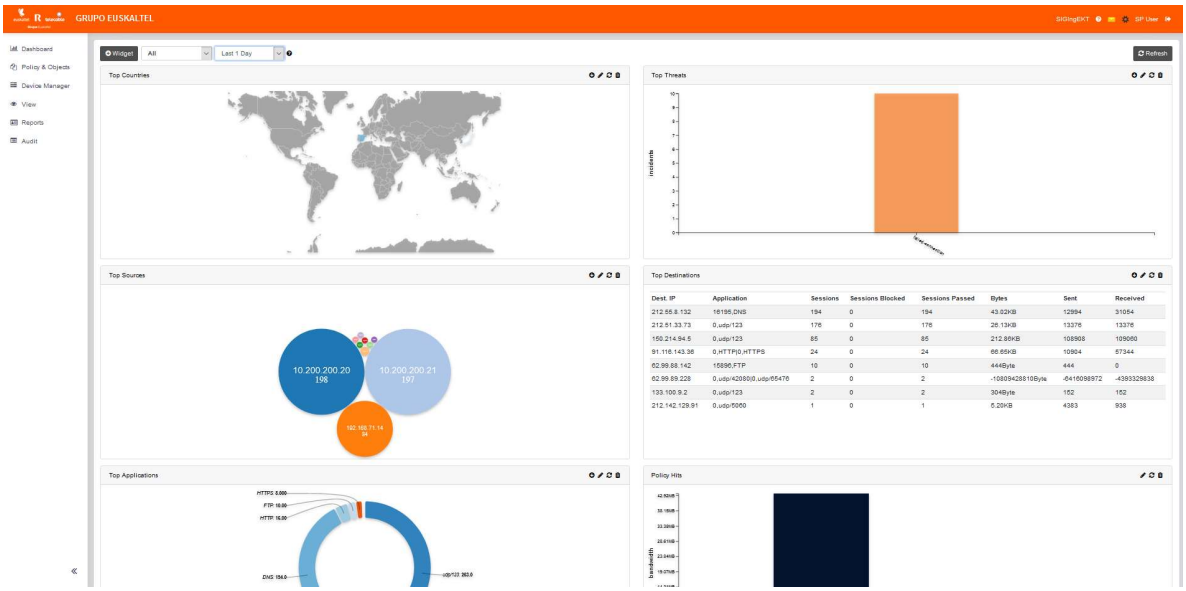


Ilustración 4

Podemos distinguir las siguientes partes:

1. **Barra de usuario**
   Está en el extremo superior derecho, y contiene los siguientes botones de acceso:

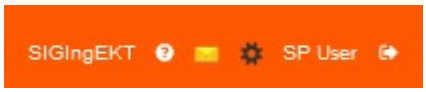


Ilustración 5

De izquierda a derecha:

Help > Abre una nueva ventana con el manual de usuario como ayuda contextual.

Alerts > Muestra en un pop-up las alertas que afectan al portal o la configuración del firewall virtual

Change Password > Abre una ventana de diálogo que permite cambiar la contraseña de acceso de nuestro usuario. Para ello debemos proporcionar la contraseña antigua y una nueva:

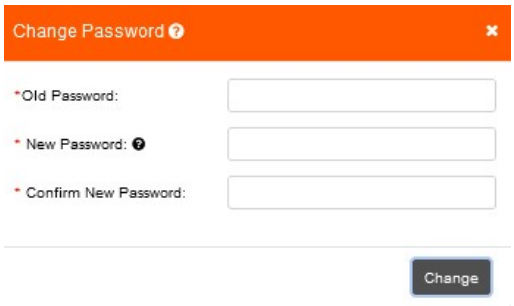
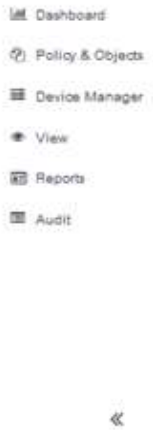


Ilustración 6

Exit > Cierra la sesión actual en FortiPortal.

2. Panel de administración



Incluye los principales menús de acceso a la información sobre el firewall virtual:

- **Dashboard** muestra el cuadro de mando con la información más relevante del estado del firewall virtual y el tráfico que gestiona
- **Policy & Objects** da acceso a la política de seguridad del firewall para revisar su configuración y modificarla si se tienen permisos suficientes
- **View** muestra información relativa a los eventos de seguridad recogidos en los logs de la plataforma. Esta información se puede filtrar o ahondar en ella de modo que podamos investigar en mayor profundidad el tráfico.
- **Reports** accede a los diferentes reportes disponibles desde FortiAnalyzer.
- **Audit** ofrece un listado de acciones efectuadas por los administradores sobre la política y configuración del firewall virtual.

El panel se oculta si pulsamos sobre **(<<) Collapse Sidebar**

3. **Panel central**

   Muestra la información seleccionada en cada uno de los menús, de forma interactiva.

A continuación, pasamos a revisar la información que muestra cada uno de los menús generales.

4 Dashboard

Es un cuadro de mando que aglutina toda la información sobre tráfico y eventos en varios gráficos y tablas que llamamos widget.

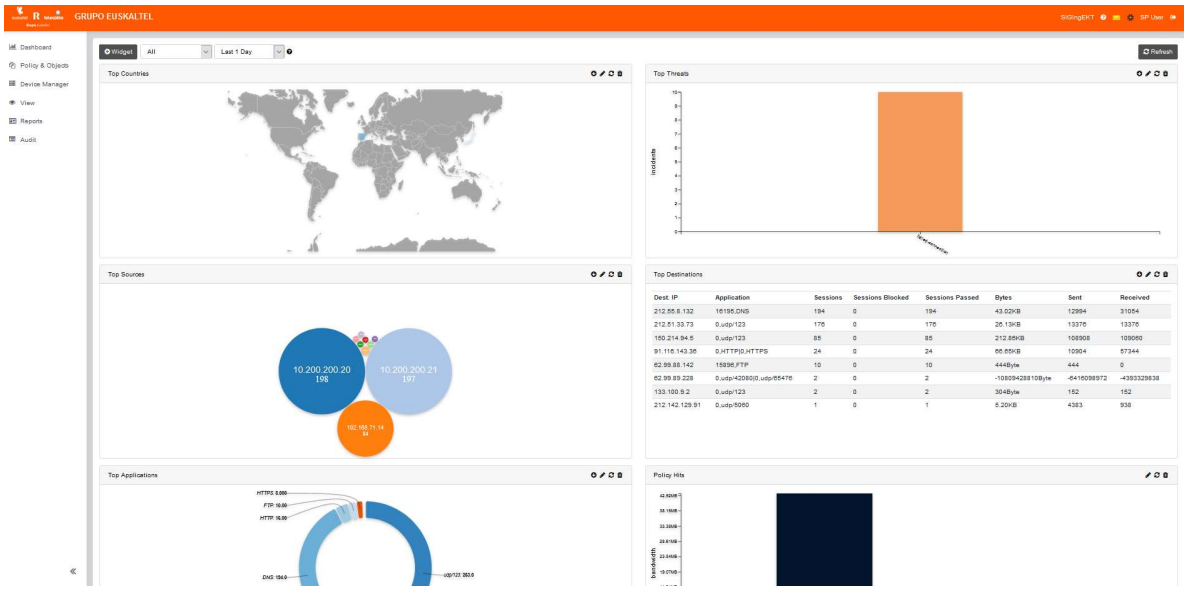


Ilustración 7

Mediante los controles de la parte superior, podemos:

- **+ Widget**, añadir un nuevo cuadro de información
- **Refresh**, refrescar la información desde FortiAnalyzer. Está en la esquina superior derecha.
- **Scope**, cambia la vista de los widgets: **All** (todos), para un **site** concreto o **Wireless** (wifi y FortiAP). En nuestro caso no existe más de un site, por lo que All y site mostrarán la misma información.
- **Filter**, filtra los datos por ventana de tiempo (última hora, último día, última semana o un filtro personalizado)

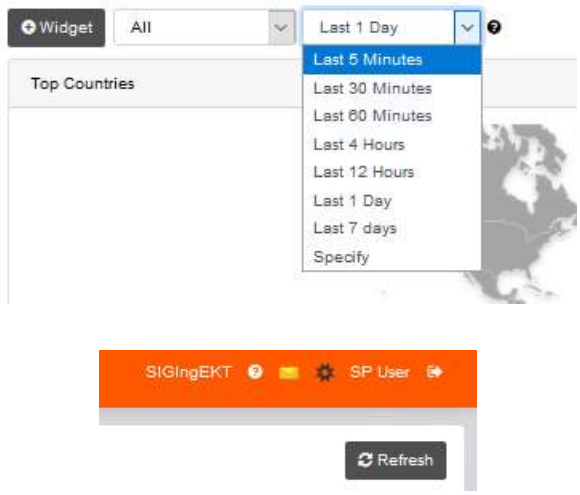


Ilustración 8

Los widgets que podemos añadir son:

- **Top Countries:** los países más visitados por la navegación de los usuarios
- **Top Threats:** las mayores amenazas de intrusión o problemas
- **Top Sources:** los orígenes con mayor número de conexiones
- **Top Destinations:** las direcciones IP públicas que más visitan los usuarios
- **Top Applications:** las aplicaciones más usadas.
- **Policy Hits:** las reglas con más uso.
- **Admin Logins:** los últimos accesos de administradores a la configuración
- **System Events:** logs de los problemas que detecta el sistema.
- **Resource Usage:** uso de los recursos asignados por la plataforma.

Los widgets son editables al pulsar sobre la barra superior el icono con forma de lápiz 

Por ejemplo, podemos modificar el tipo de gráfico, el número de elementos en el top, y el criterio para ordenarlos:

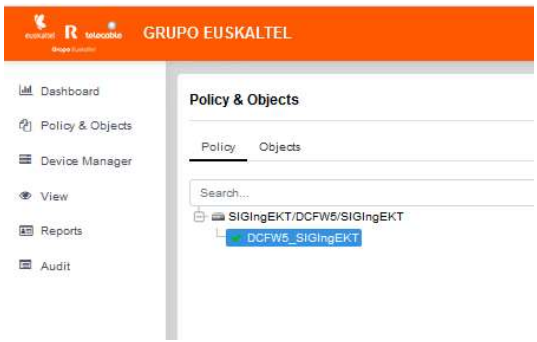
Ilustración 9

Si pulsamos sobre el icono en forma de cubo de basura, eliminamos ese widget del cuadro de mando.

5 Política Firewall

Recoge las reglas de acceso de modo secuencial tal y como están aplicadas en el firewall.

Es accesible desde el menú "**Policy & Objects**" del cliente:



En la pestaña "**Policy**" aparecerá las políticas disponibles. Normalmente sólo hay una, pero pueden ser varias si hay más de un firewall asignado, o si hay varias versiones de política en un mismo entorno.

Las características de cada una se pueden revisar, pulsando el botón derecho sobre el nombre y eligiendo "**View Package Settings**". Sólo si el usuario tiene permisos sobre la política podrá modificar el nombre, si usa o no **Central NAT** y el tipo de Inspección que utiliza globalmente para revisar el tráfico: modo **Flow** (fluido, más rápido para que el usuario no observe cortes de la comunicación) o el modo **Proxy** (la conexión se almacena en un buffer para una inspección más profunda y se sirve al destino cuando acaba esta

inspección. El usuario puede notar un poco de retraso). Por defecto será el modo **Proxy:**

Ilustración 10

Se puede elegir una de las políticas o paquetes de política, y aparecerá a la derecha, las reglas de dicha política:

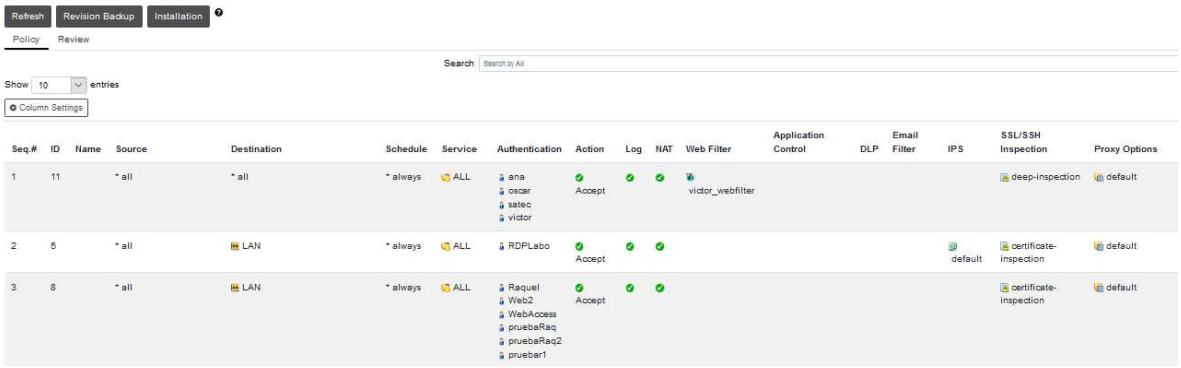


Ilustración 11

Aparecen dos números asociados a cada regla:

- **Número de secuencia (Seq. #):** es el número secuencial que indica el orden de la regla dentro de la política.
- **Número ID** de la regla: es el número unívoco que se genera al crear una nueva regla y que se le asignar para siempre. Si la regla se borra, ese número ID no vuelve a reasignarse.

Hay tres opciones que podemos realizar de forma general con la política y que aparecen encima de la misma:

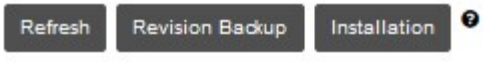


Ilustración 12

Refresh: actualiza la política desde los firewalls, mostrando en el portal la más actual y sincronizada con los firewalls.

Revision backup: guarda una copia de la política a modo de backup, para volver a ella rápidamente, si realizamos algún cambio erróneo en la misma, posterior al backup.

Si pulsamos sobre este botón, aparece un menú donde podemos ver la copia de seguridad disponible.

Si pulsamos sobre "**+Create**" se generará un nuevo backup, sobrescribiendo el anterior. Solo es posible una copia de seguridad almacenada a la vez.

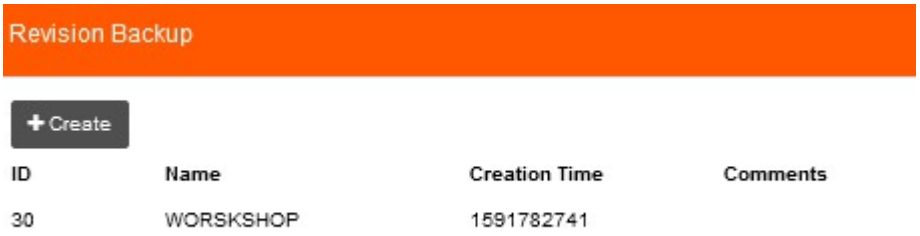


Ilustración 13

Si pulsamos sobre el backup con el botón derecho, aparece el menú de recuperación del mismo ("**Restore**"). Al pulsarlo se carga la política anterior, eliminando los cambios hechos hasta ahora en el paquete de política.

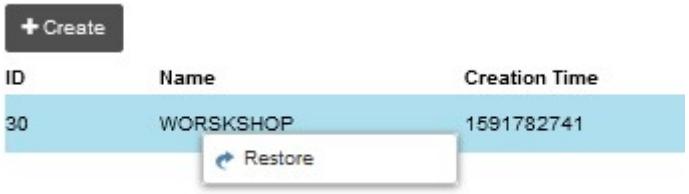


Ilustración 14

Installation nos muestra las últimas instalaciones y el botón para lanzar una nueva:

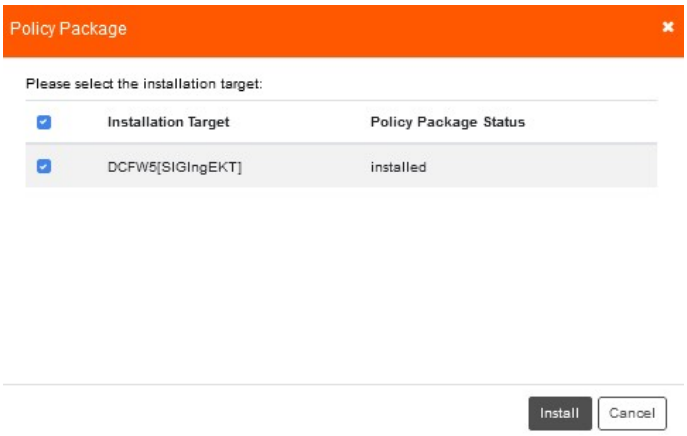


Ilustración 15

Además, existen dos pestañas:

Policy, con la política que tiene guardada el Portal (y sincronizada con FMG).

Review muestra en un formato compacto toda la información sobre las reglas que componen la política y los objetos firewall definidos y UTM en la misma:

Policy

ID	Source Interface	Destination Interface	Source	Destination	Action	Status	NAT	Service	Schedule	Authentication	Log	Security Profiles	Comments
11	sslvpn_tun_intf	* any	* all	* all	accept	enable	enable	ALL	* always	ana oscar satec victor	Enable	victor_webfilter deep-inspection default	Clone of 5 test WORK
5	sslvpn_tun_intf	* any	* all	LAN	accept	enable	enable	ALL	* always	RDPLabo	Enable	default default certificate-inspection default	
8	sslvpn_tun_intf	* any	* all	LAN	accept	enable	enable	ALL	* always	Raquel Web2 WebAccess pruebaRaq pruebaRaq2 pruebar1	Enable	default certificate-inspection default	
17	sslvpn_tun_intf	* any	* all	LAN_MAQUETA_SD_WAN VPRN_WAN	accept	enable	enable	ALL	* always	Infovista	Log Security Events	certificate-inspection default	
2	* any	* any	LAN LAN SD-WAN LAN SOLUCION EMPRESA VPRN_WAN	* all	accept	enable	enable	ALL	* always		Enable	AV-flow default certificate-inspection default_default_sc	
7	* any	* any	* all	VIP_SRV_10.10.2.10_FTP	accept	enable	enable	FTP FTP_20	* always		Enable	certificate-inspection default	
9	* any	Vlan_367	LAN	AzureNetwork	accept	enable	disable	ALL	* always		Enable	certificate-inspection default	
10	Vlan_367	Vlan_320	AzureNetwork	LAN	accept	enable	disable	ALL	* always		Enable	certificate-inspection default	
13	* any	* any	* all	VIP_10.71.32.2_SDWAN_S3	accept	enable	enable	HTTPS	* always		Log Security Events	certificate-inspection default	
19	* any	* any	* all	VIP_10.110.255.14_SDWAN_S1	accept	enable	enable	HTTPS	* always		Log Security Events	certificate-inspection default	comentario test
20	* any	* any	* all	VIP_10.110.255.22_SDWAN_S2	accept	enable	enable	HTTPS	* always		Log Security Events	certificate-inspection default	

Ilustración 16

Address

Name	Type	Interface	Default Mapping	Comments
AzureNetwork	Address	Vlan_367	IP/MASK:10.250.252.0/255.255.255.0	
FIREWALL_AUTH_PORTAL_ADDRESS	Address	any	IP/MASK:0.0.0.0/0.0.0.0	
LAN	Address	any	IP/MASK:10.10.2.0/255.255.255.0	
LAN SD-WAN	Address	any	IP/MASK:10.110.255.0/255.255.255.0	
LAN SOLUCION EMPRESA	Address	any	IP/MASK:10.200.200.0/255.255.255.0	
LAN_HUB	Address	any	IP/MASK:172.16.0.0/255.255.255.0	
LAN_MAQUETA_SD_WAN	Address Group		LAN_HUB, LAN_SPOKE_1, LAN_SPOKE_2	
LAN_SPOKE_1	Address	any	IP/MASK:172.16.1.0/255.255.255.0	
LAN_SPOKE_2	Address	any	IP/MASK:172.16.2.0/255.255.255.0	
SSLVPN_TUNNEL_ADDR1	Address	sslvpn_tun_intf	IP Range:10.212.134.200-10.212.134.210	
SSLVPN_TUNNEL_ADDR1_201_124	Address	any	IP Range:10.212.134.200-10.212.134.210	
SSLVPN_TUNNEL_IPv6_ADDR1	IPv6 Address		IP/Netmask:fdff:ffff::/120	
VPRN_WAN	Address	any	IP/MASK:192.168.71.0/255.255.255.0	
all	Address	any	IP/MASK:0.0.0.0/0.0.0.0	
all	IPv6 Address		IP/Netmask:::/0	
autoupdate.opera.com	Address	any	FQDN:autoupdate.opera.com	
google-play	Address	any	FQDN:play.google.com	
none	Address	any	IP/MASK:0.0.0.0/255.255.255.255	
none	IPv6 Address		IP/Netmask:::/128	
swscan.apple.com	Address	any	FQDN:swscan.apple.com	
update.microsoft.com	Address	any	FQDN:update.microsoft.com	

Service

Name	Category	Type	Details	Comments
AFS3	File Access	Firewall Service	TCP/7000-7009 UDP/7000-7009	
AH	Tunneling	Firewall Service	IP/51	
ALL	General	Firewall Service	IP/0	

Ilustración 17

5.1 Instalación de políticas

Hemos activado en FortiManager el modo **workspace**, de modo que un usuario desde FortiPortal y otro desde FortiManager, no puedan trabajar en un mismo ADOM, en una misma política. Así se evita sobrescribir los cambios de otro usuario.

Es por ello, que, si se hacen los cambios desde FortiManager, tenemos que hacer el bloqueo de la política para poder modificarla.

Para ello, basta con pulsar sobre el botón "Lock" que aparece al lado de nuestro ADOM:

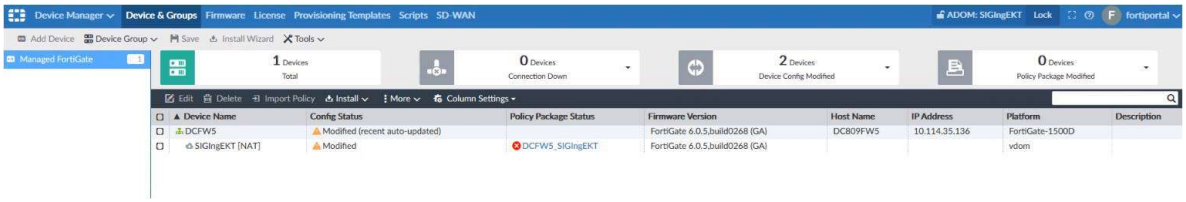


Ilustración 18

Cuando lo pulsemos, cambiará a color verde el icono de candado que aparece al lado del mismo:

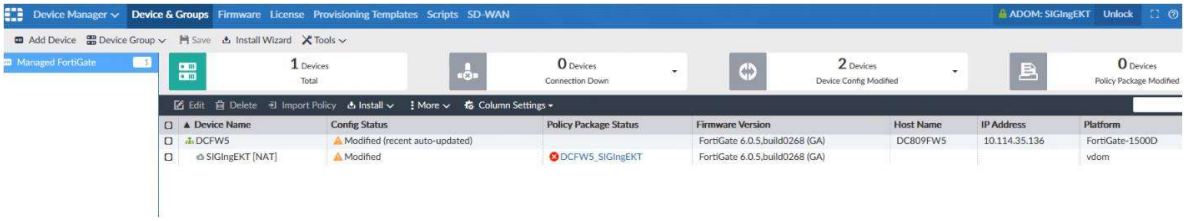


Ilustración 19

Una vez acabados los cambios, deberemos pulsar sobre "Unlock" para liberar la política y que sea modificada por otro usuario.

A veces, puede estar bloqueada por cambios desde el FortiPortal. En tal caso, aparecerá con un candado rojo al lado del nombre del ADOM, y no nos permitirá hacer cambios. Si pulsamos sobre el ADOM, nos muestra el mensaje de quién tiene bloqueada la configuración. En este caso nos indica que es el usuario del FortiPortal:

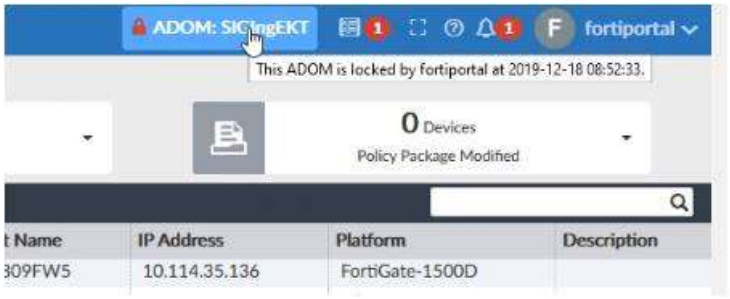


Ilustración 20

Si lanzamos la instalación desde FortiManager, tenemos antes que guardar los cambios, con el botón SAVE que aparece en la pestaña de Policy & Objects. Si no los guardamos, no permite hacer la instalación.

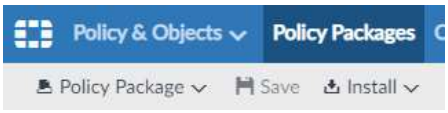


Ilustración 21

Si no está bloqueada por un usuario en el FortiManager, podemos lanzar una instalación, desde FortiPortal.

Para ello, accedemos a la pestaña **Policy,** y luego pulsamos sobre el botón **Instalation**. Aparece el **Installation target** y el estado. Si pulsamos el botón **Install**, se inicia la instalación.

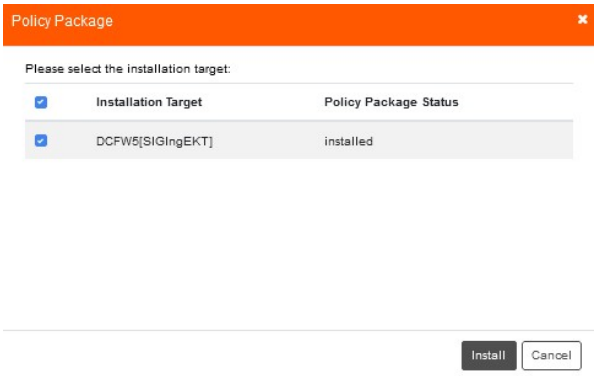


Ilustración 22

Tras pulsarlo, comienza una instalación, y se muestra su avance en una barra:

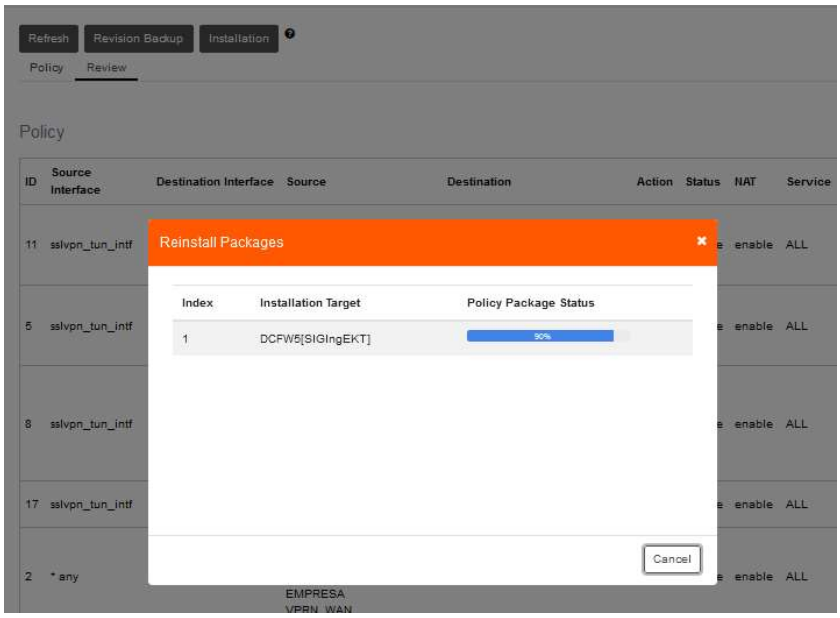


Ilustración 23

Finalmente muestra el resultado satisfactorio:

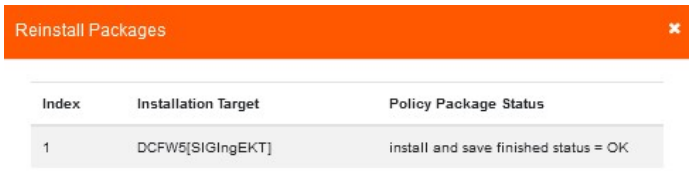


Ilustración 24

Ahora los cambios realizados en la política del portal están realmente instalados en la política de los Firewall Fortigate.

5.2 Regla de acceso

Cada regla se compone de los siguientes elementos, todos ellos editables, al seleccionar la regla con el botón derecho y pulsar "**Edit**":

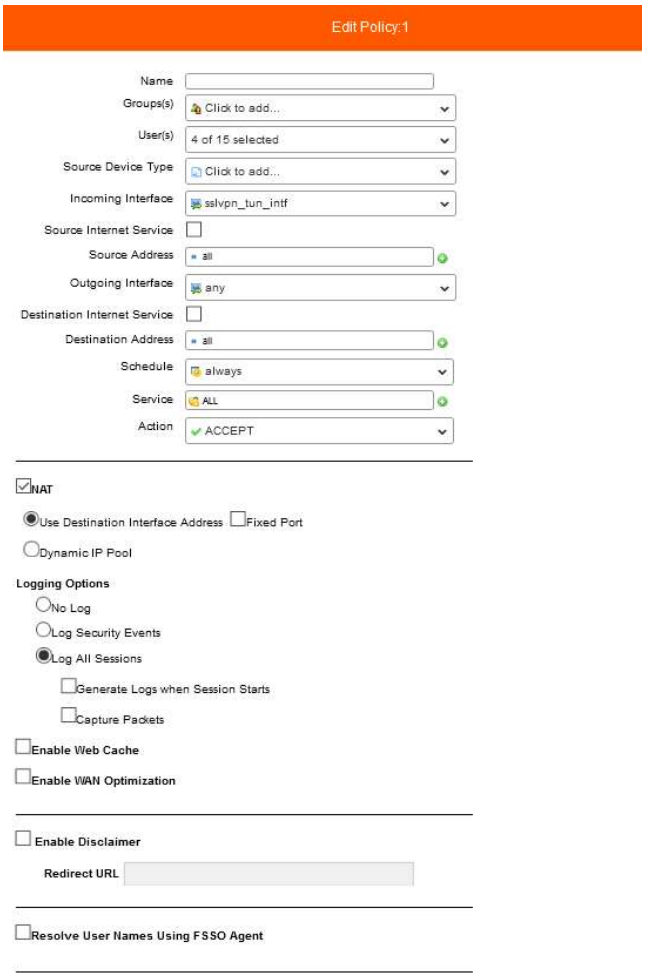


Ilustración 25

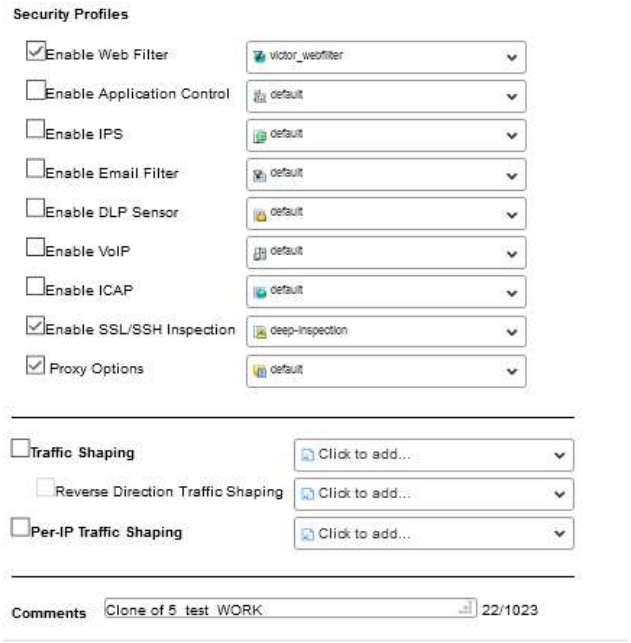


Ilustración 26

1. **Regla de acceso:**

   Define que conexiones son permitidas o no por el firewall:

Ilustración 27

Se componer de:

a. **Group(s) y User(s):** define qué usuarios o grupos de usuarios autenticados pueden acceder al destino definido en la regla, desde los orígenes definidos y por los servicios designados.

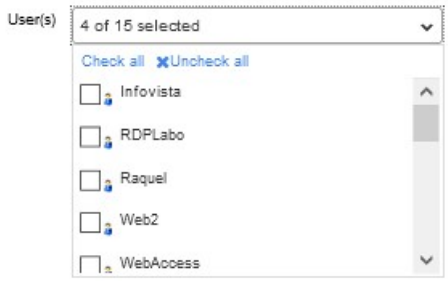


Ilustración 28

b. **Source Device Type:** indica qué tipo de dispositivo es el permitido como dispositivo origen. Se puede elegir uno o varios entre los disponibles:

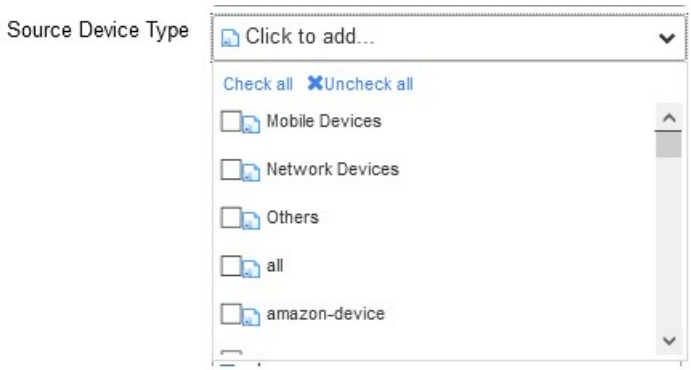


Ilustración 29

c. **Incoming/Outgoing interface:** son los interfaces desde los que tiene que venir la petición de conexión y por donde tiene que salir la petición hacia el destino. Cualquier petición de acceso, que venga por otro interfaz o salga hacia otro interfaz será rechazada, aunque esté aceptada por el resto de la regla (origen/destino/servicio)

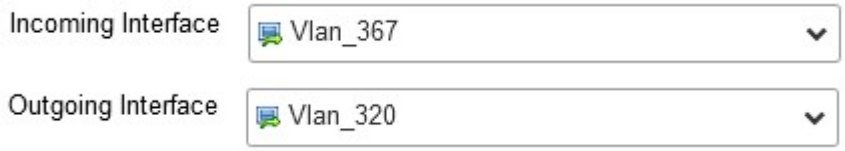


Ilustración 30

d. **Source/Destination Addres:** las direcciones IP de los orígenes válidos y los destinos alcanzables a través de la regla. Se pueden elegir entre los objetos de red previamente definidos.

e. **Service:** protocolo y servicio que usará la conexión para acceder al destino. Se puede elegir entre los servicios anteriormente definidos.

f. **Action:** define qué acción realiza el firewall con la conexión que cumple todas las condiciones anteriores. Las disponibles son:

ACCEPT (acepta la conexión)
DENY (elimina la conexión sin enviar respuesta)

Ilustración 31

Si la acción es **Accept**, aparecerá la opción de NAT, que se ven a continuación.

Si es **Deny**, aparece la opción de guardar los logs de las conexiones que intentan acceder y se rechazan, lo que supone una violación ("**Log violation Traffic**").

2. **NAT:**
Define si se aplica NAT de origen a la conexión que ha sido aceptada por la regla.

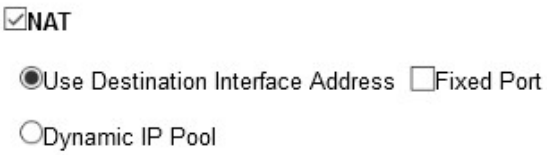


Ilustración 32

Hay dos opciones:

- **Use Destination Interface Access** está habilitado por defecto, y cambia la dirección IP origen por la dirección IP definida en el interfaz de salida de la conexión. Se puede forzar que el puerto de servicio no cambie el puerto origen de la conexión, activando la función "Fixed port"
- **Dynamic IP pool,** aplica el NAT definido en un IP pool específico. Al seleccionarlo aparece un desplegable con todos los ip pool definidos en el equipo, para seleccionar el deseado.

3. Opciones de logging

Un log por cada sesión iniciada bajo una regla en concreto se genera en el firewall y se almacena en la plataforma.

Podemos elegir entre no guardar ese log (**No Log**), guardar sólo los eventos de seguridad (**Log Security Events**) como son los eventos de antivirus, control de aplicaciones, etc., o guardar todos los logs de todas las sesiones (**Log All Sessions**).

En este último caso, podemos además guardar una captura de paquetes de la conexiones que sean aprobadas por esta regla (**Capture Packets**).

Normalmente el log de la sesión se genera cuando la sesión finaliza. Si queremos que se genere al inicio de la conexión, deberemos seleccionar **Generate Logs when Session Starts.**

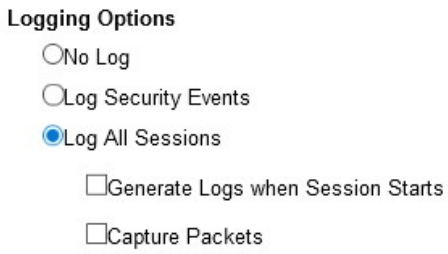


Ilustración 33

4. Caché

En cada regla hay dos opciones de caché para todo el tráfico que es aceptado en dicha regla. Puede aplicarse al tráfico de navegación web (**Enable Web Cache**) o a todo el tráfico (**Enable WAN Optimization**):

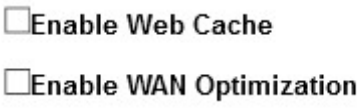


Ilustración 34

La caché habilitada permite almacenar en un buffer las páginas web y ficheros que descargan los usuarios para proveerlo rápidamente a otro usuario que pida el mismo recurso.

No se recomienda habilitar ninguna de estas dos opciones.

5. Disclaimer

Tampoco está permitido habilitar esta opción, ya que no se ha definido una política de **disclaimer** (aviso) cuando se navega a través de esta regla.

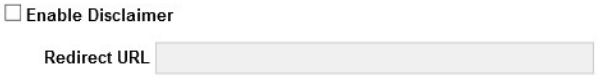


Ilustración 35

6. Resolución de nombre usando FSSO

La autenticación de usuarios mediante FSSO permite conocer el equipo desde el que está conectado, de cara a la autenticación en la regla.
Si este servicio está activo, Grupo Euskaltel procederá a habilitar las reglas con esta opción.
No está permitido que el cliente lo habilite sin consultarlo.

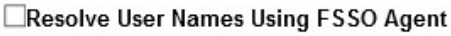


Ilustración 36

7. Securtity profiles

Permite seleccionar los perfiles de seguridad (Antivirus, Web Filter, Control de Aplicaciones, IPS, Email Filter, DLP, VoIP, ICAP, Inspección SSL/SSH y opciones de proxy) que podemos aplicar

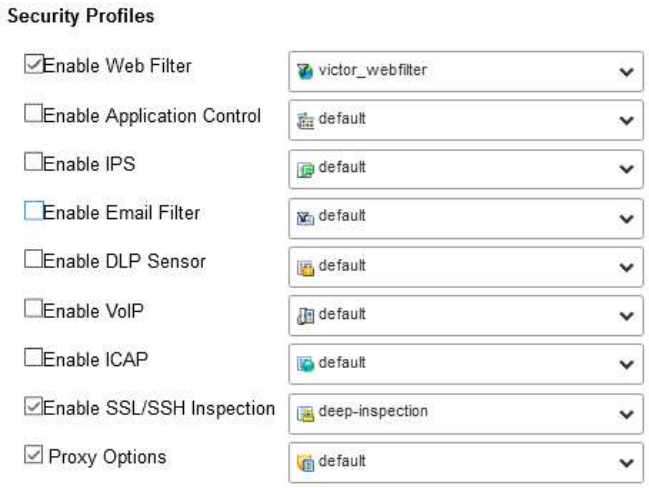


Ilustración 37

Solo serán editables los permisos asignados al perfil del cliente, contratados por el mismo.

Para aquellos perfiles de seguridad permitidos, podremos elegir cual aplica a la regla en cada caso, entre los predefinidos en el firewall.

Dichos perfiles de seguridad podrán ser editados, creados y eliminados por el cliente siempre que estén habilitados según su perfil.

La inspección SSL/SSH y las opciones de proxy no deben modificarse para no afectar al tráfico de la regla. Si se quieren modificar, se debe notificar a Grupo Euskaltel.

8. Conformado de tráfico

Se puede aplicar a las reglas una limitación de tráfico por caudal (Mbps).
Podemos seleccionar entre un perfil de conformado (**Traffic Shaping**) compartido por todas las conexiones permitidas por dicha regla, o un perfil de conformado que aplique sus límites sobre las conexiones provenientes de una misma ip (Per-IP TRaffic Shaping).

Además, en la primera opción (general), podemos aplicar también los límites del conformado al flujo inverso (destino>origen), seleccionando la opción **Reverse Direction Traffic Shaping.**

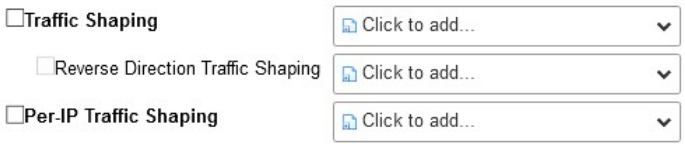


Ilustración 38

9. Comentario

Por último, podemos añadir a la regla un comentario que ayude a identificar su propósito.
No puede superar los 1023 caracteres.

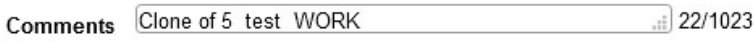


Ilustración 39

Todas estas características son visibles en la política por cada una de las reglas. Podemos elegir cuales se ven en la vista general de la política, pulsando sobre "**Column Settings**" y activando las columnas que necesitemos:

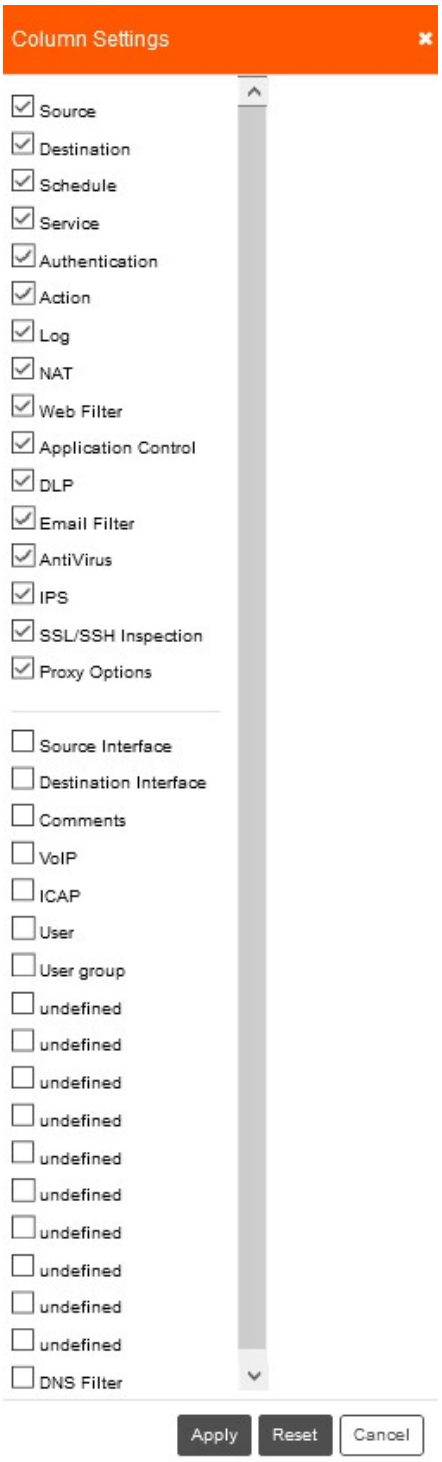


Ilustración 40

6 Objetos Firewall

Este menú recoge todos los objetos que son modificables en la política de seguridad.

Se accede desde la pestaña de **Objetcs** en la vista "**Policy & Objects**"

Allí podemos ver qué tipo de objetos están disponibles para su edición, agrupados en 4 tipos:

Ilustración 41

- **Zone/interface:** hace referencia a los interfaces de red del firewall y las zonas a las que están asociados. Dichas zonas son asociaciones de interfaces
- **Firewall objects:** son los objetos de red y servicios que se aplican en la definición de las reglas de acceso
- **Security & Profiles:** incluye los perfiles de seguridad avanzados y su definición
- **User & Device:** define los usuarios, grupos y tipos de dispositivos que se utilizan para autenticar las conexiones a través de la política de acceso.

6.1 Zone/Interface

Muestra los interfaces definidos en la política y a qué interfaces físicos o lógicos está asociados en el firewall virtual.

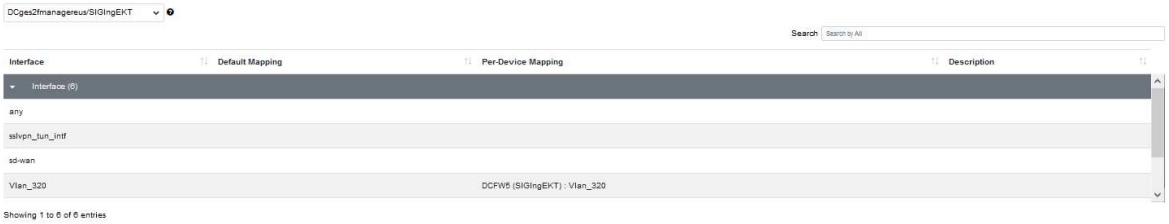


Ilustración 42

6.2 Firewall Objects

Su administración está permitida por los tres perfiles: navegación, avanzado y premium.

Incluye la definición de objetos de los siguientes tipos:

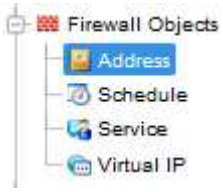
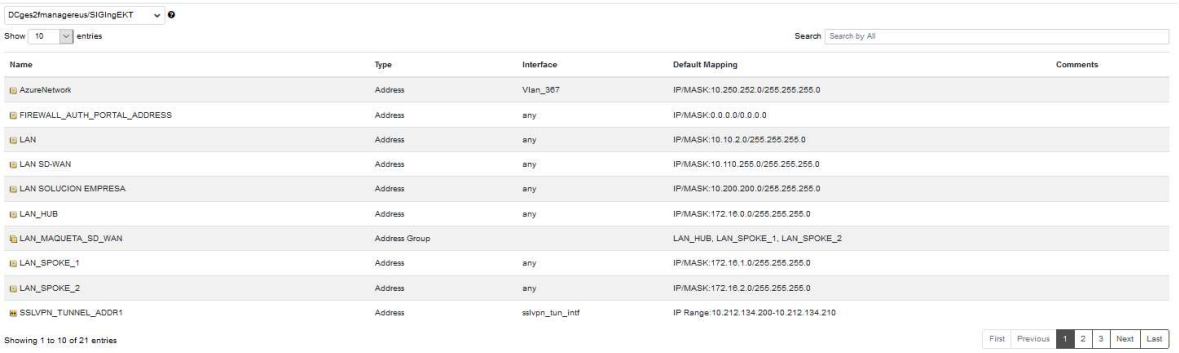


Ilustración 43

A. Address

Cada objeto define una red o host en formato IP, FQDN o un país.



Name	Type	Interface	Default Mapping	Comments
AzureNetwork	Address	Vlan_367	IP/MASK:10.250.252.0/255.255.255.0	
FIREWALL_AUTH_PORTAL_ADDRESS	Address	any	IP/MASK:0.0.0.0/0.0.0.0	
LAN	Address	any	IP/MASK:10.10.2.0/255.255.255.0	
LAN SD-WAN	Address	any	IP/MASK:10.110.255.0/255.255.255.0	
LAN SOLUCION EMPRESA	Address	any	IP/MASK:10.200.200.0/255.255.255.0	
LAN_HUB	Address	any	IP/MASK:172.16.0.0/255.255.255.0	
LAN_MAQUETA_SD_WAN	Address Group		LAN_HUB, LAN_SPOKE_1, LAN_SPOKE_2	
LAN_SPOKE_1	Address	any	IP/MASK:172.16.1.0/255.255.255.0	
LAN_SPOKE_2	Address	any	IP/MASK:172.16.2.0/255.255.255.0	
SSLVPN_TUNNEL_ADDR1	Address	sslvpn_tun_intf	IP Range:10.212.134.200-10.212.134.210	

Ilustración 44

Puede ir asociada a un interfaz o a ninguno en concreto (any):

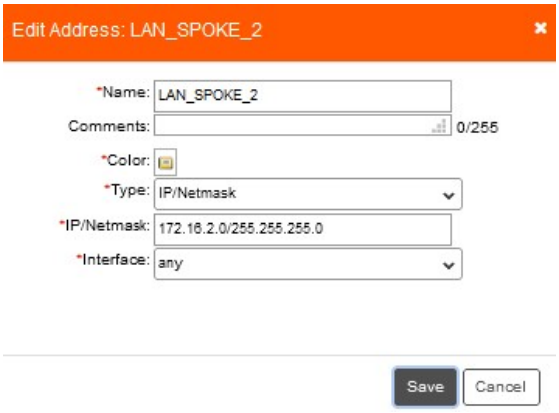


Ilustración 45

Debemos definir el nombre, y la IP y máscara de red, como podemos ver arriba.

Para los grupos, basta con definir el nombre, el color del objeto y los miembros:

Ilustración 46

B. Schedule

Es el periodo de tiempo en el que una regla está activa.
Puede ser recurrente o aplicado a una única ventana de tiempo.
Si es recurrente, podemos estipular la hora de comienzo y final, y los días de la semana en los que está activo:

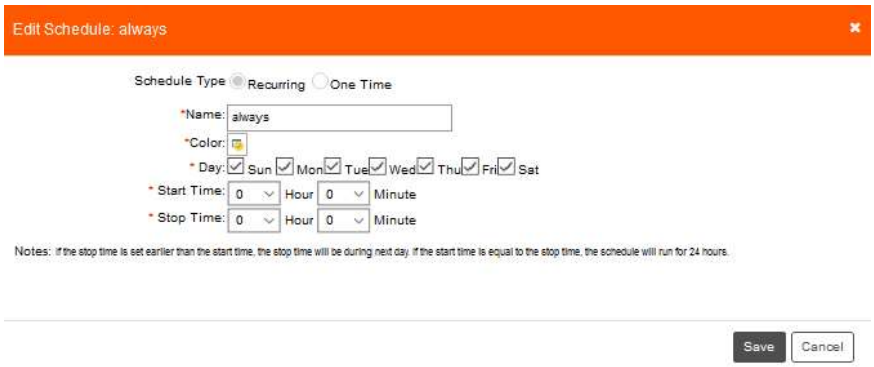


Ilustración 47

C. Service

Son los servicios IP (TCP/UDP/ICMP etc) asociados a un puerto de destino:

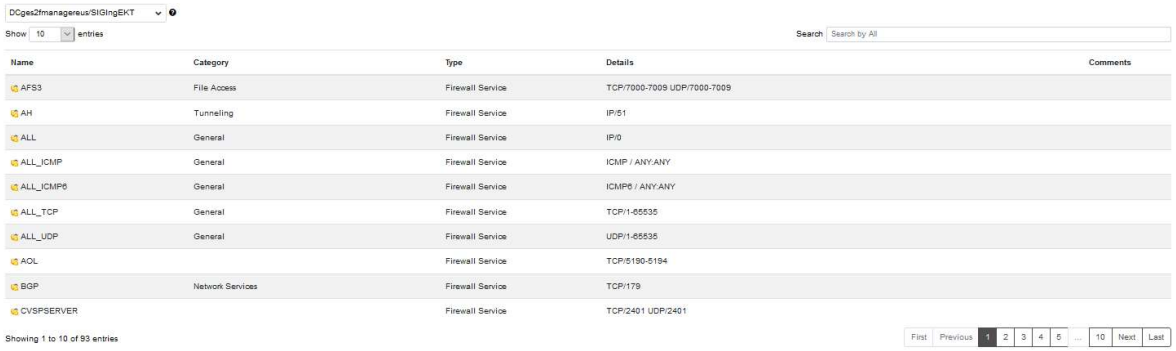


Ilustración 48

Para definirlo debemos seleccionar un nombre, el tipo de protocolo (normalmente TCP/UDP/SCTP) y los puertos de origen y destino.
Se pueden añadir varias combinaciones de puertos, para un mismo servicio, mediante el botón **Add** que aparece en la definición del servicio.

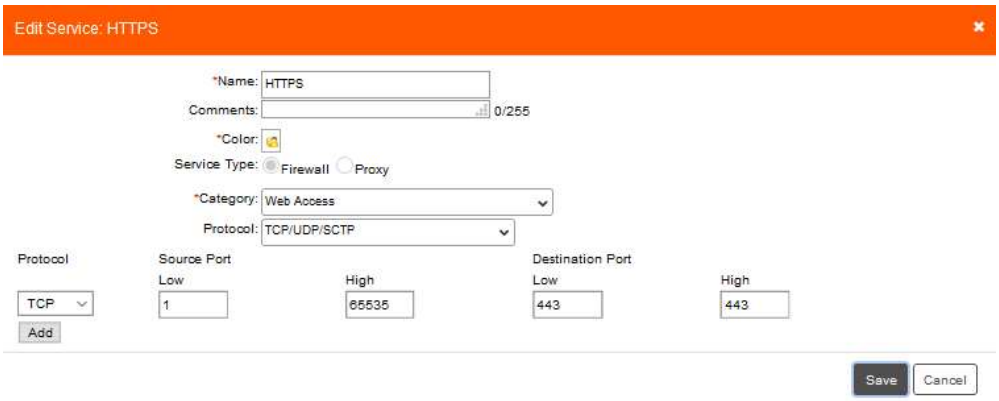


Ilustración 49

D. Virtual IP

Recoge la lista de NATs disponibles para aplicar en la política.

Ilustración 50

Pueden ser de tres tipos:

- **Virtual IP** es un NAT de entrada que cambia la IP destino pública por una privada. Sirve para natear las conexiones destinadas a un servidor publicado en Internet.

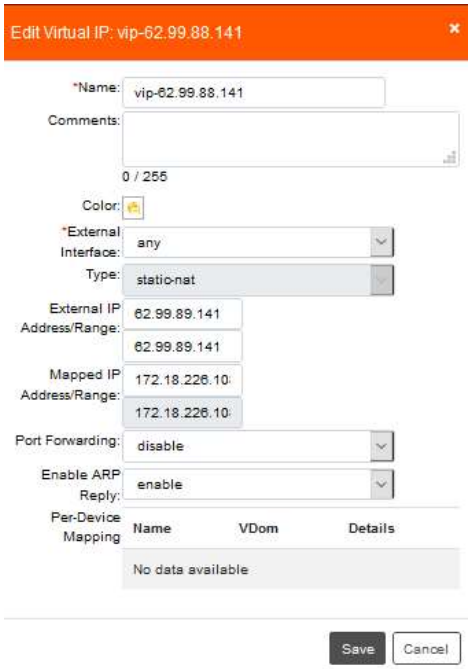


Ilustración 51

- **Virtual IP Group** es un conjunto de Virtual IP aplicables a una regla, que se asocian para una mejor operabilidad.

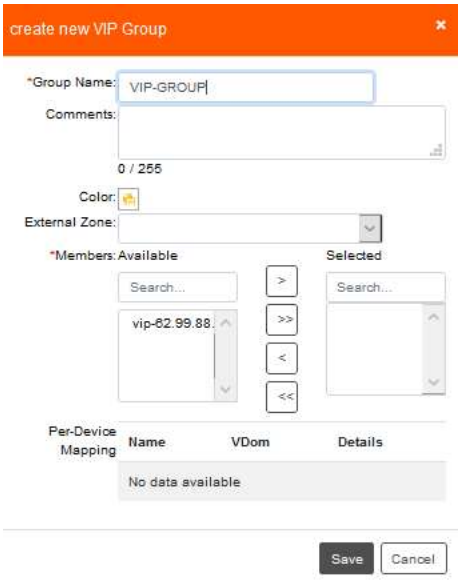


Ilustración 52

En la nueva versión, se pueden añadir diferentes mapeados o asignaciones de VIP según el FW en el que se apliquen (Per-Device Mapping)

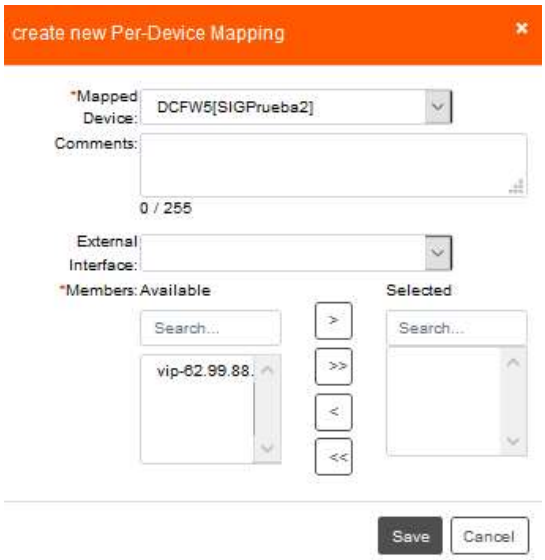


Ilustración 53

- **IP pool** es un NAT de salida, para dar acceso a las redes internas a la red pública.

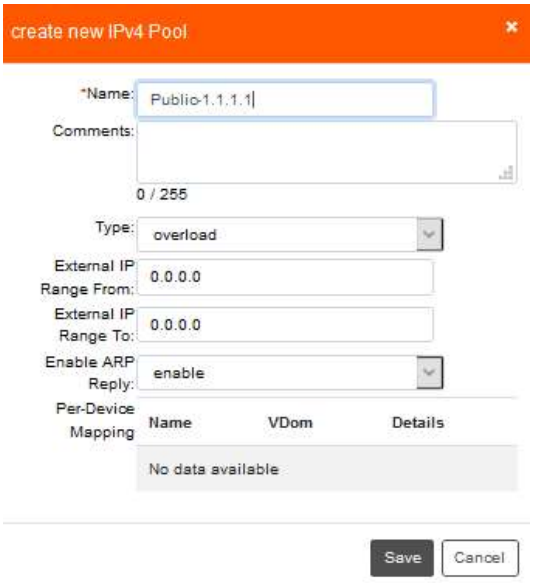


Ilustración 54

Se debe asignar la dirección IP pública a la que se natea. Así como el tipo:

- **Overload.** Asigna dinámicamente las conexiones a puertos origen traducidos (PAT), de modo que con una IP púnlica se puedan atender 60416 conexiones.
- **One-to-one.** Es un NAT estático que asocia una IP privada con una pública y no mediante la asignación de puertos concretos, como en el caso de overload.
- **Fixed-port-range.** Define un grupo de puertos asignados a cada una de las ips origen privadas que utilicen el NAT. Es un caso particular del overload.
- **Port block allocation.** Permite seleccionar el tamaño de bloques de puertos utilizados en PAT y el número de bloques por IP origen. Es como el caso anterior, pero aquí podemos definir el tamaño de los rangos.

Por defecto siempre se utilizará la opción Overload.

Se permite también en esta versión el mapeado por FW.

La opción de **ARP Reply** permite que se envíen respuestas ARP cuando se recibe una petición para una IP contenida en el pool. Se debe dejar marcada por defecto.

6.3 Security Profiles

Como hemos comentado anteriormente, los perfiles de seguridad no están accesibles para todos los clientes. Es por ello por lo que indicaremos en cada funcionalidad qué perfiles tienen acceso para gestionar la misma.

Ilustración 55

6.3.1 Antivirus

Está habilitado para los perfiles de **Navegación y Premium.**

Ilustración 56

Podemos modificar los perfiles de Antivirus, editando los siguientes parámetros:

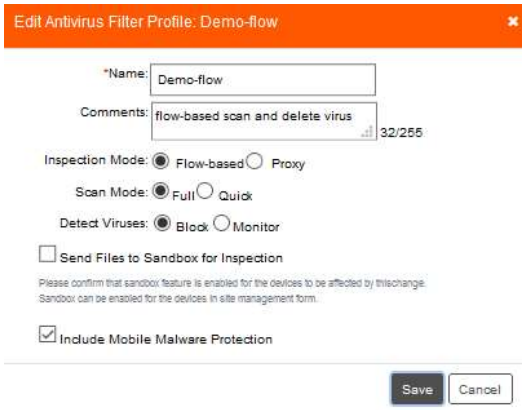


Ilustración 57

- **Inspection Mode:** Es el modo de inspeccionar el flujo de comunicación de una conexión. El modo Flow-based analiza el tráfico de modo fluido en pequeñas porciones de este, comparando con firmas de virus conocidos. El modo proxy hace uso de un buffer de memoria para almacenar temporalmente los archivos que se descargan o envían y cuando lo tiene completo, procede al análisis.
  El modo recomendado es Flow-based, porque evita que el usuario final experimente retrasos en la descarga y la potencia de escaneo es suficiente.
- **Scan Mode:** Permite elegir entre un modo rápido (**Quick**) de escaneo de archivos en búsqueda de virus, o un modo más exhaustivo (**Full**)
- **Detect Viruses:** Indica la acción a realizar con la conexión en la que se ha encontrado un virus: bloquear dicha conexión (**Block**) o dejarla pasar y solo generar un log de evento virus (**Monitor**)

- **Send Files to Sandbox for Inspection:** Permite el envío de los ficheros analizados a una segunda inspección en un sandbox o ATP que analice las acciones que genera el archivo al ser ejecutado en un pc, y poder catalogarlo como virus si el comportamiento es extraño.
- **Include Mobile Malware Protection:** Habilita la base de datos de virus que afectan a equipos móviles.

6.3.2 Control de Aplicaciones

Está habilitado para los perfiles **Avanzado, Navegación y Premium.**

Permite controlar qué aplicaciones son las que funcionan a través de un flujo habilitado en una regla.

Ilustración 58

A dicha regla se le aplicará un sensor de aplicaciones (**Application Sensor**), que no es más que una secuencia de reglas de bloqueo o Monitorización, de aplicaciones agrupadas por los siguientes campos:

- **Category:** habilita las categorías predefinidas, según la finalidad de la aplicación (tráfico P2P, Mensajería instantánea, etc).
- **Vendor:** se aplicarán todas las aplicaciones creadas por este fabricante.
- **Risk:** agrupadas por su potencial peligrosidad
- **Technology:** agrupa por el SO donde se ejecuta la aplicación
- **Popularity:** en diferentes grupos según su uso popular
- **Application:** por la aplicación en concreto.

Para las categorías, podemos elegir entre las siguientes:

- **Botnet**
- **Business**
- **Cloud.IT**
- **Collaboration**
- **Email**

- **Game**
- **General.Interest**
- **Mobile**
- **Network.Service**
- **P2P**
- **Proxy**
- **Remote.Access**
- **Social.Media**
- **Storage.Backup**
- **Update**
- **Video/Audio**
- **VoIP**
- **Web.Clients**
- **Unknown Applications**

Una vez que hemos seleccionado las aplicaciones mediante los filtros, procedemos a elegir la acción que aplicará a la conexión en la que se ha detectado una aplicación:

- **Allow** permite el paso
- **Monitor** permite el paso, pero genera un evento de seguridad que queda resistrado
- **Block** no permite el paso y la conexión no se establece

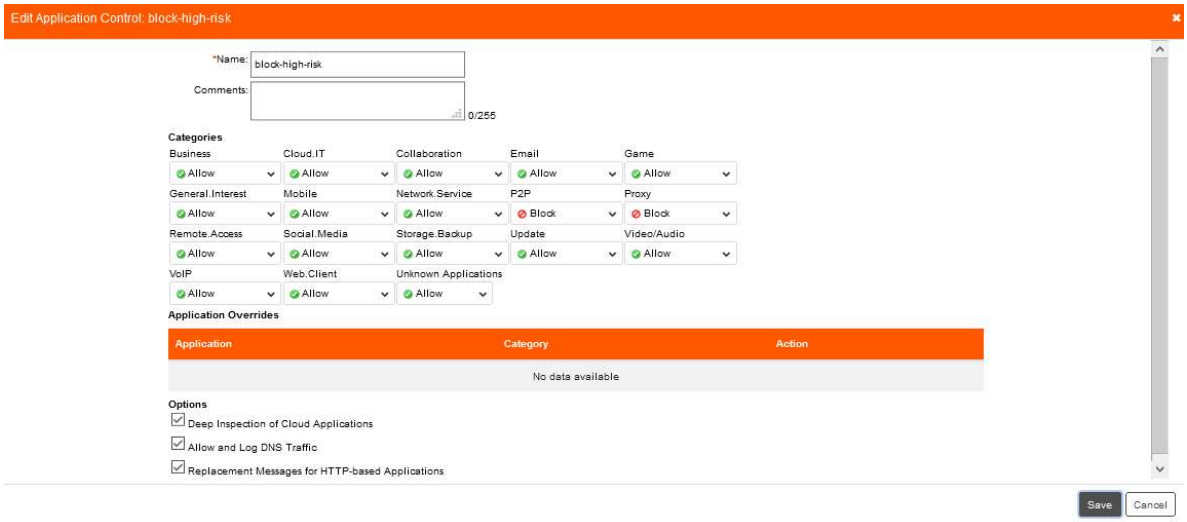


Ilustración 59

6.3.3 Data Leak Prevention

No es un servicio habilitado para ninguno de los perfiles de cliente.

6.3.4 Email Filter

No es un servicio habilitado para ninguno de los perfiles de cliente.

6.3.5 IPS

Está habilitado para los clientes con perfil **Premium**.

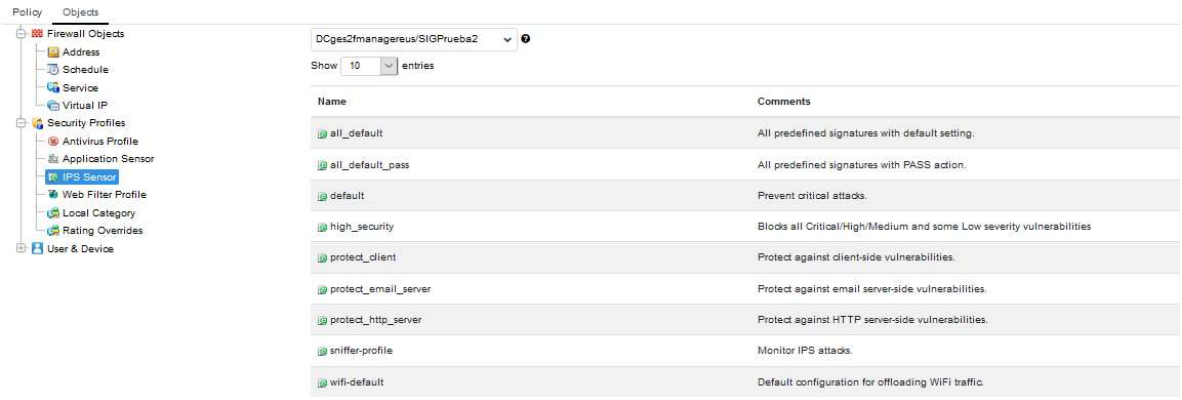


Ilustración 60

De un modo parecido al control de aplicaciones, podemos agrupar las protecciones IPS sobre perfiles, utilizando filtros para seleccionar sólo las protecciones necesarias y requeridas.

Un perfil con muchas protecciones aplicadas no es efectivo, porque tiene que analizar todas ellas sobre un mismo flujo, y ralentiza la conexión.

Es por ello por lo que es importante aplicar sólo las protecciones adecuadas para cada flujo.

Por ejemplo, para una regla que protege el acceso a un servidor web, aplicaremos el perfil **protect_http_server** que excluye protecciones para otros tipos de servidores, como SQL servers, por ejemplo.

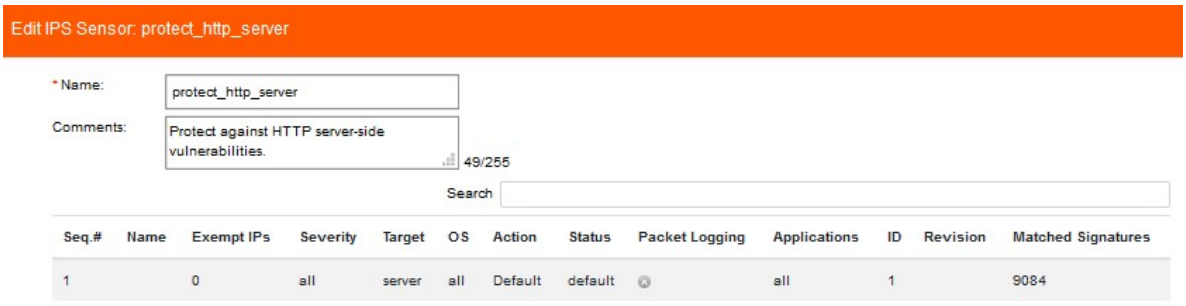


Ilustración 61

Cada regla de IPS sensor puede filtrar las protecciones por:

- **Severity:** según las consecuencias del ataque hasta la caída del servicio.
- **Target:** divide entre las intrusiones con objetivo un servidor concreto o pc de usuarios (client)
- **OS:** asocia las protecciones para equipos que comparten sistema operativo (Windows, Linux, etc).

Una vez seleccionadas las protecciones, debemos indicar la acción a aplicar sobre la conexión sospechosa:

- **block** rechaza la conexión
- **pass,** la permite
- **reject** reinicia la conexión. El atacante recibe ese **reset** y puede saber que se le ha detectado.
- **default** aplica la acción por defecto definida para cada protección, que puede ser bloquear o permitir.

6.3.6 Web Filter

Está habilitado para los clientes con perfil de navegación y perfil premium.

Permite crear filtros sobre URLs no permitidas.

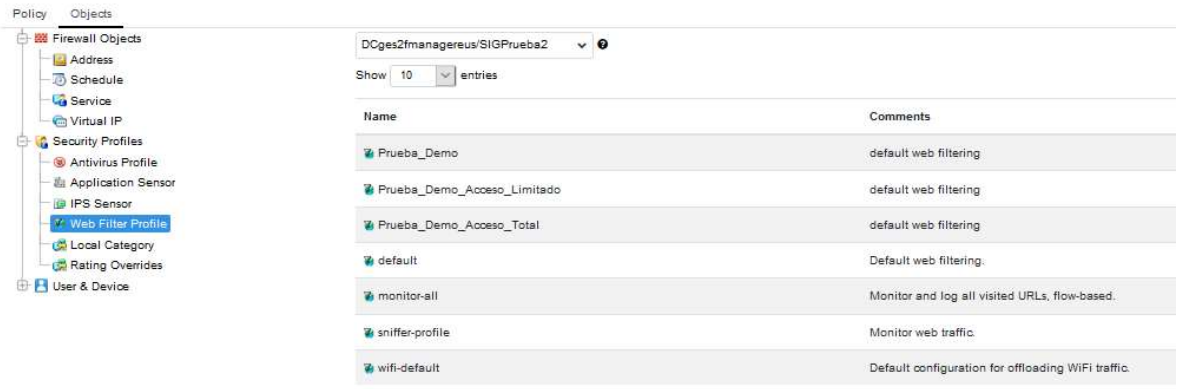


Ilustración 62

Se aplica mediante categorías y subcategorías. Cada URL es categorizada en una de ellas, y a las conexiones contra esa URL se le aplica la acción definida en su categoría:

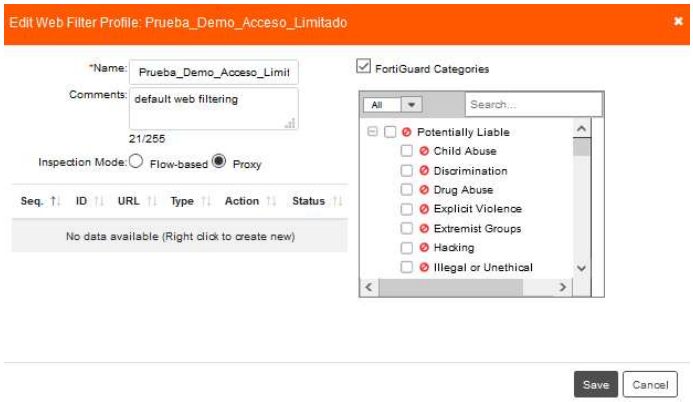


Ilustración 63

Hay dos categorías especiales que debemos tener en cuenta:

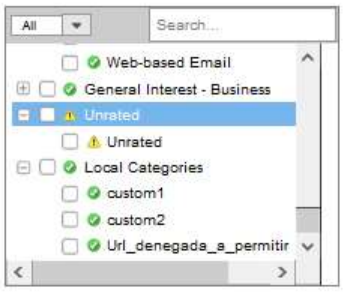


Ilustración 64

La primera es **Unrated** (No categorizadas). Aquí se incluyen todas las URLs que no pertenecen a ninguna categoría. Podemos elegir entre dejar pasar la conexión o bloquearla.

La categorización se hace mediante base de datos de Fortinet, donde hay millones de URLs asignadas a las categorías predefinidas.

La segunda categoría especial es **Local Category.** Se trata de una categoría personalizada donde podemos incluir las URLs que necesitemos para aplicar una acción específica.

Pueden ser tantas categorías locales como necesitemos. Se crean en el menú **Local Category:**

Ilustración 65

Se modificarán en Rating Override.

Rating Override

Para añadir URLs a la categoría local, o a cualquier otra categoría, se habilita la funcionalidad **Rating Override.** Para ello basta con indicar la URL y la categoría a la que la queremos añadir.

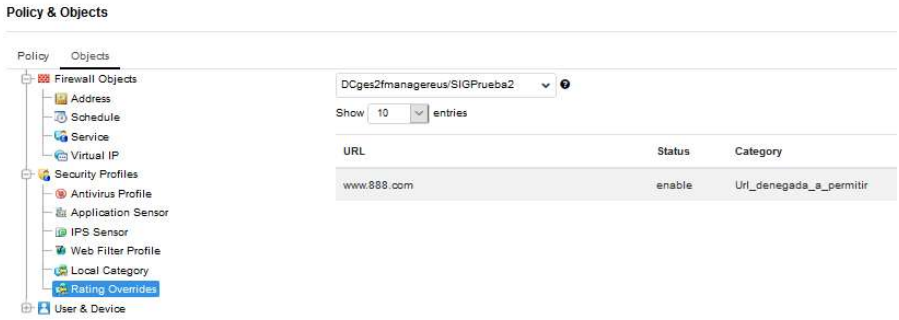


Ilustración 66

Si la URL estaba incluida en otra categoría, dejará de estar en ella, para incluirse en la nueva. Si no estaba categorizada (unrated), se incluirá en la nueva categoría.

6.4 User & Device

Aquí podremos habilitar los usuarios locales o remotos (LDAP, RADIUS, TACACS+)

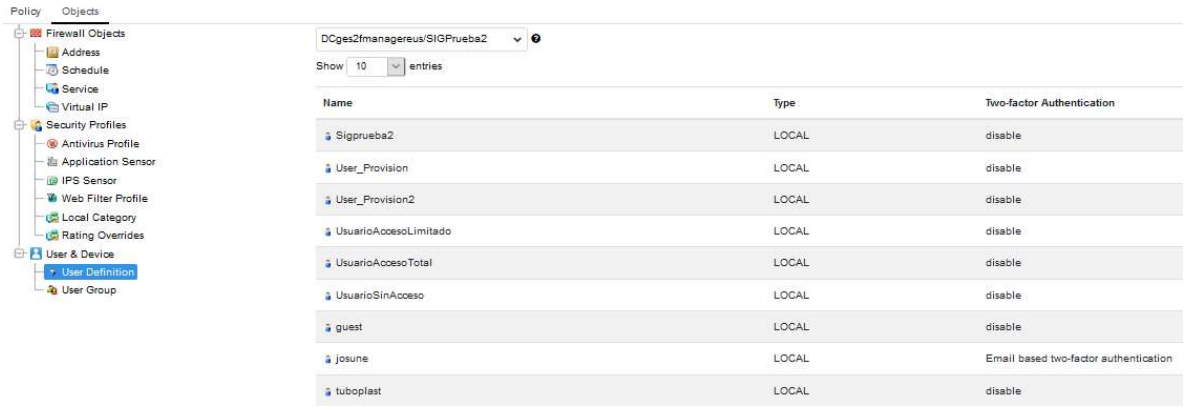


Ilustración 67

Si es un usuario remoto, deberemos especificar el servidor de autenticación que esté previamente definido (en FMG o en los propios FGT).

No está permitido crear nuevos servidores remotos desde el Portal.

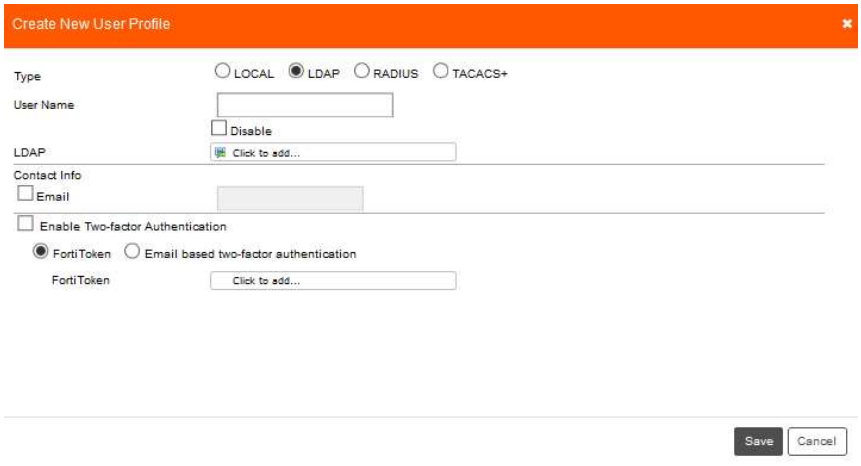


Ilustración 68

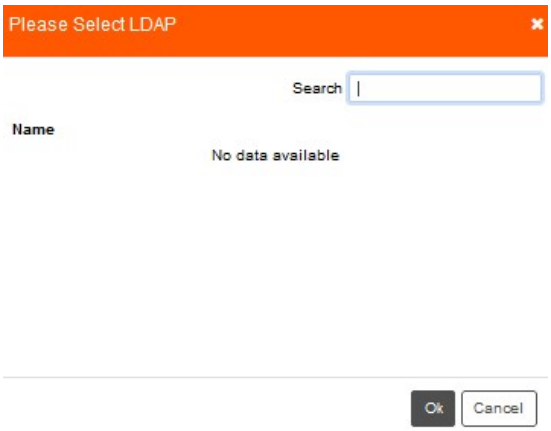


Ilustración 69

Si el usuario no está en uso, podemos marcarlo como deshabilitado (**Disable**).

Por ahora **no está implementado** un segundo factor de autenticación para los usuarios, por lo que esta funcionalidad debe dejarse sin habilitar.

7 View

Permite investigar los eventos de seguridad y logs de tráfico generados por las conexiones manejadas por el firewall.

Podemos aplicar varios filtros para obtener sólo los eventos deseados:

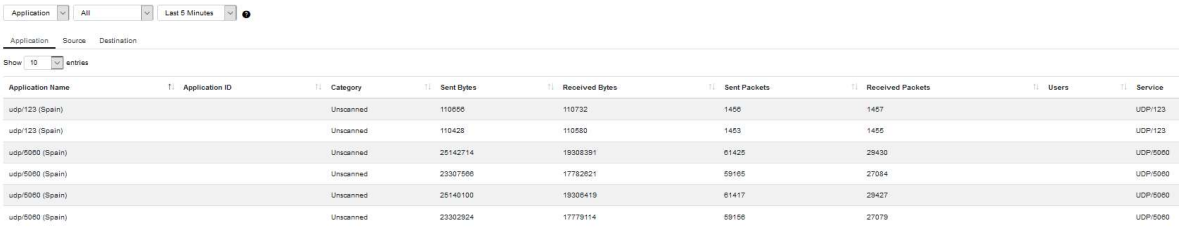


Ilustración 70

El principal filtro es la diferencia entre eventos agrupados por **Application** (Aplicación), **Attack** (Ataque, IPS) y **Sandbox** (ATP).

También permite seleccionar desde más de un firewall virtual (no aplica en nuestro caso, porque solo hay uno) y el periodo de tiempo donde se han dado los eventos (última hora, día, semana, o algo más específico):

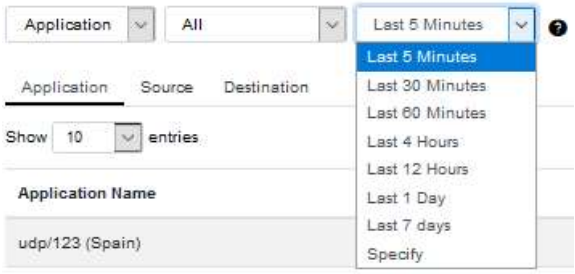


Ilustración 71

Tras seleccionar el filtro de información, podemos seleccionar cómo ordenar los eventos, seleccionando una de las pestañas que aparecen justo debajo:

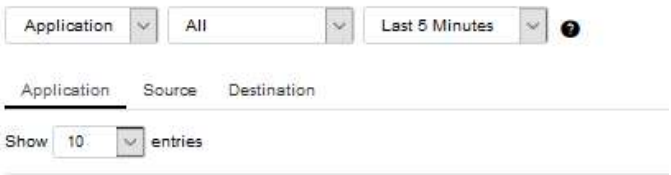


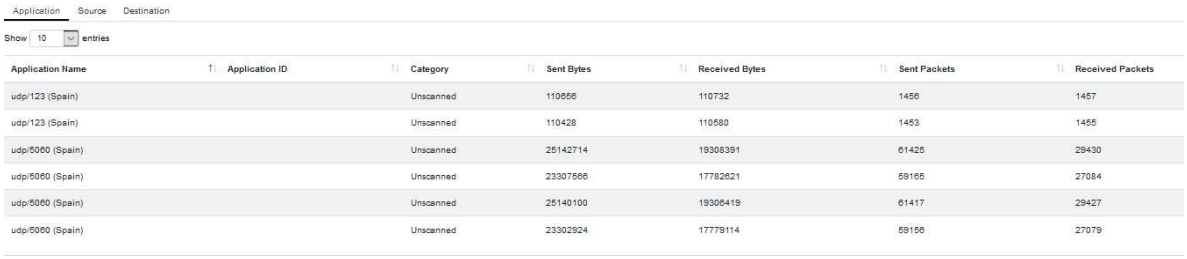
Ilustración 72

En el caso de aplicación, podemos ordenar los eventos por la aplicación concreta, por origen o por destino. La información aparecerá ordenada justo debajo.

Vemos a continuación la información que presenta cada tipo de evento:

7.1 Application View

Muestra los eventos que han activado el control de aplicaciones, ordenados por aplicación:


Application Source Destination

Show 10 entries

Application Name	Application ID	Category	Sent Bytes	Received Bytes	Sent Packets	Received Packets
udp/123 (Spain)		Unscanned	110656	110732	1456	1457
udp/123 (Spain)		Unscanned	110428	110580	1453	1455
udp/5060 (Spain)		Unscanned	25142714	19308391	61425	29430
udp/5060 (Spain)		Unscanned	23307566	17782621	59165	27084
udp/5060 (Spain)		Unscanned	25140100	19306419	61417	29427
udp/5060 (Spain)		Unscanned	23302924	17779114	59156	27079

Ilustración 73

Para cada entrada podemos ver el ID de aplicación, la categoría, los detalles de paquetes enviados y recibidos y el servicio que usó la conexión:

Category	Sent Bytes	Received Bytes	Sent Packets	Received Packets	Users	Service
Unscanned	110656	110732	1456	1457		UDP/123
Unscanned	110428	110580	1453	1455		UDP/123
Unscanned	25142714	19308391	61425	29430		UDP/5060
Unscanned	23307566	17782621	59165	27084		UDP/5060
Unscanned	25140100	19306419	61417	29427		UDP/5060
Unscanned	23302924	17779114	59156	27079		UDP/5060

Ilustración 74

Si pulsamos sobre cualquier fila, se aplica un filtro sobre las sesiones mostradas, según pulsemos sobre origen, destino o aplicación.

Ese filtro coincide con el seleccionado arriba entre **Application, Source y Destination.**

Por ejemplo, para aplicación, se ordena filtra por la aplicación (o servicio) seleccionada, y podemos ordenar por el resto de variables: origen y destino, pulsando las pestañas laterales debajo del filtro:

Ilustración 75

Para filtrar por origen o destino, pulsamos sobre el origen o destino de una sesión:

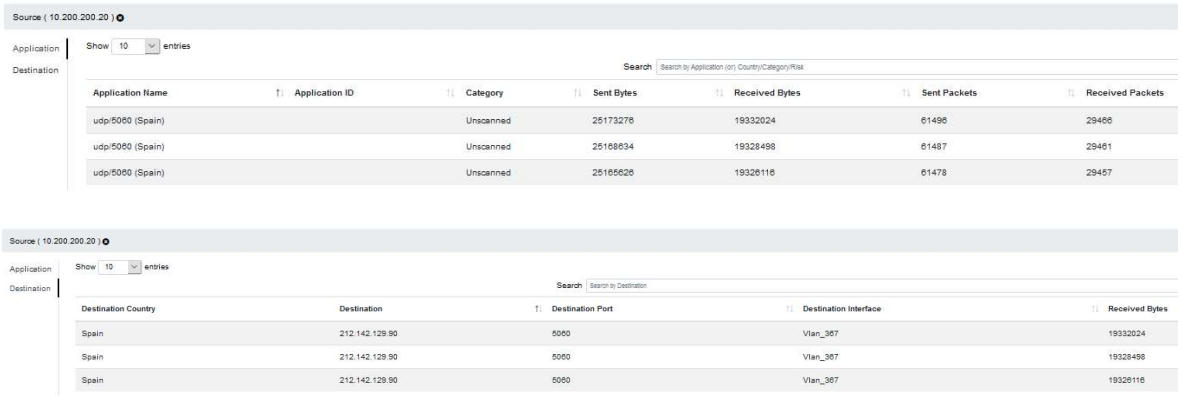


Ilustración 76

Para quitar el filtro, basta con pulsar el aspa que aparece al lado del filtro en la barra sombreada:

Si aplicamos el filtro de origen y destino, aparecerán listadas las sesiones por tiempo, y podremos ampliar la información mediante el botón desplegar (en amarillo):

Ilustración 77

Aquí podemos ver mucha más información detallada sobre tiempo, duración, NAT, etc.

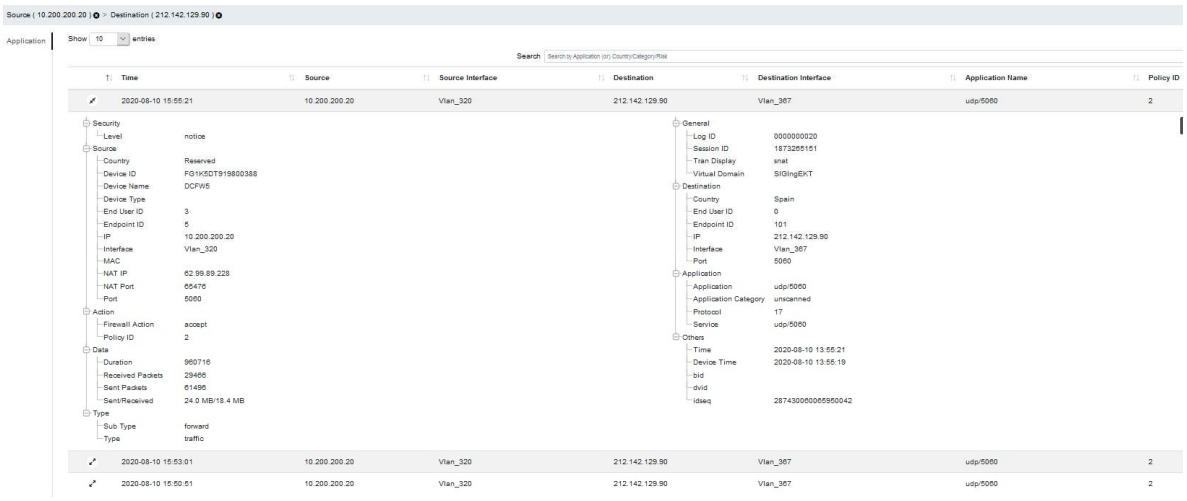


Ilustración 78

7.2 Attack

De manera similar a la vista de aplicaciones, podemos ver la vista de ataques, con los filtros que queramos aplicar:

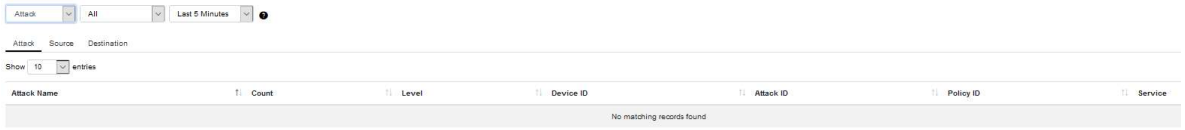


Ilustración 79

Podemos ver el ataque, el nivel de criticidad de este, cuántas veces se ha producido, la IP del atacante y la política que lo reporta.

Se ordenan de nuevo por **tipo de ataque, origen y destino**:

Ilustración 80

7.3 Sandbox

Por último, podemos ver los eventos de sandboxing.

Podemos aplicar los mismos filtros temporales y ordenación por **evento, origen o destino**:

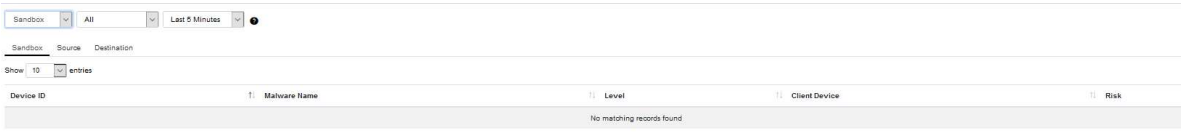
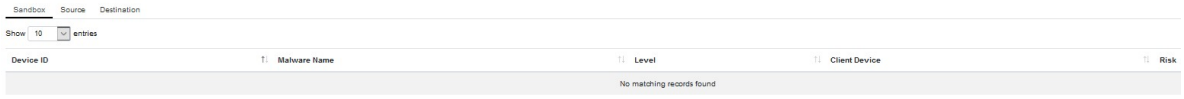


Ilustración 81

De cada evento, se muestra el Malware encontrado, la IP del cliente infectado y el riesgo asociado:



8 Reports

El enlace **Reports** del menú principal proporciona el acceso a los reportes generados en FortiAnalyzer, que pueden ser descargados por desde el enlace proporcionado (el icono de flecha bajo la columna Action):

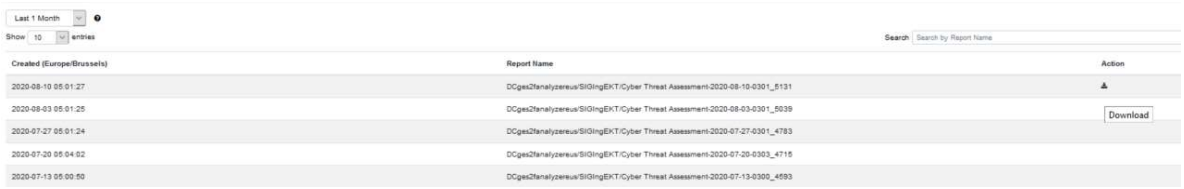


Ilustración 82

Podemos filtrar por tiempo, de modo que solo se muestren los reportes generados dentro de la ventana elegida (hoy, ayer, la última semana, el último mes o una ventana específica):

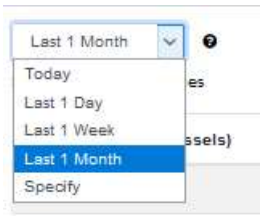


Ilustración 83

El reporte se puede descargar en formato PDF.

Ilustración 84

9 Audit

Muestra la actividad de los usuarios administradores de la política y los cambios que han aplicado sobre la misma, como pueden ser instalaciones, cambios en objetos, etc.

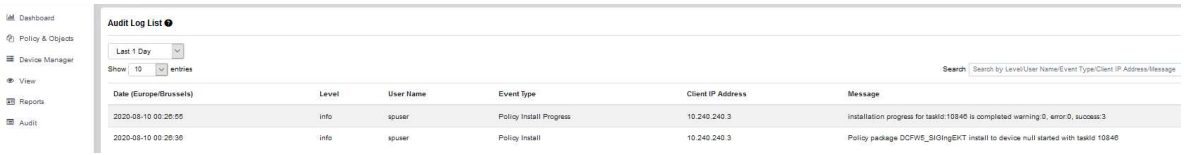


Ilustración 85

Dispone de una ventana de diálogo para realizar búsquedas por tipo de evento, usuario administrador, IP desde la que se ha conectado un administrador, el mensaje del evento, etc.

Ilustración 86

Así como un filtro temporal, con las opciones que ya hemos visto (última hora, último día, semana o ventana temporal concreta)

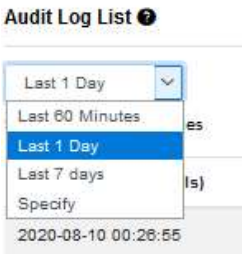


Ilustración 87

10 Recursos adicionales

Aquí se muestran accesos o enlaces web a recursos relacionados con el servicio, como las peticiones de cambios, de nuevos reportes, etc.

Por el momento no se ha implementado ningún enlace.

11 Wifi

Toda la administración de **APs (access points)**, **perfiles de administración WiFi y SSIDs**, se pueden revisar en esta pestaña.

Solo es accesible para los clientes que **han contratado el servicio WiFi** en FortiPortal, que se puede añadir a su perfil de cliente (Avanzado, Navegación o Premium).

11.1 Managed AP

Muestra los **APs** conectados al firewall, el SSID que utiliza y los canales y perfiles que utiliza cada uno de ellos.

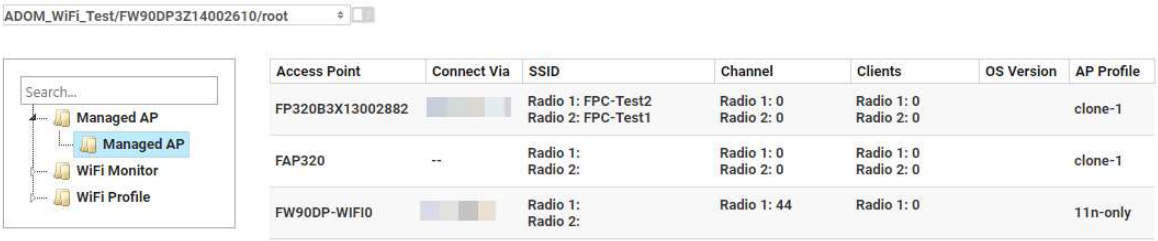


Ilustración 88

Cada uno de los AP puede ser editado (pulsando sobre el mismo, con el botón derecho y seleccionando editar). Cuando estén realizados los cambios, basta con pulsar sobre el botón "**Save**" para guardarlos.

También con el botón derecho sobre un AP, nos da la opción de borrarlo.

11.2 WiFi Monitor

Permite monitorizar el servicio Wifi, mediante los tres menús que mostramos a continuación:

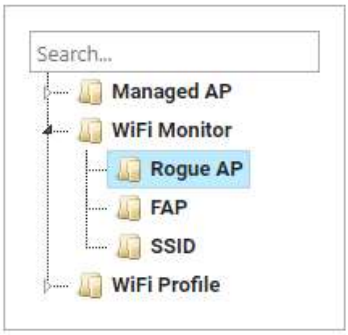
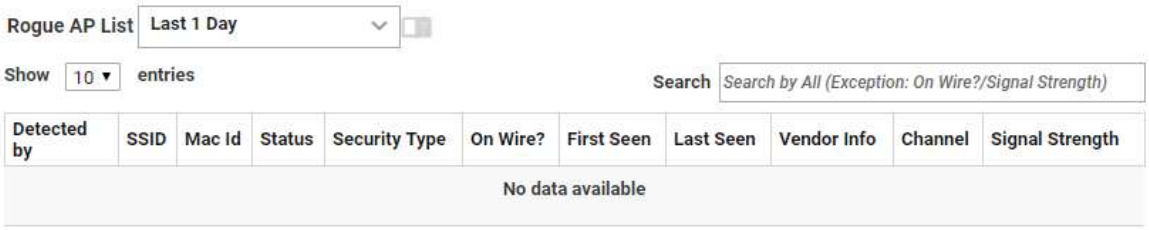


Ilustración 89

Rogue AP

Muestra la lista de eventos de AP no autorizados que intentan acceder al servicio WiFi. Se puede filtrar por tiempo o hacer una búsqueda por tipo u otra característica:



FAP

Muestra el listado de FortiAPs registrados en el firewall virtual:

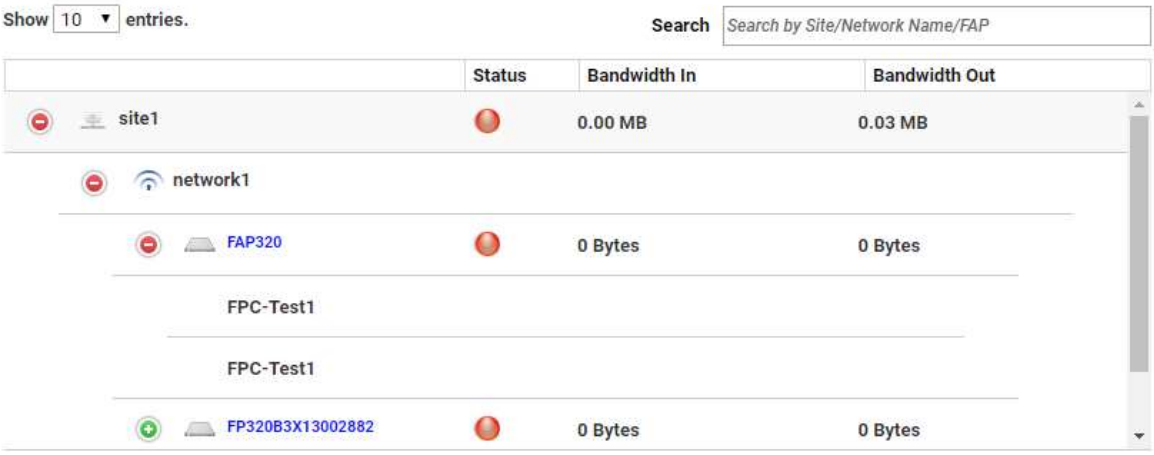


Ilustración 90

Podemos ampliar información sobre cada equipo FAP, pulsando sobre el icono de cruz verde (más):

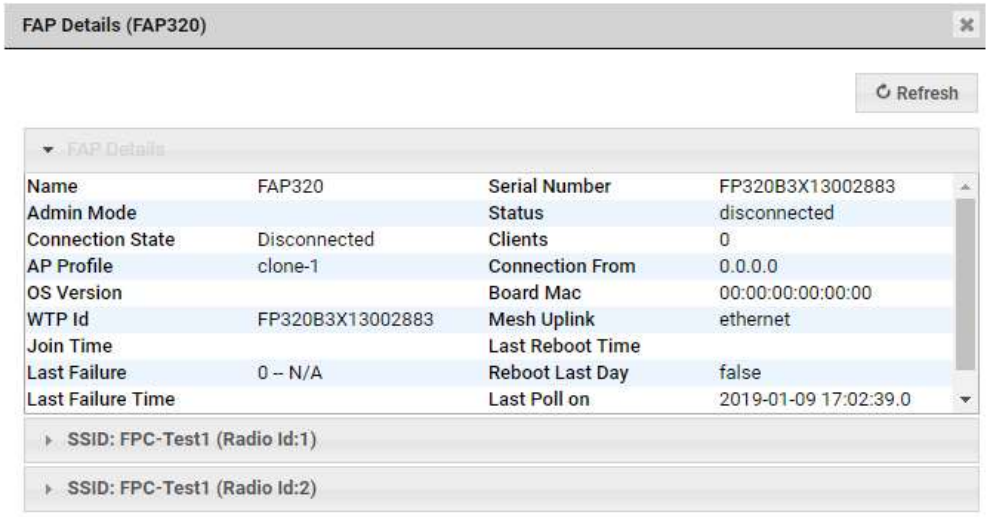


Ilustración 91

SSID

Muestra los APs ordenados por SSID

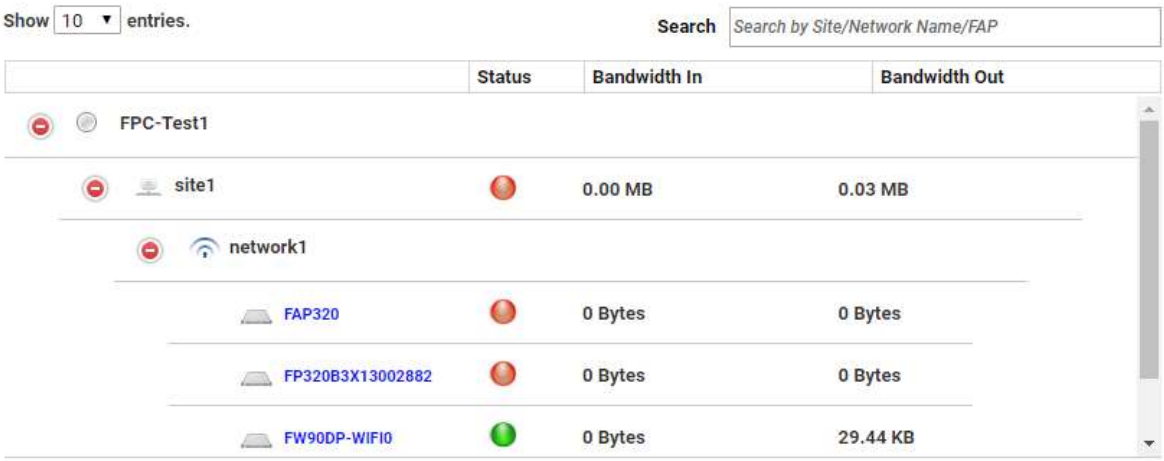


Ilustración 92

Si pulsamos sobre un nombre de FAP, la información se amplía:

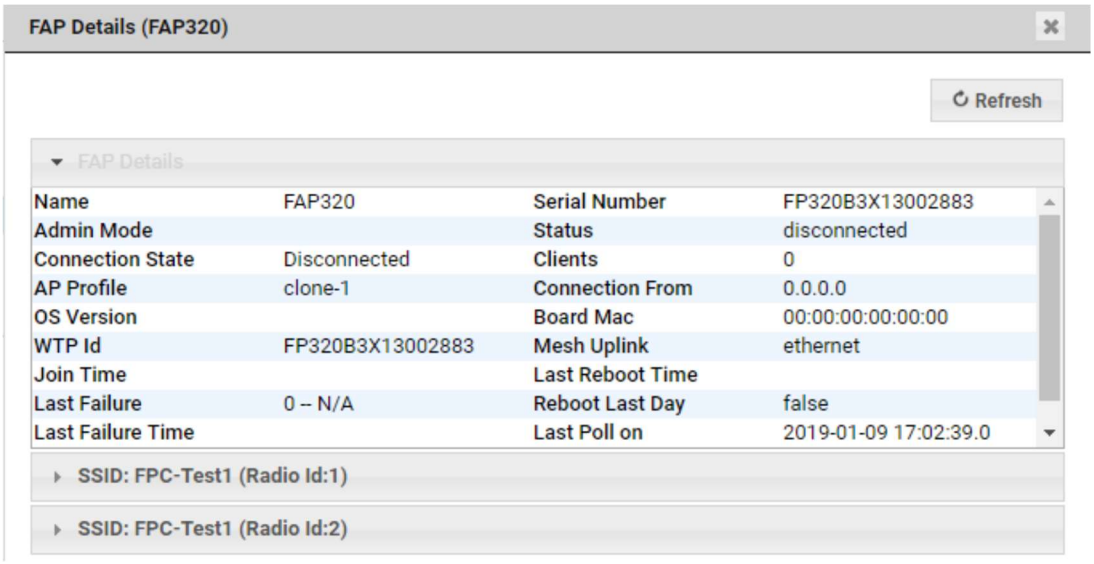


Ilustración 93

11.3 WiFi Profile

Permite actualizar y borrar perfiles AP, así como manejar los SSIDs en la política WiFi del firewall.

Ilustración 94

AP Profile

Muestra los diferentes perfiles de AP, con sus características de radio.

Cada uno de ellos puede ser modificado o borrado.

Seq.	Name	Platform	Radio 1	Radio 2	Comment
1	11n-only	FortiWiFi local radio	2.4GHz 802.11n/g/b		
2	AP-11N-default	Default 11n AP	2.4GHz 802.11n/g/b		
3	Clone of FAP320B_for_test	FAP320B	5GHz 802.11n/a	2.4GHz 802.11n/g/b	
4	FAP112B-clone	FAP112B	2.4GHz 802.11n/g/b		
5	FAP112B-default	FAP112B	2.4GHz 802.11n/g/b		
6	FAP112D-default	FAP112D	2.4GHz 802.11n/g/b		
7	FAP11C-default	FAP11C	2.4GHz 802.11n/g/b		
8	FAP14C-default	FAP14C	2.4GHz 802.11n/g/b		
9	FAP210B-default	FAP210B	2.4GHz 802.11n/g/b		
10	FAP21D-default	FAP21D	2.4GHz 802.11n/g/b		
11	FAP220B-default	FAP220B/221B	5GHz 802.11n/a	2.4GHz 802.11n/g/b	
12	FAP221C-default	FAP221C	2.4GHz 802.11n/g/b	5GHz 802.11ac/n/a	

Ilustración 95

SSID

Se muestran los **SSIDs configurados**. Se pueden modificar y borrar con el menú que aparece al pulsar el botón derecho sobre uno de ellos.

Seq.	Name	SSID	Traffic Mode	Security Mode	Schedule	Data Encryption	Maximum Clients
1	DFS_323C	DFS_323C	Local Bridge	Open	Always	AES	0
2	FPC-Captive-0	fortinet	Tunnel	WPA2 Only Personal	Always	AES	0
3	FPC-Test1	FPC-Test1	Tunnel	WPA2 Only Personal	Always	AES	0
4	FPC-Test2	FPC-Test2	Tunnel	WPA2 Only Personal	Always	AES	0
5	S311_DFS	S311S_DFS_VAP	Local Bridge	Open	Always	AES	0
6	wifi	fpc_test	Tunnel	WPA2 Only Personal	Always	AES	0

Ilustración 96

Para crear uno nuevo, se debe configurar el nombre, el pool de direcciones IP, la PSK, servidores de autenticación, y VLAN pooling.

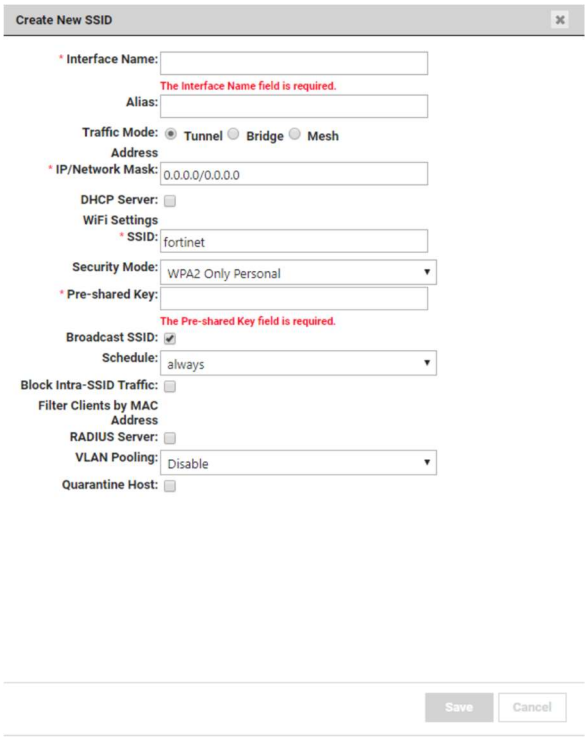


Ilustración 97

12 SDWAN

Es una característica de Device Manager, que sólo está accesible para los clientes que lo soliciten explícitamente.

SD-WAN o software-defined wide area, permite crear dos interfaces WAN redundantes para acceso a internet, de forma que la navegación esté balanceada entre ambos. También aporta redundancia en caso de que uno de ellos caiga.

El menú es accesible desde Device Manager, en la barra de acciones principal:

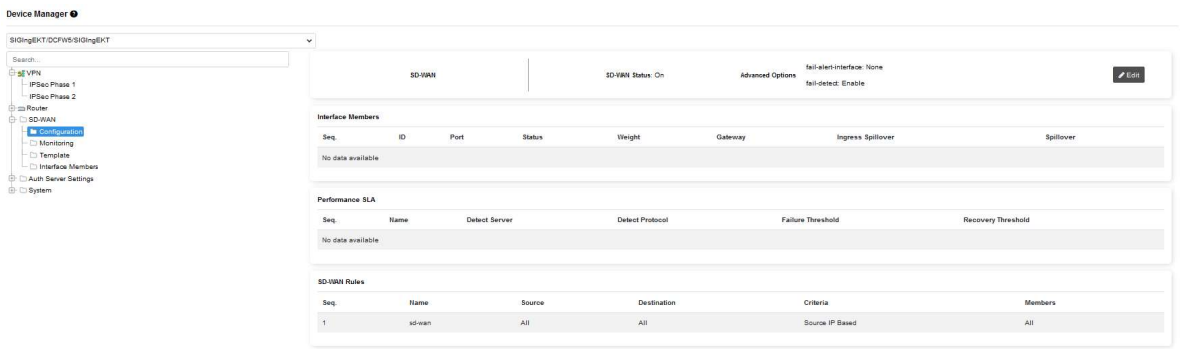


Ilustración 98

Desde FortiPortal podemos realizar las siguientes opciones:

- **Editar el estado de SD-WAN y opciones avanzadas**
- **Configurar los interfaces que participan, los SLAs aplicados y las reglas SD-WAN**
- **Monitotizar SD-WAN a través de las interfaces que participan**
- **Crear Plantillas SD-WAN para aplicarlas a un ADOM**

12.1 SD-WAN status y opciones avanzadas

El panel SD-WAN muestra el estado de este (on/off) y las opciones avanzadas:

- **Fail-alert-interface**
- **Fail-detect**

Ilustración 99

Para habilitarlo pulsamos sobre el botón "**Edit**" y aparece este cuadro de diálogo:

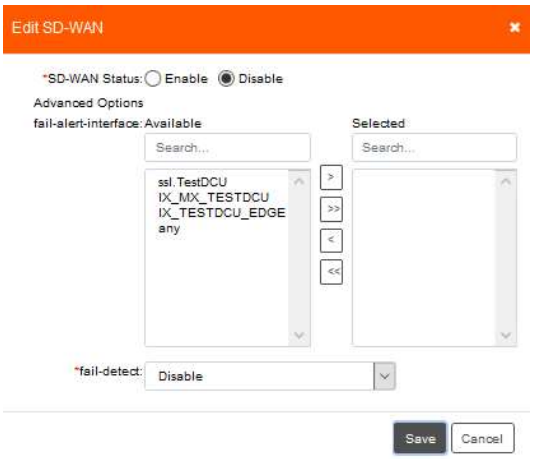


Ilustración 100

Seleccionamos "**Enable**" en **SD-WAN Status** en primer lugar. A continuación, seleccionamos el **interfaz físico** que queremos monitorizar, **fail-alert-interface** (o también puede ser None o Any, para ninguno o todos) y hablitamos **fail-detect** (detección de caída del interfaz o el acceso a Internet).

Las dos opciones de configuración y monitorización aparecen debajo de la carpeta de SD-WAN en **Device Manager**

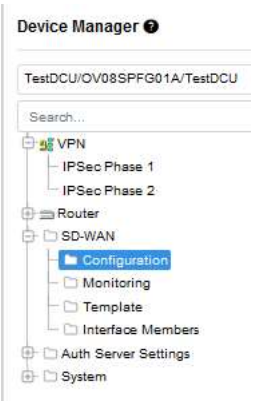


Ilustración 101

12.2 Configuración SD-WAN

Debemos seguir los siguientes pasos:

12.2.1 Configuración de interfaces

Habilitamos los siguientes puntos para la Configuración (**Configuration**) SD-WAN:

- **Interface members** son los interfaces entre los que se hará el balanceo
- **Performance SLA** define las características que debe cumplir el interfaz para ser considerado como activo dentro del grupo SD-WAN
- **SD-WAN rules** definen la prioridad de los flujos y sesiones que están establecidas a través de los interfaces físicos que comprenden el servicio SD-WAN

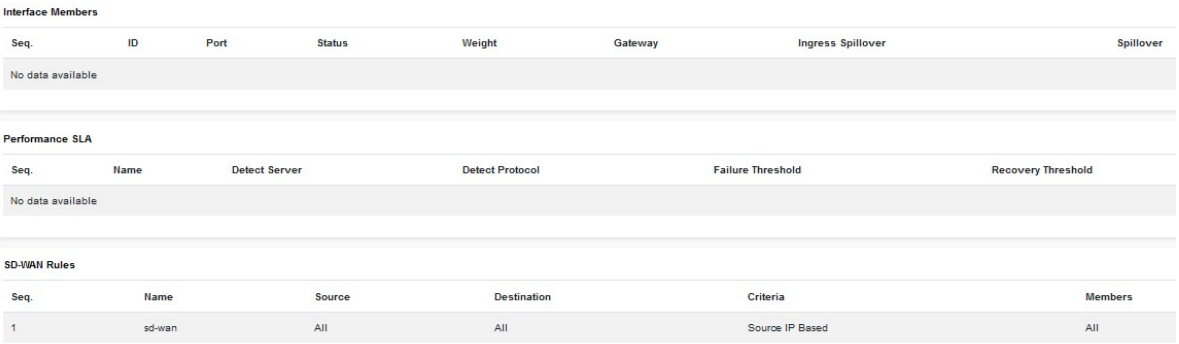


Ilustración 102

En **Interface Members** añadimos tantos interfaces como necesitemos.

Para definir sus parámetros utilizamos el siguiente cuadro:

Ilustración 103

- **Member** permite seleccionar uno de los interfaces físicos disponibles
- **Weight** da un peso sobre el reparto de carga a este interfaz. El mínimo es 0 y el máximo 255, y mientras más alto es, mayor carga soporta.
- **Gateway IP** es la dirección IP del default gateway para este interfaz. Normalmente es el definido para acceso a Internet en este interfaz.
- **Status** habilita y deshabilita este intefaz dentro del SD-WAN
- **Estimated Upstream/Downstream Bandwidth** define el ancho de banda de subida y bajada teórico para este interfaz. Se tendrá en cuenta para el reparto de carga.
- **Opciones avanzadas:**
    - **Gateway6** es la dirección IPv6 del gateway en caso de que se utilice IPV6
    - **Priority** asigna una prioridad en el reparto de carga. Mientras más alto el número, mayor prioridad tiene este interfaz.
    - **Seq-num** es el número de secuencia en el reparto de carga entre los interfaces. Va de 0 a 4294967295.
    - **Source** es la dirección origen IPv4 del interfaz
    - **Source6** es la dirección origen IPv6
    - **Volumen-ratio** es el valor de carga total que soporta el interfaz (por ejemplo: 20, entre una suma de 100 repartidos por los interfaces, da un 20%)

12.2.2 Configuración de SLA

A continuación, activamos el **SLA** que deben cumplir la conexión a través de los interfaces:

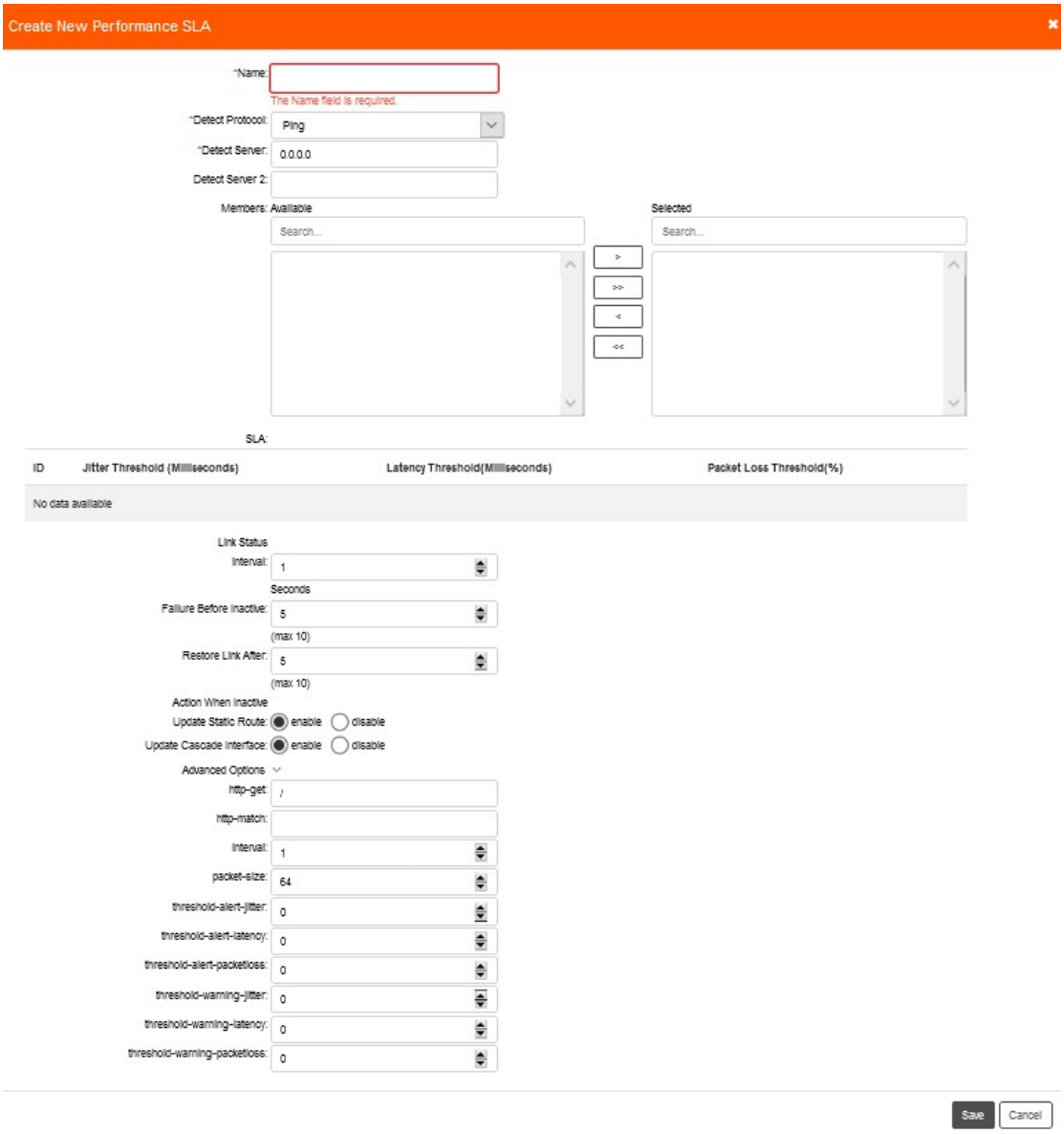


Ilustración 104

Si todos los interfaces cumplen con el SLA, se elegirá el primer link por prioridad, aunque no sea el de mejor ancho de banda. Si ese interfaz deja de cumplir uno de los criterios del SLA, pasará al siguiente con mayor prioridad que sí los cumpla.

Los parámetros para definir el SLA son los siguientes:

- **Name** o nombre del SLA

- **Detect Protocol** es el protocolo que se va a utilizar para probar el interfaz. Puede ser PING, TCP ECHO, UDP ECHO, HTTP o TWAMP
- **Detect Server** es la IP de un servidor externo al que se va a intentar acceder con el protocolo de pruebas
- **Detect Server 2** es la IP de un segundo servidor de test.
- **Members** permite seleccionar entre los interfaces de SD-WAN, los que se le va a aplicar este cumplimiento de condiciones
- **SLA fields** son los parámetros físicos para evaluar el interfaz, con sus valores umbrales máximos
    - **Link-cost factor** permite elegir entre uno o varios criterios de calidad:
        - **Jitter** o variación de los retardos
        - **Latency** o retardo
        - **Packet loss** o pérdida de paquetes

    - **Thresholds** son los valores máximos permitidos para **jitter, latency y packets loss**:

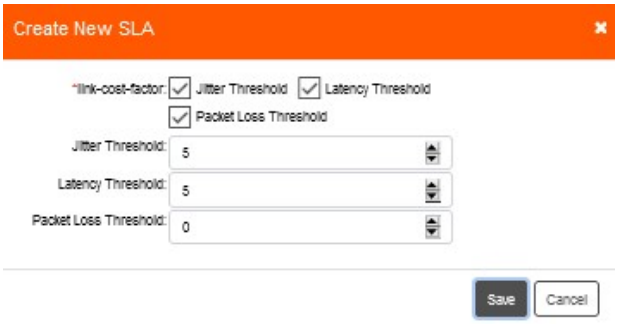


Ilustración 105

- **Link status** es relativo al estado del interfaz según el SLA
    - **Interval** es el periodo de tiempo tras el cual se intenta conectar al servidor para comprobar la calidad. Por defecto es 5 segundos, pero puede configurarse entre 1 y 3600 segundos.
    - **Failure before inactive** es el número de fallos tras el cual se considera que el interfaz es inválido. Puede ser entre 1 y 10. Por defecto es 5.
    - **Restore link after** es el número mínimo de respuestas correctas desde el servidor para considerarlo como recuperado. Tiene los mismos valores que el anterior.

- **Action when Inactive**
    - **Update Static Route** permite cambiar las rutas estáticas tras la caída del interfaz como interfaz válido.

- **Update Cascade Interface** habilita el update en cascada desde el interfaz.

- **Advanced Options**
  - **http-get** es la URL que debe utilizar en vez de ip la sonda si el servidor es HTTP
  - **http-match** es el string de respuesta del servidor que esperamos para HTTP
  - **Interval** es el tiempo que esperará la sonda entre pregunta y
  - **Packet-size** es el tamaño de paquete para twapt. El rango es 64-1024

  A partir de ahí podemos configurar los umbrales de las tres medidas de calidad (jitter, latencia y pérdida de paquetes), para lanzar alerta de sobrepasado o un aviso (warning) por estar cerca. El valor para jitter y latencia es entre 0 y 4294967295 ms y la pérdida entre 0 y 100 porciento:

  - **Threshold-alert-jitter**
  - **Threshold-alert-latency**
  - **Threshold-alert-packetloss**
  - **Threshold-alert-jitter**
  - **Threshold-alert-latency**
  - **Threshold-alert-packetloss**

12.2.3 Reglas SD-WAN

Y por último añadimos las reglas de SD-WAN para balanceo y prioridad (también conocidas como servicios). Podemos editarlas, borrarlas o crearlas según pulsemos sobre **Edit, Delet o Create New.**

Pulsando sobre **Create New,** aparecerá el menú de configuración de una nueva regla:

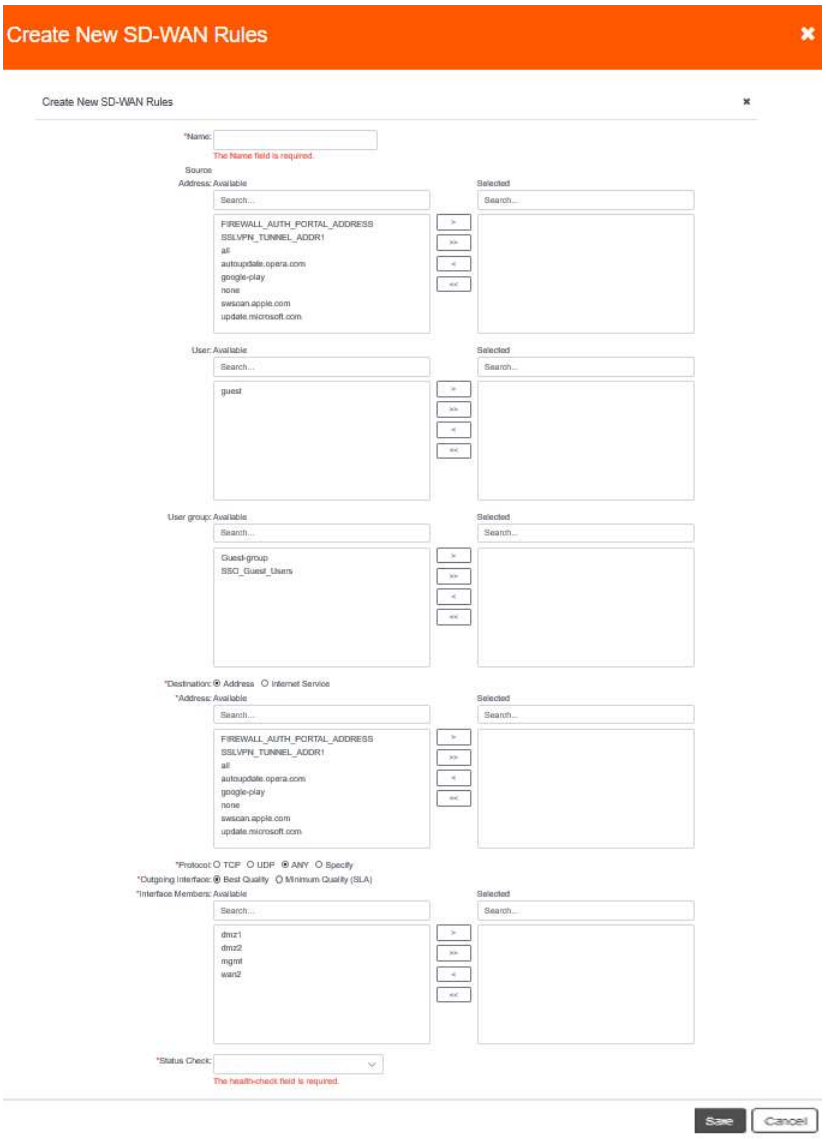


Ilustración 106

- **Name** es el nombre de la regla

- **Source** es el origen de las conexiones a las que aplicaremos la regla. Es la combinación de:
    - **Address** o la dirección IP origen
    - **User** o usuario
    - **User group** o grupos de usuarios

- **Destination** es el destino de las conexiones, formado por la elección de una dirección IP o un servicio:
    - **Address** o dirección IP destino
    - **Internet Service** predefinido
    - **Internet Service Group** también predefinido
    - **Protocol** o protocolo utilizado en las conexiones

- **Application** en el caso de Servicio, designa la aplicación de las conexiones verificadas.
- **Application Group** es el conjunto de aplicaciones para verificar en las conexiones.

- **Outgoing interface** es el criterio para elegir el mejor interfaz de salida entre los miembros del SD-WAN:
  - **Best Quality** mejor calidad en general
  - **Minimum Quality (SLA)** requiere que llegue a los estándares del SLA

- **Status Check** aparece en el caso de que hayamos elegido mejor calidad es donde se permite elegir el SLA requerido

- **Required SLA Target** aparece en el caso de elegir mínima calidad, para elegir el SLA de la lista de predefinidos.

12.3 Monitorización SD-WAN

En la pestaña de monitorización SD-WAN podemos encontrar el estado de cada una de las reglas de SDWAN en activo, con los parámetros de calidad del enlace y el número de sesiones:

Table | Map

Device	Template	Interface	Packet Loss	Volume(TX)	Volume(RX)	Session	Performace	Jitter	Latency	Bandwidth(TX)	Bandwidth(RX)
FGT60D4613055589(root)		dmz	0%	0	0	0	Ping_gateway	0	0	0	0
							Ping_FAZ	0	0	0	0
							SaaS_SLA	0	0	0	0
FGT60D4613055589(root)		wan2	0%	25.21 KB	3.59 MB	0	Ping_gateway	0	0	0	0
							Ping_FAZ	0	0	0	0
							SaaS_SLA	0	0	0	0

Ilustración 107

12.4 Plantillas SD-WAN

Permite crear plantillas para aplicar en distintos tiempos sobre el ADOM del cliente. Solo un perfil SDWAN puede estar aplicado en el entorno, a la vez.

La configuración es igual a la vista en el punto 12.2, donde nos permite identificar:

- **Los interfaces donde se aplica**
- **El SLA que tiene que cumplir**

- Las reglas SD-WAN
- El modo de fail-over entre interfaces
- El modo de balanceo
-

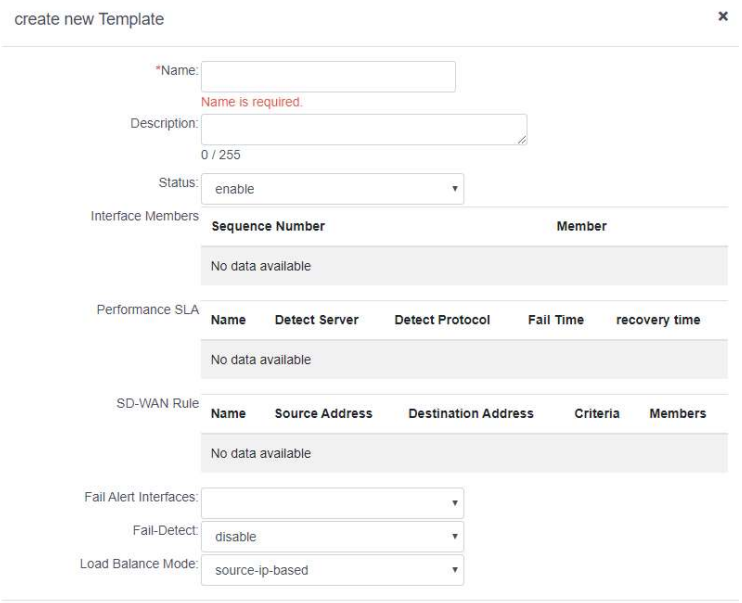


Ilustración 108