



centro criptológico nacional



VANESA

Configuración de seguridad en cortafuegos. Ejemplo en entorno Fortinet

Índice

- 1 Introducción al Firewall
- 2 Instalación Básica
- 3 Configuración de red
- 4 Gestión de políticas
- 5 Gestión de IP's Virtuales (VIPs)
- 6 SD-WAN
- 7 Security Profiles
- 8 Análisis de seguridad

Índice

1 INTRODUCCIÓN AL FIREWALL

1.1 STATEFUL VS STATELESS

1.2 EL FIREWALL UTM FORTIGATE

1.3 INSPECCIÓN SSL

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.

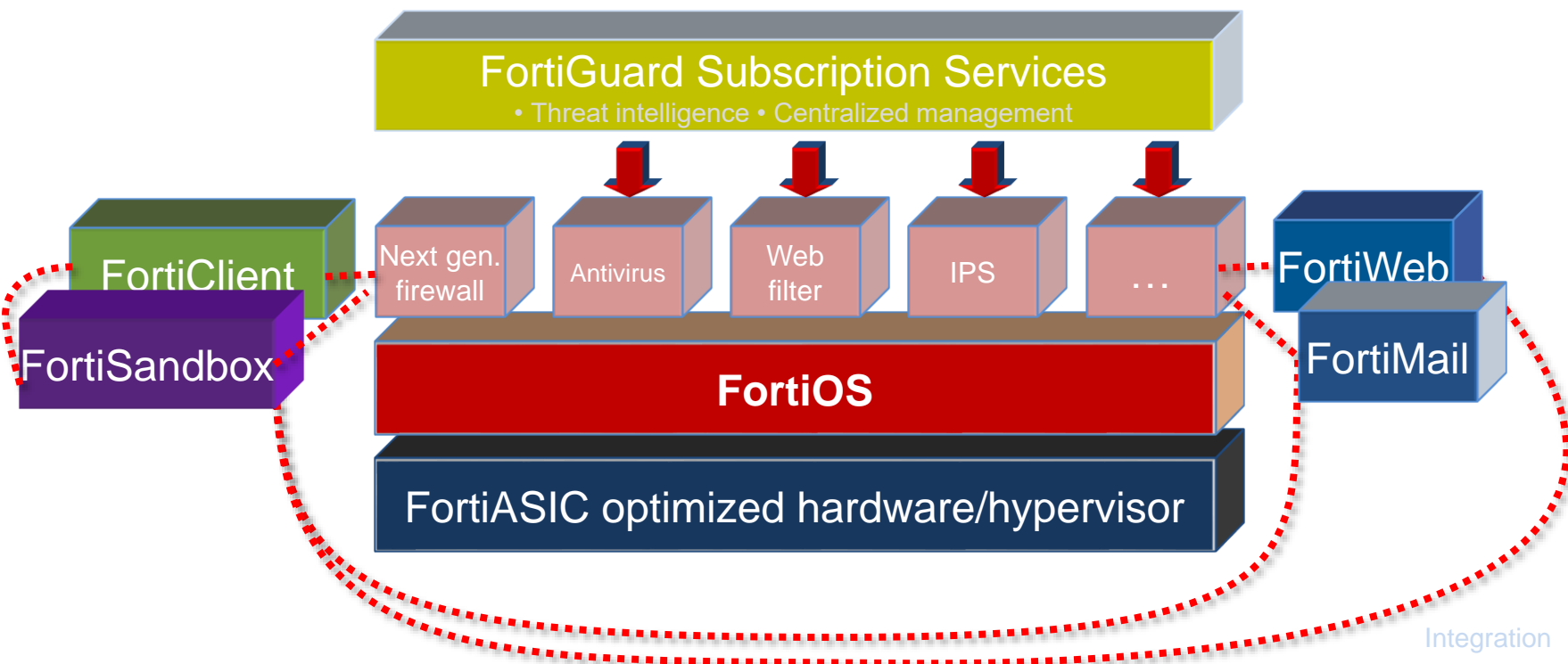
1.2- El firewall UTM FortiGate

- 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 quintupla 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



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

Fuente:
NSS Labs

- Malware Encriptado



De los ataques usarán
tráfico encriptado en 2019*

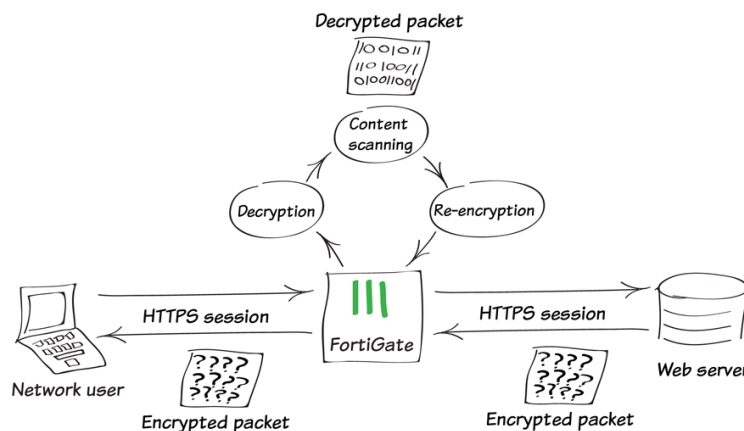
Fuente:
Gartner

1.3 Inspección SSL: Tipos de inspección

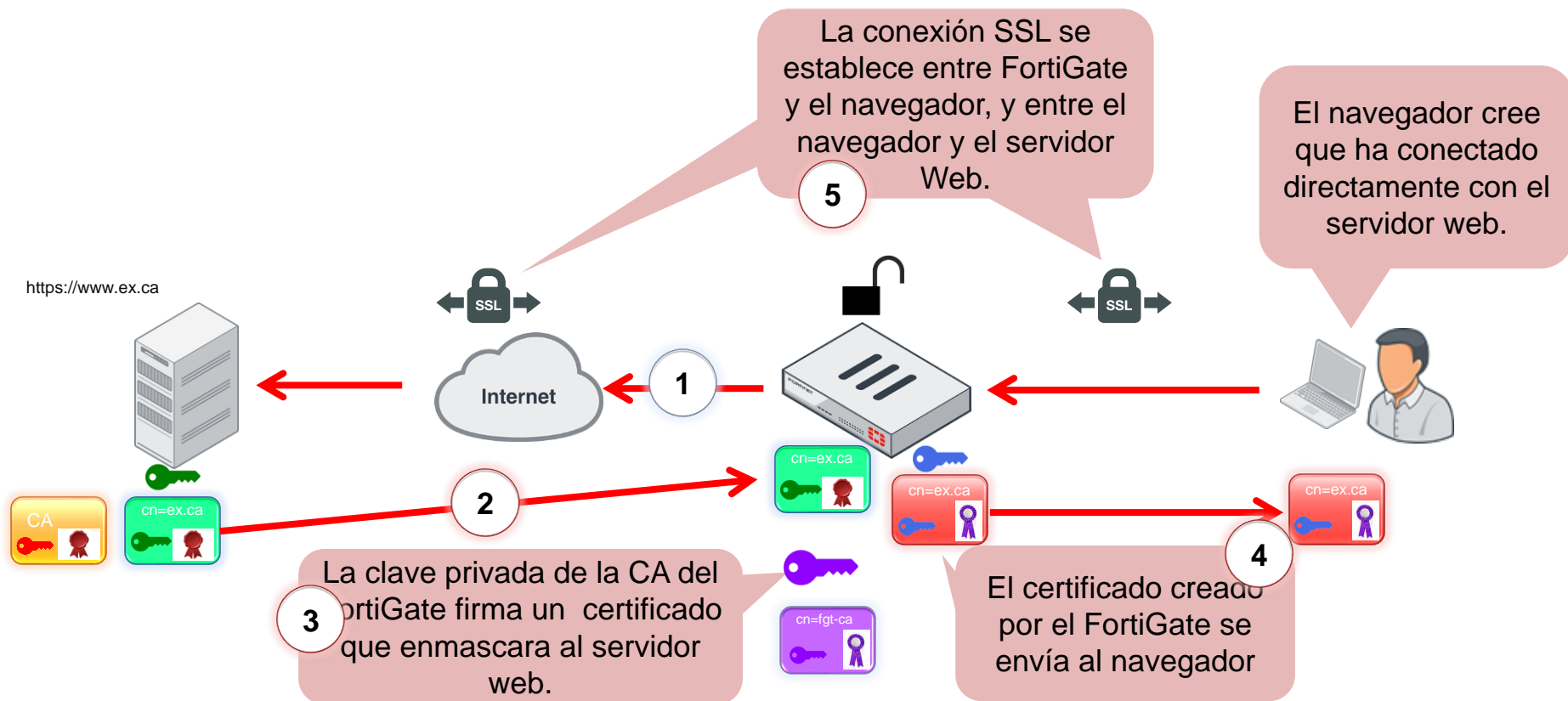
Inspección SSL Profunda

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



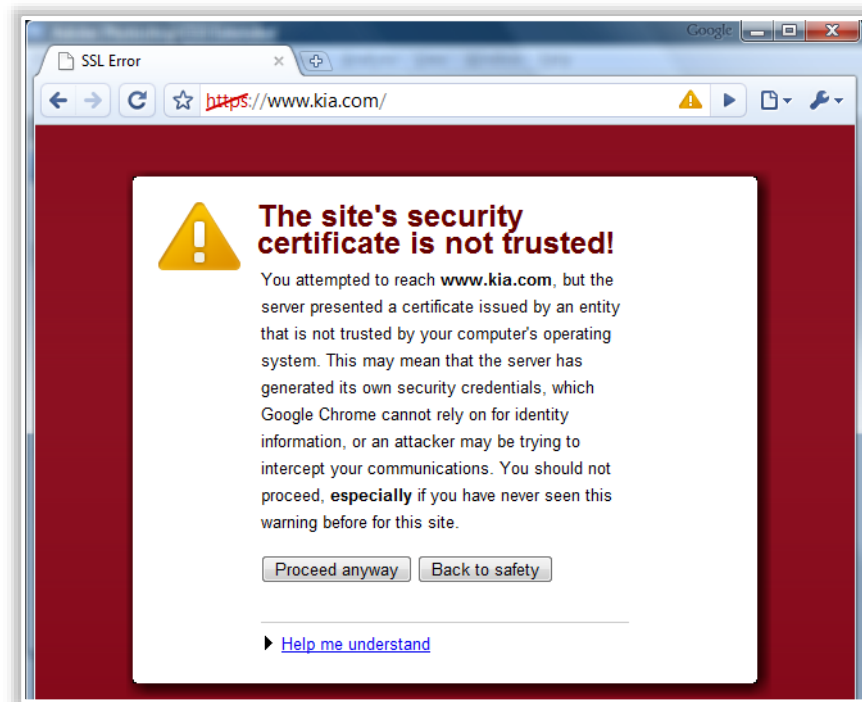
1.3 Inspección SSL: Tipos de inspección

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 INSTALACIÓN BÁSICA

2.1 PRIMERA CONFIGURACION Y REGISTRO EN SOPORTE

2.2 ACTUALIZACIÓN FIRMWARE

2.3 GESTIÓN BACKUPS

2.4 DASHBOARDS

2.5 SYSTEM SETTINGS

2.6 VISIBILIDAD DE FUNCIONES

2.7 FORTIVIEW

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

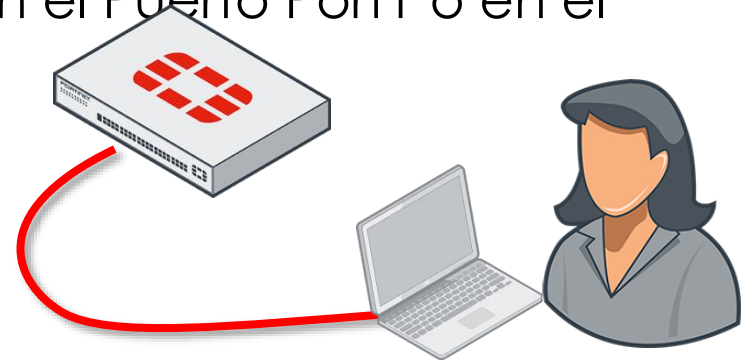
- Port1 o interface “internal” usa la IP: 192.168.1.99/24
- Está habilitado el PING, HTTP, HTTPS, y SSH
 - **La guía STIC insta a deshabilitar protocolos no seguros (HTTP y telnet)**
- Hay un servidor DHCP habilitado en el Puerto Port1 o en el interface Internal.

- Usuario por defecto:

Usuario: admin

Password: (vacío)

- También se puede acceder 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



La conexión no es privada

Es posible que los atacantes estén intentando robar tu información (por ejemplo, contraseñas, mensajes o tarjetas de crédito). [Más i](#)

admin

Password

Login



This account is using the default password, it is strongly recommended that you change your password.

Change Password

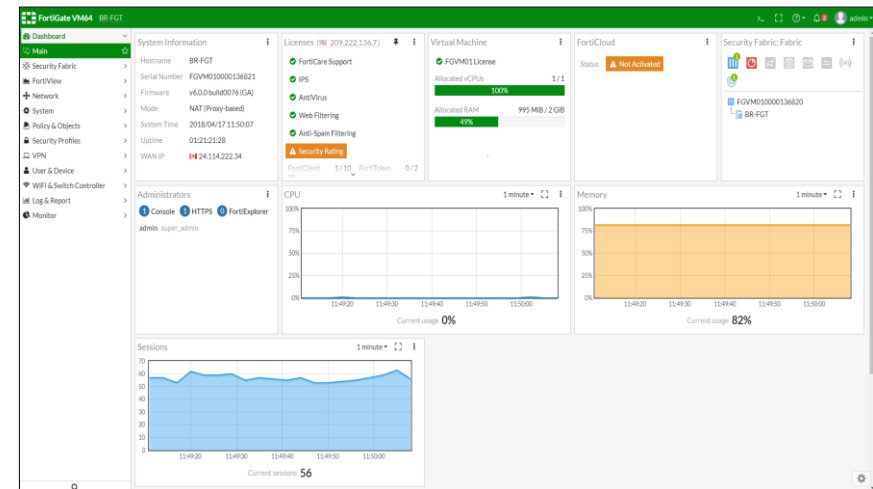
Later

2.1 Primera configuración: Administración

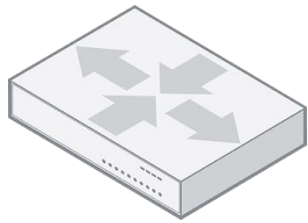


CLI
Console, SSH, Telnet, GUI Widget

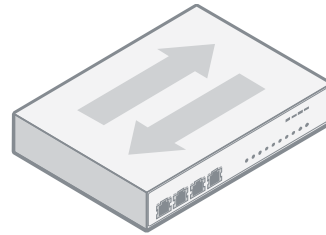
GUI
FortiExplorer, Web Browser (HTTP, HTTPS)



2.1 Primera configuración: Modo de operación



NAT

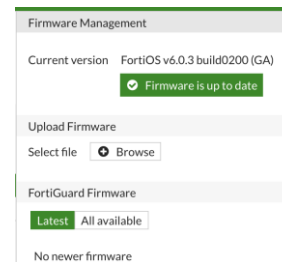
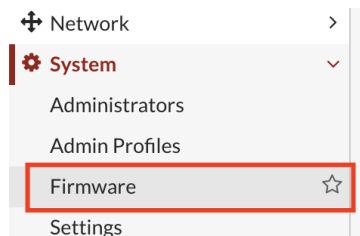


Transparente

- FortiGate es un **router**
- Los Interfaces tienen direcciones IP
- Los paquetes se encaminan por IP
- FortiGate es un **switch**
- Los interfaces no tienen IP
- No puede encaminar paquetes, solo bloquear o transmitir

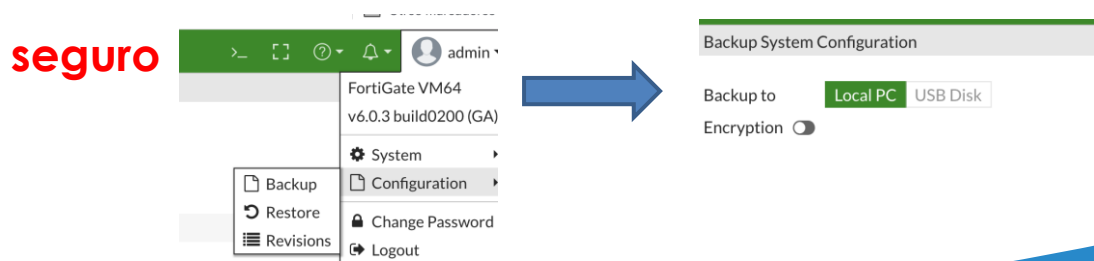
2.2 Actualización de software

- 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

Security Fabric: forticasa

Internet_GW

- FAP-PBAJA
- S108EF5918000802
- FG-ISF
- FAP-Planta arriba

Security Rating

11
Percentile

SMB (1 - 256 endpoints)
Spain - Technology

Botnet Activity

Known IPs	33841
Known Domains	51147
Activity Since	2018/11/14 19:06:23
Blocked IPs	0
Blocked Domains	0
Blocked Connections	0

Licenses (96.45.33.85)

- FortiCare Support
- Firmware & General Updates
- IPS

FortiClient	2 / 10	FortiToken	1 / 2
	20%		50%

System Information

Hostname	Internet_GW
Serial Number	FWF60E4Q16005006
Firmware	v6.2.0 build0777 (interim)
Mode	NAT (Flow-based)
System Time	2018/11/20 13:06:39
Uptime	05:18:00:16
WAN IP	47.62.8.141

FortiCloud (Europe)

Status	Activated
Log Retention	Free License
Storage Used	1.87 GiB
FortiSandbox Cloud	Disabled

CPU 1 minute

Current usage **2%**

Log Rate 1 minute

FortiAnalyzer **0/s** FortiCloud **0/s**

Memory 1 minute

Current usage **54%**

Sessions IPv4 + IPv6 1 minute

Current sessions **304**

SPU **4.6%**
nTurbo **0.0%**

Bandwidth wan1 1 hour

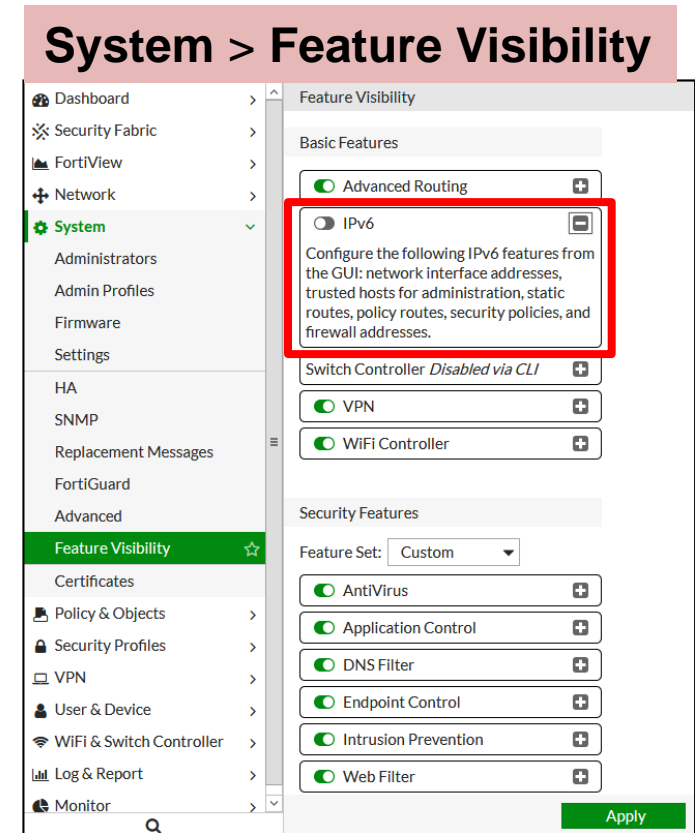
Bandwidth internal 1 hour

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**”, Selecciona 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

Name prof_admin
Comments 0/255

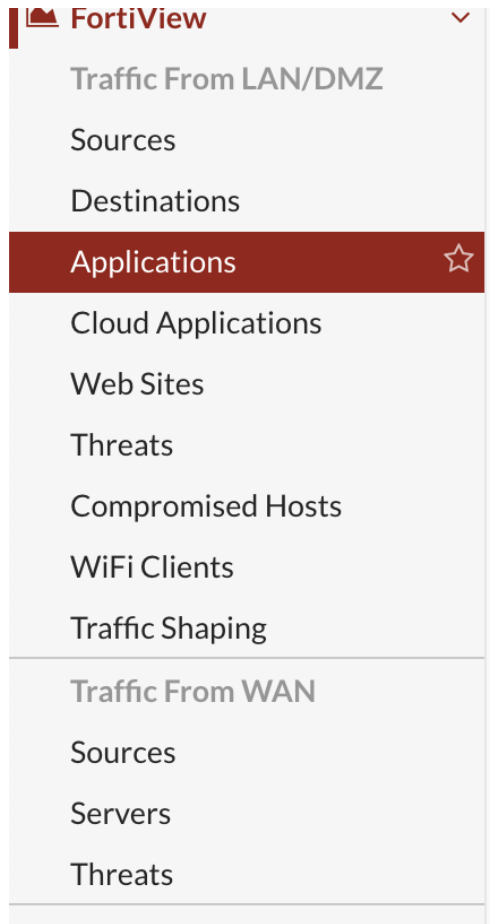
Access Permissions

Access Control	Permissions	Set All
Security Fabric	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
FortiView	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
User & Device	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
Firewall	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom	
Log & Report	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom	
Network	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom	
System	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom	
Security Profile	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write <input type="radio"/> Custom	
VPN	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	
WiFi & Switch	<input type="radio"/> None <input type="radio"/> Read <input checked="" type="radio"/> Read/Write	

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 "ATENCIÓN: Acceso restringido a personal autorizado.`
`Este equipo, incluidos los dispositivos relacionados con el mismo, es propiedad privada.`
`Toda actividad esta siendo monitorizada"`

Índice

3 CONFIGURACIÓN DE RED

3.1 INTERFACES: SOFTWARE SWITCH

3.2 INTERFACES: AGREGADO

3.3 INTERFACES: VLAN

3.4 ZONAS

3.5 DNS

3.6 DHCP

3.7 ROUTING ESTÁTICO

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**

Network > Interfaces

Edit Interface

Interface Name: port8 (00:0C:29:6F:1F:E6)

Alias: []

Link Status: Down

Type: Physical Interface

Role: Undefined

Address

Addressing mode: Manual DHCP One-Arm Sniffer Dedicated to FortiSwitch

IP/Network Mask: 0.0.0.0/0.0.0.0

One-Arm Sniffer está disponible solo cuando el interface no está referenciado en otra parte

Edit Interface

Interface Name: port3 (00:0C:29:6F:1F:B4)

Alias: []

Link Status: Up

Type: Physical Interface

Role: Undefined

Address

Addressing mode: Manual DHCP Dedicated to FortiSwitch

Retrieve default gateway from server: []

Distance: 5

Override internal DNS: []

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

FortiGate VM64 Local-FortiGate

Dashboard
FortiView
Network
Interfaces
DNS
DNS Servers
Packet Capture
WAN LLB
WAN Status Check
WAN LLB Rules
Static Routes
Policy Routes
RIP
OSPF

New Interface

Interface Name: SS1

Type: **Software Switch**

Physical Interface Members: +

Role: LAN

Address

Addressing mode: **Manual** DHCP Dedicated to FortiSwitch

IP/Network Mask: 0.0.0.0/0.0.0.0

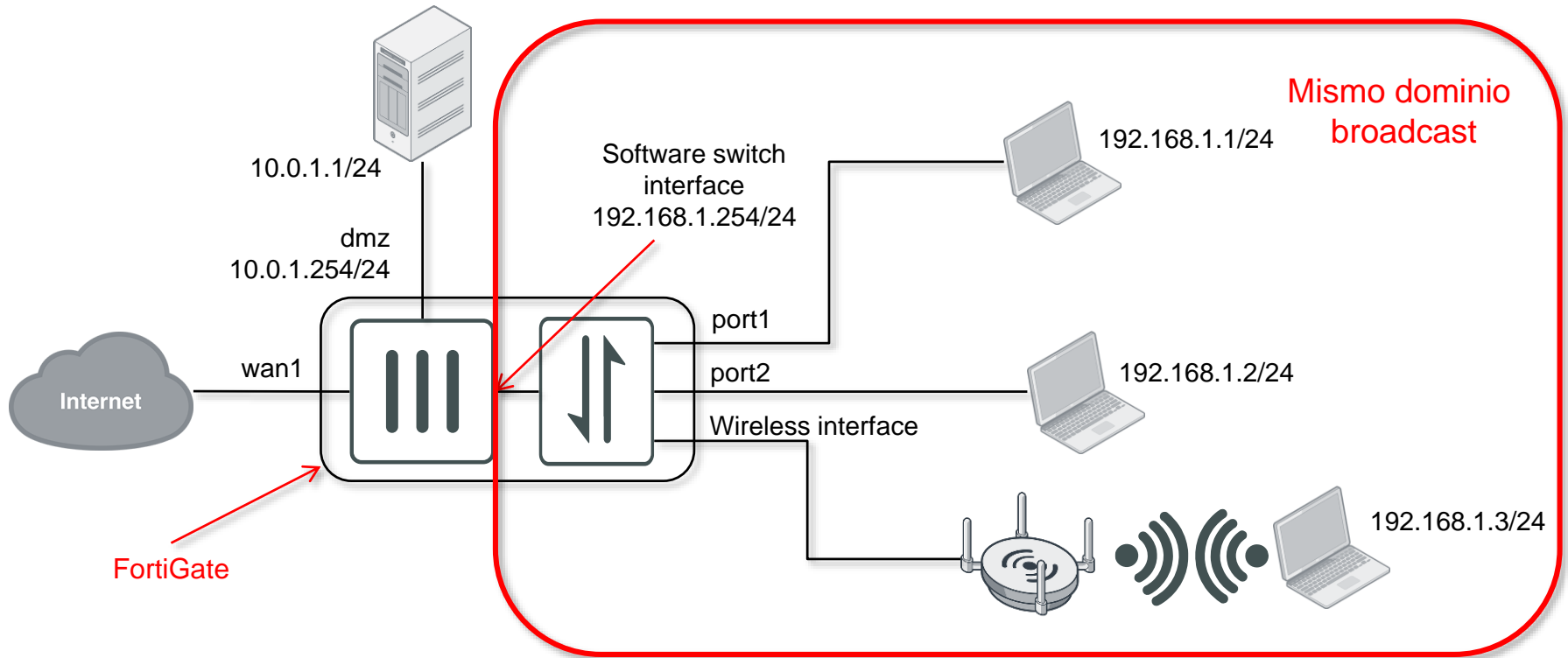
Restrict Access

Administrative Access: HTTPS PING FMG-Access CAPWAP SSH
 SNMP RADIUS Accounting FortiTelemetry

DHCP Server

Usar este nombre en la definición de políticas

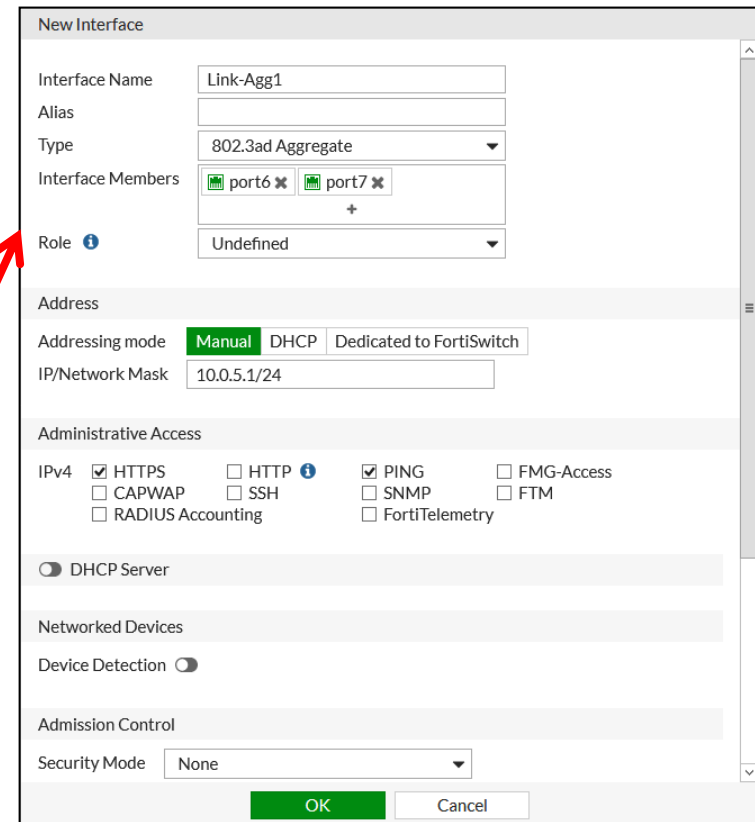
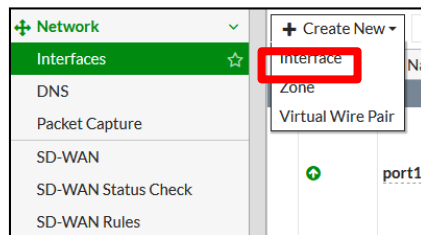
3.1 SoftSwitch: Ejemplo



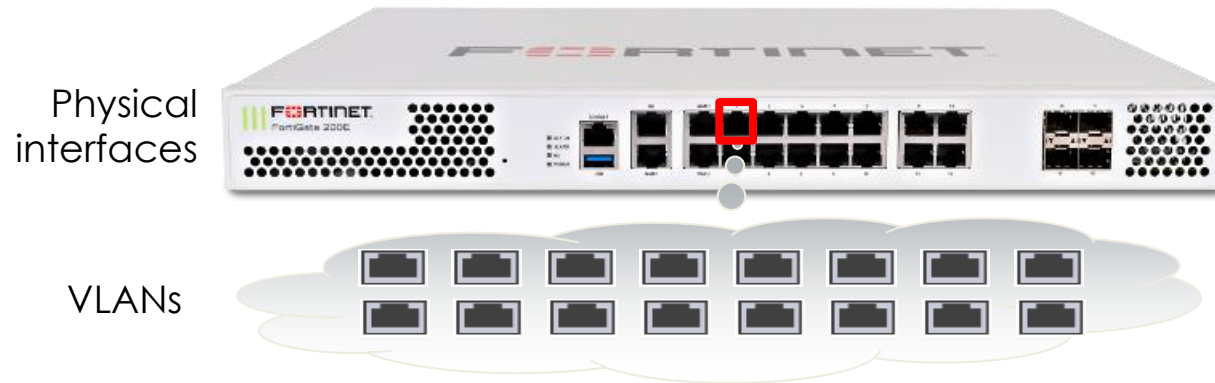
3.2 Agregación de enlaces

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

Network > Interfaces

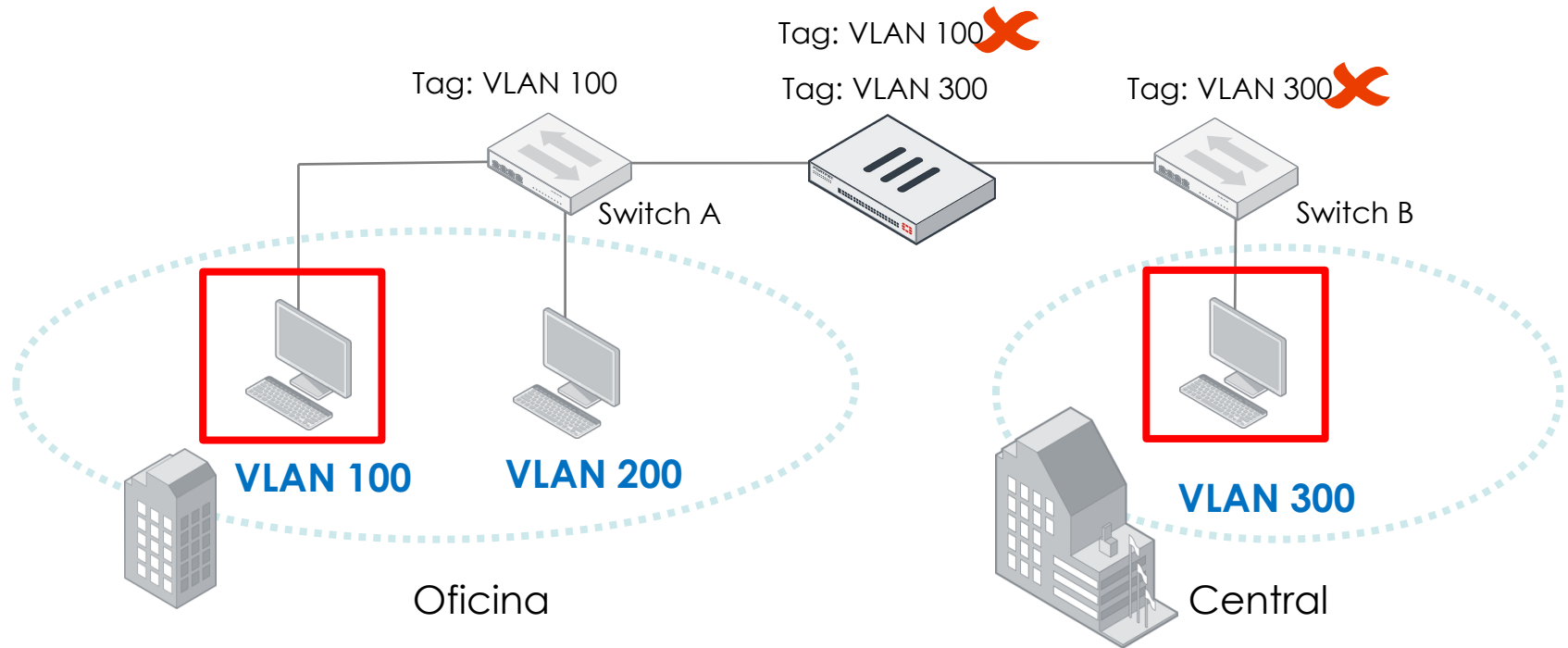
A screenshot of the 'New Interface' configuration window in Fortinet. The interface name is 'Link-Agg1'. The type is '802.3ad Aggregate'. The interface members are 'port6' and 'port7'. The role is 'Undefined'. The addressing mode is 'Manual' (selected), with 'DHCP' and 'Dedicated to FortiSwitch' also visible. The IP/Network Mask is '10.0.5.1/24'. The administrative access section shows 'IPv4' with 'HTTPS' and 'PING' checked, and 'HTTP', 'SSH', 'SNMP', 'FTM', and 'FortiTelemetry' unchecked. There are also checkboxes for 'CAPWAP', 'RADIUS Accounting', and 'FMG-Access'. The 'DHCP Server' option is disabled. The 'Security Mode' is set to 'None'. The window has 'OK' and 'Cancel' buttons at the bottom.

3.3 VLAN



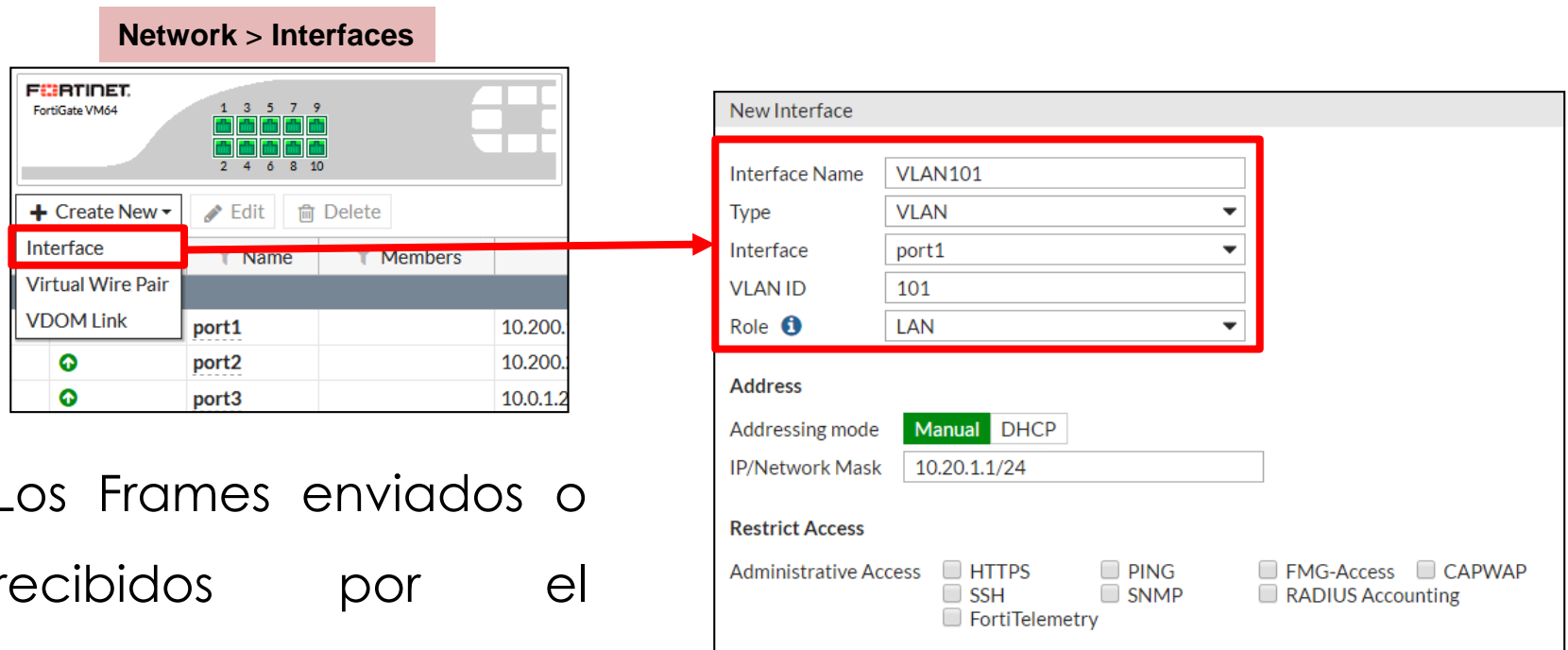
- Permite dividir la red física de nivel 2 en segmentos más pequeños.
 - Cada segmento forma una dominio broadcast separado.
 - Se añaden tags de vlan para identificar el segmento correspondiente.

3.3 VLAN: Ejemplo



3.3 VLAN: configuración

Network > Interfaces



The 'New Interface' configuration page shows the following settings:

- Interface Name: VLAN101
- Type: VLAN
- Interface: port1
- VLAN ID: 101
- Role: LAN
- Addressing mode: Manual (selected), DHCP
- IP/Network Mask: 10.20.1.1/24
- Restrict Access: Administrative Access (HTTPS, SSH, FortiTelemetry, PING, SNMP, FMG-Access, RADIUS Accounting, CAPWAP) - all unchecked.

- 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.

Network > Interfaces

Name	IP/Netmask	Type
Virtual Wire Pair		
port1	10.200.1.1 255.255.255.0	Physical Interface
port2	10.200.2.1 255.255.255.0	Physical Interface
port3	10.0.1.254 255.255.255.0	Physical Interface
port8	0.0.0.0 0.0.0.0	Physical Interface
port9	0.0.0.0 0.0.0.0	Physical Interface
port10	0.0.0.0 0.0.0.0	Physical Interface
Zone (5)		
DMZ		Zone
port4	192.168.1.1 255.255.255.0	Physical Interface
port5	192.168.10.1 255.255.255.0	Physical Interface
port6	192.168.20.1 255.255.255.0	Physical Interface
port7	0.0.0.0 0.0.0.0	Physical Interface

Incoming Outgoing

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

Edit Interface

Interface Name port3 (00:0C:29:6E:1E:B4)

Alias **internal_network**

Link Status Up

Type Physical Interface

Role **LAN**

Address

Addressing mode **Manual** DHCP Dedicated to FortiSwitch

IP/Network Mask 10.0.1.254/255.255.255.0

Administrative Access

IPv4 HTTPS HTTP PING FMG-Access
 CAPWAP SSH SNMP TELNET
 FTN RADIUS Accounting
 FortiTelemetry

DHCP Server

Address Range

Create New	Edit	Delete
Starting IP	End IP	
10.0.1.1	10.0.1.253	

Netmask 255.255.255.0

Default Gateway **Same as Interface IP** Specify

DNS Server **Same as System DNS** Same as Interface IP Specify

Advanced...

Edit Interface

DHCP Server

Address Range

Create New	Edit	Delete
Starting IP	End IP	
10.0.1.1	10.0.1.253	

Netmask 255.255.255.0

Default Gateway **Same as Interface IP** Specify

DNS Server **Same as System DNS** Same as Interface IP Specify

Advanced...

Mode **server** Relay

NTP Server **Local** Same as System NTP Specify

0.0.0.0

Time Zone **Same as System** Specify

Next Bootstrap Server 0.0.0.0

Additional DHCP Options

Create New	Edit	Delete	
Seq #	Option Code	Value	Hexadecimal Value
	51 (Lease Time)	604800	

MAC Reservation + Access Control

Create New	Edit	Delete	Add from DHCP Client List
MAC Address	Action or IP	Description	
00:00:00:00:00:00	Reserve IP	0.0.0.0	
Unknown MAC Addresses	Reserve IP		
	Assign IP		
	Block		

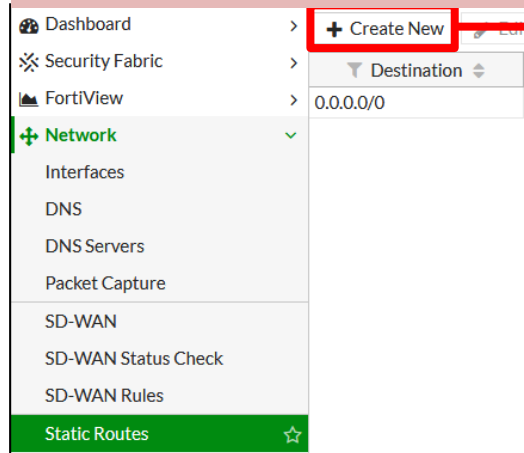
Type

OK Cancel

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.

Network > Static Routes



The 'New Static Route' configuration window is shown. The 'Destination' is set to 'Subnet' with the value '0.0.0.0/0.0.0.0'. The 'Device' is set to 'port1', and the 'Gateway' is set to '10.200.1.1'. The 'Administrative Distance' is set to '10'. The 'Status' is set to 'Enabled'. The 'Priority' is set to '0'. The 'OK' and 'Cancel' buttons are visible at the bottom.

Índice

4 GESTIÓN DE POLÍTICAS DE SEGURIDAD

4.1 GESTIÓN DE OBJETOS

4.2 DEFINICIÓN DE UNA POLÍTICA

4.3 TRABAJAR CON LA POLÍTICA

4.4 TRAFFIC SHAPPING

4.5 BEST PRACTICES

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

ID	Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
1	Internet	all	all	always	ALL	ACCEPT	Enabled	av default web default msc default ssl deep-inspection	All	20.32 MB
6	ISP2_OUT	all	all	always	ALL	ACCEPT	Enabled	av default web default msc default ssl certificate-inspection	All	0 B
7	sd-wan	all	all	always	ALL	ACCEPT	Enabled	av default web default msc default ssl certificate-inspection	All	0 B
0	Implicit Deny	all	all	always	ALL	DENY	Disabled			48.43 kB

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 protocolo)
- › Tiempo
- › NAT
- › Perfiles de seguridad.

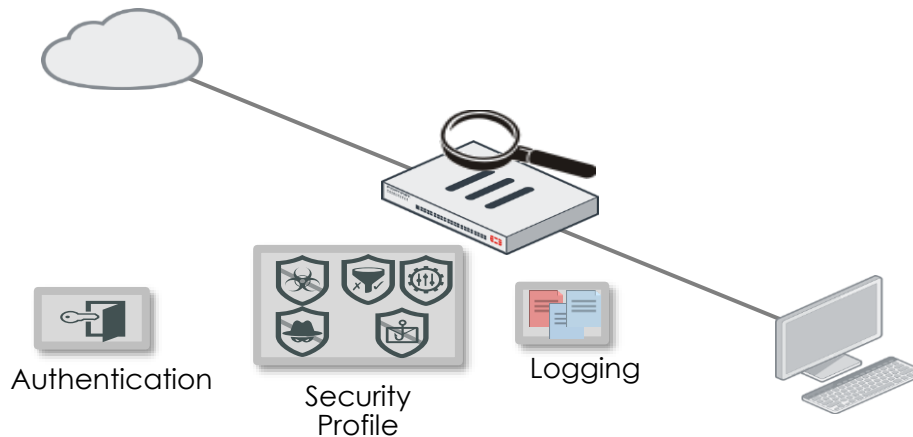
4.1- Políticas de seguridad: Gestión de objetos

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

Acción = ACCEPT o DENY

Policy & Objects > IPv4 Policy

New Policy	
Name	<input type="text"/>
Incoming Interface	<input type="text"/>
Outgoing Interface	<input type="text"/>
Source	<input type="text"/>
Destination	<input type="text"/>
Schedule	<input type="text" value="always"/>
Service	<input type="text"/>
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN



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

Obligatorio

Opcional

One address or address group is required

Unresolved FQDN: testfor123.com

FQDN (aún sin resolver)

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

New Policy

Name: Training

Incoming Interface: port3

Outgoing Interface: port1

Source: all

Destination: all, Facebook-Web

Schedule: always

Action: ACCEPT, DENY, LEARN

Select Entries

Address: Internet Service

Search

- Facebook-POP3(S)
- Facebook-SMTP(S)
- Facebook-Web
- Fortinet-DNS
- Fortinet-FortiGuard
- Fortinet-FTP(S)
- Fortinet-IMAP(S)
- Fortinet-LDAP(S)
- Fortinet-NetBIOS.Name.Service
- Fortinet-NTP
- Fortinet-POP3(S)

Addresses/groups cannot be mixed with Internet services

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

New Schedule

Type Recurring One-time

Name

Color

Days Sunday Monday Tuesday Wednesday Thursday Friday Saturday

All Day

Start Time Hour Minute

Stop Time Hour Minute



Policy & Objects > Schedules

New Schedule

Type Recurring One-time

Name

Color

Start Date

Start Time Hour Minute

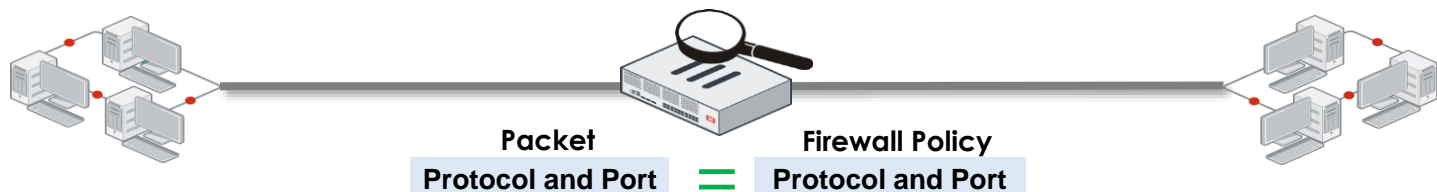
End Date

Stop Time Hour Minute

Pre-expiration event log Number of days before

4.1- Gestión de Objetos: Services

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



Policy & Objects > Services

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

Se puede ver **Por Secuencia**

Policy & Objects > IPv4 Policy

Pares de interfaces

ID	Policy Name	In Interface	Out Interface	Action	Status	Bandwidth
3	Internet	port1	ISP1 (port2)	ACCEPT	Enabled	23.78 GB
5	Internet_OUT	port1	ISP2 (port3)	ACCEPT	Enabled	36.38 MB

Interface Pair View By Sequence

▶ Por secuencia

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

Policy & Objects > IPv4 Policy

Múltiples interfaces

Interface any

ID	Policy Name	In Interface	Out Interface	Action	Status	Bandwidth
3	Internet	port1 port8	ISP1 (port2)	ACCEPT	Enabled	23.92 GB
6	Any_Interface	port4	any	ACCEPT	Enabled	0 B

Interface Pair View By Sequence

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

Después de mover

ID	Name	Source	Destination	Schedule	Service	Action
1	Full_Access	LOCAL_SUBNET	all	always	ALL	ACCEPT
2	Block_FTP	all	all	always	FTP	DENY

ID	Name	Source	Destination	Schedule	Service	Action
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

The screenshot displays the 'Edit Policy' configuration page for a policy named 'ALLOW_ALL'. The configuration includes: Incoming Interface (port3), Outgoing Interface (port1), Source (all), Destination (all), Schedule (always), Service (ALL), and Action (ACCEPT). Below the configuration, there are sections for Firewall/Network Options, Security Profiles, and Logging Options. On the right side, a red-bordered box highlights the real-time usage statistics for this policy:

- ID: 3
- Last used: 1 hour(s) ago
- First used: 1 hour(s) ago
- Hit count: 56
- Active sessions: 1
- Total bytes: 149.29 kB
- Current bandwidth: 0 B/s

At the bottom of the statistics box, there is a link for 'Online Help'.

4.4- Trabajar con la política: Agrupar objetos

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

The image illustrates the configuration of a firewall policy in Fortinet. It shows two stages of the configuration process:

Top Stage (Initial Configuration): A policy named 'port3 - port1 (1 - 3)' is shown. The 'Web_FTP' object is selected. The 'Address' field contains 'all' and the 'Service' field contains 'DNS', 'FTP', 'HTTP', and 'HTTPS'. The policy is set to 'ACCEPT' and 'Enabled'.

Bottom Stage (Final Configuration): The same policy is shown, but the 'Address' field now contains 'Local_LANs' and the 'Service' field contains 'Web-FTP'. The policy remains 'ACCEPT' and 'Enabled'.

Two red arrows indicate the transitions:

- The first arrow points from the 'Lan_1' and 'Lan_2' objects in the 'Address' field to the 'Local_LANs' object in the 'Address' field of the final configuration.
- The second arrow points from the 'DNS', 'FTP', 'HTTP', and 'HTTPS' objects in the 'Service' field to the 'Web-FTP' object in the 'Service' field of the final configuration.

Two configuration windows are shown in the middle:

- New Address Group:** Shows the creation of a group named 'Local_LANs' with members 'Lan_1' and 'Lan_2'.
- New Service Group:** Shows the creation of a group named 'Web-FTP' with members 'DNS', 'FTP', 'HTTP', and 'HTTPS'.

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.

The screenshot displays the Fortinet configuration interface for Policy & Objects > Addresses. It includes an 'Edit Policy' window, a 'Usage of Address: all' window, and a 'Properties of Policy: 4' window. Red boxes and arrows highlight key features: the 'View Properties' button in the usage window, the 'Ref.' column in the address list, and the '2 References' and '3' values in the usage table. Callouts explain that '2 References' is the number of times the object is used and '3' is the policy ID it is referenced by.

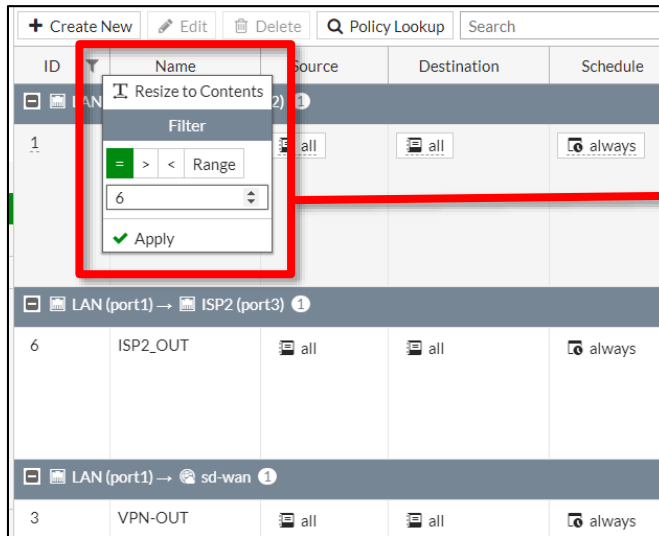
Name	Type	Details	Visibility	Ref.
LOCAL_SUBNET	Subnet	10.0.1.0/24	Visible	1
all	Subnet	0.0.0.0/0	Visible	6

Object Name	References
Address Group (1)	
Training	
Policy (3)	
4	2 References
3	2 References
5	

Name	Value
dstaddr	all
dstintf	
service	
srcaddr	all

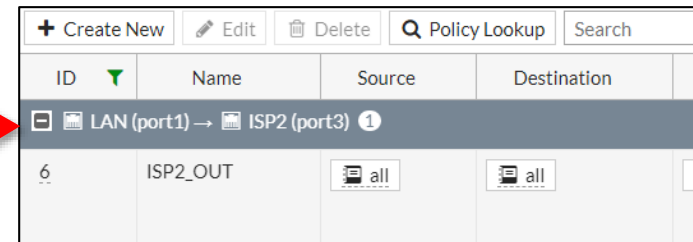
4.4- Trabajar con la política: filtrado de columnas

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



The screenshot shows the Fortinet firewall policy configuration interface. A red box highlights a 'Filter' dialog box that is open over the table. The dialog box has a 'Filter' section with a dropdown menu set to '6'. Below the dropdown is an 'Apply' button. A red arrow points from the '6' in the dropdown to the '6' in the table row.

ID	Name	Source	Destination	Schedule
1	LAN (port1) → ISP2 (port3)	all	all	always
6	ISP2_OUT	all	all	always
3	VPN-OUT	all	all	always



The screenshot shows the Fortinet firewall policy configuration interface after applying a filter. The table now only displays the policy with ID 6, 'ISP2_OUT', which matches the filter criteria.

ID	Name	Source	Destination	Schedule
6	ISP2_OUT	all	all	always

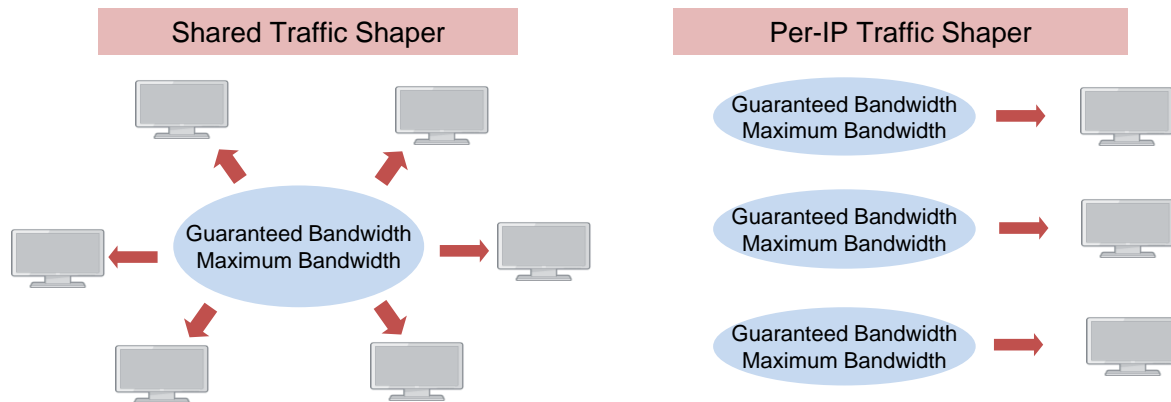
4.4- Trabajar con la política: Policy Lookup

- 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.

Policies & Objects > Traffic Shaping Policy



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 NAT

5.1 INTRODUCCIÓN

5.2 NAT DE ORIGEN

5.3 VIPS

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 Múltiple 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.

Policy & Objects > IPv4 Policy

Edit Policy

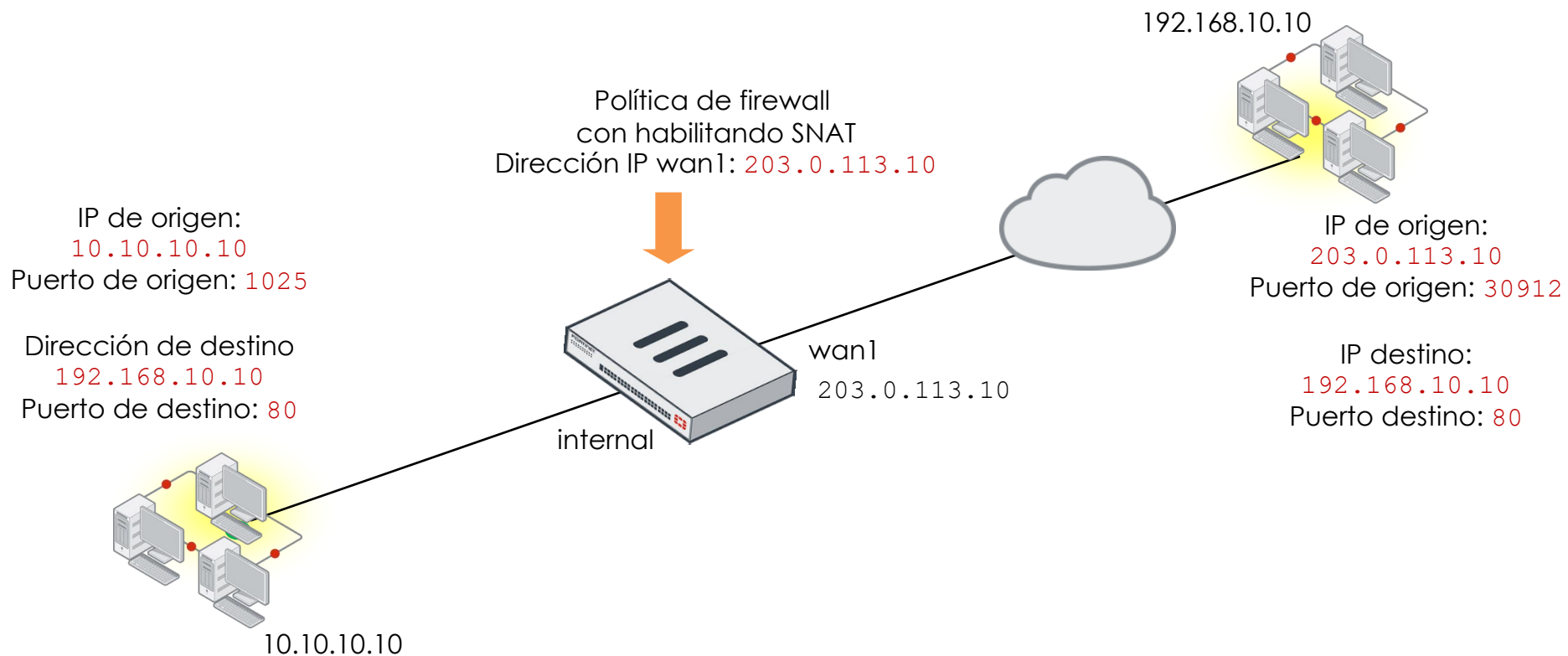
Name	Full_Access
Incoming Interface	port3
Outgoing Interface	port1
Source	all
Destination	all
Schedule	always
Service	ALL
Action	<input checked="" type="checkbox"/> ACCEPT <input type="checkbox"/> DENY <input type="checkbox"/> LEARN

Firewall / Network Options

NAT

IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

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 > IP Pools

New Dynamic IP Pool

Name

Comments 0/255

Type

Overload | One-to-One | Fixed Port Range | Port Block Allocation

External IP Range -

ARP Reply

Policy & Objects > IPv4 Policy

Edit Policy

Name

Incoming Interface

Outgoing Interface

Source

Destination

Schedule

Service

Action ACCEPT DENY LEARN

Firewall / Network Options

NAT

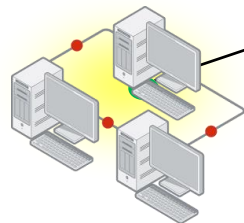
IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool

INTERNAL-HOST-EXT-IP

5.2 NAT de origen: Usando pools overload

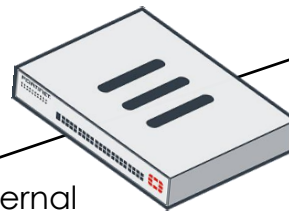
Firewall policy
With matching SNAT + IP pool enabled
wan1 IP pool: 203.0.113.2-203.0.113.5

Source IP address:
10.10.10.10
Source port: 1025
Destination IP address:
192.168.10.10
Destination port: 80



10.10.10.10

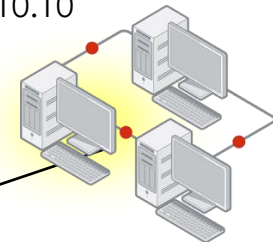
internal



wan1
203.0.113.10



192.168.10.10



Source IP address:
203.0.113.?
Source port: 30957
Destination IP address:
192.168.10.10
Destination port: 80

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

Edit Virtual IP

Name:

Comments:

Color: [Change]

Network

Interface:

Type: Static NAT

External IP Address/Range: -

Mapped IP Address/Range: -

Optional Filters:

Port Forwarding:

Policy & Objects > IPv4 Policy

Edit Policy

Name:

Incoming Interface:

Outgoing Interface:

Source:

Destination:

Schedule:

Service:

Action: ACCEPT DENY LEARN

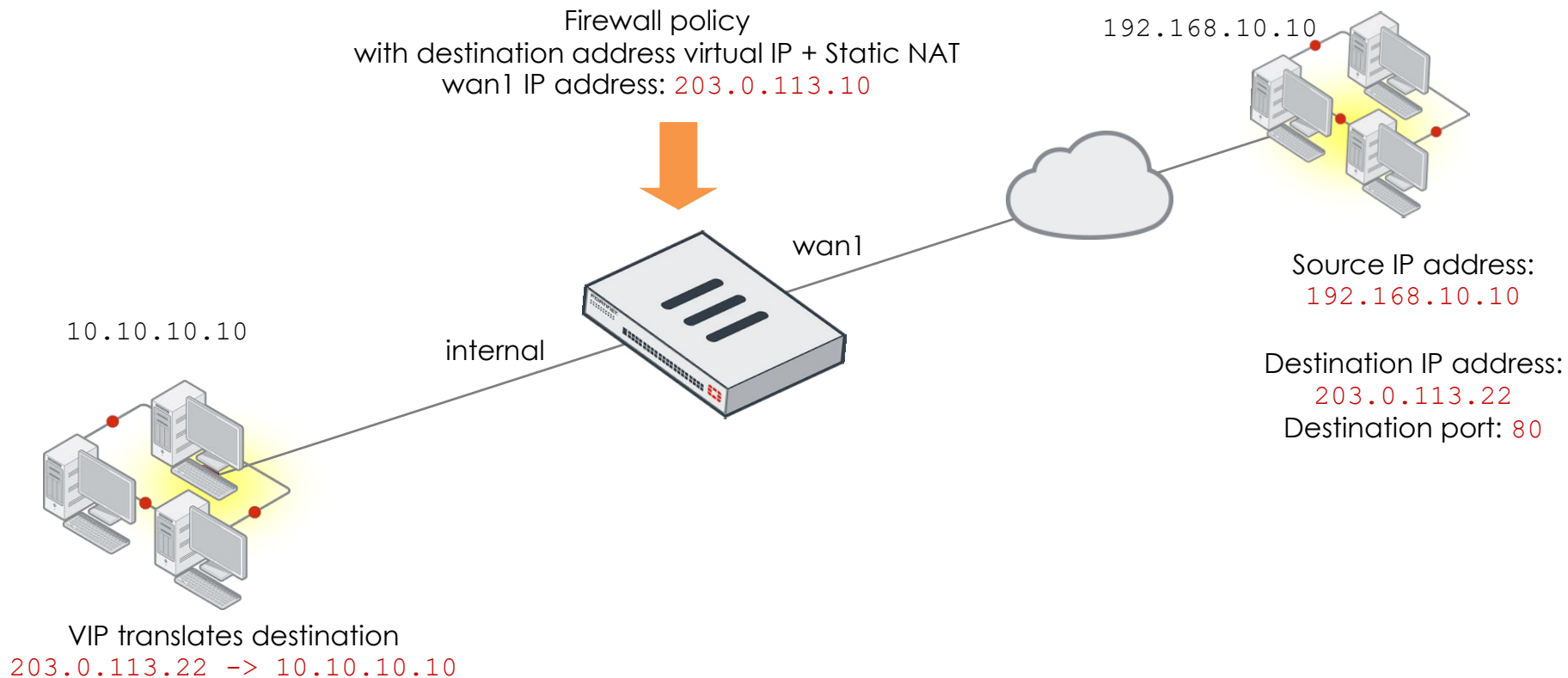
Firewall / Network Options

NAT:

El objeto VIP se usa como destino en una política

5.3 VIPS: Ejemplo

Firewall policy
with destination address virtual IP + Static NAT
wan1 IP address: 203.0.113.10



Índice

6 SD-WAN

6.1 DEFINICIÓN

6.2 CREACIÓN DE INTERFACES SDWAN

6.3 GESTIÓN DE POLÍTICAS SD-WAN

6.4 ROUTING

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.



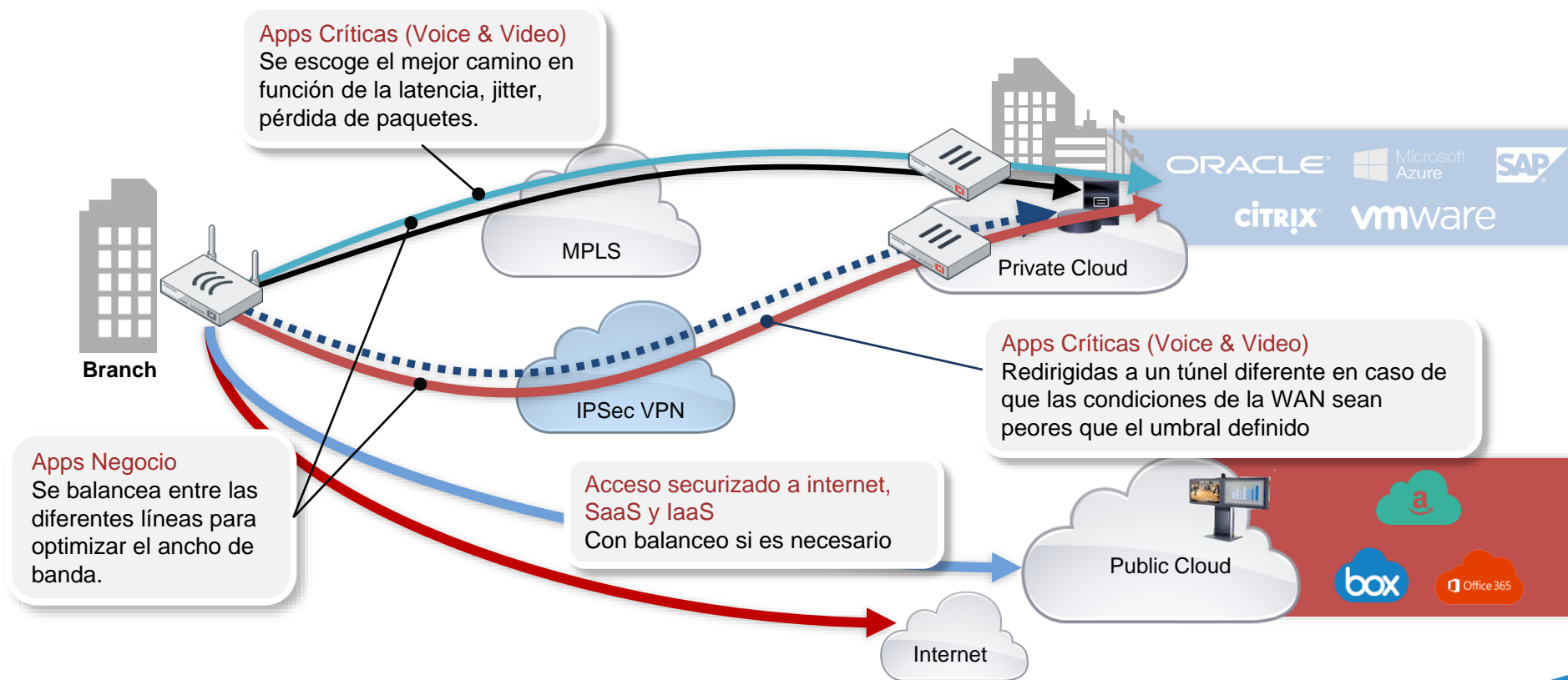
6.1 SD-WAN: Definición (caso de uso)

Migración MPLS



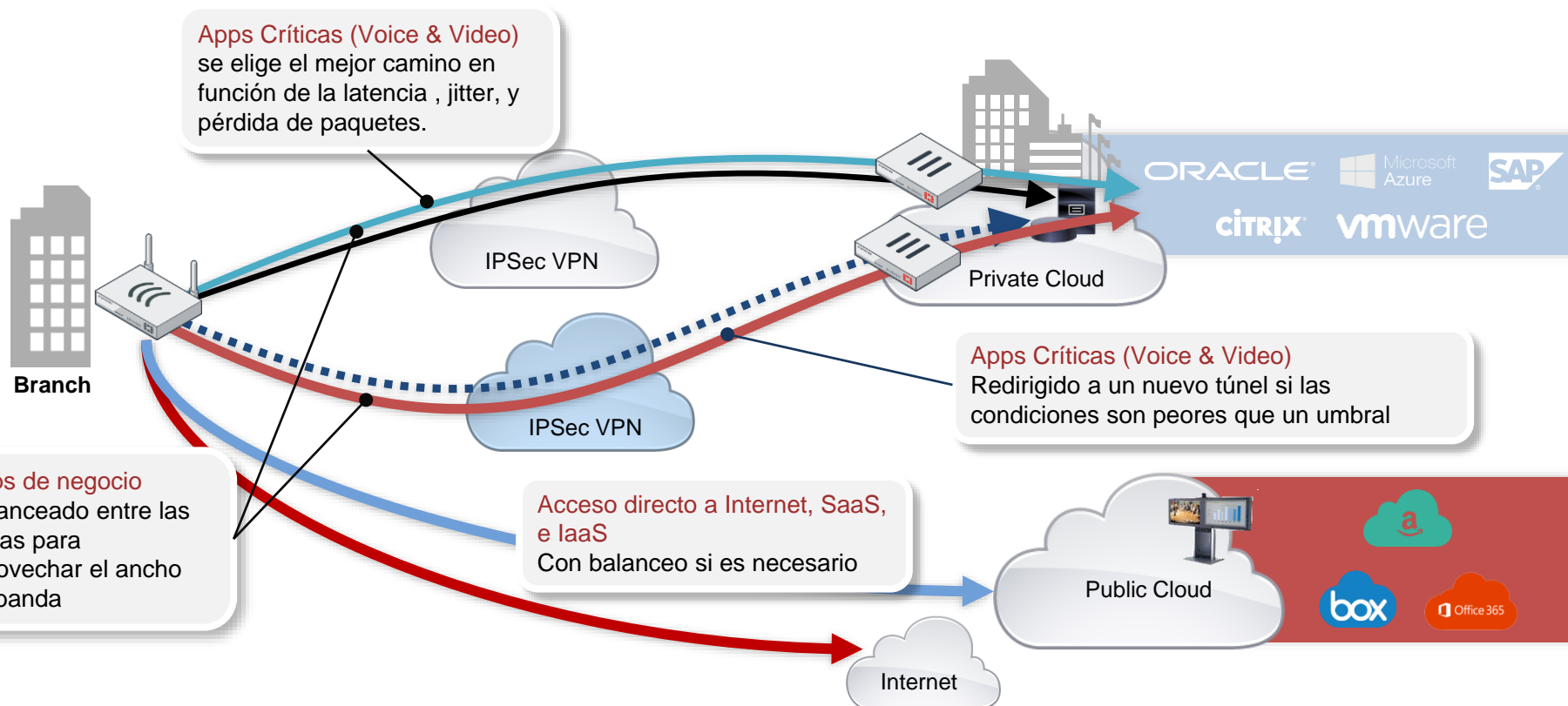
6.1 SD-WAN: Definición (caso de uso)

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.

The image displays two screenshots from the Fortinet SD-WAN configuration interface. The left screenshot, titled "Network > SD-WAN", shows the configuration for an SD-WAN interface. It includes fields for Name (SD-WAN), Type (SD-WAN Interface), and Status (Enable/Disable). Below, the "SD-WAN Interface Members" section lists two interfaces: "port1" and "port2", each with a Gateway of "10.200.1.254" and "10.200.2.254" respectively, and Status (Enable/Disable). A red box highlights the interface dropdowns, and a callout box labeled "Interfaces miembros" points to them. The bottom of the screenshot shows "SD-WAN Usage" with a bar chart for "Upstream" and "Downstream" traffic, with "port1" showing 87 bps and "port2" showing 317 bps. The right screenshot, titled "Network > SD-WAN Rules", shows the "Edit Implicit Rule" dialog. It features a "Load Balancing Algorithm" dropdown menu with options: "Source IP", "Sessions", "Spillover", "Source-Destination IP" (highlighted in green), and "Volume". "OK" and "Cancel" buttons are at the bottom.

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

The image displays three screenshots from the Fortinet configuration interface, illustrating the setup of an SD-WAN interface, a static route, and a firewall policy.

Network > Interfaces

SD-WAN Interface (3)				
sd-wan			SD-WAN Interface	
port1	10.200.1.1	255.255.255.0	Physical Interface	PING HTTPS SSH HTTP FMG-Access
port2	10.200.2.1	255.255.255.0	Physical Interface	PING HTTPS SSH HTTP

Network > Static

Edit Static Route

Destination: 0.0.0.0/0.0.0.0

Interface: SD-WAN

Administrative Distance: 1

Status: Enabled

Policy & Objects > IPv4 Policy

Name: Full_Access

Incoming Interface: port3

Outgoing Interface: sd-wan

Source: LOCAL_SUBNET

Destination: all

Schedule: always

Service: ALL

Action: ACCEPT

6.3 SD-WAN: Creación de rutas y políticas

Network > Static

Edit Static Route

Destination ⓘ Subnet Named Address Internet Service
0.0.0.0/0.0.0.0

Interface SD-WAN

Administrative Distance ⓘ 1

Comments 0/255

Status Enabled Disabled

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.

```
# 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
```

Índice

7 GESTIÓN DE PERFILES UTM

7.1 WEBFILTER

7.2 ANTIVIRUS

7.3 CONTROL DE APLICACIONES

7.4 IPS

7.5 INSPECCION SSL

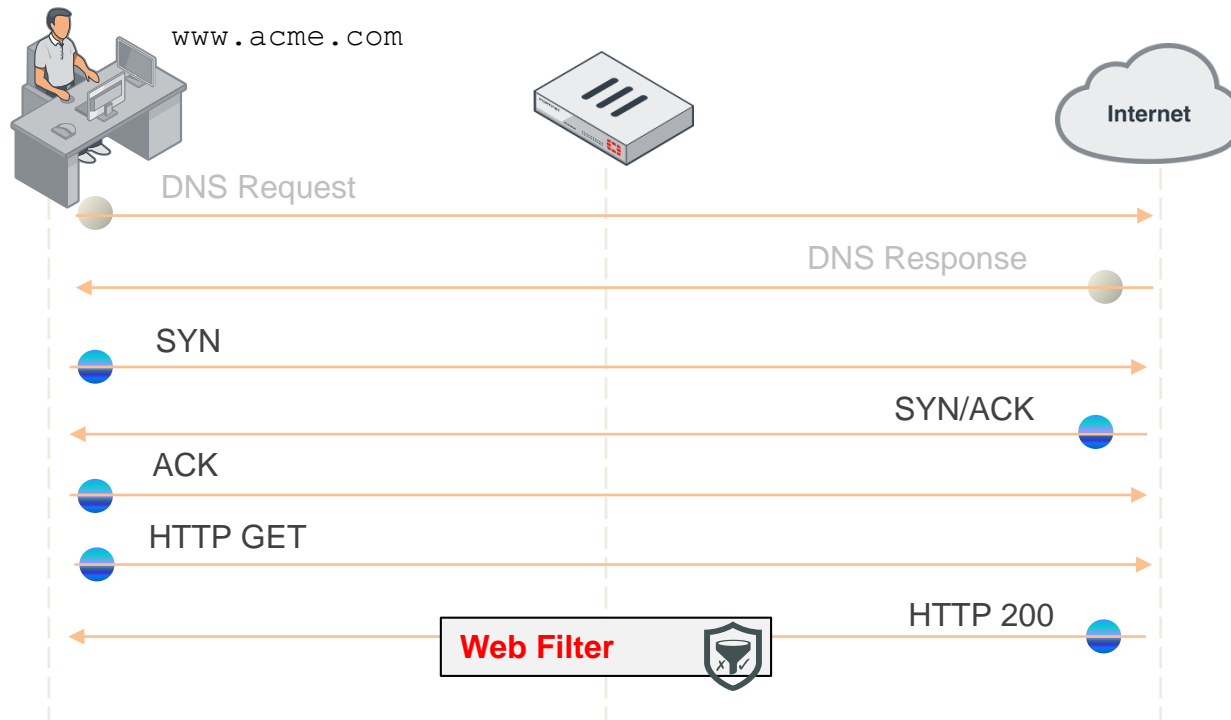
7 Asociación de perfiles a políticas

- ▶ 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
 - ▶ Previendo que ciertos datos abandonen la empresa.

Policy & Objects > IPv4 Policy

Security Profiles			
AntiVirus	<input checked="" type="checkbox"/>	AV default	
Web Filter	<input checked="" type="checkbox"/>	WEB default	
DNS Filter	<input type="checkbox"/>		
Application Control	<input checked="" type="checkbox"/>	APP default	
IPS	<input checked="" type="checkbox"/>	IPS default	
Proxy Options	<input type="checkbox"/>	PRX default	
SSL Inspection	<input type="checkbox"/>	SSL deep-inspection	

7.1 WebFiltering: Fundamentos



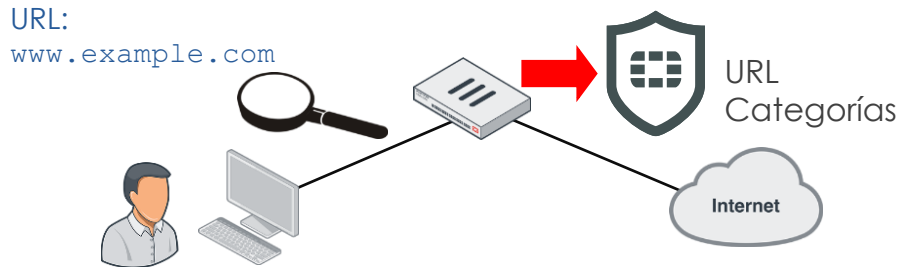
El filtrado se hace en base a la respuesta

7.1 WebFiltering: Categorías FortiGuard

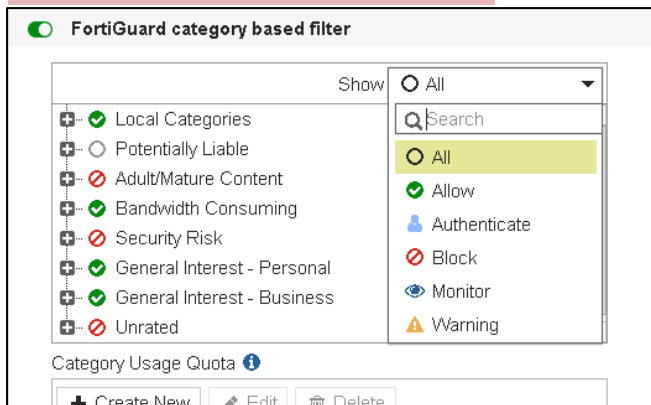
- Divide las URLs entre diferentes categorías y subcategorías
- Requiere hacer peticiones en vivo a FortiGuard
 - Requiere contrato en vigor
 - Existe un período de gracia de 7 días.
- Se puede usar FortiManager en vez de FortiGuard.



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.

Security Profiles > Web Filter

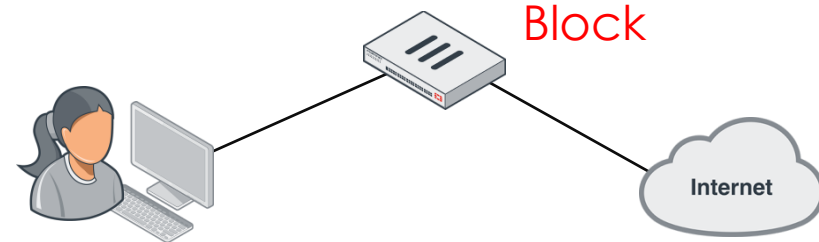
Static URL Filter

Block invalid URLs

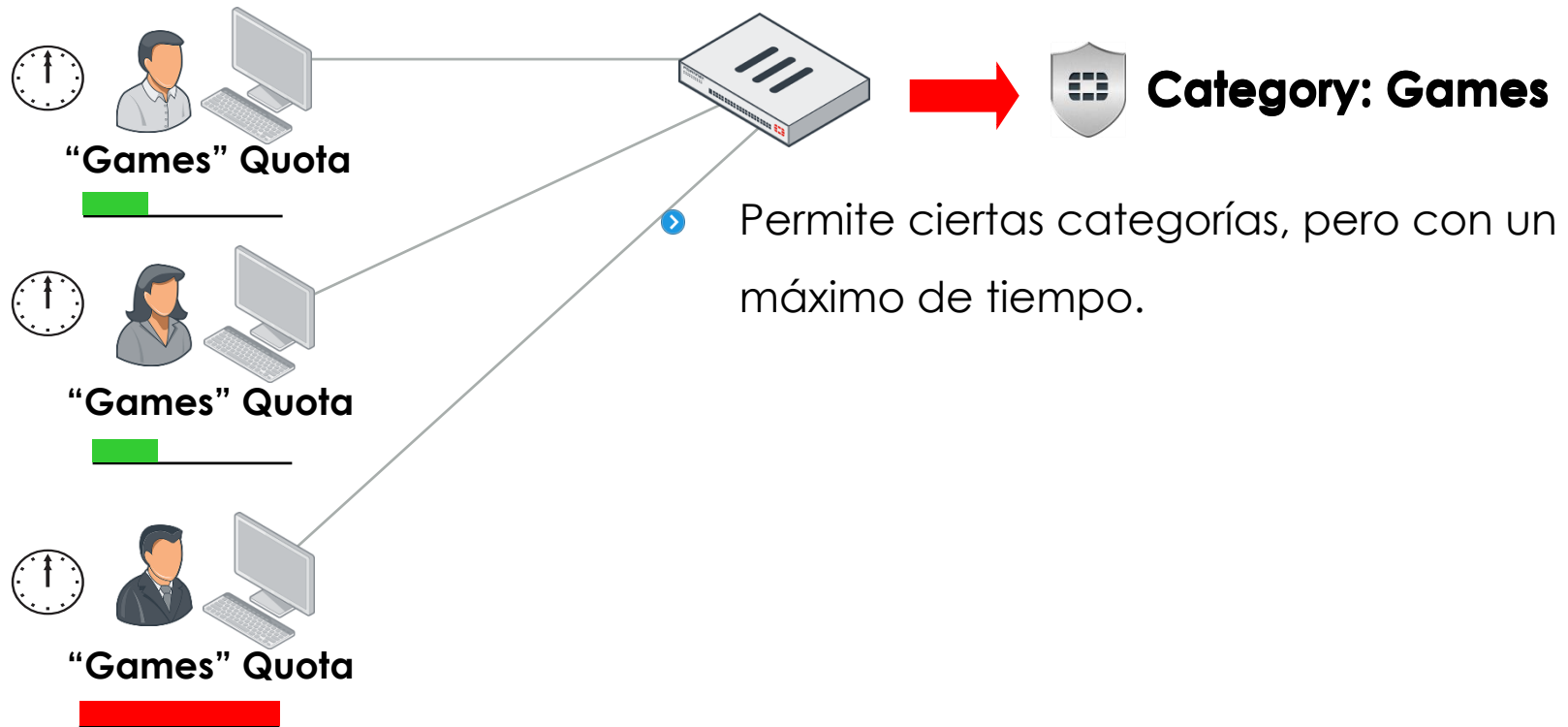
URL Filter

URL	Type	Action	Status
*\something\{org biz}	Reg. Expression	Exempt	Enable
somewhere.*	Wildcard	Monitor	Enable
www.somesite.com/someURL	Simple	Block	Enable

URL: `www.somesite.com/someurl`



7.1 WebFiltering: Cuotas



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

Orden de escaneo

1

Antivirus Scan

2

Grayware Scan

opcional (habilitado en CLI)

3

Heuristics Scan

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, para asuplementar la bbdd de firmas de FortiGuard.

Security Fabric > Settings

FortiGate Telemetry

FortiAnalyzer Logging

Sandbox Inspection

FortiSandbox type FortiSandbox Appliance FortiSandbox Cloud

FortiCloud account hkaila@fortinet.com

Applied Threat Intelligence

Dynamic Malware Detection version	not loaded
URL Threat Detection version	2.160448 (entries: 1000)

FortiSandbox Statistics (last 7 days)

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.

Admins controlan qué ficheros se envían al Sandbox.

Permite usar las firmas del FortiSandbox como complemento de las firmas de FortiGuard.

Security Profile > AntiVirus

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses. 29/255

Scan Mode: Quick Full

Detect Viruses: Block Monitor

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses:

Send Files to FortiSandbox Appliance for Inspection: None All Supported Files

Do not submit files matching types: +

Do not submit files matching file name patterns: +

Use Virus Outbreak Prevention Database:

Use FortiSandbox Database:

Apply

7.2 Antivirus: Configurar Perfiles

Security Profiles > AntiVirus

Edit AntiVirus Profile

Name: default

Comments: Scan files and block viruses.

Scan Mode: Quick **Full**

Detect Viruses: **Block** Monitor

APT Protection Options

Treat Windows Executables in Email Attachments as Viruses:

Send Files to FortiSandbox Appliance for Inspection: None **All Supported Files**

Do not submit files matching types: +

Do not submit files matching file name patterns: + File Name Pattern -

Use Virus Outbreak Prevention Database:

Use FortiSandbox Database:

Apply

System > Settings

Inspection Mode: **Flow-based** Proxy

NGFW Mode: **Profile-based** Policy-based

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

Network > Interfaces

Edit Interface

Interface Name port2 (00:0C:29:16:4D:72)
Alias
Link Status Up
Type Physical Interface
Role WAN
Estimated Bandwidth Kbps Upstream Kbps Downstream

Address
Addressing mode **Manual** DHCP
IP/Network Mask

Administrative Access
IPv4 HTTPS PING HTTP FMG-Access CAPWAP
 SSH SNMP TELNET FTM
 RADIUS Accounting FortiTelemetry

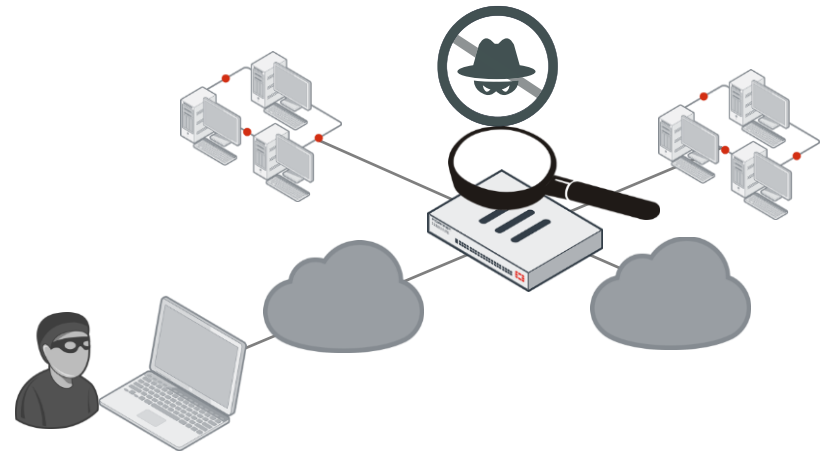
Miscellaneous
Scan Outgoing Connections to Botnet Sites
 34047 IP Addresses in botnet package.

Secondary IP Address

Status
Comments 0/255
Interface State Enabled Disabled

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

FortiGuard Distribution Network

License Information

Contract	Status	
FortiCare Support	Registered - [redacted]@fortinet.com	Launch Portal
Firmware	Web/online - expires on 2019/06/08	
Application Control Signatures	Version 6.00741	Upgrade Database
IPS	Licensed - expires on 2019/06/08	Upgrade Database
IPS Definitions	Version 6.00741	
IPS Engine	Version 4.00012	
Malicious URLs	Version 1.00001	

System > FortiGuard

AntiVirus & IPS Updates

Accept push updates [?](#)

Use override push

Scheduled Updates Every Hours

Improve IPS quality [?](#)

Use extended IPS signature package

[Update AV & IPS Definitions](#)

7.3 IPS: Firmas

Security Profiles > Intrusion Prevention

Edit IPS Sensor default

Name: default [View IPS Signatures]

Comments: Prevent critical attacks. 25/255

IPS Signatures

+ Add Signatures Delete Edit IP Ex

Name	Exempt IPs	Severity	Target
No matching entries found			

IPS Filters

+ Add Filter Edit Filter Delete

+ Create New Edit Delete Search Standard Package

Name	Severity	Target	OS	Action
3Com.3CDaemon.FTP.Server.Buffer.Overflow	■■■■	Server	Windows	Block
3Com.3CDaemon.FTP.Server.Information.Disclosure	■ ■ ■ ■	Client	Windows	Block
3Com.Intelligent.Management.Center.Information.Disclosure	■■■■	Server	Windows	Block
3Com.OfficeConnect.ADSL.Wireless.Firewall.Router.DoS	■■■■	Server	Linux	Block
3ivx.MPEG4.File.Processing.Buffer.Overflow	■■■■	Client	Windows	Block
3S-Smart.GmbH.CODESYS.Web.Server.Buffer.Overflow	■■■■	Server	Windows	Block
3S.CODESYS.Gateway.Server.Heap.Buffer.Overflow	■■■■	Server	Windows	Block

BBDD Activa

Acción por defecto

7.3 IPS: Sensores

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

Security Profiles > Intrusion Prevention

New IPS Sensor

Name

Comments

IPS Signatures

+ Add Signatures Delete Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action
No matching entries found						

IPS Filters

+ Add Filter Edit Filter Delete

Filter Details	Action	Packet
No matching entries found		

Rate Based Signatures

Add Signatures

Q Search Total Selected Signatures: 3

Name	Severity	Target	OS
3Com.3CDaemon.FTP.Server.Buffer.Overflow	■■■■■	Server	Windows
3Com.3CDaemon.FTP.Server.Information.Disclosure	■■■■■	Client	Windows
3Com.3CDaemon.FTP.Server.Information.Disclosure	■■■■■	Server	Windows
35-Smart.GmbH.CODESYS.Web.Server.Buffer.Overflow	■■■■■	Server	Windows
7TIGSS.ODBC.Server.Memory.Corruption	■■■■■	Server	Windows

Use Selected Signatures Cancel

Add Filter

OS: Windows Protocol: HTTP Severity: Critical Target: server Add Filter

Name	Severity	Target	OS
35-Smart.GmbH.CODESYS.Web.Server.Buffer.Overflow	■■■■■	Server	Windows
ABNR.Botnet	■■■■■	Server	All
ADKR.Botnet	■■■■■	Server	All
Adobe.Acrobat.and.Reader.mailto.URI.Code.Execution	■■■■■	Server; Client	Windows
Adobe.Acrobat.And.Reader.TrueTypeFont.Parsing.Buffer.Overflow	■■■■■	Server; Client	All
Adobe.Acrobat.BMP.Colors.Parsing.Memory.Corruption	■■■■■	Server; Client	Windows; MacOS
Adobe.Acrobat.GetIcon.Method.Stack.Overflow	■■■■■	Server; Client	Windows
Adobe.Acrobat.ICC.Profile.Description.Tag.Buffer.Overflow	■■■■■	Server; Client	Windows; MacOS

Total: 779

Use Filters Cancel

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)
<input checked="" type="checkbox"/>	Apache.HTTPD.mod_http2.DoS	300	1	Source IP	Block	Expires 4 Hour(s)
<input type="checkbox"/>	DotNetNuke.Padding.Oracle.Attack	1000	5	Any	Block	None
<input checked="" type="checkbox"/>	FTP.Login.Brute.Force	200	10	Source IP	Block	Expires 1 Hour(s)
<input type="checkbox"/>	FreeBSD.TCP.Reassembly.DoS	10	2	Any	Block	None
<input checked="" type="checkbox"/>	IMAP.Login.Brute.Force	60	10	Source IP	Block	Expires 1 Hour(s)
<input checked="" type="checkbox"/>	MS.Active.Directory.LDAP.Packet.Handling.DoS	100	1	Source IP	Block	Expires 5 Minute(s)
<input type="checkbox"/>	MS.OWA.Brute.Force	15	1	Any	Block	None
<input checked="" type="checkbox"/>	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

Name: SERVER

Comments: 0/255

IPS Signatures

+ Add Signatures Delete Edit IP Exemptions

Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
4D.WebStar.Tomcat.Plugin.Remote.Buffer.Overflow	0	■■■■■	Server	TCP,HTTP	Windows	Monitor	✖

IPS Filters

+ Add Filter Edit Filter Delete

Filter Details	Action	Packet Logging
Severity: ■■■■■, ■■■■■, ■■■■■ Location: server OS: Windows	Default	✖

Rate Based Signatures

Enable	Signature	Threshold	Duration (seconds)	Track By	Action	Block Du
--------	-----------	-----------	--------------------	----------	--------	----------

OK Cancel

Las acciones individuales preceden a los filtros

7.3 IPS: Acciones

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

Security Profiles > Intrusion Prevention

IPS Signatures

+ Add Signatures Delete Edit IP Exemptions

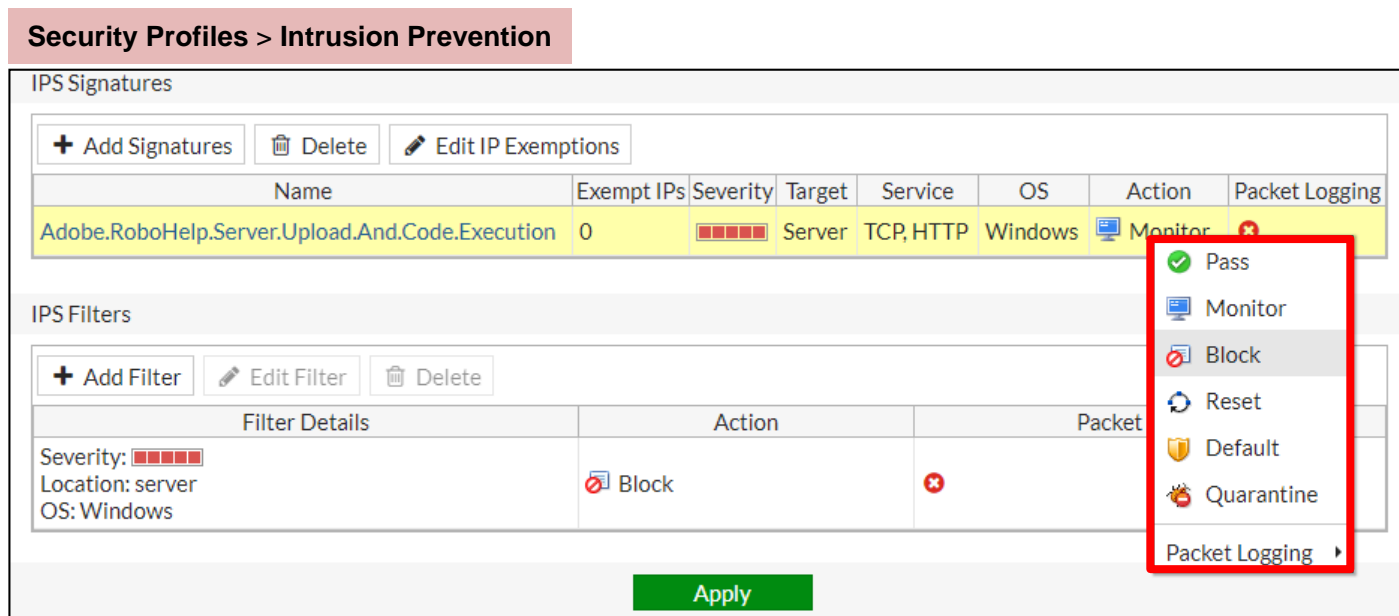
Name	Exempt IPs	Severity	Target	Service	OS	Action	Packet Logging
Adobe.RoboHelp.Server.Upload.And.Code.Execution	0	■■■■■	Server	TCP,HTTP	Windows	Monitor	⊕

IPS Filters

+ Add Filter Edit Filter Delete

Filter Details	Action	Packet
Severity: ■■■■■ Location: server OS: Windows	Block	⊕

Apply



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

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

System > FortiGuard

License Information		
Contract	Status	
FortiCare Support	✓ Registered - [redacted]@fortinet.com	Launch Portal
Firmware	✓ Web/online - expires on 2019/06/08	
Application Control Signatures	🔄 Version 6.00741	Upgrade Database

BBDD de aplicaciones instalada

System > FortiGuard

AntiVirus & IPS Updates	
Accept push updates ⓘ	<input type="checkbox"/>
Scheduled Updates	<input checked="" type="checkbox"/> Every 2 Hours
Improve IPS quality ⓘ	<input type="checkbox"/>
Use extended IPS signature package	<input type="checkbox"/>
🔄 Update AV & IPS Definitions	

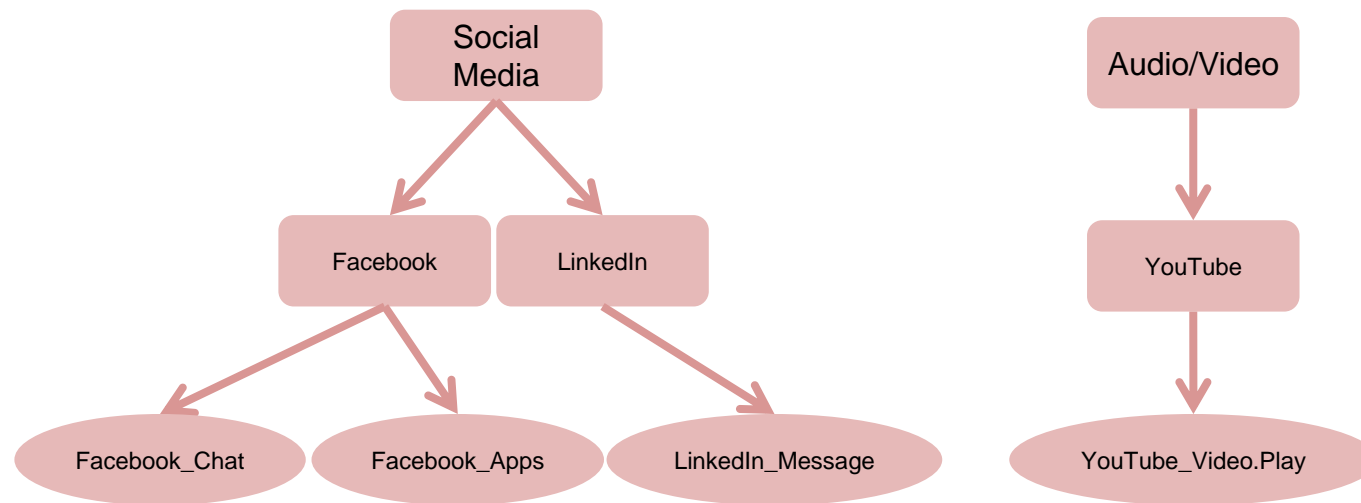
Actualizaciones "push"

Actualizaciones periódicas

Fuerza a FortiGate a comprobar si hay actual.

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

Security Profiles > Application Control

Edit Application Sensor

96 Cloud Applications require deep inspection.
0 policies are using this profile.

Name: default

Comments: Monitor all applications. 29/255

Categories

- All Categories
- Business (148, 6)
- Industrial (596)
- Social.Media (117, 31)
- Unknown Applications
- Cloud.IT (41)
- Mobile (3)
- Storage.Backup (171, 17)
- Collaboration (275, 10)
- Network.Service (321)
- Update (49)
- Email (79, 13)
- P2P (69)
- Video/Audio (161, 13)
- Game (82)
- Proxy (139)
- VolP (27)
- General.Interest (226, 6)
- Remote.Access (84)
- Web.Client (21)

Application Overrides

Application Sig	Category	Action
No matching entries found		

Filter Overrides

Filter Details	Action
No matching entries found	

Aplica una acción a todas las cats a la vez

Muestra una lista de todas las firmas de aplicación

Aplicaciones sin identificar

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

Security Profiles > Application Control

Edit Application Sensor

Name: default

Comments: Monitor all applications. 25/255

3 Categories

All Categories

- Business (148, 6)
- Industrial (516)
- Social.Media (118, 31)
- Unknown Applications
- Cloud.IT (41)
- Mobile (3)
- Storage.Backup (171, 17)
- Collaboration (275, 10)
- Network.Service (320)
- Update (49)
- Email (0)
- P2P (6)
- Video (0)

1 Application Overrides

+ Add Signatures Edit Parameters Delete

Application Signature	Category
No matching entries found	

2 Filter Overrides

+ Add Filter Edit Delete

Filter Details
No matching entries found

Options

Allow and Log DNS Traffic

QUIC Allow Block

Replacement Messages for HTTP-based Applications

Apply

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**.

Security Profiles > Application Control

Name: default [View Application Signatures]

Comments: Monitor all applications. 25/255

Categories

All Categories

- Business (148, △ 6)
- General.Interest (226, △ 6)
- Proxy (139)
- Video/Audio (161, △ 13)
- Cloud.IT (41)
- Industrial (596)
- Remote.Access (84)
- VoIP (27)
- Collaboration (275, △ 10)
- Mobile (3)
- Social.Media (117, △ 31)
- Web.Client (21)
- Email (79, △ 13)
- Network.Service (321)
- Storage.Backup (171, △ 17)
- Unknown Applications
- Game (82)
- P2P (69)
- Update (49)

Application Overrides

+ Add Signatures | Edit Parameters | Delete

Application Signature	Category	Action
Battle.Net	Game	Monitor
Dailymotion	Video/Audio	Monitor

Filter Overrides

+ Add Filter | Edit | Delete

Filter Details	Action
Behavior: Excessive-Bandwidth (417, △ 49)	Block

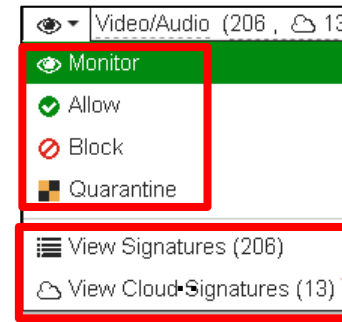
3

1

2

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

Edit SSL/SSH Inspection Profile

custom-deep-inspection

Name: custom-deep-inspection

Comments: Customizable deep inspection profile. 37/255

SSL Inspection Options

Enable SSL Inspection of: Multiple Clients Connecting to Multiple Servers

Inspection Method: **SSL Certificate Inspection** Full SSL Inspection

CA Certificate: Fortinet_CA_SSL Download Certificate

Untrusted SSL Certificates: Allow Block View Trusted Certificates List

Protocol Port Mapping

Inspect All Ports:

HTTPS: 443

Nombre de perfil:
custom-deep-inspection.

SSL Certificate
Inspection.

7.5 INSPECCION SSL

Security Profiles > SSL/SSH Inspection

SSL Inspection Options

Enable SSL Inspection of **Multiple Clients Connecting to Multiple Servers**
Protecting SSL Server

Inspection Method **Full SSL Inspection**
SSL Certificate Inspection

CA Certificate ⚠ **Fortinet_CA_SSL** [Download Certificate](#)

Untrusted SSL Certificates **Allow** Block [View Trusted CAs List](#)

RPC over HTTPS

Índice

8

ANÁLISIS DE SEGURIDAD

8.1

ACTIVACIÓN Y ANÁLISIS DE LOGS

8.2

EJEMPLO DE EVENTOS DE SEGURIDAD

8.3

ANÁLISIS DE VULNERABILIDADES

8.4

HOSTS COMPROMETIDOS

8.5

OTRA INFORMACIÓN

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

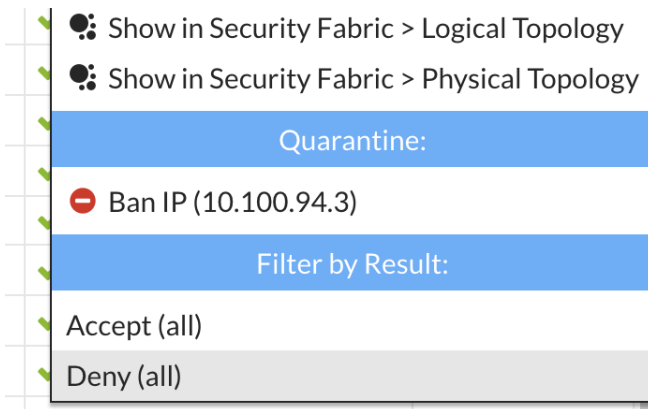
- Log & Report -> Forward Traffic
- Se pueden obtener todos los logs de tráfico, la acción asociada (permitir/denegar) y los eventos de seguridad asociados, si los hay.

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

Event	Event Status	Event Type	Count	Severity	First Occurrence	Last Update	Additional Info
Access to Malicious Websites ...	Unhandled	Web Filter	97	High	2018-11-25 13:01:56	2018-11-25 15:44:43	Security Risk
Access to Malicious Websites ...				High	2018-11-25 13:05:58	2018-11-25 15:44:42	Security Risk
> 10.100.92.19 (5)				Critical	3 hours ago	A few seconds ago	...
> 10.100.92.15 (5)				Critical	3 hours ago	A few seconds ago	...
> 10.100.92.10 (5)				Critical	3 hours ago	A minute ago	...

Topology

- FGVM010000166026
- 10.100.92.10

Addresses MAC: 00:0c:95:55:00:0a
IP: 10.100.92.10

- 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 Blo
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

urltbls	213.211.198.58:80:HTTP
epid	1033
itime_t	1543157489
byod_device	router-nat-device
Log ID	0000000022
saasinfo	0
Security Events	AV 1 WEB 1 APP 1
threattys	"Malicious Websites",malwa detected
dvid	1028
apps	HTTP.BROWSER_Firefox
Tune	traffic

8.2 Ejemplo de evento de seguridad

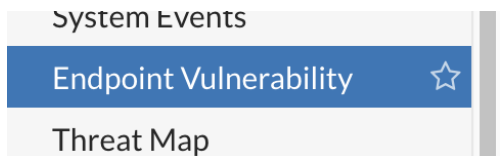
- Desde un EndPoint, accedemos a eicar.org
- Descargamos el fichero eicar sobre una conexión **cifrada**:
 - No se recibe un mensaje de reemplazo
 - Quien deniega el acceso es el antivirus de puesto (en este caso el FortiClient)

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.



Device	Source	Detected Vulnerabilities
harry-pc	Harry_Martin (10.100.94.100)	82
Alex-Laptop	Alex_Fox (10.100.94.5)	4
Cale-Laptop	Cale_Williamson (10.100.94.2)	1

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

10.100.92.13	00:0c:95:55:00:0d	Compromised
10.100.92.4	00:0c:95:55:00:04	Compromised
10.100.93.2	02:09:0f:00:07:02	Compromised
10.100.92.3	00:0c:95:55:00:03	Compromised

- 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