centro criptológico nacional

CN-CERT
centro criptológico nacional

VANESA

Configuración de seguridad en cortafuegos. Ejemplo en entorno Fortinet

Índice

Índice

1.- Introducción al firewall

- Los firewalls son más que un simple Gateway de la red.
- Están diseñados para responder a los retos de los entornos actuales, en los que no hay un perímetro identificable (red confiable y red no confiable):
  - Fuerza de trabajo móvil
  - Acceso remoto a los servicios internos
  - Clouds públicas y privadas
  - Internet of Things (IoT)
  - Bring Your Own Device (BYOD)

1.1- Stateless vs Statefull

- Stateless: Típicamente un router con listas de acceso. Las decisiones se toman paquete a paquete.
- Stateful: Los firewalls son conscientes de las sesiones que pasan a través de ellos
  - Guardan la información en una tabla de sesiones.
  - Son capaces de analizar el contenido de las sesiones.

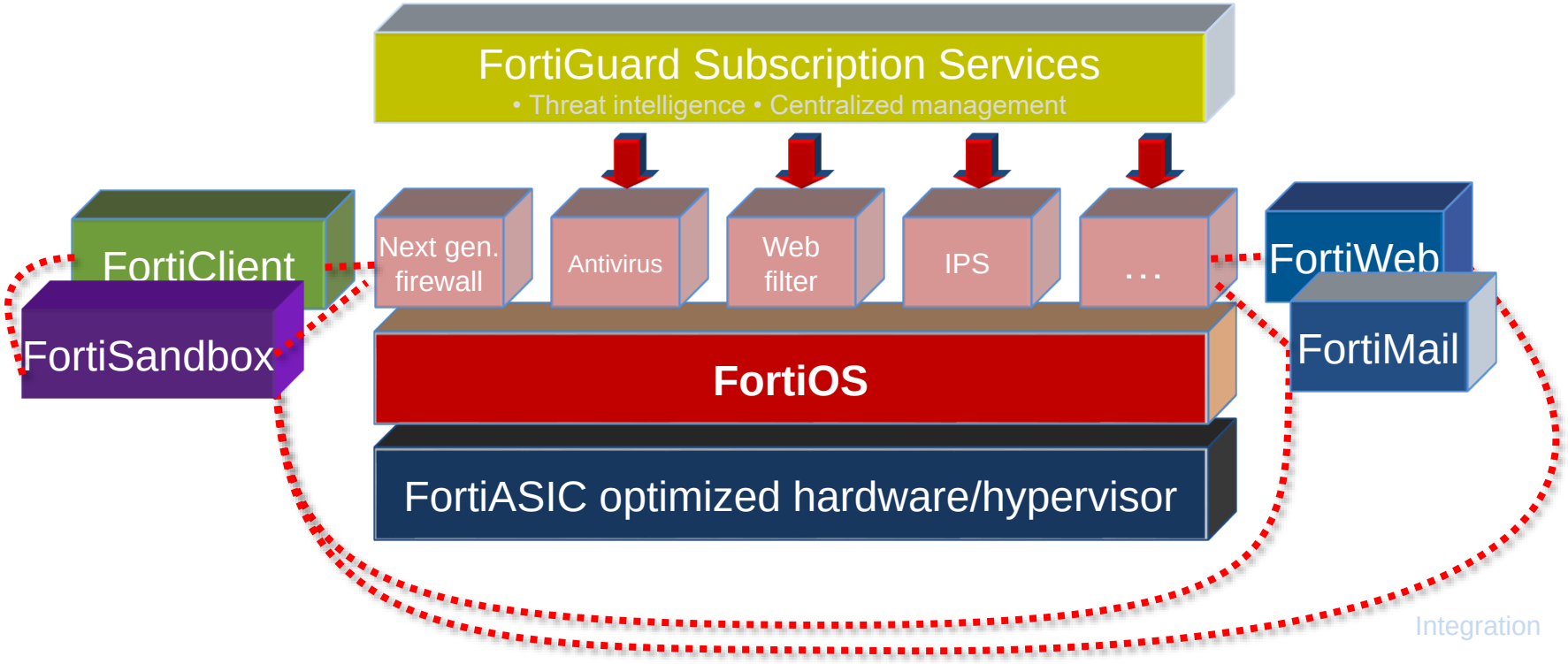
1.2- El firewall UTM FortiGate

- Firewall de aplicación: Evolución del firewall stateful de capa 7, que añade la capacidad de inspeccionar la información de capa 7, tomando decisiones más allá de la quíntupla IP/puerto origen, IP/puerto destino y protocolo.
- La capacidad de inspección a nivel 7 permite añadir funcionalidades que antes se distribuían entre diferentes equipos de seguridad
  - Proxy Explícito
  - Antivirus
  - Filtrado de contenido WEB
  - IPS/IDS
  - Control de aplicaciones
  - Identificación de usuarios

1.2- El firewall UTM FortiGate

- Ventajas de la integración de funcionalidades
  - Flexibilidad en el despliegue.
  - Reducción de costes
  - Reducción de la complejidad
  - Facilidad de despliegue e integración

1.2- El firewall UTM FortiGate



1.2- El firewall UTM FortiGate

FortiGuard Security Services Available (FortiGate)

FortiGuard Bundles & Services	Advanced Threat Protection (ATP)	Unified Protection (UTM)	Enterprise Protection (ENT)	Available Individually
Threat Intelligence Service				✓
Industrial Security Service			✓	✓
Security Rating			✓	✓
CASB			✓	✓
Web Filtering		✓	✓	✓
Advanced Malware Protection Includes Antivirus, FortiSandbox Cloud, Mobile, Botnet, VOS, CDR	✓	✓	✓	✓
IPS	✓	✓	✓	✓
Anti-Spam		✓	✓	
Internet DB	✓	✓	✓	
IP Reputation	✓	✓	✓	
Application Control	✓	✓	✓	

1.3 Inspección SSL: Por qué es necesaria

- Tráfico SSL

más **75%**

Del tráfico en internet estará cifrado en 2019(SSL/TLS)

Fuente:
NSS Labs

- Malware Encriptado

más **50%**

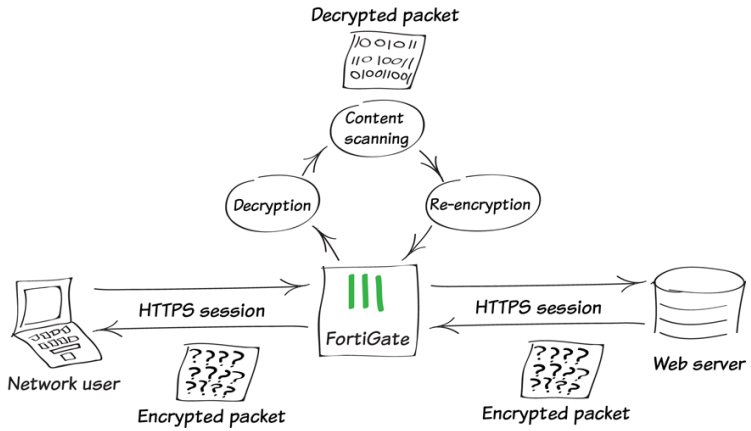
De los ataques usarán tráfico encriptado en 2019*

Fuente::
Gartner

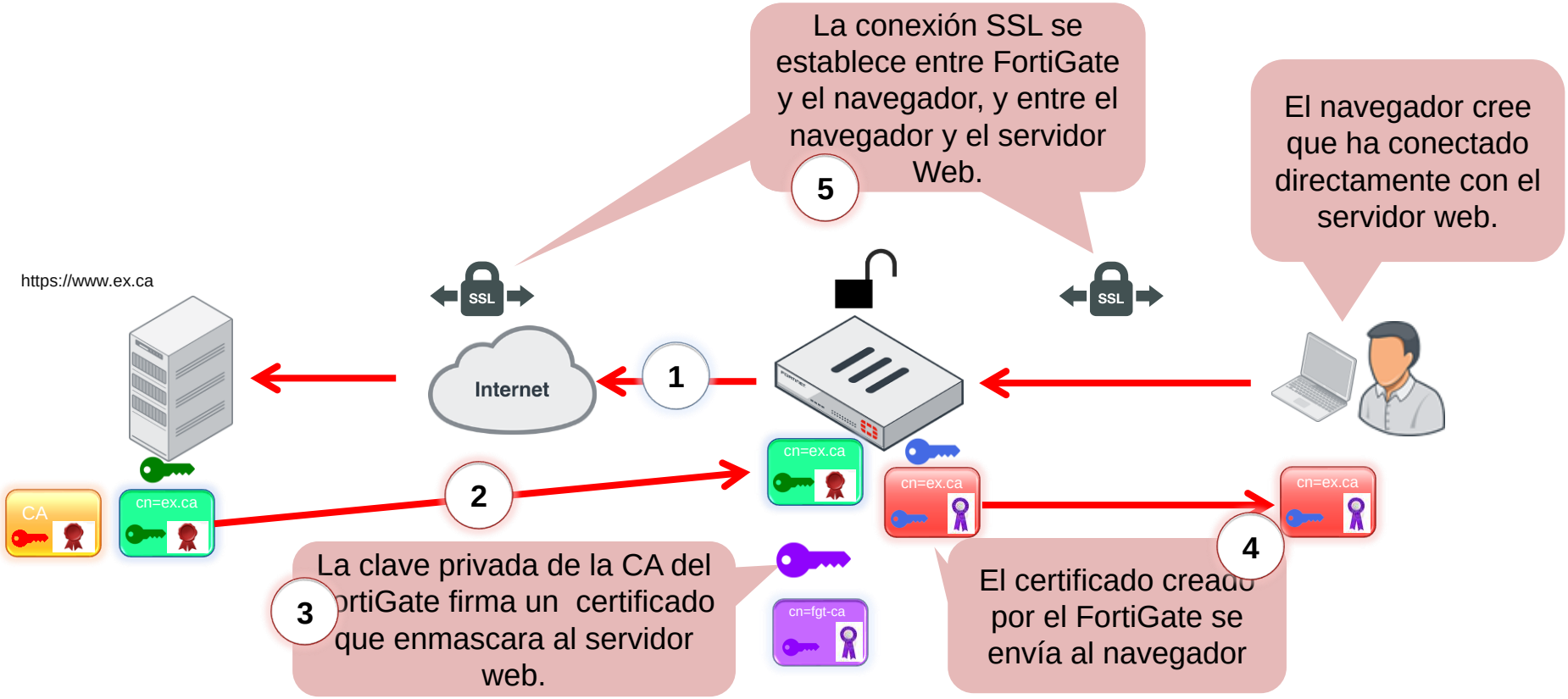
1.3 Inspección SSL: Tipos de inspección

Inspección SSL Profunda

Se usa inspección profunda cuando queremos asegurar la inspección de todo el contenido de los flujos que atraviesan el firewall.
En este escenario, el FortiGate impersona al servidor original y descifra e inspecciona el contenido. El FortiGate entonces crea una sesión SSL contra el servidor inicial, impersonando al origen y vuelve a cifrar el contenido.



1.3 Inspección SSL: Tipos de inspección



1.3 Inspección SSL: Tipos de inspección

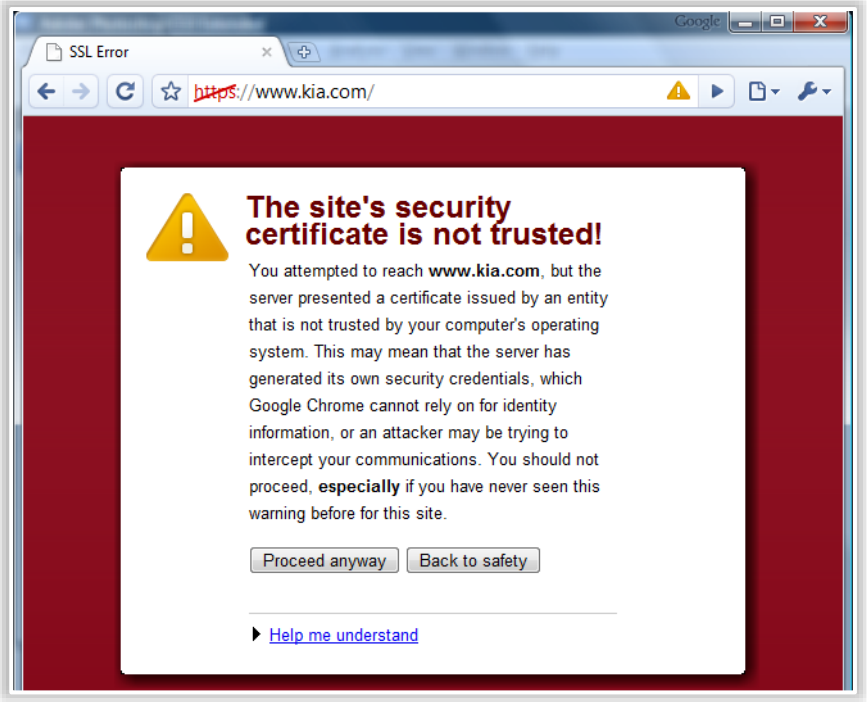
Inspección de certificado.

- En este caso, el FortiGate solo inspecciona la cabecera de los paquetes. La inspección de certificado se usa para verificar la identidad del servidor web y asegurar que no se está usando el protocolo HTTPS para saltarse las restricciones impuestas por el filtrado web.

- Como solo se inspecciona el contenido y no se impersona al servidor, este método no introduce errores de certificados y es una alternativa sencilla para desplegar filtrado web

1.3 Inspección SSL: Errores de certificado

Al hacer una inspección profunda e impersonar al servidor, se está haciendo un "Man in the Middle" que rompe la conexión segura entre cliente y servidor que resulta en un error de certificado.



1.3 Inspección SSL: Best Practices

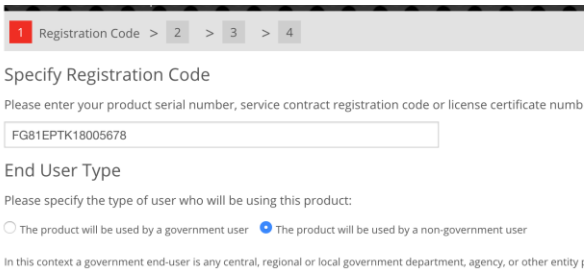
Como el tráfico necesita ser descifrado, inspeccionado y vuelto a cifrar, la inspección SSL puede reducir el rendimiento global del equipo. Para asegurar el menor impacto posible, es necesario:

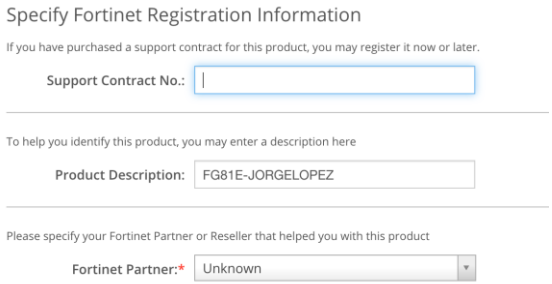
- **Conoce tu tráfico:** Saber cuánto tráfico tendrá que procesar el firewall y qué porcentaje de ese tráfico estará encriptado.
- **Sé selectivo:** Usa listas blancas o segmenta la política para aplicar inspección SSL solo donde sea necesaria.
- **Usa aceleración hardware:** Los modelos FortiGate con ASICS CP9 tienen más capacidad de procesar tráfico encriptado.
- **Testea el rendimiento SSL:** Aprovecha la granularidad en la definición de los perfiles SSL y la flexibilidad del despliegue de políticas para habilitar la inspección gradualmente.

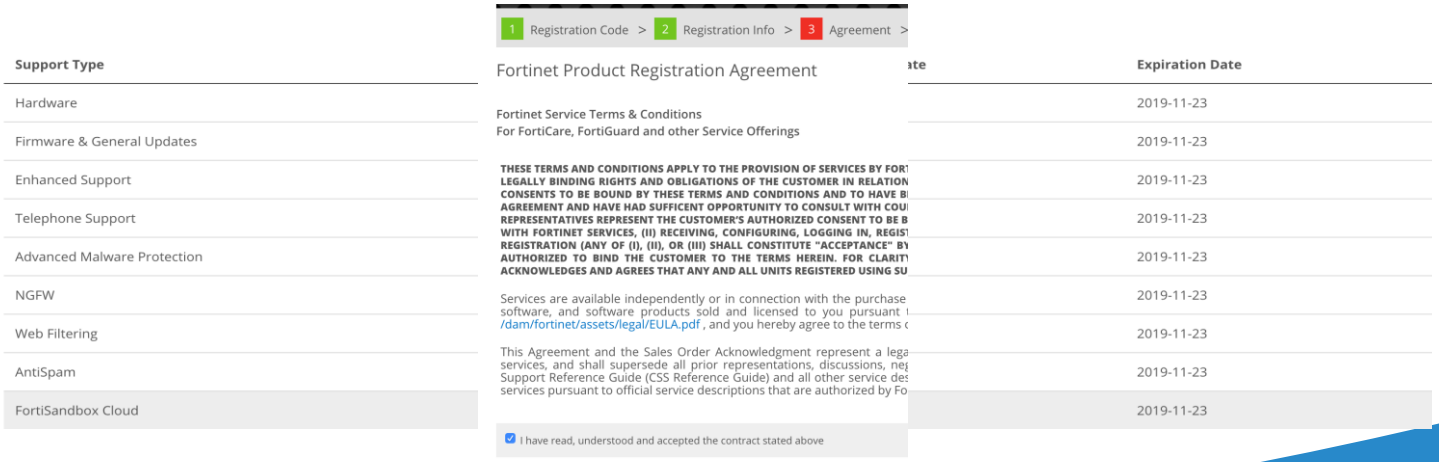
Índice

2.1 Primera configuración y registro en soporte

Support.Fortinet.com





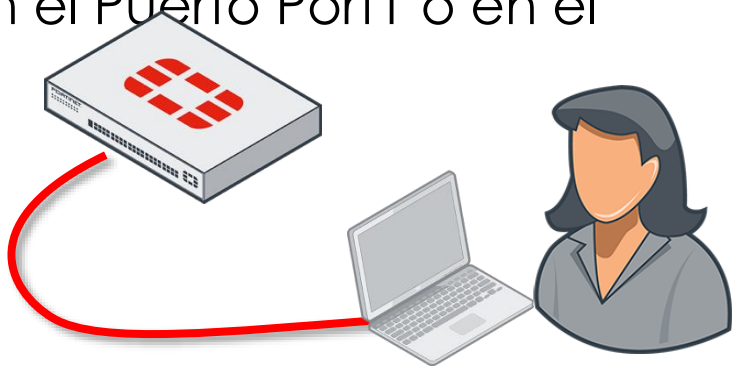


2.1 Primera configuración: Registro

- Se requiere un contrato válido y acceso a internet
- Proporcionado por FortiGuard Distribution Network (FDN)
  - DataCenters en Europa, América y Asia
    - También localmente si se usa FortiManager
  - FortiGate seleccionará el Data Center en la zona horaria más cercana pero se ajustará en función de la carga.
- Actualización de firmas: FortiGuard Antivirus e IPS
- Petición en vivo: FortiGuard Web Filtering, DNS Filtering, y Antispam

2.1 Primera configuración y registro en soporte

- Port1 o interface "internal" usa la IP: 192.168.1.99/24
- Está habilitado el PING, HTTP, HTTPS, y SSH
  - **La guía STIC insta a deshabilitar protocolos no seguros (HTTP y telnet)**
- Hay un servidor DHCP habilitado en el Puerto Port1 o en el interface Internal.
- Usuario por defecto:

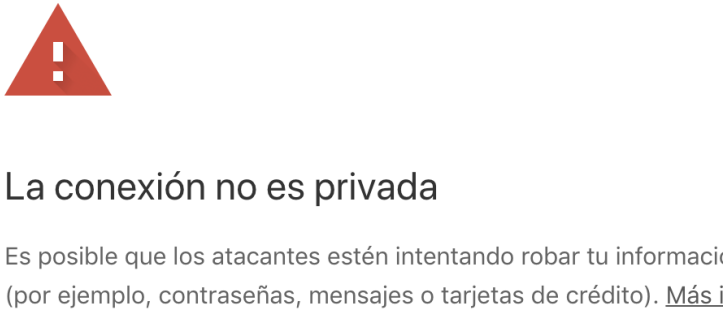


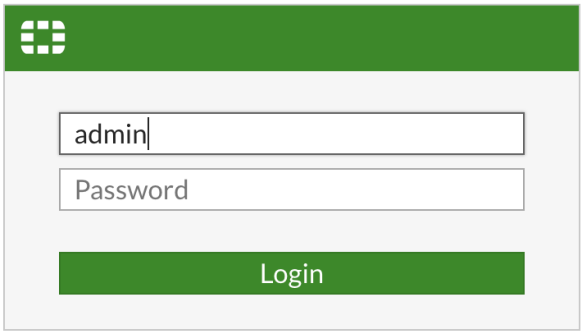
Usuario: admin

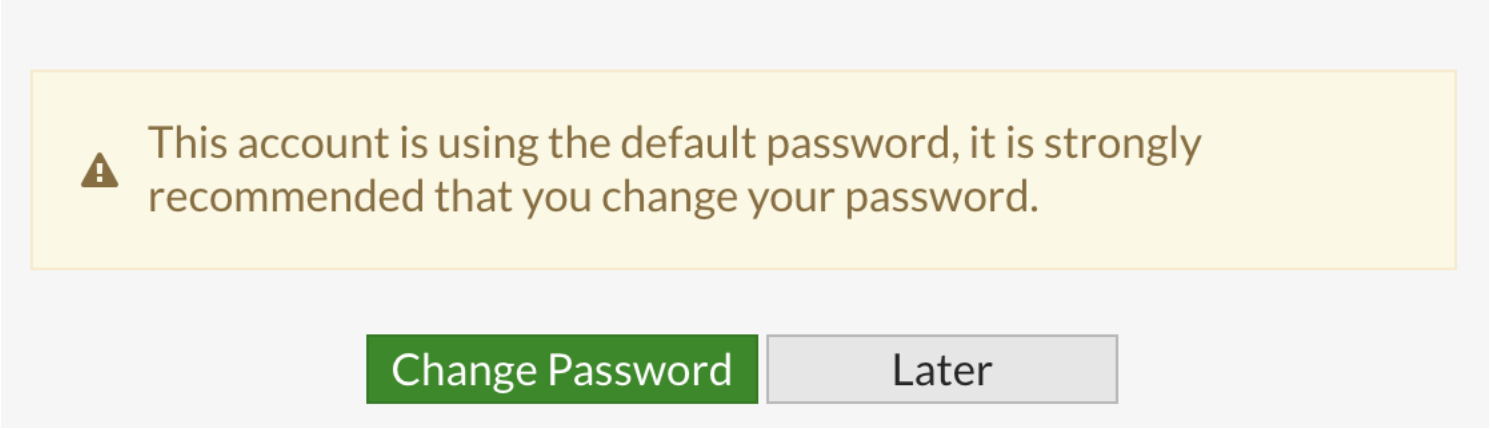
Password: (vacío)

- También se puede accede al FortiGate usando el CLI:
  - Consola: Sin red
  - CLI : A través del widget embebido en el interface GUI, o bien a través de un emulador de terminal, (PUTTY, Tera Term…)

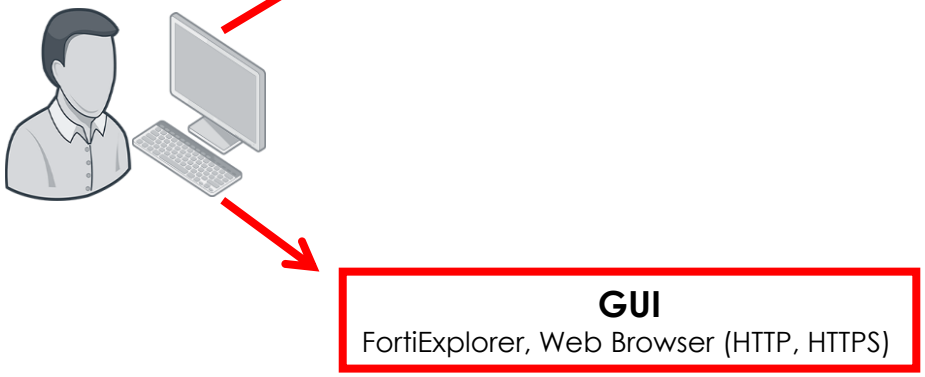
2.1 Primera configuración y registro en soporte

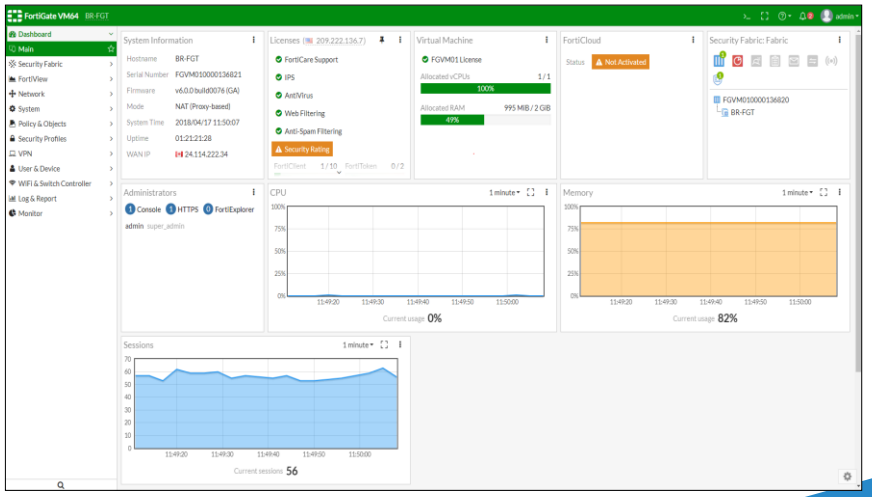




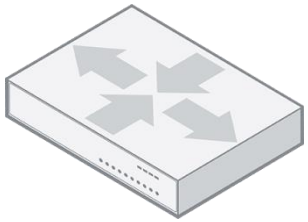


2.1 Primera configuración: Administración



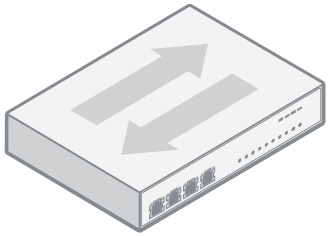


2.1 Primera configuración: Modo de operación



NAT

- FortiGate es un **router**
- Los Interfaces tienen direcciones IP
- Los paquetes se encaminan por IP

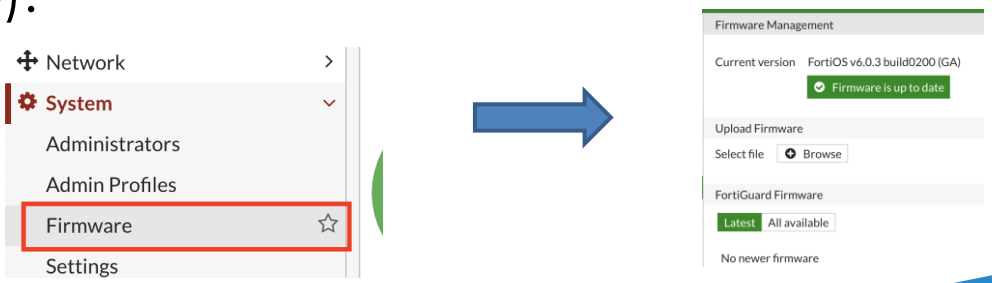


Transparente

- FortiGate es un **switch**
- Los interfaces no tienen IP
- No puede encaminar paquetes, solo bloquear o transmitir

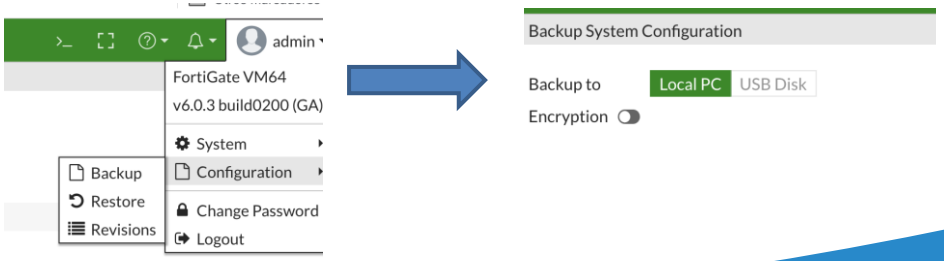
2.2 Actualización de software

- Es aconsejable actualizar el equipo antes de empezar a configurar.
- Los equipos con contrato activo pueden buscar nuevas versiones en FortiGuard
- Siempre se puede cargar una versión manualmente de la página de soporte (support.Fortinet.com), con un usuario y password válido (p.e. el que hayamos creado al registrar el equipo).



2.3 Gestión de backups

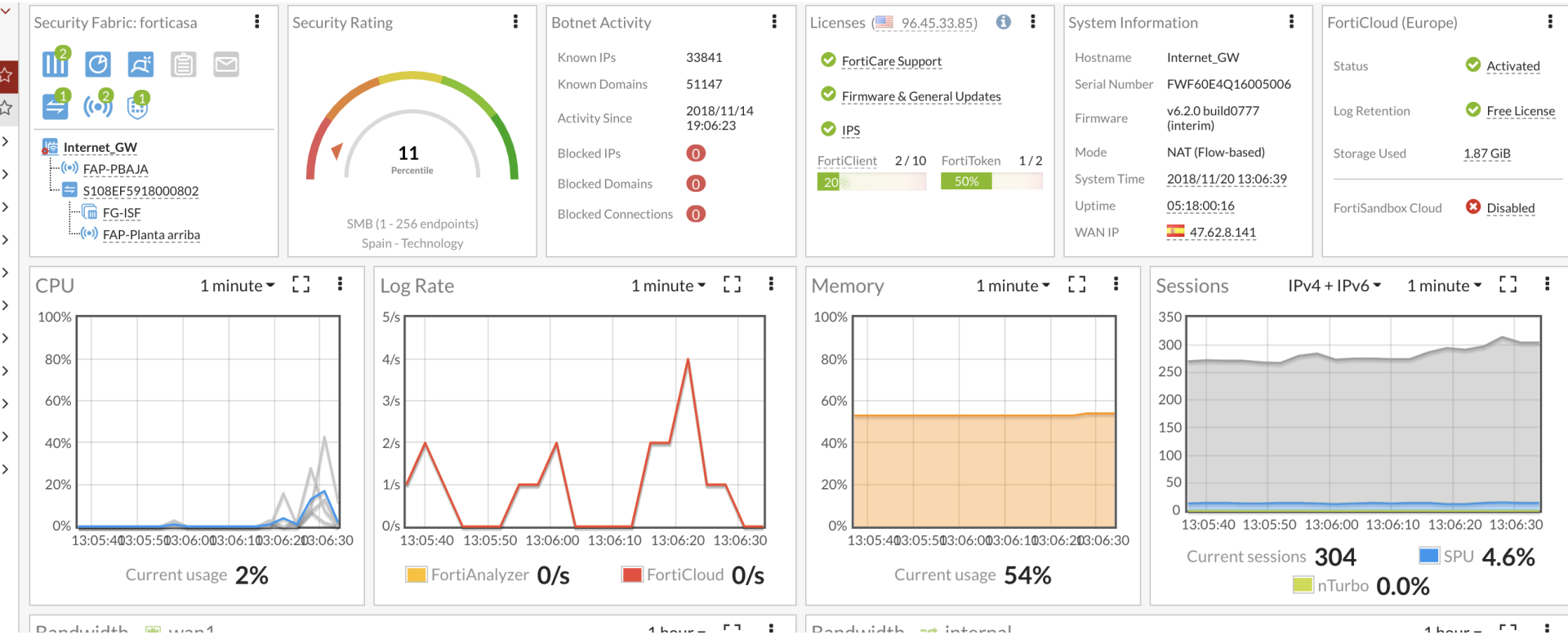
- Es aconsejable hacer backups de las configuraciones.
- El backup se puede hacer manual, en cualquier momento, o automatizar para que se envíe a un servidor centralizado
- El backup incluye sólo la configuración, y es un fichero de texto editable offline, que se puede volver a cargar en el dispositivo.
- Se pueden generar revisiones de configuración
  - **La guía STIC recomienda Cifrar los backups y custodiarlos en lugar seguro**



2.4 Dashboards

- Se pueden personalizar diferentes Dashboards, para presentar al administrador información sobre el estado de la red y del dispositivo
- A cada Dashboard se le añaden Widgets, que contienen un tipo concreto de información (tráfico, amenazas, usuarios logados…)
- Los Widgets se pueden redimensionar, reubicar….

2.4 Dashboards

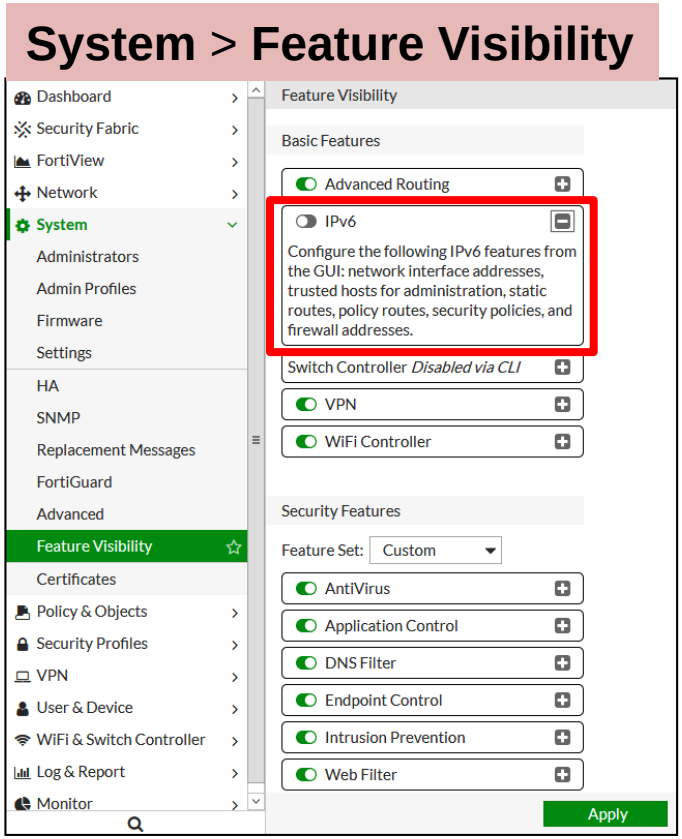


2.5 System Settings

- Diferentes configuraciones globales:
  - Password Policy: Características que tienen que tener los passwords que se configuren localmente
  - NTP: Sincronización con un servidor NTP externo
    - **La guía STIC recomienda configurar siempre un servidor de tiempos que asegure que los logs y eventos tienen una hora válida, y coherente con otros logs que se puedan recopilar**
  - Hostname: Nombre del equipo.
  - **LA guía STIC indica que es necesario limitar el timeout de usuario**
  - System -> Advanced -> Usb Settings
    - **STIC recomienda deshabilitar la autoinstalación a través de USB**

2.6 Habilitar funciones

- Por defecto, algunas funciones (como IPv6) están ocultas en la GUI
  - Que estén ocultas no quiere decir que estén deshabilitadas.
- En "**Feature Visibility**", Seleccione mostrar/ocultar grupos de funcionalidades que se usan normalmente juntas.
- **LA guía STIC recomienda deshabilitar funcionalidades que no se utilicen**



2.7 FortiGuard

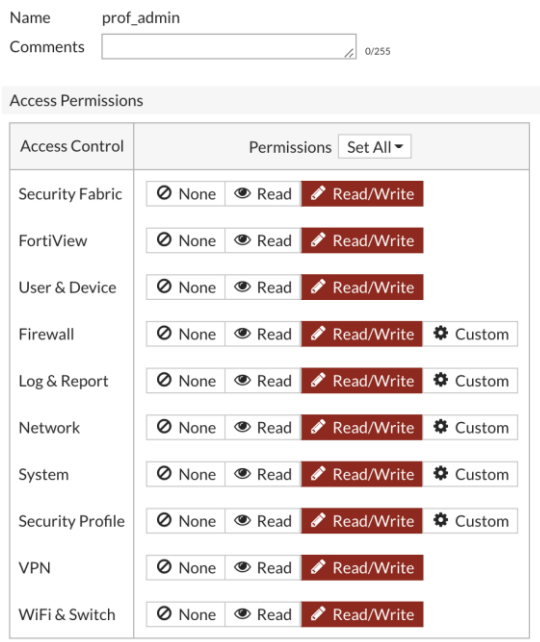
- En entornos con alto nivel de seguridad puede no ser posible tener acceso a una red pública para lo cual se deberán implementar soluciones para la actualización de la base de datos sin conexión directa. En este sentido FortiManager puede actuar como nodo para los equipos que gestiona sin que tengan acceso a la red pública. .

2.7 Administradores

- La guía STIC recomienda que dado que el usuario "admin" es un usuario creado por defecto debe limitarse su uso a la gestión local y siempre desde dispositivos seguros y emplear para la administración usuarios personalizados (nominales) y con el perfil estrictamente necesario

- Es posible usar 2FA (FortiToken)

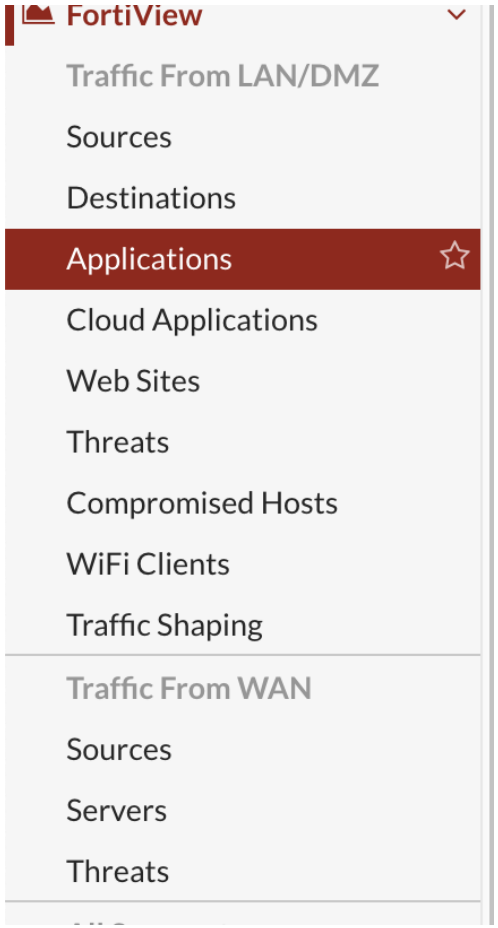
System – Admin Profiles



2.8 FortiView

- Ayuda a la monitorización de la red, integrando información en tiempo real e histórica en una única vista consolidada.
- FortiView se puede para investigar la actividad de red y las amenazas.
- Diferentes categorías, que resultan de la consolidación de logs.
- Capacidad de "drill down".

2.8 FortiView



Application	Category
Netflix	Video/Audio
HTTPS.BROWSER	Web.Client
WhatsApp	Collaboration
Google.Talk	Collaboration
YouTube	Video/Audio
Google.Services	General.Interest

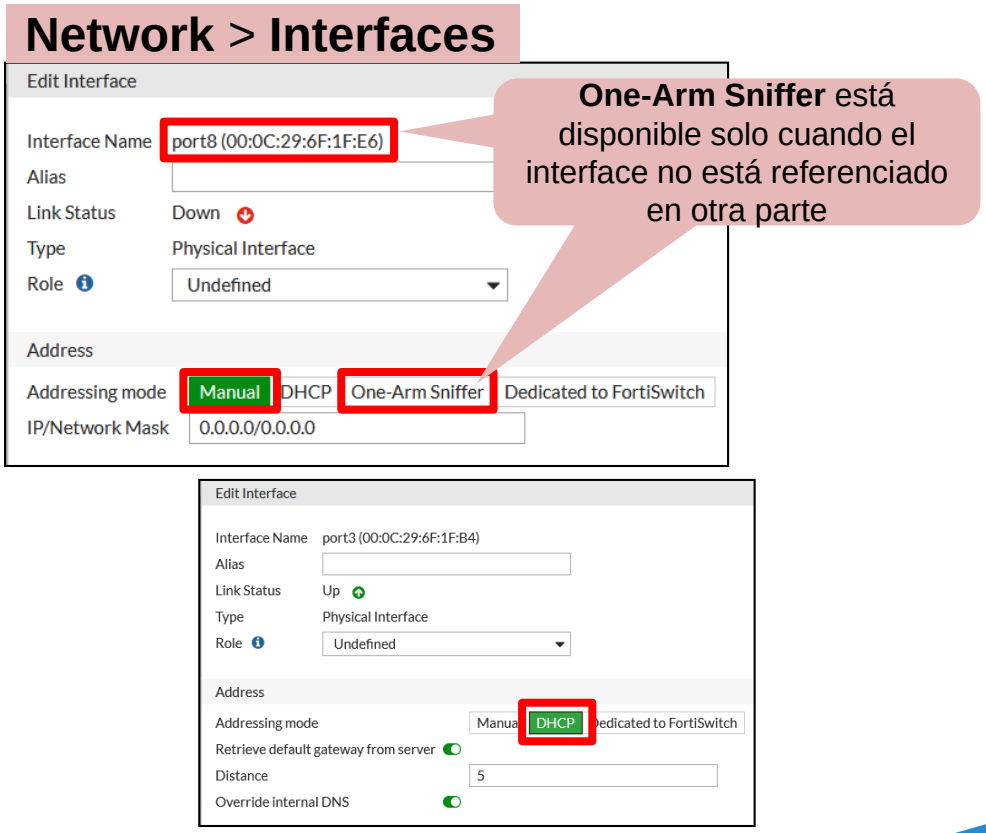
2.8 Otras configuraciones (guía STIC)

- Deshabilitar el usuario "Maintainer" para impedir acceso a la configuración de la máquina en caso de tener acceso físico a la misma.
  - config system global
    set admin-maintainer disable
    end
- Configurar un mensaje de advertencia antes del acceso:
  - config system replacemsg admin "admin-disclaimer-text"
    set buffer "ATENCION: Acceso restringido a personal autorizado.
    Este equipo, incluidos los dispositivos relacionados con el mismo, es propiedad privada.
    Toda actividad esta siendo monitorizada"

Índice

3 IP's en interfaces

- En modo NAT, una interface no puede usarse hasta que no tiene una IP:
  - Configurada manualmente
  - Automática
    - DHCP / PPPoE
- **La guía STIC recomienda : deshabilitar administrativamente los interfaces no utilizados y usar etiquetas descriptivas**

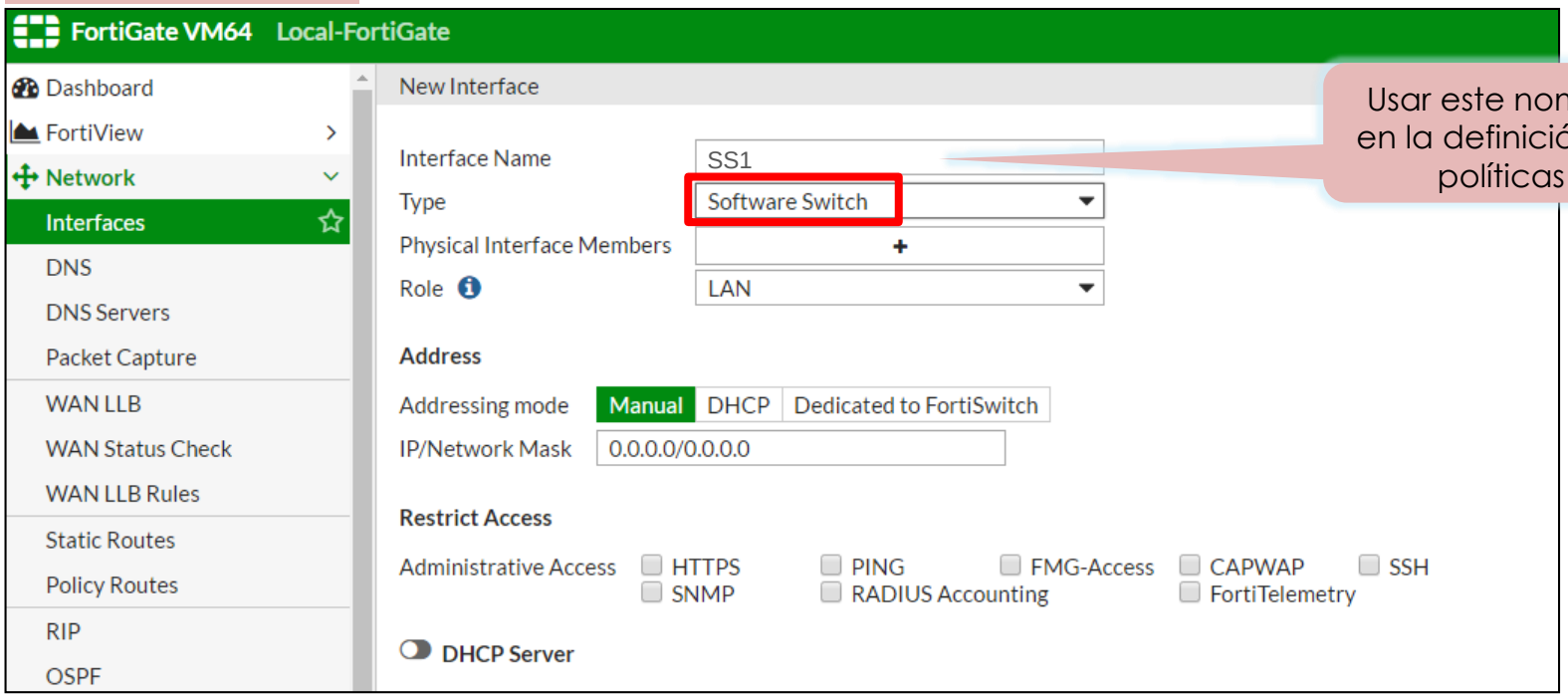


3.1 SoftSwitch

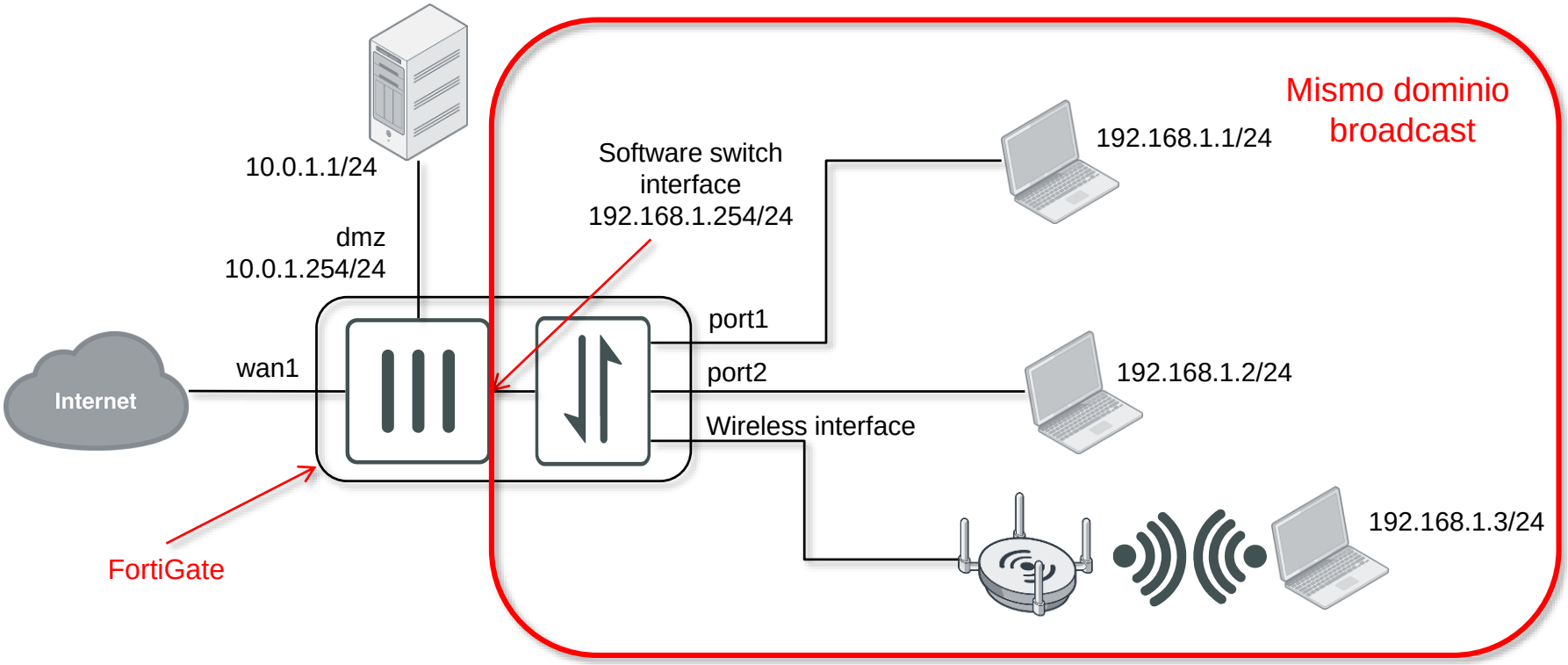
- Puede agrupar múltiples interfaces físicos y Wireless en un único interface "virtual switch"
- Sólo soportado en modo NAT.
- Funciona como un switch de nivel 2 tradicional.
- Los interfaces:
  - Comparten la misma IP
  - Pertenecen al mismo dominio Broadcast

3.1 SoftSwitch: Configuración

Network > Interfaces



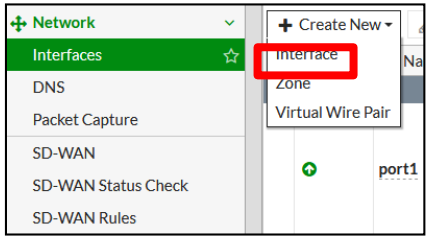
3.1 SoftSwitch: Ejemplo

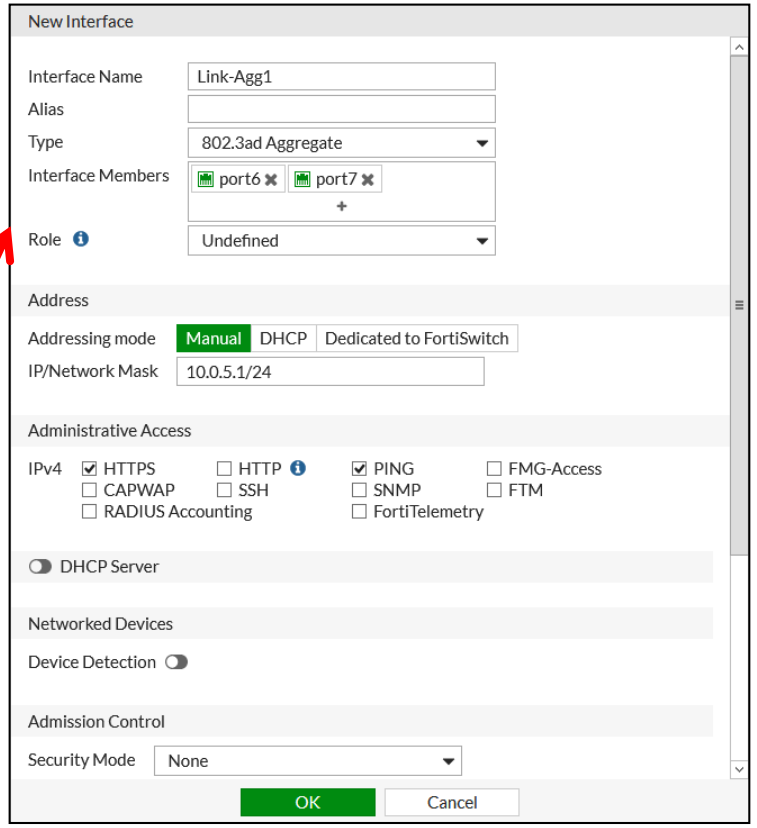


3.2 Agregación de enlaces

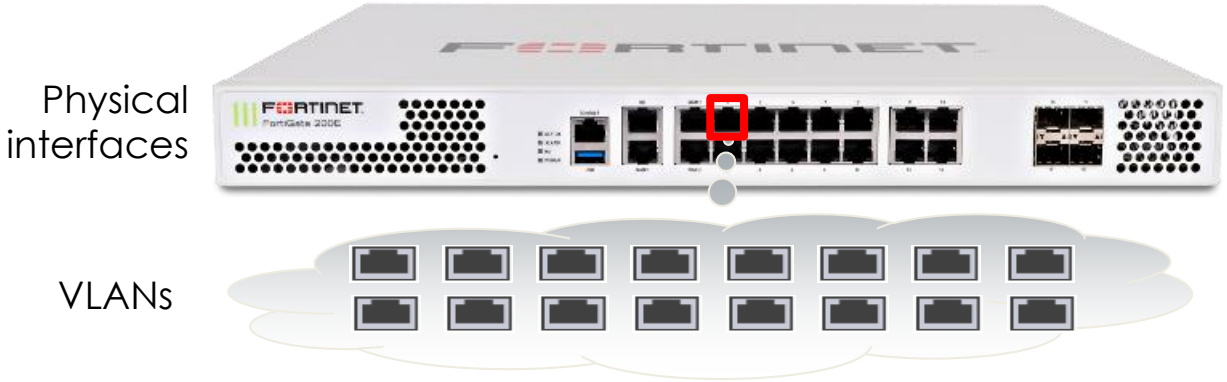
- Une varios puertos físicos para construir un único canal lógico de más ancho de banda.
  - Incrementa la redundancia, mejorando la disponibilidad.

Network > Interfaces



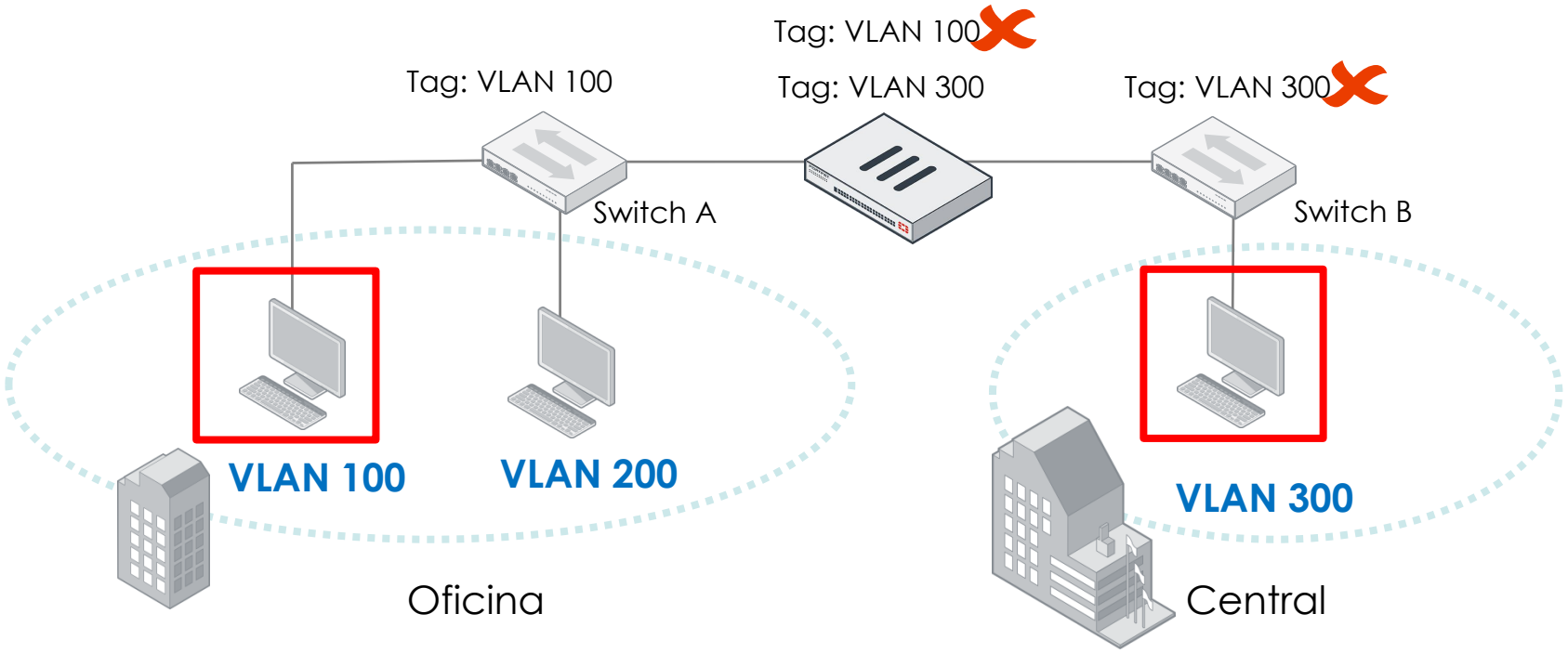


3.3 VLAN



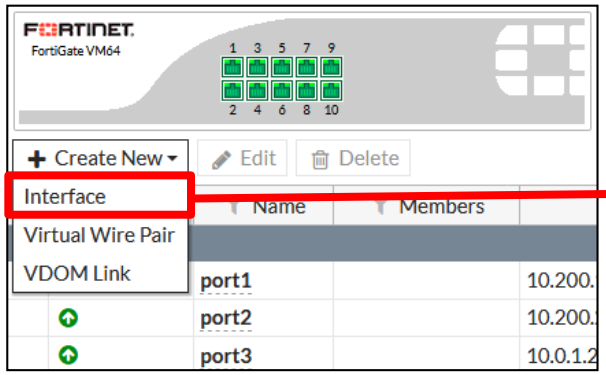
- Permite dividir la red física de nivel 2 en segmentos más pequeños.
  - Cada segmento forma una dominio broadcast separado.
  - Se añaden tags de vlan para identificar el segmento correspondiente.

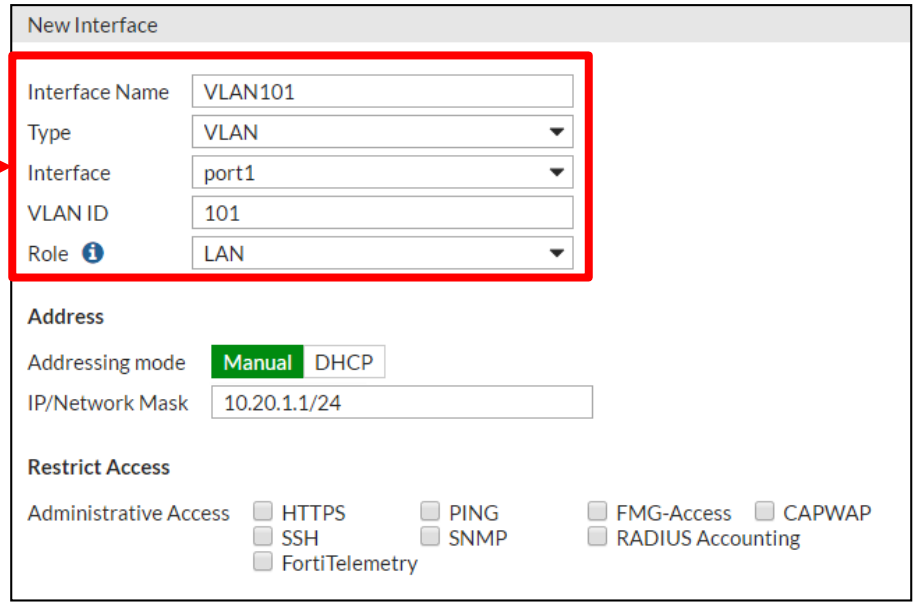
3.3 VLAN: Ejemplo



3.3 VLAN: configuración

Network > Interfaces

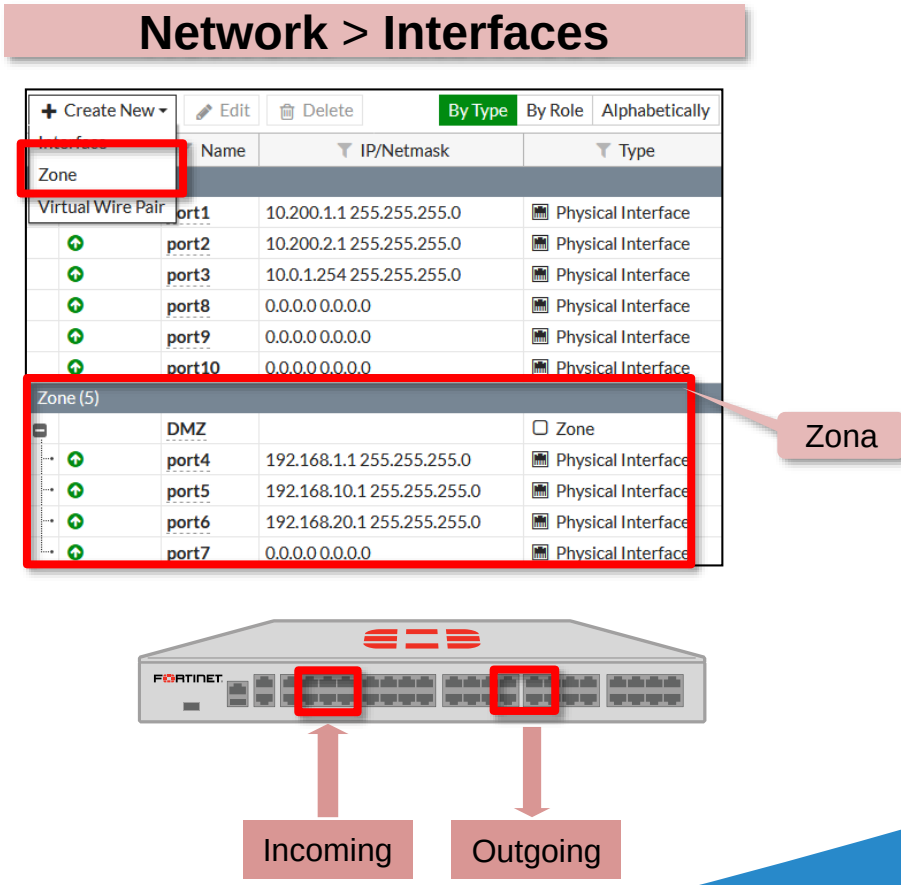




- Los Frames enviados o recibidos por el interface físico que no llevan tag, pertenecen a la VLAN Nativa.

3.4 Zonas

- Se pueden agrupar diferentes interfaces, que tienen características de seguridad comunes, en Zonas.
- Las zonas son agrupaciones lógicas de interfaces que se pueden usar en las políticas, para simplificar la política reduciendo su número.

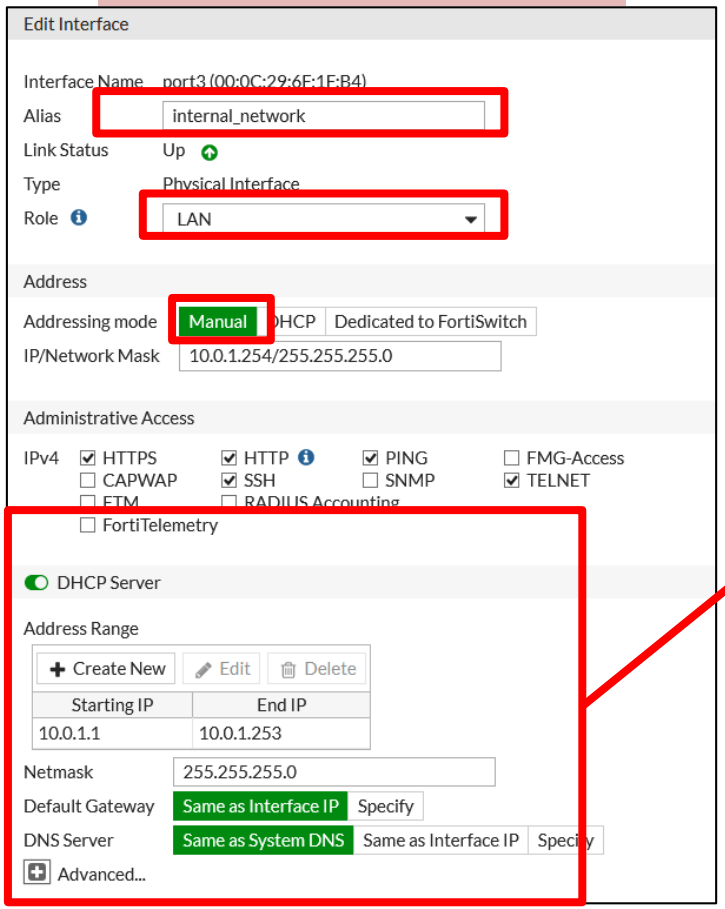


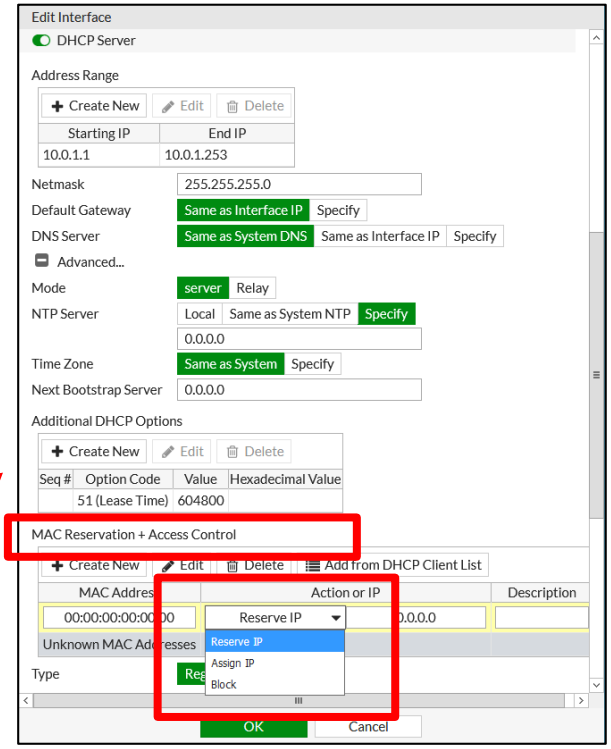
3.5 DNS

- FortiGate incluye un servidor DNS que resuelve peticiones DNS de la red interna.
  - Habilitado por interface
- La BBDD de DNS puede compartirse entre todos los interfaces.
- Métodos de resolución:
  - Forward: reenviar las peticiones al siguiente servidor DNS (configurado en "DNS settings").
  - Non-recursive: Usa solo la BBDD configurada en FortiGate.
  - Recursive: Usa primero la BBDD DNS de FortiGate; reenvía aquellas peticiones para las que no tenga una entrada local al servidor configurado en DNS-> Settings.

3.6 DHCP

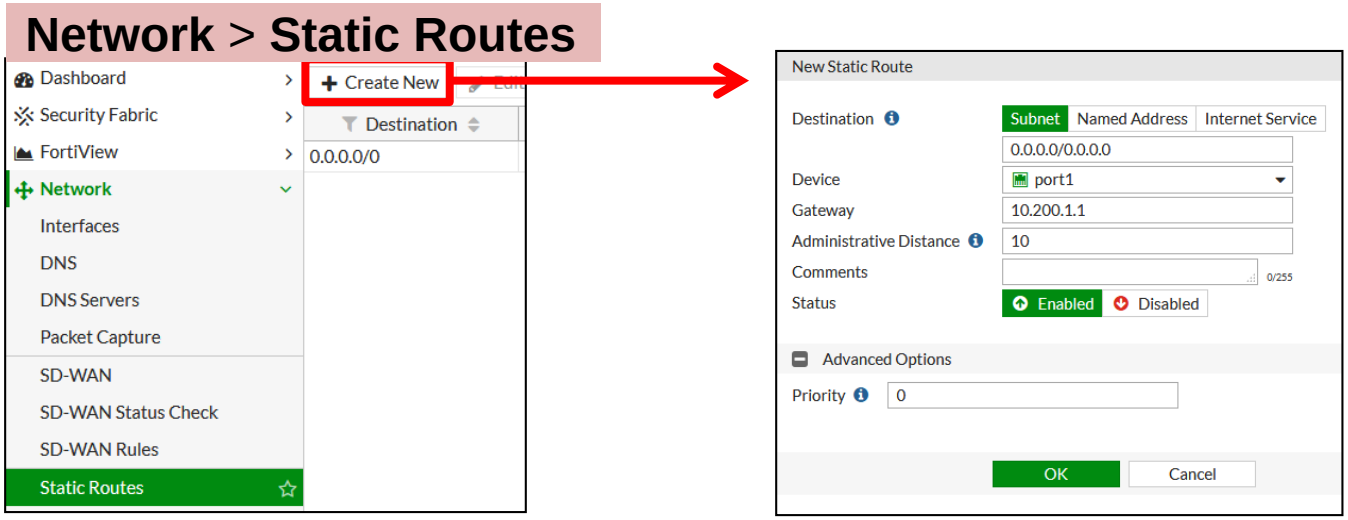
Network > Interfaces





3.7 Routing Estático

- Lo normal es que exista al menos un Gateway por defecto.
- Si el interface recibe la IP por DHCP o PPPoE, se puede recibir también el Gateway por defecto.

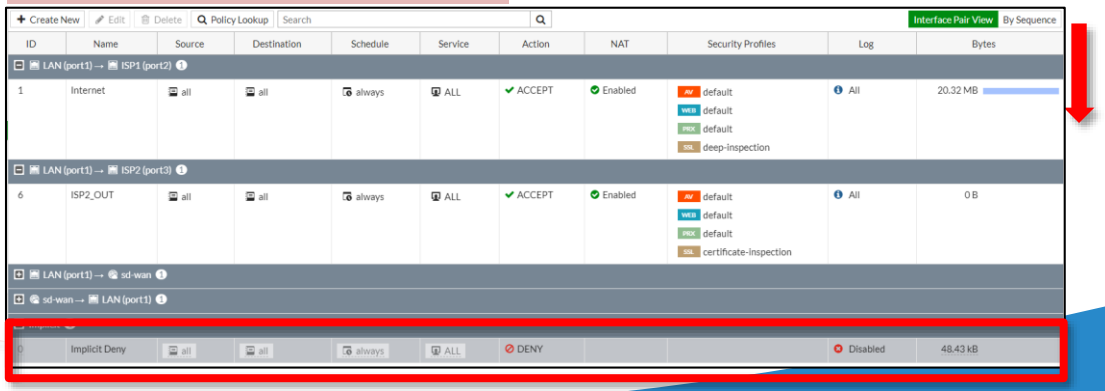


Índice

4.- Políticas de Seguridad

- En las políticas se define:
  - Qué tráfico se gestiona en cada regla
  - Cómo procesar ese tráfico.
- Cuando llega una nueva sesión, FortiGate:
  - Comienza a buscar la política que encaja de arriba hacia abajo
  - Aplica la primera política e ignora el resto.
- **Deny implícito**
  - Si la sesión no encaja con ninguna política, se deniega.

Policy & Objects > IPv4 Policy



Deny implícito

4.1- Políticas de Seguridad: Gestión de objetos

Las políticas usan diferentes tipos de objetos

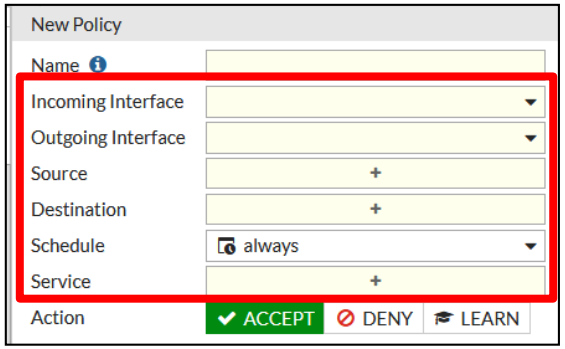
- Interfaces y grupos de interfaces
- Dirección, usuario, dispositivo, Internet Service Definition
- Servicios (puertos más protocol)
- Tiempo
- NAT
- Perfiles de seguridad.

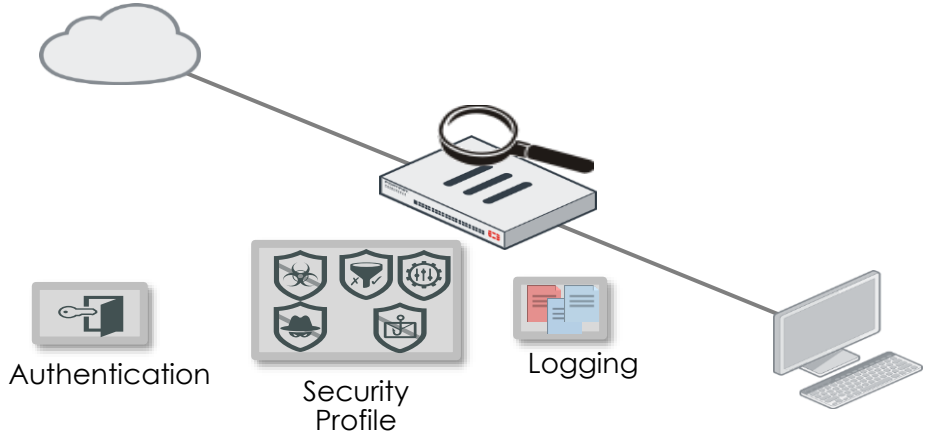
4.1- Políticas de seguridad: Gestión de objetos

- Interfaces de entrada y salida ✓
- Origen: IP, usuario, Dispositivo ✓
- Destino: IP o Internet Services ✓
- Servicios ✓
- Tiempo ✓

Ación = ACCEPT o DENY

Policy & Objects > IPv4 Policy

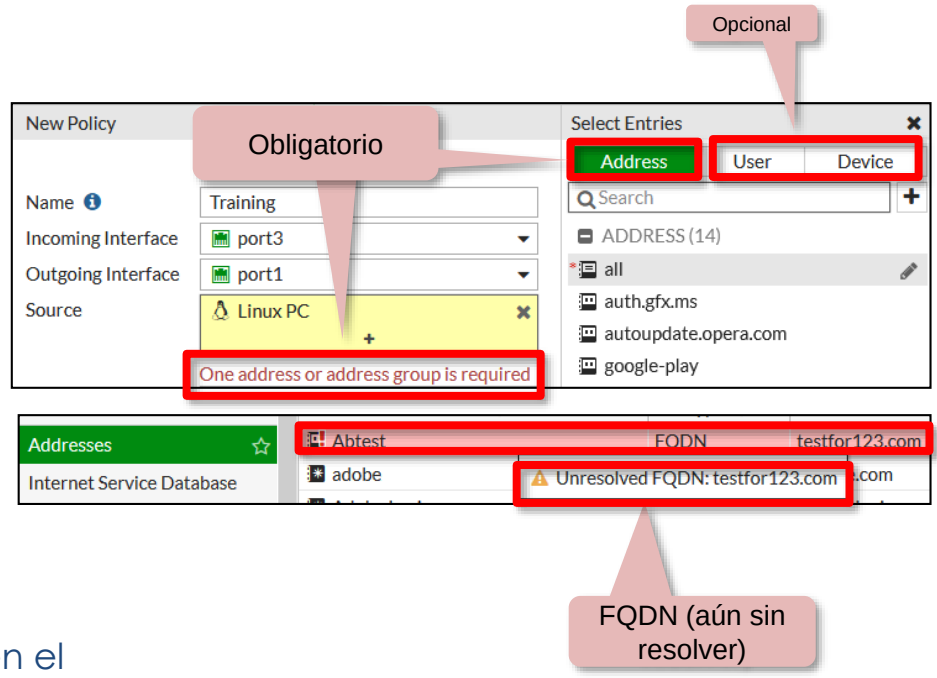




4.1- Gestión de Objetos: ORIGEN

- *Siempre se incluye un objeto que indique dirección de origen:*
  - IP o rango
  - Subred (IP/Netmask)
  - FQDN
  - Geografía
- *Adicionalmente, puede incluir:*
  - Usuario/grupo Origen
  - Dispositivo Origen
- Identificación de dispositivos:
  - Permite la identificación de dispositivos en el interface de origen
- Internet Service Database (ISDB)

Policy & Objects > IPv4 Policy



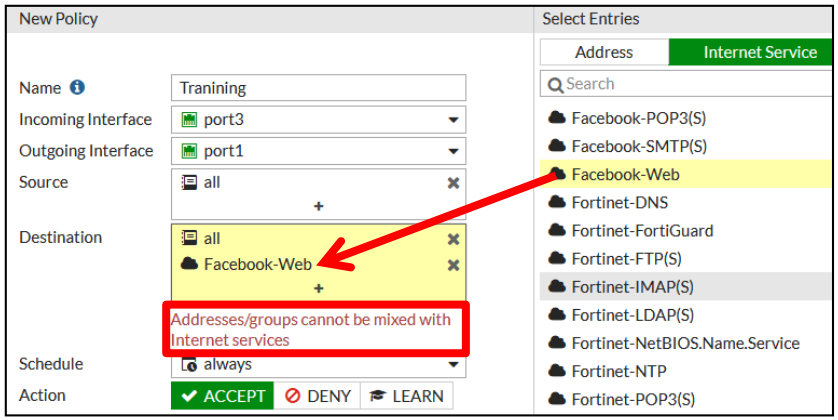
4.1- Gestión de Objetos: Internet Services

- Base de datos que contiene IP's, protocolos y puertos asociados a los servicios de internet más comunes.
  - Actualizado desde FortiGuard
- Se puede usar como **Origen** o como **Destino** de la política.
- Si se usa un **Internet Service** como **origen**:
  - No se puede usar una **Dirección** como **Origen**
- Si se usa un **Internet Service** como **Destino**:
  - No se puede usar **Address** en el **origen**
  - No se puede usar **Service** en la política.

Policy & Objects > Internet Service Database

Name	Protocol Number	Port	# of Entries
LinkedIn-Web	TCP	80,443	2496
LogMeIn-DNS	UDP	53	3
LogMeIn-NetBIOS.Name.Service	UDP	137	6
LogMeIn-SMTP(S)	TCP	25,465,587,2525	3
LogMeIn-Web	TCP	80,443	1095

Policy & Objects > IPv4 Policy



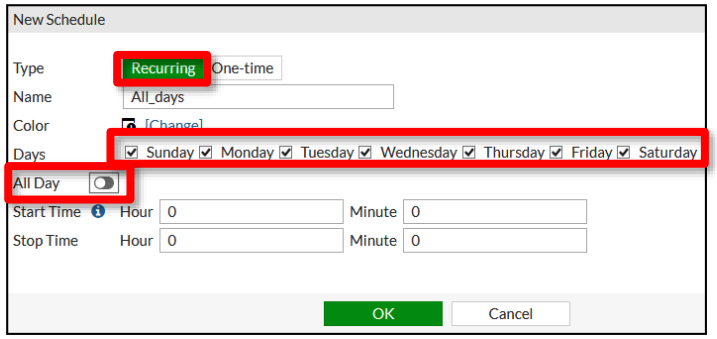
4.1- Gestión de Objetos: Schedules

- Las políticas son válidas solo durante ciertas horas del día.

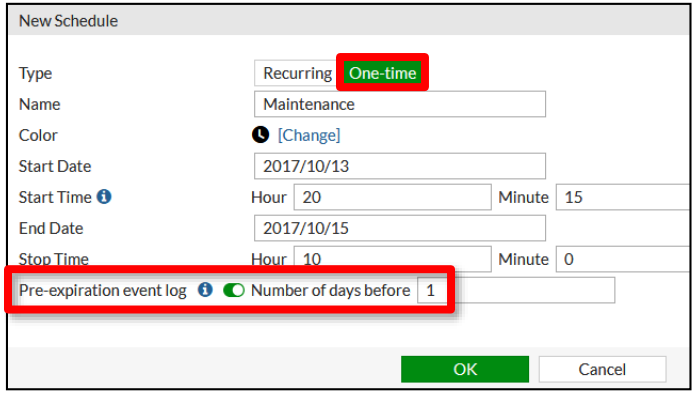
- Recurrente
  - Cada vez durante ciertas horas de todos los fines de semana

- Una vez
  - Ocurre solo en una ocasión

Policy & Objects > Schedules

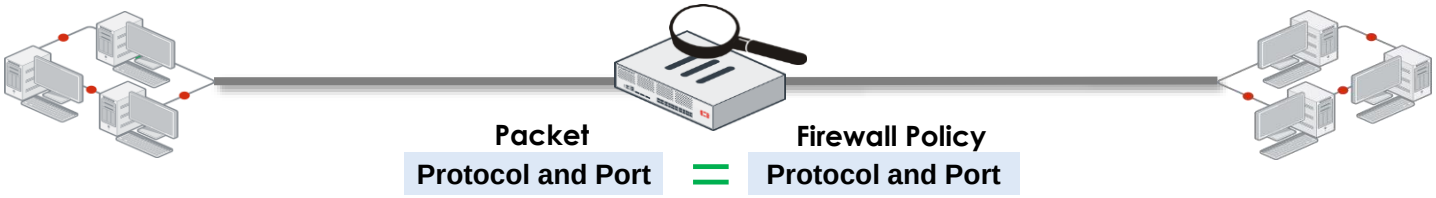


Policy & Objects > Schedules



4.1- Gestión de Objetos: Services

- El servicio determina el protocol (UDP, TCP…) y número de puerto
- Puede ser predefinido o creado por el usuario.



Policy & Objects > Services

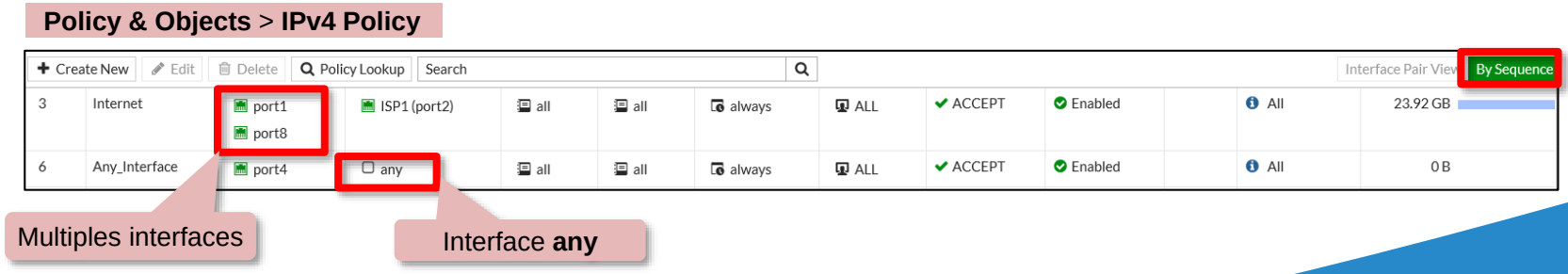
+ Create New | Edit | Clone | Delete | Category Settings | Search | By Category | Alphabetically

Service Name	Category	Details	IP/FQDN	Show in Service List	Ref.
General (4)					
ALL	General	ANY		✓	3
ALL_ICMP	General	ICMP/ANY		✓	0
ALL_TCP	General	TCP/1-65535	0.0.0.0	✓	0
ALL_UDP	General	UDP/1-65535	0.0.0.0	✓	0
Web Access (2)					
HTTP	Web Access	TCP/80	0.0.0.0	✓	1
HTTPS	Web Access	TCP/443	0.0.0.0	✓	2

4.3- Trabajar con la política

- Interface Pair View
  - Lista las políticas agrupadas por interface de entrada y salida

- Por secuencia
  - Si se crea alguna política con múltiples interfaces de entrada o salida (o any)



4.4- Trabajar con la política: Mover políticas

- Desde la GUI, se puede cambiar el orden de las políticas simplemente seleccionando y moviendo (*Drag and Drop*)

Antes de mover

ID	Name	Source	Destination	Schedule	Service	Action
port3 → port1 (2)						
1	Full_Access	LOCAL_SUBNET	all	always	ALL	ACCEPT
2	Block_FTP	all	all	always	FTP	DENY

Después de mover

ID	Name	Source	Destination	Schedule	Service	Action
port3 → port1 (2)						
2	Block_FTP	all	all	always	FTP	DENY
1	Full_Access	LOCAL_SUBNET	all	always	ALL	ACCEPT

ID permanece igual

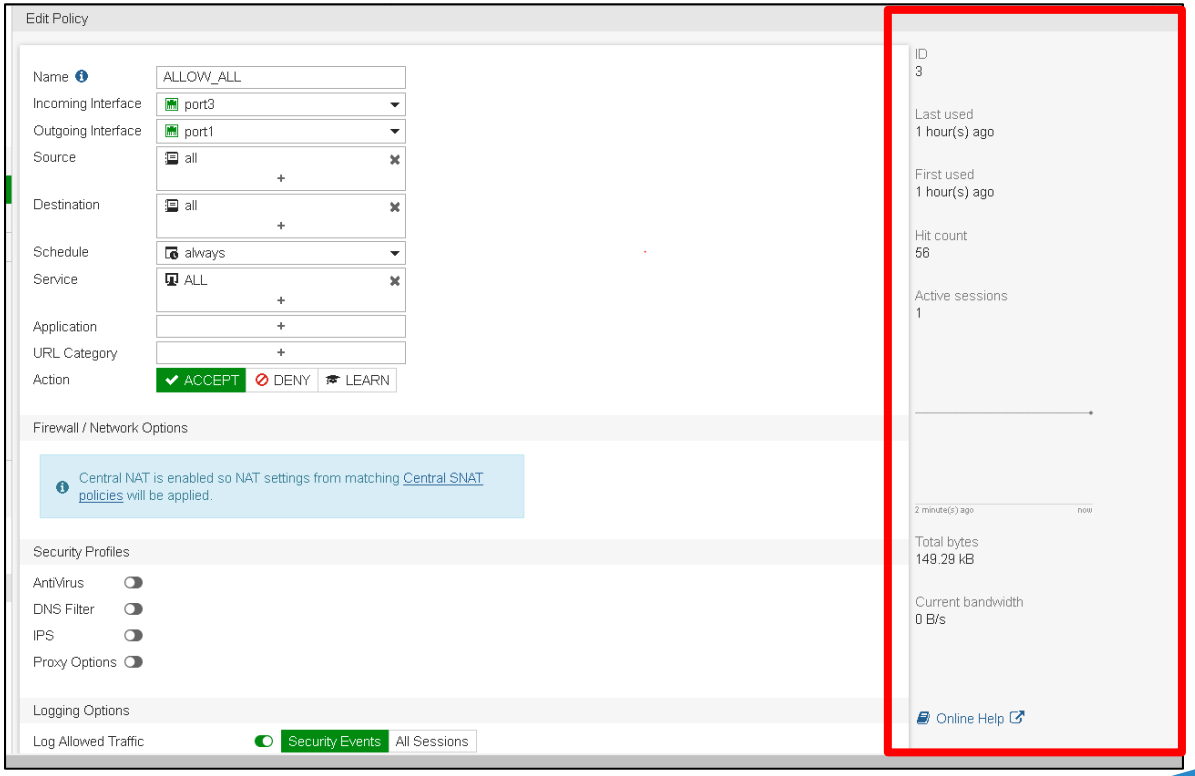
```
config firewall policy
  edit 1
    set name "Full_Access"
...
next
  edit 2
    set name "Block_FTP"
```

```
config firewall policy
  edit 2
    set name "Block_FTP"
...
next
  edit 1
    set name " Full_Access"
```

4.4- Trabajar con la política: Estadísticas de uso

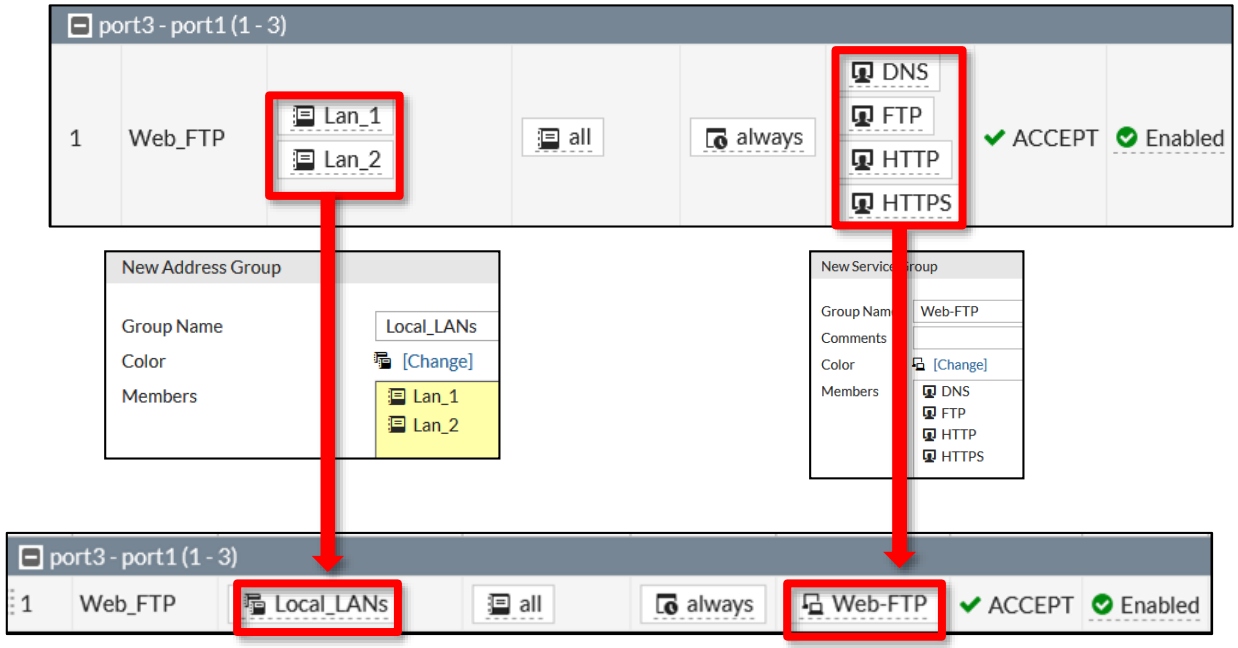
- Mientras se edita, Se puede ver el uso de la política en tiempo real

  - ID
  - Last Used
  - First Used
  - Hit Count
  - Active Sessions
  - Total Bytes
  - Current Bandwidth



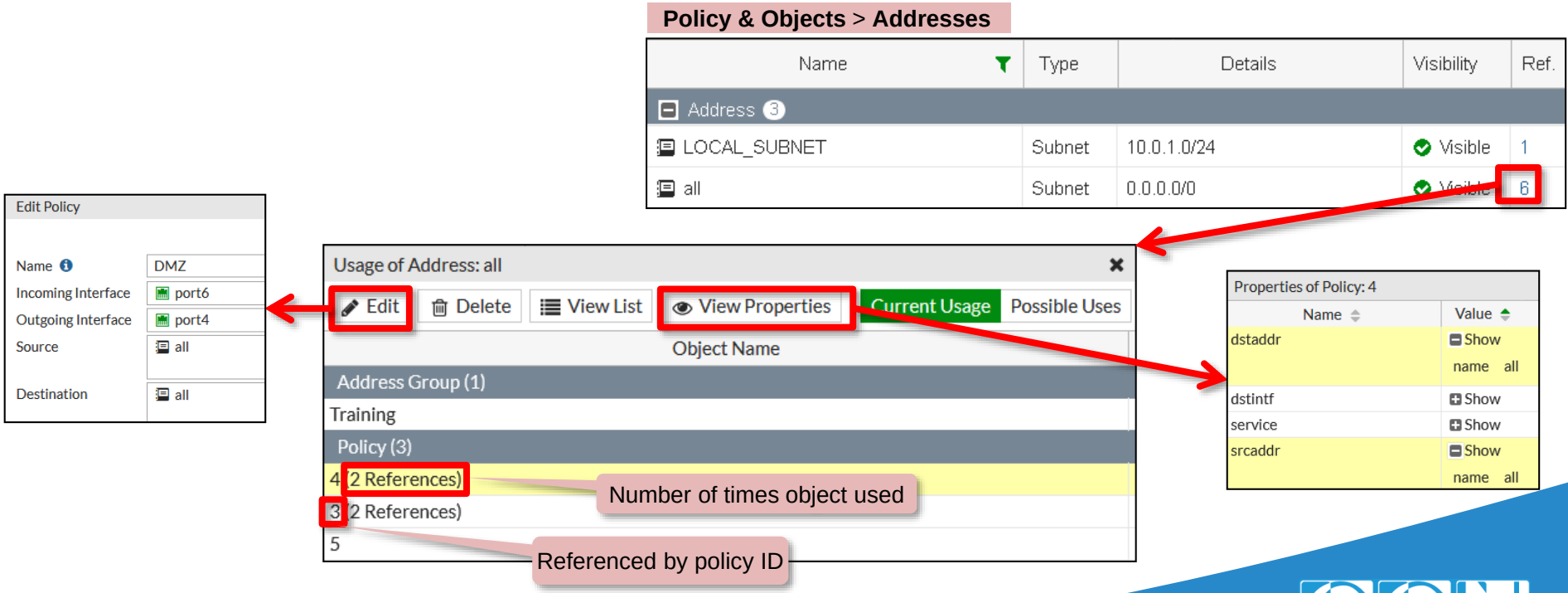
4.4- Trabajar con la política: Agrupar objetos

- Se pueden agrupar objetos (address group, Service Group) para simplificar las políticas.



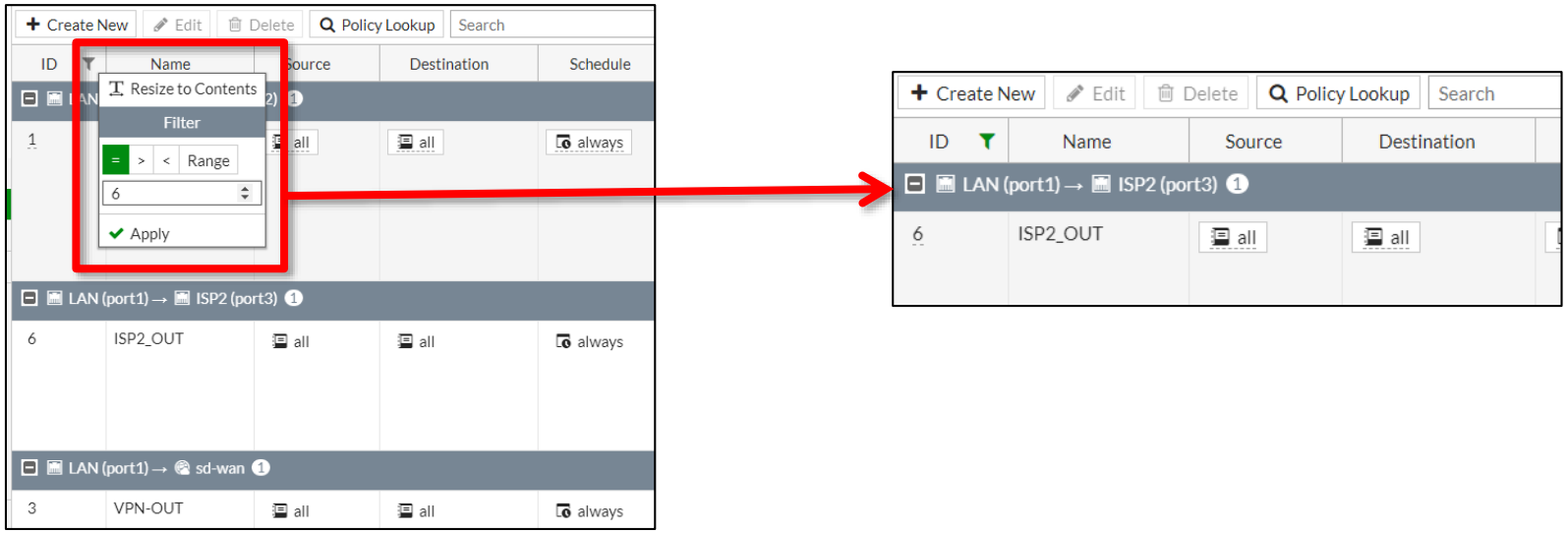
4.4- Trabajar con la política: Uso de objetos

- Permite evaluar el uso de un objeto
- Existe una columna de referencia que indica en cuántos sitios se usa, e incluso se puede obtener un listado.



4.4- Trabajar con la política: filtrado de columnas

- Se pueden realizar diferentes filtrados de columnas, con el fin de encontrar una o más políticas que respondan a un criterio determinado.

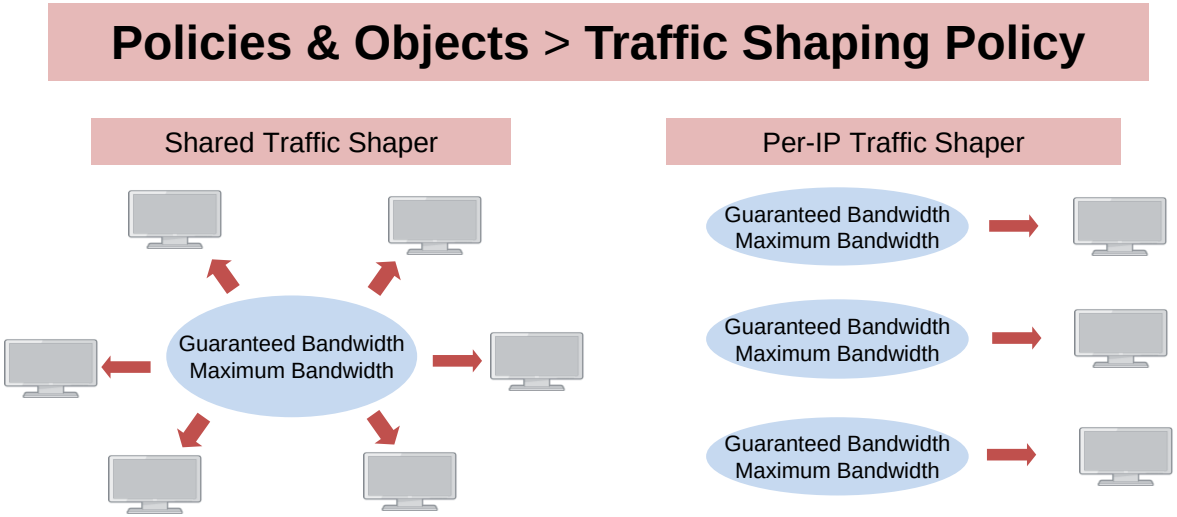


4.4- Trabajar con la política: Policy Lookup

- Permite identificar qué política procesaría un flujo sin que sea necesario que exista ese flujo
  - No genera ningún paquete.
- Busca qué política encaja en función de los criterios que se marquen
  - Interface de origen / Protocolo / IP origen / IP-FQDN Destino
- la funcionalidad además comprueba:
  - Que se cumple el Reverse Path forward (RPF)
  - El NAT de destino, si cae en una política asociada a una VIP
  - Búsqueda de rutas

4.5- Traffic Shapping

- Permite limitar la cantidad de tráfico, según un criterio definido por el administrador.
  - Ancho de banda de entrada y de salida
  - Define un máximo y un garantizado.



4.5- Best Practices (guía STIC)

- Sólo deberá utilizarse la variable "any" cuando esté debidamente justificado. "
- Siempre debe seguirse el principio de mínima funcionalidad y mínimo privilegio de modo que sólo se permita el tráfico necesario y no otro en la franja horaria necesaria"
- Como el procesado se hace de arriba abajo, es conveniente disponer las reglas que mas se usan al principio
- Cuando se desactiven o activen reglas en un entorno en producción hay que hacerlo cuidadosamente al tomar efecto inmediatamente
- Es conveniente poner descripciones a las reglas para una mas fácil administración de las mismas
- Es recomendable activar el log a todas las reglas, incluida la implícita , vigilando el uso de recursos.

4.5- Best Practices (guía STIC)

- Se recomienda configurar el equipo para que registre los logs de forma centralizada en un dispositivo externo. Este dispositivo puede ser un servidor de Syslog o Siem (Fortinet dispone de FortiAnalyzer y FSIEM). “
- Al final de la guía (pág.62) de la guía hay un checklist que ayuda a verificar si se han llevado a cabo las recomendaciones de la misma, esto facilita hacer una revisión rápida de la instalación segura del equipo y además sirve para guardar registro de la correcta instalación.
- La herramienta ROCIO puede hacer una auditoría automatizada usando un archivo de configuración en modo texto, y entregando

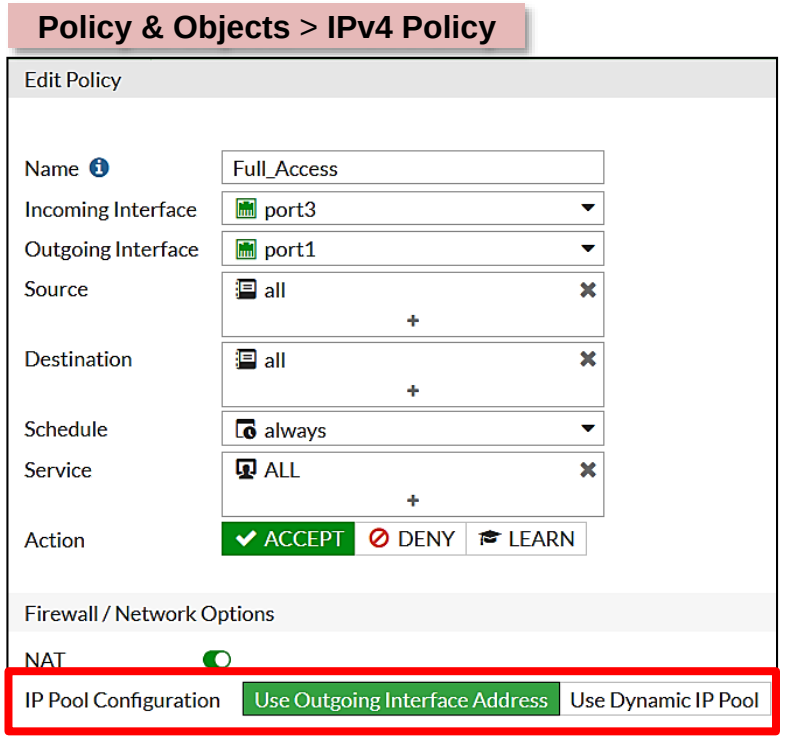
Índice

5.1 NAT: Introducción

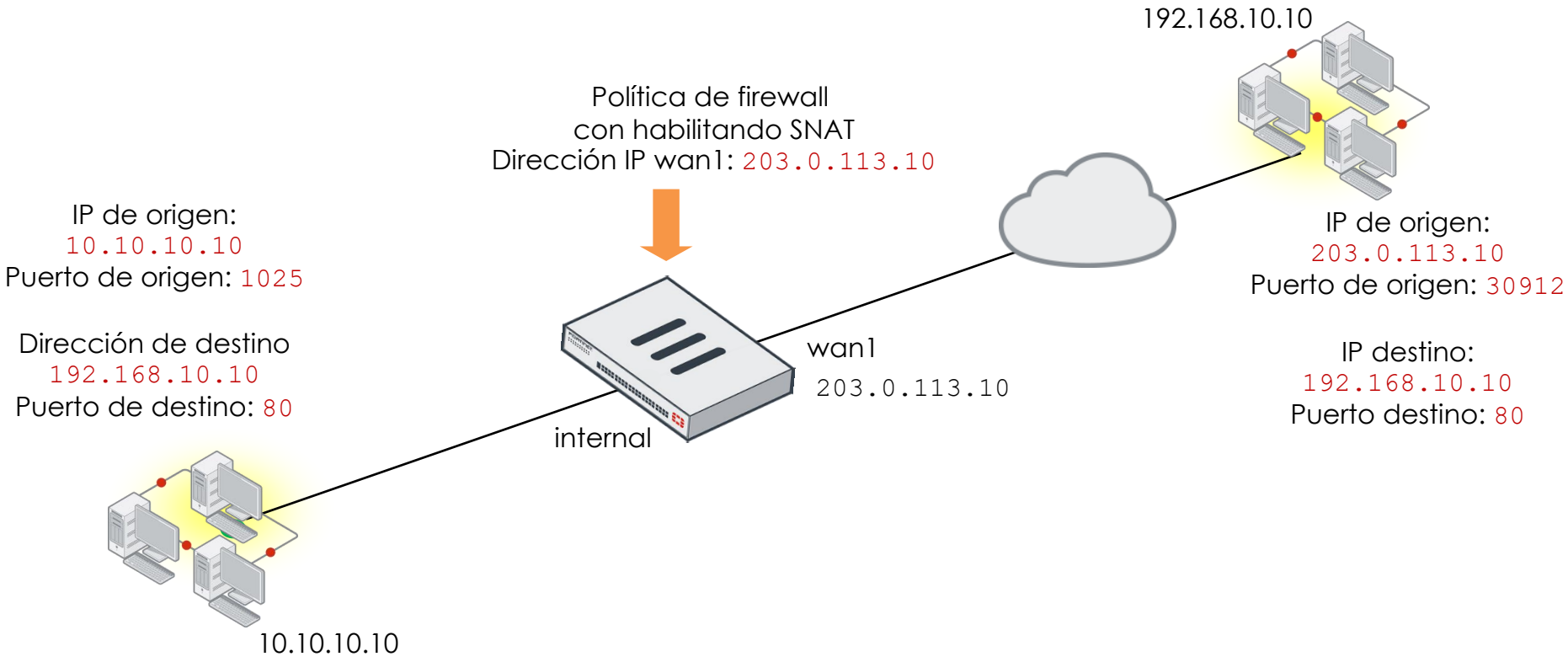
- NAT
  - Cambia la dirección IP de ciertos paquetes que atraviesan el firewall
  - Las redes interiores usan direccionamiento Privado. Este direccionamiento sólo tiene sentido dentro de la propia red, Internet no lo encamina.
  - Es necesario que el tráfico que tenga que atravesar internet use una IP Pública como origen y como destino.
  - Source NAT (SNAT): Típicamente, tráfico generado en mi red y destinado a un servidor público (en internet)
  - Destination NAT (DNAT): Típicamente, tráfico con origen en internet y destino un servidor de mi red, que aparece al exterior con una IP pública, pero que usa una IP Privada.
- PAT (NAT Overload)
  - Mapea Mútliple IP's privadas a una única IP pública, usando un Puerto de origen distinto para cada IP privada

5.2 NAT de origen: Configuración

- Existen dos formas de configurar SNAT:
  - Usando la IP del interface de salida
  - Usando un Pool dinámico.



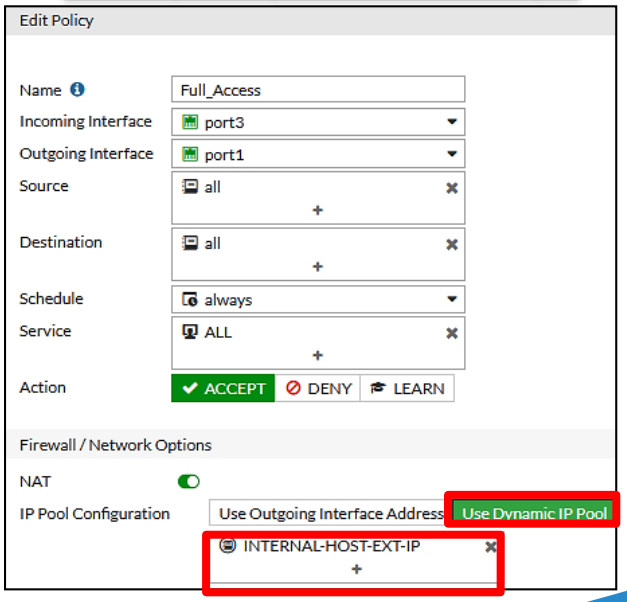
5.2 NAT de origen: Usando la IP del interface



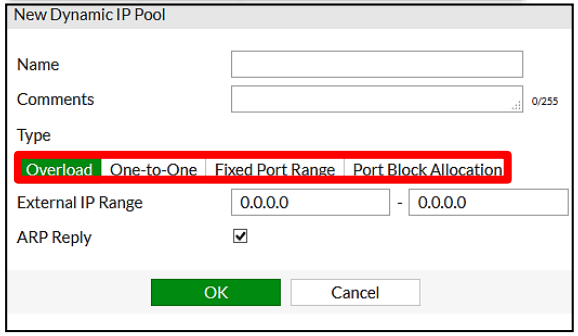
5.2 NAT de origen: Usando pools "overload"

- Los Pools IP definen una IP o rango de IP's que pueden usarse como IP de origen traducida durante la duración de la sesión.
- Los Pools IP (normalmente) usan IP's del mismo rango que la interface de salida
- FortiGate soporta 4 tipos de pool:
  - Overload (por defecto)
  - One-to-one – (1-a-1)
  - Fixed port range (Puerto Fijo)
  - Port block allocation (asignación de bloques de puertos)

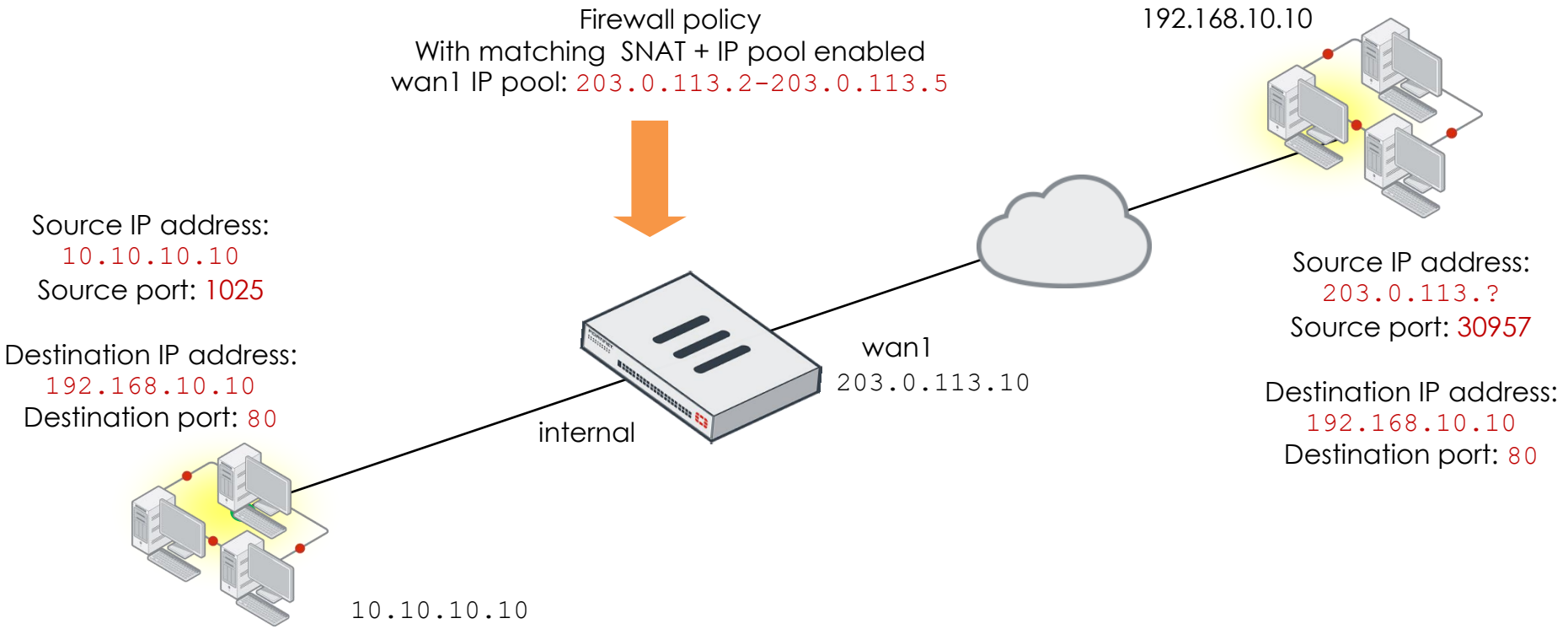
Policy & Objects > IPv4 Policy



Policy & Objects > IP Pools



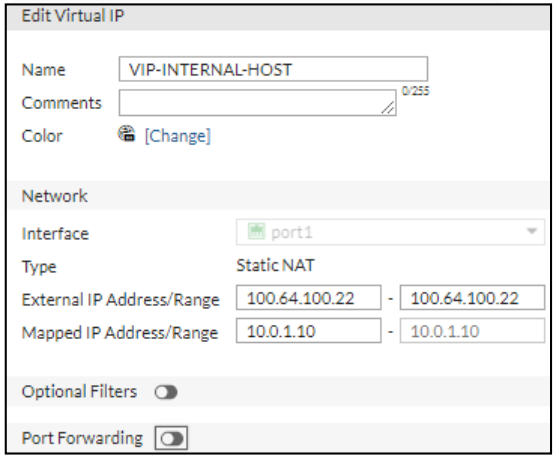
5.2 NAT de origen: Usando pools overload



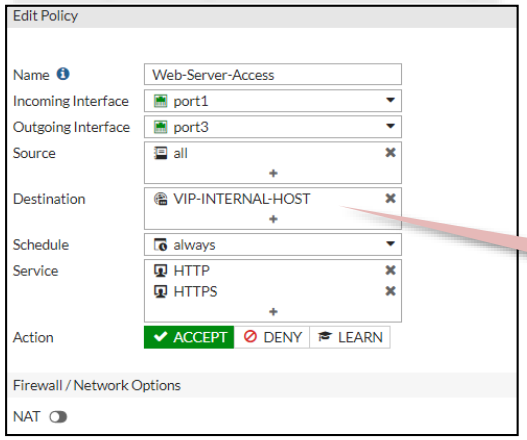
5.3 Nat de destino (VIPS – Virtual IP)

- Objetos VIP
- Normalmente es una traducción estática que se usa para publicar servidores

Policy & Objects > Virtual IPs

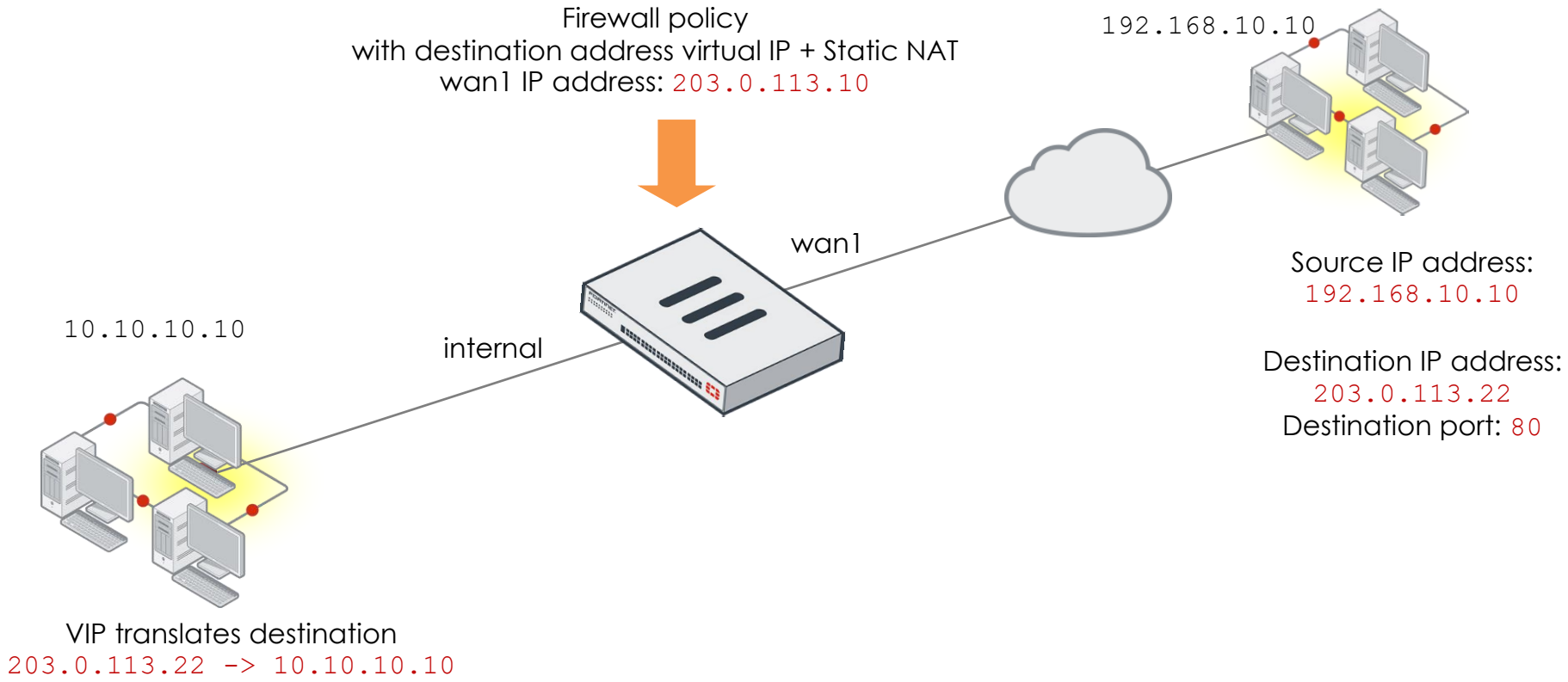


Policy & Objects > IPv4 Policy



El objeto VIP se usa como destino en una política

5.3 VIPS: Ejemplo



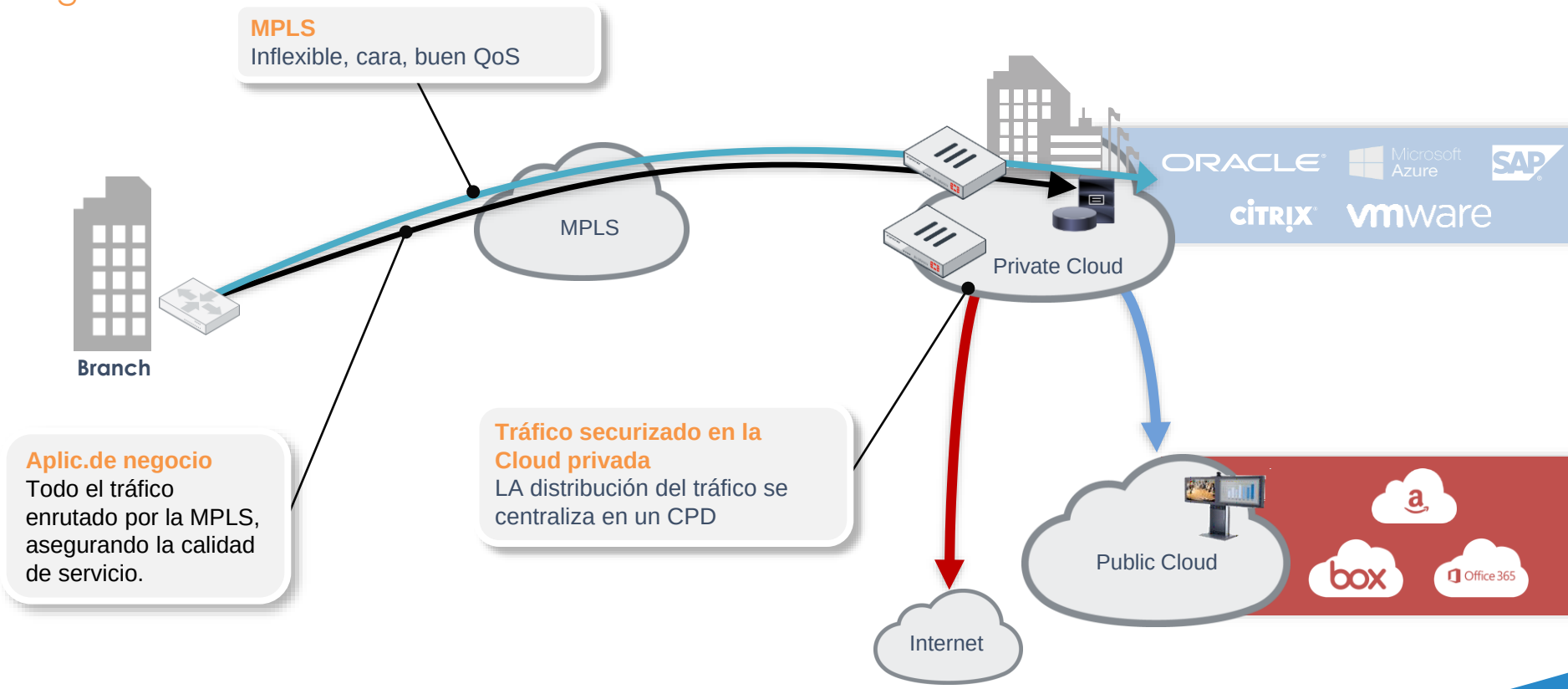
Índice

6.1 SD-WAN: Definición

- Interface Virtual que consiste en una agrupación de interfaces que pueden ser de diferentes tipos.
- Permite el uso efectivo de la WAN gracias a la implementación de diversos algoritmos de balanceo.
- Permite medir la calidad de los enlaces
  - Selección dinámica de los enlaces basada en la calidad
  - Alta disponibilidad para las aplicaciones críticas.

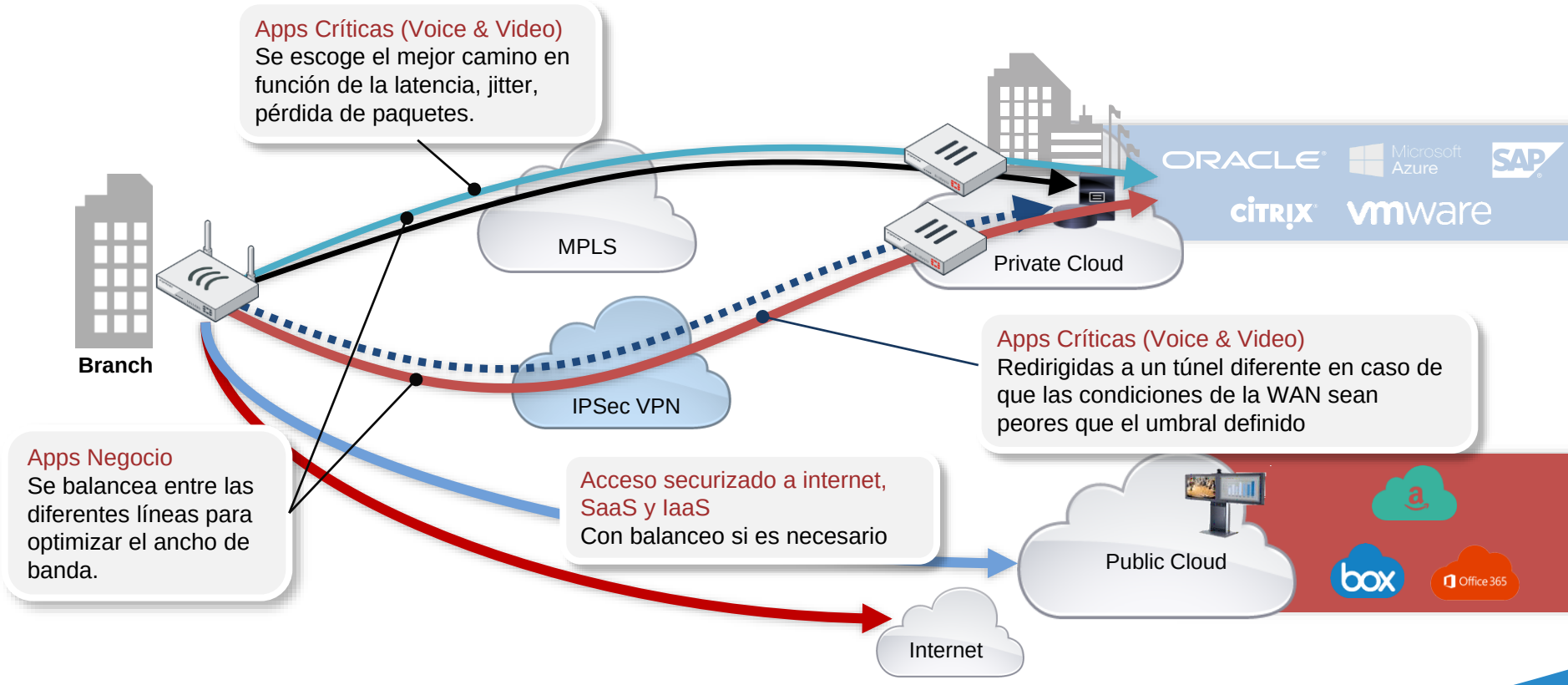
6.1 SD-WAN: Definición (caso de uso)

Migración MPLS



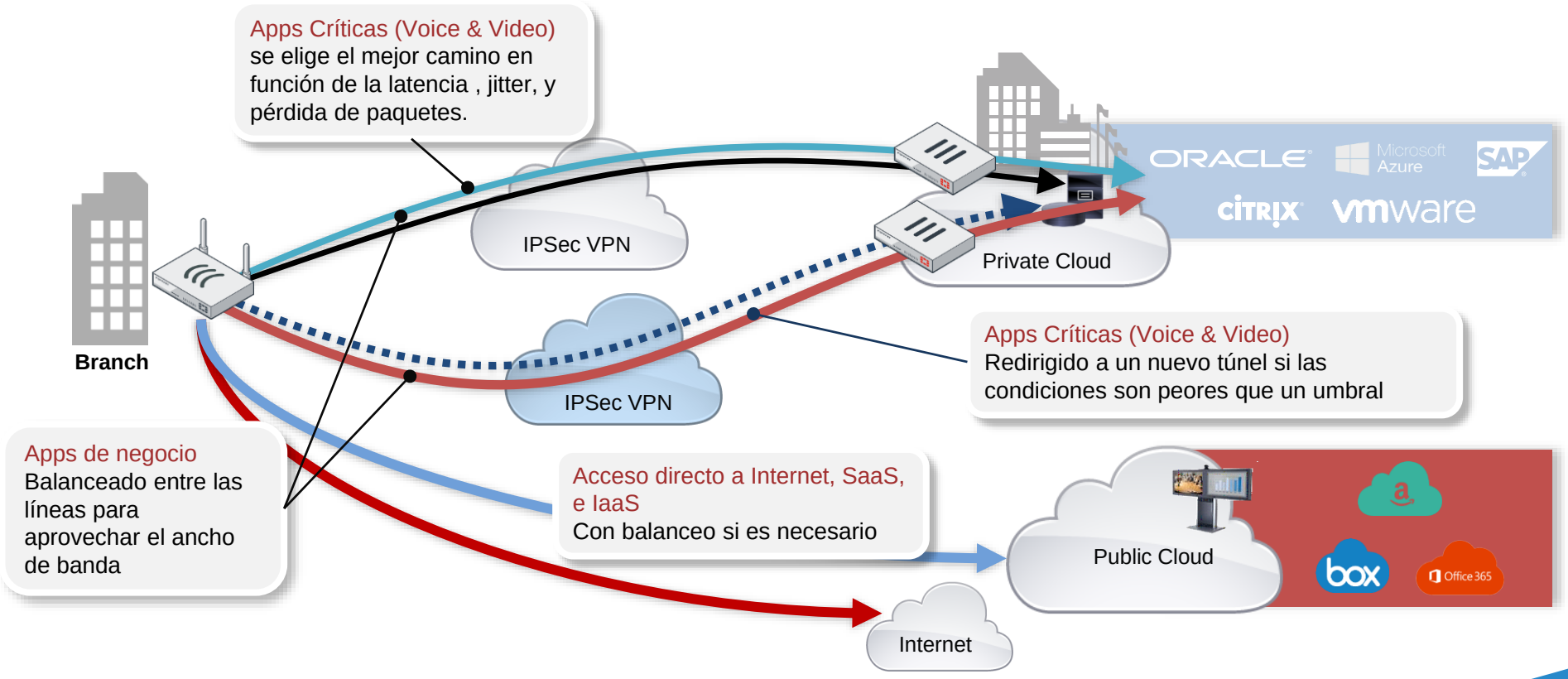
6.1 SD-WAN: Definición (caso de uso)

MPLS backup más acceso local.



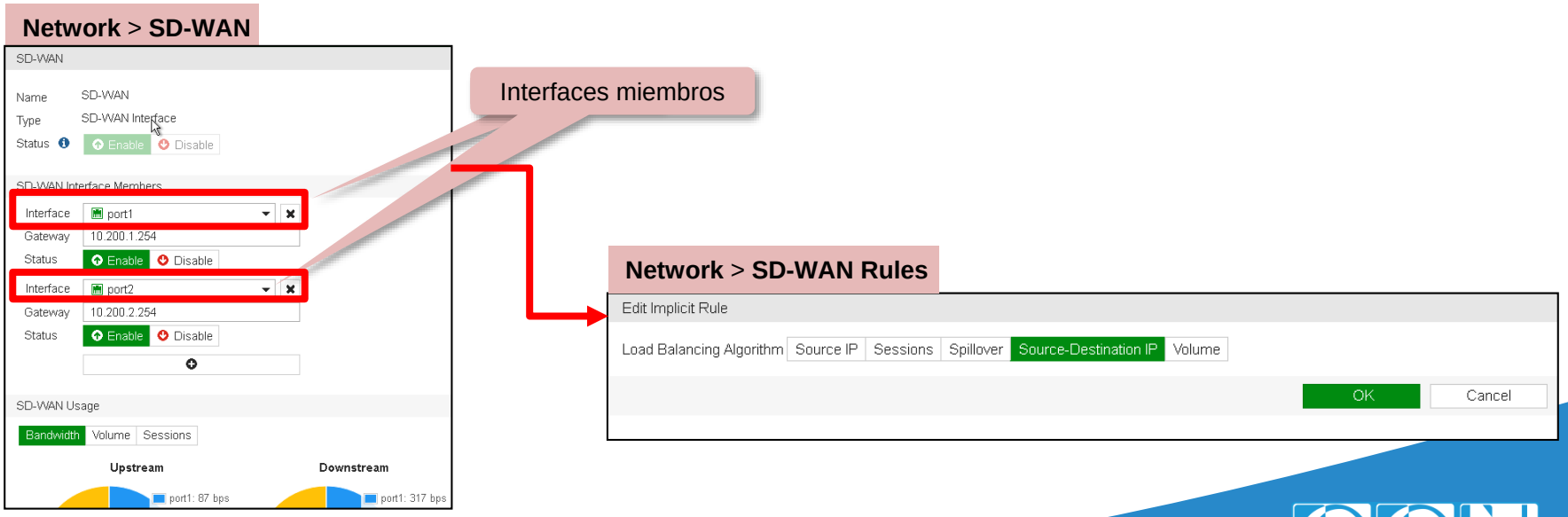
6.1 SD-WAN: Definición (caso de uso)

Reemplazo de la MPLS



6.2 SD-WAN: Creación de interfaces

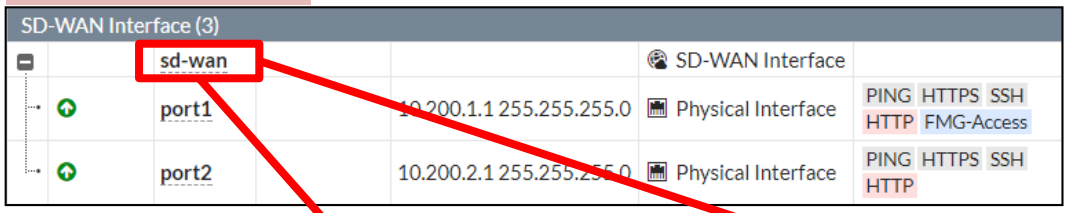
- Especificar al menos dos interfaces y sus Gateway correspondientes
  - Para poder elegirlos, no deberían de estar referenciados en ninguna otra parte de la configuración (rutas o políticas)
  - Soporta interfaces agregados, VLAN, Ipsec…
- Se genera una regla implícita automáticamente para balancear el tráfico.



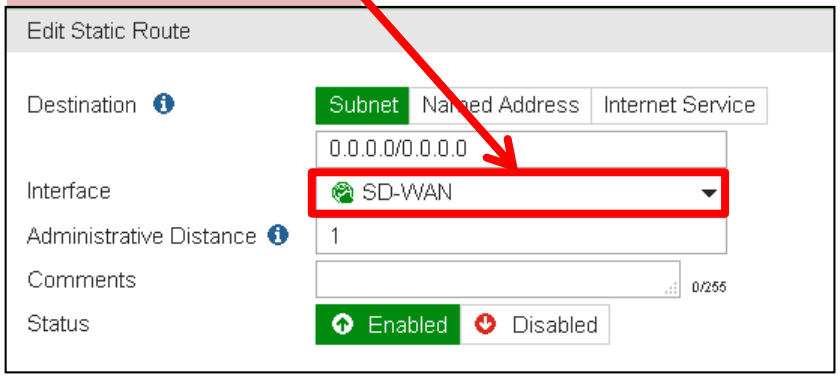
6.3 SD-WAN: Creación de rutas y políticas

- Se crea el interface virtual **sd-wan**
  - Es necesario añadir rutas estáticas y políticas de firewall que se refieran a este interface

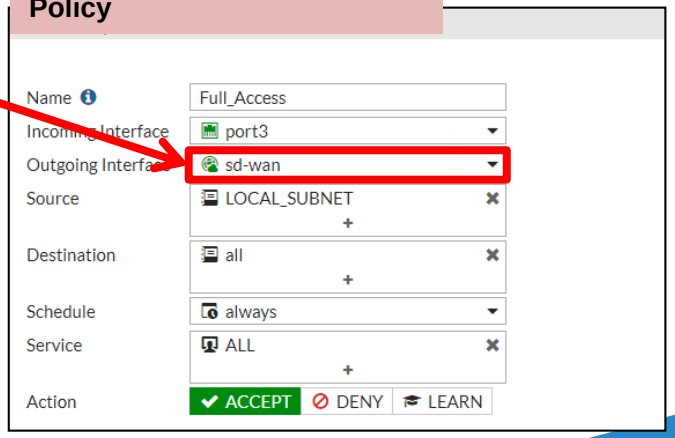
Network > Interfaces



Network > Static

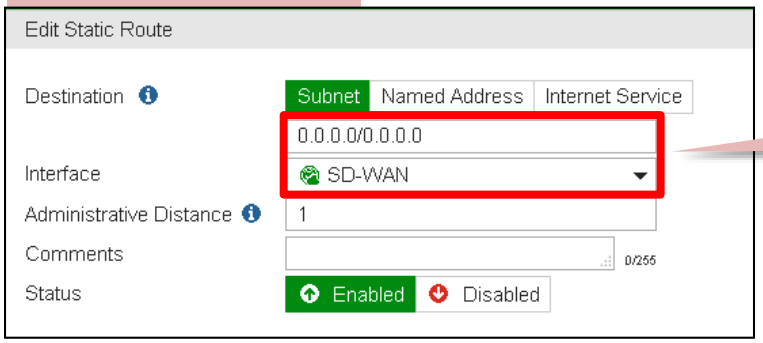


Policy & Objects > IPv4 Policy



6.3 SD-WAN: Creación de rutas y políticas

Network > Static




```
# get router info routing-table all
...omitted output...

S*      0.0.0.0/0 [1/0] via 10.200.2.254, port2
                  [1/0] via 10.200.1.254, port1
C       10.200.2.0/24 is directly connected, port2
C       10.200.1.0/24 is directly connected, port1
```

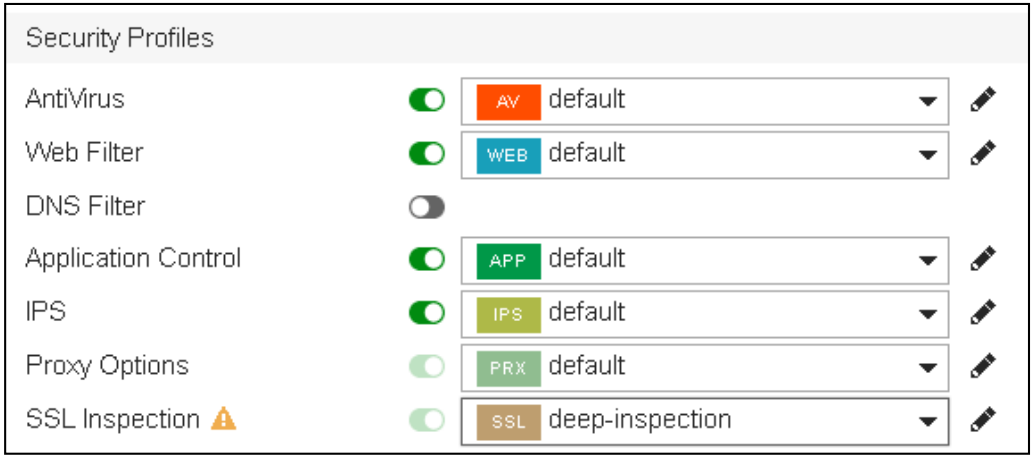
Aunque el admin añade una ruta por defecto que usa el interface **sd-wan**, FortiGate instala rutas individuales para todos los interfaces miembros del interface sd-wan.

Índice

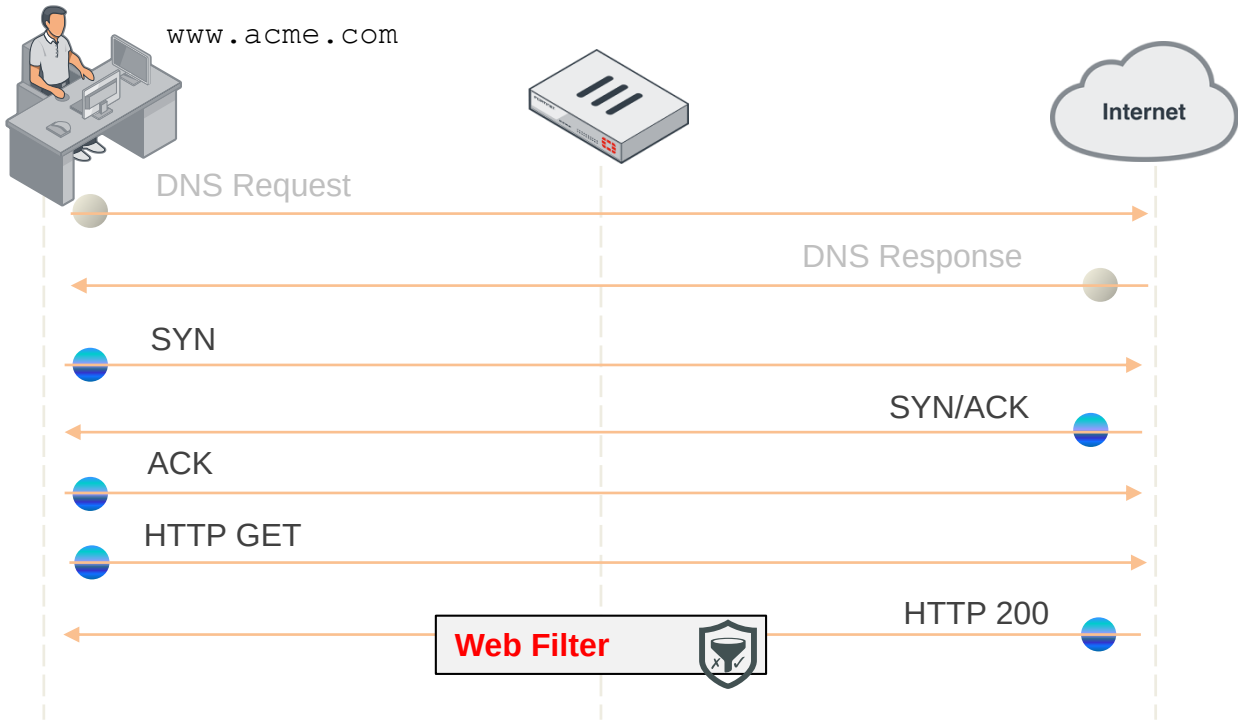
7 Asociación de perfiles a políticas

- Las políticas de seguridad permiten o deniegan el acceso a redes y recursos.
- Los perfiles de seguridad asociados a las políticas protegen la red:
  - Bloqueando Amenazas
  - Controlando el acceso a ciertas aplicaciones y URL's
  - Previniendo que ciertos datos abandonen la empresa.

Policy & Objects > **IPv4 Policy**



7.1 WebFiltering: Fundamentos

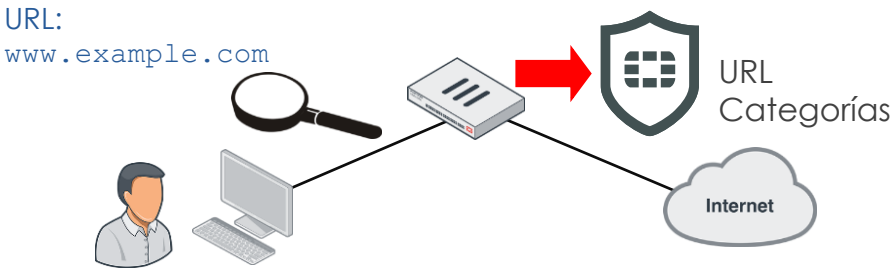


El filtrado se hace en base a la respuesta

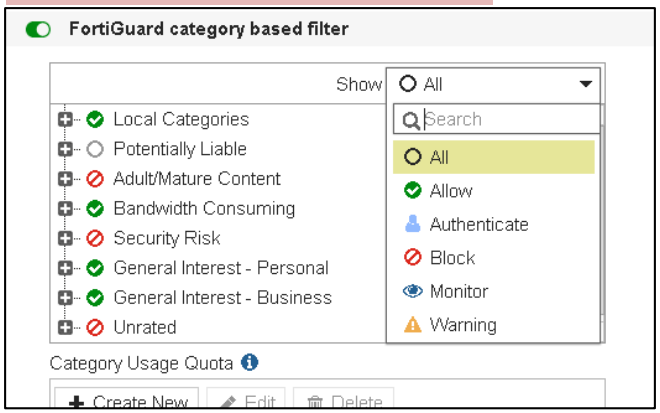
7.1 WebFiltering: Categorías FortiGuard

- Divide las URLS entre diferentes categorías y subcategorías
- Requiere hacer peticiones en vivo a FortiGuard
  - Requiere contrato en vigor
  - Existe un período de gracia de 7 días.
- Se puede usar FortiManager en vez de FortiGuard.

7.1 WebFiltering: Funcionamiento



Security Profiles > Web Filter

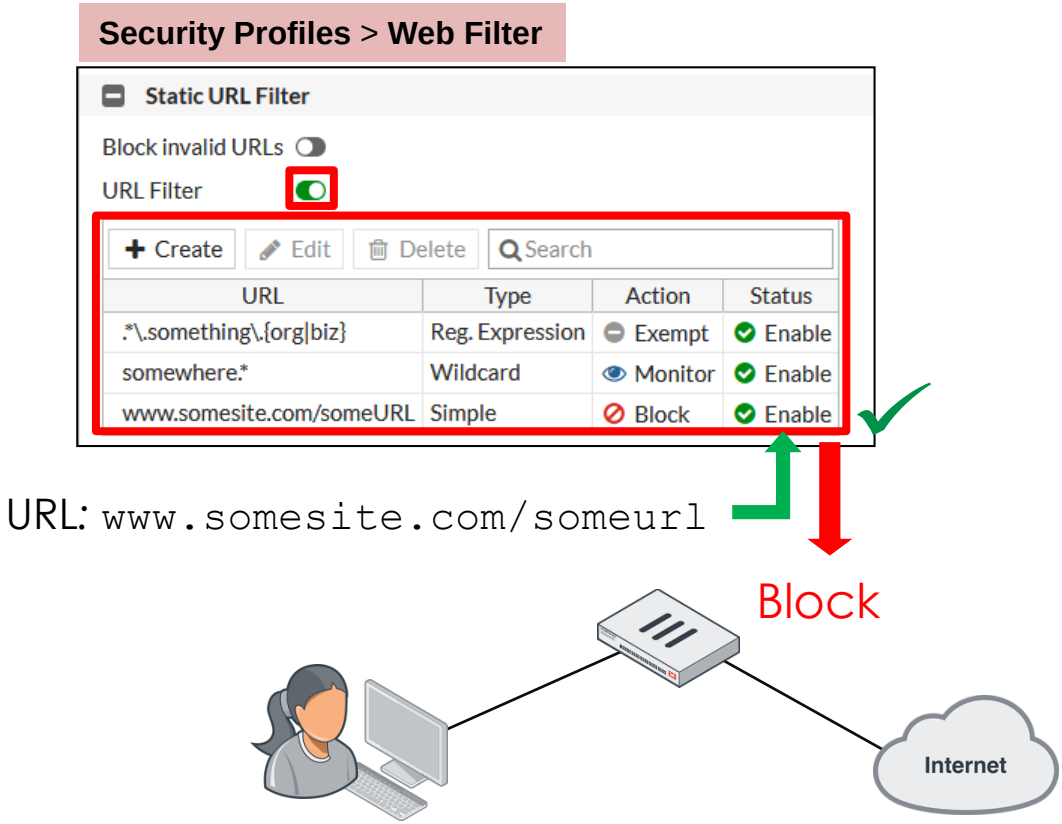


Acciones:

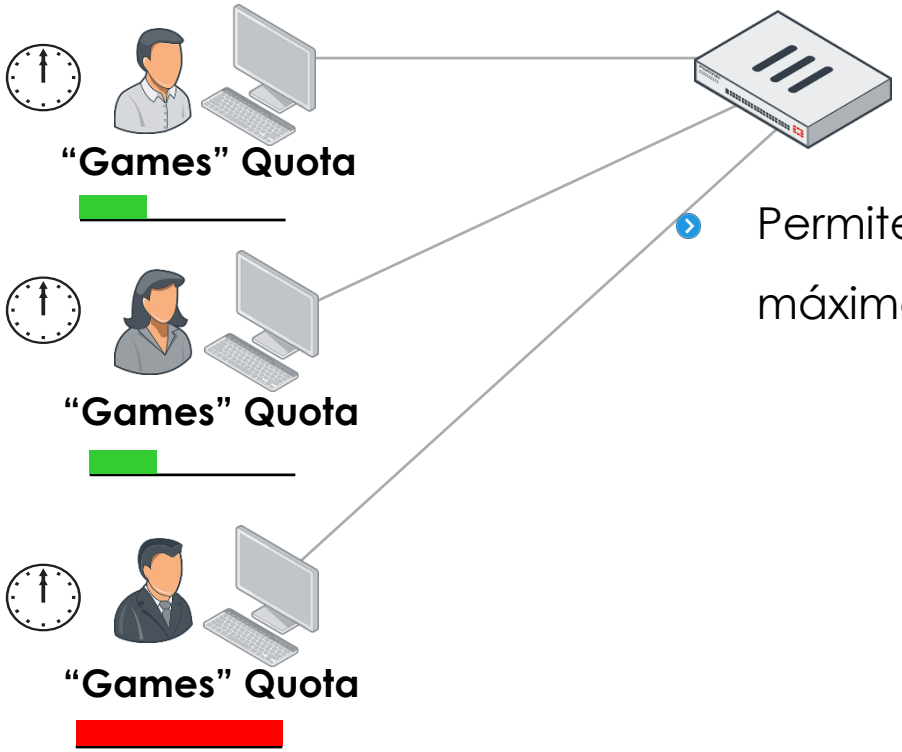
Proxy-Based
Allow
Block
Monitor
Warning
Authenticate

7.1 WebFiltering: URLS estáticas

- Se pueden configurar entradas estáticas.
  - Se chequeen en orden
- 4 Acciones posibles
  - **Allow**: El acceso se permite, el tráfico se somete al resto de operaciones (antivirus, filtrados de contenido…)
  - **Block**: Se deniega el acceso y el usuario recibe un mensaje de aviso.
  - **Monitor** : El tráfico se permite, se genera un log y se somete al resto de operaciones.
  - **Exempt**: El tráfico se permite y se le exime del resto de operaciones.



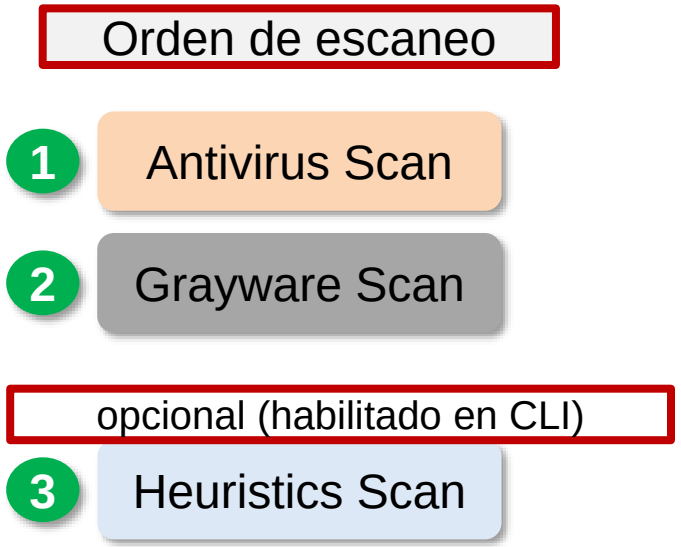
7.1 WebFiltering: Cuotas



Permite ciertas categorías, pero con un máximo de tiempo.

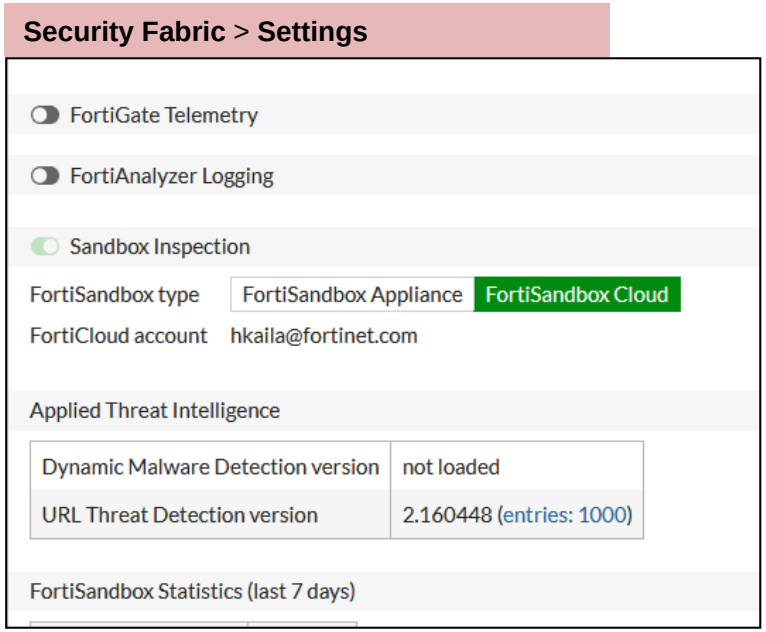
7.2 AntiVirus

- El modulo de antivirus detecta y elimina el malware en tiempo real
- Grayware scan:
  - Usa firmas de grayware
  - Detecta y bloquea programas no solicitados
- Heuristics scan:
  - Busca por Código que parezca un virus
    - (P.E.: Modifica el registro para reiniciarse)
  - Cuenta los atributos que parecen de virus
  - Si se supera un umbral, se declara sospechoso
  - Posibles falsos Positivos



7.2 AntiVirus: Sandboxing

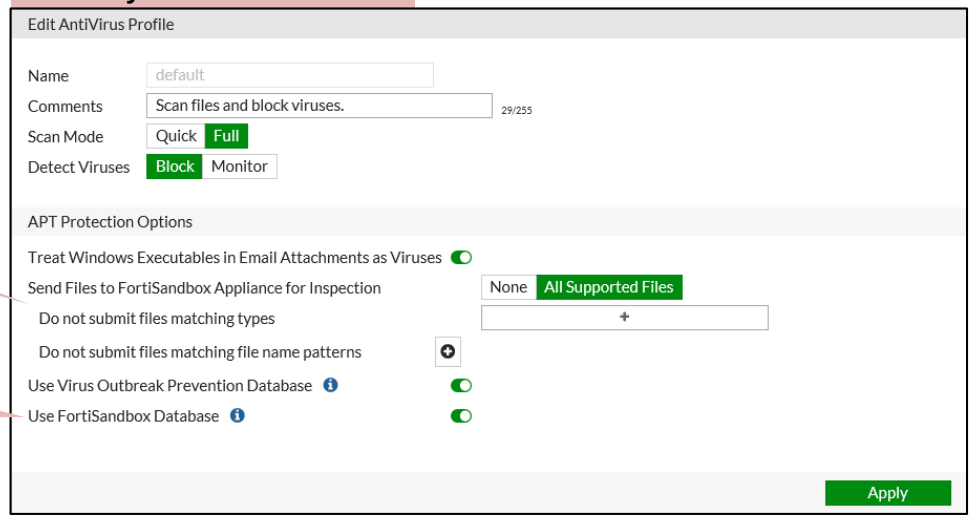
- FortiSandbox detecta ataques de día zero:
  - FortiGate sube los archivos a FortiSandbox Cloud o FortiSandbox Hardware..
  - Los archivos se ejecutan en un entorno aislado (VMs).
  - FortiSandbox examina los efectos de la ejecución.
- Se puede configurar al FortiGate para recibir una base de datos de firmas de FortiSandbox, par asuplementar la bbdd de firmas de FortiGuard.



7.2 AntiVirus: Sandboxing

- El envío de ficheros a un Sandbox se realiza a través del propio perfil de antivirus.
  - Se pueden enviar todos los ficheros o sólo los sospechosos.
  - Las características que determinan que un fichero sea sospechoso se actualizan desde FortiGuard, basándose en los eventos globales.

Security Profile > AntiVirus

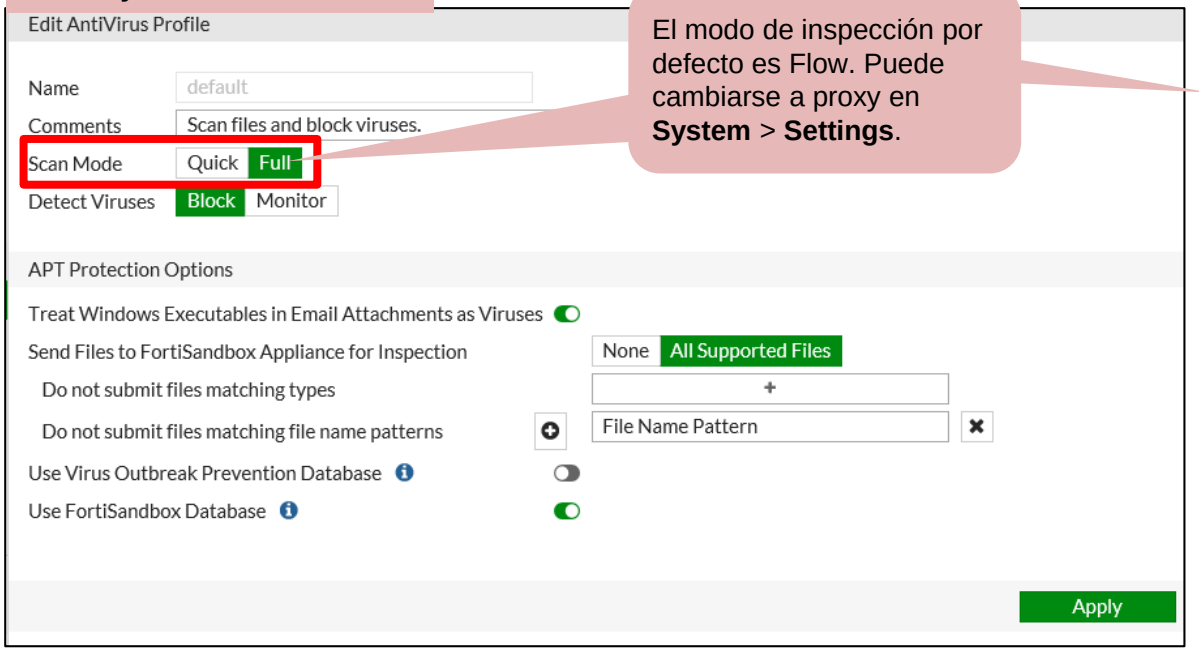


Admins controlan qué ficheros se envían al Sandbox.

Permite usar las firmas del FortiSandbox como complementeo de las firmas d eFortiGuard.

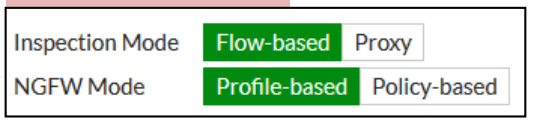
7.2 Antivirus: Configurar Perfiles

Security Profiles > **AntiVirus**



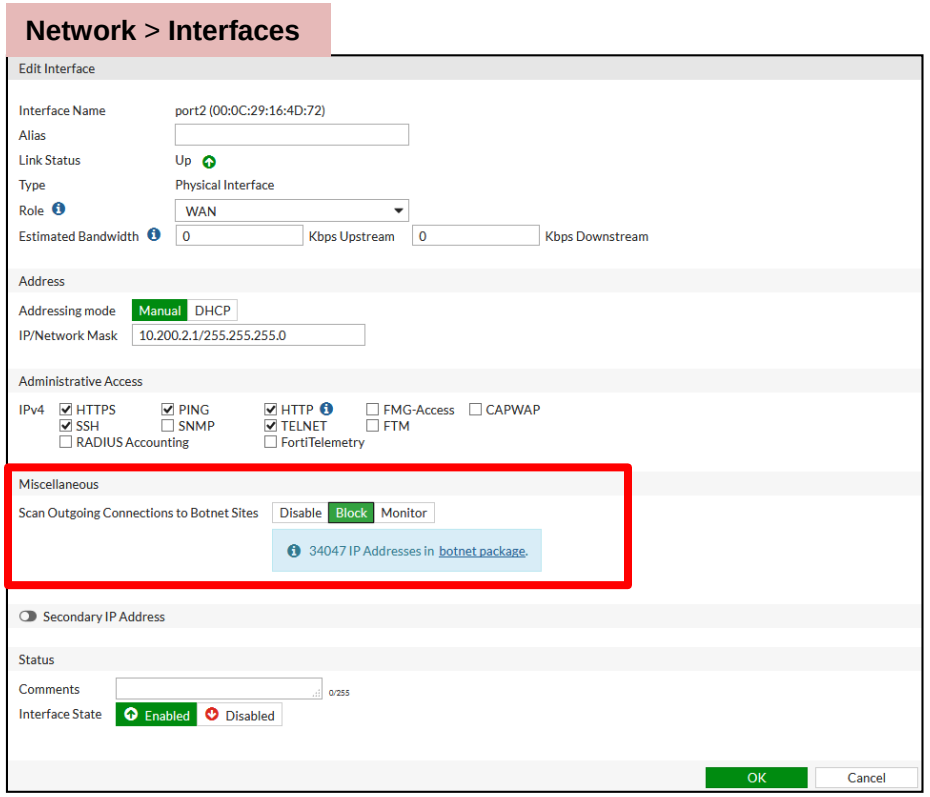
El modo de inspección por defecto es Flow. Puede cambiarse a proxy en **System** > **Settings**.

System > **Settings**



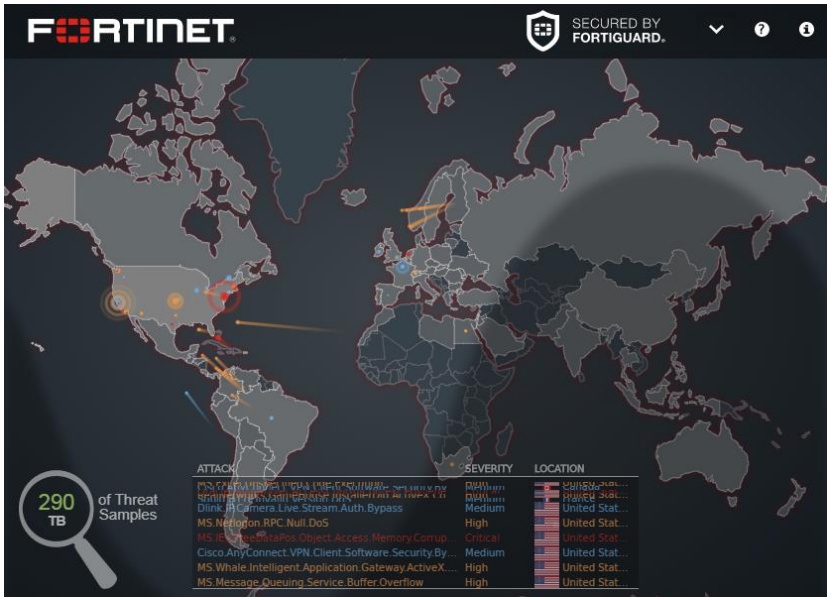
7.2 Antivirus: Control de BotNets

- Existe una BBDD de BotNets
  - Parte de la de antivirus
  - Debería de usarse junto a los perfiles de antivirus.
- BotNet se aplica solo a los interfaces externos
- Se puede configurar la acción a **Block** o **Monitor.**



7.3 IPS

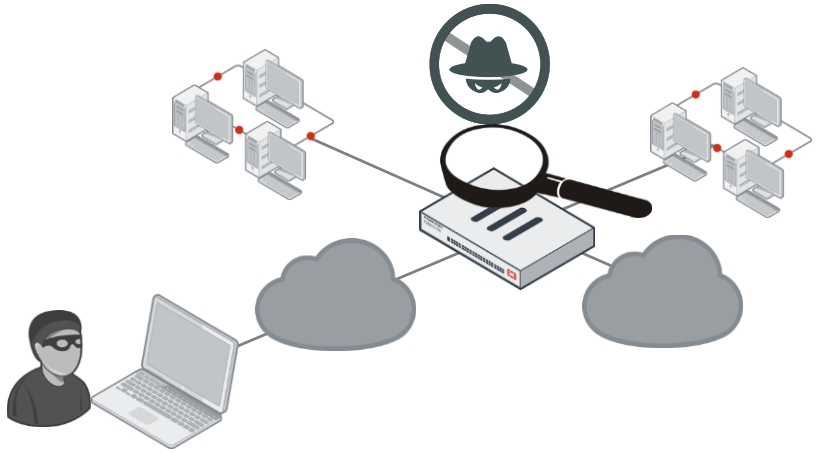
- Los ataques sobre las organizaciones son cada vez más frecuentes y sofisticados.
- Más ataques sobre aplicaciones de cliente y Cloud
  - No solo sobre servidores.
- El BYOD y los teletrabajadores aumentan el riesgo



En la página de FortiGuard se muestran los ataques en tiempo real que se producen en todo el mundo.

7.3 IPS

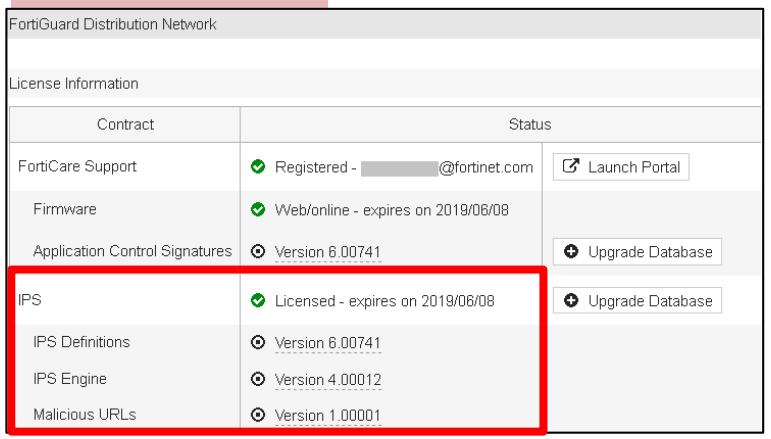
- Detección y bloqueo basado en inspección en modo Flow
  - Exploits conocidos que explotan vulnerabilidades.
  - Errores de red y anomalías del protocolo
- Componentes del IPS
  - Base de datos IPS
  - Protocol Decoders
  - Motor IPS
    - Application Control
    - Antivirus (flow)
    - Web filter (flow)
    - Email filter (flow)
    - Data Leak Prevention (DLP)



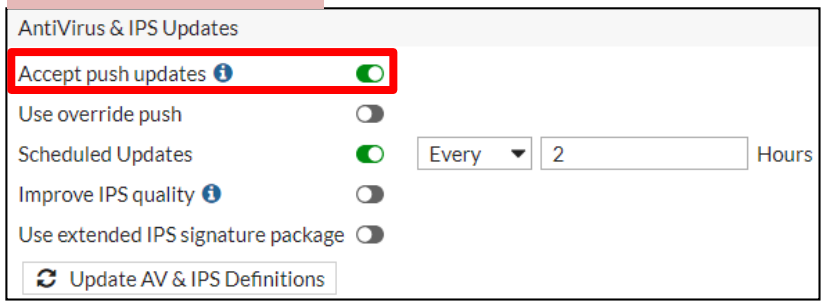
7.3 IPS: Updates FortiGuard

- El IPS se actualiza periódicamente desde FortiGuard.
  - Base de datos de firmas
  - Protocol Decoders
  - Motor IPS
- Las actualizaciones son imprescindibles para garantizar que el IPS sigue siendo efectivo.

System > FortiGuard

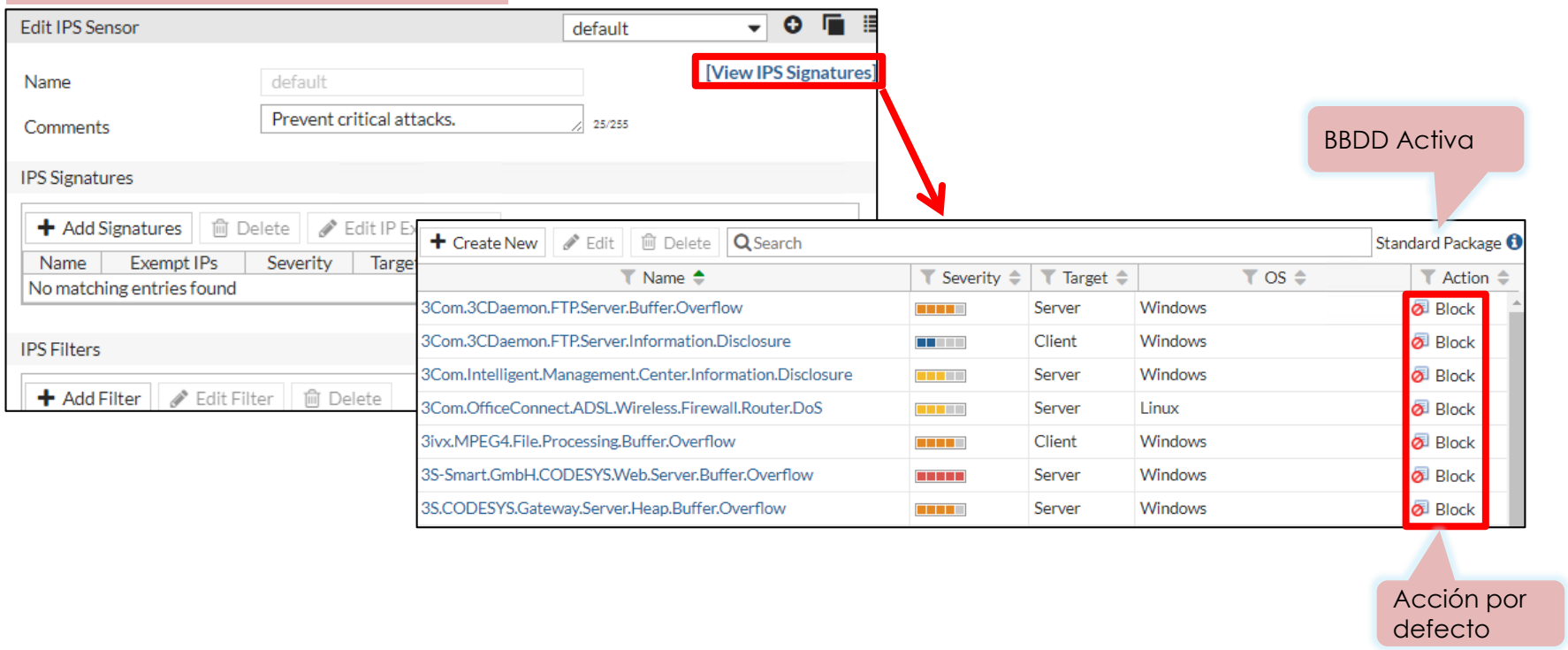


System > FortiGuard



7.3 IPS: Firmas

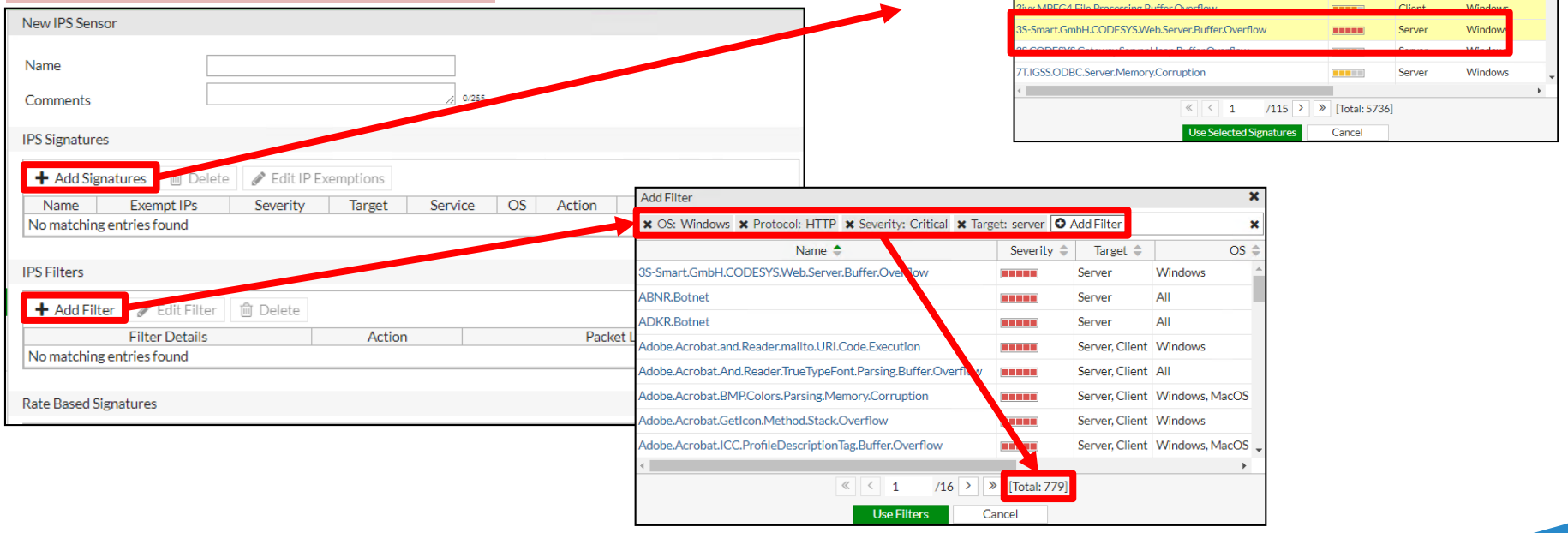
Security Profiles > **Intrusion Prevention**



7.3 IPS: Sensores

- Se pueden añadir firmas individuales.
- Se pueden usar grupos de firmas: Filtros.

Security Profiles > Intrusion Prevention



7.3 IPS: Configurar Sensores

- Adicionalmente, se pueden activar firmas basadas en umbrales, para bloquear el tráfico cuando se supera ese umbral.
  - Gestiona el tráfico basada en la IP de origen o destino.

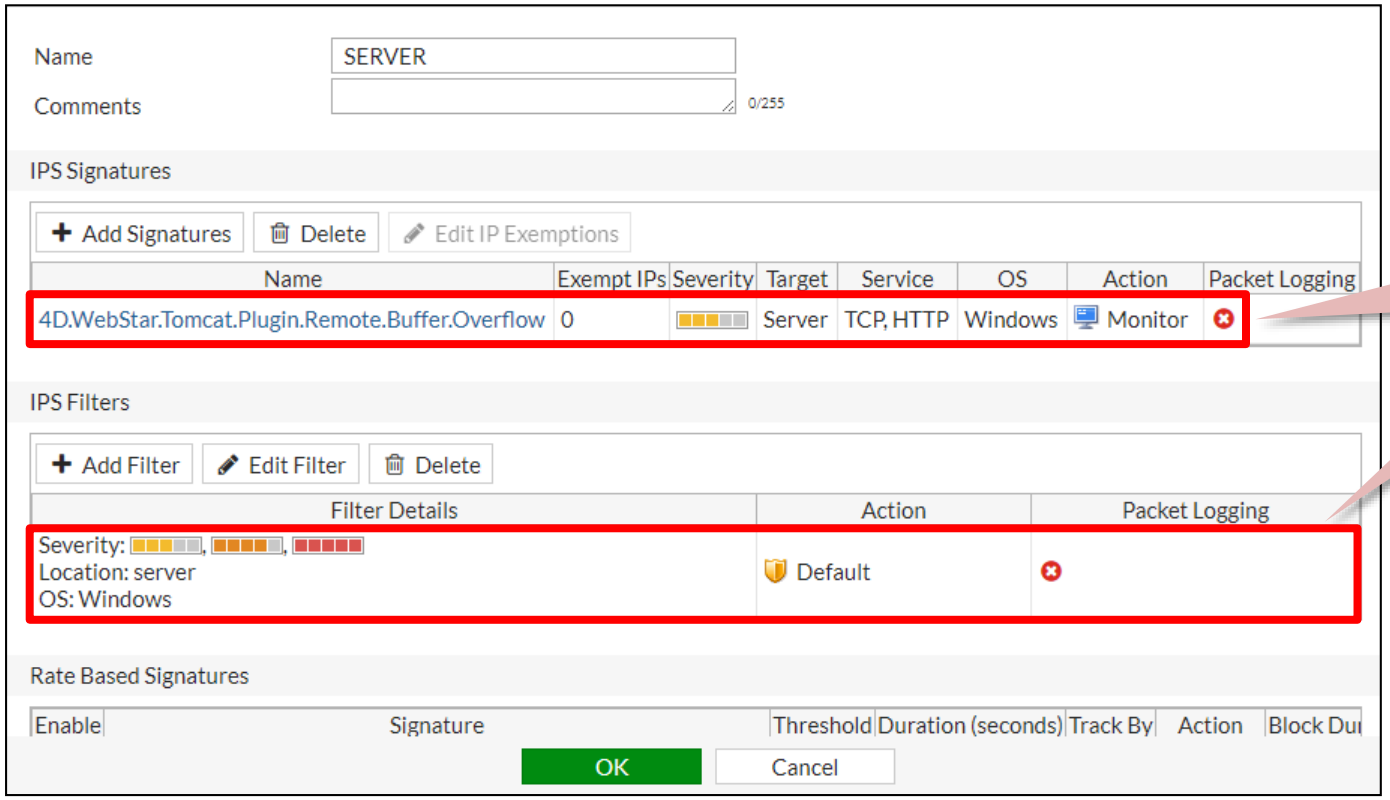
Security Profiles > **Intrusion Prevention**

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Duration (min
●	Apache.HTTPD.mod_http2.DoS	300	1	Source IP	Block	Expires 4 Hour(s)
○	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	Block	None
●	FTP.Login.Brute.Force	200	10	Source IP	Block	Expires 1 Hour(s)
○	FreeBSD.TCP.Reassembly.DoS	10	2	Any	Block	None
●	IMAP.Login.Brute.Force	60	10	Source IP	Block	Expires 1 Hour(s)
●	MS.Active.Directory.LDAP.Packet.Handling.DoS	100	1	Source IP	Block	Expires 5 Minute(
○	MS.OWA.Brute.Force	15	1	Any	Block	None
●	MS.RDP.Connection.Brute.Force	200	10	Source IP	Block	Expires 1 Day(s)

7.3 IPS: Secuencia de inspección de un sensor

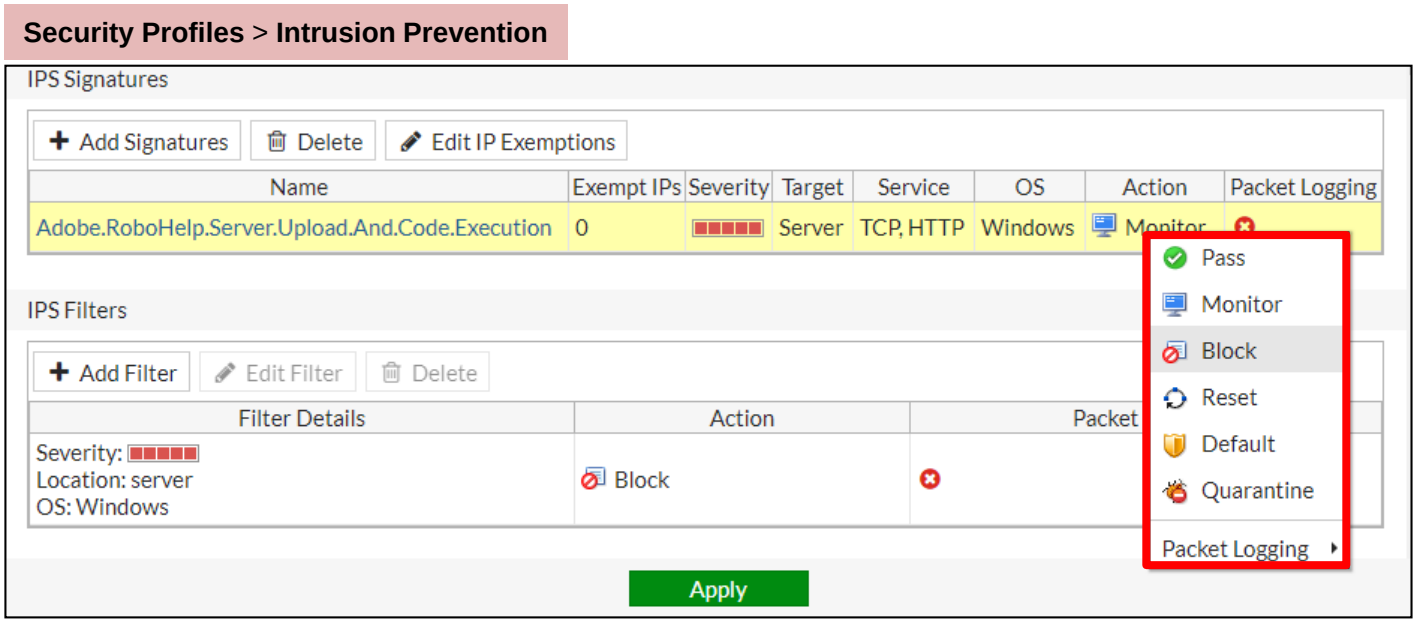
Security Profiles > **Intrusion Prevention**



Las acciones individuales preceden a los filtros

7.3 IPS: Acciones

- Acciones a tomar cuando el tráfico coincide con una firma.



7.4 APPCONTROL

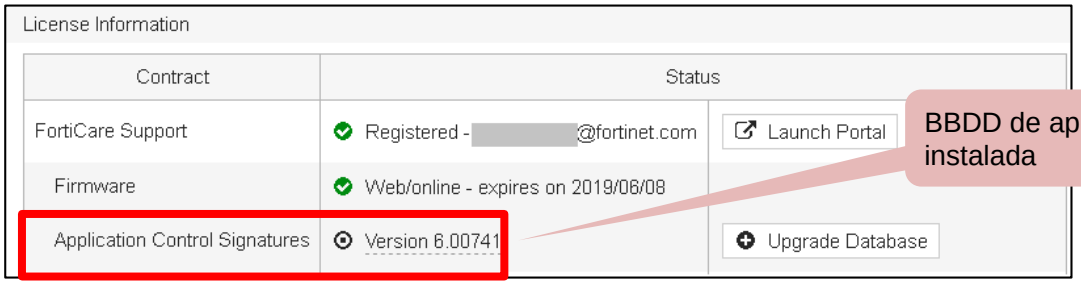
- Detecta y actúa sobre las aplicaciones en la red
  - Facebook, Skype, Gmail, LogMeIn…
  - Soporta miles de aplicaciones, y categorías, incluyendo P2P y proxy
  - Puede escanear protocolos seguros
    - Requiere perfiles de inspección SSL/SSH

- ¿Cómo funciona?
  - Usa el motor del IPS
  - Escaneo Flow-based (no proxy-based)
  - Compara el tráfico con patrones de aplicación conocidos

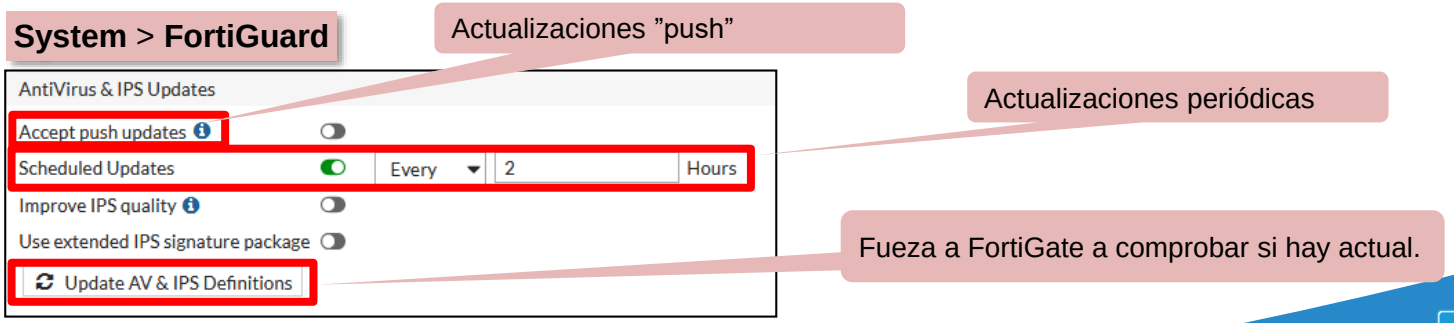
7.4 APPCONTROL: Firmas

- Aplication Control es un servicio incluido con el soporte del equipo
  - La BBDD de Aplicaciones está separada de la BBDD de IPS.

System > FortiGuard

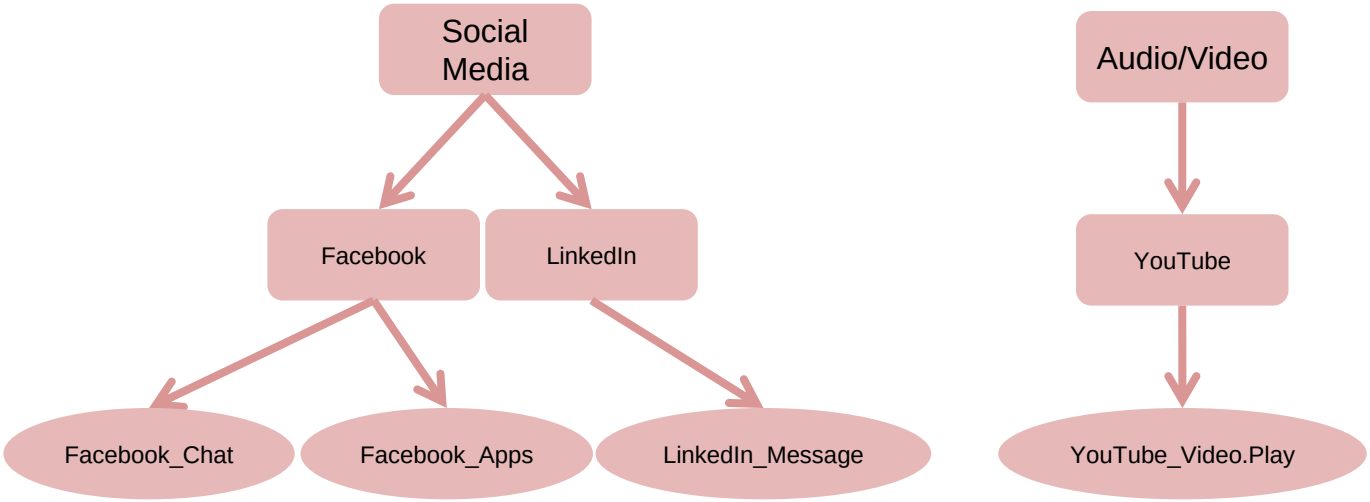


System > FortiGuard



7.4 APPCONTROL: Estructura Jerárquica

- Las firmas de aplicaciones se organizan de manera jerárquica.



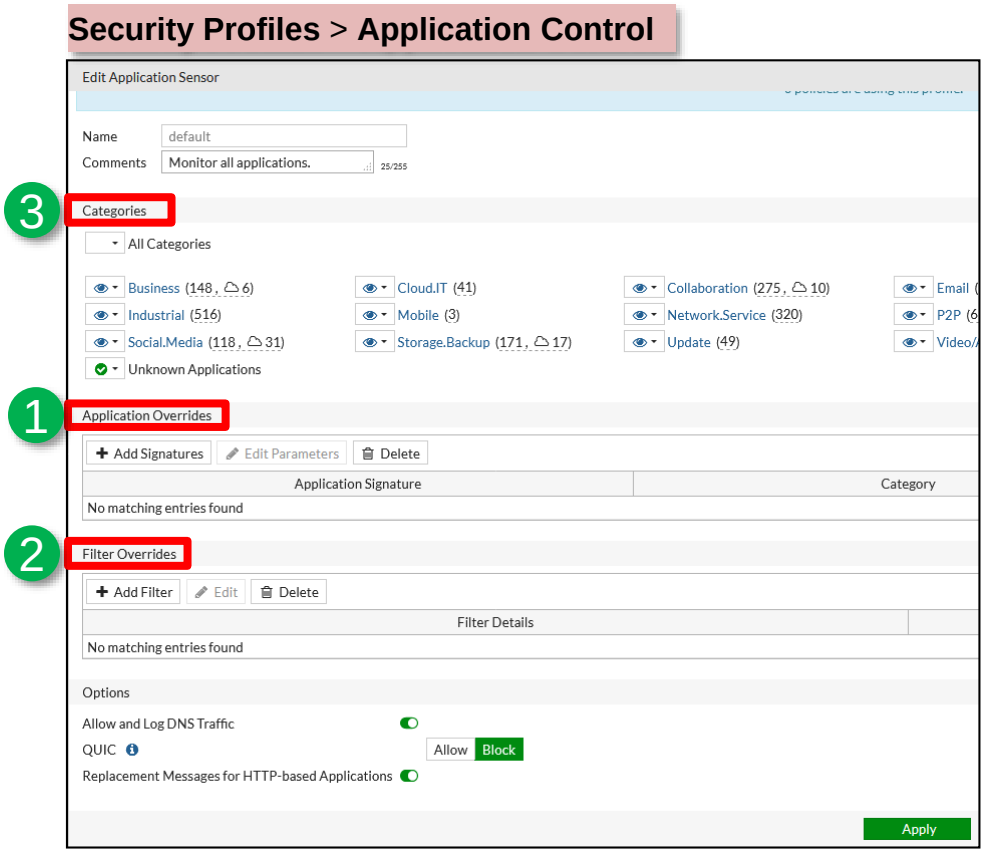
7.4 APPCONTROL: Configuración de perfiles

- Se pueden configurar diferentes perfiles, basados en categorías, aplicaciones concretas y filtros.

Security Profiles > Application Control

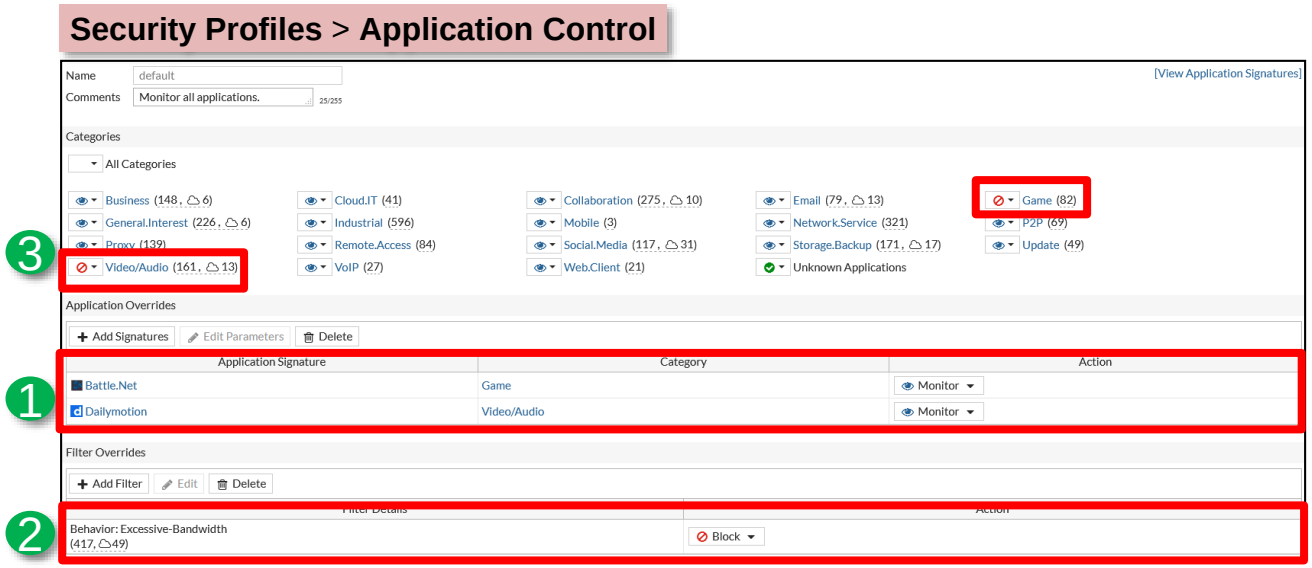
7.4 APPCONTROL: Orden de escaneo

- El motor IPS identifica la aplicación.
- La prioridad es la siguiente:
  1. Application overrides
  2. Filter overrides
  3. Categories



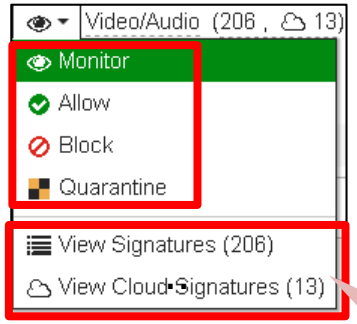
7.4 APPCONTROL: Orden de escaneo

1. **Application Overrides**: Battle.Net y Dailymotion se configuran como **Monitor.**
2. **Filter Overrides**: "Excessive bandwidth · se configuran como **Block.**
   - Contiene aplicaciones de diferentes categorías: – BitTorrent (P2P), Adobe.Update (Update),FaceTime (VOIP), Flickr (Social.Media)
3. **Categories**: **Game** y **Video/Audio** se configuran como **Block** y las demás como **Monitor**.



7.4 APPCONTROL: Acciones

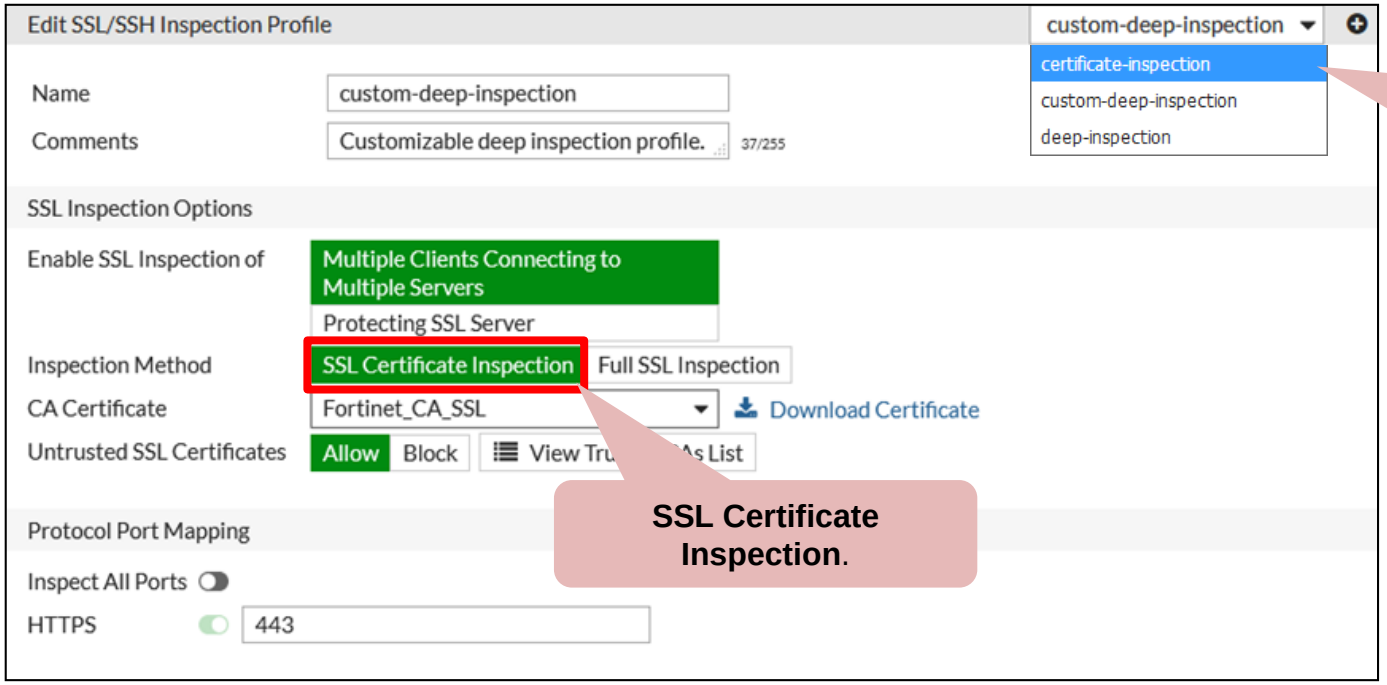
- Allow
  - No se guarda log
- Monitor
  - Permite y guarda log
- Block
  - Deniega el acceso y guarda log
- Quarantine
  - Bloquea y guarda log de la IP de origen de ese tráfico durante un tiempo determinado.



Muestra la lista de aplicaciones asociadas a esa categoría

7.5 INSPECCION SSL

Security Profiles > SSL/SSH Inspection

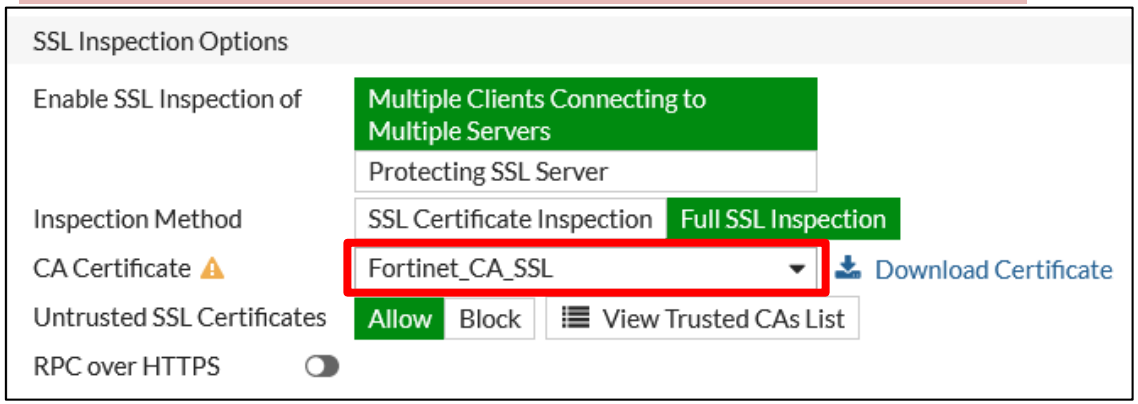


Nombre de perfil: custom-deep-inspection.

SSL Certificate Inspection.

7.5 INSPECCION SSL

Security Profiles > SSL/SSH Inspection



Índice

8.1 Activación y análisis de logs

- Para poder analizar los eventos de seguridad es necesario activar los logs en las políticas
  - All logs: Se guarda información de cada sesión procesada por esa regla.
  - Security Events: Se guarda la información de aquellas sesiones que tienen asociadas un evento de seguridad asociado con un Perfil UTM (antivirus, aplicación…)
- Los logs se pueden almacenar en diferentes lugares
  - Memoria del FGATE
  - Disco Duro del FGATE (dispositivos con disco)
  - FortiAnalyzer
  - FortiCloud.

8.1 Activación y análisis de logs

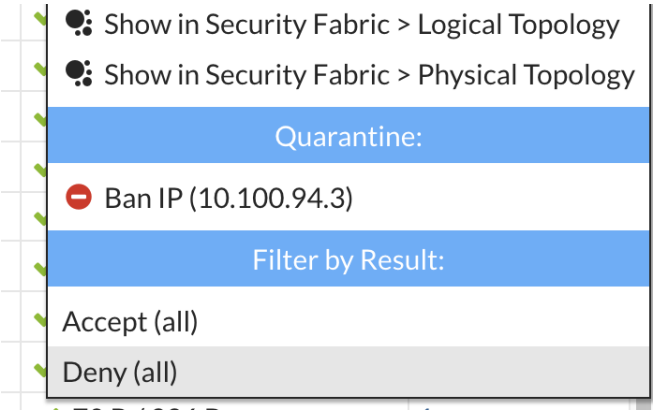
- Log & Report -> Forward Traffic
- Se pueden obtener todos los logs de tráfico, la acción asociada (permitir/denegar) y los eventos de seguridad asociados, si los hay.

Source	Destination	Application Name	Security Events	Result
00:09:0f:00:03:02	185.60.216.35 (facebook.com)	Facebook	WEB 1 APP 2	779 B / 3.63 kB
00:09:0f:00:03:01	208.91.113.80 (mail.fortinet.com)	IMAP		240 B / 60 B
00:09:0f:00:03:01	77.238.185.51 (imap.mail.yahoo.com)	Yahoo.Mail		1.32 kB / 6.47 kB
00:09:0f:00:03:01	155.133.82.221	HTTP.BROWSER	APP 1	UTM Allowed
00:09:0f:00:03:02	184.154.206.12 (16fmusic.com)	HTTP.BROWSER	WEB 1 APP 1	76 B / 427 B

- Diferentes acciones para poder investigar en detalle los eventos de seguridad
  - Ir a la política asociada, ver detalle de los eventos, ver detalle de la sesión.

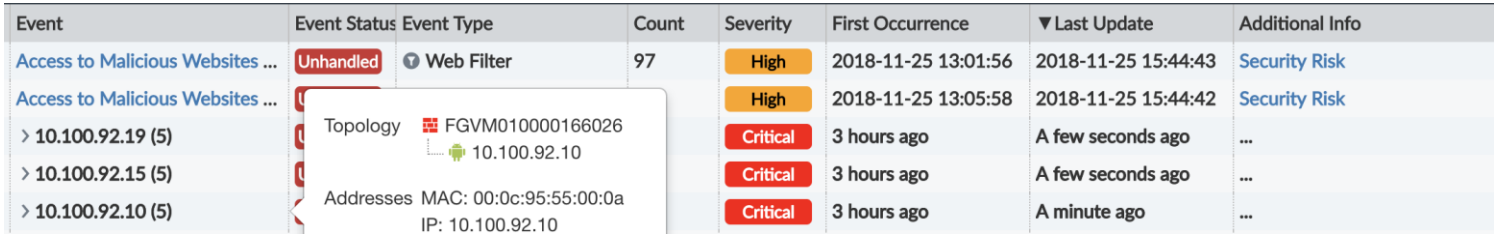
8.1 Activación y análisis de logs

- Es posible filtrar por cualquiera de los campos e incluso aislar al equipo de origen (por IP)



8.1 Activación y análisis de logs

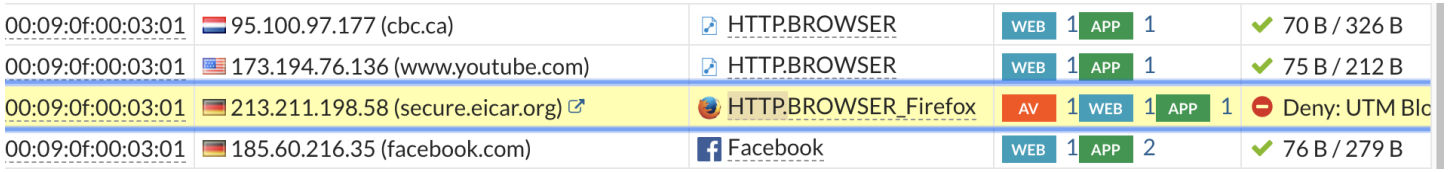
- FortiAnalyzer es capaz de generar alarmas de seguridad en función de la criticidad y tipo de eventos recibidos



- Incluso se pueden configurar acciones automatizadas ante la recepción de un determinado tipo de eventos (p.e. antivirus) en un lapso de tiempo configurable.
- Esta configuración permite notificar a los administradores de desviaciones de la línea base, que pueden denotar algún problema de seguridad.

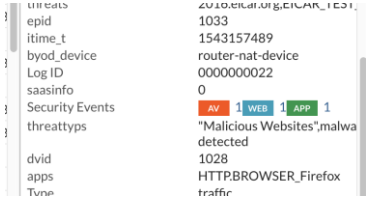
8.2 Ejemplo de evento de seguridad

- Desde un EndPoint, accedemos a eicar.org
- Descargamos el fichero eicar sobre una conexión no cifrada:
  - Se recibe un mensaje de reemplazo
  - El evento aparece en el log de tráfico y en el de eventos de seguridad.



00:09:0f:00:03:01	95.100.97.177 (cbc.ca)	HTTP.BROWSER	WEB 1 APP 1	70 B / 326 B
00:09:0f:00:03:01	173.194.76.136 (www.youtube.com)	HTTP.BROWSER	WEB 1 APP 1	75 B / 212 B
00:09:0f:00:03:01	213.211.198.58 (secure.eicar.org)	HTTP.BROWSER_Firefox	AV 1 WEB 1 APP 1	Deny: UTM Blc
00:09:0f:00:03:01	185.60.216.35 (facebook.com)	Facebook	WEB 1 APP 2	76 B / 279 B

  - En rojo el evento que ha causado la denegación del tráfico (AV). Se puede ver el detalle



epid	1033
itime_t	1543157489
byod_device	router-nat-device
Log ID	0000000022
saasinfo	0
Security Events	AV 1 WEB 1 APP 1
threattyps	"Malicious Websites",malwa detected
dvid	1028
apps	HTTP.BROWSER_Firefox

8.2 Ejemplo de evento de seguridad

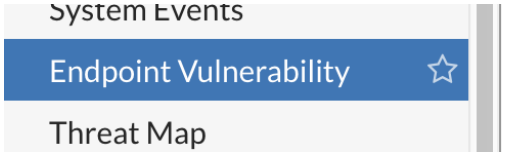
- Desde un EndPoint, accedemos a eicar.org
- Descargamos el fichero eicar sobre una conexión **cifrada**:
  - No se recibe un mensaje de reemplazo
  - Quien deniega el acceso es el antivirus de puesto (en este caso el FortiClient)

8.2 Ejemplo de evento de seguridad

- Cambiamos el perfil de SSL Inspection asociado a la política del EndPoint → Usamos Deep Inspection
- Accediendo a la descarga del fichero sobre https
  - Primero una notificación de página insegura: No hemos importado la CA
  - Luego se obtiene el mensaje de reemplazo -> Ahora el análisis se hace en FortiGate antes de en el Endpoint.

8.3 Análisis de Vulnerabilidades

- Cuando los EndPoints usan FortiClient, se integran con el FortiGate (y/o el gestor de endpoints), mediante una conexión de telemetría FortiClient – FortiGate.
- Desde FortiGate/FortiAnalyzer se pueden analizar las vulnerabilidades de cada cliente
- Se puede usar la funcionalidad de Drill Down para obtener información detallada.



8.4 Hosts Comprometidos

- Se puede obtener un listado de hosts comprometidos
- FortiGate analiza los datos de acceso de los equipos, incluido los accesos pasados, para determinar que un equipo está comprometido.
- FortiView -> Compromised Host

- Se puede ir al detalle mediante Drill Down.

Blacklist | Suspicious

Detected Pattern	Threat Type	Threat Name
00uq.com	PUP	SpywareCnC
00uq.com	PUP	SpywareCnC

8.5 Otra Información

- Se puede obtener en tiempo real diferente información
  - Monitor -> Firewall User : Usuarios de la red

Jackie Lawrence		3 hour(s), 8 minute(s) and 10 second(s)	10.100.91.2
Danny Rose		3 hour(s), 8 minute(s) and 8 second(s)	10.100.91.3
Jody Dawson		3 hour(s), 8 minute(s) and 5 second(s)	10.100.91.4
Gail Harper		3 hour(s), 8 minute(s) and 3 second(s)	10.100.91.5

  - Monitor -> FortiClient Monitor: FortiClients detectados

port2 (Sales Department) (FortiClient not enforced) (10)		
Alex Fox Alex-Laptop	10.100.94.5	Registered - Online
Aubrey Henry Aubrey-Desktop	10.100.94.7	Registered - Online
Avery Cooper Avery-Laptop	10.100.94.8	Registered - Online
Carmen Matthews Carmen-Laptop	10.100.94.3	Registered - Online

  - Monitor -> DHCP Server: Leases DHCP

Interface	Device	MAC	IP	Host Information	Expires	Status
Sales Department (port2)	harry-pc	02:09:0f:00:08:02	10.100.94.100	Hostname: harry-pc	2018/12/02 12:57:49	Leased out