

Em- pre- sas.



Cercanía para llegar lejos.

Manual de usuario servicio Fortimanager



euskaltel




telecable

Grupo Euskaltel

Índice

0.	Introducción	3
1.	Servicio de Fortimanager.....	4
1.1.	Creación de objetos	4
1.2.	Creación de servicios.....	7
1.3.	Creación de VIPs	8
1.4.	Creación de objetos IP Pools.....	10
1.5.	Configuración política básica de navegación.....	12
1.6.	Configuración política básica de navegación con NATs específicos ..	14
1.7.	Integración de políticas en FortiGate	16
1.8.	Configuración de políticas con calidad de servicio (QoS)	18
1.9.	Creación de usuarios y grupos locales	20
1.10.	Configuración URL Filtering.....	22
1.11.	Configuración Control de aplicaciones	24
1.12.	Configuración IPS.....	26
1.13.	Configuración perfiles antivirus para navegación.....	29
1.14.	Configuración VPN SSL	30
1.15.	Configuración VPN IPSEC	34
1.16.	Configuración Política DLP.....	42
1.17.	Políticas de navegación por grupo de usuarios.....	46
1.18.	Proxy Web	47
1.19.	Balancedores de carga.....	51
1.19.1	Definición del servicio balanceado	51
1.19.2.	Creación de la granja de servidores	53
1.19.3.	Utilización en la política.....	54

0. Introducción

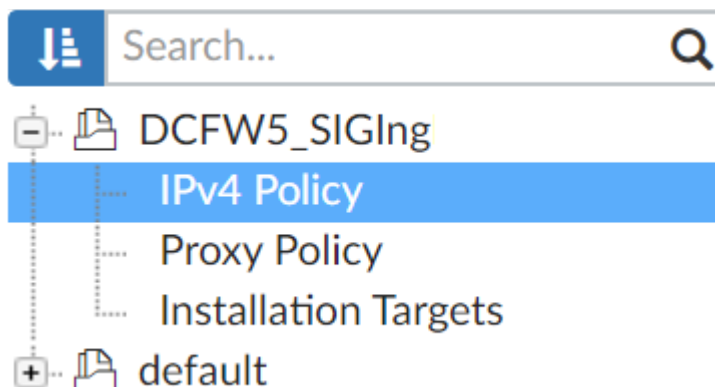
Dentro del proceso de actualización y mejora del servicio de firewall virtual, el grupo Euskaltel proporciona un nuevo portal de acceso web para la gestión, y monitorización de las políticas, que además de permitir a los clientes acceder a un panel único, aporta las siguientes características y ventajas:

- Nuevo Interface más sencillo, e intuitivo para ayudar a la identificación y respuesta a incidentes de seguridad.
- Administración centralizada: mediante un amplio conjunto de herramientas que permite gestionar todos los dispositivos Fortinet del cliente.
- Realizar copias de seguridad de la configuración.

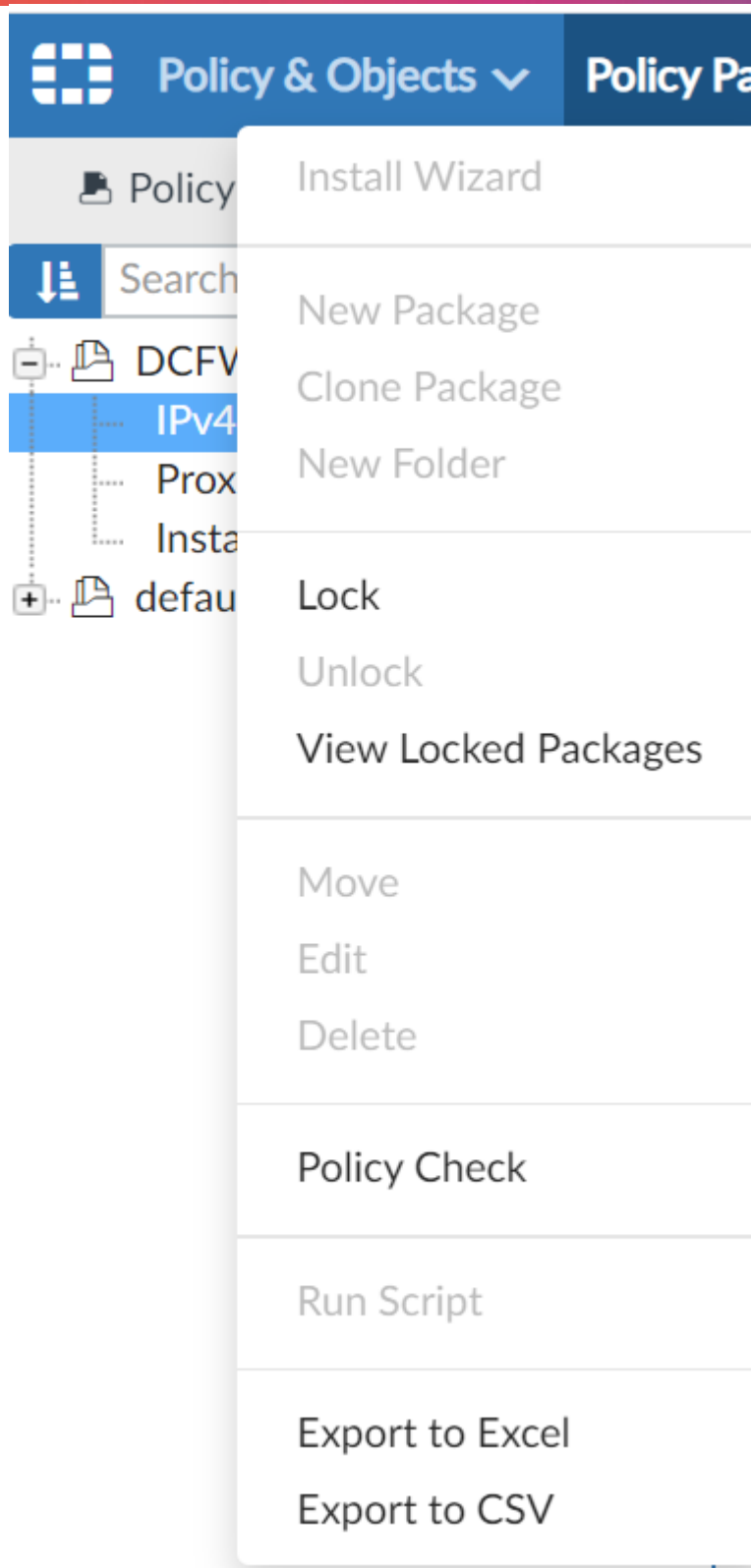
A continuación, se describe cómo realizar las acciones más habituales de gestión y monitorización de la política del firewall.

1. Servicio de Fortimanager

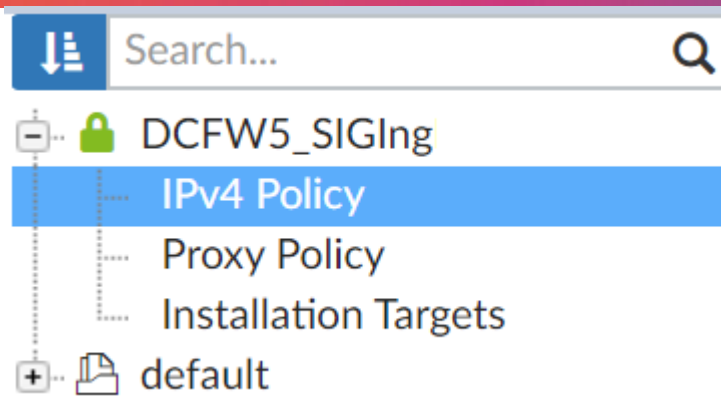
Para poder realizar cambios sobre las políticas y objetos es necesario bloquearlo.



Para ello sobre el menú de la izquierda nos ponemos sobre IPv4 Policy, botón derecho y seleccionamos **Lock**. Esto permitirá hacer cambio sobre la política, objetos, perfiles de seguridad...



Al hacerlo aparecerá un candado en verde indicando que se ha bloqueado y ya podremos realizar nuevas configuraciones.



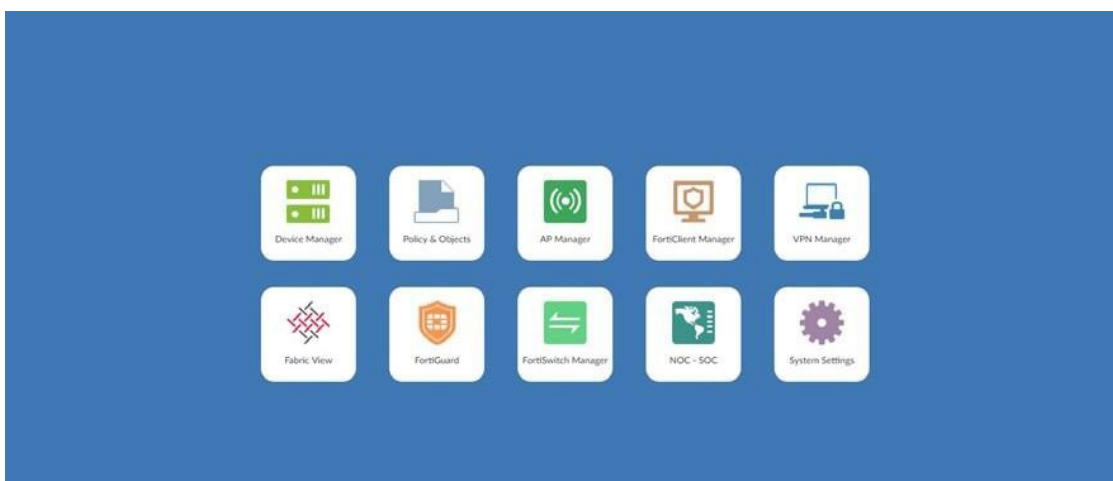
Antes de aplicar cualquier cambio, es decir, ejecutar un Install, tendremos que hacer click sobre el botón Save, que como se puede ver, cambia de color cuando se detecta algún cambio.



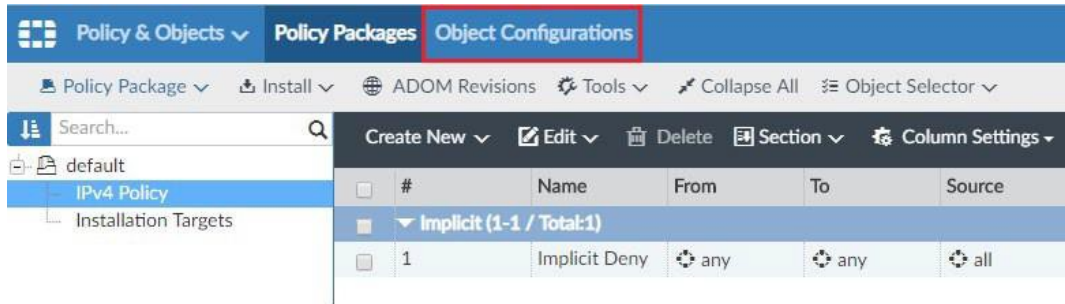
1.1. Creación de objetos

Un objeto es una referencia, en la que viene definido habitualmente una dirección IP.

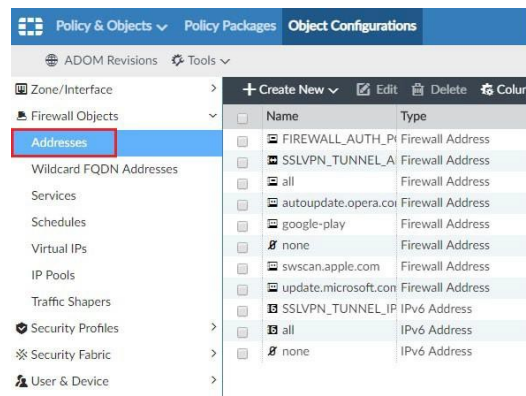
1. Seleccionar en el menú principal la opción de "Policy & Objects".



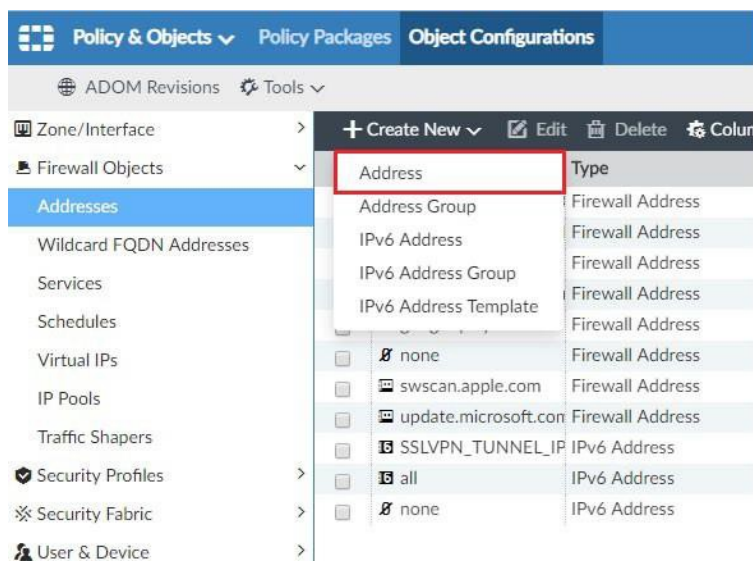
2. Seleccionar en el menú superior la opción “Object Configurations”.



3. Elegir en el menú lateral izquierdo la opción de “Firewall Objects” y “Addresses”.

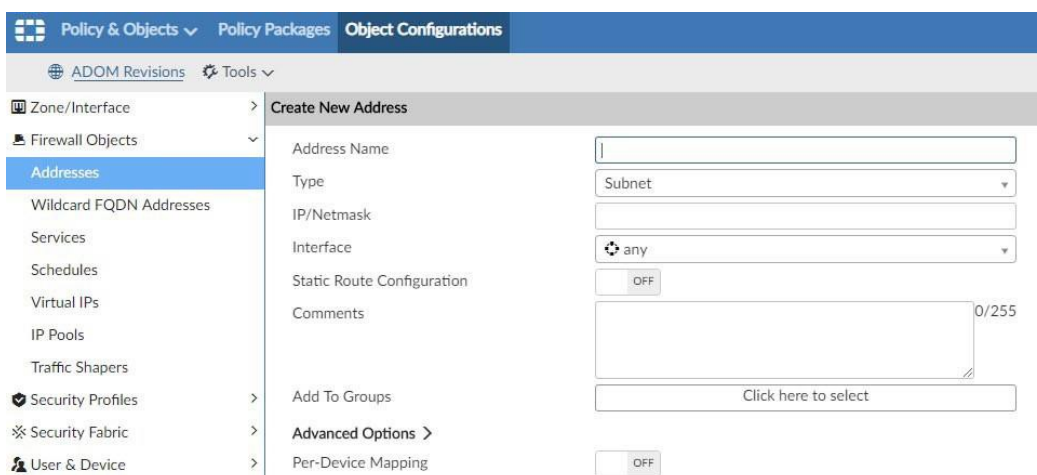


4. Hacer click en la pestaña “Create new” y en la opción de “Address”.



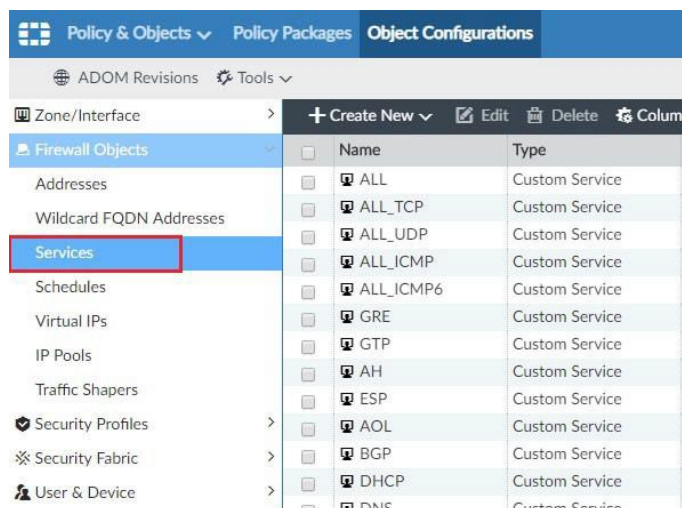
5. Procedemos a crear el objeto:

- En el campo Address Name incluiremos un nombre identificativo para el objeto a crear.
- En el campo Type, elegiremos subnet.
- En el campo IP/Netmask especificamos la IP del objeto con su correspondiente máscara.
- En el campo Interface elegiremos “any” No será necesario especificar la interfaz en la creación del objeto. Si se desea utilizar será aquella interfaz a través de la cual se enrutará el tráfico para alcanzar la dirección del objeto que se está creando.

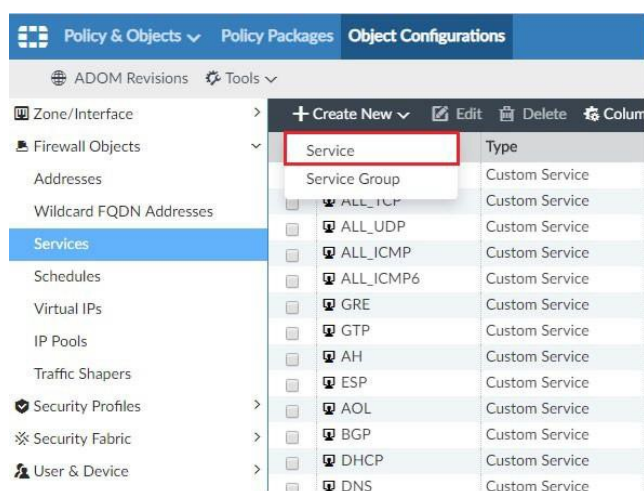


1.2. Creación de servicios

1. Seleccionar en el menú principal la sección “Policy & Objects” y en la parte superior “Object Configurations”. En el panel izquierdo, dentro de “Firewall Objects” seleccionar “Services”.



2. Para la creación: seleccionar el botón “Create New” y dentro del desplegable la opción “Service”.



3. Una vez dentro de la configuración, distinguimos los campos siguientes:

- Name: Nombre significativo con el que se verá el servicio en el editor de políticas.
- Service Type: Por defecto Firewall.

- Category: Nombre de la categoría en la que queremos añadir el servicio nuevo. Normalmente se añadirá en Uncategorized.
- Protocol type: Lo más habitual seleccionar la opción "TCP/UDP/SCTP"
- Protocol: Seleccionamos el protocolo correspondiente "TCP/UDP/SCTP".
- Source Port: Rango de Puertos Origen, por defecto [1-65535].
- Destination Port: Este campo es el que define el servicio, si únicamente se quiere especificar un puerto sería [8080-8080] .

The screenshot shows the 'Create New Service' configuration interface in Fortimanager. The left sidebar is expanded to 'Services' under 'Firewall Objects'. The main configuration area includes the following fields and options:

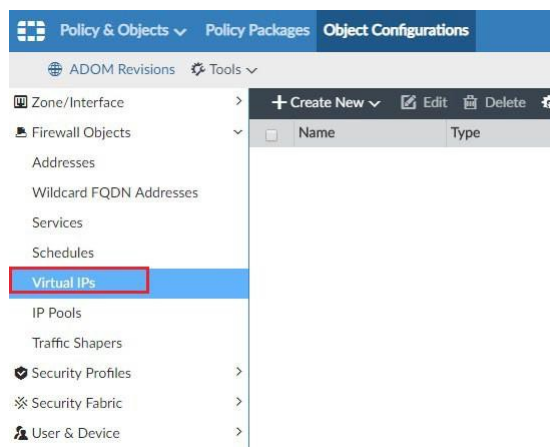
- Name:** A text input field.
- Comments:** A text area with a character limit of 0/255.
- Service Type:** Radio buttons for 'Firewall' (selected) and 'Proxy'.
- Category:** A dropdown menu set to 'Uncategorized'.
- Protocol Type:** A dropdown menu set to 'TCP/UDP/SCTP'.
- IP/FQDN:** A text input field containing '0.0.0.0'.
- Add To Groups:** A button labeled 'Click here to select'.
- Protocol:** A dropdown menu set to 'TCP'.
- Source Port:** Two input fields: the first contains '1' and the second contains '65535'.
- Destination Port:** Two input fields: the first contains '0' and the second contains '0'.
- Advanced Options:** A link to expand more configuration options.

1.3. Creación de VIPs

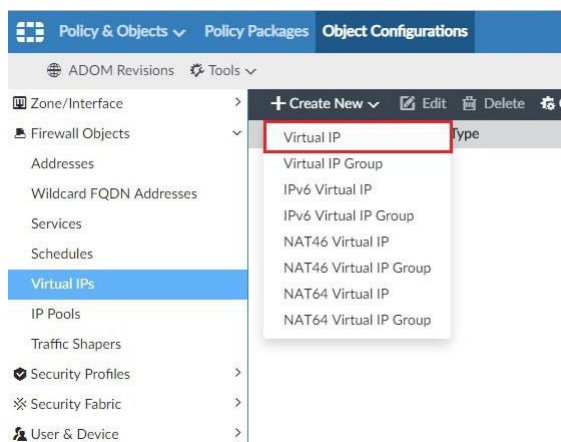
Una dirección IP virtual (VIP) es una dirección IP que no corresponde a una interfaz de red física real.

Se establecerá una correspondencia entre una IP pública y una IP privada, de forma que todo el tráfico con destino a esa IP pública se traducirá a la IP privada. Esta traducción se podrá hacer para todos los puertos y protocolos o bien se podrá traducir únicamente un puerto. Incluso cabe la posibilidad de utilizar una única IP para publicar varias IPs privadas, con distintos servicios en cada una de ellas. Por ejemplo, es posible redirigir el puerto SMTP a la dirección privada del servidor de correo, con distinta IP del servidor web, al que se dirigirá el tráfico http.

1. Seleccionar en el menú principal la sección "Policy & Objects" y en la parte superior "Object Configurations". En el panel izquierdo, dentro de "Firewall Objects" seleccionar "Virtual IPs".



2. Para la creación: seleccionar el botón “Create New” y dentro del desplegable la opción “Virtual IP”.



3. Una vez dentro de la configuración, distinguimos los campos siguientes:

- Name: Nombre significativo con el que se verá el objeto en el editor de políticas.
- Interface: En caso de escoger una interfaz específica, solo se podrá utilizar este VIP en aquellas reglas cuya interfaz origen sea la seleccionada.
- Type: Por defecto NAT Estático.
- External IP Address/Range: IP pública que se va a ver internet y sobre las que se van a establecer las conexiones, será traducida por el Firewall a la IP privada.
- Mapped IP Address/Range: IP privada a la que se va a traducir.

The screenshot shows the 'Create New Virtual IP' configuration window in Fortimanager. The left sidebar is expanded to 'Virtual IPs'. The main area contains the following fields and options:

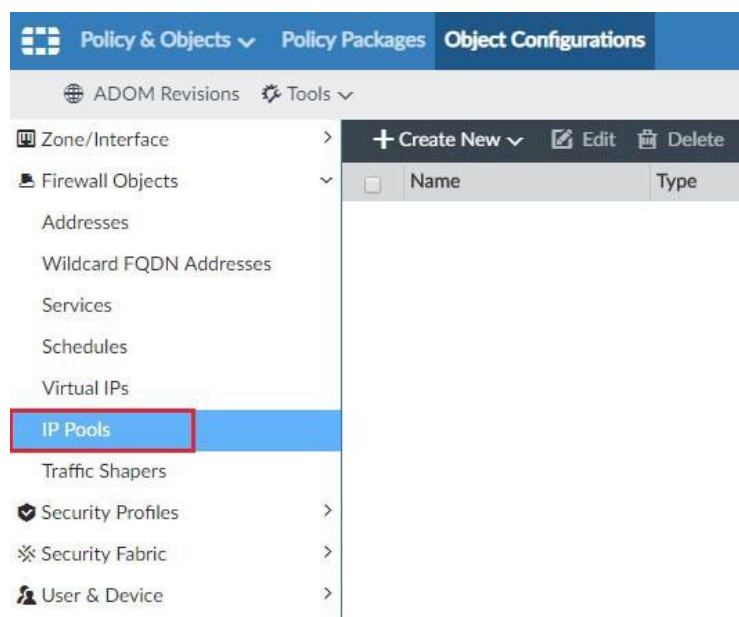
- Name:** Text input field.
- Comments:** Text area with a character count of 0/255.
- Color:** Color selection icon.
- Interface:** Dropdown menu with 'any' selected.
- Configure Default Value:** Toggle switch set to 'ON'.
- Network:** Section header.
- Type:** Radio buttons for 'Static NAT' (selected), 'DNS Translation', and 'FQDN'.
- External IP Address/Range:** Text input field with '0.0.0.0'.
- Mapped IP Address/Range:** Two text input fields, both with '0.0.0.0'.
- Source Interface Filter:** Text input field with 'Click to add ...'.
- Optional Filters:** Toggle switch set to 'OFF'.
- Port Forwarding:** Toggle switch set to 'OFF'.
- Enable ARP Reply:** Checked checkbox.
- Add To Groups:** Text input field with 'Click here to select'.
- Advanced Options:** Expandable section.

Buttons for 'OK' and 'Cancel' are located at the bottom right.

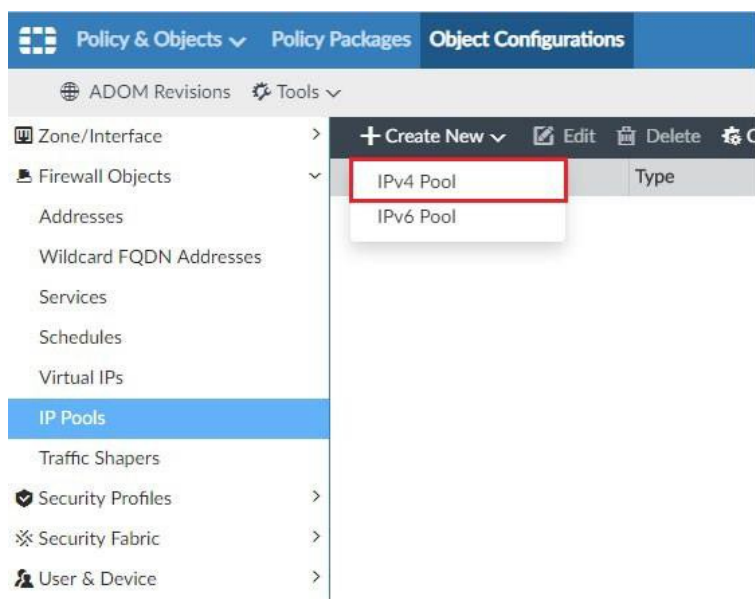
1.4. Creación de objetos IP Pools

Se indicará una IP o un rango de IPs que se utilizarán para traducir las direcciones orígenes de la regla, normalmente cuando esas direcciones IPs origen sean privadas y quieran tener acceso a Internet.

1. Seleccionar en el menú principal la sección “Policy & Objects” y en la parte superior “Object Configurations”. En el panel izquierdo, dentro de “Firewall Objects” seleccionar “IP Pools”.

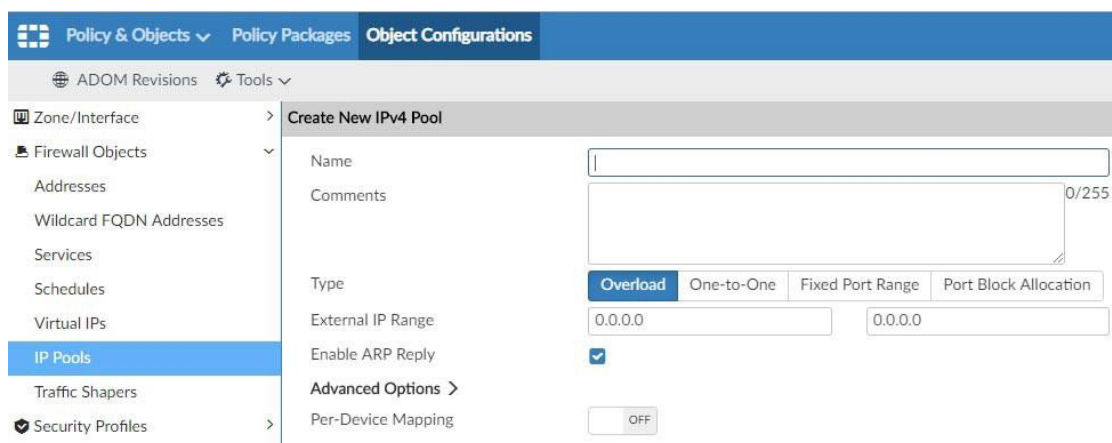


2. Para la creación: seleccionar el botón “Create New” y dentro del desplegable la opción “IPv4 Pool”.



3. Una vez dentro de la configuración, distinguimos los campos siguientes:

- Name: Nombre significativo con el que se verá el objeto en la edición de la regla.
- Type: Podemos definir varias opciones para la asignación de la IP o rango públicos a las IPs privadas, hacer una asignación uno-a-uno, con sobrecarga, un rango de puerto fijo o la asignación de bloque de puertos.
- External IP Range: IP o Rango de IPs con las que se va a salir a Internet, normalmente será una IP únicamente pero podría definirse un rango o una subred.



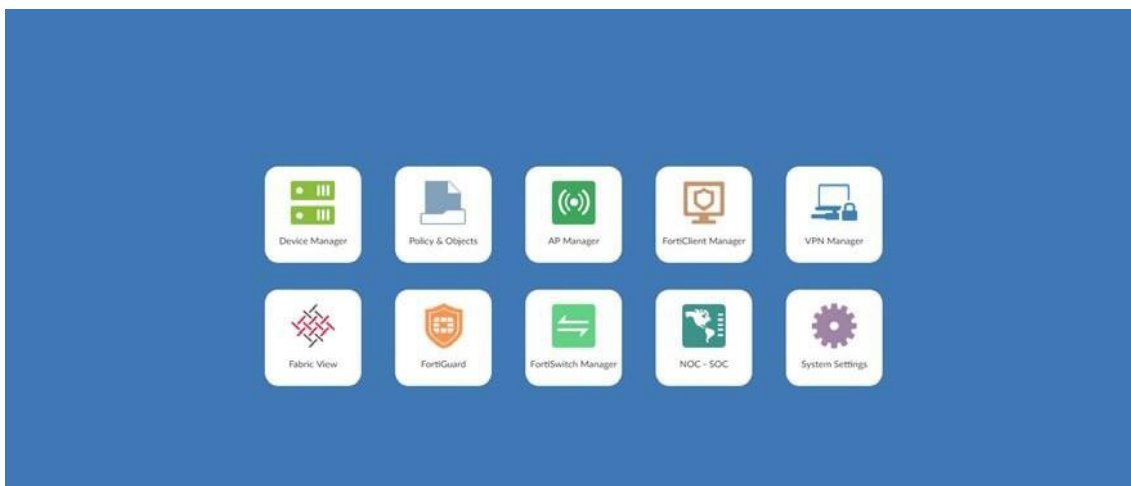
1.5. Configuración política básica de navegación

Una política se trata de un conjunto de reglas que definen los accesos permitidos de internet a los servicios internos y viceversa. Estas reglas se definen como una IP o grupo de IPs origen y una IP o grupo de IPs destino así como uno o varios servicios y puertos y la acción que se quiere que se lleve a cabo cuando a través del Firewall se detecte un tráfico que coincide con lo especificado en la regla.

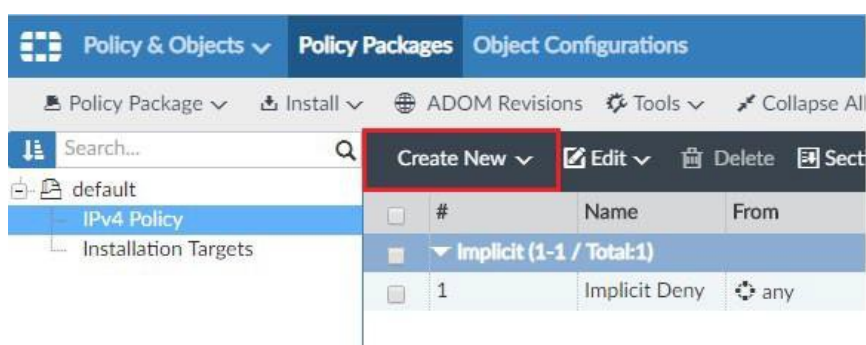
Dicha acción podrá ser básicamente aceptar o rechazar la conexión.

Las reglas se ejecutan de forma secuencial en orden, es decir, se empiezan a aplicar desde la regla más baja, la 1 hasta que se encuentre la primera coincidencia. Habitualmente la última regla es una de denegación total.

1. Seleccionar en el menú principal la opción de “Policy & Objects”.



2. Aparecemos directamente en el menú de las políticas, por lo que hacemos click en “Create new”.



3. Procedemos a crear la política.

Create New IPv4 Policy

Name	<input type="text"/>
Incoming Interface	<input type="text" value="any"/> ✕
Outgoing Interface	<input type="text" value="any"/> ✕
Source Internet Service	<input type="checkbox"/> OFF
Source Address	<input type="text" value="all"/> ✕
Source User	<input type="text" value="+"/> +
Source User Group	<input type="text" value="+"/> +
Source Device	<input type="text" value="+"/> +
Destination Internet Service	<input type="checkbox"/> OFF
Destination Address	<input type="text" value="all"/> ✕
Service	<input type="text" value="ALL"/> ✕
Schedule	<input type="text" value="always"/> ✕
Action	<input type="checkbox"/> Deny <input checked="" type="checkbox"/> Accept <input type="checkbox"/> IPSEC

- En el campo Name introduciremos el nombre (se recomienda que sea identificativo) de la política.
- En Incoming Interface se seleccionará la interfaz de entre aquellas configuradas desde donde se recibirá el tráfico proveniente de las IPs origen.
- En Outgoing interface se seleccionará la interfaz de entre aquellas configuradas por la cual el firewall enviará el tráfico hacia la IP destino de la conexión.
- En Source Address se especificará el objeto creado previamente para representar la IP, rango, red o grupos de IPs que será el origen de la conexión establecida.
- En Destination Address se especificará el objeto creado previamente para representar la IP, rango, red, grupos de IPs o IP virtual que será el destino de la conexión establecida.
- En Service se seleccionará el servicio, predefinido o personalizado, o grupo de ellos, que representa el protocolo al que se dará acceso o se rechazará en el destino de la conexión.
- En Action básicamente las acciones que se aplicarán serán ACCEPT, en caso de la que conexión deba ser permitida, o DENY en caso de que sea rechazada.

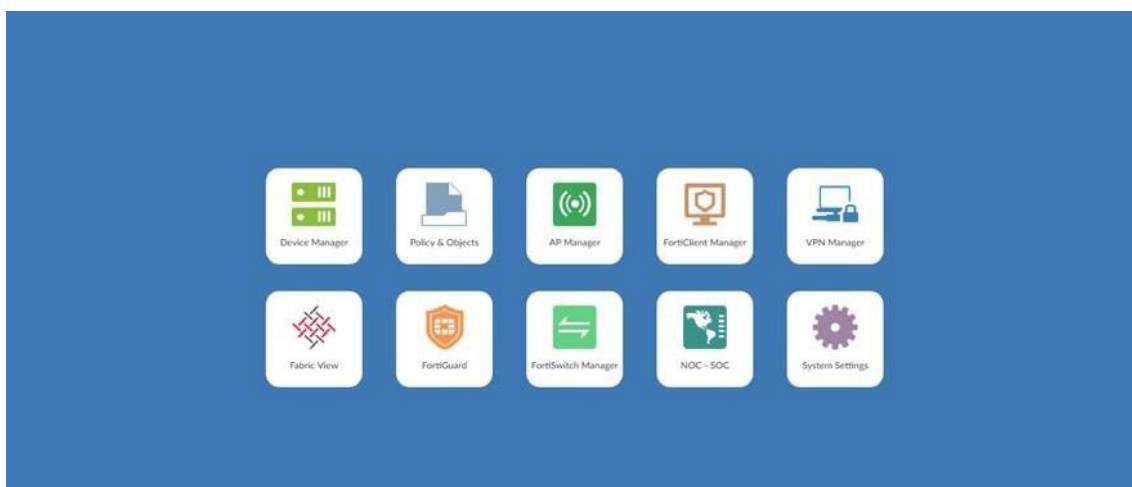
4. Por último, terminamos haciendo click en OK para crear la regla.

1.6. Configuración política básica de navegación con NATs específicos

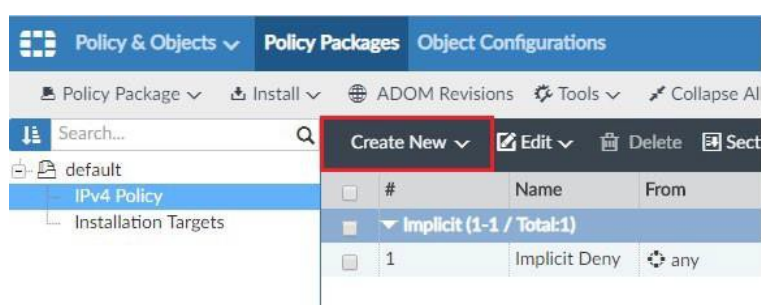
El NAT, es una funcionalidad que nos permite realizar una traducción de direcciones para convertir las IPs privadas de la red local de cliente en IPs públicas que tengan acceso a Internet. De forma inversa nos permitirá publicar en Internet una dirección privada de algún servidor al que se tenga que tener acceso desde una red pública.

Esta funcionalidad no siempre será requerida. Se habilitará el NAT si es necesario realizar una traducción de las IPs origen de la regla. Si simplemente se activa esta casilla, se traducirán automáticamente con la IP de la interfaz de destino en el firewall. En caso de que se quiera utilizar otra IP se marcará la opción "Dynamic IP Pool" y se escogerá una de entre las disponibles que se hayan configurado previamente.

1. Seleccionar en el menú principal la opción de "Policy & Objects".



2. Aparecemos directamente en el menú de las políticas, por lo que hacemos click en "Create new".



3.Procedemos a crear la política.

The screenshot shows the 'Create New IPv4 Policy' configuration interface. The fields and their values are as follows:

- Name: (empty text box)
- Incoming Interface: any
- Outgoing Interface: any
- Source Internet Service: OFF
- Source Address: all
- Source User: +
- Source User Group: +
- Source Device: +
- Destination Internet Service: OFF
- Destination Address: all
- Service: ALL
- Schedule: always
- Action: Deny (selected), Accept, IPSEC
- Log Traffic: Log Violation Traffic
- Generate Logs when Session Starts
- Comments: (empty text box)

En el campo Name introduciremos el nombre (se recomienda que sea identificativo) de la política.

- En Incoming Interface se seleccionará la interfaz de entre aquellas configuradas desde donde se recibirá el tráfico proveniente de las IPs origen.
- En Outgoing interface se seleccionará la interfaz de entre aquellas configuradas por la cual el firewall enviará el tráfico hacia la IP destino de la conexión.
- En Source Address se especificará el objeto creado previamente para representar la IP, rango, red o grupos de IPs que será el origen de la conexión establecida.
- En Destination Address se especificará el objeto creado previamente para representar la IP, rango, red, grupos de IPs o IP virtual que será el destino de la conexión establecida
- En Service se seleccionará el servicio, predefinido o personalizado, o grupo de ellos, que representa el protocolo al que se dará acceso o se rechazará en el destino de la conexión.
- En Action básicamente las acciones que se aplicarán serán ACCEPT, en caso de la que conexión deba ser permitida, o DENY en caso de que sea rechazada.
- Para la aplicación de una NAT específica, se habilitará la opción de NAT y podremos elegir dos opciones, que la NAT se realice mediante la ip de la interfaz de salida, o con un Ip Pool dinámico que nosotros hayamos creado.

Create New IPv4 Policy

Destination Address: all

Service: ALL

Schedule: always

Action: Deny **Accept** IPSEC

Log Traffic:

 No Log Log Security Events Log All Sessions

 Generate Logs when Session Starts

 Capture Packets

NAT

 Use Destination Interface Address Fixed Port

 Dynamic IP Pool

Security Profiles:

Shared Shaper: +

Reverse Shaper: +

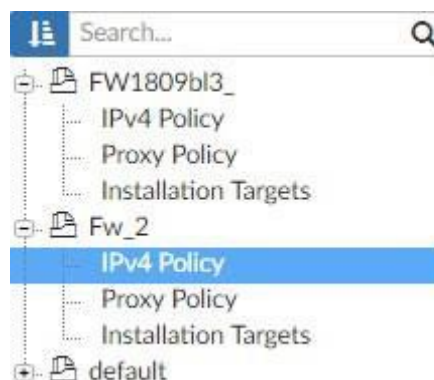
Per-IP Shaper: +

OK Cancel

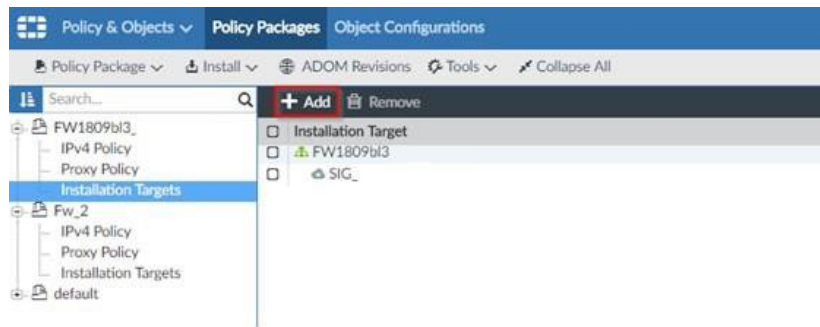
4. Por último, terminamos haciendo click en OK para crear la regla.

1.7. Integración de políticas en FortiGate

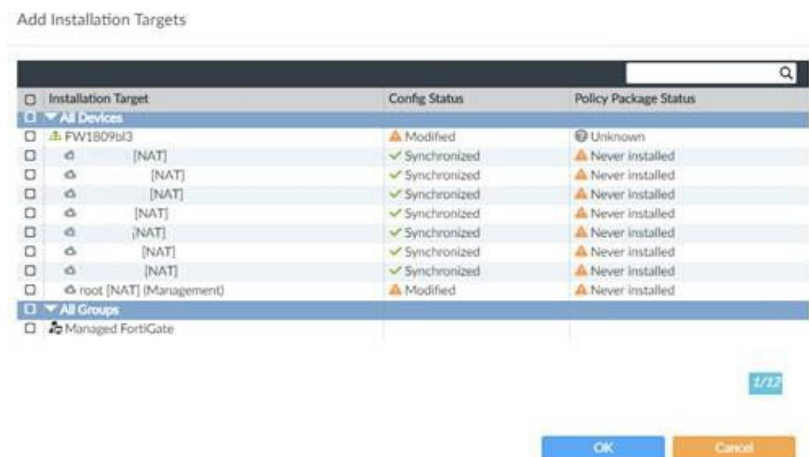
Una vez tenemos creadas un conjunto de políticas, agrupadas en un paquete, hay que integrarlas con el Fortigate. Para ello debemos ir al apartado de Policy & Objects. En el lateral izquierdo de la pantalla y podemos comprobar que tenemos tantos paquetes de políticas como hayamos creado. En nuestro caso tenemos 2 grupos, uno para un firewall y otro para un firewall distinto.



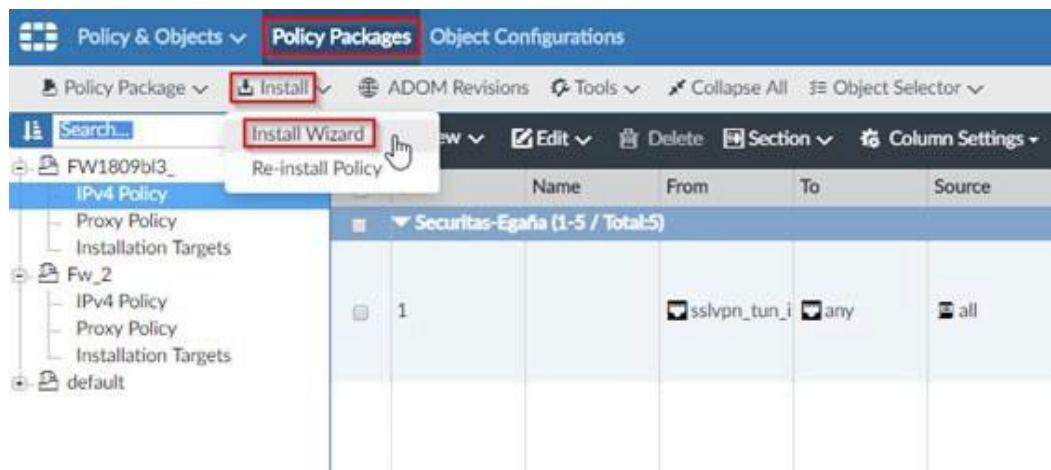
Una vez tenemos creado una política de red para nuestro firewall, debemos incluir dicho firewall en el apartado de Installation Targets. Para ello debemos hacer click en Add.



Entonces se nos desplegará una pantalla con los posibles objetivos de la instalación del paquete de políticas, de las que deberemos elegir el que deseemos.



El siguiente paso sería instalar dicho paquete de políticas en el objetivo. Para ello desde la pantalla de Policy Packages, hacemos click en Install, y elegimos Install Wizard.



Ahora se nos muestra una pantalla donde debemos elegir cual es el paquete de políticas que queremos instalar.

Install Wizard

Install Policy Package & Device Settings
Install a selected policy package. Any device specific settings for devices associated with the package will also be installed.

Policy Package: FW1809bl3

Comment:

Create ADOM Revision

Schedule Install

Install Device Settings (only)

Next > Cancel

Por último, en función del paquete de políticas que hayamos elegido, y de los Installation Targets que le hayamos asignado, se nos dispondrán unas opciones u otras para instalar dicho paquete de políticas, de las que se podrán elegir como objetivo tantas unidades como queramos.

Install Wizard - Policy Package and Device Setting FW1809bl3

Please select one or more devices to install (Use checkbox or Ctrl or Shift key for multiple selections)

Search...

Device Name	IP Address	Platform
FW1809bl3	192.168.1.1	FortiGate-1500D
FW1809bl3	192.168.1.2	vdom

< Back Next > Cancel

Una vez hayamos hecho click en Next, comenzará la carga del paquete en la unidad elegida.

1.8. Configuración de políticas con calidad de servicio (QoS)

QoS (Quality of Service en inglés) es un conjunto de mecanismos utilizados para asegurar la priorización de tráfico y garantizando un ancho de banda mínimo para la correcto funcionamiento del servicio. QoS básicamente mide el ancho de banda y prioriza los paquetes de tráfico en función de las colas de prioridad.

No debemos confundir QoS con limitador de ancho de banda ya que, básicamente el limitador limita la conexión independientemente del tipo de tráfico que haya pero no realiza priorización de los paquetes en la cola.

Para la creación de políticas con calidad de servicio el proceso a seguir es el mismo que el anterior.

Antes de hacer click en OK para terminar de crear la regla nos fijaremos en

una de las últimas opciones dentro de la creación de políticas. Aquí será donde elegiremos cómo queremos

Security Profiles	<input type="checkbox"/>
Shared Shaper	<input style="width: 50px;" type="text" value="+"/>
Reverse Shaper	<input style="width: 50px;" type="text" value="+"/>
Per-IP Shaper	<input style="width: 50px;" type="text" value="+"/>
Comments	<input style="width: 100%;" type="text"/>

Esto nos permitirá limitar el ancho de banda en las políticas. En caso de habilitar Shared Shaper se limitará la subida o el tráfico saliente y en caso de que sea Reverse Shaper limitará la descarga o el tráfico entrante.

También existe la posibilidad de limitarlo para una ip en concreto y no para todos los objetos que entren dentro de esa regla. Para su elección disponemos de Shapers ya creados por defecto o en caso de querer crear uno podremos hacer click en el “+” de arriba a la derecha.

Traffic Shaper + - ✎ □ ✕

🔍

SHARED SHAPER (5) ▼

◆ **guarantee-100kbps**
Guaranteed: 100 Kbps, Maximum: 1048576 Kbps, Traffic Priority: H...

◆ **high-priority**
Guaranteed: 0 Kbps, Maximum: 1048576 Kbps, Traffic Priority: High

◆ **low-priority**
Guaranteed: 0 Kbps, Maximum: 1048576 Kbps, Traffic Priority: Low

◆ **medium-priority**
Guaranteed: 0 Kbps, Maximum: 1048576 Kbps, Traffic Priority: Med...

◆ **shared-1M-pipe**
Guaranteed: 0 Kbps, Maximum: 1024 Kbps, Traffic Priority: High

Entonces se nos abrirá una ventana para la creación de un nuevo Shaper.

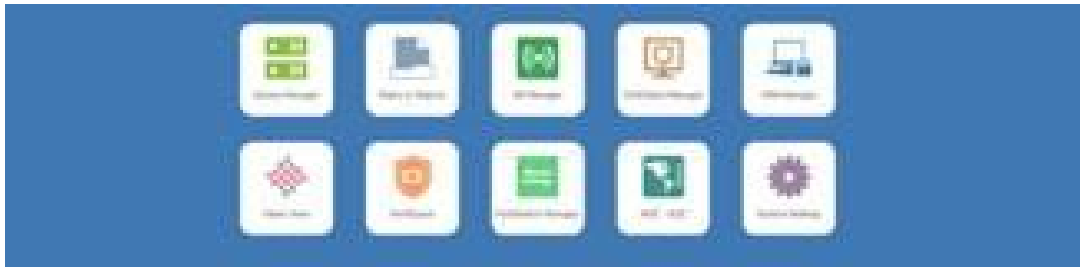
Para su configuración lo único que necesitamos es asignarle un nombre y dos anchos de banda. Uno de ellos es el “Guaranteed Bandwidth” que nos permitirá establecer un ancho de banda mínimo, es decir, la política que tenga dicho shaper asociado dispondrá siempre de un bando de ancho garantizado a su elección. El otro es “Maximum Bandwidth” que limitará el ancho de banda de la regla que lo tenga asociado a la elegida.

Create New Shared Traffic Shapers

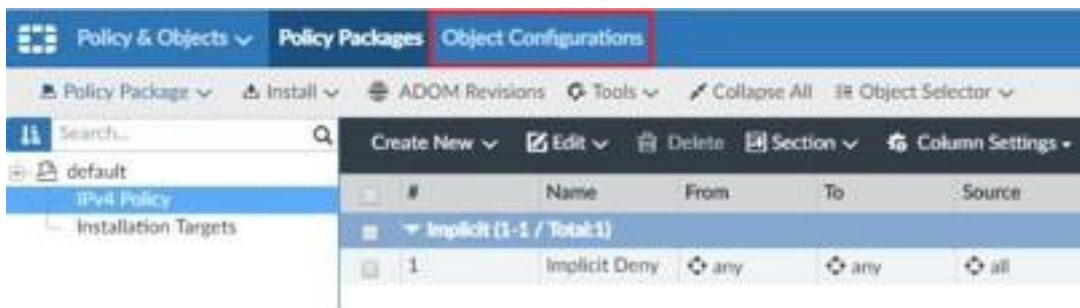
Name	<input type="text"/>
Apply Shaping	<input type="radio"/> Per Policy <input checked="" type="radio"/> For all policies using this shaper
Bandwidth Unit	<input type="button" value="Kbps"/> <input type="button" value="Mbps"/> <input type="button" value="Gbps"/>
Guaranteed Bandwidth (G - 16776000)	<input type="text" value="0"/>
Maximum Bandwidth (G - 16776000)	<input type="text" value="0"/>
Traffic Priority	<input type="button" value="High"/> <input type="button" value="Medium"/> <input type="button" value="Low"/>
<input type="checkbox"/> DSCP (000000 - 1111111)	<input type="text" value="000000"/>

1.9. Creación de usuarios y grupos locales

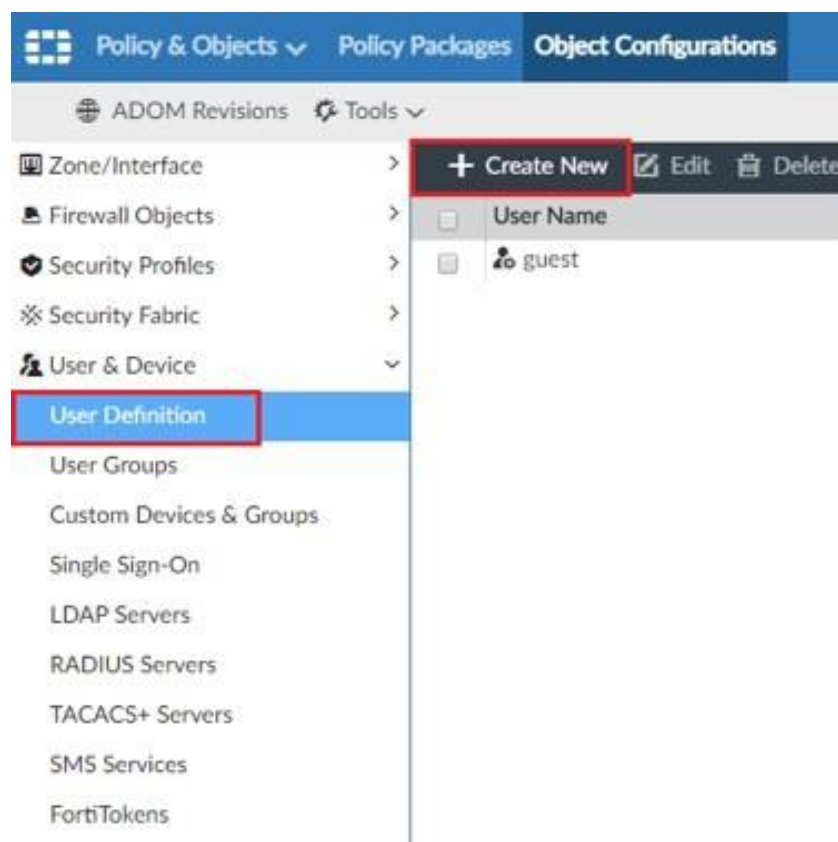
1. Seleccionar en el menú principal la opción de “Policy & Objects”.



2. Seleccionar en el menú superior la opción “Object Configurations”.



3. En el menú lateral izquierdo elegimos la opción de “User definition” primeramente para crear un usuario y hacemos click en “Create New”.



4. Una vez abierto el menú para crear el usuario introduciremos:

- En el campo de Type, el tipo de usuario, local por defecto.
- En el campo de User Name el nombre del usuario asociado.
- En el campo de Password la contraseña asociada a dicho usuario

The screenshot shows the 'Create New Local User' interface. It features a tabbed interface for user types: LOCAL (selected), LDAP, RADIUS, and TACACS+. Below the tabs are input fields for 'User Name' and 'Password', and a 'Disable' checkbox. The 'Contact info' section includes an 'Email' field and an 'SMS' section with radio buttons for 'FortGuard Messaging Service' (selected) and 'Custom'. Below this are 'Country/Region' and 'Phone Number' fields. The 'Two-factor Authentication' section has radio buttons for 'Disable' (selected), 'FortToken', 'Email based two-factor authentication', and 'SMS based two-factor authentication'. At the bottom, there is an 'Add To Groups' section with a 'Click here to select' button and an 'Advanced Options' link.

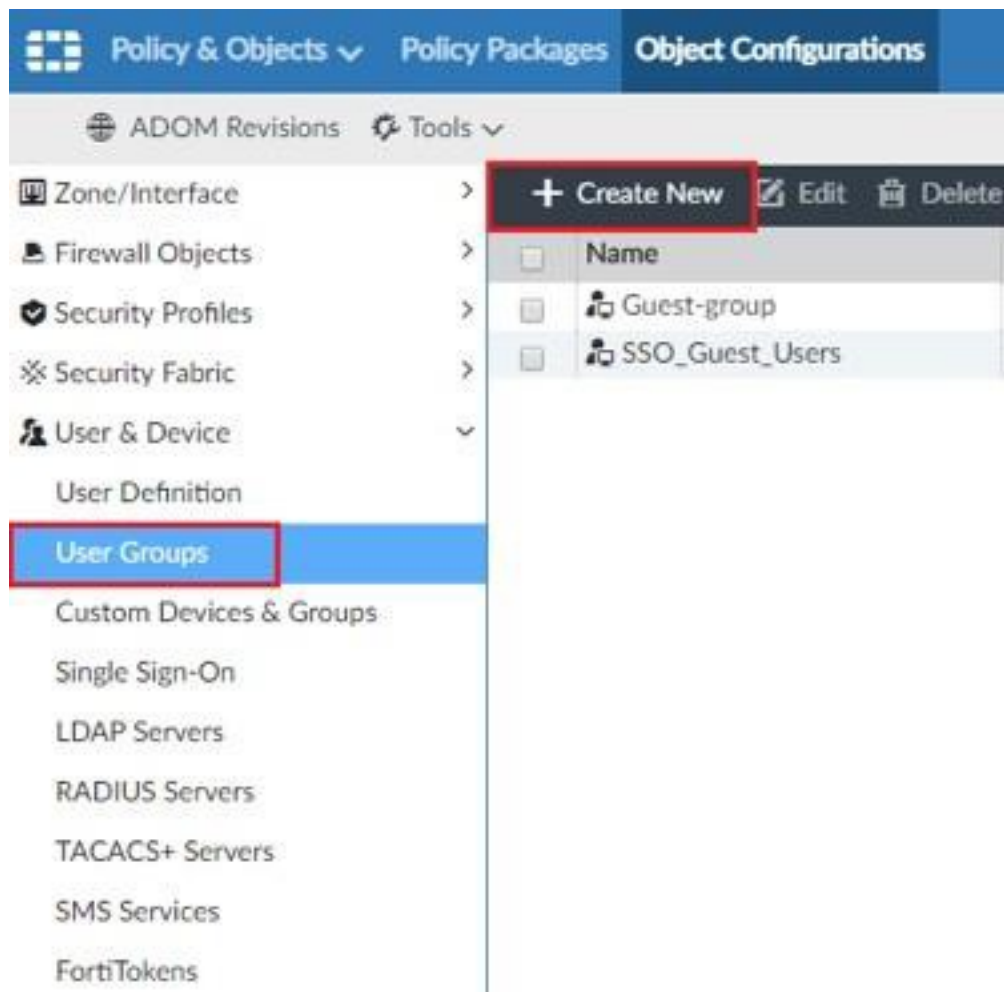
El resto de los campos se obviarán por ahora.

5. Por último, haremos click en OK para finalizar la creación del usuario.

6. Para la segunda parte, la creación de grupos, nos situaremos de nuevo en la pestaña en la que estábamos antes, donde elegimos User definition, pero en este caso elegiremos User Groups y haremos click en Create New.

7. Aquí solo tendremos que especificar un nombre para el grupo en el campo "Group Name" y los miembros de dicho grupo en el campo "Members".

8. Por último hacemos click en OK y el grupo se crearía.



1.10. Configuración URL Filtering

Este módulo nos permitirá definir a qué páginas de internet pueden navegar nuestros usuarios y cuales tendrán denegadas. Podremos aplicar este filtrado por categoría de página y también podremos crear varios perfiles de navegación: básica, avanzada o navegación VIP.

1. Seleccionar en el menú principal la opción de "Policy & Objects".
2. En la barra superior elegir la opción de "Object Configurations".
3. En el menú lateral izquierdo elegir "Web Filter", dentro de "Security Profiles" y hacemos click en "Create New".
4. Una vez estamos creando un nuevo filtro habilitamos las siguientes opciones:
 - FortiGuard Categories: esto permitirá o bloqueará ciertas páginas en

función de la categoría que tengan asociada por Forti.

Create New Web Filter Profile

Advanced Options >

Inspection Mode: **Proxy** Flow-based

Log all URLs

FortiGuard Categories

Expand All Collapse All All

<input type="checkbox"/>	Category	Authenticate
<input type="checkbox"/>	Local Categories	
<input type="checkbox"/>	Potentially Liable	
<input type="checkbox"/>	Adult/Mature Content	
<input type="checkbox"/>	Bandwidth Consuming	
<input type="checkbox"/>	Security Risk	
<input type="checkbox"/>	General Interest - Personal	
<input type="checkbox"/>	General Interest - Business	
<input type="checkbox"/>	Unrated	

+ Create Edit Delete

- URL Filter: aquí incluiremos URL's especificadas y creadas por nosotros pudiendo indicar la acción que queremos que se haga: allow, que la permitirá; block, que la bloqueará; monitor, que la monitorizará y exempt, que lo que hace es pasar por alto cualquier acción adicional en la lista de filtros para toda conexión que coincida con el dominio en la entrada URL.

Static URL Filter

Block Invalid URLs

URL Filter

Select an URL Filter [Create New]

+ Add Edit Delete Move Up Move Down

#	URL	Type	Action	Referrer Host	Status
---	-----	------	--------	---------------	--------

Block malicious URLs discovered by FortiSandbox

Web Content Filter

URL Filter Entries

Entry	->
URL	<input type="text"/>
Type	simple
Action	exempt
Referrer Host	<input type="text"/>
Enable	<ul style="list-style-type: none"> allow block exempt monitor

Cancel

- Allow Websites When a Rating Error Occurs: se recomienda habilitar para permitir el acceso a páginas web que devuelven un error de clasificación del servicio de filtro web FortiGuard. Si su unidad FortiGate no puede ponerse en contacto con el servicio FortiGuard temporalmente, esta configuración determina qué acceso permite la unidad FortiGate hasta que se restablezca el contacto. Si está habilitado, los usuarios tendrán acceso completo sin filtros a todos los sitios web. Si está desactivado, los usuarios no podrán acceder a ningún sitio web.

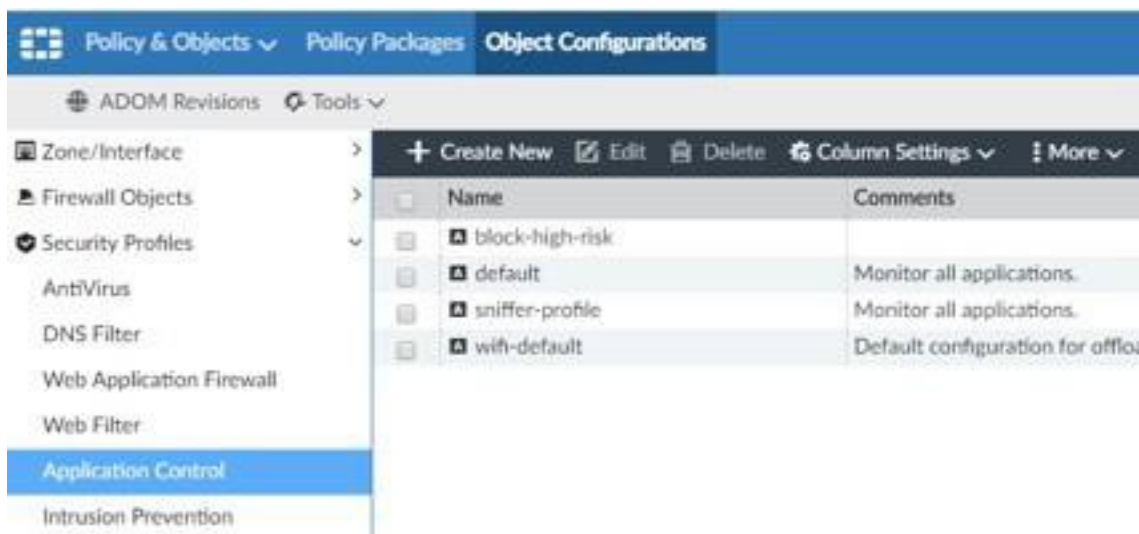
Rating Options

- Allow Websites When a Rating Error Occurs
- Rate URLs by Domain and IP Address
- Rate Images by URL (Blocked images will be replaced with blanks)

1.11. Configuración Control de aplicaciones

El control de aplicaciones de Fortinet protege equipos y servidores permitiendo y denegando el uso de aplicaciones basándose en políticas establecidas por el administrador de la red.

1. Para acceder a la configuración del Control de Aplicaciones, dentro de “Policy & Objects” → “Object Configurations” y en el panel izquierdo seleccionamos “Security Profiles” → “Application Control”.



En esta pantalla podemos ver todos los perfiles de Control de aplicaciones, si queremos editar alguno, hacemos click encima del perfil y seleccionamos el botón “Edit”. Para crear un perfil nuevo, seleccionamos el botón “Create New”.

2. Una vez dentro de la configuración inicial, distinguimos los campos siguientes:

- Name: el nombre del perfil.
- Categories: se selecciona la acción para cada una de las categorías: Allow, Monitor, Block, Traffic Shaping, Quarantine, or Reset.
- Application Overrides: permite seleccionar aplicaciones individuales.
- Filter Overrides: permite seleccionar grupos de aplicaciones y anular la configuración de la firma de la aplicación para ellas.
- Deep Inspection of Cloud Applications: realizar una inspección profunda de aplicaciones en la nube.
- Allow and Log DNS Traffic: permitir y registrar el tráfico DNS.
- Replacement Messages for HTTP-based Applications: mensajes de reemplazo para aplicaciones basadas en HTTP.

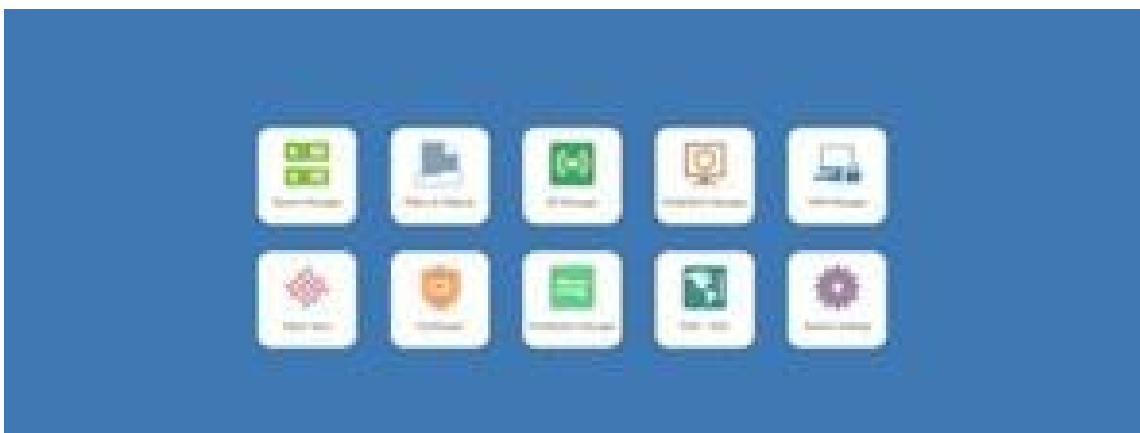


1.12. Configuración IPS

La configuración del protocolo IPS (Intrusion Prevention System), nos permitirá proteger nuestra red de ataques externos. Un IPS es un sistema de prevención/protección contra las intrusiones y no solo para reconocerlas e informar acerca de ellas. El IPS tiene la habilidad de bloquear inmediatamente las intrusiones, sin importar el protocolo de transporte empleado y sin reconfigurar un dispositivo externo. Esto significa que el IPS puede filtrar y bloquear paquetes de manera nativa (al utilizar técnicas como la caída de una conexión, la caída de paquetes ofensivos, el bloqueo de un intruso, etc.).

En este protocolo se lleva a cabo una defensa basada en firmas contra ataques o vulnerabilidades conocidas. El atacante en estos casos tratará de comunicarse con un host para ganar acceso al mismo, para lo cual hará uso de una serie de comandos particulares. Las firmas IPS incluyen estos comandos, de forma que permiten al Fortigate detectar y parar el ataque.

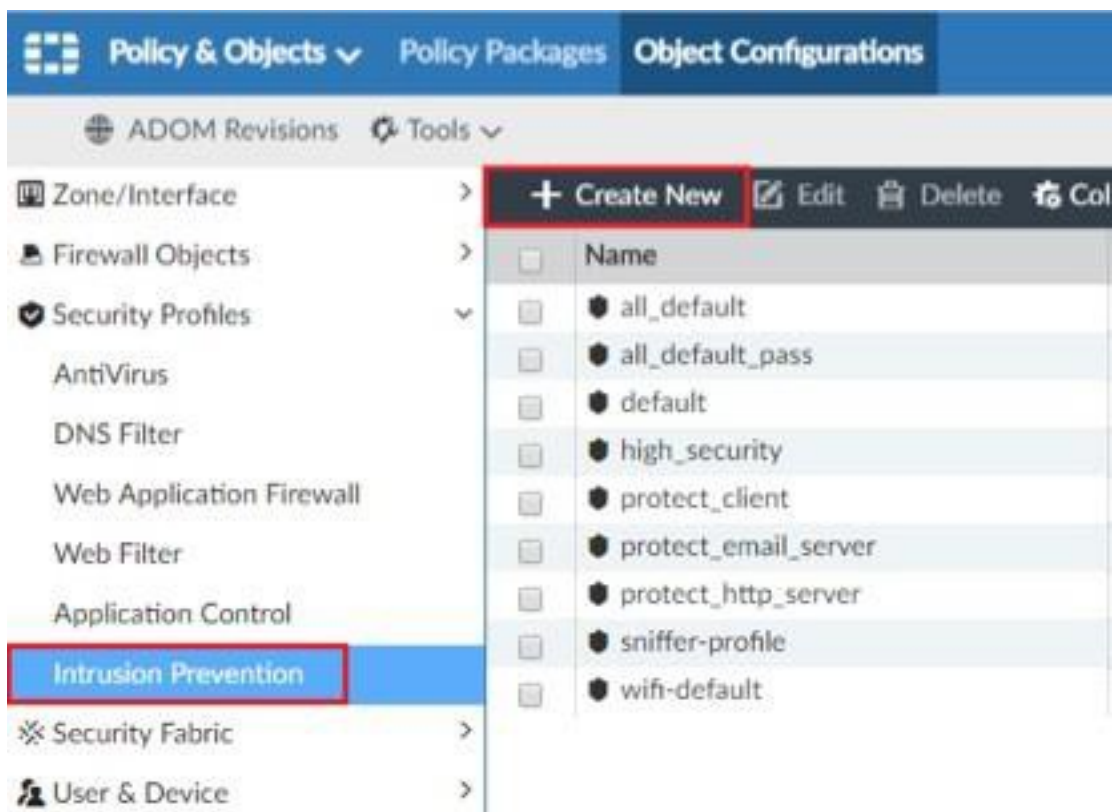
1. Seleccionar en el menú principal la opción de “Policy & Objects”.



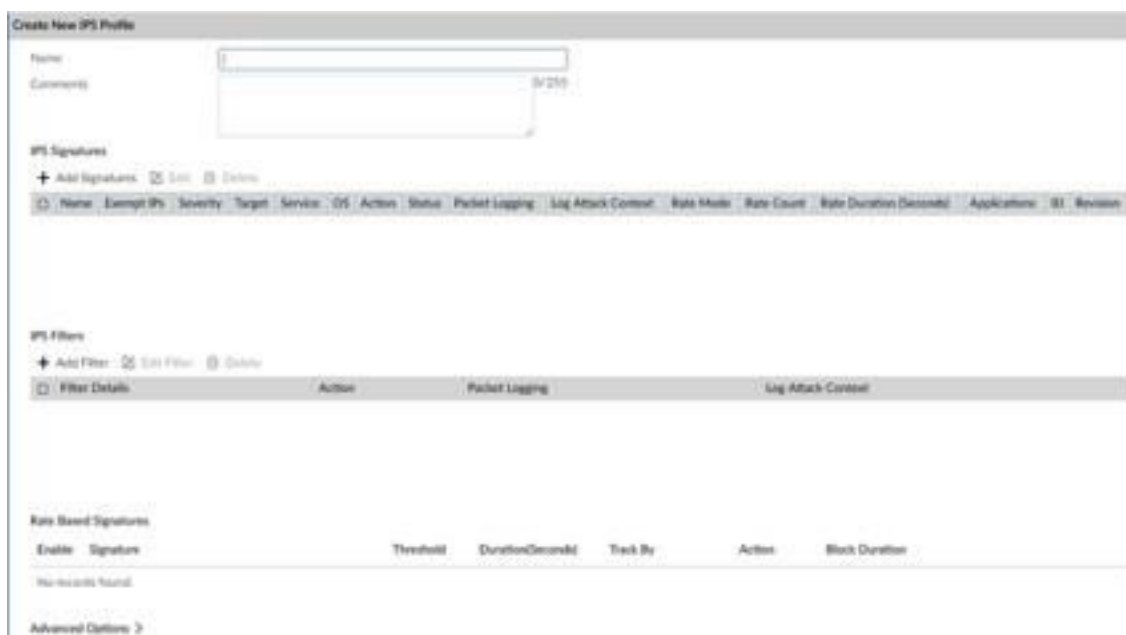
2. En la barra superior elegir la opción de “Object Configurations”.



3. En el menú lateral izquierdo hacemos click en “Intrusion Prevention”, dentro de la categoría de “Security Profiles” y pulsamos “Create New”.



4. Los campos que tenemos para configurar un perfil IPS serían los siguientes:



- Name: Donde indicaremos el nombre del escaner IPS.
- Comment: en caso de querer establecer algún comentario.
- IPS Signatures: para añadir una firma hacer click en Add Signatures. Estas firmas nos permiten proteger los equipos frente a ciertas amenazas concretas. Dichas firmas se actualizan automáticamente. En el caso de ejemplo disponemos de casi 13000 firmas.

Agregar Firmas

Nombre	Severidad	Objetivo	DB	OS	Servicio	Acción	Estado	CVE-ID	
3D-Link (AD) Local Buffer Overflow (PoC)	medium	server-client	Industrial	Windows	TCP HTTP FTP	Block	enable		
32Bit DNS Spoofing (NTP File Pollution)	high	server	Extended	Windows, Linux, BSD	TCP HTTP	Block	enable		
3Ware Windows Router XDR Password Reset	medium	server-client	Extended	Linux	TCP HTTP	Block	enable	CVE-2007-438	
3CX Phone System W3, Desktop Address & File Upload	high	server	Extended	Windows	TCP HTTP	Block	enable		
3Com 3C-Dxpress F79 Server Buffer Overflow	high	server	Regular, Extended	Windows	TCP FTP	Block	enable	CVE-2009-007	
3Com 3C-Dxpress F79 Server Information Disclosure	low	client	Regular, Extended	Windows	TCP FTP	Block	enable	CVE-2009-007	
3Com Intelligent Management Center Information	medium	server	Regular	Extended	Windows	TCP HTTP	Block	enable	
3Com OfficeConnect K95B Wireless Ethernet Router	medium	server	Regular, Extended	Linux	TCP FTP	Block	enable		
3DLife Player WinPlayer Attack Control Buffer Overflow	high	client	Extended	Windows	TCP HTTP	Block	enable		
3P-Proxy VMS ActiveX Control Buffer Overflow	medium	client	Extended	Windows	TCP HTTP	Block	enable	CVE-2014-4300	
3P-Smart (OOBE) DNS Gateway Server Directory Traversal	high	server-client	Industrial	Windows	TCP	Block	enable	CVE-2013-4707	
3P-Smart (OOBE) DNS Gateway Smart DNS	high	server-client	Industrial	Windows	TCP	Block	enable	CVE-2013-4708	
3P-Smart (OOBE) DNS Gateway Server Heap Buffer Overflow	high	server	Industrial	Windows	TCP	Block	enable	CVE-2013-4709	
3P-Smart (OOBE) DNS Gateway Server Integer Overflow	high	server	Regular, Extended	Windows	TCP	Block	enable	CVE-2013-0005	
3P-Smart (OOBE) DNS Gateway Server Primary Access	critical	server-client	Industrial	Windows	TCP	Block	enable	CVE-2012-4700	
3P-Smart (OOBE) DNS Gateway Server Remote Heap Overflow	critical	server-client	Industrial	Windows	TCP	Block	enable	CVE-2012-4706	
3P-Smart (OOBE) DNS Gateway Server Stack Buffer Overflow	critical	server-client	Industrial	Windows	TCP	Block	enable	CVE-2012-4705	
3P-Smart (OOBE) DNS Web Service Buffer Overflow	critical	server	Industrial	Windows	TCP HTTP	Block	enable	CVE-2012-4700	
3P-Smart (OOBE) DNS Web Service LibStack Buffer Overflow	high	server	Industrial	Windows	TCP HTTP	Block	enable	CVE-2012-4700	

Version: 34.635 DB: Regular, Extended, Industrial Total: 97

- IPS Filters: hacer click en Add Filter. Las firmas están incluidas en los filtros, de forma que en función del filtro que elijamos, se aplicarán unas firmas u otras. Se recomienda perfilar bien los filtros de forma que no se consulten firmas innecesarias. En este ejemplo hemos elegido como filtro que el OS sea Windows y el protocolo DNS, aplicándose 97 firmas.

Agregar Firmas

Nombre	Severidad	Objetivo	DB	OS	Servicio	Acción	Estado	CVE-ID
ADAM exploit	critical	server	Regular, Extended	AS	UDP DNS	Block	enable	
Backdoor/Callback In-File Execution	high	server-client	Regular, Extended	Windows	TCP HTTP SSL SMB	pass	enable	
Backdoor/Server	high	server-client	Regular, Extended	AS	TCP HTTP UDP DNS	Block	enable	
Backdoor/Server	critical	client	Regular, Extended	AS	TCP HTTP UDP DNS	Block	enable	
DCT Data Corruption	low	server	Extended	AS	ICMP UDP DNS	Block	enable	
DNS Amplification/Reflection	low	server-client	Regular, Extended	AS	UDP DNS	pass	enable	
DNS Amplified Denial of Service/Attack	low	server	Extended	Windows	UDP DNS	Block	enable	CVE-2009-1847
DNS Flood/Flooding	low	client	Regular, Extended	AS	UDP DNS	Block	enable	
DNS Spoofed Label Length	info	server	Extended	AS	TCP DNS	pass	disable	
DNS Spoofed IP/Port	info	server	Extended	AS	TCP DNS	pass	disable	
DNS Spoofed Parameters	low	server	Extended	AS	TCP DNS	pass	disable	
DNS Spoofed Pointer	low	server	Extended	AS	TCP DNS	pass	disable	
DNS Spoofed Compression/Recursive Data	high	server	Regular, Extended	Windows, Linux	TCP UDP SMB	pass	enable	CVE-2007-1800
DNS Name Overflow	low	client	Extended	AS	TCP DNS	pass	disable	
DNS Overload/Message	low	server	Extended	AS	TCP DNS	pass	enable	
DNS Poison/Cache	high	server	Regular, Extended	AS	TCP DNS	pass	enable	CVE-2010-1846
DNS Reverse Address Lookup Spoofing	medium	client	Extended	Windows	UDP DNS	Block	enable	CVE-2009-0892
DNS Server Response Spoofing	medium	server-client	Regular, Extended	Windows	UDP DNS	Block	enable	CVE-2007-3895
DNS Spoofing/Attack	high	client	Regular, Extended	AS	UDP DNS	Block	enable	CVE-2009-1847

Version: 34.635 DB: Regular, Extended, Industrial Total: 97


Por último, tenemos una lista de firmas en las que hay que especificar un umbral de tiempo y una duración. De esta forma se bloqueará solo en caso de cumplir estos campos.

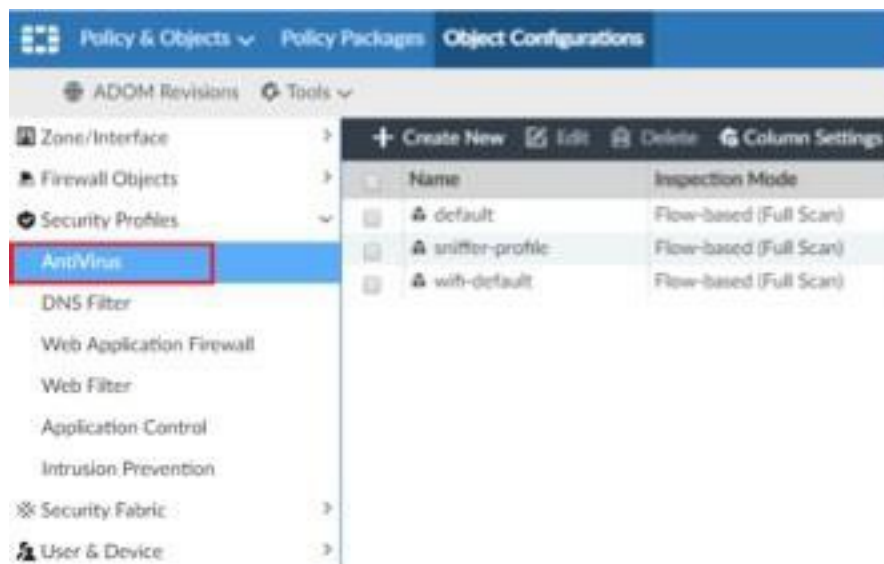
Enable	Signature	Threshold	Duration(Seconds)	Track By	Action	Block Duration
<input type="checkbox"/>	Digipun.AlertInfo.File.Description.Dns	20	1	Any	Block	None
<input type="checkbox"/>	Digipun.AlertInfo.MX2.Call.Number.Dns	275	1	Any	Block	None
<input type="checkbox"/>	DnsPortProbe.Pooping/Doxxing/Attack	1000	5	Any	Block	None
<input type="checkbox"/>	FTP.Login.Brute.Force	200	10	Any	Block	None
<input type="checkbox"/>	FlowSIGTCP.Reassembly.Dns	10	2	Any	Block	None
<input type="checkbox"/>	IMAP.Login.Brute.Force	40	10	Any	Block	None
<input type="checkbox"/>	MS.Active.Directory.LDAP.Packet.Handling.Dns	100	1	Any	Block	None
<input type="checkbox"/>	MS.DNS.Brute.Force	15	1	Any	Block	None
<input type="checkbox"/>	MS.POP.Connection.Brute.Force	200	10	Any	Block	None
<input type="checkbox"/>	MS.Windows.Group.Policy.Security.Feature.Bypass	1	2	Any	Block	None

5. Para terminar, hacer click en OK.

1.13. Configuración perfiles antivirus para navegación

La protección Antivirus se encarga de detectar, desinfectar y/o eliminar códigos maliciosos, con actualizaciones en tiempo real para proteger contra nuevos ataques. Está certificado por ICISA Network Antivirus y es capaz de analizar los siguientes protocolos: HTTP, SMTP, POP3, IMAP, MAPI, FTP y IM.

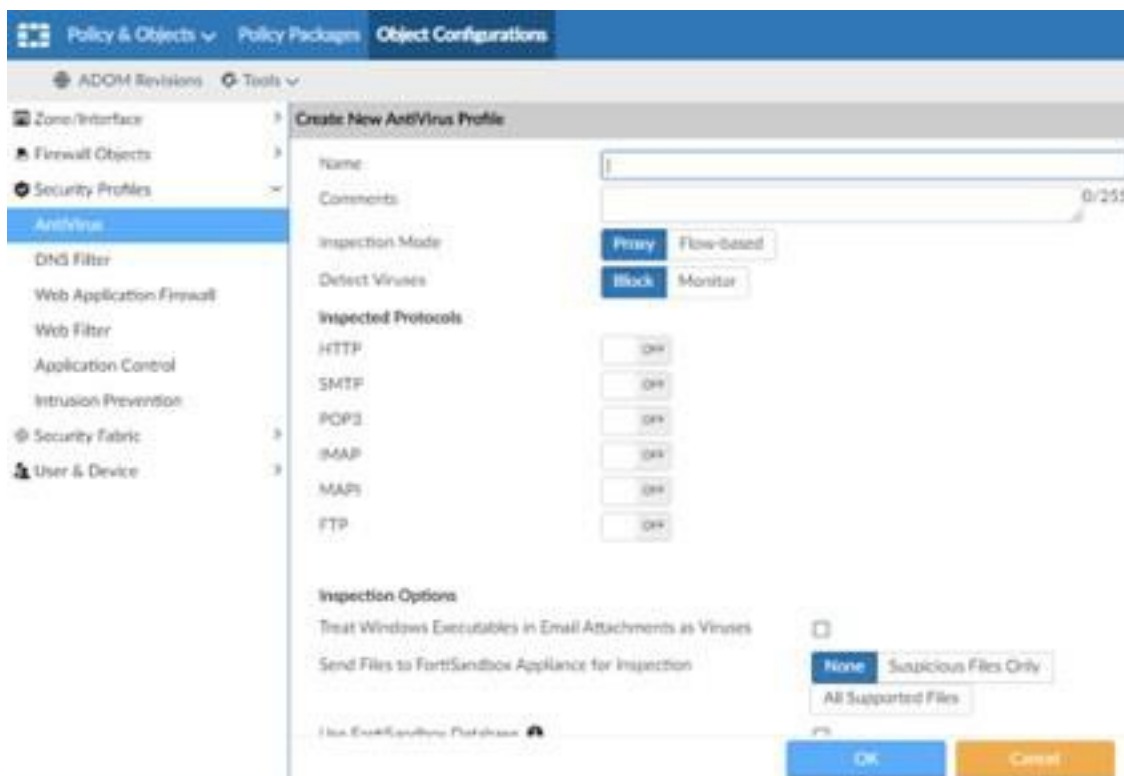
1. Para acceder a la configuración del Antivirus, dentro de “Policy & Objects”  “Object Configurations” y en el panel izquierdo seleccionamos “Security Profiles” “Antivirus”.



En esta pantalla podemos ver todos los perfiles de seguridad, si queremos editar alguno, hacemos click encima del perfil y seleccionamos el botón “Edit”. Para crear un perfil nuevo, seleccionamos el botón “Create New”.

2. Una vez dentro de la configuración inicial, distinguimos los campos siguientes:

- Name: nombre identificativo del perfil que estamos creando.
- Inspection Mode: por defecto "Proxy".
- Detect Viruses: tenemos dos opciones, "Block" o "Monitor".
- Seleccionamos los protocolos que queremos analizar.



1.14. Configuración VPN SSL

Una VPN SSL permitirá a usuarios remotos acceder a la red de la empresa. Esta conexión se hará vía web o mediante un túnel utilizando FortiClient.

El modo web permitirá a los usuarios acceder a los recursos de la red sin necesidad de un cliente pesado, solo con un navegador web.

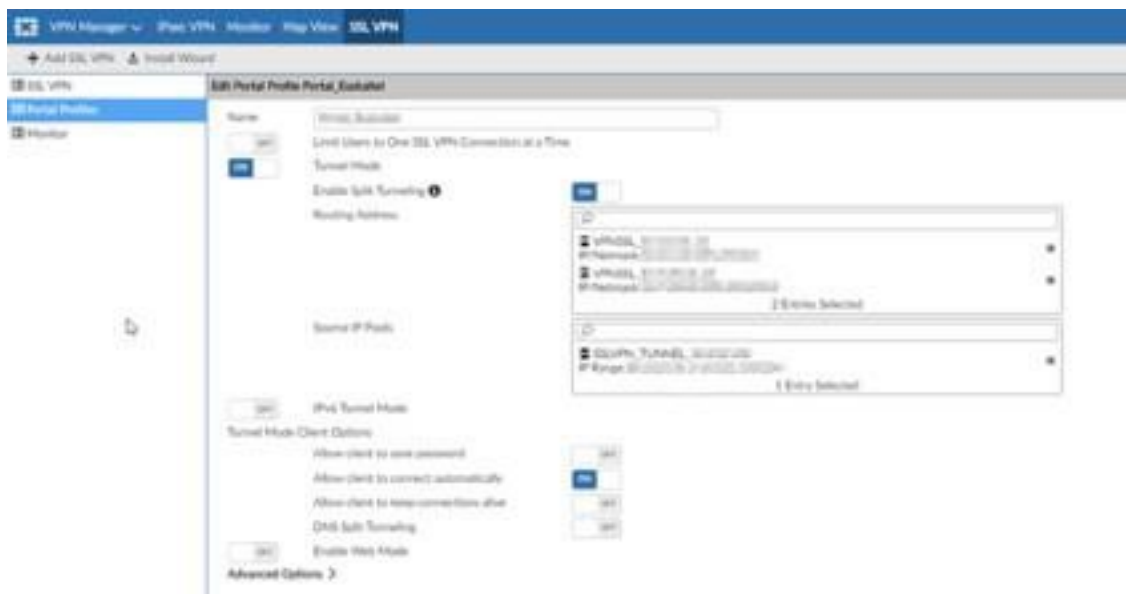
Para los usuarios que se conecten mediante el modo túnel, será necesario instalar un cliente pesado llamado Forticlient para poder realizar esta conexión. Se podrá configurar Split – tunnel para evitar el paso de la navegación a internet del usuario por el FW, de modo que no sobrecargue la red.

1. Para configurar una VPN SSL en primer lugar, nos dirigimos al menú principal y seleccionamos "VPN Manager", en el menú superior pulsamos el botón "SSL VPN" y hacemos click en Portal Profiles y luego en CreateNew.



2. Si habilitamos Tunnel Mode:

- Split Tunneling. Permite que las conexiones a internet del usuario vayan por fuera del túnel de modo que puedes configurar un proxy para la navegación.
- Routing Address: aquí indicamos routing que se nos asignará una vez conectados a la VPN
- Source IP Pools: Aquí se indica el rango de direccionamiento que se asignará a los clientes conectados a la VPN.



Si habilitamos Web Mode:

- Portal Message: Breve descripción del portal al que se conectan los usuarios.
- Show Session information: marcar si queremos que se muestre información de la sesión al usuario remoto
- Show connection launcher: marcar si queremos añadir la herramienta de conexión a los usuarios remotos
- Show login history: marcar si queremos mostrar el historial a los usuarios remotos
- User bookmarks: Se indican los accesos rápidos a determinados recursos para cada portal de VPN creado. Para crear los marcadores pincharemos sobre "Create New"

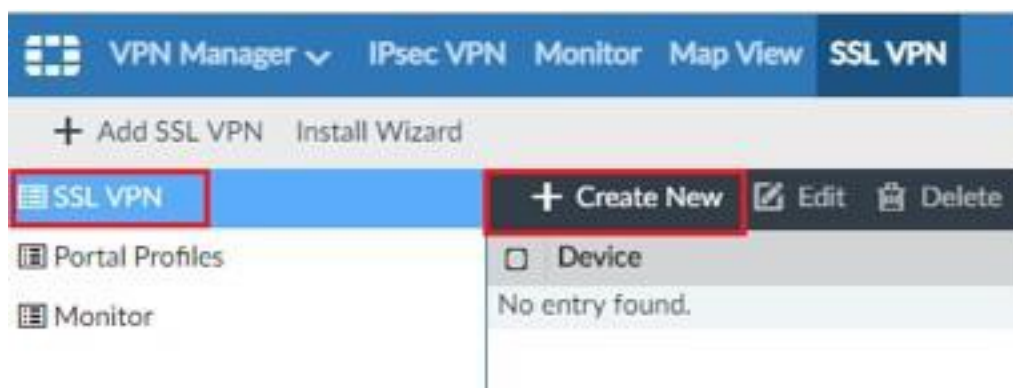
Create New Bookmark

Name	<input type="text" value="Bookmark"/>
Type	<input type="text" value="HTTP/HTTPS"/>
URL	<input type="text"/>
Description	<input type="text"/>
Single Sign-On	<input checked="" type="radio"/> Disabled <input type="radio"/> Automatic <input type="radio"/> Static

OK

Cancel

- Enable FortiClient Download: marcar si queremos mostrar el link de descarga del software FortiClient.
3. Nos dirigimos al menú principal y seleccionamos “VPN Manager”, en el menú superior pulsamos el botón “SSL VPN” y hacemos click en SSL VPN y luego en Create New.



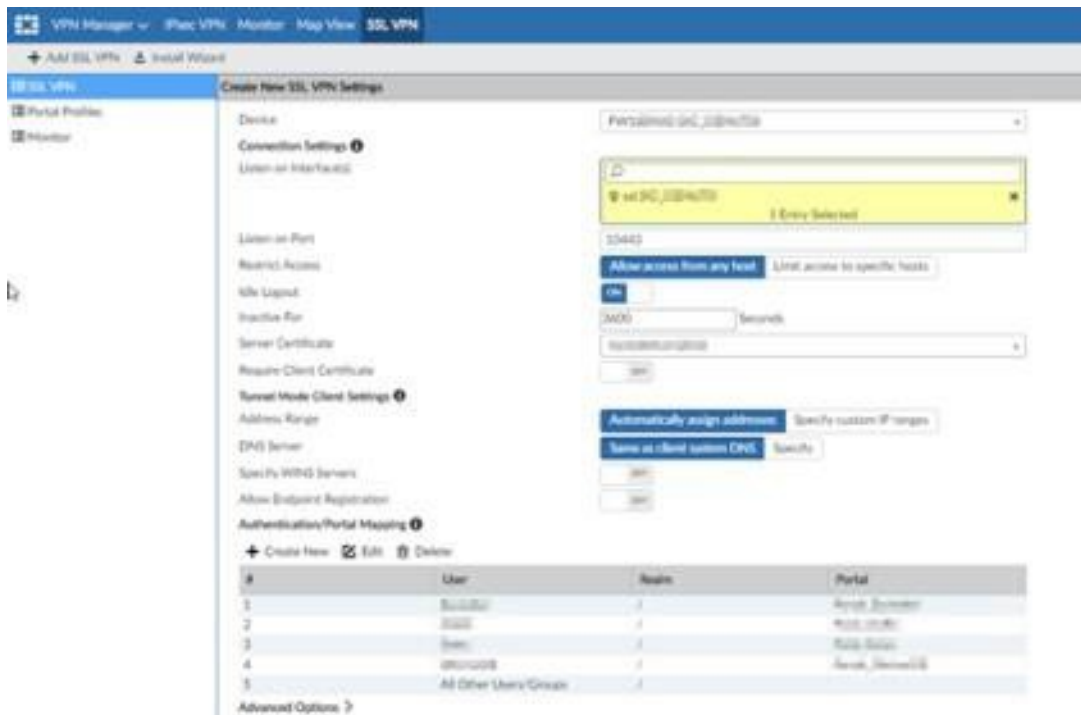
4. Para realizar la configuración inicial tenemos que indicar la siguiente información:

- Device: seleccionar un dispositivo manejado por el FortiManager.
- Listen on Interface: definir la interfaz que Fortigate va a usar para escuchar las peticiones SSL VPN. Generalmente es la propia interfaz externa.
- Listen on Port: añadir el número de puerto para el acceso HTTPS.
- Restrict Access: limitar el acceso a hosts específicos en caso de así quererlo.
- Idle Logout: si seleccionamos la opción “on”, debemos indicar la cantidad de tiempo que la conexión puede estar inactiva antes de realizar el logout del usuario.

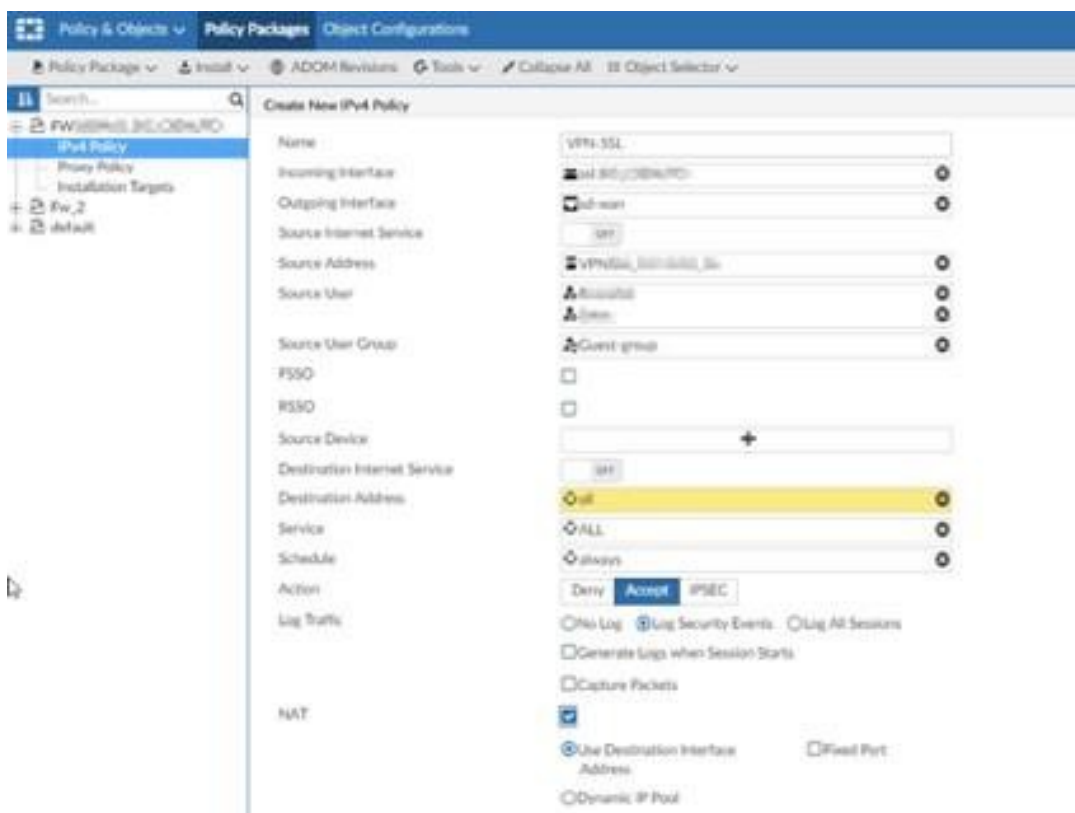
En cuanto a la configuración del “Modo túnel”, tenemos que especificar la información de los siguientes campos:

- Address Range: podemos escoger el rango automático o personalizado.
- DNS Server: podemos seleccionar el mismo DNS que el sistema del cliente o uno específico.

- Specify WINS Servers: si seleccionamos la opción "on", podemos especificar los servidores WINS.
- Authentication/Portal Mapping: aquí indicamos los usuarios que tendrán acceso a dicha VPN, y el portal al que tendrán acceso.



5. Por último, debemos crear una regla de seguridad para el acceso remoto. Para ello vamos a Policy & Objects y hacemos click en Create New:



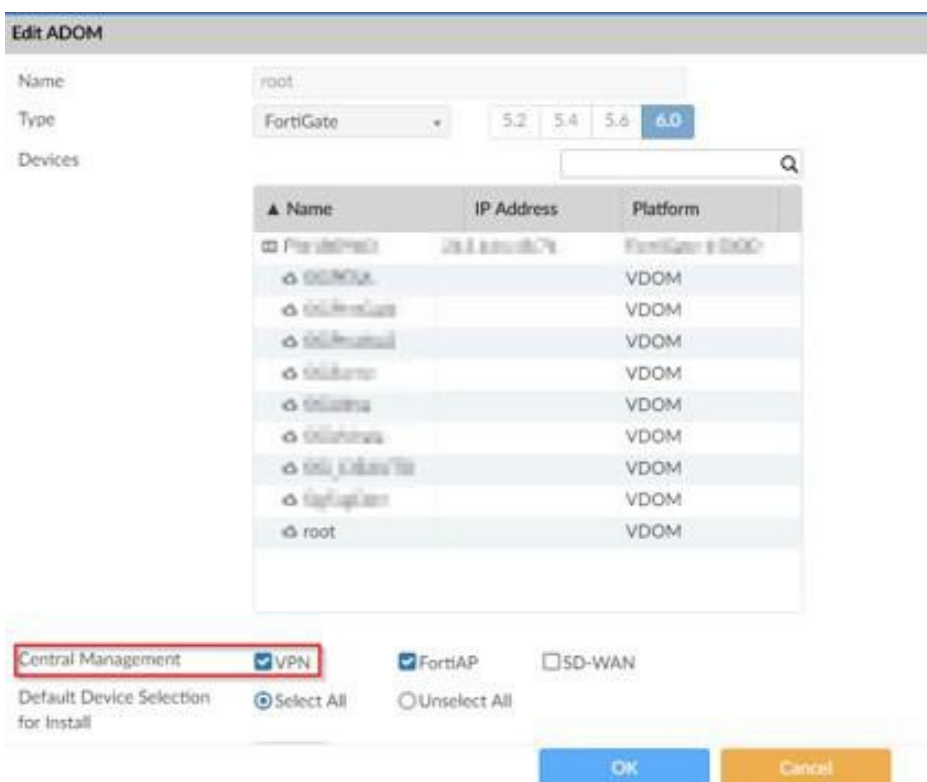
- Name: nombre de la regla de la VPN.
- Incoming interface: interfaz virtual SSL.
- Outgoing interface: interfaz local a la que acceden los usuarios remotos.
- Source Address: objeto con el pool de usuarios remotos.
- Source user: usuarios que queremos que accedan a la red.
- Source user group: grupo de usuarios que queremos que accedan a la red.
- Destination address: dirección de la red local a la que acceden los usuarios remotos.
- NAT: si se habilita se usará la dirección IP de la interfaz de salida.

En esta regla se puede filtrar los accesos por usuario si se quiere restringir para determinados usuarios.

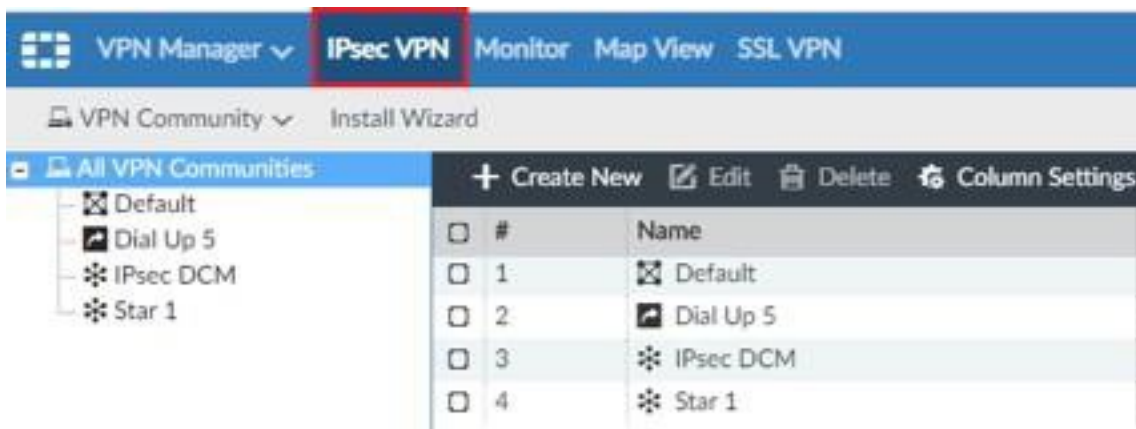
1.15. Configuración VPN IPSEC

IPsec es un protocolo de VPN que se usa para proteger la comunicación por internet a través de una red IP. Se establece un túnel en un sitio remoto que permite el acceso a tu sitio central. Una IPsec funciona protegiendo la comunicación del protocolo de internet verificando cada sesión y codificando individualmente los paquetes de datos durante la conexión.

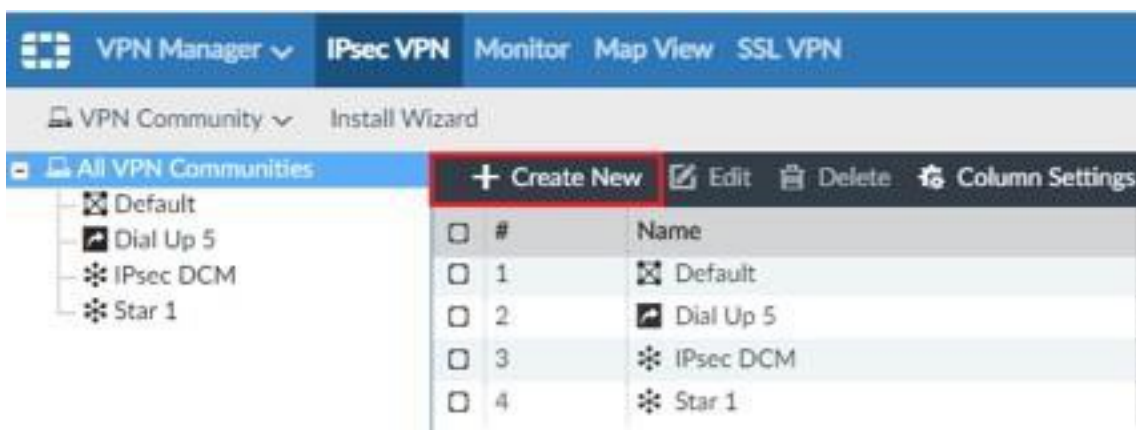
1. Antes de pasar a la configuración de la VPN, tenemos que dirigirnos a “System Settings” y en el menú izquierdo seleccionar el apartado “All ADOMs”. Activamos la opción “VPN” en “Central Management”.



2. Para configurar una VPN IPSEC en primer lugar, nos dirigimos al menú principal y seleccionamos “VPN Manager”, en el menú superior pulsamos el botón “IPsec VPN”.



3. En este menú podemos ver las distintas VPNs ya creadas, las cuales podemos editar pinchando encima y pinchando en el botón “Edit”. También podemos crear una seleccionando el botón “Create New”.



4. En esta primera ventana tenemos que indicar el nombre, opcionalmente una descripción y escogemos la topología de la VPN. Tenemos tres opciones:

- Full Meshed: cada puerta tiene un túnel para todas las demás puertas.
- Star: cada puerta tiene un túnel hacia un hub central.
- Dial Up: algunas puertas, a menudo usuarios móviles, tienen direcciones IP dinámicas y se ponen en contacto con la puerta para establecer el túnel.

Una vez escogida esta configuración, le damos a next.

VPN Topology Setup Wizard

Name:

Description:

Choose VPN Topology

Full Meshed
 Star
 Dial up

5. Ahora tenemos que configurar la información de la autenticación y encriptación para la topología escogida, para ello se hace uso del protocolo IKE. Una vez escogida, seleccionamos next.

VPN Topology Setup Wizard

Authentication & Encryption Settings:

Authentication

Generate (random)
 Specify

Encryption

IKE Security (Phase 1) Properties

IKE Version:

#	Encryption	Authentication
Click here to add a new entry. <input type="button" value="+"/>		

IPsec Security (Phase 2) Properties

#	Encryption	Authentication
Click here to add a new entry. <input type="button" value="+"/>		

6. Por último, tenemos que configurar la Zona VPN, escogiendo entre crear una zona predeterminada o personalizada. También hay que personalizar las Propiedades avanzadas de IKE Security Phase 1 y 2. Volvemos a seleccionar el botón next.

VPN Topology Setup Wizard

VPN Zone On

Create Default Zones

Use Custom Zone

IKE Security Phase 1 Advanced Properties

Diffe-Hellman Group(s) 1 2 5 14 15 16
 17 18 19 20 21 27
 28 29 30 31

Exchange Mode Aggressive Main(DD Protection)

Key Life (120-172800 seconds)

Dead Peer Detection Disable On Idle On Demand

IPsec Security Phase 2 Advanced Properties

Diffe-Hellman Group(s) 1 2 5 14 15 16
 17 18 19 20 21 27
 28 29 30 31

7. Nos aparecerá una última ventana con toda la información que hemos ido personalizando, revisamos que este todo correcto y para terminar seleccionamos el botón OK.

VPN Topology Setup Wizard

Summary

Name Prueba

Topology Star

Authentication Pre-shared Key (Generic)

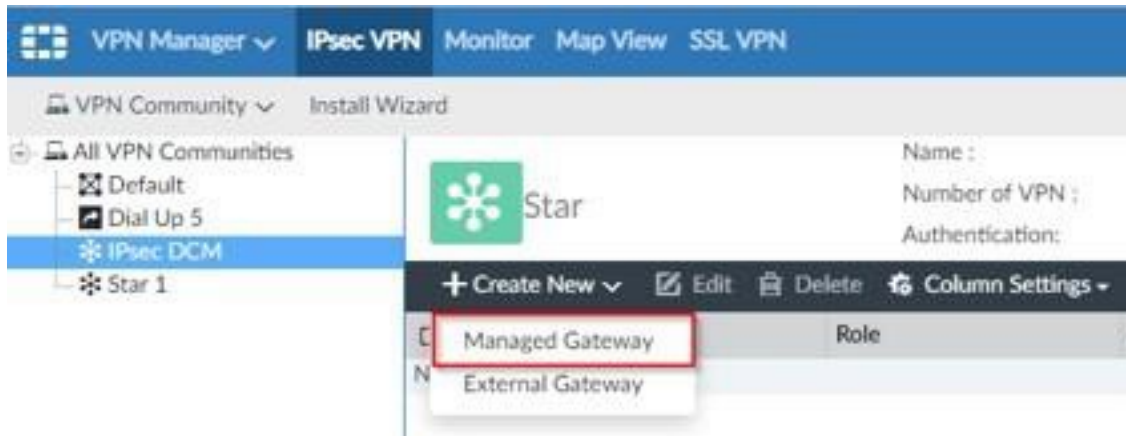
Encryption IKE Security (Phase 1) Properties

- Diffie-Hellman Groups: 2,5
- Key Life: 28800 (seconds)
- Dead Peer Detection: On Demand

IPsec Security (Phase 2) Properties

- Diffie-Hellman Groups: 2,5
- Replay Detection
- Perfect Forward Secrecy(PFS)
- Key Life: 1800(seconds)

8. Ahora tenemos que crear una Gateway para la VPN IPsec. Para ello en el menú principal seleccionamos “VPN Manager” y seleccionamos la VPN creada. Pinchamos en “Create New” y en el desplegable “Managed Gateway”.



9. En primer lugar, seleccionamos la subnet.



10. En este ejemplo se va a crear el Hub, también tenemos que crearlo con el rol Spoke, para ello se siguen los pasos siguientes de la misma forma, con la diferencia de seleccionar el rol en la primera pantalla. Una vez tenemos el rol seleccionado, indicamos el dispositivo.

VPN Gateway Setup Wizard - Prueba1

Protected Network Device Default VPN Interface Local Gateway Advanced

Role Hub Spoke

Device Prueba1 (Cisco, 2800)

< Back Next > Cancel

11. En el apartado “Default VPN Interface” seleccionamos la interfaz por defecto (normalmente es la interfaz que da a internet) y hub-to-hub (únicamente requerida para múltiples hubs).

VPN Gateway Setup Wizard - Prueba1

Protected Network Device Default VPN Interface Local Gateway Advanced

Default VPN Interface eth0 (Cisco)

Hub-to-Hub Interface eth0 (Cisco) (Required for multiple Hubs)

< Back Next > Cancel

12. Indicamos la dirección IP para la Local Gateway.

VPN Gateway Setup Wizard - Prueba1



Protected Network Device Default VPN Interface **Local Gateway** Advanced

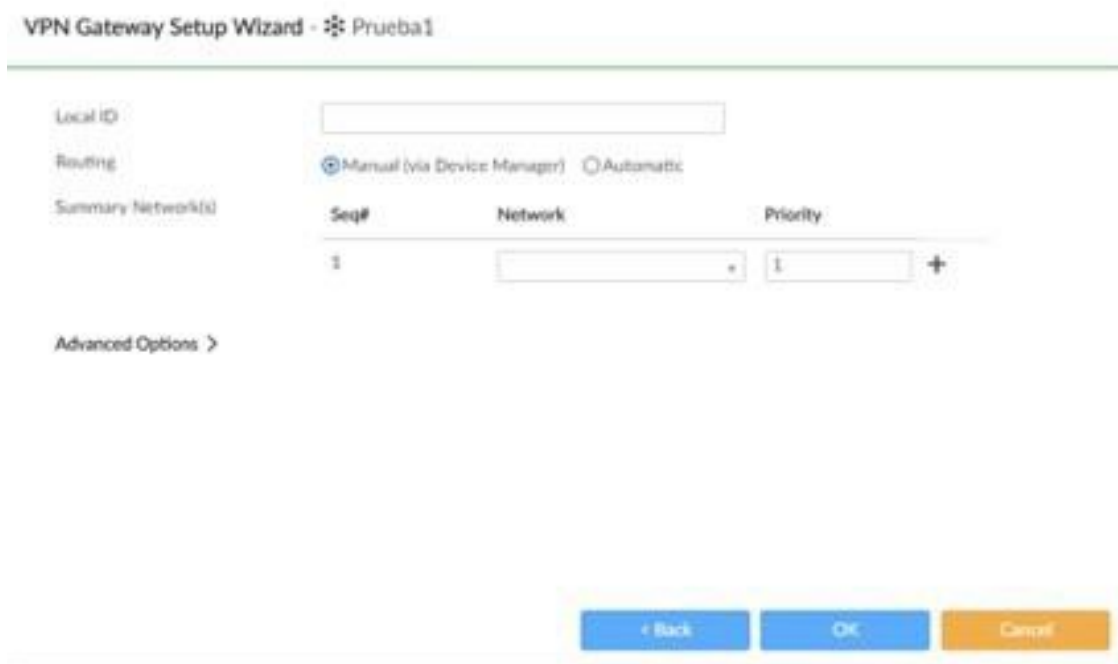
Local Gateway

IP Address

< Back Next > Cancel

13. Por último, podemos escoger el routing de forma manual o automática. Por defecto se deja como está.

VPN Gateway Setup Wizard - Prueba1



Local ID

Routing Manual (via Device Manager) Automatic

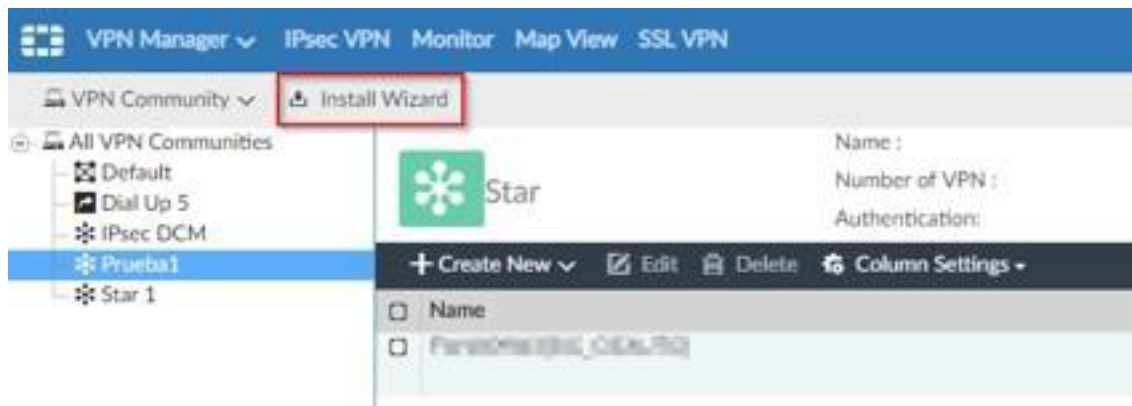
Summary Network(s)

Seq#	Network	Priority
1		1

Advanced Options >

< Back OK Cancel

14. Para realizar la instalación, en la misma pantalla de antes hacemos click en “Install Wizard”.



15. Seleccionamos la política creada en el anterior apartado.



16. Confirmamos que está seleccionada.



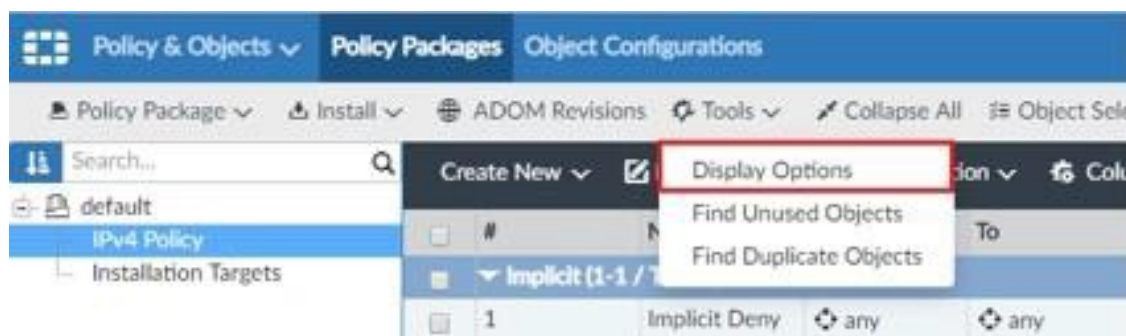
17. Una vez se realice la carga seleccionamos el botón “Install”



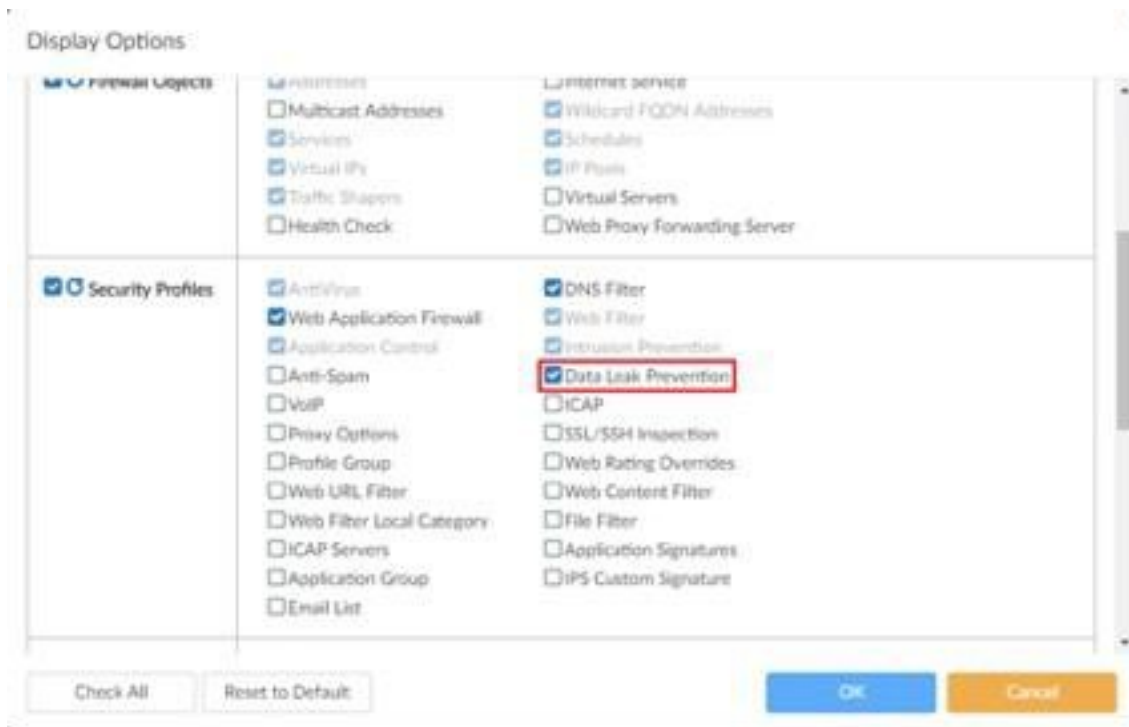
1.16. Configuración Política DLP

Esta política es una estrategia que sirve para asegurarse de que los usuarios finales no envíen información sensible o crítica fuera de la red corporativa. Para ello, se utilizan reglas que examinan el contenido de los archivos y etiquetan la información de confidencial o crítica, para que los usuarios no puedan divulgarla.

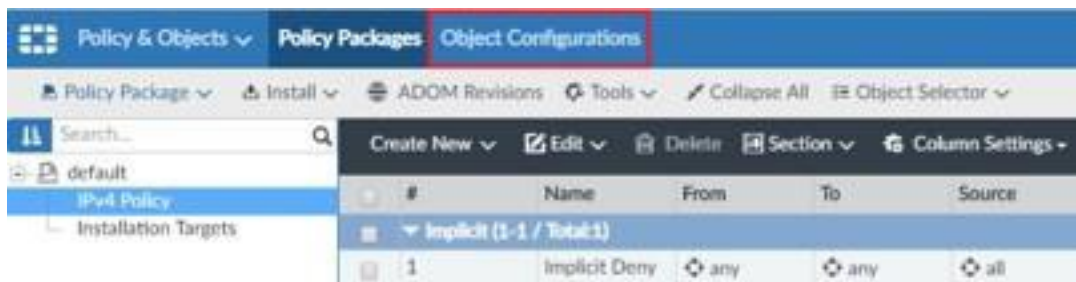
1. El primer paso es habilitar el DLP (Data Leak Prevention). Para ellos nos dirigimos a “Policy & Objects” y hacemos click en la opción “Display options” de la pestaña “Tools”.



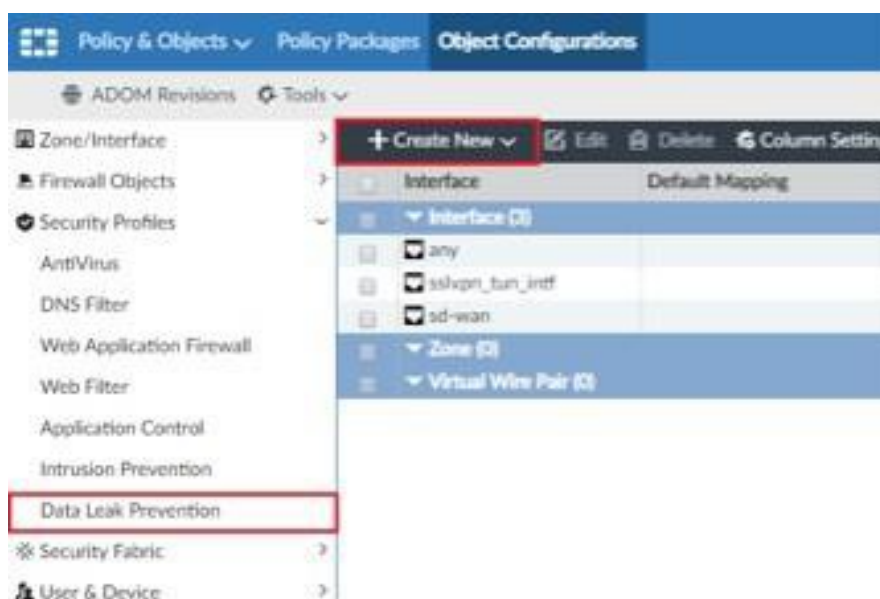
2. Ahora habilitamos la opción “Data Leak Prevention”.



3. En la barra superior nos dirigimos a “Object Configurations”.



4. En “Security Profiles” seleccionamos “Data Leak Prevention” y hacemos click en “Create New”.



5. Para la creación de un nuevo perfil DLP tendremos que rellenar los siguientes campos:



- Name: nombre del perfil DLP.
- Inspection mode: por defecto se deja en modo proxy. En Flow-based, el Fortimanager examina los archivos sin ningún almacenamiento, a medida que llega cada paquete de tráfico, se procesa y reenvía sin esperar el archivo completo o la página web, esto permite respuestas más rápidas para peticiones http, con la desventaja de que pueden darse con mayor facilidad falsos positivos o negativos en el análisis de la información, además de que varias características que pueden ser usadas en el modo proxy no pueden ser usadas aquí.
- Por el contrario el modo Proxy almacena en el buffer y lo examina todo como un conjunto antes de determinar una acción. Esto permite una inspección más completa que en otros métodos, obteniendo menos falsos positivos o negativos en los análisis de datos.
- DLP filter: para crear un filtro DLP debemos hacer click en Create New y se abrirá una pestaña así, donde deberemos indicar que queremos aplicar al perfil DLP para evitar que salga de nuestra red.

Create New DLP Filter

Filter: Messages Files

Containing Credit Card #

Containing SSN

File Size larger than: KB

File Type included in:

File Finger Print:

Watermark Sensitivity:

Regular Expression:

Encrypted

Examine the Following Services

Web Access: HTTP_POST HTTP_GET

Email: SMTP POP3 IMAP IMAP4

Others: FTP NNTP

Action:

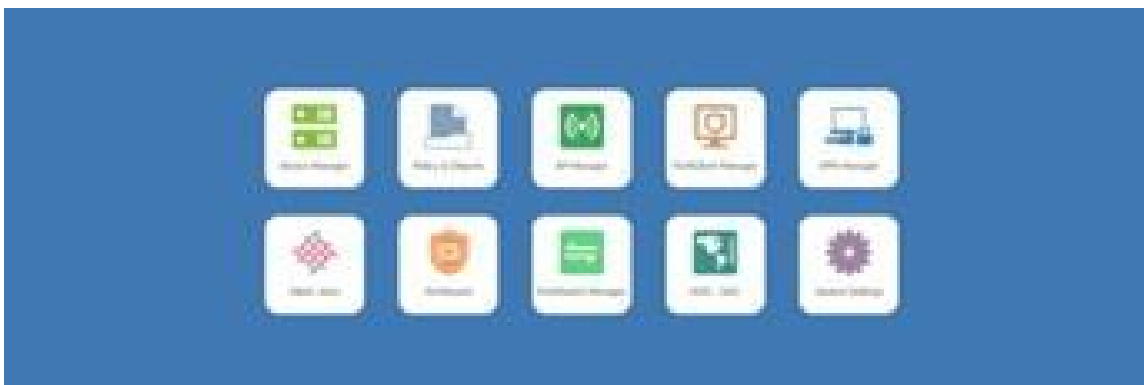
Archive: Enable

Tenemos diversas opciones para filtrar, que son las siguientes:

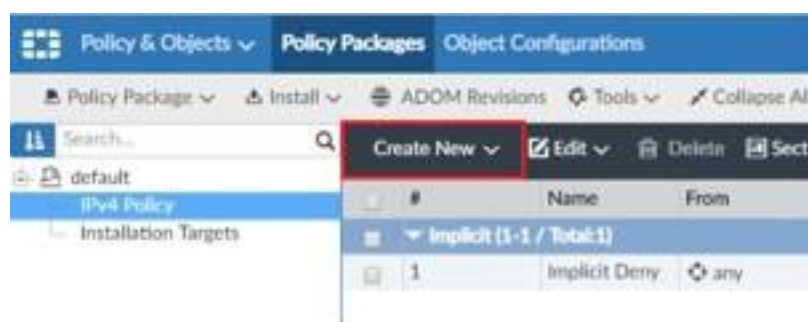
- Lo primero es elegir si queremos filtrar sobre el contenido de cierto mensaje o sobre archivos.
- Filtrar cuando contenga números de tarjetas de crédito.
- Filtrar archivos que contengan SSN.
- Filtrar archivos mayores de cierto tamaño.
- Filtrar archivos ejecutables.
- Filtrar archivos en función de la huella digital.
- Filtrar archivos que contengan ciertas marcas de agua.
- Filtrar archivos en función de expresiones regulares.
- Filtrar archivos encriptados.
- También tenemos la opción de filtrar en función del servicio (web access, email, FTP y NNTP).
- Deberemos establecer también la acción a aplicar sobre estos filtros, pudiendo permitirlo, bloquearlo, hacer que quede registrado en un log o poner en cuarentena la dirección ip de la que proviene.

1.17. Políticas de navegación por grupo de usuarios

1. Seleccionar en el menú principal la opción de “Policy & Objects”.



2. Aparecemos directamente en el menú de las políticas, por lo que hacemos click en “Createnew”.



3. Los campos de esta configuración vienen explicados en el apartado 2.5 “Configuración política básica de navegación”. A continuación, para crear una política de usuarios de FSSO seleccionamos el grupo de usuarios correspondiente.

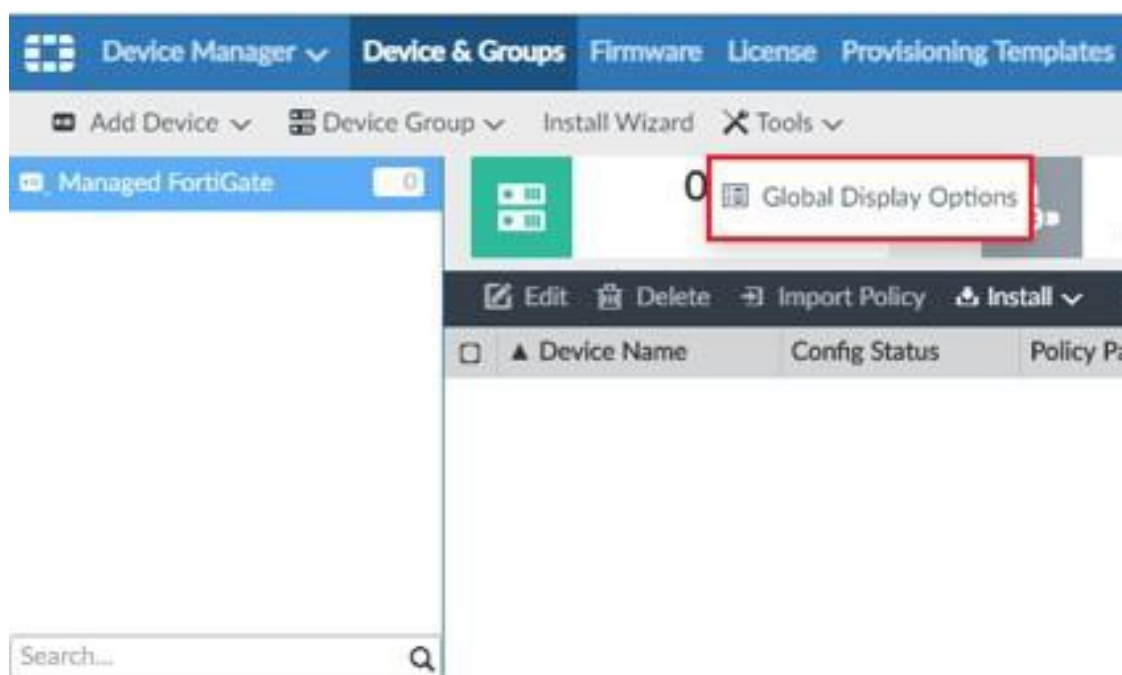
Name	
Incoming Interface	<input checked="" type="checkbox"/> any
Outgoing Interface	<input checked="" type="checkbox"/> any
Source Address	<input checked="" type="checkbox"/> IP_10.148.8.0/24
Source User	+
Source User Group	<input checked="" type="checkbox"/> FSSO_Subscripción_AccPkg <input checked="" type="checkbox"/> FSSO_AccPkg
FSSO	<input checked="" type="checkbox"/>
RSSO	<input type="checkbox"/>
Source Device	+
Destination Internet Service	OFF
Destination Address	<input checked="" type="checkbox"/> all
Service	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS
Schedule	<input checked="" type="checkbox"/> always
Application	+

1.18. Proxy Web

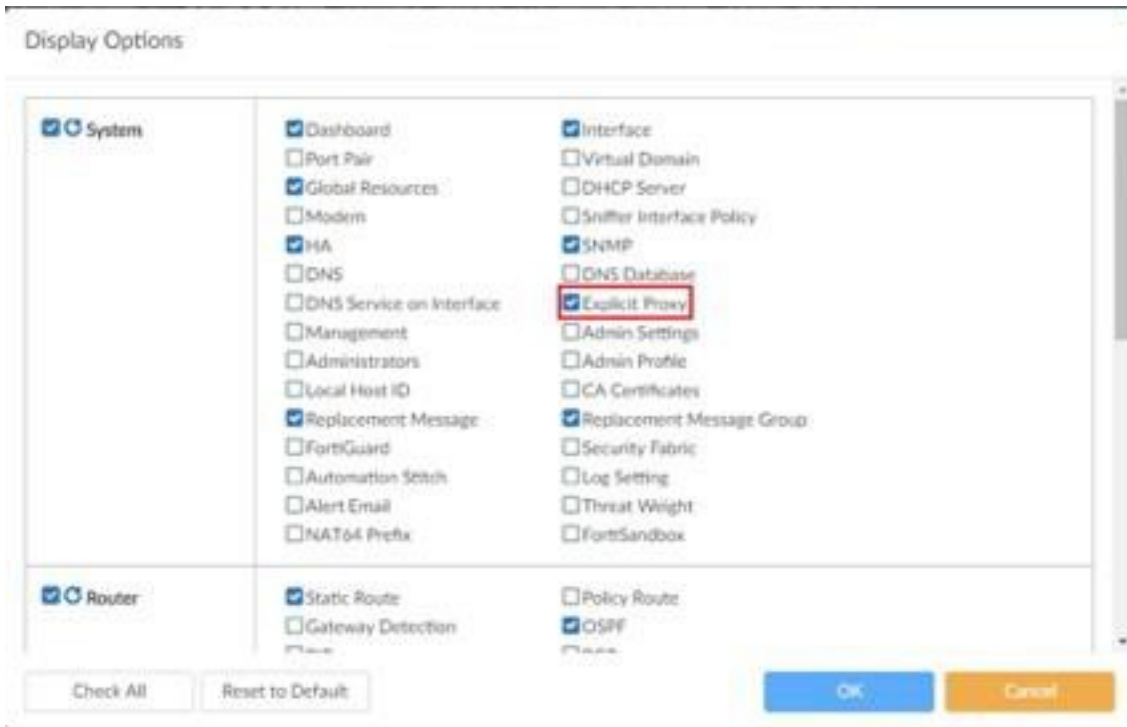
1. En primer lugar, nos dirigimos en el menú principal al apartado “Device Manager”.



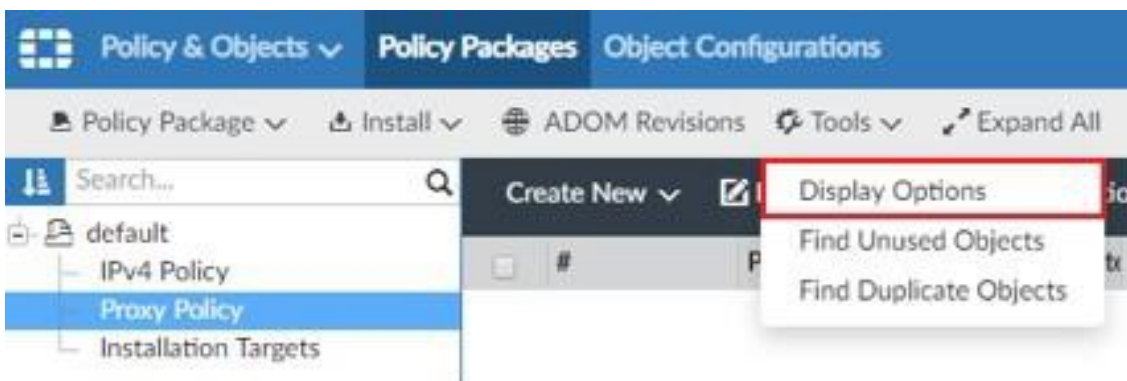
2. En la pestaña “Tools” seleccionamos la opción “Global Display Options”.



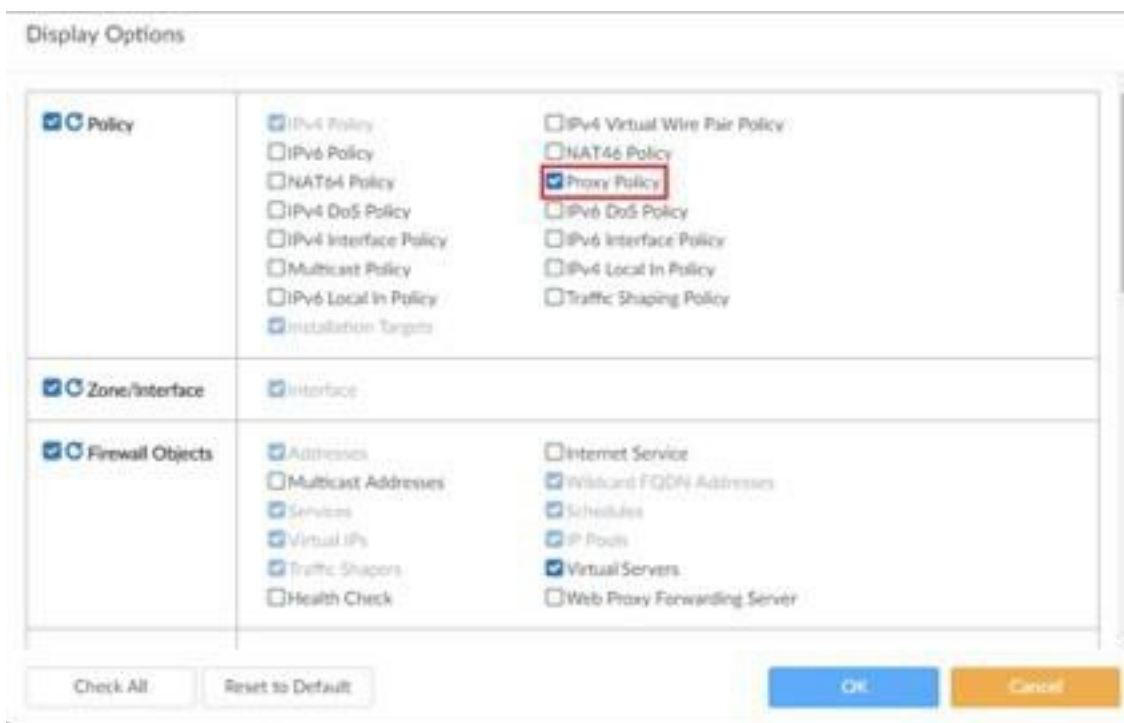
3. En la ventana nos aparecerán varias opciones para activar o desactivar, en nuestro caso activamos la casilla “Explicit Proxy”.



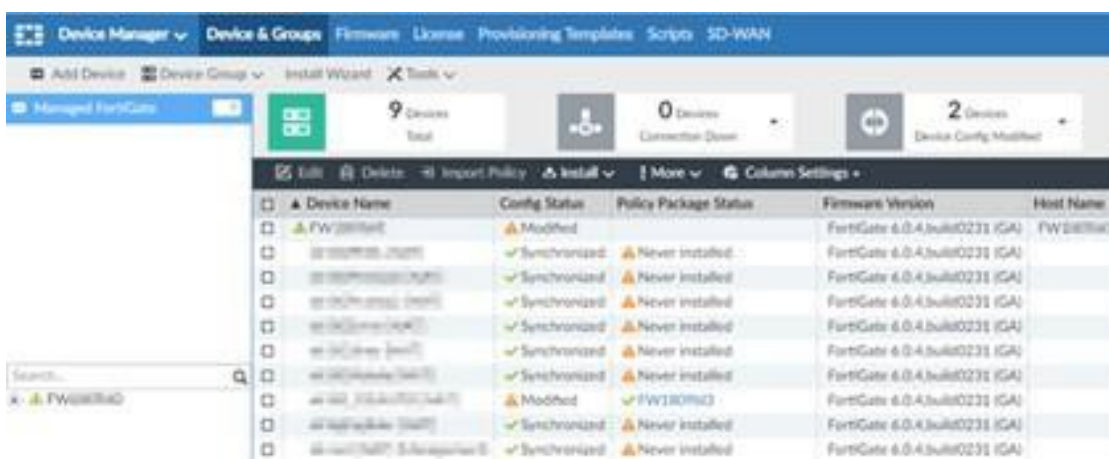
4. En el menú principal seleccionamos el apartado “Policy & Objects” y dentro de “Policy Packages”(por defecto entramos en este menú),hacemos click en la pestaña “Tools”y en el menú desplegable la opción “Display Options”.



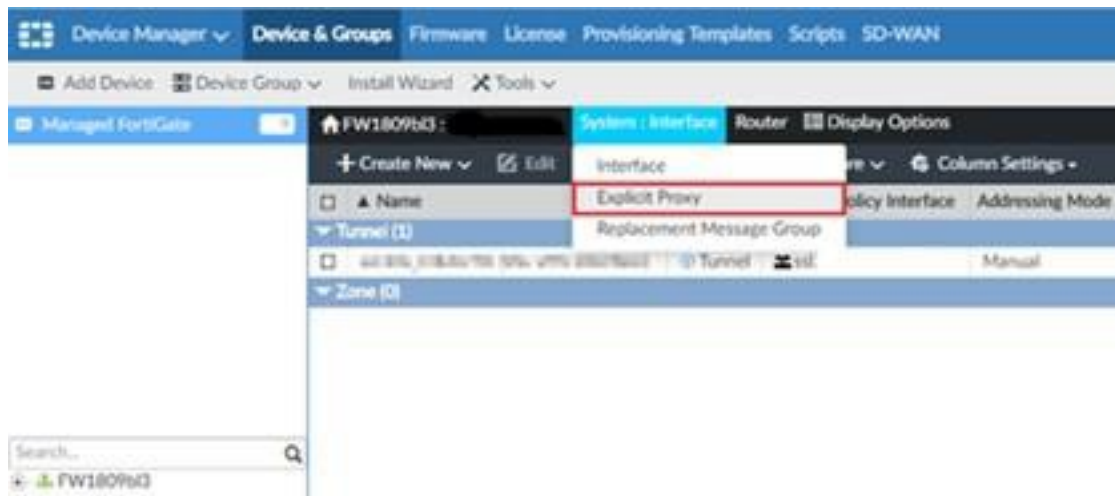
5. En la ventana activamos la opción “Proxy Policy”.



6. Una vez habilitadas las opciones anteriores, nos dirigimos a “Device Manager” ➔ “Device & Groups”.



7. Seleccionamos el dispositivo sobre el que queremos configurar el Proxy. A continuación nos posicionamos encima de "System: Interface" y hacemos click en "ExplicitProxy".



8. Una vez en la ventana de configuración activamos el Proxy y seleccionamos las interfaces. Indicamos el puerto en el que escuchará el proxy web, por defecto es el 8080.

Explicit Web Proxy

Enable Explicit Web Proxy: HTTP / HTTPS FTP PAC

Listen on Interfaces ⓘ

x

1 Entry Selected

HTTP Port:

HTTPS Port:

PAC File Content:

Unknown HTTP version:

Proxy FQDN:

Max HTTP request length (2-64):

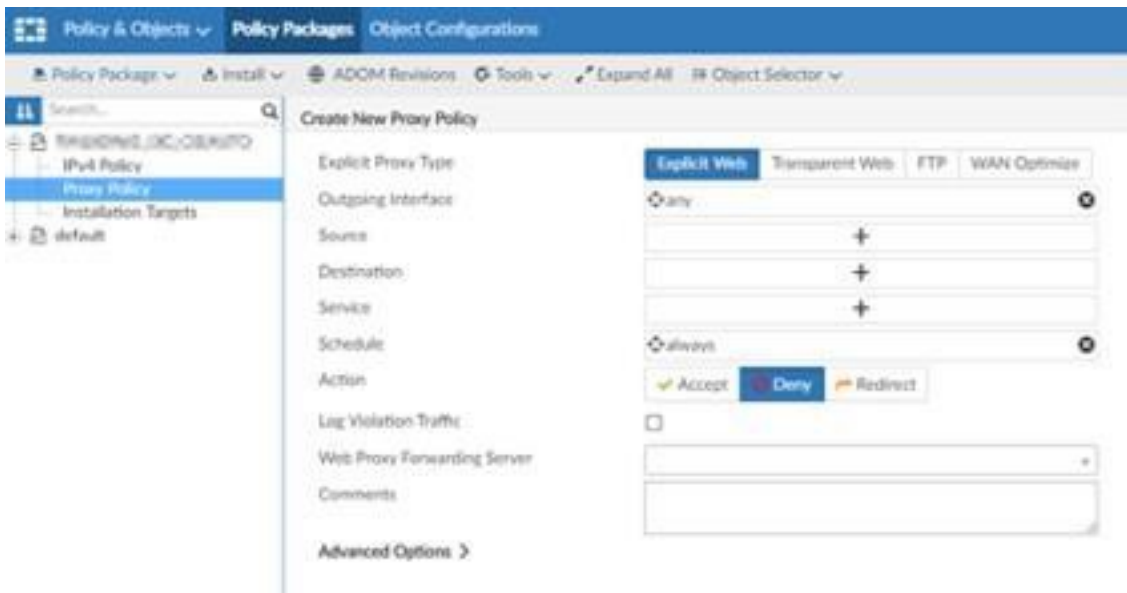
Max HTTP message length (16-256):

Realm:

Default Firewall Policy Action:

Web Proxy Forwarding Servers:

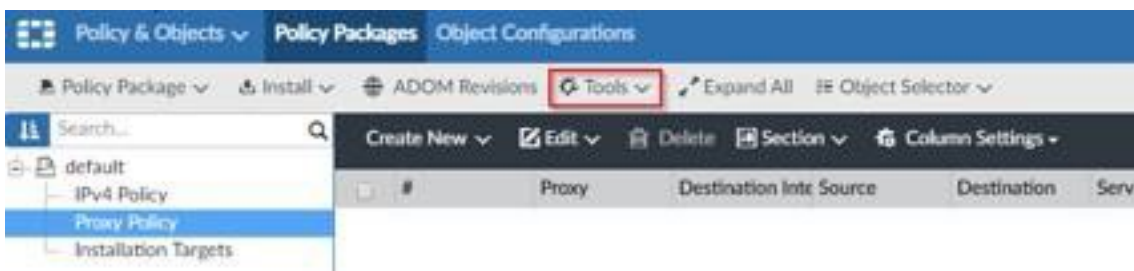
9. Finalmente en FortiManager, la política la rellenamos al igual que en el apartado 1.5.



1.19. Balanceadores de carga

1.19.1 Definición del servicio balanceado

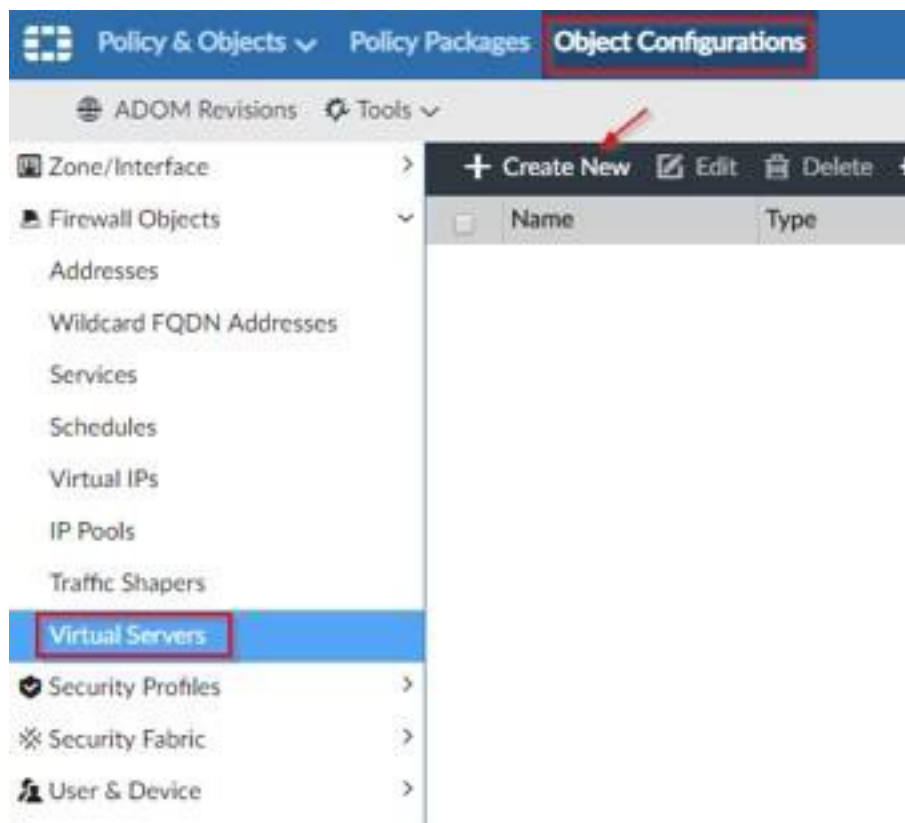
Lo primero que debemos hacer es habilitar una opción que encontraremos en el apartado "Policy & Objects", en Tools.



Aquí deberemos habilitar "Virtual Servers" y "Health Check".



Una vez hemos habilitado esta opción nos dirigimos a Virtual Servers, dentro de "Policy & Objects", en la sección de "Object Configurations" y hacemos click en "Create New".



Ahora tenemos que crear un nuevo servidor virtual.

Para ello debemos de rellenar los siguientes campos:

- Name: nombre del servicio balanceado.
- Interface: Interfaz por la que el firewall correspondiente recibirá las conexiones.

- Type: protocolo que va a ser balanceado.
- Virtual Server IP: IP del servicio a la que se van a conectar los clientes.
- Virtual Server Port: Puerto en la que va a estar el servicio y por lo tanto al que se van a conectar los clientes al servicio.
- Load Balance Method: Forma en la que se van a repartir (balancear) las conexiones a los nodos de servicio reales.
- Persistence: Asegura que un usuario se conecta al mismo nodo real durante una sesión para los protocolos HTTP, HTTPS.
- Health Check: Métodos para determinar la salud de los nodos. Existen tres posibilidades, mediante ping, mediante conexión TCP o mediante un GET HTTP.

1.19.2. Creación de la granja de servidores

En esta parte debemos dar de alta los nodos que constituyen la granja de servidores. Para ello hacemos click en "Create New".



Create New Real Servers

IP Address	0.0.0.0
Port	0
Weight	1
Max Connections	0
HTTP Host	
Mode	Active
Client IP	0.0.0.0 (e.g. R.X.X.X, X.X.X.X-Y.Y.Y.Y)

Advanced Options >

OK Cancel

Debemos rellenar entonces los siguientes campos:

- IP Address: IP del servidor real.
- Port: puerto de servicio en el servidor real.
- Max Connections: número de conexiones máximas establecidas para el nodo del servicio.
- Mode: Active o disable por defecto. En caso de estar desactivado no daría servicio.

1.19.3. Utilización en la política

El objeto virtual server se utilizará en la política como destino en la regla, para permitir el acceso desde todo Internet o las redes que se quiera limitar el acceso.

Name	2
Incoming Interface	any
Outgoing Interface	any
Source Internet Service	OFF
Source Address	all
Source User	+
Source User Group	+
Source Device	+
Destination Internet Service	OFF
Destination Address	Virtual_server
Service	ALL
Schedule	always
Action	Deny Accept IPSEC