UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERIA Y ARQUITECTURA

ESCUELA DE INGENIERÍA ELÉCTRICA

TEMA:

CURSO DE ESPECIALIZACIÓN: TECNOLOGÍA, ECONOMÍA Y POLÍTICAS EN REDES INALÁMBRICAS

SUB-TEMA:

PROPUESTA DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA EMPRESAS DEL SECTOR ELÉCTRICO Y DE TELECOMUNICACIONES.

PRESENTADO POR:

JUAN RENÉ GUTIÉRREZ JUÁREZ

BRENDA AZUCENA GUZMÁN COTO

REYNALDO DE JESÚS NÚÑEZ CARTAGENA

JULIO ARMANDO SOLANO TOLEDO

PARA OTORGAR EL TÍTULO DE:

INGENIERO ELECTRICISTA

CIUDAD UNIVERSITARIA, ABRIL DEL 2025

UNIVERSIDAD DE EL SALVADOR

RECTOR:

MSC. JUAN ROSA QUINTANILLA

SECRETARIO GENERAL:

LIC. PEDRO ROSALIO ESCOBAR CASTANEDA

FACULTAD DE INGENIERÍA Y ARQUITECTURA

DECANO:

ING. LUIS SALVADOR BARRERA MANCÍA

SECRETARIO:

ARQ. RAÚL ALEXANDER FABIÁN ORELLANA

ESCUELA DE INGENIERÍA ELÉCTRICA

DIRECTOR INTERINO:

ING. WERNER DAVID MELÉNDEZ VALLE

UNIVERSIDAD DE EL SALVADOR

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA DE INGENIERÍA ELÉCTRICA

Trabajo de graduación previo a la opción al grado de:

INGENIERO ELECTRICISTA

Título:

CURSO DE ESPECIALIZACIÓN: TECNOLOGÍA, ECONOMÍA Y POLÍTICAS EN REDES INALÁMBRICAS

Subtítulo:

PROPUESTA DE UN SISTEMA DE SEGURIDAD PERIMETRAL PARA EMPRESAS DEL SECTOR ELÉCTRICO Y DE TELECOMUNICACIONES.

Presentado por:

JUAN RENÉ GUTIÉRREZ JUÁREZ

BRENDA AZUCENA GUZMÁN COTO

REYNALDO DE JESÚS NÚÑEZ CARTAGENA

JULIO ARMANDO SOLANO TOLEDO

Docente asesor:

Dr. CARLOS OSMIN POCASANGRE JIMENEZ

SAN SALVADOR, ABRIL 2025

Trabajo de Graduación Aprobado por:

Docente Asesor:

Dr. CARLOS OSMIN POCASANGRE JIMENEZ

NOTA Y DEFENSA FINAL

En esta fecha martes 18 de marzo de 2025, en la Sala de Lectura de la Escuela de Ingeniería Eléctrica, a las 10:00 a.m. horas, en presencia de las siguientes autoridades de la Escuela de Ingeniería Eléctrica de la Universidad de El Salvador:

1. Ing. Werner David Meléndez Valle
   Director Interino
   Firma

2. MSc. José Wilber Calderón Urrutia
   Secretario
   Firma

Y, con el Honorable Jurado de Evaluación integrado por las personas siguientes:

- DR. CARLOS OSMIN POCASANGRE JIMÉNEZ
  (Docente Asesor)
  Firma

- ING. WERNER DAVID MELENDEZ VALLE
  Firma

- ING. LUIS ERNESTO ESCOBAR BRIZUELA
  Firma

Se efectuó la defensa final reglamentaria del Trabajo de Graduación (Curso de Especialización): TECNOLOGÍA, ECONOMÍA Y POLÍTICAS EN REDES INALÁMBRICAS

A cargo de los Bachilleres:

- GUTIÉRREZ JUÁREZ JUAN RENÉ
- GUZMÁN COTO BRENDA AZUCENA
- NÚÑEZ CARTAGENA REYNALDO DE JESÚS
- SOLANO TOLEDO JULIO ARMANDO

Habiendo obtenido en el presente Trabajo una nota promedio de la defensa final: 7.8
(Siete punto ocho)

AGRADECIMIENTOS

Agradezco a Dios por darme la fortaleza, la salud y la sabiduría necesarias para culminar esta etapa tan importante en mi vida.

A mi familia, por su amor incondicional, por creer en mí en cada paso del camino y por brindarme su apoyo en los momentos de mayor dificultad. Sin su respaldo, este logro no habría sido posible.

Expreso mi sincero agradecimiento al Ing. Werner David Meléndez Valle, por su guía, orientación y disponibilidad constante durante el desarrollo de este trabajo de graduación. Su acompañamiento fue clave para avanzar con claridad y confianza. Asimismo, al Dr. Carlos Osmin Pocasangre Jiménez, por sus valiosas observaciones, exigencia académica y aportes que enriquecieron este proyecto. Su experiencia y compromiso con la formación profesional fueron una inspiración.

A mis compañeros de carrera, quienes compartieron conmigo este proceso lleno de retos, aprendizajes y crecimiento personal.

Y finalmente, a todas las personas e instituciones que, de alguna manera, contribuyeron a que hoy pueda alcanzar esta meta. Este logro es el resultado de un esfuerzo colectivo y significativo.

Reynaldo De Jesús Núñez Cartagena

A Dios, por ser mi guía constante en cada paso de este camino. Por darme fuerzas cuando sentí que ya no podía más, por brindarme sabiduría y por recordarme que nunca estuve solo, incluso en los momentos más difíciles. Sin su presencia, este logro no habría sido posible.

A mi prometida, mi compañera de vida, gracias por tu amor incondicional, tu paciencia infinita y tu apoyo en cada etapa de este proceso. Gracias por creer en mí incluso cuando yo dudaba, por tus palabras de aliento y por estar a mi lado en los días buenos y en los complicados. Tu presencia ha sido una fuente de motivación y fortaleza. Esta meta también es tuya. Gracias por darme la serenidad que tanto necesitaba cuando el estrés me sobrepasaba, por entender mis ausencias y por esperarme siempre con una sonrisa. Tus abrazos fueron mi hogar en medio del cansancio, y tus palabras, el impulso que me empujó a seguir. Eres parte fundamental de este logro, y lo dedico con todo mi corazón a ti.

Julio Armando Solano Toledo

Primero que todo, agradezco a Dios por darme la vida, la salud y la oportunidad de llegar hasta aquí.

A mis padres, por su amor incondicional, sus consejos y por enseñarme con el ejemplo el valor del esfuerzo y la perseverancia. Gracias por creer en mí, este logro también es suyo.

A toda mi familia, por su apoyo constante, sus palabras de aliento y su comprensión en los momentos de ausencia y estrés. Gracias por estar presentes, incluso en la distancia.

A mi novia Sofía Rivera, por su paciencia, su apoyo en los días complicados y por motivarme constantemente a seguir adelante. Gracias por estar a mi lado y compartir conmigo esta etapa.

A mi amiga Tania Díaz, por ser un apoyo confiable durante este camino.

A mis docentes y asesores, por compartir sus conocimientos con dedicación y por su guía a lo largo de esta etapa académica.

A mis compañeros y amigos, por su compañía en este proceso, por las risas, los desvelos compartidos, y por ser una parte fundamental de esta etapa.

Finalmente, gracias a todas aquellas personas que, de una u otra forma, formaron parte de este camino. Cada gesto, palabra o acción tuvo un impacto que me ayudó a llegar hasta aquí.

Juan René Gutiérrez Juárez

Llegar hasta aquí ha sido un camino lleno de desafíos, aprendizajes y también de muchas personas valiosas que me acompañaron en cada etapa. En primer lugar, agradecer a Jehová Dios, por permitirme terminar mi carrera. Quiero agradecer profundamente a mi madre, Isabel, quién siempre estuvo apoyándome en todo aspecto, pendiente de mí, hizo todo lo que pudo para brindarme los medios para desarrollarme hasta esta etapa de la vida, ¡MUCHISIMAS GRACIAS, MAMI!, que la vida me alcance para retribuirle todo lo que me ha brindado. Gracias a mi padre, aprecio todo lo que ha hecho por apoyarme. A mis hermanos, René y Mario, por su amor incondicional, por ser mi ejemplo de perseverancia y por estar siempre presentes, brindándome los medios y herramientas para mi desarrollo académico, alentándome con su confianza y apoyo en cada paso que he dado. Por sus consejos, sin ellos no estuviera aquí. Y a mi cuñada, Isabel, por su cariño, y por estar siempre dispuesta a brindar una palabra de aliento. A Sergio, quien estuvo apoyándome, por sus palabras de ánimo cuando más las necesitaba, y por creer en mí incluso cuando yo misma dudaba.Su presencia ha significado más de lo que las palabras pueden expresar.

Agradezco a Rigoberto, Walter, Bairon, Luis, Daniel, Alfonso y Ceci, por el apoyo como compañeros en la carrera universitaria y por la amistad brindada dentro y fuera de ella, quienes hicieron de este proceso una experiencia más enriquecedora. Gracias por las ideas compartidas, las largas jornadas de estudio y el compañerismo que marcó estos años. Y todos aquellos a quienes no menciono, pero fueron parte de este proceso, mi más sincero agradecimiento.

Gracias a niña Reinita, secretaria de nuestra facultad. Agradecida con todo el apoyo brindado durante mi trayecto en la universidad, por su guía y orientación, fue una parte fundamental, le deseo mis más sinceros éxitos.

Finalmente, quiero expresar mi sincera gratitud al Ing. Werner David Meléndez Valle, por su guía, su orientación y su constante disposición durante el desarrollo de este trabajo. Su acompañamiento fue esencial para avanzar con seguridad y enfoque. Asimismo, agradezco al PhD. Carlos Osmin Pocasangre Jiménez, por sus observaciones acertadas, su exigencia académica y sus valiosos aportes, que enriquecieron significativamente este proyecto. Su compromiso y experiencia han sido una fuente de inspiración.

A cada uno de ustedes, mi más profundo agradecimiento por su invaluable contribución a este viaje académico.

Brenda Azucena Guzmán Coto

Tabla de contenido

Lista De Tablas

Lista De Figuras

1 INTRODUCCION, OBJETIVOS Y ALCANCES

1.1 Introducción

La seguridad de la información se ha convertido en una preocupación crucial para la industria empresarial, lo que lleva a un mayor enfoque en la seguridad perimetral, especialmente en un entorno global donde las amenazas cibernéticas están en constante evolución.

En El Salvador, las organizaciones se enfrentan a una serie de desafíos que complican la implementación de medidas efectivas de seguridad perimetral. Con el aumento de ciberataques, la proliferación de dispositivos IoT y el crecimiento del trabajo remoto, la necesidad de contar con una infraestructura de seguridad robusta se vuelve más urgente.

Una de las medidas que puede ayudar a mitigar estos problemas es establecer un perímetro de seguridad, con el objetivo de colocar una barrera o límite impenetrable entre una red interna y una red externa Internet, restringiendo y controlando los datos que entran y salen de la organización o empresa. La principal ventaja es que permite a los administradores centrarse en los puntos de entrada sin tener que olvidar la seguridad del resto de servidores internos de la red para protegerlos de posibles ataques invasivos.

La seguridad perimetral lógica hace referencia a la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático, la seguridad es una herramienta valiosa para cualquier negocio, lo cual conlleva a cuestionarse sobre la manera en que se puede formalizar la intención que tiene la misma en las organizaciones. En el contexto actual cuando se habla de seguridad sobre las tecnologías de la información (TI) se definen o establecen desde diversas áreas, tales como la seguridad informática, la seguridad de la información y la Ciberseguridad.

1.2 Objetivos

1.2.1 Objetivo General:

- Evaluar alternativas de sistemas de seguridad perimetral para empresas del sector eléctrico y telecomunicaciones.

1.2.2 Objetivos Específicos:

- Investigar opciones de diseños de seguridad perimetral para redes de gestión y monitoreo de empresas del sector eléctrico y telecomunicaciones.
- Desarrollar políticas de seguridad perimetral orientadas a la segregación de dispositivos y aplicaciones.
- Sugerir planes de formación en materia de ciberseguridad utilizando el sistema operativo FortiOS orientado al sector eléctrico.
- Documentar el procedimiento para gestionar, instalar y administrar el equipo que será donado al laboratorio de telemática de la Escuela de Ingeniería Eléctrica.

1.3 Alcances:

- Robustecer la seguridad perimetral en empresas del sector eléctrico y telecomunicaciones.
- Establecer reglas de seguridad granulares que permitan filtrar el tráfico hacia internet.
- Balancear tráfico entre dos o más conexiones de internet.
- Configurar el firewall como un concentrador VPN para conexiones de clientes externos.
- Configurar políticas de firewall, NAT, y control de aplicaciones.
- Implementar protocolos de seguridad en la capa de aplicación.
- Realizar la donación de un equipo FortiGate a la escuela de ingeniería eléctrica de la Universidad de El Salvador para realizar prácticas de laboratorios.
- Elaborar guías de laboratorio para el uso del dispositivo FortiGate.

2 PLANTEAMIENTO DEL PROBLEMA, JUSTIFICACION Y LISTA DE ABREVIATURAS

2.1 Planteamiento del problema

En El Salvador, las empresas se encuentran en un entorno de creciente digitalización, lo que las hace más vulnerables a amenazas cibernéticas. A pesar de la importancia crítica de la seguridad perimetral para proteger sus redes de datos, muchas organizaciones enfrentan serias deficiencias en sus estrategias de seguridad.

Los problemas más destacados incluyen:

1. *Aumento de Ciberataques*: Con el crecimiento del uso de tecnología, las empresas están experimentando un incremento en ciberataques, como ransomware y phishing, que comprometen sus datos y operaciones.
2. *Infraestructura de Seguridad Desactualizada*: Muchas organizaciones dependen de tecnologías obsoletas que no pueden manejar las amenazas contemporáneas, dejándolas expuestas a vulnerabilidades.
3. *Falta de Capacitación*: La escasa formación en ciberseguridad entre los empleados puede dar lugar a errores humanos, que a menudo son el eslabón más débil en la cadena de seguridad.
4. *Recursos Limitados*: Las PYMEs, en particular, carecen de los recursos necesarios para implementar soluciones de seguridad efectivas, lo que incrementa su exposición a riesgos.
5. *Conectividad Remota*: El auge del trabajo remoto ha generado nuevos desafíos para la seguridad, dificultando la protección de conexiones externas y dispositivos no administrados.
6. *Regulación Inadecuada:* La falta de un marco normativo claro en ciberseguridad impide que muchas empresas establezcan políticas robustas para mitigar riesgos.
7. *Complejidad de la Seguridad en la Nube:* La adopción de servicios en la nube plantea retos adicionales en la protección de datos y en la configuración segura de estos entornos.

8. *Amenazas Internas*: Las acciones intencionadas o no intencionadas de los empleados pueden comprometer la seguridad de la información, lo que plantea un riesgo considerable.

La suma de estos factores crea un panorama preocupante para la seguridad perimetral en las empresas de El Salvador, afectando no solo la integridad de sus datos, sino también su continuidad operativa y reputación en el mercado. Por lo tanto, es esencial identificar y abordar estas problemáticas para fortalecer la resiliencia cibernética en el país.

algunos sucesos específicos que han ocurrido en El Salvador en relación con problemas de seguridad perimetral:

1. Ataque de Ransomware a una Empresa de Telecomunicaciones (2021):

- Una conocida empresa de telecomunicaciones en El Salvador fue víctima de un ataque de ransomware que afectó sus operaciones durante varios días. Los atacantes cifraron datos críticos y exigieron un rescate para devolver el acceso, lo que causó una interrupción significativa en sus servicios.

2. Filtración de Datos en una Institución Financiera (2020):

- En 2020, se reportó que una entidad financiera sufrió una filtración de datos sensibles debido a una vulnerabilidad en su infraestructura de seguridad perimetral. Esto llevó a la exposición de información personal de miles de clientes, resultando en sanciones por parte de autoridades reguladoras.

3. Incidente de Phishing Masivo (2022):

- Un ataque de phishing dirigido a empleados de varias empresas locales llevó a que numerosos trabajadores ingresaran sus credenciales en sitios web falsos. Esto facilitó el acceso no autorizado a sistemas internos y compromisos de datos sensibles.

4. DDoS a un Portal de Gobierno (2021):

- Un ataque de denegación de servicio distribuido (DDoS) afectó a un portal gubernamental, causando la inactividad del sitio durante horas. Este ataque puso de manifiesto la falta de protección adecuada en la infraestructura de seguridad perimetral.

5. *Acceso No Autorizado a Sistemas de Salud (2020):*

- En el contexto de la pandemia, se reportó que sistemas de salud de varias instituciones sufrieron accesos no autorizados debido a configuraciones inadecuadas de seguridad, comprometiendo información sensible sobre pacientes.

6. Vulnerabilidades en Dispositivos IoT (2021):

- Varias empresas manufactureras reportaron incidentes relacionados con dispositivos IoT mal configurados, que permitieron a atacantes acceder a sus redes y manipular datos operativos.

Estos sucesos ilustran la vulnerabilidad de las empresas en El Salvador frente a las amenazas cibernéticas y la importancia de mejorar las estrategias de seguridad perimetral.

2.2 Justificación

La seguridad perimetral es esencial para proteger infraestructuras críticas, como las del sector eléctrico, telecomunicaciones y entidades gubernamentales, ya que estas dependen de sistemas digitales y físicos altamente sensibles. En los últimos años, varios eventos han demostrado la importancia crítica de reforzar la seguridad perimetral, por ejemplo, las filtraciones al Gobierno de El Salvador (2021): En mayo de 2021, el gobierno de El Salvador sufrió un ciberataque que expuso datos confidenciales y la más reciente, el ciberataque al ISSS (Instituto Salvadoreño del Seguro Social) (2024), el ISSS fue blanco de un ataque cibernético que comprometió información de miles de usuarios.

Estos eventos ponen en evidencia que la seguridad perimetral cibernética, es vital para proteger infraestructuras clave frente a las crecientes amenazas de ciberataques y filtraciones de información. Implementar firewalls avanzados, como FortiGate, y contar con equipos de seguridad puede marcar la diferencia en la prevención de daños a largo plazo.

2.3 Lista de abreviaturas

- **GU**I: Interfaz Gráfica de Usuario, conocida en inglés como Graphical User Interface
- **CLI:** interfaz de línea de comandos (en inglés: command-line interface, CLI)

- **LAN**: Local Área Network, que traduce Red de Área Local
- **WAN**: Wide Area Network, o sea, Red de Área Amplia
- **DMZ**: zona desmilitarizada (por su traducción del inglés, Demilitarized Zone).
- **USB**: Bus Serie Universal (Universal Serial Bus)
- **IP**: Internet Protocol
- **TFTP**: Trivial file transfer Protocol (Protocolo de transferencia de archivos trivial).
- **VLAN**: Redes de área local virtuales
- **FTP**: Protocolo de transferencia de archivos (en inglés File Transfer Protocol o FTP)
- **VDOM**: Dominio virtual.
- **OSPF**: Open Shortest Path First, "Abrir el camino más corto primero"
- **NAT**: La traducción de direcciones de red, también llamado enmascaramiento de IP o NAT (del inglés Network Address Translation)
- **SNAT**: NAT de origen
- **IP POOL**: Grupo de direcciones IP dedicadas.
- **ARP**: Address Resolution Protocol, (protocolo de resolución de direcciones)
- **DNAT**: NAT de destino.
- **DHCP**: Protocolo de configuración dinámica de host (en inglés: Dynamic Host Configuration Protocol)
- **DNS**: Sistema de nombres de dominio (Domain Name System)
- **VPN**: "Virtual Private Network" (Red privada virtual)
- **IPSec**: Internet Protocol security.
- **TRAFFIC SHAPING**: Conformado de tráfico.
- **SDWAN**: Red de área amplia definidas por software.

3 MARCO TEORICO

3.1 Antecedentes

Mantener una red corporativa sin protección y sin visibilidad pone en riesgo la integridad y la operatividad de una empresa. Por otro lado, las amenazas cibernéticas han aumentado, haciendo crucial la protección efectiva del perímetro, por esta razón surge la necesidad de tecnologías que nos permitan tener granularidad y control del tráfico en la red.

FortiGate es un firewall de próxima generación que ofrece seguridad avanzada para el sector eléctrico y de telecomunicaciones, protegiendo infraestructuras críticas con capacidades de inspección y prevención de amenazas. Su integración con otras herramientas de seguridad permite una defensa coordinada. Además, es esencial contar con un equipo de seguridad en el perímetro para asegurar tanto el control de acceso como la protección frente a amenazas cibernéticas.

Las instituciones educativas están incorporando tecnologías avanzadas como FortiGate en sus programas para proporcionar a los estudiantes experiencia práctica y prepararlos para el mercado laboral. Actualmente en la escuela de ingeniería eléctrica de la Universidad de El Salvador no se cuenta con este tipo de equipos para realizar estas prácticas de laboratorio. La donación de equipos tecnológicos a instituciones académicas mejora la formación práctica de los estudiantes y fomenta la colaboración entre la industria y la educación.

3.2 Comparación de Firewalls

Como parte del trabajo de graduación, se realizó un estudio comparativo de firewalls con el objetivo de seleccionar el equipo más adecuado para desarrollar las guías prácticas de laboratorio. A continuación, se presenta una tabla comparativa entre el FortiGate 60F y otros firewalls de marcas reconocidas en el mercado. La comparación considera aspectos clave como el throughput de firewall, throughput con inspección profunda de paquetes (DPI), throughput SSL, capacidad de usuarios y costos estimados.

Marca/Modelo	Throughput (Firewall)	Throughput con DPI	Throughput SSL	Usuarios recomendados	Costo aproximado
FortiGate 60F	10 Gbps	1 Gbps	750 Mbps	50-100	$600 - $1,000
Cisco Meraki MX68	450 Mbps	No especificado	No especificado	50-100	$700 - $1,200
Palo Alto PA-220	580 Mbps	560 Mbps	500 Mbps	50-75	$800 - $1,500
Sophos XGS 87	7 Gbps	1 Gbps	850 Mbps	25-50	$500 - $900
Check Point 1530	2 Gbps	450 Mbps	250 Mbps	50-100	$1,000 - $1,500

Tabla 3.2-1: Comparación entre firewalls de marcas reconocidas.

Soluciones de Software Libre

En el mercado de firewalls, no solo existen soluciones comerciales como FortiGate, Cisco, Palo Alto y otros, sino que también hay opciones de software libre que pueden ser una alternativa atractiva, especialmente en entornos de laboratorio y educativos debido a su costo reducido y flexibilidad. Algunas de las soluciones de firewall de software libre más conocidas son:

- *pfSense:* Es una plataforma de firewall de código abierto basada en FreeBSD. pfSense es ampliamente utilizado en redes pequeñas y medianas, y ofrece características avanzadas como VPN, IPSec, NAT, filtrado de contenido y balanceo de carga. Además, permite una configuración flexible y es ideal para entornos educativos donde los estudiantes pueden aprender sobre redes y seguridad sin los costos asociados a soluciones comerciales.
- *IPFire:* Otro firewall de código abierto basado en Linux. IPFire es conocido por su facilidad de uso, incluso en redes complejas. Ofrece protección contra amenazas externas, control de acceso, monitoreo de tráfico, y también es compatible con tecnologías como VPN y IPSec. Es una excelente opción para entornos de laboratorio que necesitan una solución económica pero robusta.

- *Untangle NG Firewall:* Aunque tiene una versión comercial, Untangle también ofrece una edición gratuita con características como filtrado de contenido, VPN, anti-virus y protección contra malware. Es particularmente útil en pequeñas redes o como punto de partida para estudiantes que están aprendiendo sobre administración de redes.
- *Smoothwall Express:* Este firewall de código abierto ofrece una solución de seguridad para pequeñas redes y es muy accesible para quienes están comenzando a aprender sobre seguridad informática. Es fácil de instalar y administrar, y tiene opciones de filtrado y control de acceso a la red.

Aunque las soluciones de software libre pueden no ofrecer el mismo nivel de soporte o las características avanzadas de los firewalls comerciales, son una excelente opción para prácticas educativas y pruebas en entornos controlados. Ofrecen una buena oportunidad para que los estudiantes comprendan los principios de funcionamiento de un firewall y aprendan a configurarlos sin tener que invertir en hardware costoso.

Selección del FortiGate 60F para el Laboratorio

Para el desarrollo de las guías prácticas de laboratorio, se adquirió el **FortiGate 60F**, ya que cumple con los requisitos necesarios para un entorno educativo. Algunos de los factores que se tomaron en cuenta para su adquisición son:

- **Facilidad de uso y configuración**, lo que permite a los estudiantes familiarizarse con el manejo de firewalls de próxima generación (NGFW).
- **Capacidad de procesamiento adecuada**, ya que su throughput de firewall de 10 Gbps y throughput con inspección DPI de 1 Gbps garantizan un rendimiento óptimo en el laboratorio.
- **Compatibilidad con escenarios de aprendizaje**, incluyendo filtrado de contenido, VPN, inspección SSL y control de aplicaciones.
- **Costo accesible en comparación con otros modelos similares**, asegurando una buena relación calidad-precio dentro del presupuesto del proyecto.

El FortiGate 60F fue elegido para que los estudiantes puedan desarrollar guías prácticas y adquirir experiencia en la administración y configuración de firewalls. Su implementación permite simular escenarios reales de seguridad perimetral, facilitando la comprensión de conceptos clave en la protección de redes corporativas.

3.3 Seguridad Perimetral en Redes

La seguridad perimetral es un conjunto de medidas y tecnologías diseñadas para proteger los límites de una red corporativa de accesos no autorizados y ataques cibernéticos. Estas soluciones incluyen firewalls, sistemas de detección y prevención de intrusiones (IDS/IPS), segmentación de redes y autenticación multifactorial (MFA). Su objetivo principal es monitorear, filtrar y controlar el tráfico de red para prevenir amenazas y garantizar la integridad de la información (Pfleeger & Pfleeger, 2012).

3.3.1 Principales Amenazas a la Seguridad Perimetral

Las organizaciones del sector eléctrico y de telecomunicaciones están expuestas a diversas amenazas cibernéticas, que incluyen:

Ataques de denegación de servicio (DDoS): Buscan sobrecargar los servidores con tráfico malicioso, lo que provoca la interrupción de los servicios esenciales.

Ransomware: Secuestra datos críticos a cambio de un rescate, afectando principalmente a infraestructuras críticas en sectores como el eléctrico (Symantec, 2020).

Phishing: Obtención fraudulenta de credenciales mediante engaños, especialmente dirigido a empleados que tienen acceso a sistemas sensibles (Fruhlinger, 2019).

Exfiltración de datos: Robo de información sensible mediante accesos no autorizados, lo cual pone en riesgo la confidencialidad de la información estratégica de las empresas (Mogull, 2021).

3.4 Tecnologías de Seguridad Perimetral

La implementación efectiva de tecnologías de seguridad perimetral es crucial para proteger las infraestructuras críticas. Algunas de las tecnologías más relevantes incluyen:

Firewalls de próxima generación (NGFW): Estos dispositivos realizan inspección profunda de paquetes (DPI) y control de aplicaciones, lo que permite filtrar tráfico de forma más eficaz que los firewalls tradicionales (Fortinet, 2020).

Sistemas IDS/IPS: Los sistemas de detección y prevención de intrusiones permiten identificar y bloquear actividades sospechosas en la red, reduciendo los riesgos de intrusiones externas (Kim & Kankanhalli, 2014).

VPNs y Cifrado: Garantizan la transmisión segura de datos entre usuarios remotos y la red corporativa, protegiendo la información durante su transmisión (Chauhan & Bedi, 2015).

SD-WAN: Optimiza el tráfico de red y mejora la seguridad en conexiones entre sucursales de empresas distribuidas, una necesidad clave en sectores como telecomunicaciones (Sundararajan & Raj, 2017).

3.5 Desafíos Específicos del Sector Eléctrico y de Telecomunicaciones

Las empresas del sector eléctrico y telecomunicaciones enfrentan varios desafíos únicos relacionados con la seguridad perimetral, como:

Infraestructuras críticas: Las redes eléctricas y de telecomunicaciones son esenciales para el funcionamiento de la sociedad, y cualquier interrupción puede tener consecuencias devastadoras. Esto requiere una protección constante contra amenazas avanzadas (Burns, 2019).

Conectividad remota: Las empresas necesitan ofrecer acceso remoto a los empleados y socios, lo que incrementa la superficie de ataque. Las soluciones de VPN y SD-WAN ayudan a mitigar este riesgo, pero también requieren un monitoreo continuo para evitar vulnerabilidades (Zhou et al., 2018).

Cumplimiento regulatorio: Las empresas deben cumplir con estrictas normativas de ciberseguridad, como las regulaciones de la NERC CIP para el sector eléctrico, que exigen medidas adicionales de protección (U.S. Department of Energy, 2020).

Evolución de las amenazas: Las amenazas están en constante cambio, y las empresas deben adaptarse a nuevas tácticas utilizadas por los atacantes, como el ransomware dirigido a infraestructuras de control industrial (Brown et al., 2020).

3.6 Modelos de Seguridad Perimetral en Empresas del Sector Eléctrico y Telecomunicaciones

Existen varios modelos de seguridad perimetral que son aplicables específicamente a las empresas de estos sectores:

Defensa en profundidad: Este modelo establece múltiples capas de defensa (firewalls, IDS/IPS, control de acceso) para garantizar que, aunque una capa sea vulnerada, otras seguirán protegiendo la red (Shostack, 2014).

Zero Trust (Confianza Cero): Basado en el principio de que "nunca se debe confiar en nada ni nadie dentro o fuera de la red", este modelo requiere verificación continua para todos los usuarios y dispositivos (Kindervag, 2010).

3.7 Implementación de Firewalls en Centrales de Generación Eléctrica

Las centrales de generación eléctrica modernas están altamente automatizadas y dependen de sistemas SCADA (Supervisory Control and Data Acquisition) para la supervisión y control remoto de sus procesos. Sin una adecuada protección perimetral, estos sistemas pueden ser vulnerables a diversos ataques cibernéticos, lo que representa un riesgo crítico para la infraestructura eléctrica.

Riesgos sin un firewall en una central eléctrica

- Acceso no autorizado a los sistemas de control.
- Interrupción del servicio mediante ataques de denegación de servicio (DoS).
- Manipulación de datos de sensores y actuadores.
- Inyección de malware o ransomware en la red operativa.

Implementación de un firewall para protección

- *Segmentación de la red:* Separar la red operativa (OT) de la red corporativa (IT) mediante un firewall de próxima generación (NGFW).
- *Inspección profunda de paquetes (DPI):* Identificar y bloquear tráfico malicioso que intente acceder a los sistemas SCADA.
- *VPN segura:* Garantizar que los operadores remotos accedan a la red de manera segura.
- *Control de aplicaciones:* Restringir el tráfico solo a protocolos y servicios autorizados, reduciendo la superficie de ataque.

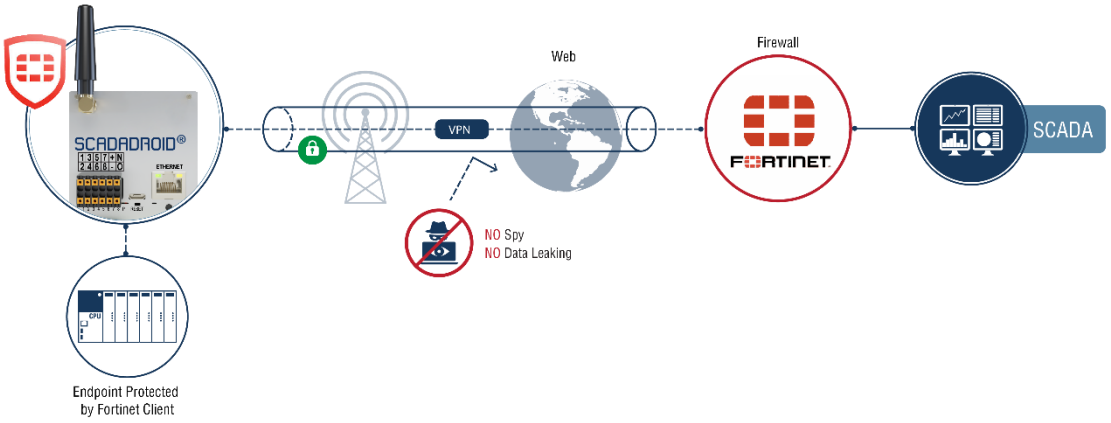


Figura 3.7-1: Esquema de conexión a un sistema SCADA mediante VPN

La implementación de un firewall como el FortiGate 60F en una central eléctrica permite proteger los sistemas críticos contra amenazas cibernéticas, asegurando la continuidad operativa y la seguridad de la infraestructura energética.

Normas y Estándares de Seguridad en Infraestructuras Críticas y Sectores Tecnológicos

La implementación de firewalls en una central de generación eléctrica, así como en otras empresas del sector eléctrico y de telecomunicaciones, debe cumplir con diversas normativas y estándares de seguridad que buscan garantizar la protección de los sistemas críticos. Estas normativas no solo se aplican a las infraestructuras de generación de energía, sino también a las redes de telecomunicaciones y otras instalaciones tecnológicas esenciales. Algunas de las normativas más relevantes incluyen:

- *NIST SP 800-82:* Guía sobre seguridad en sistemas de control industrial. El NIST proporciona directrices para la protección de redes industriales, incluidas las redes de control de infraestructura energética y telecomunicaciones.
- *IEC 62443*: Estándar internacional para la seguridad cibernética en redes industriales. La IEC 62443 establece requisitos y mejores prácticas para proteger las redes de control industrial de amenazas externas y internas. Su aplicación es crucial tanto en el sector eléctrico como en telecomunicaciones, donde la disponibilidad de los sistemas es esencial.

- *ISO/IEC 27001:* Norma de gestión de seguridad de la información, que establece los requisitos para la implementación de un sistema de gestión de seguridad de la información (SGSI) en organizaciones, incluyendo aquellas que operan en sectores críticos como la generación de energía y telecomunicaciones.
- *NERC CIP:* Conjunto de normas del *North American Electric Reliability Corporation* que establece los requisitos de ciberseguridad para las infraestructuras críticas del sector energético en América del Norte, y que son de vital importancia también en las redes de telecomunicaciones que soportan los servicios de comunicación críticos.

Cumplir con estos estándares y normativas es esencial para garantizar la seguridad, disponibilidad e integridad de las infraestructuras críticas en las centrales de generación eléctrica, así como en las redes de telecomunicaciones y otras empresas del sector tecnológico.

3.8 Tendencias y Tecnologías Emergentes en Seguridad Perimetral

A medida que las amenazas evolucionan, las tecnologías de seguridad también avanzan. Algunas de las tendencias emergentes incluyen:

Inteligencia artificial (IA) y machine learning (ML): Estas tecnologías están ayudando a identificar patrones inusuales y amenazas avanzadas más rápidamente que las soluciones tradicionales basadas en firmas (Raman, 2020).

Seguridad en la nube: A medida que las empresas adoptan soluciones en la nube, se hace necesario implementar firewalls adaptados a este entorno, como los firewalls de próxima generación (NGFW) en la nube (Panda et al., 2020)

Automatización de la seguridad: Las herramientas de SIEM y SOAR permiten la automatización del monitoreo de seguridad y la respuesta ante incidentes, optimizando los tiempos de respuesta y mejorando la capacidad de detección de amenazas (Garcia & Martin, 2021).

3.9 Beneficios de la Implementación de Seguridad Perimetral en Empresas del Sector Eléctrico y Telecomunicaciones

Los beneficios más destacados de implementar una estrategia robusta de seguridad perimetral en estos sectores incluyen:

Reducción de vulnerabilidades: A través de la segmentación de la red y el control de acceso, las empresas protegen sus infraestructuras críticas y datos sensibles, reduciendo las posibilidades de ataques exitosos (Kaspersky, 2020).

Mejora en la visibilidad y monitoreo continuo: La implementación de tecnologías de monitoreo ayuda a detectar actividades sospechosas en tiempo real, lo que mejora la capacidad de respuesta ante incidentes (Pfleeger & Pfleeger, 2012).

Cumplimiento normativo: Adoptar estándares como ISO 27001 o NIST Cybersecurity Framework asegura que las empresas cumplen con las regulaciones y protegen sus datos de acuerdo con las mejores prácticas del sector (NIST, 2020).

4 METODOLOGIA Y DESARROLLO

4.1 Metodología de Investigación

El enfoque de la investigación es cualitativo y pedagógico, con el objetivo de desarrollar guías prácticas que se presentarán a los estudiantes en un futuro cercano. Estas guías están diseñadas para que los estudiantes las desarrollen en un entorno de laboratorio, con el fin de aprender a implementar y gestionar soluciones de seguridad perimetral. A través de estas guías, los estudiantes adquirirán habilidades prácticas esenciales para enfrentar desafíos de seguridad en redes, especialmente en empresas del sector eléctrico y telecomunicaciones.

La metodología adoptada incluyó:

Revisión bibliográfica y técnica: Se recopiló información relevante sobre las mejores prácticas en seguridad perimetral y las características de dispositivos como el FortiGate 60F, con el fin de fundamentar la creación de las guías prácticas.

Desarrollo de guías prácticas: Las guías están orientadas a que los estudiantes implementen soluciones de seguridad perimetral, tales como la configuración de firewalls, segmentación de redes y establecimiento de políticas de acceso, sin necesidad de realizar simulaciones de ataques.

4.2 Implementación del Sistema de Seguridad Perimetral

La implementación de las soluciones de seguridad perimetral se guiará mediante las guías prácticas, que los estudiantes recibirán para ser desarrolladas en un entorno de laboratorio. Estas guías cubrirán los aspectos clave de la configuración y gestión de un sistema de

seguridad, y se adaptarán a las necesidades específicas de las redes de empresas en los sectores eléctrico y de telecomunicaciones.

4.2.1 Configuración del Firewall FortiGate 60F

Las guías proporcionarán un conjunto detallado de instrucciones para que los estudiantes configuren el FortiGate 60F de acuerdo con las mejores prácticas en seguridad perimetral, incluyendo:

Conexión inicial y configuración básica: Los estudiantes aprenderán a realizar la configuración básica del dispositivo, como la configuración de interfaces de red y credenciales, para garantizar una instalación segura.

Segmentación de red mediante VLANs: A través de las guías, los estudiantes aprenderán a crear VLANs para segmentar redes y controlar el tráfico entre diferentes segmentos, lo cual es crucial para proteger la red de accesos no autorizados.

Políticas de acceso: Se les enseñará a crear políticas de firewall para gestionar el tráfico entre distintas redes y controlar los accesos según reglas predefinidas, optimizando la seguridad perimetral.

Implementación de VPNs seguras: Los estudiantes configurarán VPNs para habilitar el acceso remoto seguro, aprendiendo a proteger la comunicación entre usuarios y redes corporativas.

Monitoreo y gestión de incidentes: Las guías también incluirán instrucciones sobre cómo utilizar herramientas de monitoreo y generación de alertas para que los estudiantes puedan detectar y responder a incidentes de seguridad en tiempo real.

4.2.2 Evaluación de Desempeño

Aunque no se realizarán simulaciones de ataques, los estudiantes evaluarán el desempeño del sistema de seguridad que implementen en el laboratorio, midiendo aspectos como:

Latencia y rendimiento: A través de las guías, los estudiantes evaluarán el impacto de las políticas de seguridad en el rendimiento de la red, midiendo la latencia antes y después de la implementación de las medidas de seguridad.

Capacidad de gestión de tráfico: Los estudiantes verificarán cómo el FortiGate 60F puede gestionar grandes volúmenes de tráfico mientras mantiene un nivel adecuado de seguridad.

Estabilidad de servicios críticos: Los estudiantes también examinarán la estabilidad de los servicios, asegurando que las políticas de seguridad no afecten la disponibilidad de servicios esenciales para el funcionamiento de la red.

4.3 Evaluación de Resultados

La evaluación de los resultados se centrará en la aplicación práctica de las guías por parte de los estudiantes. Se espera que los estudiantes sean capaces de:

Implementar soluciones efectivas de seguridad: Utilizando las guías, los estudiantes deberán ser capaces de implementar medidas de seguridad perimetral eficaces, como la segmentación de redes y la protección de datos sensibles.

Evaluar el impacto en la red: Los estudiantes deberán ser capaces de analizar cómo las soluciones implementadas afectan al rendimiento de la red y encontrar un equilibrio entre seguridad y eficiencia operativa.

Gestionar incidentes de seguridad: Los estudiantes aprenderán a gestionar incidentes de seguridad utilizando las herramientas proporcionadas por el FortiGate 60F, evaluando su capacidad para detectar amenazas y responder a ellas de manera oportuna.

4.4 Beneficios y Limitaciones de la Implementación

4.4.1 Beneficios

Las guías prácticas que se presentarán a los estudiantes ofrecerán múltiples beneficios.

Aprendizaje experiencial: Los estudiantes tendrán la oportunidad de aplicar los conceptos aprendidos en un entorno realista de laboratorio, lo que les proporcionará una experiencia práctica valiosa.

Desarrollo de habilidades prácticas: Los estudiantes adquirirán habilidades directamente aplicables en la industria, como la configuración de firewalls, la segmentación de redes y la gestión de VPNs.

Comprensión de la seguridad en redes críticas: Al trabajar con las guías, los estudiantes comprenderán cómo implementar soluciones de seguridad efectivas en infraestructuras críticas, como las redes de telecomunicaciones y las redes eléctricas.

4.4.2 Limitaciones

Algunas de las limitaciones que podrían surgir con las guías prácticas incluyen:

Tiempo necesario para dominar los conceptos: Aunque las guías son detalladas, los estudiantes pueden necesitar tiempo adicional para comprender completamente las configuraciones y las prácticas recomendadas en seguridad perimetral.

Escalabilidad en escenarios reales: Las guías están diseñadas para un entorno de laboratorio controlado, lo que podría presentar desafíos al momento de implementarlas en un entorno empresarial real con infraestructuras más complejas.

4.5 Recomendaciones para Futuras Implementaciones

Con base en los resultados obtenidos de la implementación de estas guías prácticas en el laboratorio, se recomienda lo siguiente:

Capacitación continua para los estudiantes: Las guías deben acompañarse de materiales educativos adicionales y sesiones de capacitación para que los estudiantes puedan continuar desarrollando sus habilidades en seguridad perimetral.

Actualización periódica de las guías: Las guías deben revisarse y actualizarse de manera regular para incluir los avances más recientes en tecnologías de seguridad y en los marcos de trabajo utilizados por la industria.

Ampliación de escenarios de laboratorio: Se recomienda desarrollar escenarios de laboratorio más complejos que imiten de forma más precisa los entornos reales de las empresas del sector eléctrico y telecomunicaciones.

5 DESARROLLO DE PRACTICAS DE LABORATORIO UTILIZANDO EL FORTIGATE 60F

5.1 Práctica 1: Primeros pasos de administración de un FortiGate.

Introducción

En la presente práctica se explicarán los primeros pasos para conectarnos a un equipo de seguridad del fabricante Fortinet modelo FortiGate 60F usando una conexión por consola. También se explicará cómo gestionar el equipo vía GUI desde la dirección IP por defecto en su puerto de gestión.

Objetivo general

- Detallar el proceso de administración por consola y web del dispositivo de seguridad.

Objetivos específicos

- Administrar el Fortigate 60F desde su puerto consola.
- Autenticarnos en el dispositivo usando las credenciales por defecto.
- Gestionar el equipo vía web por su dirección IP de gestión.
- Realizar el cambio de la contraseña por defecto.

Desarrollo

El FortiGate 60F es un dispositivo compacto de seguridad de red de la serie FortiGate, diseñado para pequeñas y medianas empresas.

- Dimensiones:
  - Ancho: 216 mm (8.5 pulgadas)
  - Profundidad: 160 mm (6.3 pulgadas)
  - Altura: 40 mm (1.6 pulgadas)
- Peso:
  - Aprox. 1.2 kg (2.6 libras)
- Puertos:
  - 5 puertos GE RJ45 (10/100/1000 Mbps) para red local (LAN)
  - 2 puertos WAN GE RJ45 (10/100/1000 Mbps) para conexiones de red de área amplia (WAN)
  - 1 puerto DMZ GE RJ45
  - 1 puerto de consola (RJ45)
  - 1 puerto USB
- Alimentación:
  - Entrada de alimentación: 12V DC
  - Consumo: alrededor de 18 W máximo
- Montaje:
  - Es un dispositivo de escritorio, aunque también puede ser montado en rack con el kit adecuado.
- Indicadores LED:
  - Tiene luces LED en el panel frontal para indicar el estado de energía, actividad de red y el estado de los puertos.

El FortiGate 60F es conocido por su pequeño tamaño y eficiencia, ideal para implementar seguridad avanzada en redes de oficinas con espacio limitado.

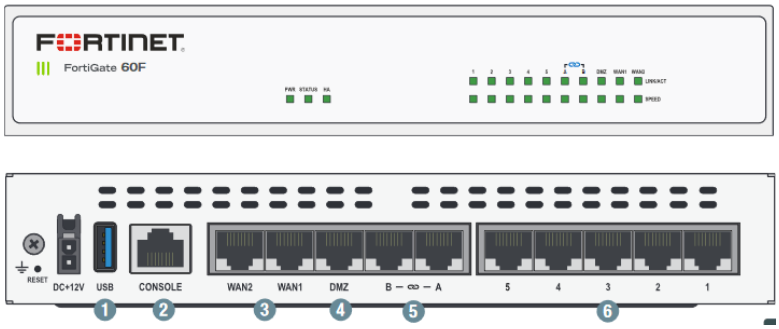


Figura 5.1-1 Detalle de puertos de FortiGate 60F.

1. Primeros pasos de administración.

1.1 Diagrama

En la Figura 5.1-2 se presenta una ilustración de cómo se realiza una conexión física por cable consola

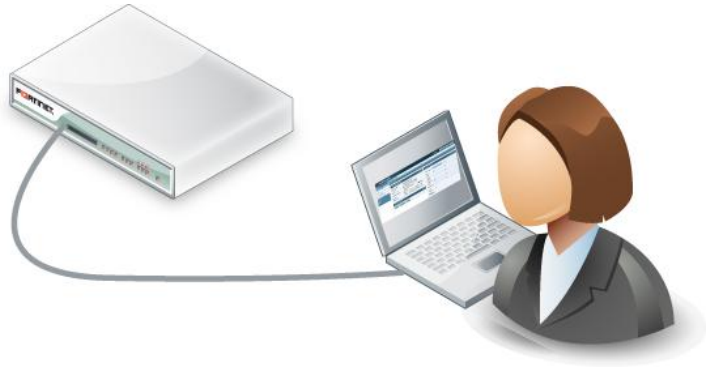


Figura 5.1-2: Conexión por cable consola.

1.2 Conexión por consola.

Figura 5.1-3: Cable consola

Paso 1: Lo primero que haremos es identificar el cable consola, estos cables son como se muestra en la Figura 5.1-3, este modelo ya nos permite la conexión directa USB-Consola sin necesidad de adaptador.

Paso 2: Lo siguiente es descargar un software para realizar nuestra conexión, todas las practicas se realizarán usando el software Putty[1] que es gratuito y no necesita instalación, pero también existen otros softwares con más características como Secure CRT, MobaXterm, Hyperterminal entre otros.

Ejecutamos Putty y nos saldrán las opciones que se muestran en la Figura 5.1-4.

[1] Este software se descargar desde el sitio oficial https://www.putty.org/

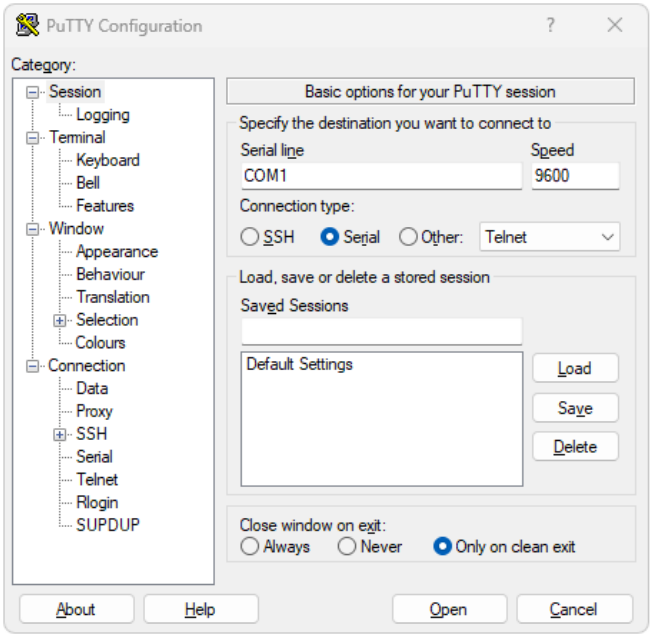


Figura 5.1-4 :Opciones de Putty.

Paso 3: Seleccionamos la opción “Serial” en la parte de Connetion type.

Paso 4: Para saber cuál COM nos ha asignado la computadora nos vamos al Device Manager[2] de Windows y buscamos las conexiones Ports (COM & LPT)[3].

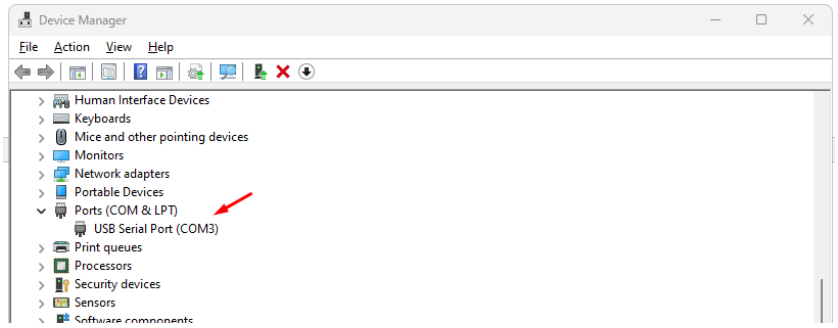


Figura 5.1-5: Ubicación de conexiones COM.

Paso 5: Una vez colocamos el COM3 (para nuestro caso) y hacemos click en “Open” se debe abrir el siguiente Consola (si no aparece nada dar ENTER).

[2] Para abrir el **Device Manager** basta con escribir *device manager* en la barra de búsqueda de Windows.
[3] Si no nos aparece ningún COM en esta parte significa que la maquina no está reconociendo el cable o que se necesita un controlador.

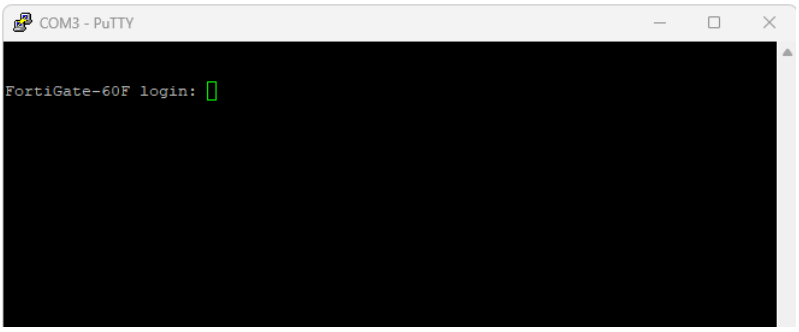


Figura 5.1-6: Conexión por Consola al Fortigate 60F.

La conexión por consola fue completada, si queremos ingresar al equipo las credenciales son.

User: admin

Password: <sin password>

Nota: Cuando ingresemos por primera vez nos pedirá cambio de contraseña.

1.3 Conexión por GUI

Paso 1: Conectarse por cable de red a cualquiera de los puertos 1-5 del Fortigate 60F, -por defecto- este modelo de Firewall trae un *bridge*[4] en esos puertos con la dirección IP[5] 192.168.1.99/24.

Paso 2: Configurar una dirección IP estática[6] en la computadora en el segmento de red 192.168.1.0/24, note que la IP 192.168.1.99 ya está usada por el FortiGate por cual no se debe configurar en la máquina.

---

[4] Similar a un *switch*

[5] Para los FortiGate que tienen puerto de *management* dedicado la dirección de gestión viene configurada en ese Puerto.

[6] Configurar una IP estática es parte de los conocimientos previos que se deben tener antes de la práctica.

[7] Notar que en la configuración de la IP no se estableció *gateway* esto debido a que ambas IP están en el mismo dominio de broadcast.

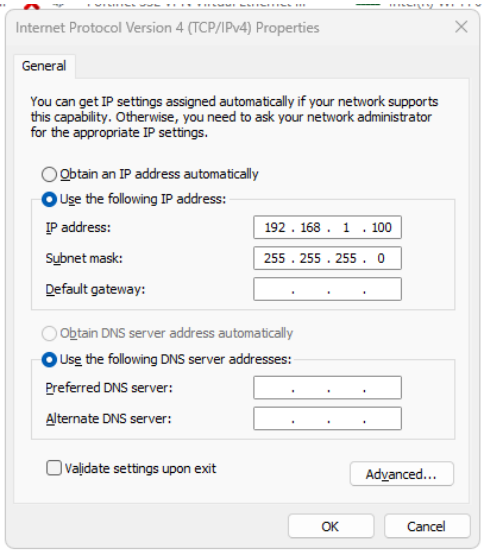


Figura 5.1-7: Dirección IP estática configurada en Windows.

Paso 3: Cargar el portal del firewall https://192.168.1.99/ si nos sale alerta de certificado debemos darle click en opciones avanzadas y aceptar el riesgo y continuar, esta alerta sale debido a que el firewall usa un certificado auto firmado que no es público por lo tanto el navegador no confía en él.

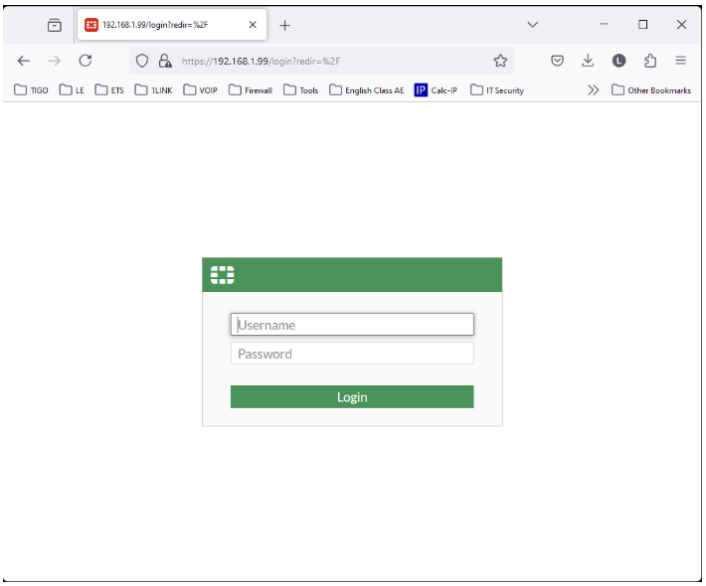


Figura 5.1-8: Portal de login del firewall.

La conexión por GUI fue completada, si queremos ingresar al equipo las credenciales son:

User: admin

Password: <sin password>

Nota: Cuando ingresemos por primera vez nos pedirá cambio de contraseña.

1.4 Autenticación y configuración IP en puerto.

Paso 1: Autenticarnos en el firewall usando las credenciales por defecto.

Realizar el cambio por siguientes credenciales[7]:

User: admin

Password: admin

Cuando hagamos el cambio nos volverá a cargar el portal de login para ingresar las nuevas credenciales.

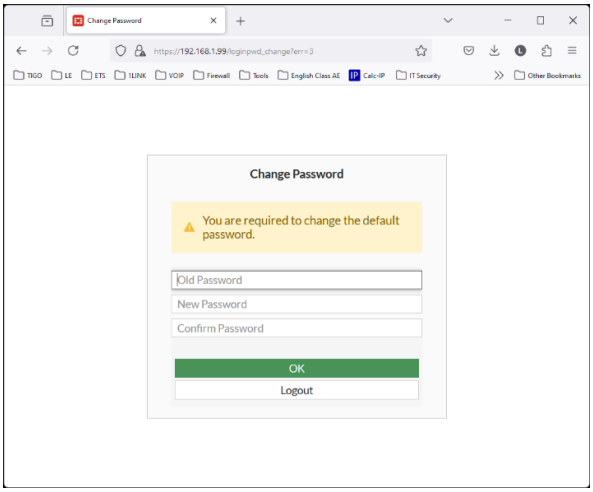


Figura 5.1-9: Solicitud de cambio de password.

Paso 2: Una vez dentro del firewall podemos realizar configuraciones como las siguientes:

- Para establecer una dirección IP en una interface ir a ***Network > Interfaces.***

[8] Se ha dejado de contraseña admin solo para fines didácticos, a nivel operativo en cualquier equipo nunca se deben utilizar este tipo de contraseñas inseguras y fáciles de descifrar.

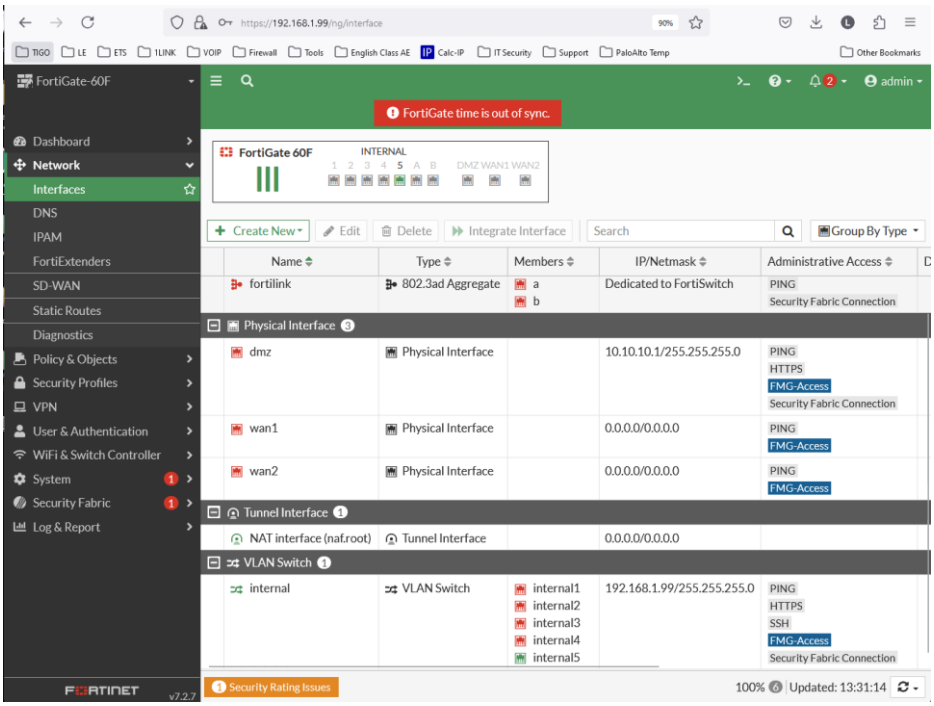


Figura 5.1-10: Menú de interfaces del firewall.

- Entrar al puerto *wan1* y establecer la dirección IP 10.200.10.1/24, para eso se deberá dar doble click sobre *wan1* o seleccionarla y a continuación edit.

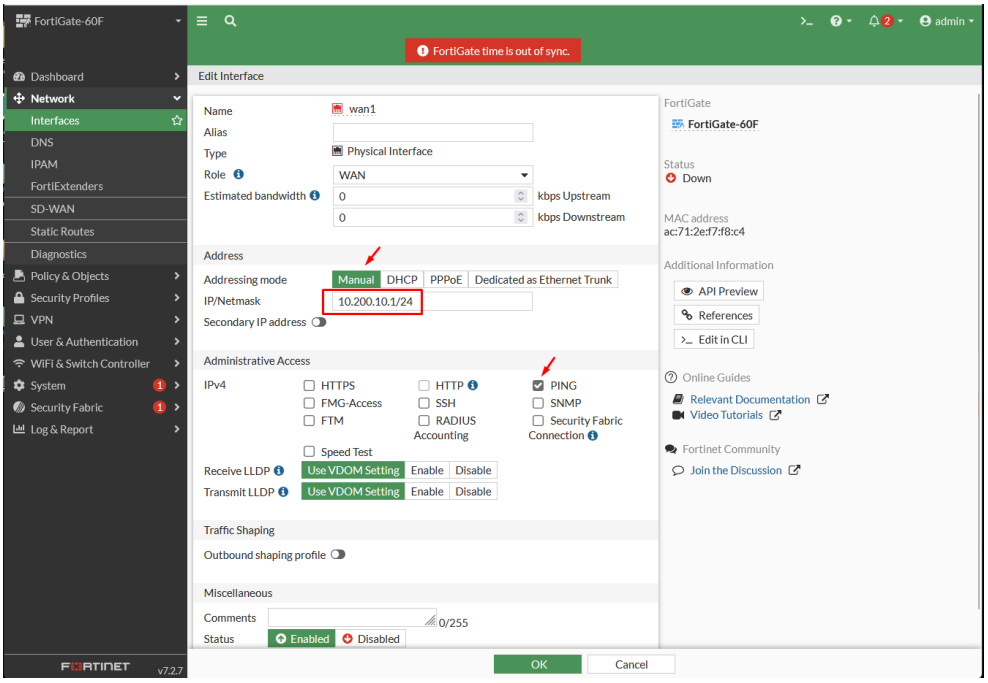


Figura 5.1-11:Estableciendo una dirección IP en un puerto.

Conclusiones

- La administración del Fortigate 60F se puede realizar mediante conexión por consola y GUI siempre que se cuente con los cables correctos.
- Para administrar el firewall por consola implica tener conocimientos de la CLI del equipo.
- La contraseña por defecto del equipo solo se utiliza la primera vez.
- La gestión vía Web del FortiGate es más intuitiva que cuando se realiza vía CLI.

5.2 Práctica 2: Actualización del sistema operativo FortiOS.

Introducción

En la presente practica se explica el proceso para actualizar el sistema operativo de un firewall específicamente del FortiGate 60F.

Objetivo general

- Actualizar el sistema operativo del FortiGate 60F

Objetivos específicos

- Monitorear el proceso de actualización.
- Descargar las versiones de sistema operativo disponibles para el FortiGate 60F.

Desarrollo:

Los sistemas operativos[8] para los FortiGate se ordenan de la siguiente manera:

FortiGate / v5.00		
5.0.0	*Hasta*	*5.0.14*
5.2.0	*Hasta*	*5.2.15*
5.4.0	*Hasta*	*5.4.13*
5.6.0	*Hasta*	*5.6.14*

Tabla 5.2-1: Versiones de FortiOS 5.x.x

FortiGate / v6.00		
6.0.0	Hasta	6.0.18
6.2.0	Hasta	6.2.16
6.4.0	Hasta	6.4.15

Tabla 5.2-2: Versiones de FortiOS 6.x.x

FortiGate / v7.00

[8] Hay sistemas operativos antes de estos en las versiones 2.0.0, 3.0.0 y 4.0.0 pero estos ya son muy antiguos

7.0.0	Hasta	7.0.16
7.2.0	Hasta	7.2.10
7.4.0	Hasta	7.4.5
7.6.0		

Tabla 5.2-3: Versiones de FortiOS 7.x.x

Muy pocos dispositivos aún están en versiones 5.x.x o 6.x.x por ser versiones viejas, por lo que nos enfocaremos en las versiones 7.x.x que son las versiones que actualmente tienen desarrollo.

Paso 1: Autenticarse en el firewall vía GUI, de la práctica 1 cambiamos la contraseña por defecto.

User: admin

Password: admin[9]

Si es la primera vez que ingresamos al equipo por defecto no se tiene contraseña configurada.

Paso 2: Revisar la versión actual del firewall y ubicarla en las tablas que se presentaron de las versiones de los equipos. *Dashboard > Status*

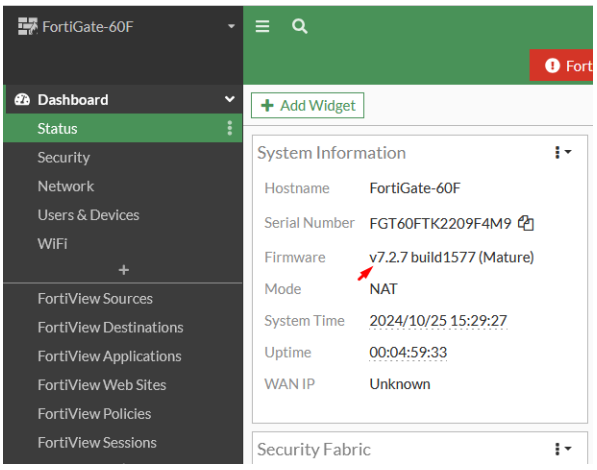


Figura 5.2-1: Versión del sistema operativo de dispositivo FortiGate.

Paso 3: Realizar la actualización[10] para esto nos debemos mover en el siguiente menú, como se muestra en la figura 5.2-2.

[9] Por defecto el firewall no tiene contraseña, pero la primera vez que nos autenticamos nos pide que le establezcamos una.

[10] Si el dispositivo tiene conexión a internet se puede realizar la actualización descargando directamente de internet.

System > Fabric Management > Upgrade

Seleccionamos el dispositivo y damos click en *Upgrade* se nos desplegará un nuevo menú en el cual nos vamos a la pestaña *File Upload* como se muestra en la figura 5.2-3.

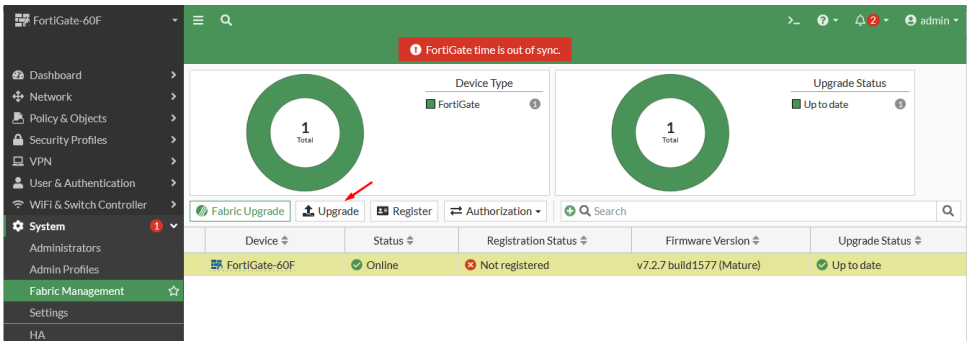


Figura 5.2-2: Menú para actualizar el FortiOS.

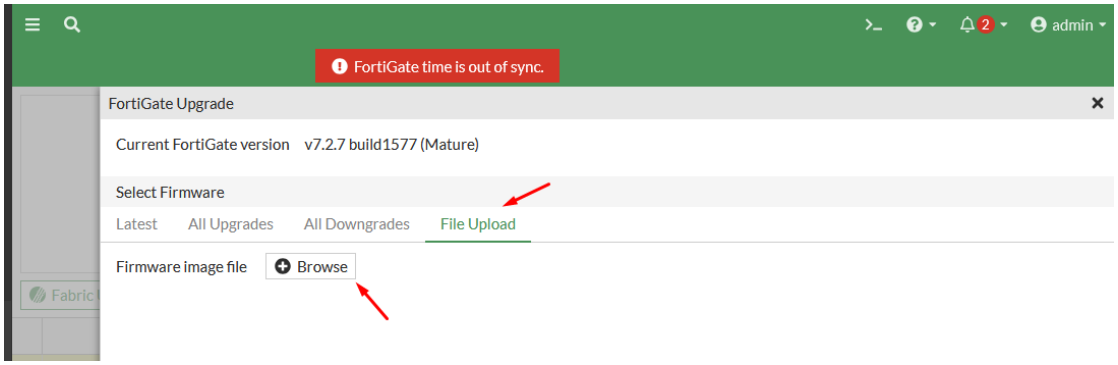


Figura 5.2-3: Menú para subir el sistema operativo.

Paso 4: Navegar en el directorio para ubicar el firmware, para este caso le subiremos la versión 7.2.8 previamente descargada[11].

[11] El proceso se descarga del firmware no se explica ya que se necesita tener un equipo registrado con el fabricante para poder tener acceso al portal de Soporte, pero todos los sistemas operativos hasta la fecha serán entregados digitalmente al laboratorio de Telemática de la EIE.

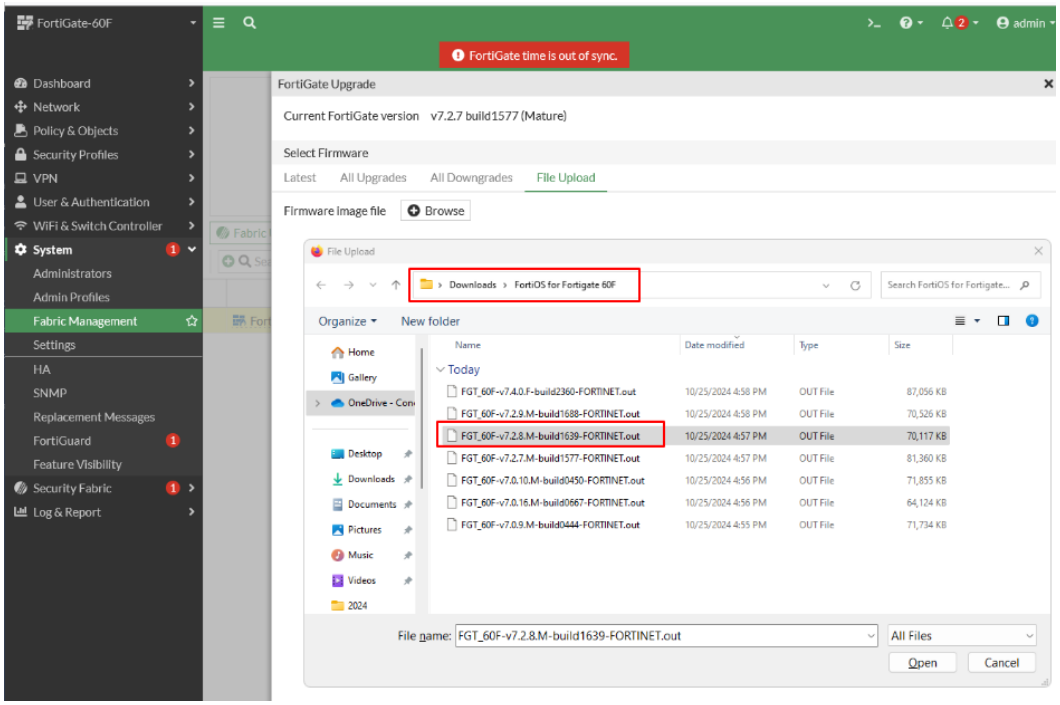


Figura 5.2-4: Menú para seleccionar el firmware que cargaremos.

Paso 5: Cargar el sistema operativo y realizar respaldo de configuraciones.

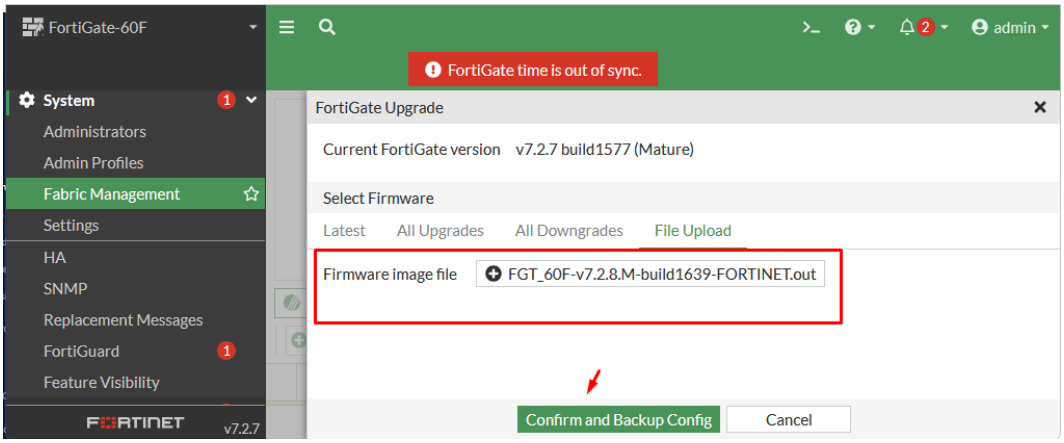


Figura 5.2-5: Menú para iniciar la carga del archivo.

Nos saldrá el siguiente mensaje que nos advierte que el dispositivo se reiniciará al finalizar el proceso, damos click en *Continue.*

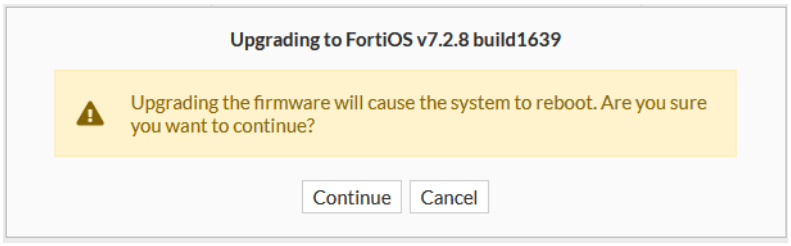


Figura 5.2-6: Mensaje de advertencia.

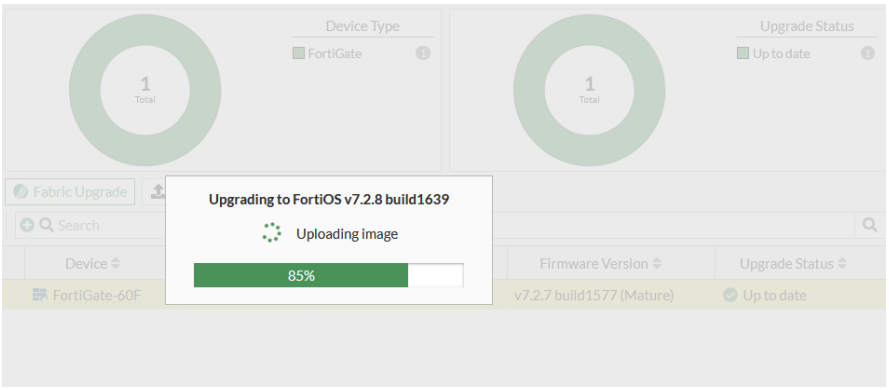


Figura 5.2-7:Proceso de carga del sistema operativo.

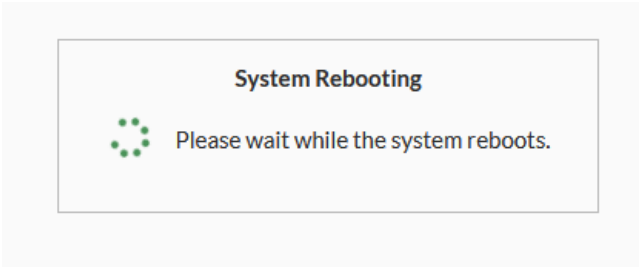


Figura 5.2-8: Proceso de reinicio del dispositivo.

Paso 6: *Nos autenticamos nuevamente en el Firewall y revisamos la versión.*

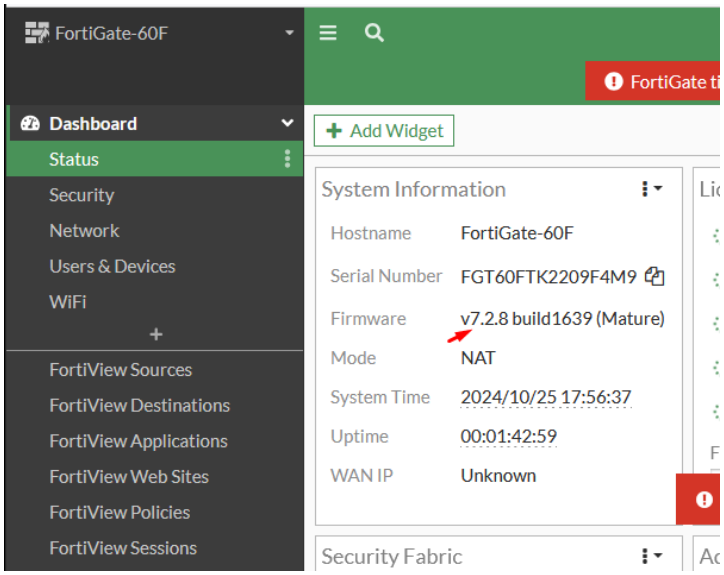


Figura 5.2-9: Versión del firewall después del upgrade.

Como se observa en la figura 5.2-9 ahora el dispositivo tiene la versión 7.2.8.

Conclusiones

- Se realizó exitosamente la actualización del sistema operativo y se presentaron las diferentes versiones disponibles para este modelo, la elección de cual sistema operativo usar dependerá de los bugs existentes y de la estabilidad que se tenga cuando el equipo este en operación.

- Se registró todo el proceso de actualización del firmware llevando el paso a paso de cómo realizarlo.

- Las versiones de sistema operativo en las que se han trabajado las prácticas son las 7.x.x debido a que son las versiones que tienen soporte y desarrollo por el fabricante.

5.3 Práctica 3: Configuración de dirección IP en interfaz física.

Introducción

En la presente práctica se detallará el proceso para establecer una dirección IP en una interfaz física del FortiGate de la WAN y LAN respectivamente.

Esta práctica nos será útil cuando nos toque crear políticas de seguridad posteriormente.

Objetivo general

- Configurar direccionamiento IP en la WAN y LAN

Objetivos específicos

- Asociar el puerto destinado a la WAN a una zona de seguridad
- Agregar el puerto de LAN a la zona de seguridad destinada
- Identificar las diferentes opciones que se activan dependiendo del rol que se asigne a las interfaces.

Desarrollo

En base a la figura que se muestra en la figura 5.3-1 configure la WAN y la respectivamente con el direccionamiento IP que se presenta.

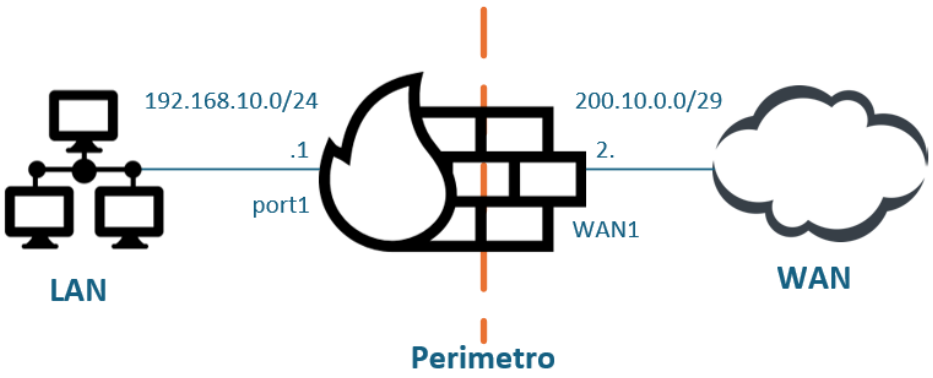


Figura 5.3-1: Detalle de direccionamiento IP.

Asignación de direccionamiento LAN

Paso 1: Lo primero que haremos es asegurarnos que el port1 este libre, es decir que no esté asignado a ningún “software switch” o “hardware switch”.

Nos vamos al menú *Network* > *Interfaces*

Para el caso del FortiGate 60F el port1 está asignado a un *VLAN Switch* llamado *internal* por lo que procedemos a eliminarlo del grupo como se muestra en la Figura 5.3-2.

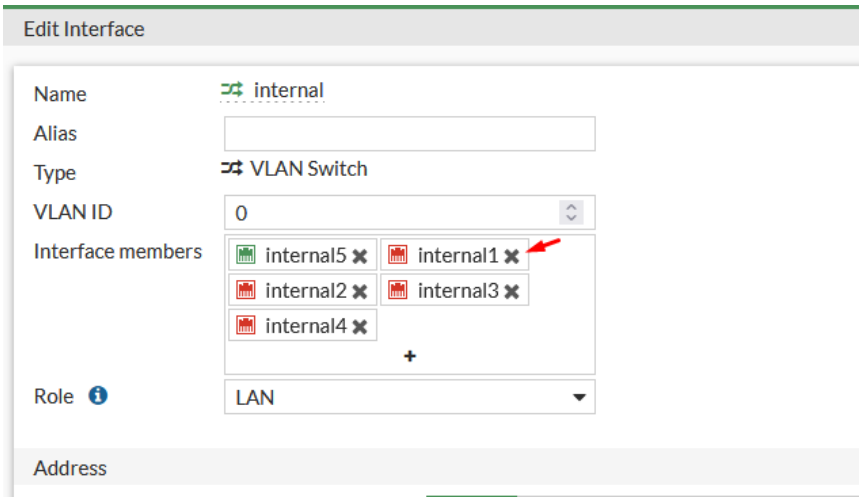


Figura 5.3-2: Editando el VLAN Switch.

Paso 2. Una vez libre el port1 lo podemos editar y asignarle el direccionamiento requerido. Como nos indica la figura 5.3-3 este puerto debe tener la dirección IP 192.168.10.1/24 por lo que procedemos a configurarla de la siguiente manera.

Alias: LAN
Role: LAN
Addressing mode: Manual
IP/Netmask: 192.168.10.1/24
Administrative Access: PING

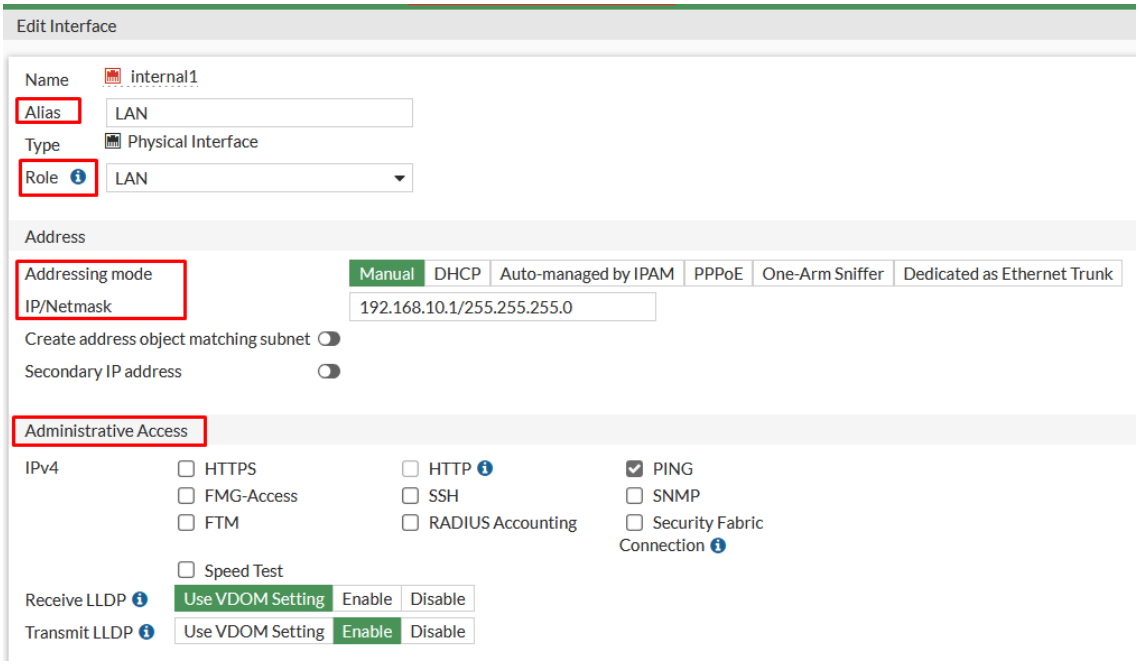


Figura 5.3-3: Parámetros de configuración para la interfaz LAN.

Al finalizar la configuración damos click en OK para guardar los cambios.

Paso 3[12]**:** Siempre en el menú *Network* > *Interfaces* damos click a la opción ***Create New*** y seleccionamos ***Zone*** la editamos como se muestra en la Figura 5.3-4 y damos click en OK.

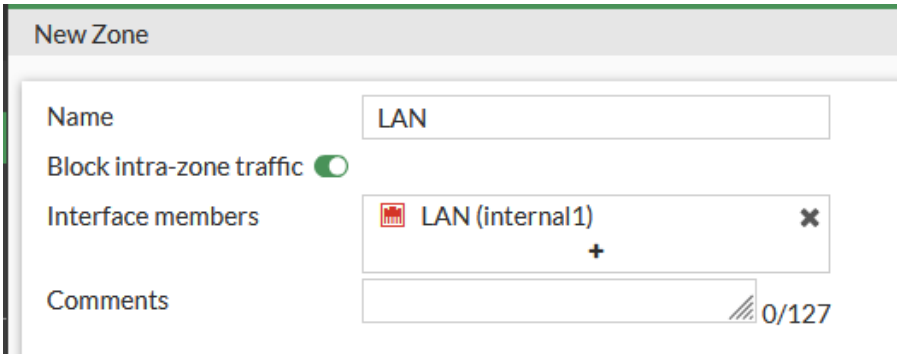


Figura 5.3-4: Creación de Zona LAN.

Paso 4: Para ver por CLI la configuración aplicada usamos el siguiente comando:

[12] El paso 3 es opcional ya que el sistema operativo de los FortiGate permite trabajar sin zonas, pero es recomendable hacerlo para trabajar de una manera más ordenada y facilitar una posible migración a otras tecnologías.

show system interface | grep -f LAN

```
FortiGate-60F # show system interface | grep -f LAN
config system interface
    edit "internal1"
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping
        set type physical
        set alias "LAN" <---
        set device-identification enable
        set lldp-transmission enable
        set role lan
        set snmp-index 4
    next
end
```

Figura 5.3-5: Revisión por CLI de configuración de interfaz LAN.

Asignación de direccionamiento WAN

Paso 1: Lo primero que haremos es asegurarnos que el port1 este libre, es decir que no esté asignado a ningún “software switch” o “hardware switch”.

Nos vamos al menú *Network* > *Interfaces*

Para el caso del FortiGate 60F el wan1 está libre.

Paso 2. Como nos indica la Figura 5.3-6 este puerto debe tener la dirección IP 200.10.0.2/29 por lo que procedemos a configurarla de la siguiente manera.

Alias: WAN
Role: WAN
Addressing mode: Manual
IP/Netmask: 200.10.0.2/29
Administrative Access: PING

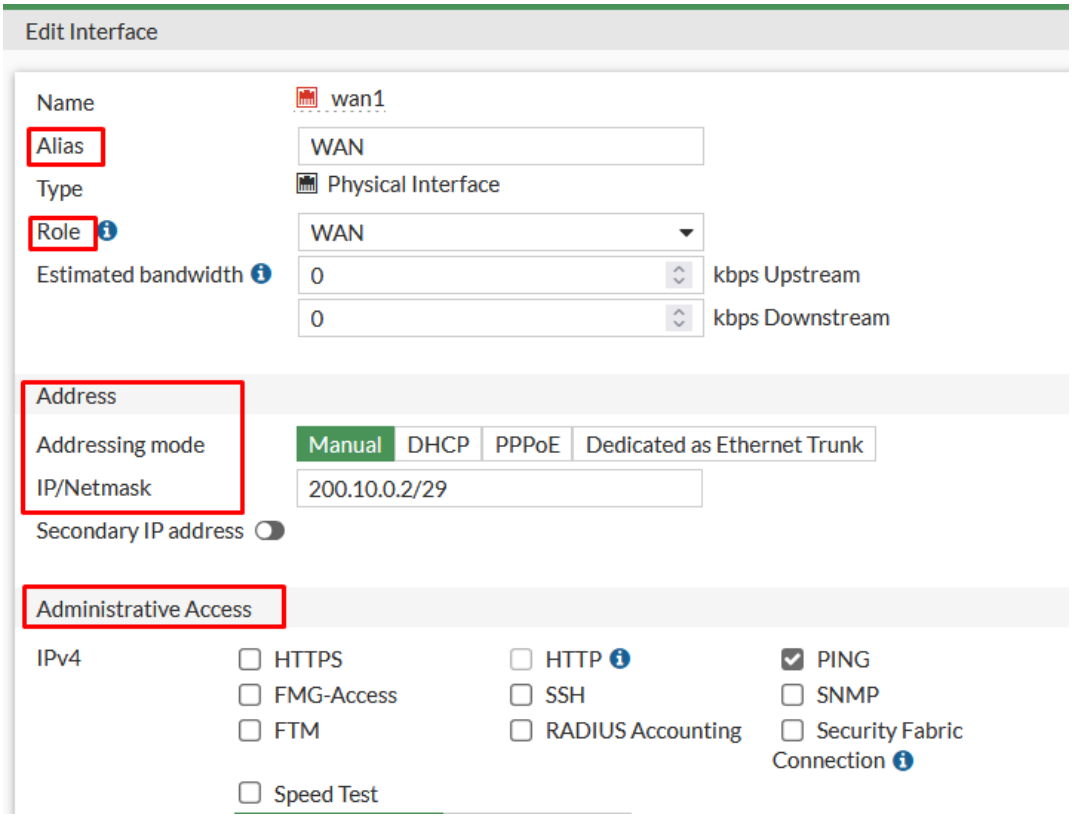


Figura 5.3-6: Parámetros de configuración para la interfaz WAN.

Al finalizar la configuración damos click en OK para guardar los cambios.

Paso 3[13]: Siempre en el menú *Network* > *Interfaces* damos click a la opción ***Create New*** y seleccionamos ***Zone*** la editamos como se muestra en la Figura 3_ 7 y damos click en OK.

[13] El paso 3 es opcional ya que el sistema operativo de los FortiGate permite trabajar sin zonas, pero es recomendable hacerlo para trabajar de una manera más ordenada y facilitar una posible migración a otras tecnologías.

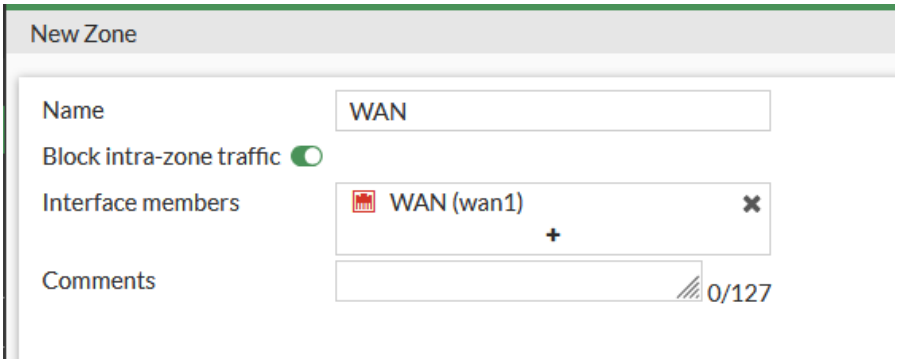


Figura 5.3-7: Creación de Zona WAN.

Paso 4: Para ver por CLI la configuración aplicada usamos el siguiente comando **show system interface | grep -f WAN**

```
FortiGate-60F # show system interface | grep -f WAN
config system interface
    edit "wan1"
        set vdom "root"
        set ip 200.10.0.2 255.255.255.248
        set allowaccess ping
        set type physical
        set alias "WAN" <---
        set role wan
        set snmp-index 1
    next
end
```

Figura 5.3-8: Revisión por CLI de configuración de interfaz WAN.

Conclusiones

- Se configuró exitosamente el direccionamiento IP de la WAN y LAN usando la GUI y se confirmó que estuviera aplicada mediante la CLI.

- Se aprendió como asociar puertos a zonas de seguridad esto nos permite crear políticas de ipv4 usando las zonas en lugar de las interfaces físicas.

- Se identifico que dependiendo role que se le asigne a la interfaz así serán las opciones que nos dará para configurar.

5.4 Práctica 4: Creación de subinterfaces.

Introducción

En la presente practica se detallará el proceso para crear y configurar una sub-interface de tipo vlan.

Esta práctica nos será útil creemos políticas de seguridad por vlan posteriormente.

Objetivo general

- Crear sub-interfaces lógicas que dependan de una interfaz física

Objetivos específicos

- Aplicar el concento de segregación de redes
- Asignar direccionamiento IP a las sub-interfaces
- Identificar las diferentes opciones que se activan dependiendo del rol que se asigne a las sub-interfaces.

Desarrollo

En base a la topología que se muestra en la figura 5.4-1 cree y configure las interfaces como se indica.

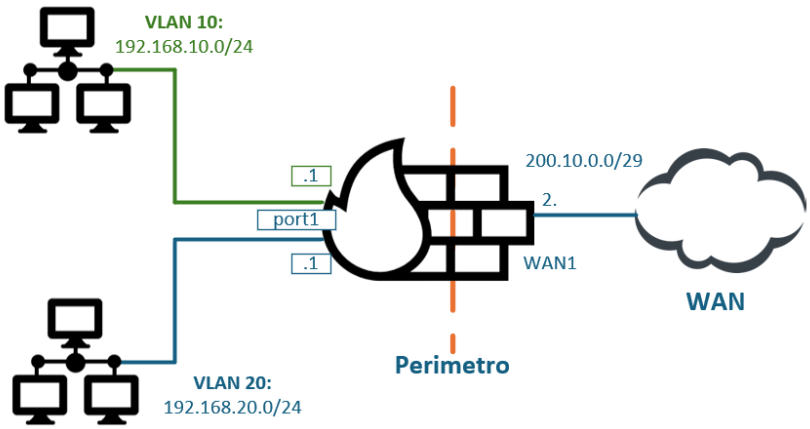


Figura 5.4-1: Detalle de direccionamiento IP y sub-interfaces.

Paso 1: Lo primero que haremos es asegurarnos que el port1 este libre, es decir que no esté asignado a ningún “software switch” o “hardware switch”.

Nos vamos al menú *Network* > *Interfaces*

Para el caso del FortiGate 60F el port1 (internal1) está asignado a un *VLAN Switch* llamado *internal* por lo que procedemos a eliminarlo del grupo como se explicó en la práctica 3.

Paso 2. Una vez libre el port1 lo podemos editar para usarlo como puerto principal del que dependerán las subinterfaces de la LAN. Lo configuramos de la siguiente manera.

Alias: LAN
Role: LAN
Addressing mode: Manual
IP/Netmask: 0.0.0.0/0.0.0.0

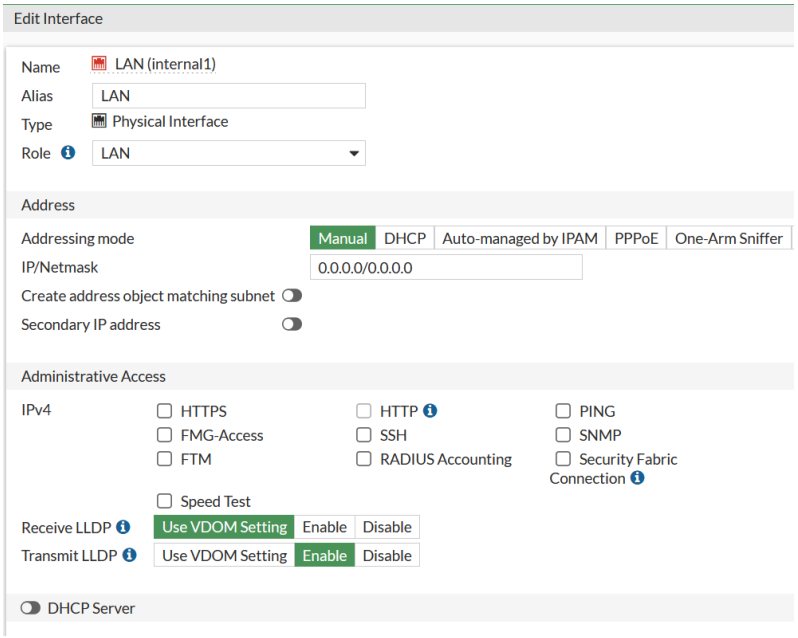


Figura 5.4-2: Parámetros de configuración para la interfaz LAN.

Al finalizar la configuración damos click en OK para guardar los cambios.

Paso 3: Siempre en el menú *Network* > *Interfaces* damos click a la opción ***Create New*** y seleccionamos ***Interface*** la editamos de la siguiente manera.

Name: VLAN_10

Type: VLAN

VLAN protocol: 802.1Q

Interface: LAN (Interal1)

Addressing mode: Manual

IP/Netmask: 192.168.10.1/24

Administrative Access: PING

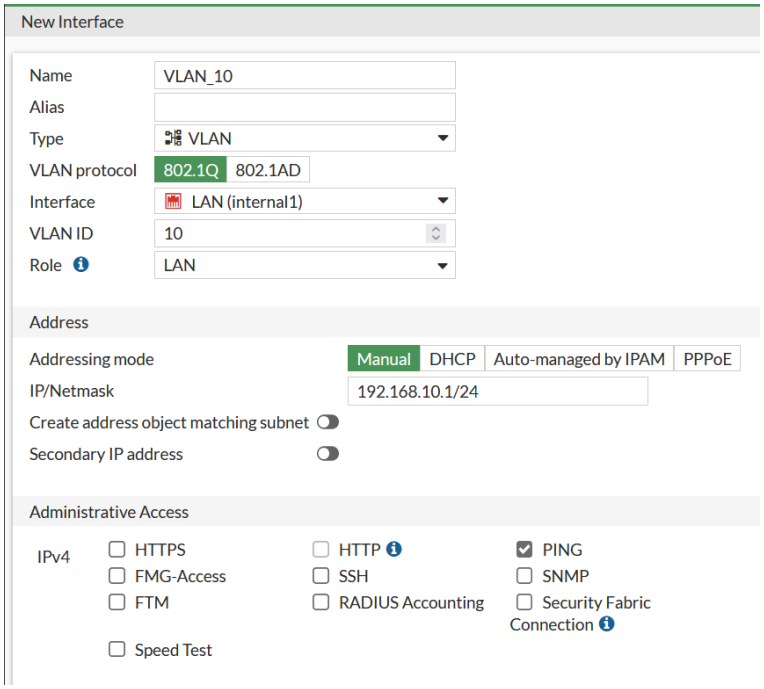


Figura 5.4-3: Creación de sub-interfaz VLAN_10.

Paso 4: Para ver por CLI la configuración aplicada usamos el siguiente comando

show system interface | grep -f LAN

```
FortiGate-60F # show system interface | grep -f VLAN_10
config system interface
    edit "VLAN_10" <---
        set vdom "root"
        set ip 192.168.10.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 17
        set interface "internal1"
        set vlanid 10
    next
end
```

Figura 5.4-4: Revisión por CLI de configuración de interfaz VLAN_10.

Paso 5: Ahora procedemos a configurar la otra sub-interface siempre en el menú *Network* > *Interfaces* damos click a la opción ***Create New*** y seleccionamos ***Interface*** la editamos de la siguiente manera.

Name: VLAN_20
Type: VLAN
VLAN protocol: 802.1Q
Interface: LAN (Interal1)
Addressing mode: Manual
IP/Netmask: 192.168.20.1/24
Administrative Access: PING

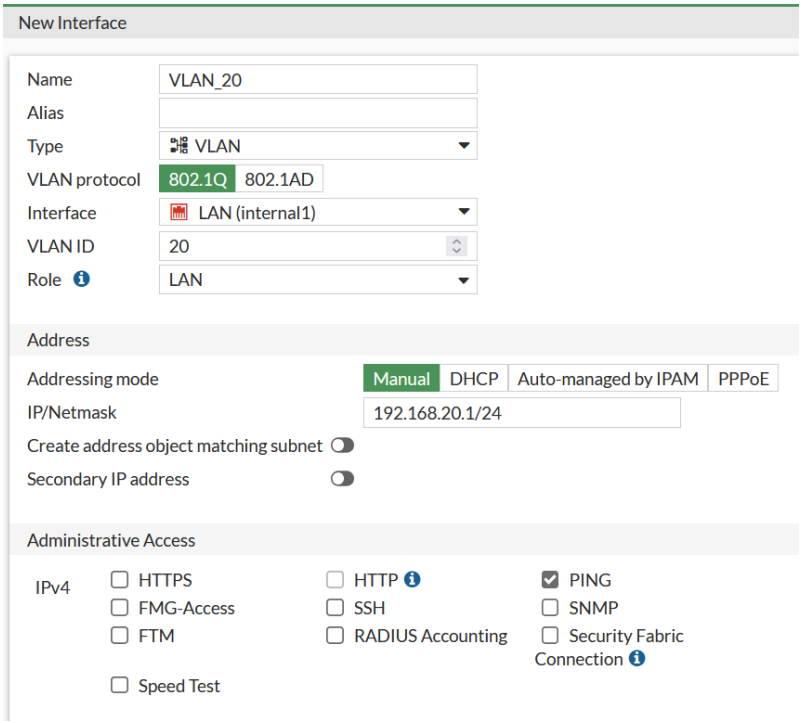


Figura 5.4-5: Creación de sub-interfaz VLAN_20.

Paso 6: Para ver por CLI la configuración aplicada usamos el siguiente comando **show system interface | grep -f VLAN_20**

```
FortiGate-60F # show system interface | grep -f VLAN_20
config system interface
    edit "VLAN_20" <---
        set vdom "root"
        set ip 192.168.20.1 255.255.255.0
        set allowaccess ping
        set device-identification enable
        set role lan
        set snmp-index 18
        set interface "internal1"
        set vlanid 20
    next
end
```

Figura 5.4-6: Revisión por CLI de configuración de interfaz VLAN_20.

Ambas interfaces deben agregarse en su respectiva zona como se detalló en la práctica 3 la cual puede consultarse para referencia.

Asignación de direccionamiento WAN

Paso 1: Lo primero que haremos es asegurarnos que el port1 este libre, es decir que no esté asignado a ningún “software switch” o “hardware switch”.

Nos vamos al menú *Network* > *Interfaces*

Para el caso del FortiGate 60F el wan1 está libre

Paso 2. Como nos indica la Figura 5.4-7 este puerto debe tener la dirección IP 200.10.0.2/29 por lo que procedemos a configurarla de la siguiente manera.

Alias: WAN
Role: WAN
Addressing mode: Manual
IP/Netmask: 200.10.0.2/29
Administrative Access: PING

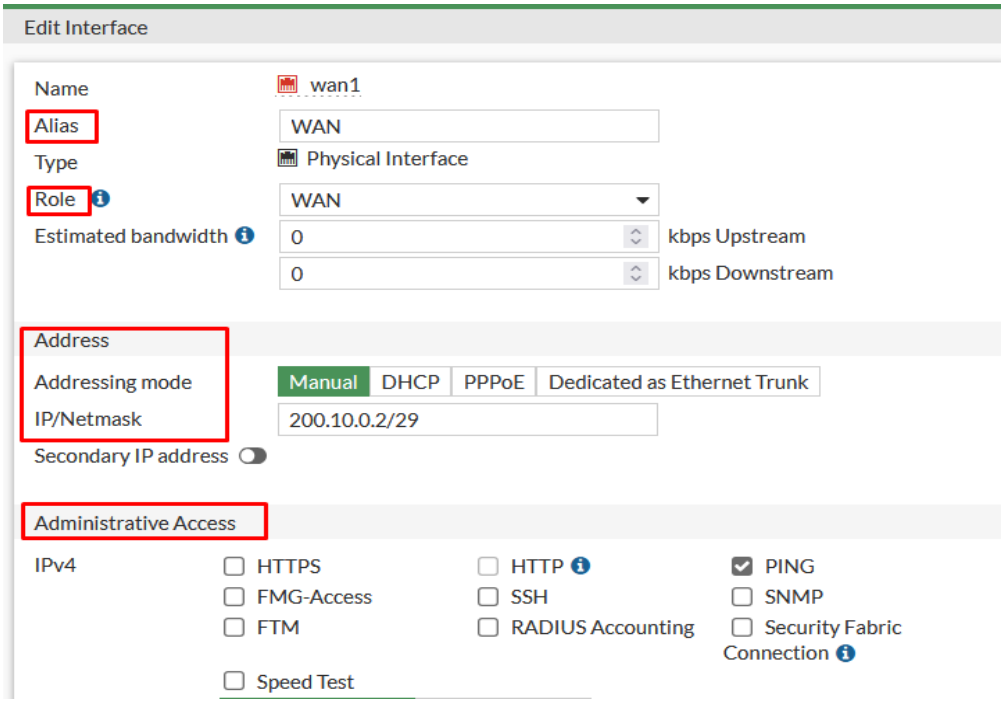


Figura 5.4-7: Parámetros de configuración para la interfaz WAN.

Al finalizar la configuración damos click en OK para guardar los cambios.

Paso 3[14]**:** Siempre en el menú *Network* > *Interfaces* damos click a la opción ***Create New*** y seleccionamos ***Zone*** la editamos como se muestra en la Figura 5.4-8 y damos click en OK

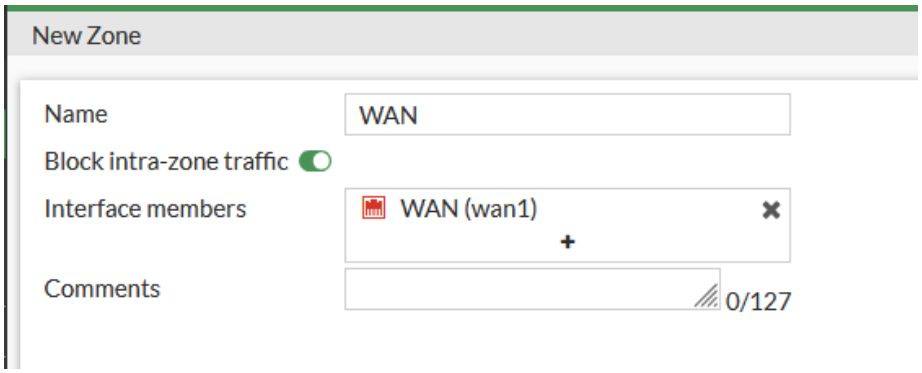


Figura 5.4-8: Creación de Zona WAN.

Paso 4: Para ver por CLI la configuración aplicada usamos el siguiente comando **show system interface | grep -f WAN**

```
FortiGate-60F # show system interface | grep -f WAN
config system interface
    edit "wan1"
        set vdom "root"
        set ip 200.10.0.2 255.255.255.248
        set allowaccess ping
        set type physical
        set alias "WAN" <---
        set role wan
        set snmp-index 1
    next
end
```

Figura 5.4-9: Revisión por CLI de configuración de interfaz WAN.

Conclusiones

- Se crearon exitosamente las sub-interfaces VLAN_10 y VLAN_20 las cuales dependen a nivel lógico de la interfaz principal Internal1

[14] El paso 3 es opcional ya que el sistema operativo de los FortiGate permite trabajar sin zonas, pero es recomendable hacerlo para trabajar de una manera más ordenada y facilitar una posible migración a otras tecnologías.

- Se aplico el concentro de segregación de redes al crear 2 interfaces lógicamente separadas en diferente dominio de broadcast
- Se asigno direccionamiento IP diferente a cada sub-interface lo que obliga al usuario a crear reglas de firewall si es requerido que estas redes tengan comunicación a nivel de capa 3.

5.5 Práctica 5: Políticas de seguridad ipv4.

Introducción

En la presente práctica se explicará el proceso para crear políticas de seguridad de IPv4 para permitir tráfico entre diferentes redes.

Objetivo general

- Crear diferentes políticas de seguridad para permitir tráfico entre dos redes internas y bloquear direcciones IP especificas

Objetivos específicos

- Filtrar tráfico entre dos direcciones IP especificas
- Permitir tráfico por servicios específicos
- Crear y configurar objetos

Desarrollo

De la práctica anterior ya tenemos configurado el direccionamiento IP porque nos enfocaremos en configuración de las políticas de seguridad. En base a la topología que se muestra en la Figura 5.5-1 cree y configure las interfaces y políticas de seguridad como se indica.

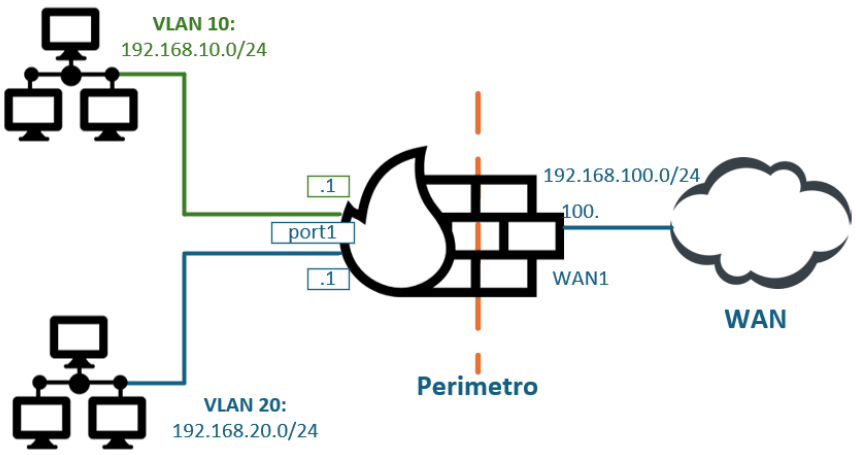


Figura 5.5-1: Detalle de direccionamiento IP y VLAN.

Configuración de objetos

Paso 1: Lo primero que haremos es irnos al menú ***Policy & Objects > Addresses***

Seleccionamos la opción de ***Create new*** y configuramos lo siguiente.

Name: NET_VLAN_10

Type: Subnet

IP/Netmask : 192.168.10.0/24

Interface: Any

Comments: El comentario es opcional

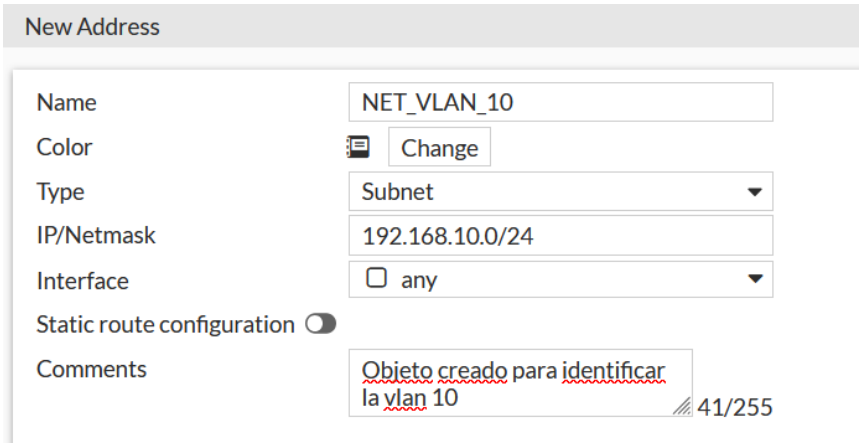


Figura 5.5-2: Detalle de configuración de un objeto.

Paso 2: Seguir el mismo procedimiento para crear el objeto para la vlan 20, cuando tengamos creados ambos objetos nos aparecerán de la siguiente manera.

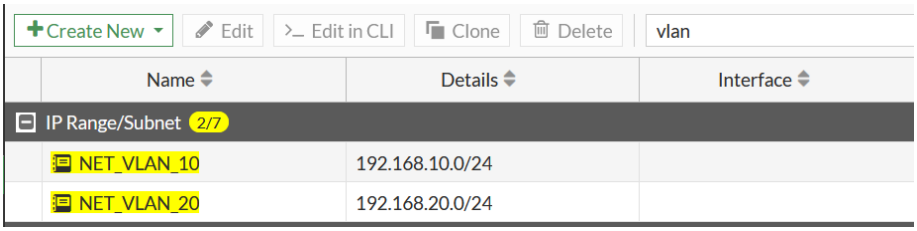


Figura 5.5-3: Creación de objetos para vlan 10 y 20.

Configuración de políticas para permitir trafico

Paso 1: Para crear una política de seguridad que nos permita comunicación entre las redes 192.168.10.0/24 y 192.168.20.0/24 se debe ir primero al menú ***Policy & Objects > Firewall Policy*** y luego click en ***Create New*** y configuramos los parámetros como se muestra en la Figura 5.5-4.

Name: FROM VLAN_10 TO VLAN_20
Incoming Interface: VLAN_10
Outgoing Interface: VLAN_20
Source: NET_VLAN_10
Destination: NET_VLAN_20
Schedule: always
Service: ALL
Action: ACCEPT
NAT: Disable

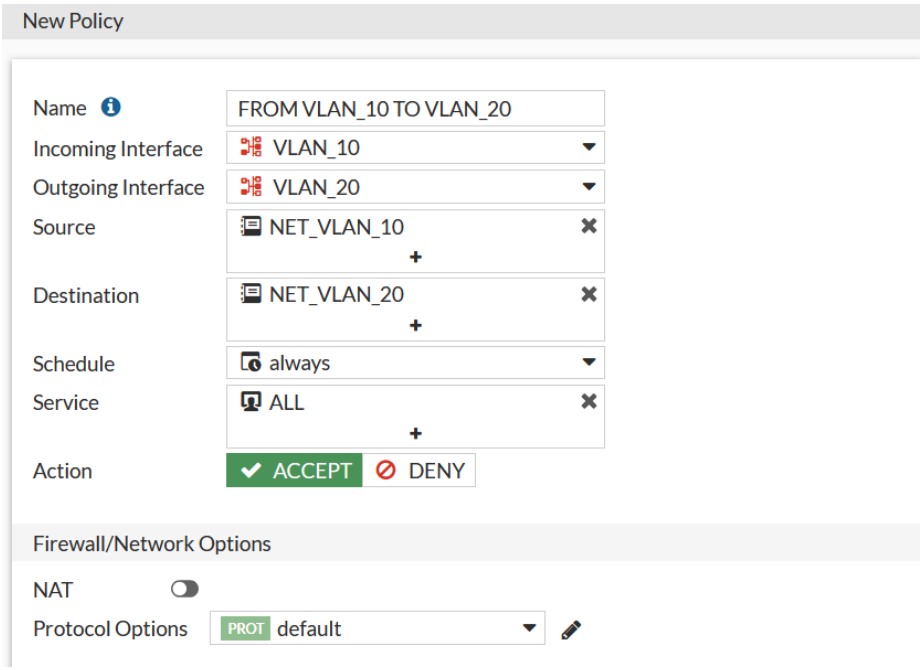


Figura 5.5-4: Creación de política de seguridad con origen la VLAN_10.

Notar que estamos usando los objetos que creamos tanto para el origen como para el destino.

Paso 2: Seguimos los mismos pasos, pero ahora todo tendrá origen VLAN_20 y destino la VLAN_10, esto es así para que exista comunicación bidireccional entre ambas redes.

Name: FROM VLAN_20 TO VLAN_10
Incoming Interface: VLAN_20
Outgoing Interface: VLAN_10
Source: NET_VLAN_20
Destination: NET_VLAN_10
Schedule: always
Service: ALL
Action: ACCEPT
NAT: Disable

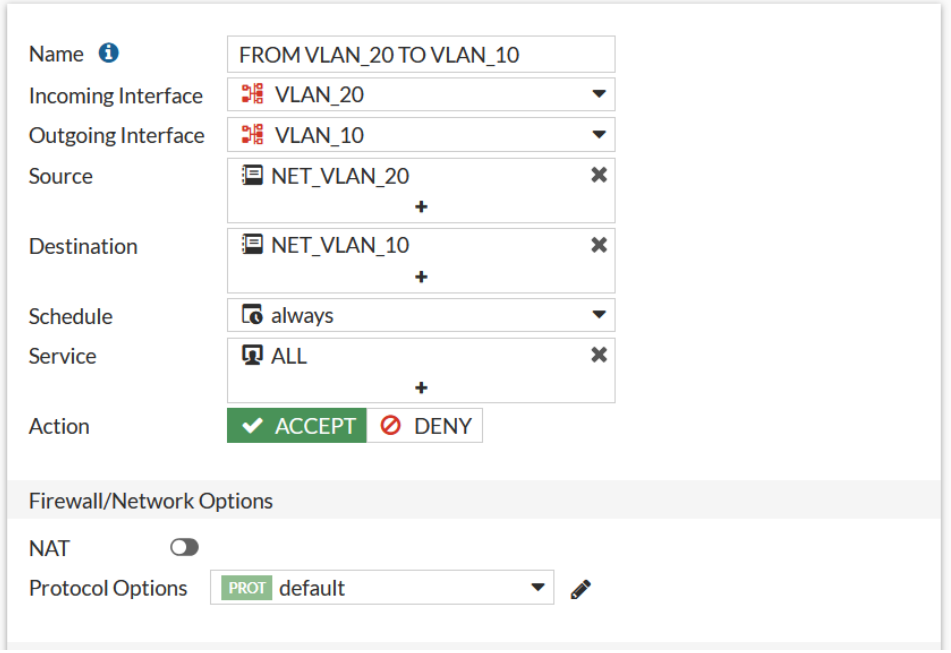


Figura 5.5-5: Creación de política de seguridad con origen la VLAN_20.

Paso 3: Para revisar por CLI las políticas usamos el siguiente comando. **show firewall policy**

```
FortiGate-60F # show firewall policy
config firewall policy
    edit 1
        set name "FROM VLAN_10 TO VLAN_20"
        set uuid 87c435c0-ae96-51ef-dea1-1d0900df2a74
        set srcintf "VLAN_10"
        set dstintf "VLAN_20"
        set action accept
        set srcaddr "NET_VLAN_10"
        set dstaddr "NET_VLAN_20"
        set schedule "always"
        set service "ALL"
    next
    edit 2
        set name "FROM VLAN_20 TO VLAN_10"
        set uuid 8b1490c6-ae96-51ef-2f8a-f0f3f710f1bb
        set srcintf "VLAN_20"
        set dstintf "VLAN_10"
        set action accept
        set srcaddr "NET_VLAN_20"
        set dstaddr "NET_VLAN_10"
        set schedule "always"
        set service "ALL"
    next
end
```

Figura 5.5-6: Revisión de políticas usando la CLI.

Configuración de políticas para bloquear trafico

Paso 1: Se deben crear los objetos a los cuales les queremos bloquear el tráfico, para la práctica se debe bloquear el tráfico con origen 192.168.10.10 y destino 192.168.20.20 por el servicio específico de FTP.

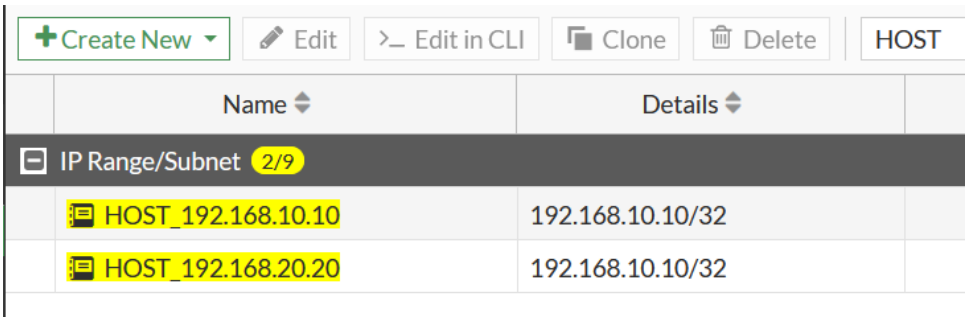


Figura 5.5-7: Creación de objetos específicos.

Paso 2: Ahora creamos la política de seguridad teniendo en cuenta que nos han pedido bloquear el servicio específico de FTP.

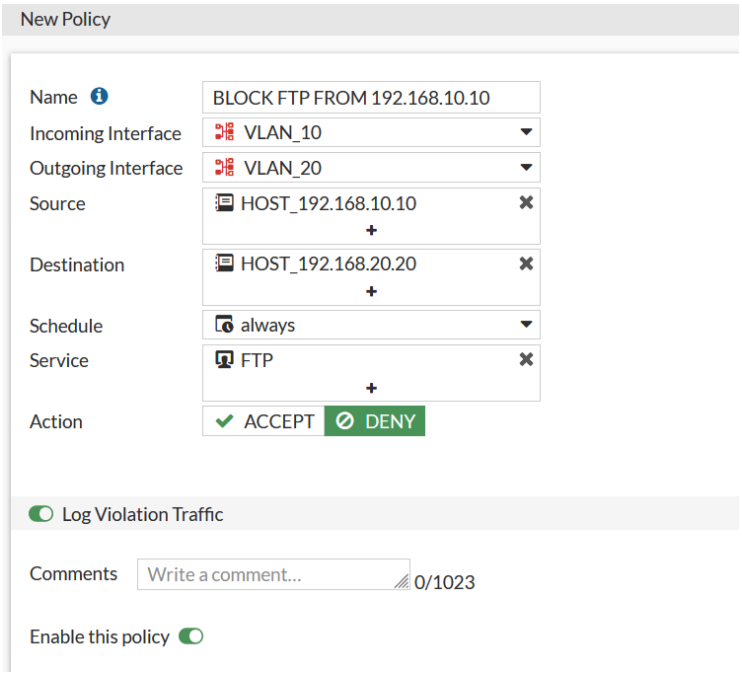


Figura 5.5-8: Bloqueo de FTP en IP específica.

Paso 3: Nos aseguramos de que la política de bloqueo esta arriba de las políticas que permiten el tráfico de toda la red, si está de ultimo la debemos subir arrastrándola con el puntero.

ID	Name	From	To	Source	Destination
1	FROM VLAN_10 TO VLAN_20	VLAN_10	VLAN_20	NET_VLAN_10	NET_VLAN_20
2	FROM VLAN_20 TO VLAN_10	VLAN_20	VLAN_10	NET_VLAN_20	NET_VLAN_10
3	BLOCK FTP FROM 192.168.10.10	VLAN_10	VLAN_20	HOST_192.168.10.10	HOST_192.168.20.20
0	Implicit Deny	any	any	all	all

Figura 5.5-9: Stack de políticas creadas.

ID	Name	From	To	Source	Destination	Schedule	Service	Actio
3	BLOCK FTP FROM 192.168.10.10	VLAN_10	VLAN_20	HOST_192.168.10.10	HOST_192.168.20.20	always	FTP	DE
1	FROM VLAN_10 TO VLAN_20	VLAN_10	VLAN_20	NET_VLAN_10	NET_VLAN_20	always	ALL	AC
2	FROM VLAN_20 TO VLAN_10	VLAN_20	VLAN_10	NET_VLAN_20	NET_VLAN_10	always	ALL	AC
0	Implicit Deny	any	any	all	all	always	ALL	DE

Figura 5.5-10: Políticas ordenadas para bloquear FTP.

Conclusiones

- Se crearon diferentes políticas de seguridad que permiten y crean conectividad entre dos redes asociadas a una sub-interfaz.
- Se vio la posibilidad de bloquear tráfico por un protocolo especifico, esto nos permite ser granulares al momento de configurar nuestras políticas.
- Se aprendió a configurar objectos con redes específicas para delimitar las políticas de seguridad.

5.6 Práctica 6: Dominios virtuales.

Introducción

En la presente práctica se explicará el proceso para crear y configurar dominios virtuales, este método se usa cuando necesitamos crear particiones en el firewall, es decir, crear un recurso que tenga su propia tabla de enrutamiento y sus propias políticas de seguridad.

Objetivo general

- Crear un dominio virtual que tenga sus propias características de configuración como rutas, interfaces y políticas.

Objetivos específicos

- Agregar un *inter-vdom-link* para comunicar el *vdom-root* con el nuevo *vdom*
- Establecer direccionamiento IP a los vdom link para comunicar particiones a nivel de capa 3.
- Navegar sobre el menú global del firewall y moverse hacia los diferentes *vdom* creados.

Desarrollo

Tomando como referencia la topología que se muestra en la Figura 5.6-1 debemos crear una partición llamada vdom-A.

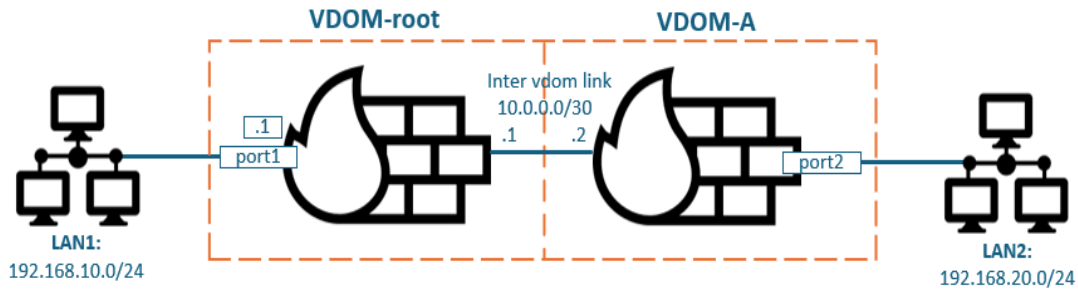


Figura 5.6-1: Topología de dos vdom.

Configuración de nuevo VDOM

Paso 1: Para activar los dominios administrativos en el firewall ejecutamos los siguientes comandos.

```
FortiGate-60F # config system global
FortiGate-60F # set vdom-mode multi-vdom
FortiGate-60F # end
```

Nos mostrará un mensaje que al aplicar esta opción se cambiará el modo de operación del firewall y que debemos volver a autenticarnos.

Cuando entremos al firewall nuevamente nos mostraré el menú que se observa en la Figura 5.6-2 en el cual vemos que ahora nos aparecen 2 particiones.

Global: Desde aquí se administran las configuraciones globales del firewall como el hostname, hora, SNMP, licencias, alta disponibilidad.

Root: Aquí está el plano administrativo y este vdom pasa a ser nuestra partición principal donde están asignadas todas las interfaces del firewall.

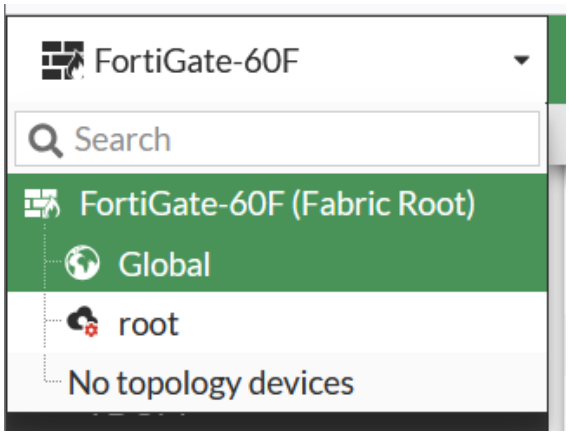


Figura 5.6-2: Menú para cambiar de vdom.

Paso 2: Para crear un nuevo vdom nos vamos al menú ***System > VDOM*** y seleccionamos la opción ***Create New.***

El nuevo vdom debe tener las siguientes características:

Type: Traffic

NGFW Mode: Profile-based

Central SNAT: Disable

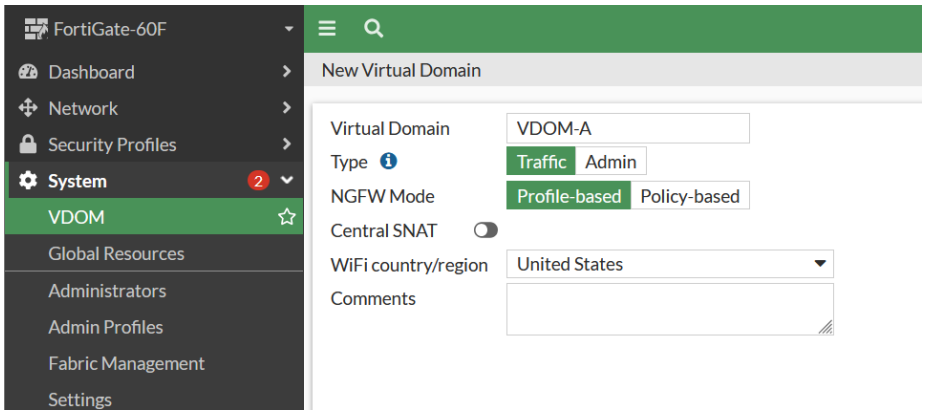


Figura 5.6-3: Creación de nuevo vdom.

Paso 3: Ahora que esta creado el nuevo vdom le asignamos el port2 como se muestra en la topología de referencia de la Figura 5.6-4.

Para esto nos vamos al menú ***Global > Network > Interfaces***

Alias: LAN2

Type: Physical Interfaces

Virtual domain: VDOM-A

Role: LAN

Addressing mode: Manual

IP/Netmask: 192.168.20.1/24

Administrative Access: PING

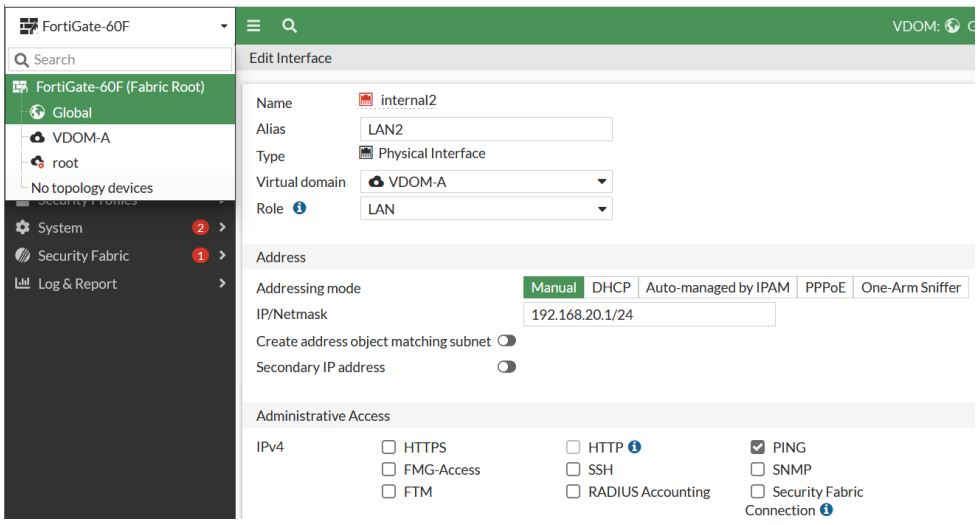


Figura 5.6-4: Asignación de interface a VDOM-A.

Paso 4: El port1 ya está asignado al vdom root por lo que solo procedemos a configurar la dirección IP de la siguiente manera:

Alias: LAN1
Type: Physical Interfaces
Virtual domain: root
Role: LAN
Addressing mode: Manual
IP/Netmask: 192.168.10.1/24
Adminitrative Access: PING

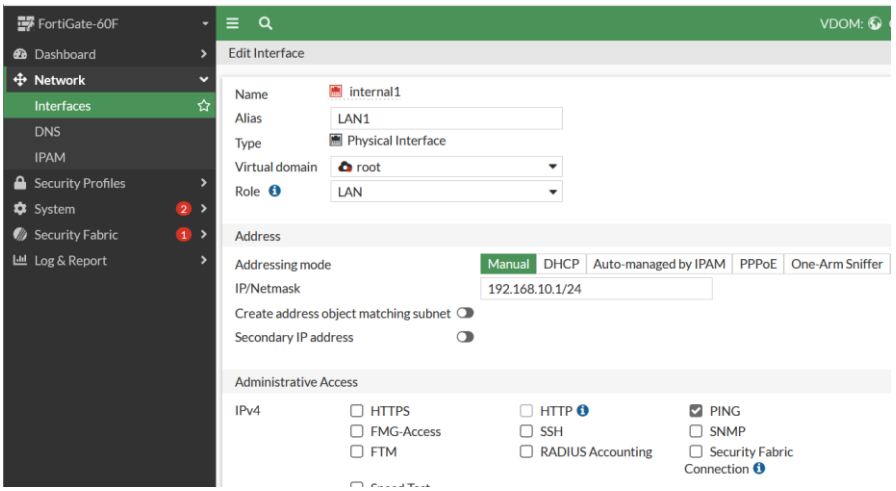


Figura 5.6-5: Asignación de interface a VDOM root.

Paso 5: Revisar que ambas interfaces estén configuradas con la dirección IP correcta y asignadas al vdom que le corresponde.

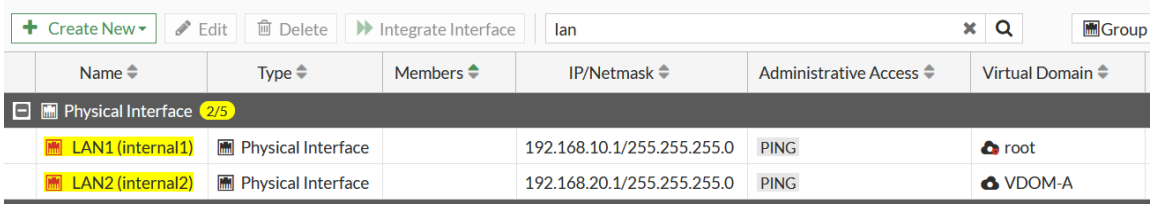


Figura 5.6-6: Revisión de interfaces.

Configuración de *Inter-vdom-link*

Paso 1: Para configurar el ***inter vdom link*** que nos permite que ambas particiones pasen tráfico nos vamos al menú ***Global > Network > Interfaces*** y seleccionamos ***Create New*** y elegimos la opción ***VDOM Link.***

Paso 2: Configurar el *vdom link* de la siguiente manera:

Name: vdomlink

Interface 0 (vdomlink0)

Virtual Domain: root

IP/Netmask: 10.0.0.1/30

Administrative Access: PING

Status: Enabled

Interface 1 (vdomlink1)

Virtual Domain: VDOM-A

IP/Netmask: 10.0.0.2/30

Administrative Access: PING

Status: Enabled

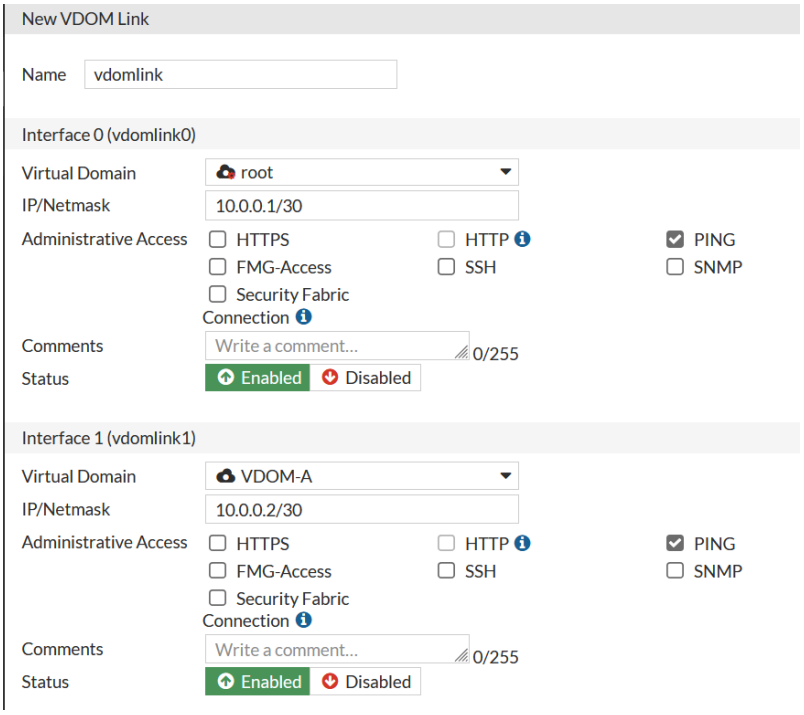


Figura 5.6-7: Creación de inter vdom link.

Paso 3: Revisar que ambas interfaces estén configuradas con la dirección IP correcta y asignadas al vdom que le corresponde.

Name	Type	Members	IP/Netmask	Administrative Access	Virtual Domain
VDOM Link 3					
vdomlink	VDOM Link				root VDOM-A
vdomlink0	VDOM Link Interface		10.0.0.1/255.255.255.252	PING	root
vdomlink1	VDOM Link Interface		10.0.0.2/255.255.255.252	PING	VDOM-A

Figura 5.6-8: Revisión de inter vdom link.

Paso 4: Realizar una prueba de conectividad usando el comando ping entre ambos vdom.

```
FortiGate-60F (root) # execute ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2): 56 data bytes
64 bytes from 10.0.0.2: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 10.0.0.2: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=255 time=0.1 ms

--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.2 ms
```

Figura 5.6-9: Prueba de PING desde el vdom root.

```
FortiGate-60F (VDOM-A) # exe ping 10.0.0.1
PING 10.0.0.1 (10.0.0.1): 56 data bytes
64 bytes from 10.0.0.1: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 10.0.0.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=255 time=0.0 ms

--- 10.0.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.2 ms
```

Figura 5.6-10: Prueba de PING desde el vdom A.

Conclusiones

- Se confirmó el proceso para crear dominios virtuales desde la CLI y se aplicó al FortiGate 60F
- Se creo exitosamente un *vdom link* y se asignó a cada partición
- El direccionamiento IP asignado a cada inter *vdom link* nos permitió comunicar a nivel de capa 3 ambas particiones y con esto ya podemos enrutar tráfico.
- Se aprendió como cambiarse entre *vdom* a través de la GUI de una manera intuitiva.

5.7 Práctica 7: Enrutamiento estático.

Introducción

En la presente practica se explicará el proceso para crear rutas estáticas en FortiOS para comunicar redes a nivel de capa 3.

Objetivo general

- Crear rutas estáticas para establecer conectividad de capa 3 entre redes asignadas a diferente dominio administrativo.

Objetivos específicos

- Revisión de la tabla de enrutamiento usando la CLI.
- Conocer los parámetros necesarios para agregar una ruta estática.

Desarrollo

Tomando como referencia la topología de la práctica anterior vamos a configurar 2 rutas estáticas, una en cada vdom para que exista comunicación entre ambas redes.

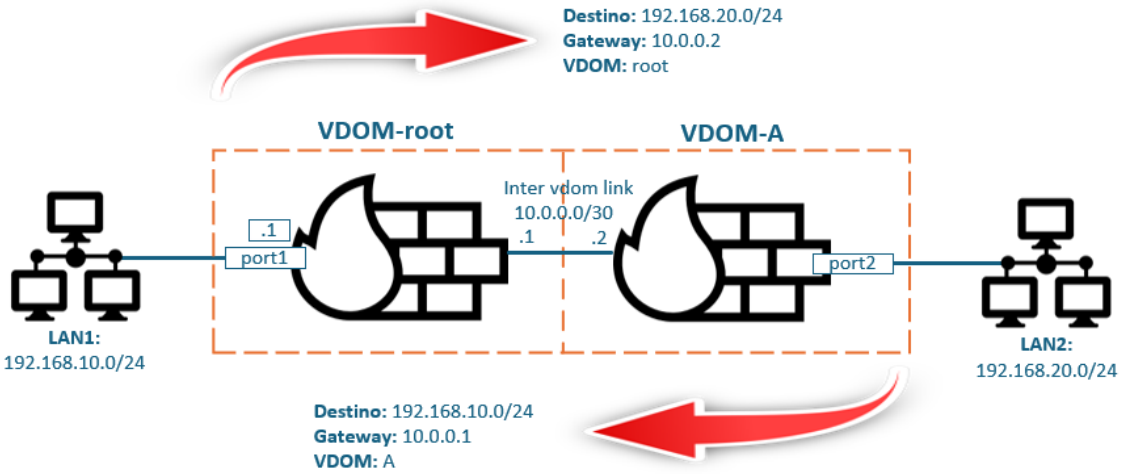


Figura 5.7-1: Topología para agregar rutas estáticas.

Vamos a partir de la topología previamente configurada en la práctica 6 de dominios administrativos y a partir de ahí agregaremos las rutas estáticas que se nos solicitan.

Configuraciones en VDOM root

Paso 1: Agregamos la ruta con destino la red 192.168.20.0/24 en el vdom root, para esto nos vamos al menú ***VDOM Root > Network > Static Routes*** y damos click en *Create New.*

Destination: 192.168.20.0/24
Gateway Address: 10.0.0.2
Interface: vdomlink0
Administrative Distance: 10
Comments: El comentario es opcional.
Status: Enabled

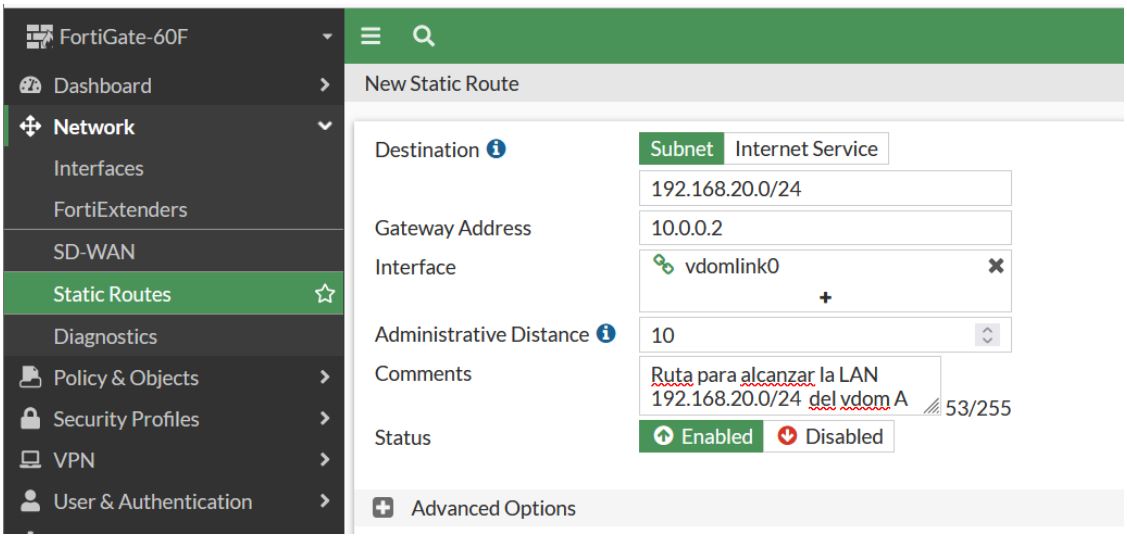


Figura 5.7-2: Ruta estática en vdom root.

Paso 2: Debemos revisar que efectivamente se haya agregado la ruta en la tabla de enrutamiento, para verificar usaremos el comando:

get router info routing-table details 192.168.20.0

```
FortiGate-60F (root) # get router info routing-table details 192.168.20.0

Routing table for VRF=0
Routing entry for 192.168.20.0/24
  Known via "static", distance 10, metric 0, best
  * vrf 0 10.0.0.2, via vdomlink0
```

Figura 5.7-3: Verificación de ruta estática por CLI en vdom root.

Paso 3: Ahora debemos crear el objeto y la política de seguridad para permitir el tráfico que se origine en la red 192.168.10.0/24 con destino 192.168.20.0/24 en vdom root.

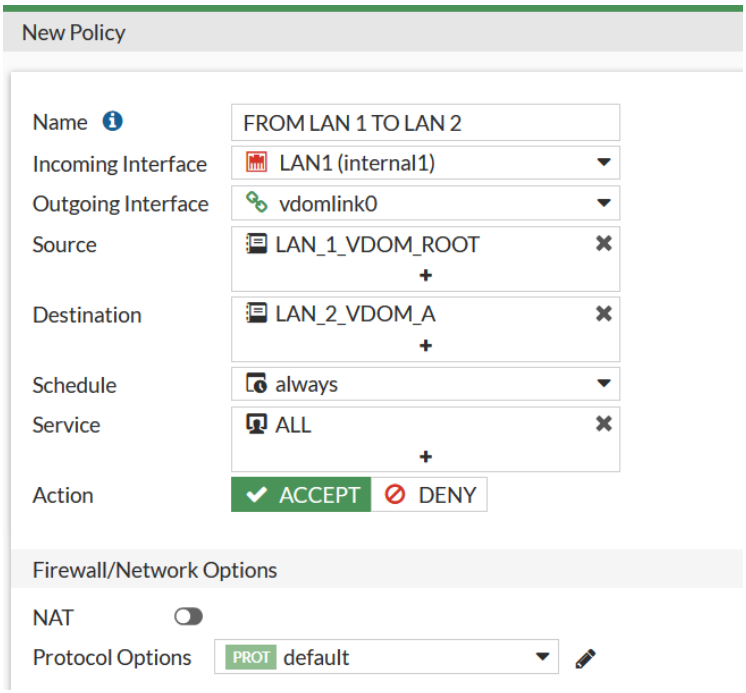


Figura 5.7-4: Creación de política 1 en vdom root.

Paso 4: Ahora debemos crear el objeto y la política de seguridad para permitir el tráfico que se origine en la red 192.168.20.0/24 con destino 192.168.10.0/24 en vdom root.

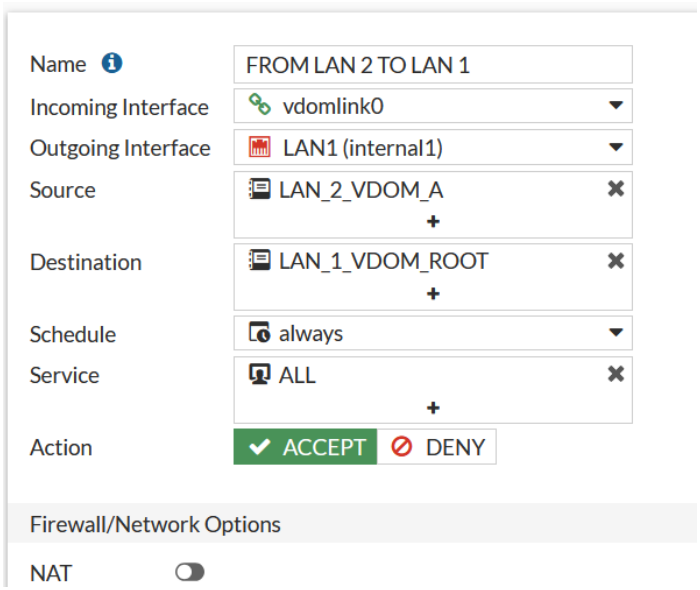


Figura 5.7-5: Creación de política 2 en vdom root.

Configuraciones en VDOM A

Paso 1: Agregamos la ruta con destino la red 192.168.10.0/24 en el vdom A, para esto nos vamos al menú ***VDOM Root > Network > Static Routes*** y damos click en *Create New.*

Destination: 192.168.10.0/24
Gateway Address: 10.0.0.1
Interface: vdomlink1
Administrative Distance: 10
Comments: El comentario es opcional
Status: Enabled

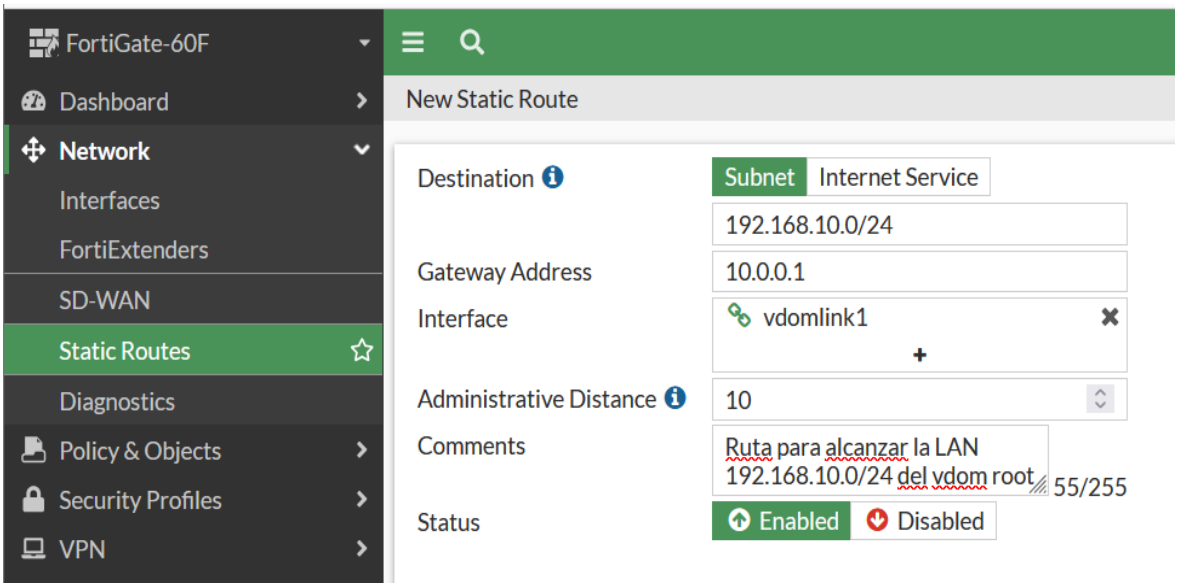


Figura 5.7-6: Ruta estática en vdom A.

Paso 2: Debemos revisar que efectivamente se haya agregado la ruta en la tabla de enrutamiento, para verificar usaremos el comando:

get router info routing-table details 192.168.10.0

```
FortiGate-60F (VDOM-A) # get router info routing-table details 192.168.10.0

Routing table for VRF=0
Routing entry for 192.168.10.0/24
  Known via "static", distance 10, metric 0, best
  * vrf 0 10.0.0.1, via vdomlink1
```

Figura 5.7-7: Verificación de ruta estática por CLI en vdom A.

Paso 3: Ahora debemos crear el objeto y la política de seguridad para permitir el tráfico que se origine en la red 192.168.20.0/24 con destino 192.168.10.0/24 en vdom A.

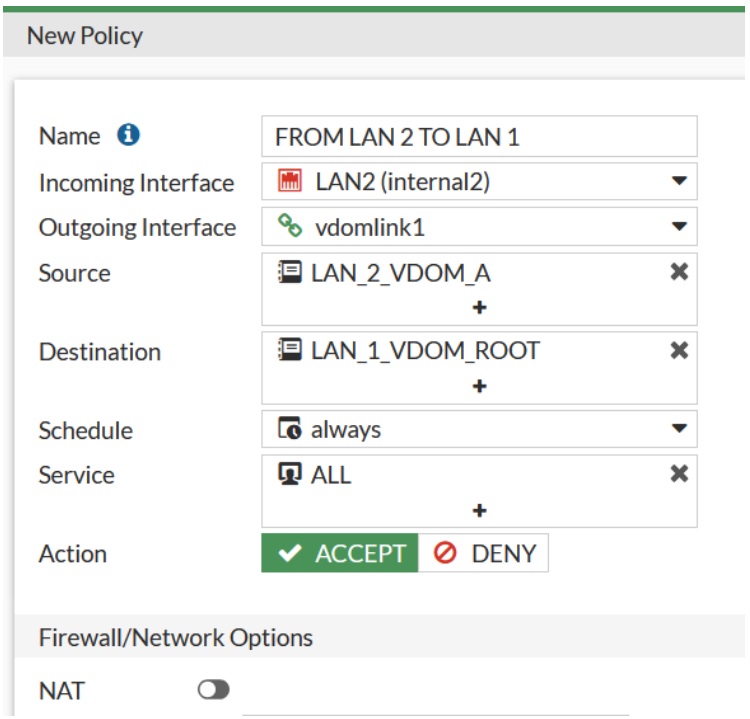


Figura 5.7-8: Creación de política 1 en vdom A.

Paso 4: Ahora debemos crear el objeto y la política de seguridad para permitir el tráfico que se origine en la red 192.168.10.0/24 con destino 192.168.20.0/24 en vdom A.

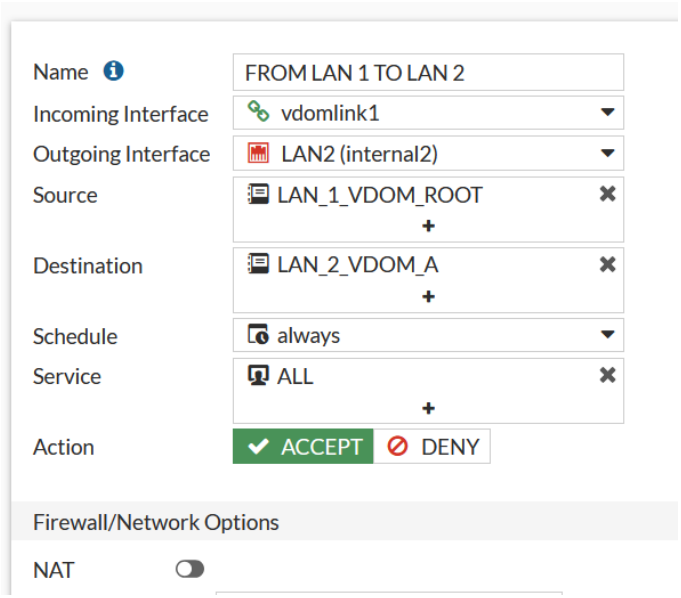


Figura 5.7-9: Creación de política 2 en vdom A.

Pruebas de conectividad

Paso 1: Realizamos la prueba de conectividad desde LAN_1 del vdom root hacia LAN_2 del vdom A.

```
FortiGate-60F (root) #   exe ping-options source 192.168.10.1

FortiGate-60F (root) # exe ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1): 56 data bytes
64 bytes from 192.168.20.1: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 192.168.20.1: icmp_seq=1 ttl=255 time=0.0 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from 192.168.20.1: icmp_seq=4 ttl=255 time=0.1 ms

--- 192.168.20.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.1/0.2 ms
```

Figura 5.7-10: Prueba de conectividad desde el vdom root.

Paso 2: Realizamos la prueba de conectividad desde LAN_2 del vdom A hacia LAN_1 del vdom root.

```
FortiGate-60F (VDOM-A) # execute ping-options source 192.168.20.1

FortiGate-60F (VDOM-A) # exe ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1): 56 data bytes
64 bytes from 192.168.10.1: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 192.168.10.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=255 time=0.1 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=255 time=0.0 ms

--- 192.168.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.1/0.2 ms
```

Figura 5.7-11: Prueba de conectividad desde el vdom A.

Conclusiones

- Se crearon exitosamente las rutas estáticas para establecer conectividad IP entre dos redes en diferente vdom.
- Con el uso del CLI se aprendió como revisar la tabla de enrutamiento para una red especifica.
- Al agregar una ruta estática nos dimos cuenta de que se pueden manipular los parámetros de distancia administrativa y prioridad al igual que en un router para elegir una ruta como principal.

5.8 Práctica 8: Regla de SNAT.

Introducción

En la presente práctica se explicará el proceso para crear un NAT de origen desde una LAN directamente conectada al firewall y desde una LAN que este conectada a otro firewall.

Objetivo general

- Comprender el concepto de NAT de origen o SNAT para navegación hacia internet.

Objetivos específicos

- Realizar un SNAT desde una red que no esté directamente conectada en el FortiGate.
- Crear un IP Pool para una dirección especifica de SNAT

Desarrollo

Tomando como referencia la topología de la práctica anterior vamos a configurar 2 reglas de NAT, uno para una LAN1 directamente conectada en el VDOM root y otra para LAN2 conectada en el VDOM-A

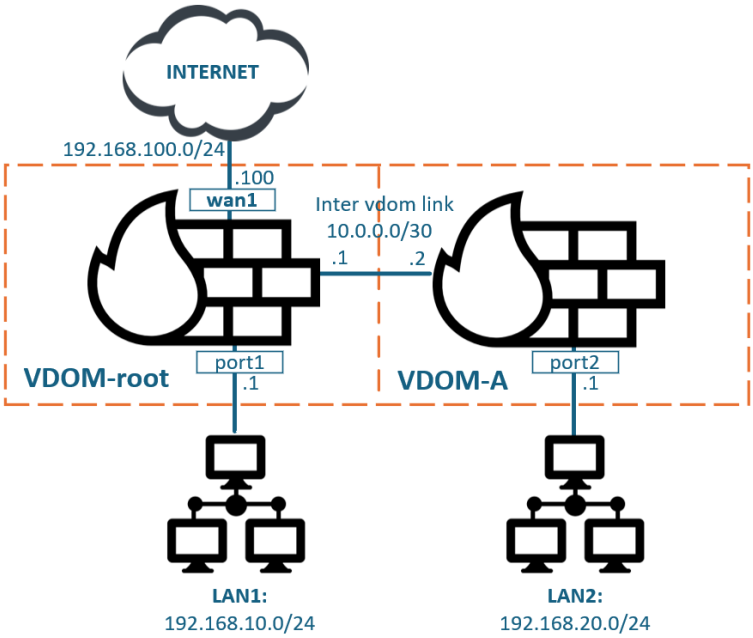


Figura 5.8-1: Topología para SNAT.

Configuración de SNAT en VDOM root

Paso 1: Creamos el objeto para la red que requerimos sea el origen de NAT, como se observa en la Figura 5.8-2 la red del vdom root es la 192.168.10.0/24, para esto nos iremos al menú ***Policy & Objects > Addresses*** y damos click en ***Create New***

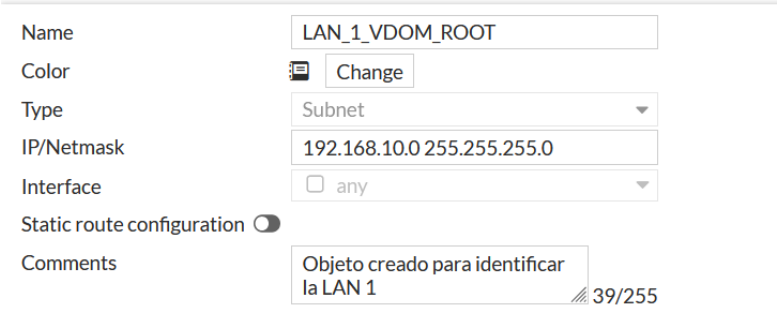


Figura 5.8-2: Objeto para identificar LAN1.

Paso 2: Ahora procedemos a crear la política que permitirá el acceso y realizará el SNAT para el tráfico que se origine en LAN1.

Nos vamos al menú ***Policy & Objects > Firewall Policy*** y damos click en ***Create New***

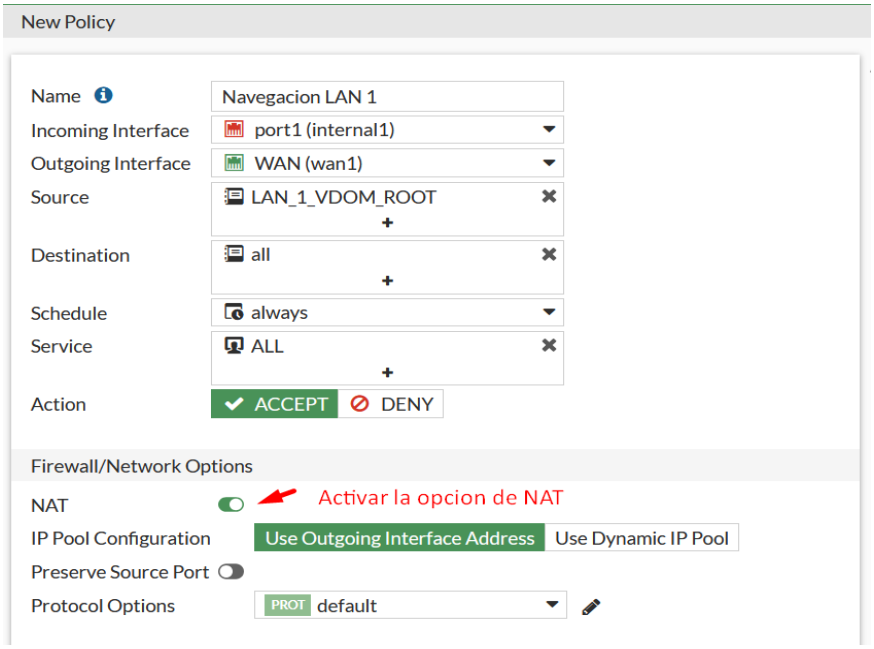


Figura 5.8-3: Política de SNAT para navegación.

Paso 3: Conectar una computadora al port1 del firewall y colocarle la siguiente configuración estáticamente.

IP: 192.168.10.2

Mascara: 255.255.255.0

Puerta de enlace: 192.168.10.1

DNA: 8.8.8.8

Paso 4: Realizar pruebas de navegación desde la computadora que se conectó.

Paso 5: Revisar el tráfico que se está generando desde la computadora, para esto nos vamos a **Dashboard > Fortiview Sources**

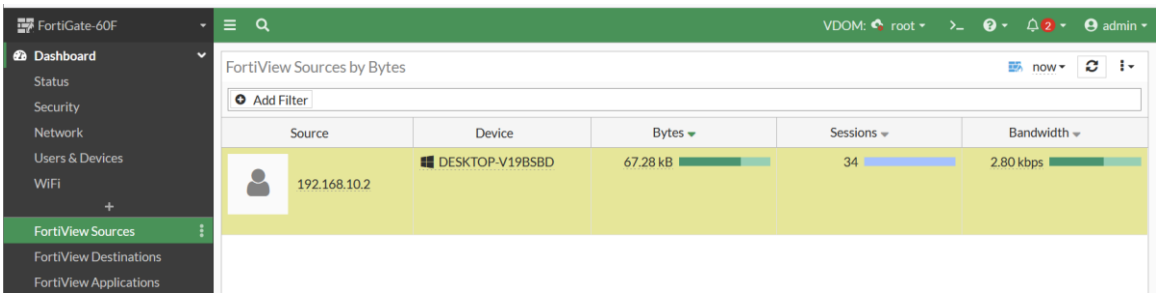


Figura 5.8-4: Revisión de orígenes desde el Fortiview.

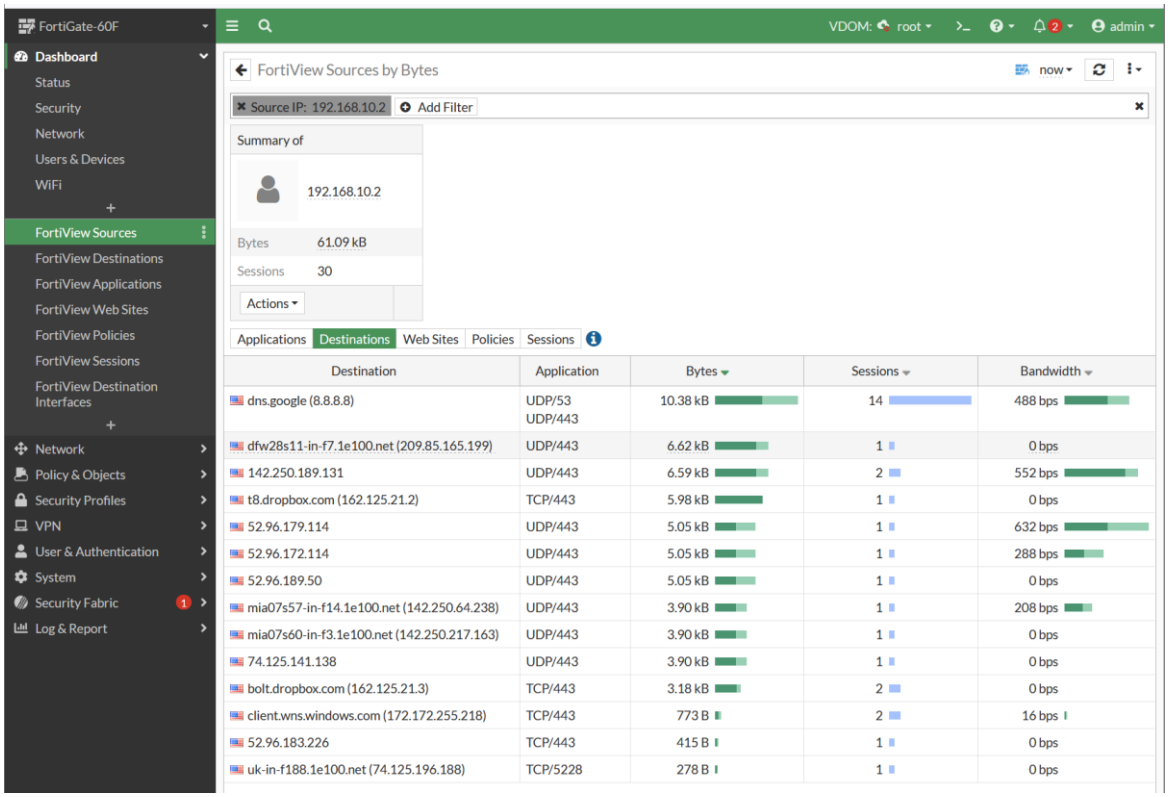


Figura 5.8-5: Detalle de tráfico para una IP específica.

Paso 6: Ahora nos iremos a la opción ***Log & Report > Forward Traffic*** y filtraremos la dirección IP de la computadora 192.168.10.2.

Al dar doble click sobre cualquier ***log*** podemos ver el detalle y al ubicar el campo de ***source*** podemos identificar que nos está haciendo NAT con la dirección IP 192.168.100.100 que es la WAN del FortiGate.

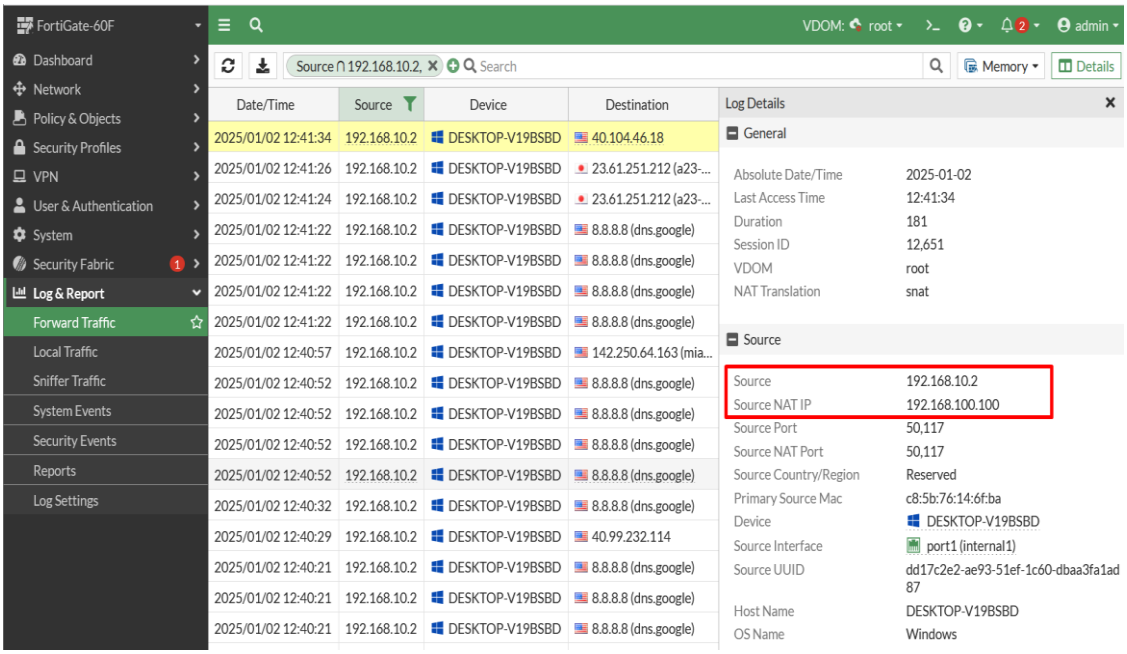


Figura 5.8-6: revisión de Log desde el forward traffic.

Configuración de IP Pool para hacer SNAT con IP específica.

Paso 1: Primero creamos el Pool para esto nos vamos a ***Policy & Objects > IP Pools*** y creamos uno nuevo.

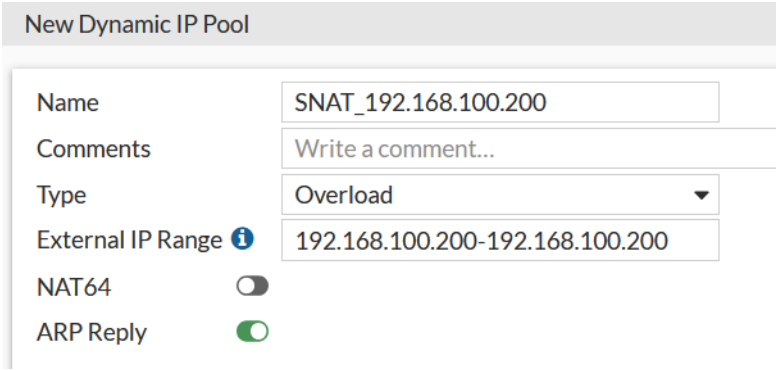


Figura 5.8-7: Creación de IP Pool.

El NAT debe ser del tipo Overload para que nos haga sobrecarga de puertos y debemos habilitar el ***ARP Reply*** para que aparezca en la tabla ARP.

Paso 2: Nos vamos a la política de seguridad en ***Policy & Objects > Firewall Policy*** para editar la política.

En la opción de ***IP Pool Configuration*** habilitamos la opción ***Use Dynamic IP Pool*** y seleccionamos el *IP Pool* que creamos.

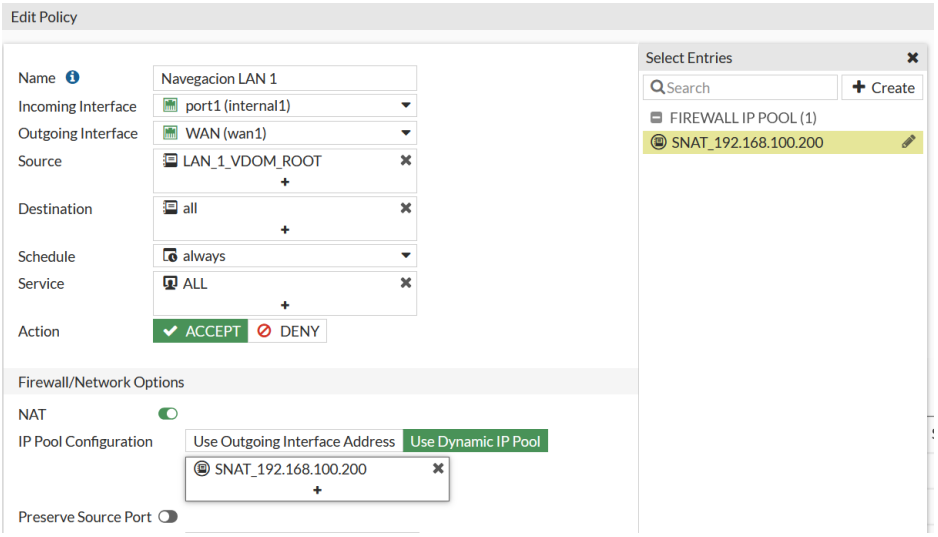


Figura 5.8-8: Aplicación de IP Pool en política de seguridad.

Paso 3: Generar tráfico desde la computadora y revisar los *logs* para confirmar que se haya actualizado la IP de ***Source NAT.***

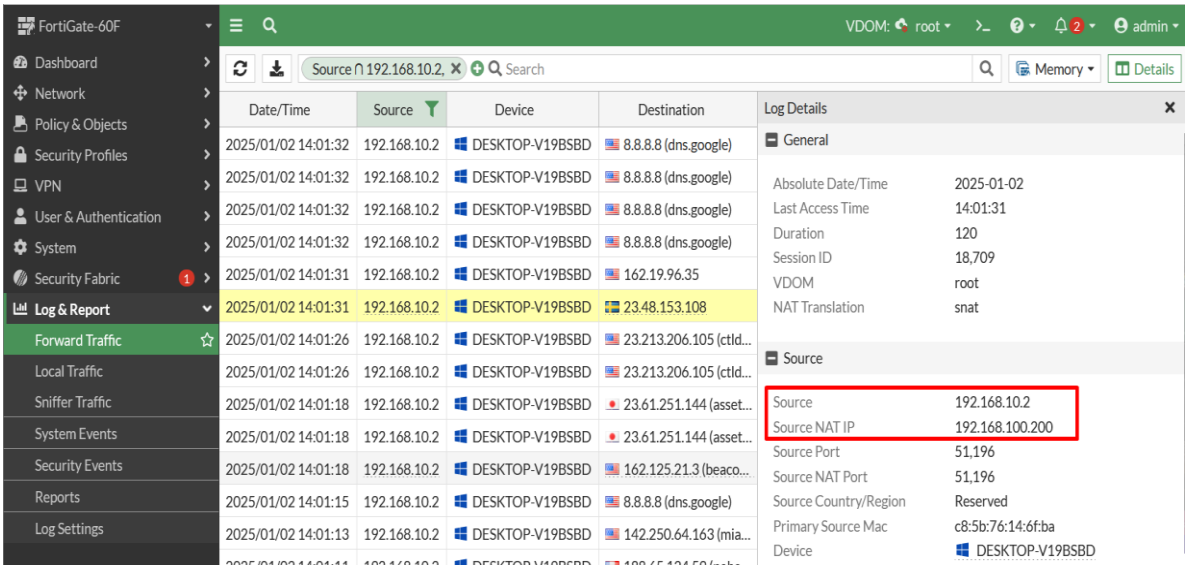


Figura 5.8-9: Revisión de logs con la nueva IP de SNAT.

Configuración de SNAT en VDOM-A.

Paso 1: Crear ruta por defecto desde el VDOM-A hacia el vdom root.

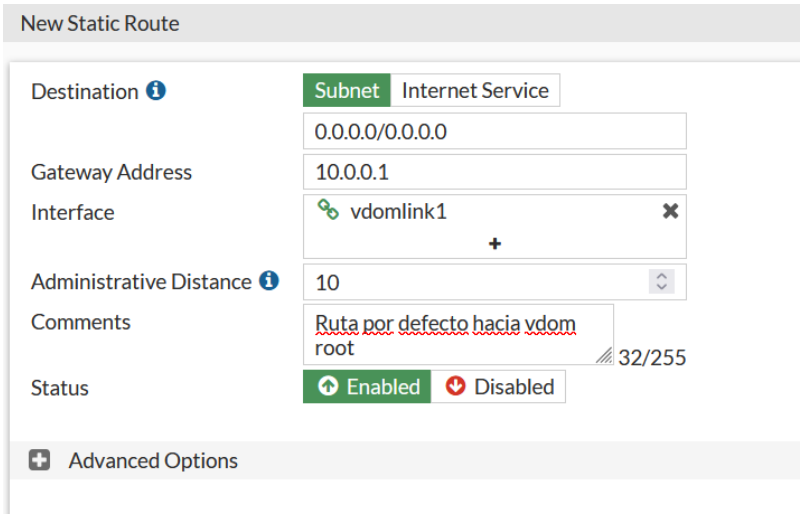


Figura 5.8-10: Ruta por defecto en vdom A.

Paso 2: Crear política de seguridad en vdom A que permita el tráfico desde la red 192.168.20.0/24 hacia todas redes (representado por el objeto ALL).

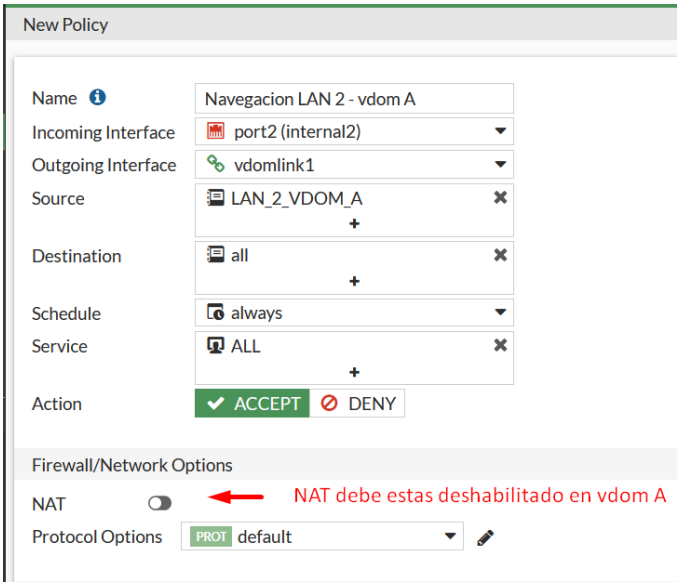


Figura 5.8-11: Política en vdom A.

Paso 3: A continuación, creamos la política de seguridad en vdom root en esta política debemos activar el SNAT.

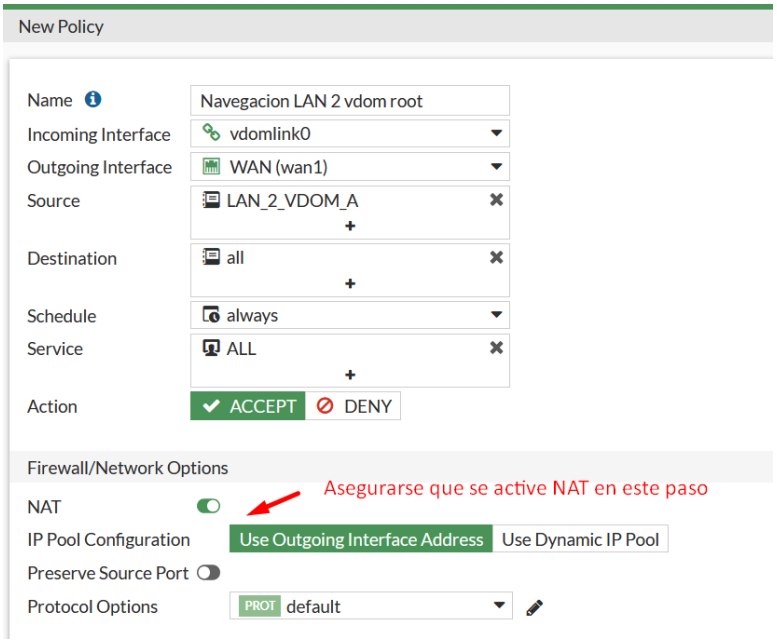


Figura 5.8-12: Política de SNAT para LAN2 en vdom root.

Paso 4: Conectar la computadora en el *port2* del FortiGate y colocarle la siguiente IP estática.

IP: 192.168.20.2
Mascara: 255.255.255.0
Puerta de enlace: 192.168.20.1
DNA: 8.8.8.8

Paso 5: Revisar los Logs en el ambos vdom para confirmar que estén registrando el tráfico.

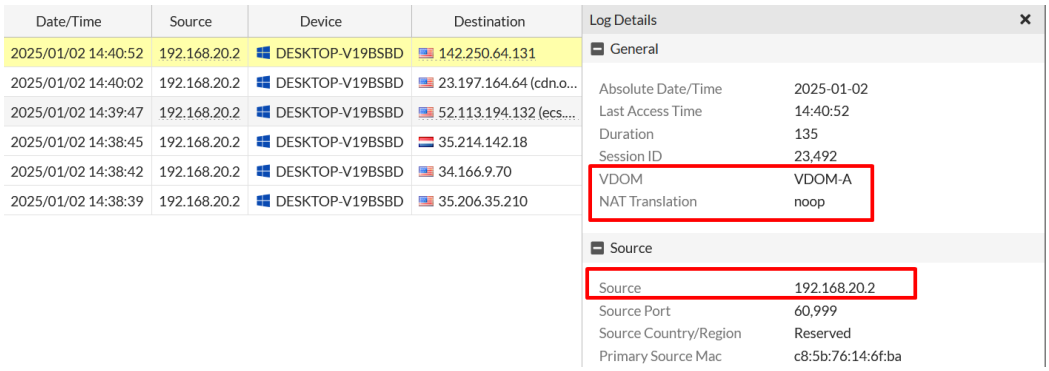


Figura 5.8-13: Revisión de LOGs en vdom A.

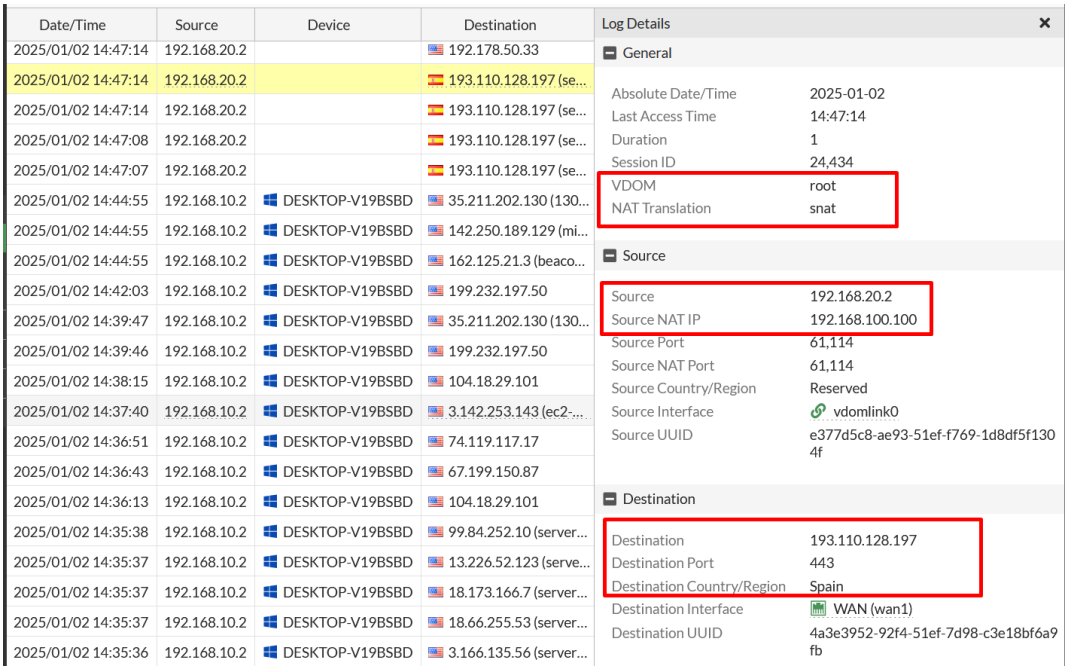


Figura 5.8-14: Revisión de LOGs en vdom root.

Notar que el vdom root ya no logra detectar el hotsname del dispositivo esto es debido a que ya no está directamente conectado.

Conclusiones

- Se aplicó correctamente el concepto de NAT haciendo la traslación de IP para dar navegación a una LAN directamente conectada y a una LAN remota que existe en otro dispositivo de red.
- Usando el concepto de IP Pool se configuro exitosamente para hacer sobrecarga de puertos a una IP diferente a la WAN del FortiGate.

5.9 Práctica 9: Servidor DHCP.

Introducción

En la presente práctica se configurará el servicio DHCP en el FortiGate para asignar dinámicamente direccionamiento IP a los dispositivos de una LAN.

Objetivo general

- Configurar asignación dinámica de direccionamiento IP usando el servicio DHCP

Objetivos específicos

- Crear política de seguridad para permitir tráfico desde la LAN hacia internet
- Monitorear la asignación de direccionamiento IP desde el firewall

Desarrollo

Como se muestra en la figura 5.9-1 se debe configurar la topología de red en la cual en el port1 del FortiGate se asigne direccionamiento dinámico para la red 10.0.0.0/24.

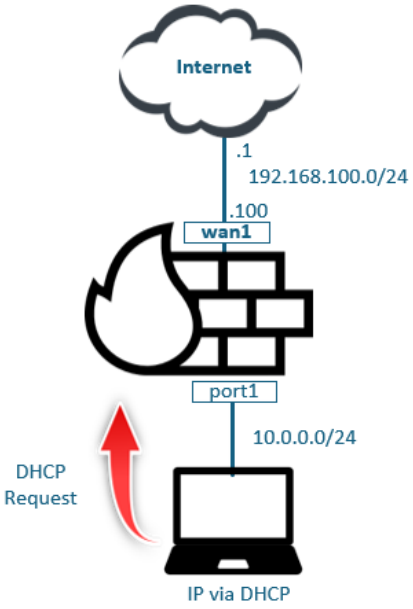


Figura 5.9-1: Topología de DHCP.

Configuración de DHCP

Paso 1: Configurar el port1 con el direccionamiento IP que muestra la Figura 5.9-2 para esto nos vamos a ***Network > Interfaces***

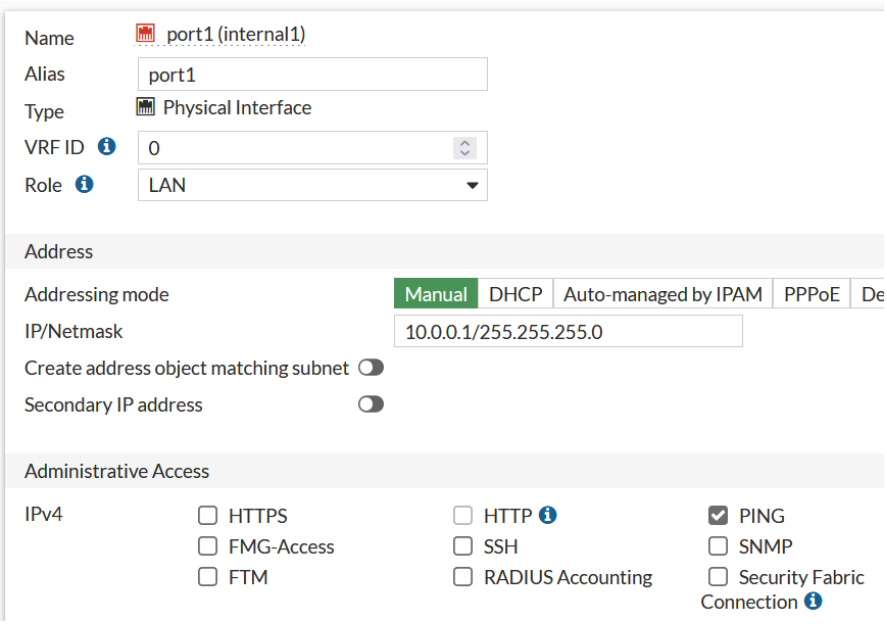


Figura 5.9-2: Configuración IP de port1.

Paso 2: Siempre dentro de las configuraciones de la interfaz debemos activar la opción de DHCP Server para que se nos desplieguen las opciones.

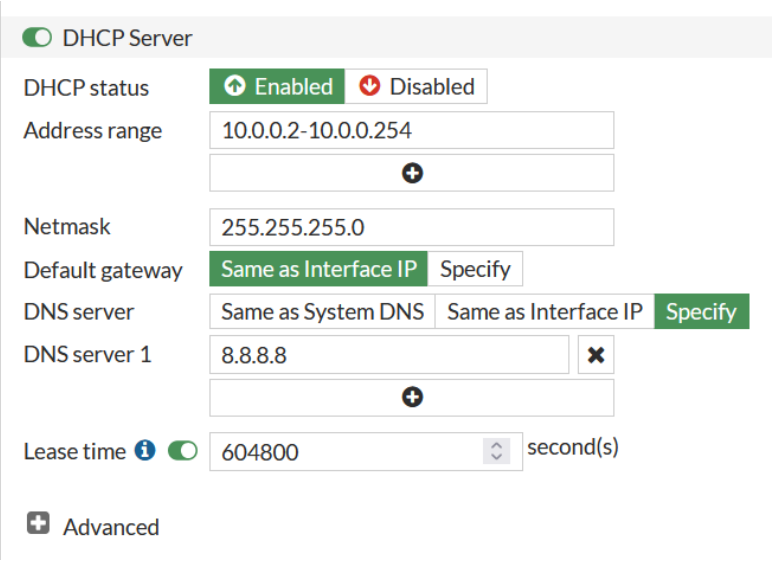


Figura 5.9-3: Configuración IP de port1.

Notar en la figura 5.9-3 que hemos especificado el servidor DNS 8.8.8.8 que pertenece a Google, en este punto se puede configurar cualquier DNS público o interno que tengamos en nuestra red.

Configuración de política

Paso 1: Ahora procederemos a crear la política para esto nos vamos a ***Policy & Object > Firewall Policy*** y creamos una nueva.

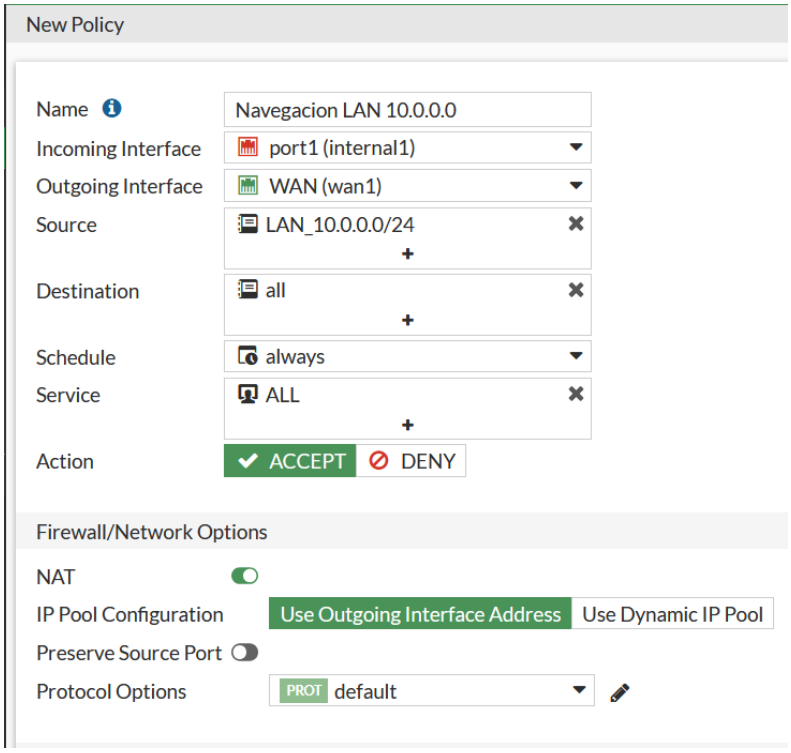


Figura 5.9-4: Política de seguridad para el DNAT.

En la Figura 5.9-4 se observa que hemos activado la opción de NAT como vimos en la practica 8 para dar navegación a toda la LAN.

Pruebas

Prueba 1: Conectar una máquina al port1 del FortiGate y asegurarse que se le asigne direccionamiento IP de forma dinámica para esto nos vamos a ***Dashboard > DHCP Monitor***

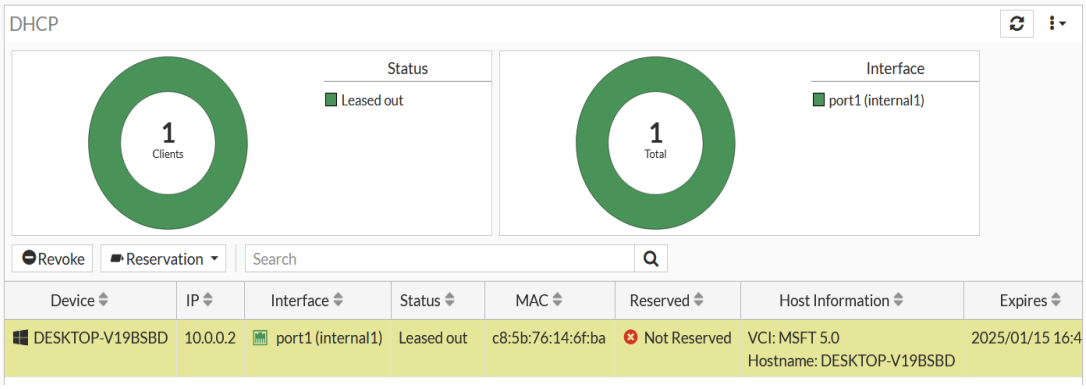


Figura 5.9-5: Monitoreo de clientes DHCP en el FortiGate.

Prueba 2: Navegar por internet desde la máquina que conectamos y revisar el tráfico en Log ***& Report > Forward traffic***

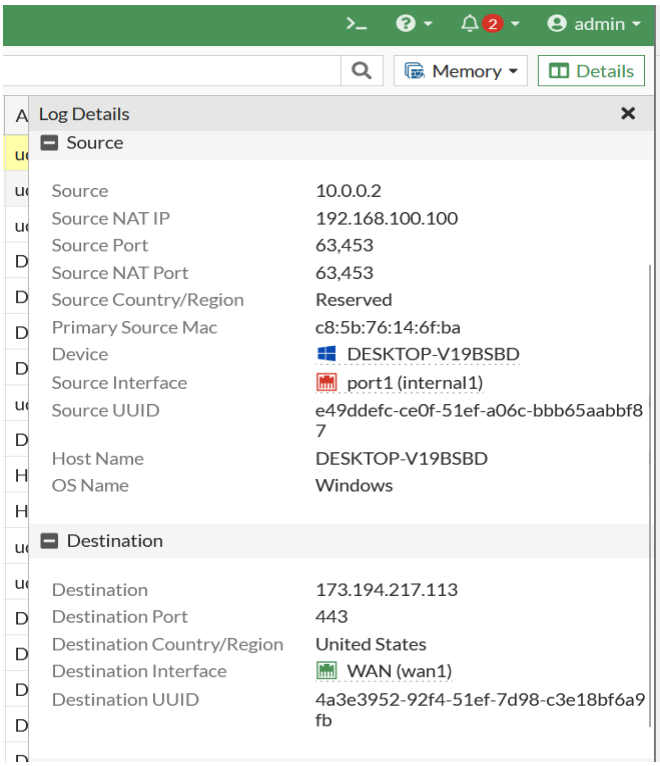


Figura 5.9-6:Revisión de logs.

Conclusiones

- Se realizó la asignación dinámica de direcciones IP de forma exitosa, se observa que es de una manera sencilla y se tiene el control grafico del inventario de direcciones que se han concedido.

- Se creó una política de seguridad con SNAT que permitió darle navegación a la máquina que conectamos en la LAN sin restricciones.

- Se presentó una forma de monitorear los dispositivos y las direcciones IP que tienen asignadas.

5.10 Práctica 10: Perfil para control de aplicaciones.

Introducción

En la presente práctica se aplicarán perfiles de seguridad a las políticas que permiten el tráfico hacia internet, específicamente se estará configurando un perfil para controlar aplicaciones específicas, en ese sentido se establecerá cuales estarán permitidas y cuáles serán bloqueadas.

Objetivo general

- Configurar un perfil para controlar las aplicaciones permitidas y denegadas.

Objetivos específicos

- Conocer las características de seguridad para control de tráfico que posee el FortiGate
- Monitorear el tráfico permitido o bloqueado por el perfil de seguridad.

Desarrollo

Partiendo de la topología básica que se muestra en la figura 88 de una computadora conectada al port1 del lado de la LAN se configurará un perfil de seguridad para el tráfico que atraviesa el firewall y establecer que aplicaciones están permitidas o bloqueadas.

Vamos a partir de que las configuraciones base ya están aplicadas, es decir, que la LAN ya está configurada con DHCP y que ya existe una política de navegación.

Nos centraremos en la configuración nueva que es para el control de aplicaciones.

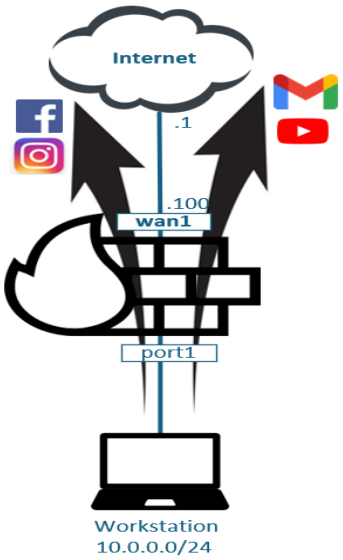


Figura 5.10-1: Topología para control de aplicaciones.

Configuración de control de aplicaciones.

Paso 1: Para configurar el control de aplicaciones nos vamos al siguiente menú ***Security Profiles > Application Control*** y creamos un nuevo perfil.

Podremos a seleccionar categorías para permitir completamente grupos de URL que Fortinet tiene perfiladas.

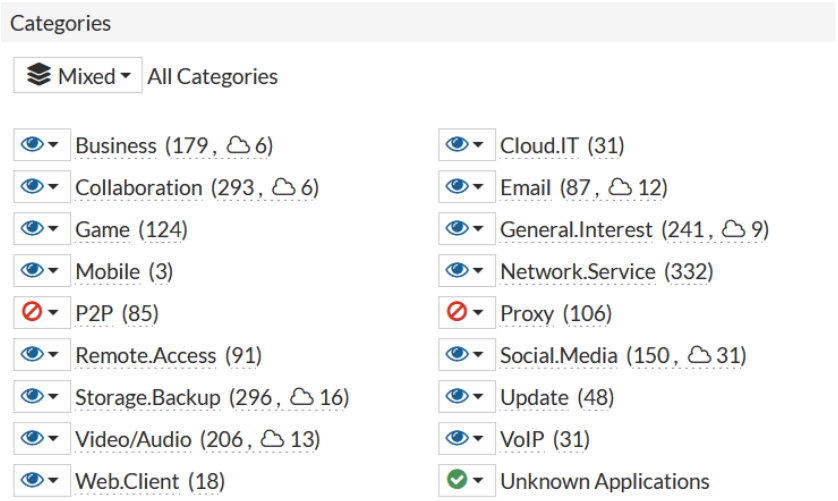


Figura 5.10-2: Categorías en el FortiGate predefinidas.

También tenemos la opción de hacer una sobreescritura de aplicaciones, es decir, que si permitimos una categoría tenemos la opción de bloquear una aplicación especifica.

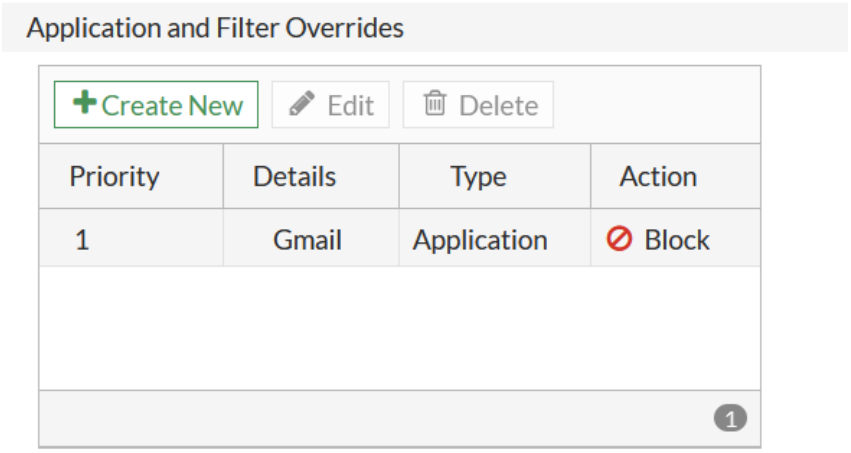


Figura 5.10-3: Sobreescritura de aplicaciones.

Paso 2. Ahora procedemos a configurar nuestro perfil, para esto vamos a establecer todas las aplicaciones en Allow y vamos a bloquear la aplicación de Facebook.

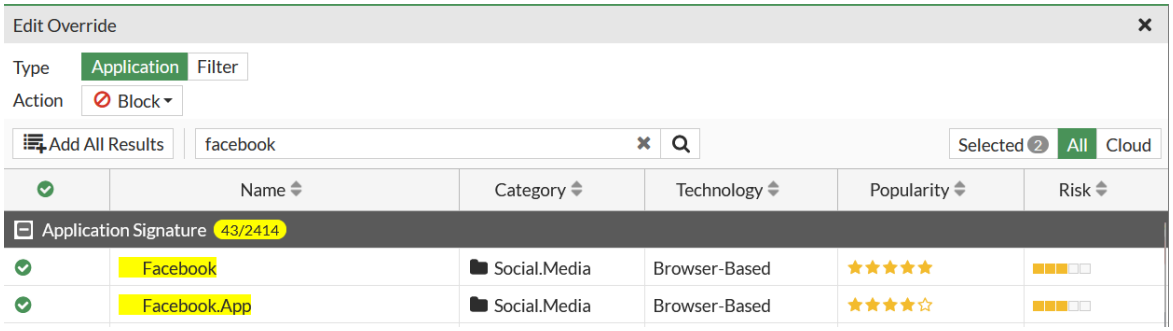


Figura 5.10-4: Sobreescritura de aplicación Facebook.

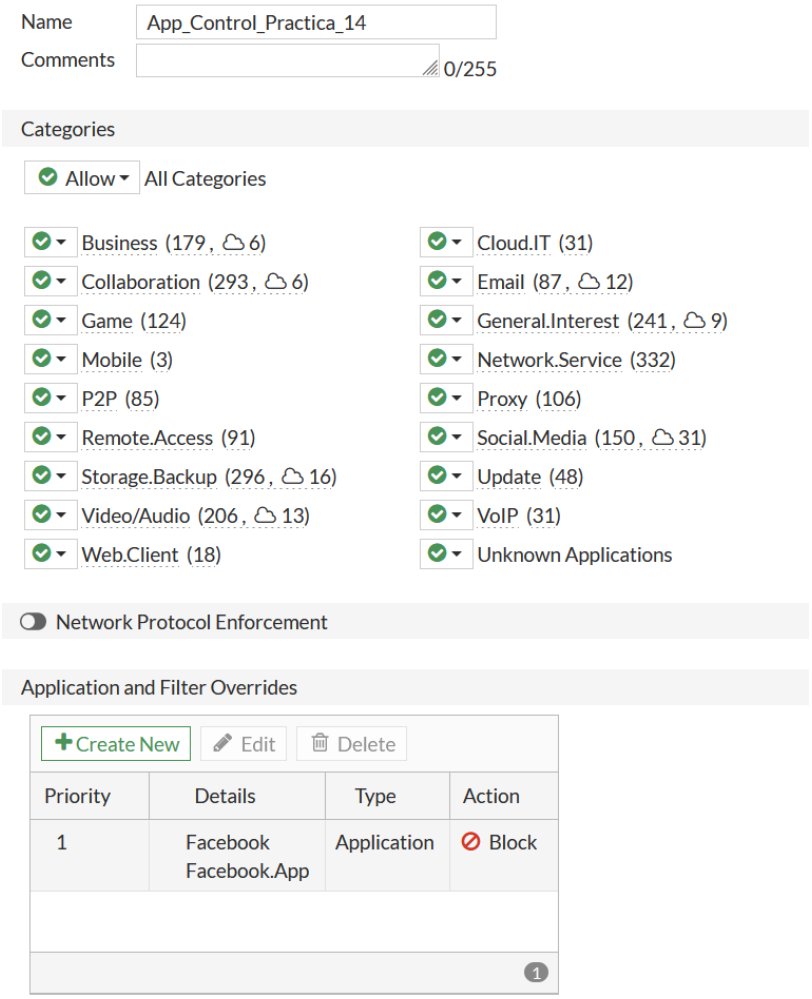


Figura 5.10-5: Perfil para control de aplicaciones.

Aplicar perfil de en política de ipv4

Paso 1: Para aplicar el perfil de control de aplicaciones que creamos nos vamos a ***Policy & Objects > Firewall Policy*** y editamos la política existente para navegación.

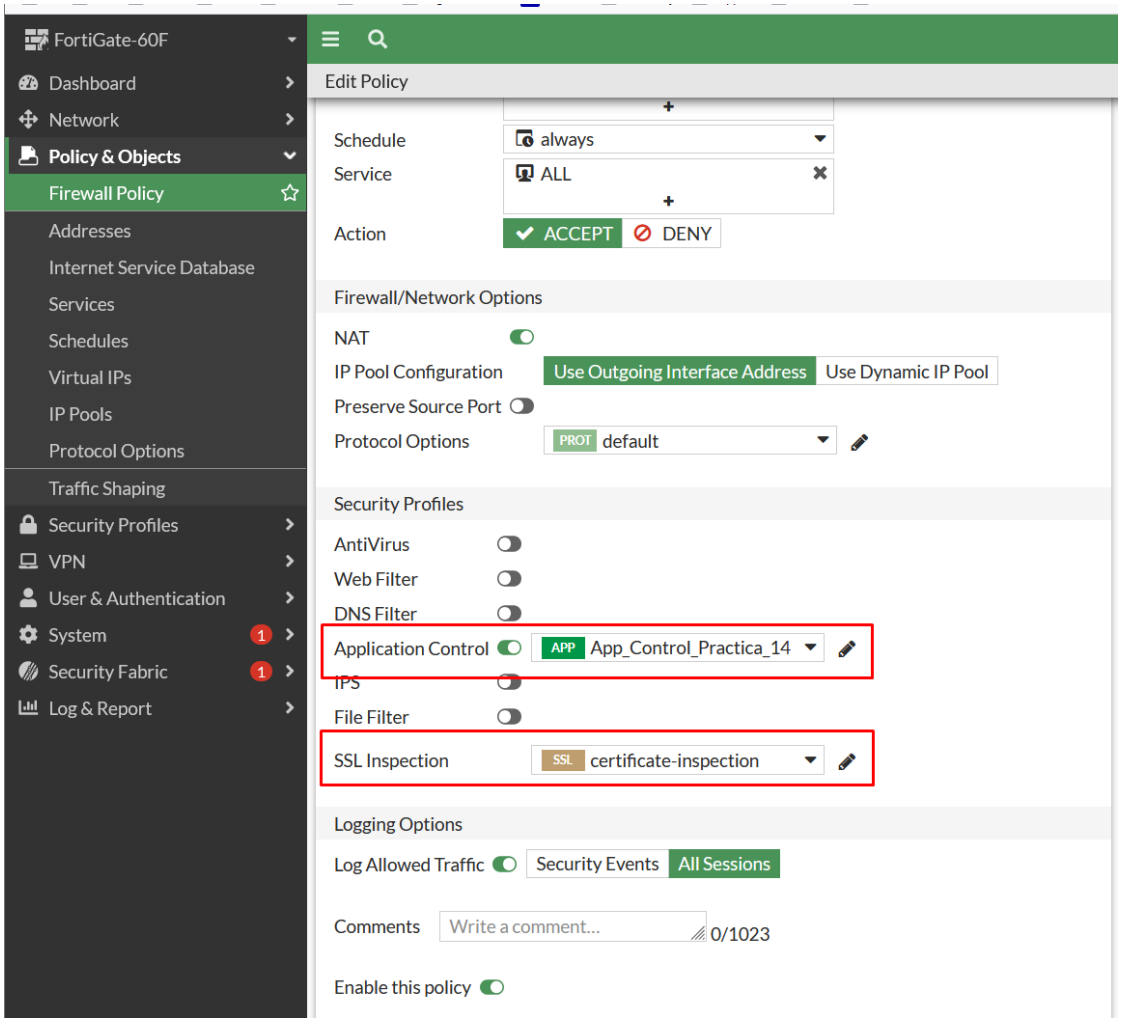


Figura 5.10-6: Aplicando perfil para control de aplicaciones en política.

Pruebas y monitoreo de tráfico

Prueba 1: Desde la computadora que tenemos en nuestra LAN cargamos la página de Facebook y miramos los resultados.

Como se observa en la Figura 5.10-7, la computadora tiene la IP 10.0.0.2 y la pagina de Facebook no está cargando, muestra un mensaje que no se puede acceder al sitio.

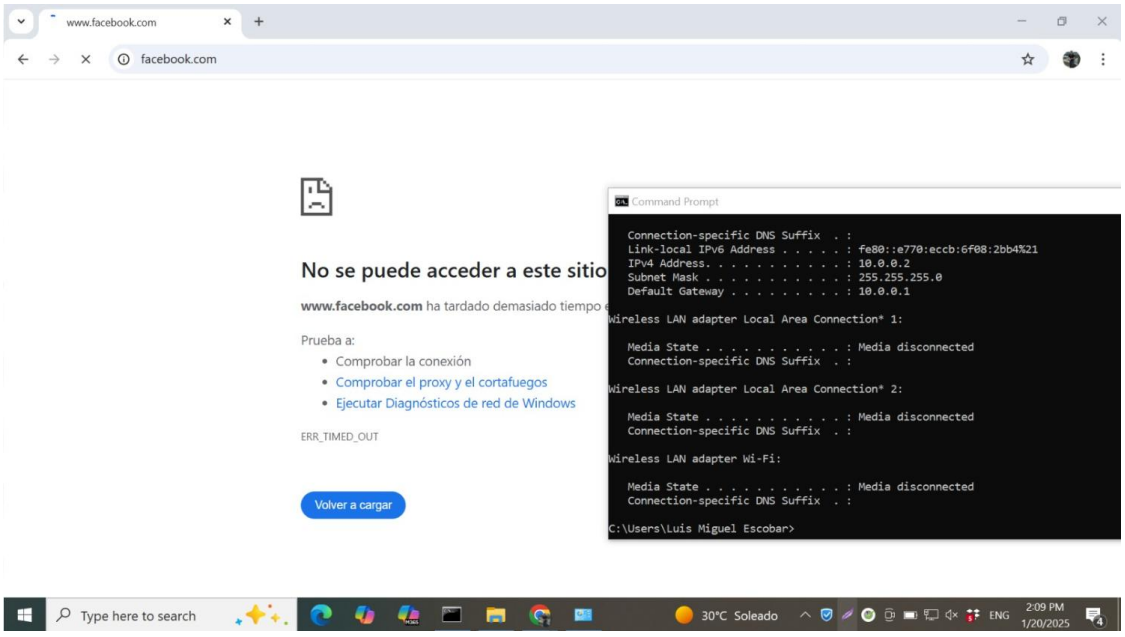


Figura 5.10-7: Mensaje al intentar cargar página de Facebook.

Ahora nos vamos a revisar los LOG en el firewall para identificar si el evento nos quedó registrado.

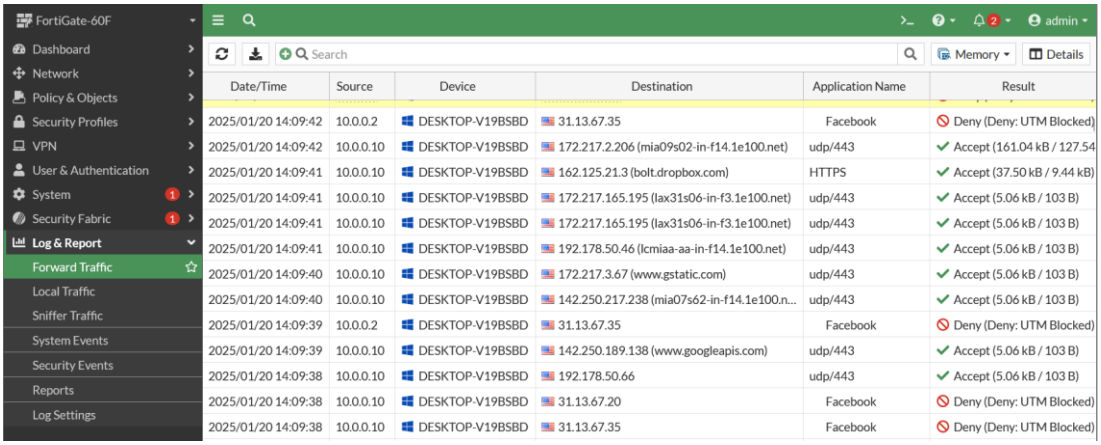


Figura 5.10-8: Eventos de bloqueo hacia Facebook.

Hacemos doble click sobre el evento para ver los detalles de la razón por la que fue bloqueado.

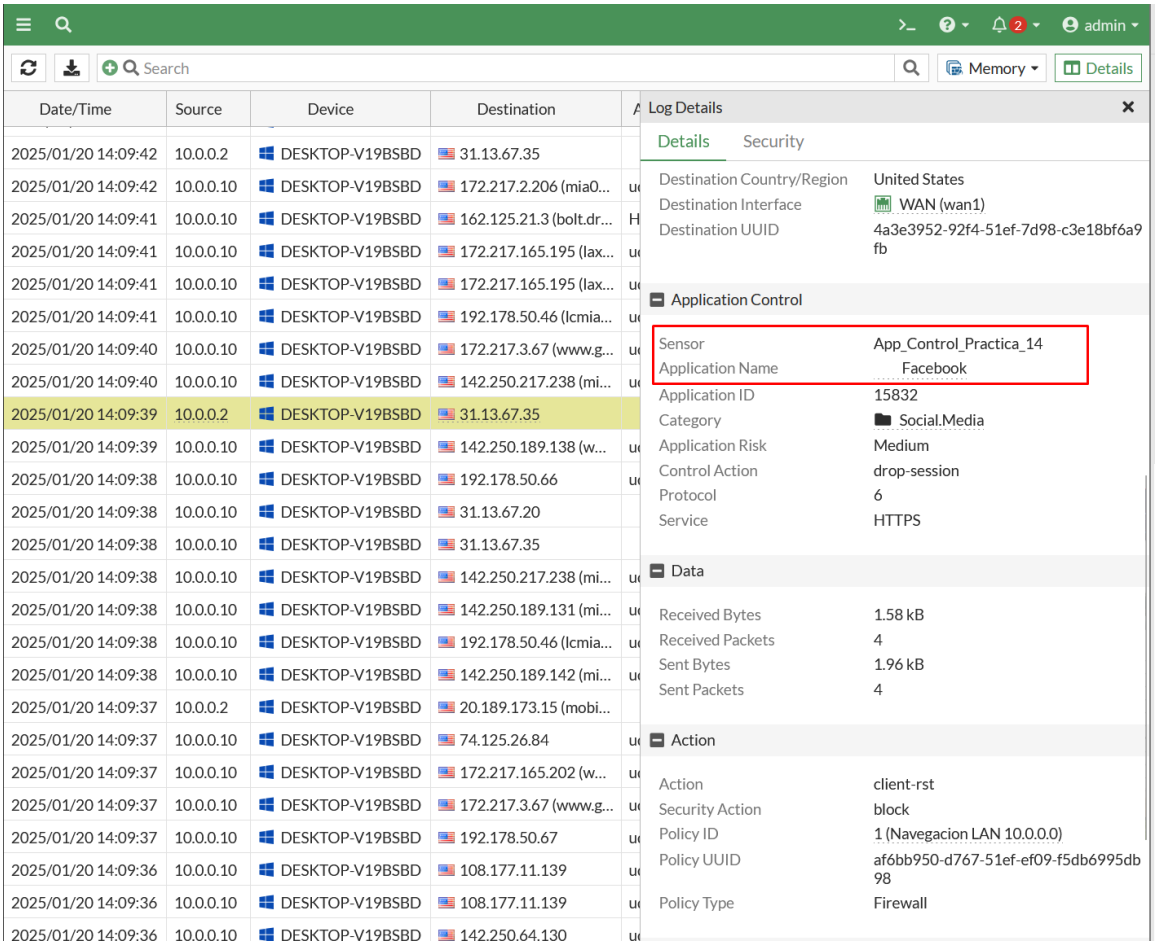


Figura 5.10-9: Detalle de eventos de bloqueo hacia Facebook.

Prueba 1: Modificar el perfil de control de aplicaciones y en lugar de bloquearlo lo permitiremos.

Para esto pondremos en estado de ***monitor*** para que nos genere un evento que podamos registrar en los LOG.

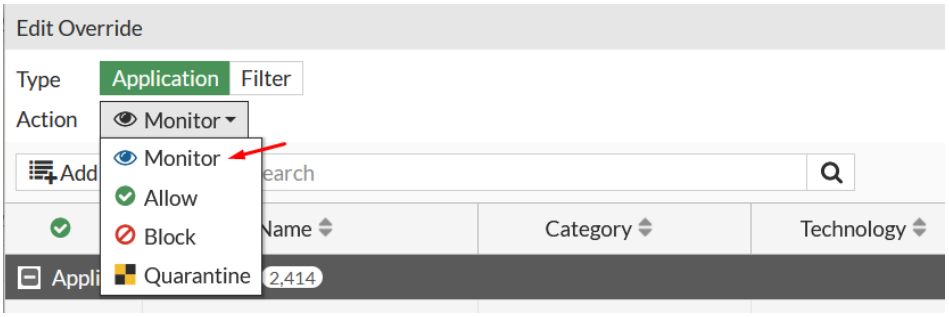


Figura 5.10-10: Cambiando el tipo de acción a "Monitor".

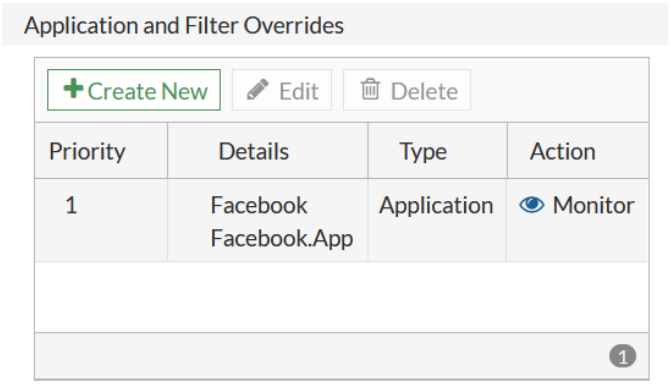


Figura 5.10-11: Aplicando el cambio al tipo de acción en el perfil.

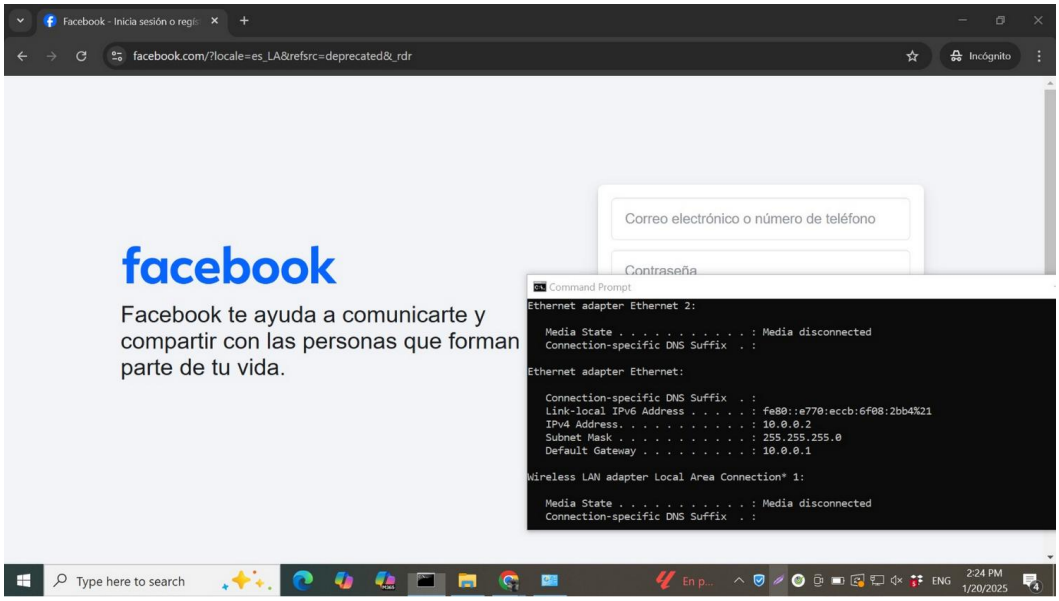


Figura 5.10-12: Ahora la aplicación ya está permitida y monitoreada.

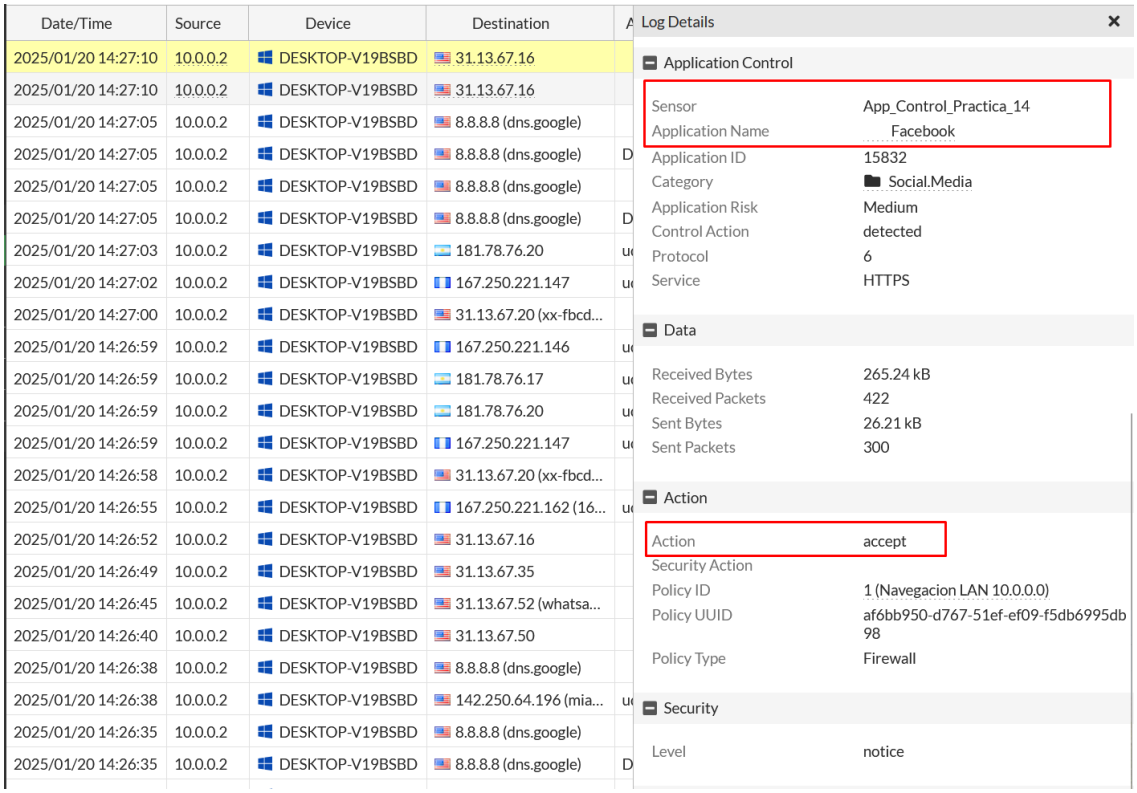


Figura 5.10-13: Registro del FortiGate que permite la aplicación.

Conclusiones

- Se configuró exitosamente un perfil para permitir o bloquear aplicaciones específicas que queramos controlar en nuestra red interna.

- Luego de realizar la práctica se observa que esta característica de seguridad es intuitiva y fácil de configurar, contrario a otras soluciones de otras tecnologías que implican procesos más complicados para lograr la misma acción.

- Se revisaron los eventos y se observó que todos quedan registrados para posterior analizar de lo que está pasando en nuestra red.

5.11 Práctica 11: Políticas de Traffic Shapping.

Introducción

En la presente práctica se aplicará un perfil de ***Traffic Shaping*** a una red específica para limitar o garantizar tráfico y así mantener una calidad de servicio en nuestra red interna para evitar saturaciones por tráfico con origen identificado.

Objetivo general

- Limitar el tráfico de un origen especifico usando políticas de T***raffic shaping***

Objetivos específicos

- Explicar la diferencia entre ancho de banda garantizado y ancho de banda máximo en un perfil de ***Traffic shapers.***
- Medir las velocidades de internet antes y después de aplicar el perfil de ***Traffic shaping***

Desarrollo

Partiendo de la topología que se muestra en la Figura 5.11-1 de una computadora conectada al port1 del lado de la LAN se configurará un ***Traffic Shapers*** para limitar el tráfico originado desde la LAN 10.0.0.0/24.

Las configuraciones base ya están aplicadas, es decir, que la LAN ya está configurada con DHCP y que ya existe una política de navegación.

Nos centraremos en la configuración del ***Traffic Shapers*** y de la política de ***Traffic Shaping.***

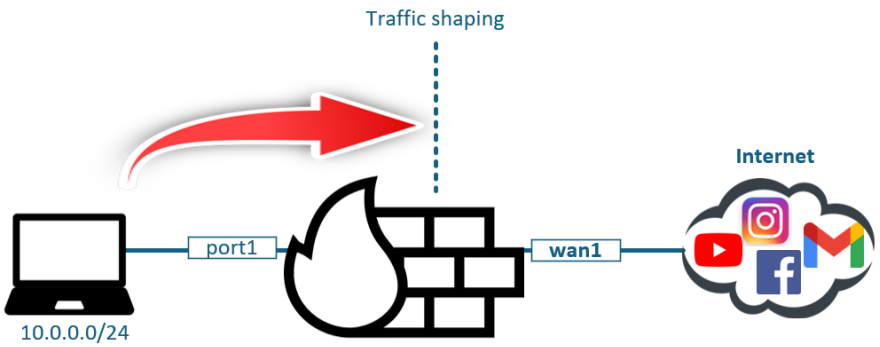


Figura 5.11-1: Topología para establecer política de Traffic Shaping.

Configuración de Traffic Shapers.

Paso 1: Para configurar el perfil nos iremos al siguiente menú ***Policy & Objects > Traffic Shaping*** y creamos un nuevo **Traffic Shapers** y le establecemos un valor máximo de 1024 kbps que es lo mismo que 1 Mbps.

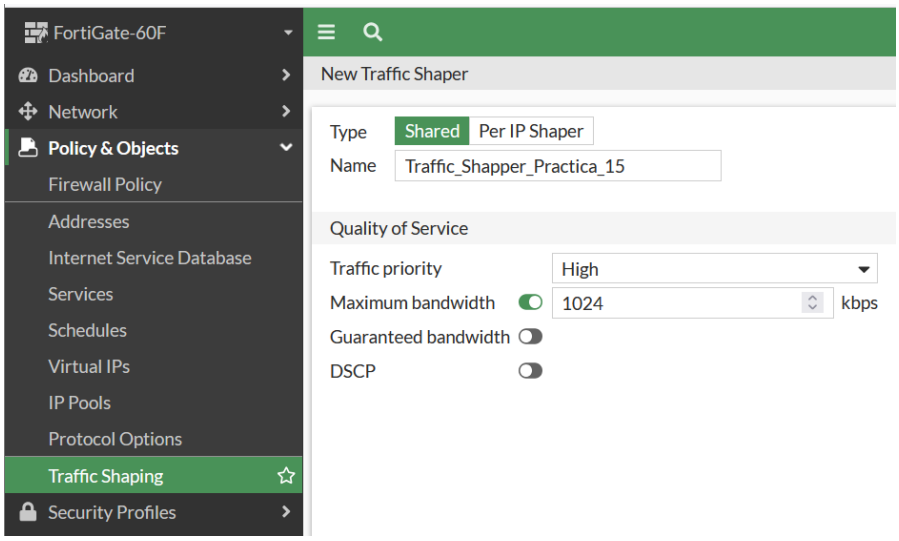


Figura 5.11-2: Configuración de Traffic Shapers.

Debemos notar que tenemos una opción de ***Guaranteed bandwidth*** donde podemos establecer un valor especifico que este reservado para la red a la que se aplique este ***Traffic Shapper***, esto parámetro nos es útil cuando queremos aplicar calidad de servicio a los servicios de telefonía IP.

Configuración de política de Traffic Shaping

Paso 1: Nos movemos en la pestaña de Traffic Shaping Policies y creamos una nueva.

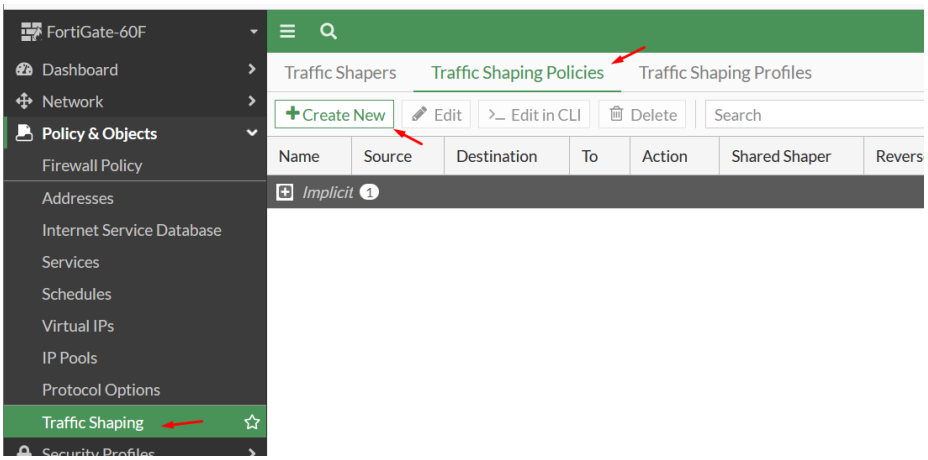


Figura 5.11-3: Menú para política de Traffic Shaping.

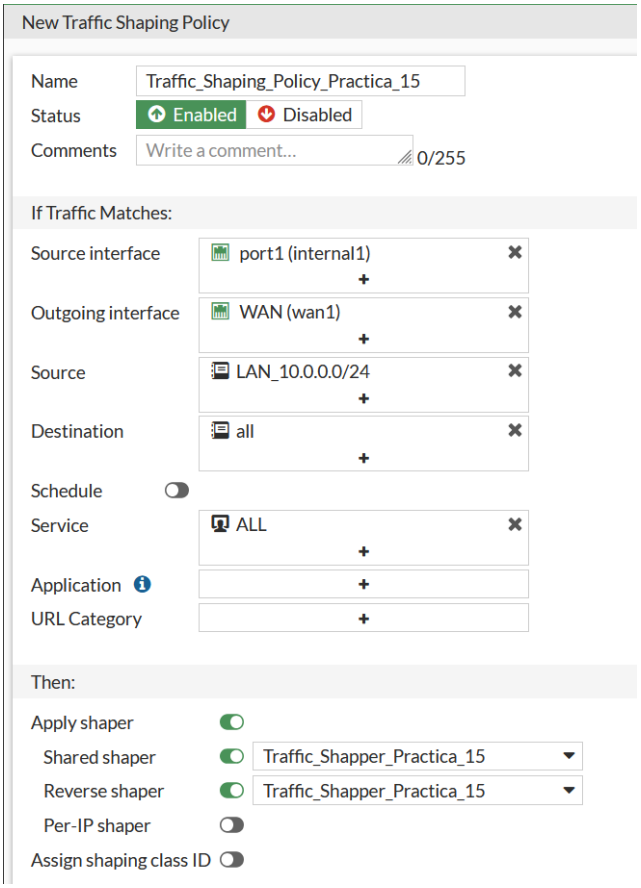


Figura 5.11-4: Nueva política de Traffic Shaping.

Como se muestra en la Figura 5.11-4, habilitamos la opción de ***Apply shaper*** y aplicamos el Traffic Shapers que creamos en el paso anterior.

Pruebas y monitoreo de trafico

Prueba 1: Desde la computadora conectada en la LAN correr una prueba de velocidad y documentar la velocidad que registra el dispositivo.

Figura 5.11-5: Registro de velocidad con Traffic Shaping Policy.

Como se observa en la Figura 5.11-5 el registro del ancho de banda disponible fue de aproximadamente 1024 kbps que fue lo que establecimos en nuestra política, la variación se debe a que siempre hay ancho de banda que el sistema Windows utiliza para su conexión hacia Microsoft.

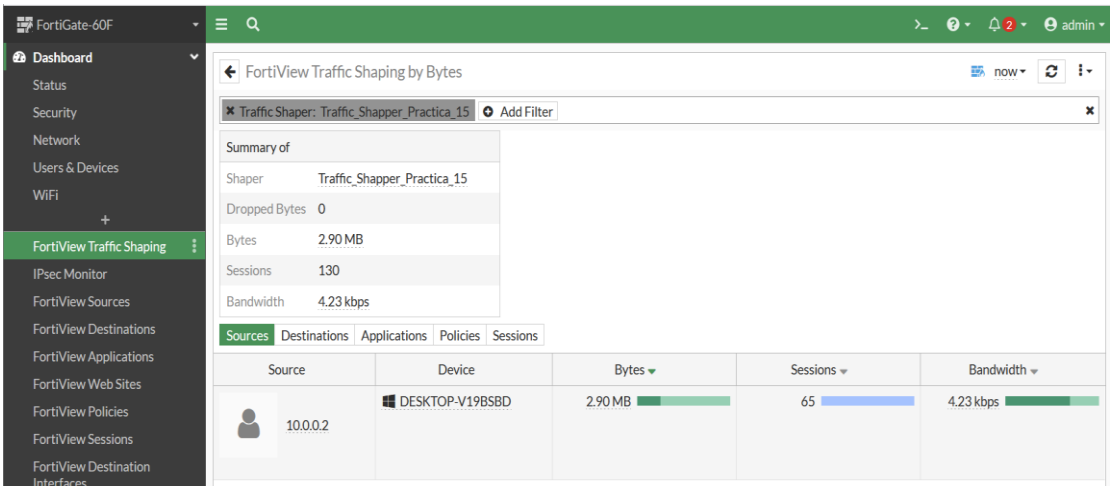


Figura 5.11-6 Monitoreo de sesiones desde Fortiview.

Si monitoreamos las sesiones desde el menú ***Dashboard > Foriview Traffic Shaping*** podemos ver todo el tráfico que limitó nuestra política.

Prueba 2: Aumentar el ancho de banda en el traffic shapers a 10 Mbps o el equivalente de 10240 kbps y registrar la lectura de la prueba de velocidad.

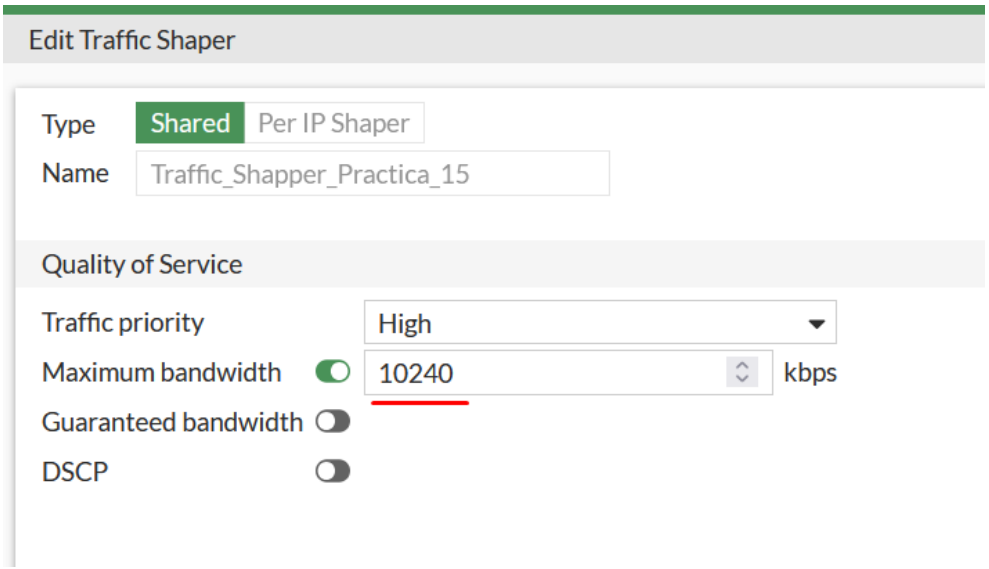


Figura 5.11-7 Aumento de velocidad en el Traffic Shapers.

Figura 5.11-8: Registro de la velocidad al incrementar el ancho de banda.

El valor que obtuvimos ahora es cercano a los 10 Mbps que configuramos.

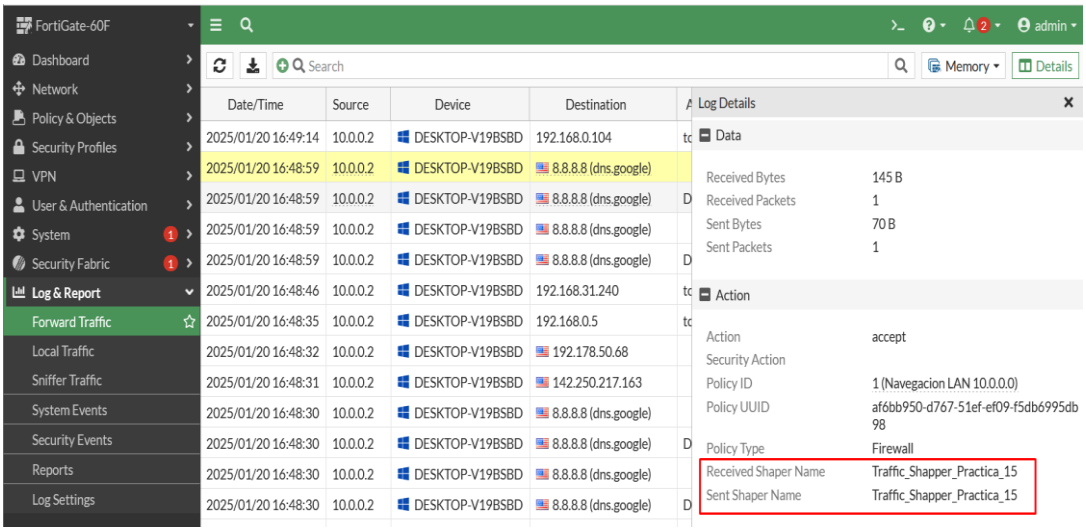


Figura 5.11-9: Revisión de LOG.

En el menú **Log & Report > Forward Traffic** Podemos ver en los detalles que nos genera un mensaje que el tráfico se ve limitado por una política de traffic shaping.

Prueba 2: Desactivar la política de traffic shaping y volver a tomar la prueba de velocidad desde la computadora.

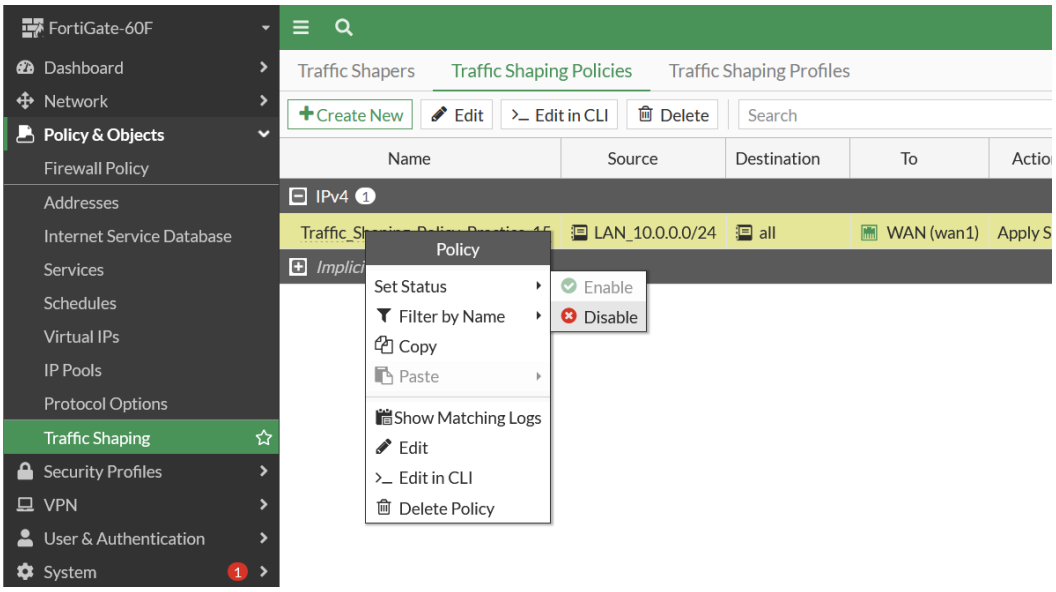


Figura 5.11-10: Desactivación de política de Traffic Shaping..

Figura 5.11-11: Registro de la velocidad sin política de Traffic Shaping.

Conclusiones

- Se configuró exitosamente la política de traffic shaping obteniendo resultados esperados, el tráfico fue gradualmente limitado desde 1 Mbps, 10 Mbps y al desactivar la política la prueba nos mostró la capacidad total de la conexión.

- Se encontró que la diferencia entre el tráfico máximo permitido y el garantizado es que uno sirve para limitar a un valor especifico y el otro sirve para dar calidad de servicio con ancho de banda garantizado a tráfico sensible a la latencia.

- Luego de tomar las lecturas de velocidad de internet antes y después de aplicar y ajustar la política confirmamos que la el ***Traffic Shaping*** está logrando su finalidad de limitar el ancho de banda disponible.

5.12 Práctica 12: Limitar tráfico por aplicaciones específicas.

Introducción

En la presente practica se aplicará un perfil de ***Traffic Shaping*** a una aplicación específica para limitar o garantizar tráfico y así mantener una calidad de servicio en nuestra red interna para evitar saturaciones por tráfico con destino identificado.

Objetivo general

- Limitar el tráfico hacia una aplicación especifica usando políticas de T***raffic shaping***

Objetivos específicos

- Implementar las ***traffic shaping policy*** con asociamos aplicaciones.
- Monitorear el tráfico hacia las aplicaciones antes y después de aplicar el perfil de ***Traffic shaping***

Desarrollo

Partiendo de la topología que se muestra en la Figura 5.12-1 de una computadora conectada al port1 del lado de la LAN se configurará un ***Traffic Shapers*** para limitar el tráfico originado desde la LAN 10.0.0.0/24 hacia las aplicaciones Mega, Instagram, YouTube y Facebook.

Las configuraciones base ya están aplicadas, es decir, que la LAN ya está configurada con DHCP y que ya existe una política de navegación.

Nos centraremos en la configuración del ***Traffic Shapers*** y de la política de ***Traffic Shaping*** por aplicación.

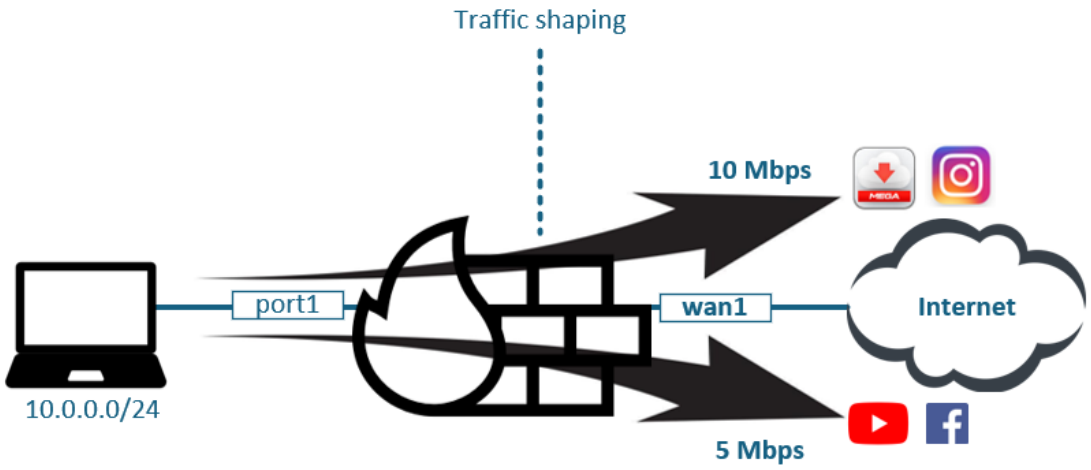


Figura 5.12-1: Topología para establecer política de Traffic Shaping.

Configuración de Traffic Shapers.

Paso 1: Para configurar el perfil nos iremos al siguiente menú ***Policy & Objects > Traffic Shaping*** y creamos dos nuevos **Traffic Shapers** y les establecemos un valor máximo de 1024 kbps y 5120 kbps respectivamente.

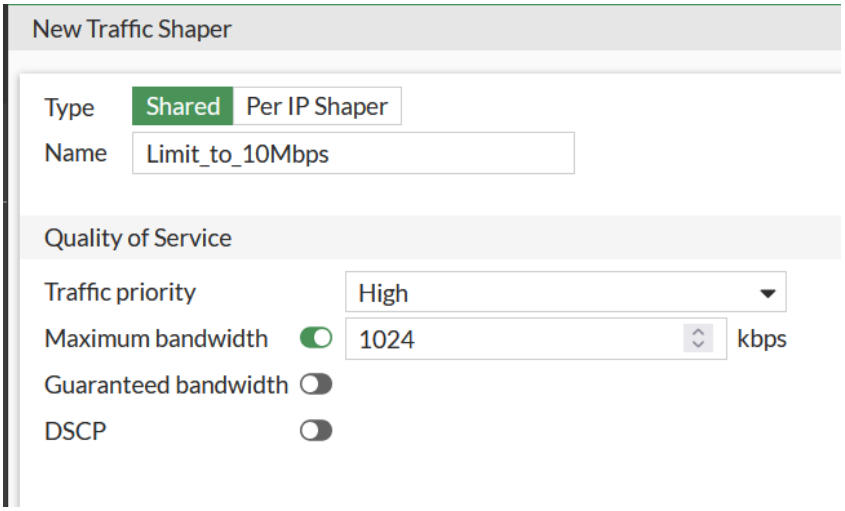


Figura 5.12-2: Configuración de Traffic Shapers de 1024 kbps.

.

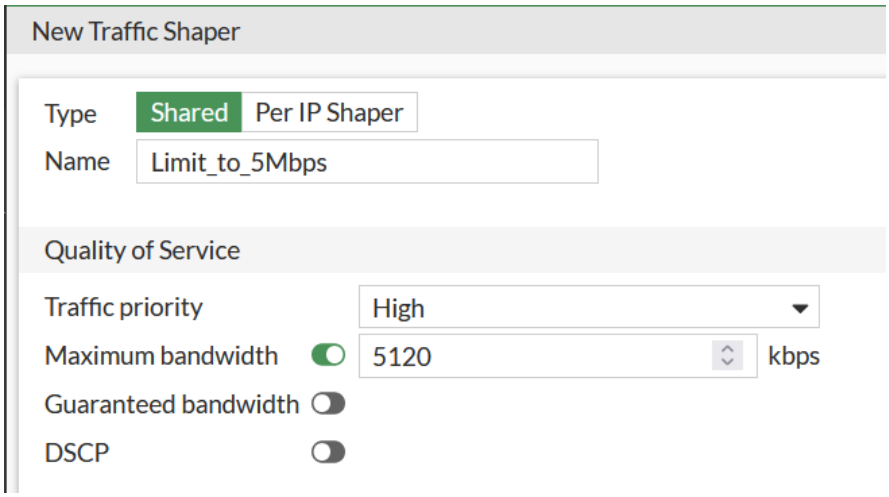


Figura 5.12-3: Configuración de Traffic Shapers de 5120 kbps.

Configuración de política de Traffic Shaping

Paso 1: Nos movemos en la pestaña de Traffic Shaping Policies y creamos una nueva.

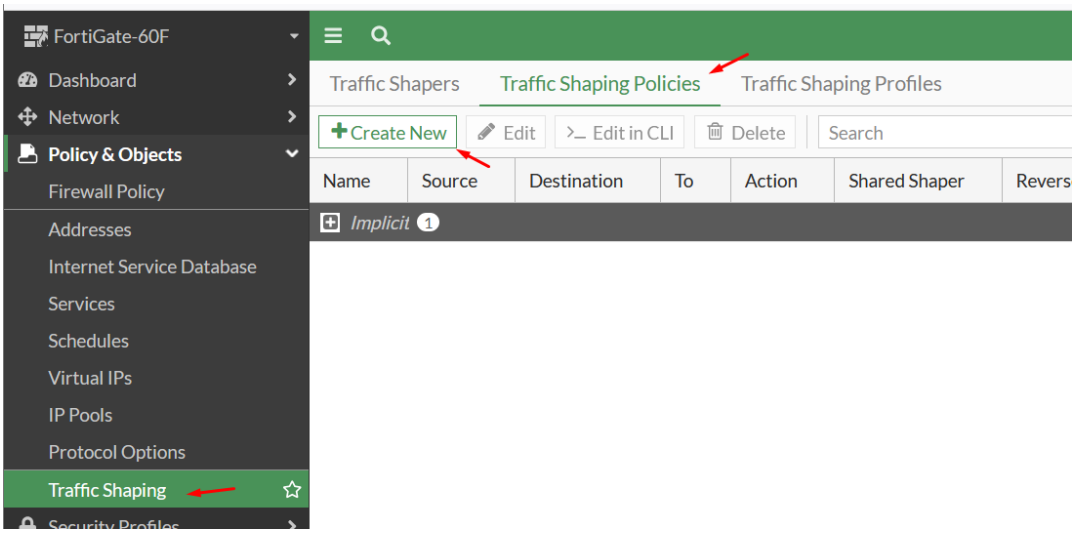


Figura 5.12-4: Menú para política de Traffic Shaping.

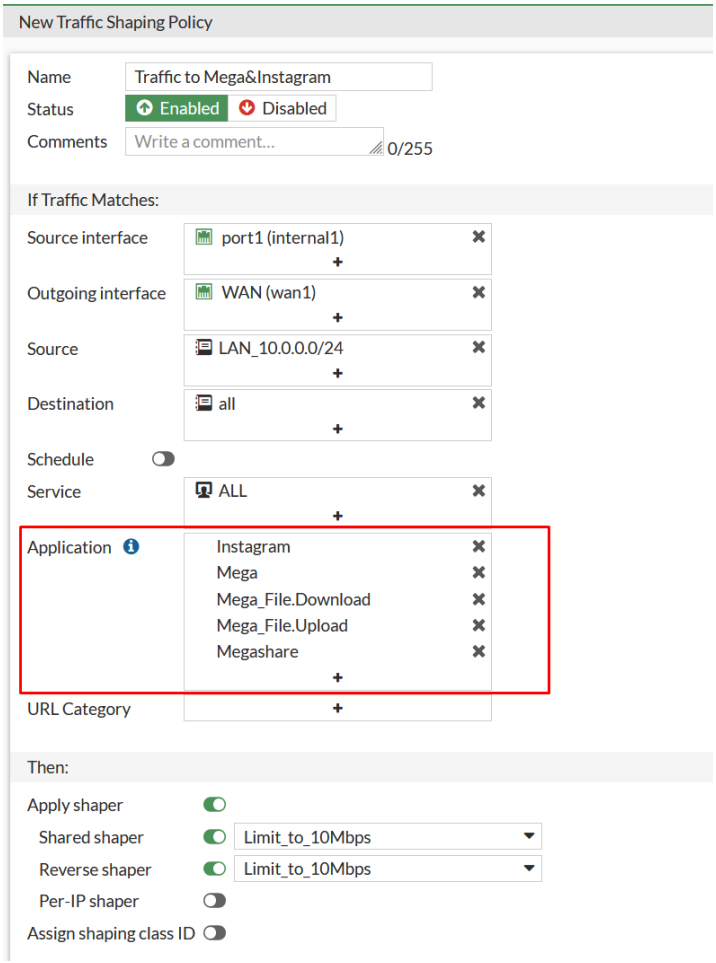


Figura 5.12-5: Política 1 de Traffic Shaping por aplicación.

.

Como se muestra en la Figura 5.12-5, habilitamos la opción de ***Apply shaper*** y aplicamos el Traffic Shapers que creamos en el paso anterior.

También creamos una política para las aplicaciones de YouTube y Facebook.

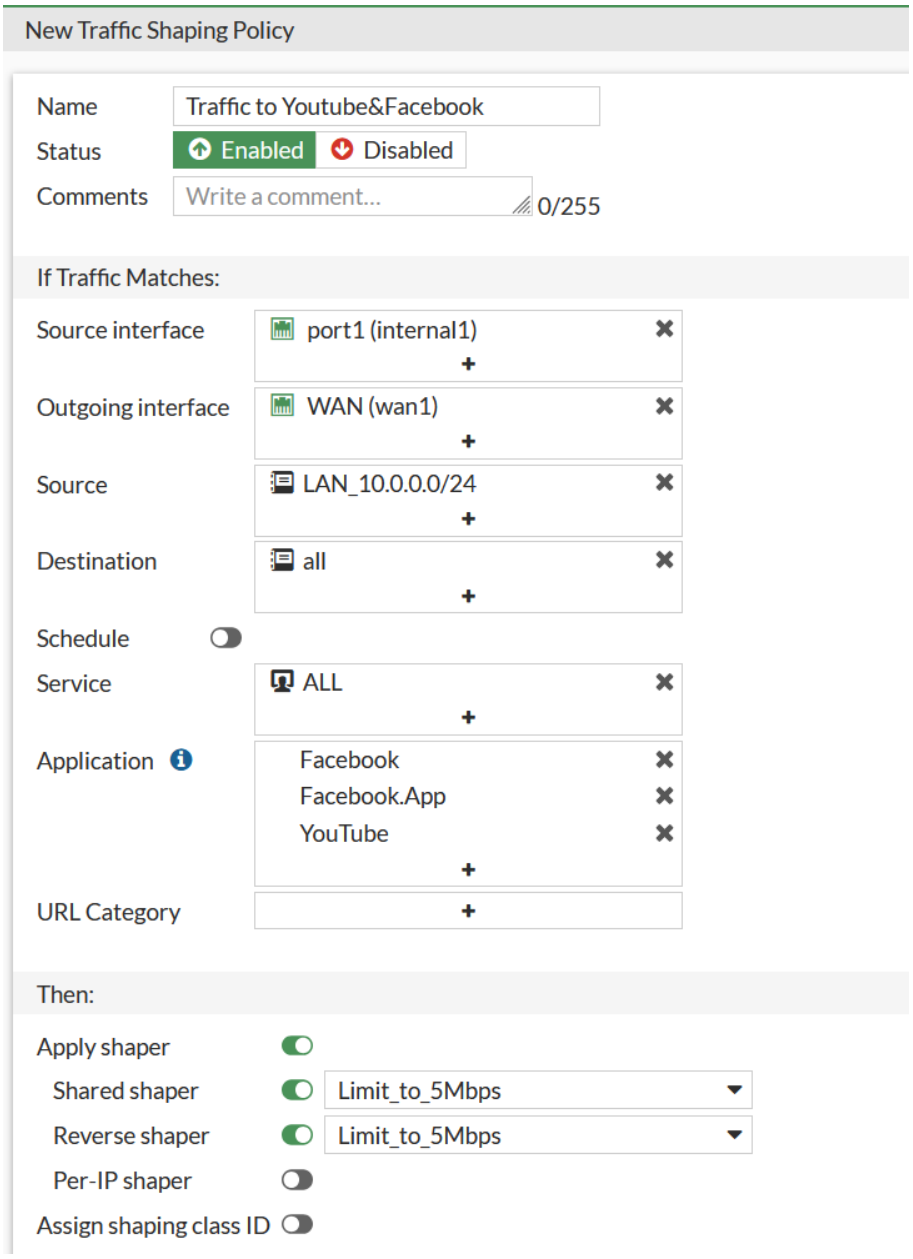


Figura 5.12-6: Política 2 de Traffic Shaping por aplicación.

Como se aprecia en las Figuras 5.12-5 y Figura 5.12-6 es posible tener nuestro tráfico limitado por aplicaciones específicas, esto nos ayuda a tener controlado lo que pasa en

nuestra LAN y evitar saturaciones de las capacidades y afectar otras aplicaciones que son más críticas.

Configuración de control de aplicaciones

Es importante que para que nuestras políticas de Traffic Shaping por aplicación funcionen correctamente debemos configurar un perfil de control de aplicaciones en la política de seguridad.

Paso 1: Nos vamos al menú ***Security Profiles > Application Control*** y creamos uno nuevo y establecemos todas las aplicaciones en **Monitor**.

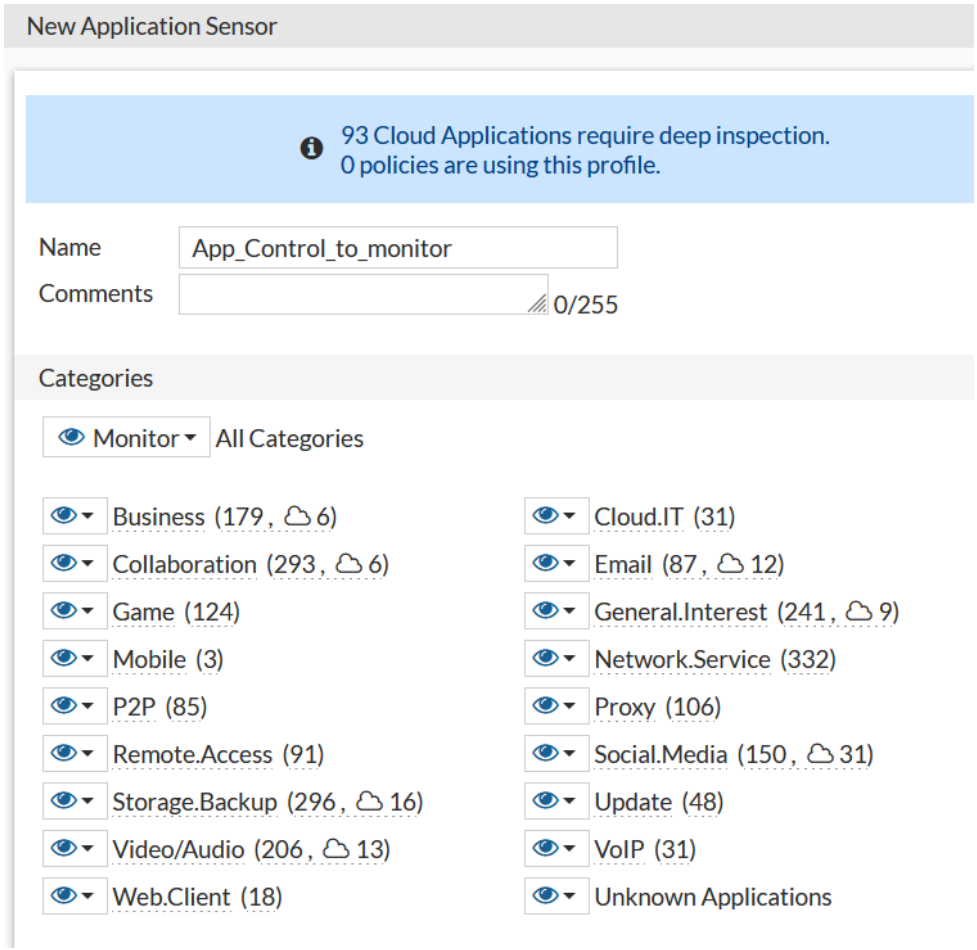


Figura 5.12-7: Control de aplicaciones.

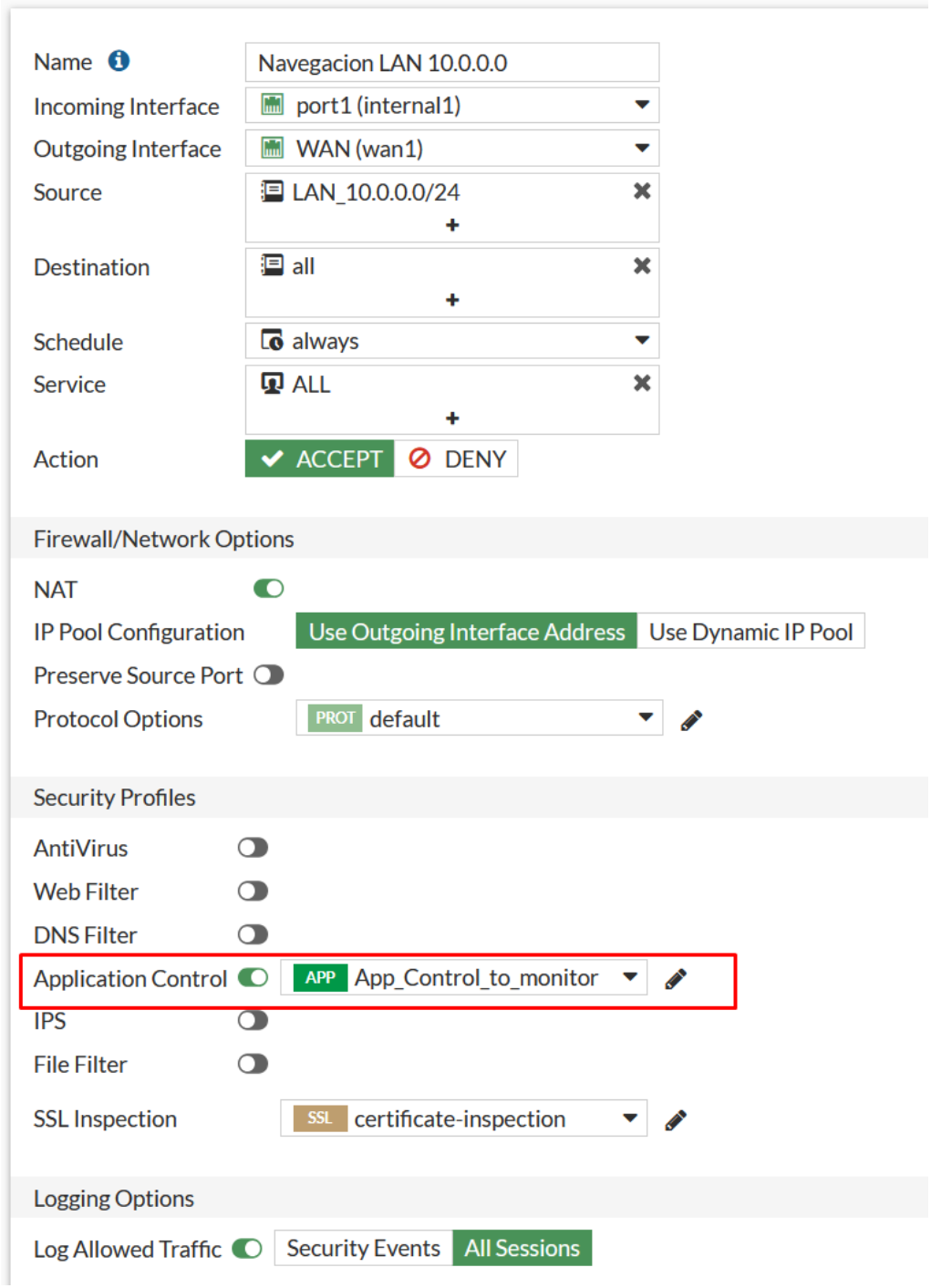


Figura 5.12-8: Configuración de control de aplicaciones en política de seguridad.

Pruebas y monitoreo de trafico

Prueba 1: Desde la computadora conectada en la LAN generar tráfico hacia YouTube y Facebook y confirmar que se le esté aplicación la política de Traffic Shaping establecida.

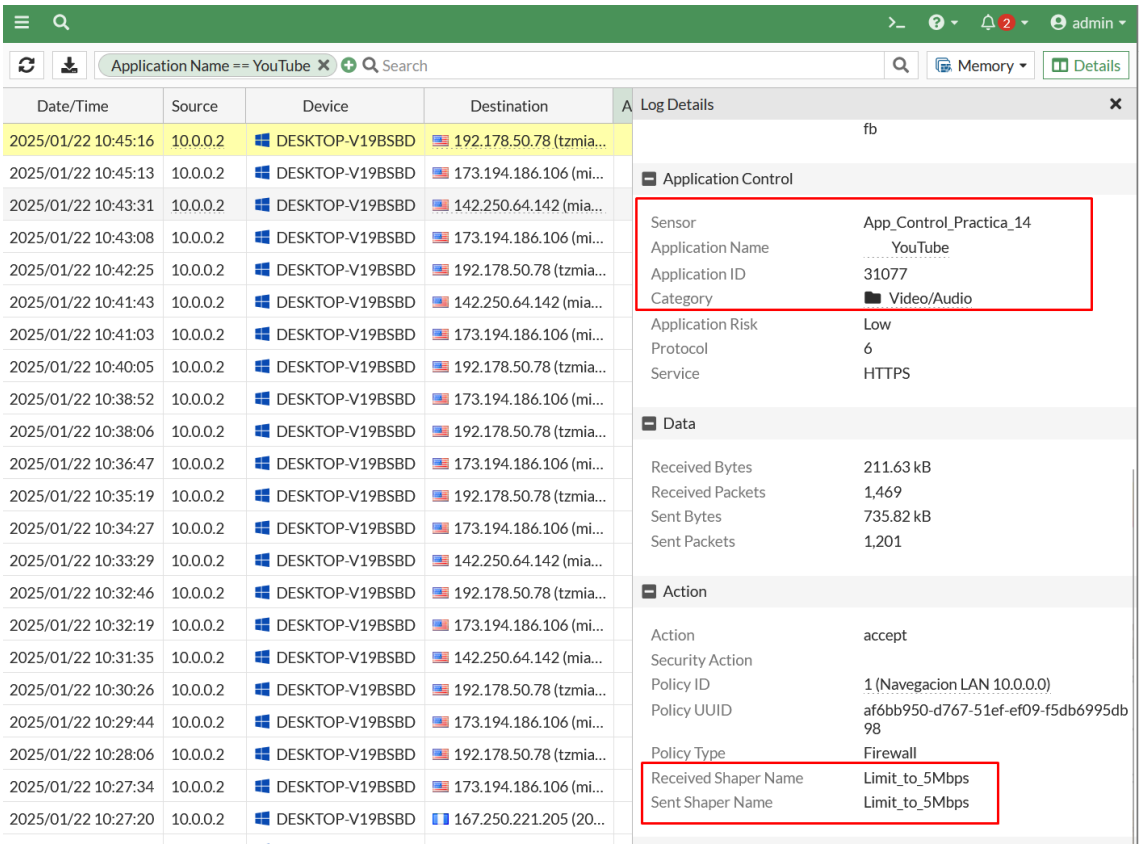


Figura 5.12-9: Registro de tráfico hacia YouTube con Traffic Shaping Policy.

.

Como se observa en la Figura 5.12-9 en el tráfico hacia YouTube registrado es de 5 Mbps que fue lo que establecimos en nuestra política.

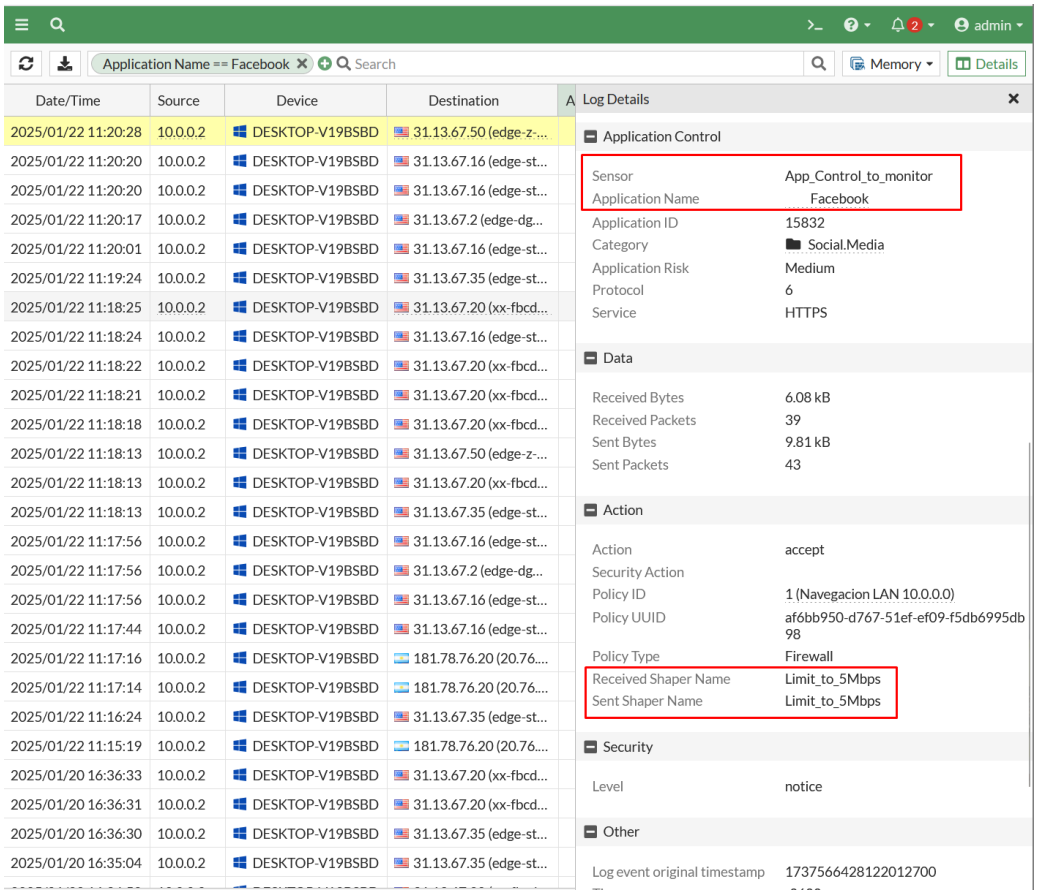


Figura 5.12-10: Monitoreo de sesiones desde Fortiview..

Como se observa en la Figura 5.12-10 en el tráfico hacia Facebook registrado del ancho de banda disponible es de 5 Mbps que fue lo que establecimos en nuestra política.

Prueba 2: Generar una descargar desde la aplicación Mega y revisar en FortiView las sesiones que se establecen y que están limitadas por la política de traffic shaping.

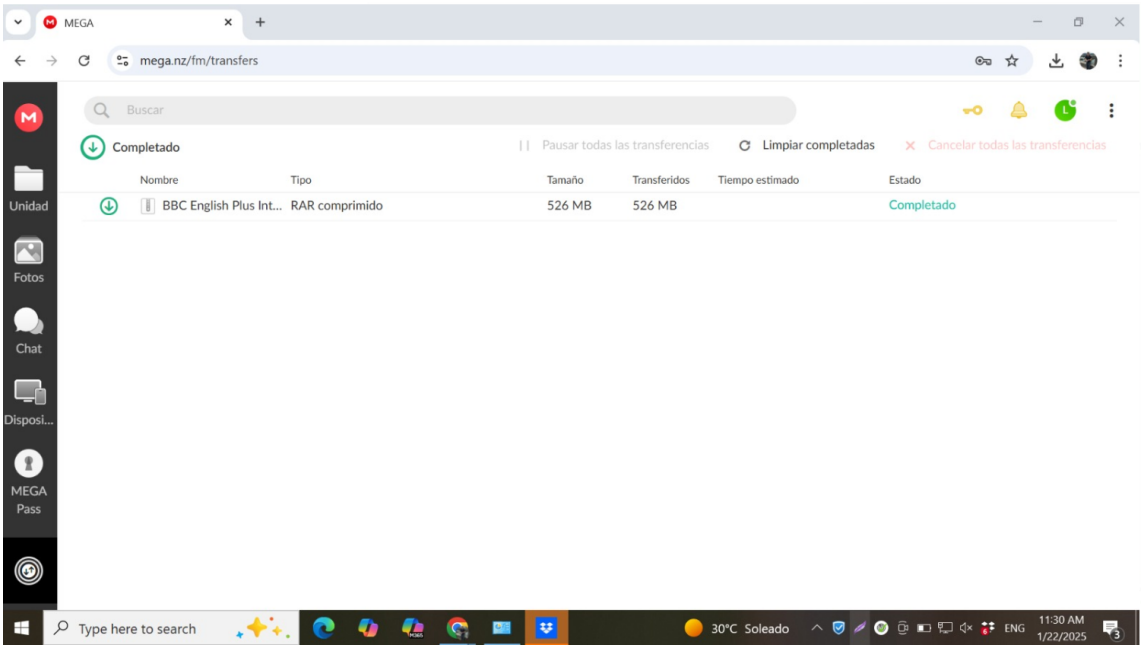


Figura 5.12-11: Tráfico generado hacia Mega desde la computadora.

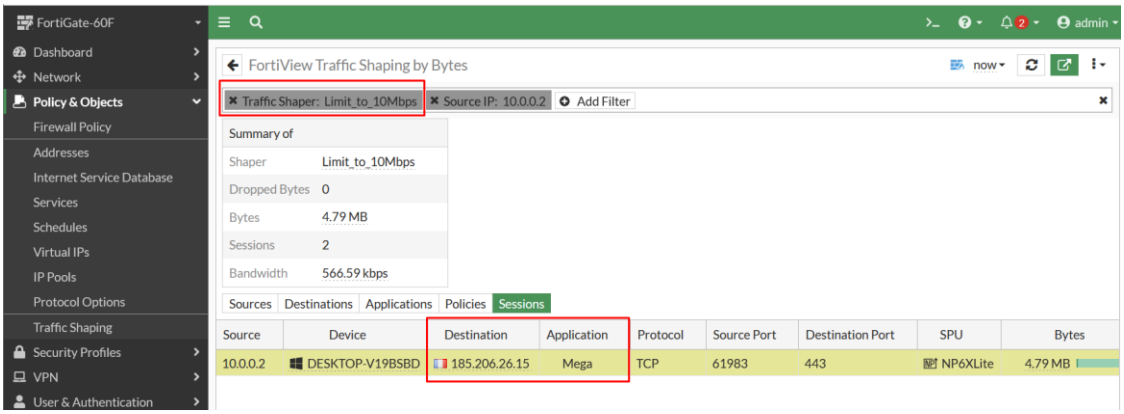


Figura 5.12-12: Tráfico detectado hacia Mega en FortiView.

También podemos consultar los LOG de las aplicaciones en el menú ***Log & Report > Security Event*** y seleccionamos la opción de ***Application Control.***

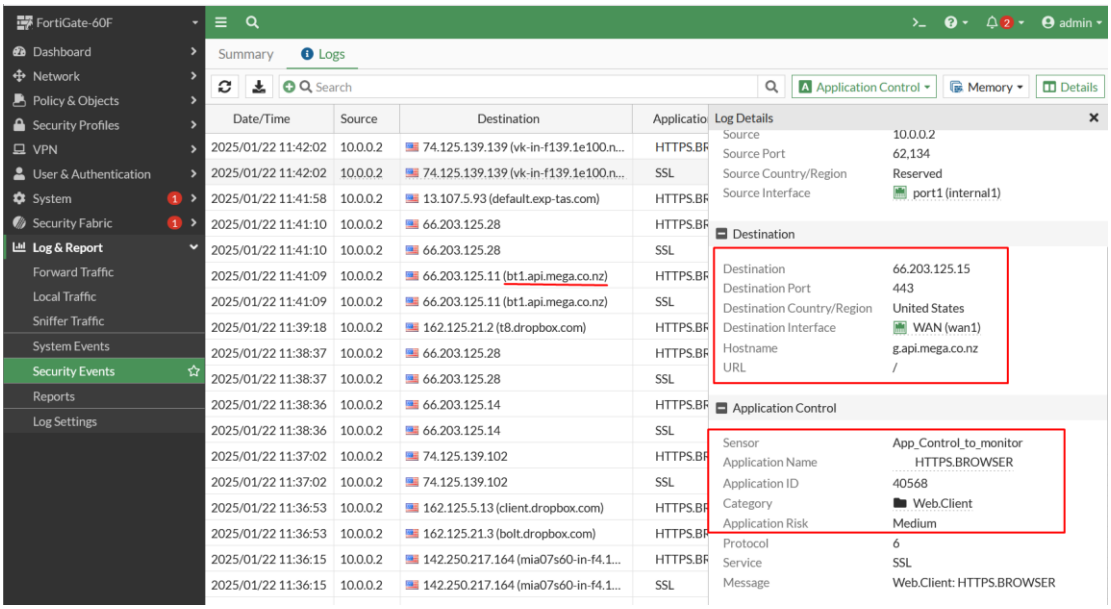


Figura 5.12-13: Log generado en el Security Event.

Conclusiones

- Se aplicó exitosamente el límite de ancho de banda por aplicaciones, de lo que podemos concluir que es posible establecer umbrales amplios para aplicaciones críticas y restringir con anchos de banda más bajos para aplicaciones que no sean criticas

- Luego de realizar la práctica nos percatamos que con políticas de traffic shapping también se pueden realizar bloqueos de aplicaciones al establecer anchos de banda que tiendan a cero.

- Se presentaron diferentes formas de consultar los logs de los eventos que se generan cuando se usa alguna aplicación desde la computadora conectada a la LAN.

5.13 Práctica 13: Balanceo de enlaces con SDWAN.

Introducción

En la presente práctica se explicará el proceso para configurar SDWAN en el FortiGate y balancear tráfico entre dos enlaces de internet conectados a la WAN.

También se aprenderá a manipular tráfico mediante reglas de SDWAN para alcanzar destinos específicos por los enlaces que requiramos.

Objetivo general

- Detallar el proceso de creación de SDWAN y garantizar la conectividad de la LAN por dos servicios de internet diferentes.

Objetivos específicos

- Crear reglas de SDWAN para manipular trafico
- Medir la salud de los servicios de internet mediante sensores en el FortiGate.

Desarrollo

Tomando como referencia la topología de la Figura 5.13-1, vamos a configurar 2 servicios de internet en la WAN1 y WAN2 respectivamente, luego procederemos a balancear el tráfico entre ambos servicios.

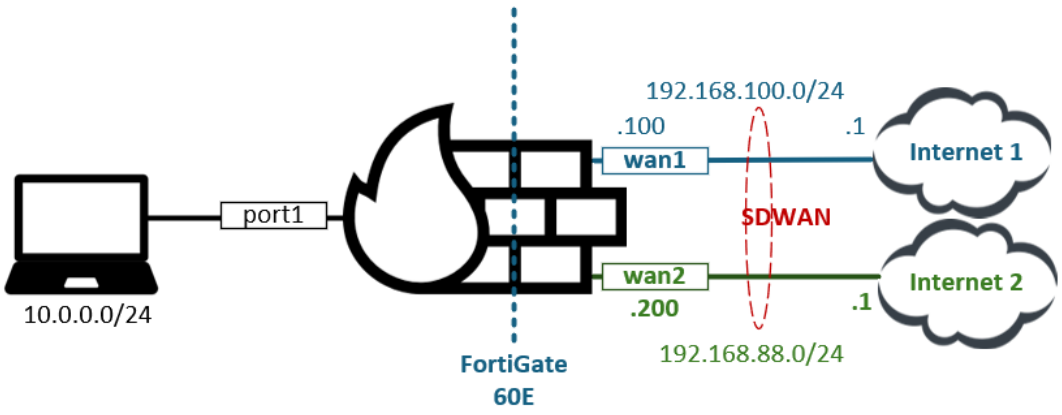


Figura 5.13-1: Topología para SDWAN.

Configuración de WAN

Paso 1: Conectamos y configuramos los puestos wan1 y wan2 con el direccionamiento que nos muestra la Figura 5.13-2, para esto nos vamos al menú ***Network >Interfaces*** y establecemos las direcciones IP con su mascara de red

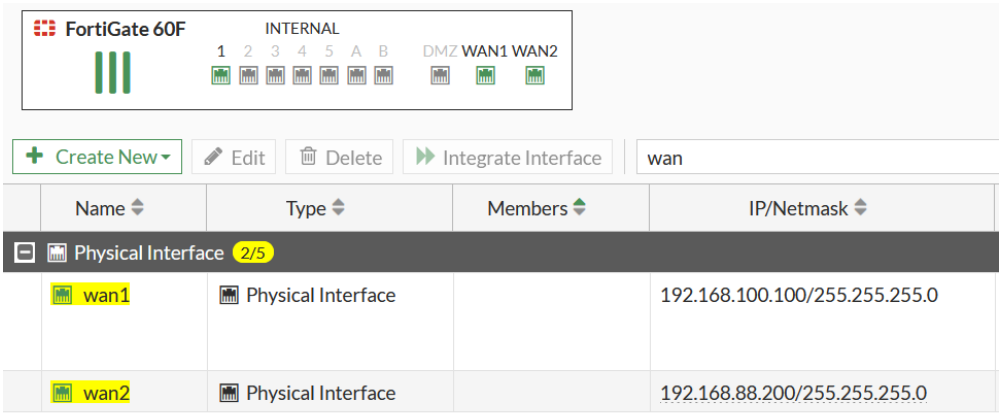


Figura 5.13-2: Configuración de la WAN.

Configuración de LAN

Paso 1: Conectamos y configuramos el puerto internal1 con el direccionamiento que nos muestra la Figura 13_3, para esto nos vamos al menú ***Network >Interfaces*** y establecemos las direcciones IP con su mascara de red **.**

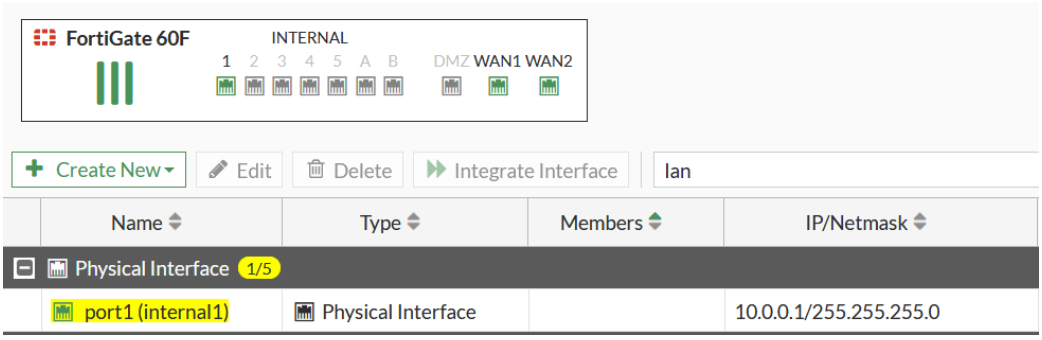


Figura 5.13-3: Configuración de la LAN.

Configuración de SDWAN

Paso 1: Primero debemos crear los miembros que pertenecerán a nuestra zona SD-WAN, para esto nos vamos al menú ***Network > SD-WAN*** y en Create New seleccionamos la opción SD-WAN Member.

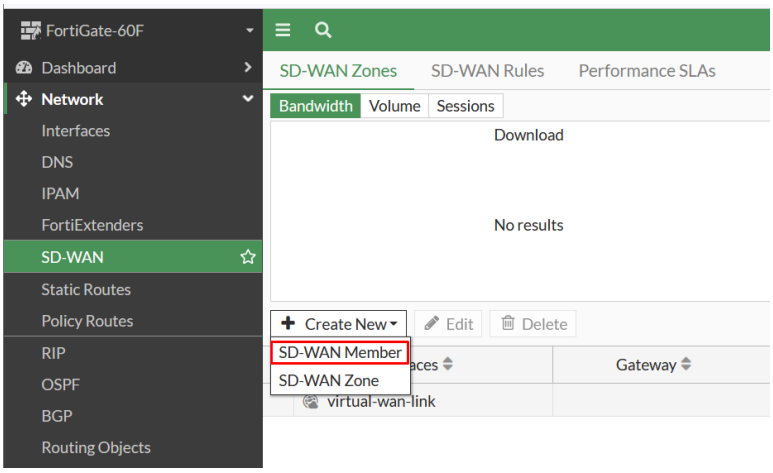


Figura 5.13-4: Creación de miembro SD-WAN.

Paso 2: En el menú para crear el miembro seleccionamos las opciones que se muestran en la Figura 5.13-5 y 5.13-6 para wan1 y wan2 respectivamente.

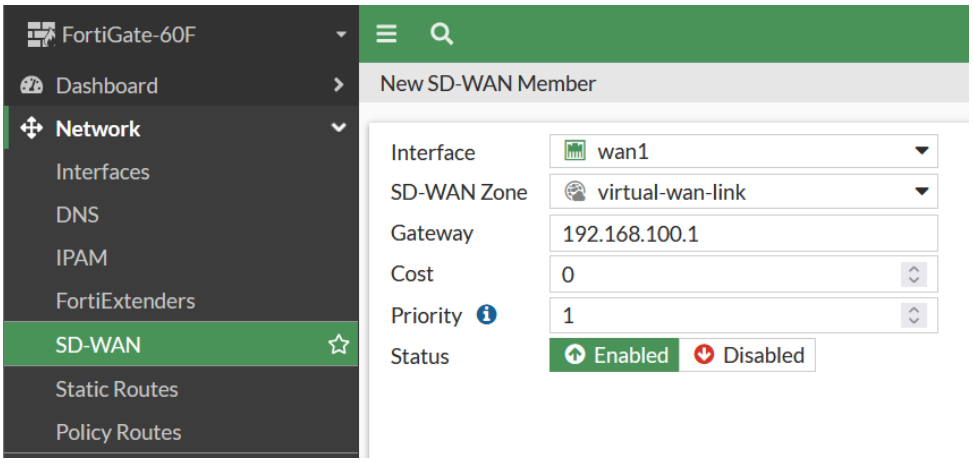


Figura 5.13-5: Creación de miembro SD-WAN para wan1.

Hacemos el mismo proceso para crear el segundo miembro asociado a la wan2.

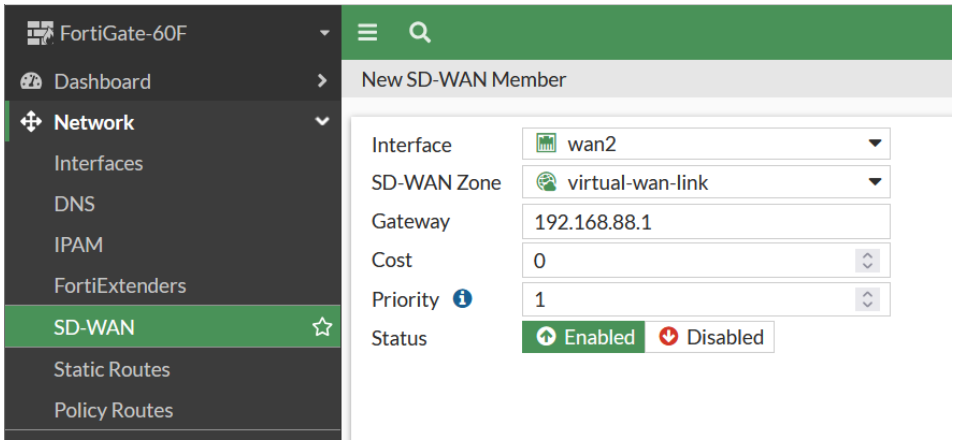


Figura 5.13-6: Creación de miembro SD-WAN para wan2.

Al revisar las zonas ahora nos deben aparecer ambos miembros wan1 y wan2 con su respectivo Gateway.

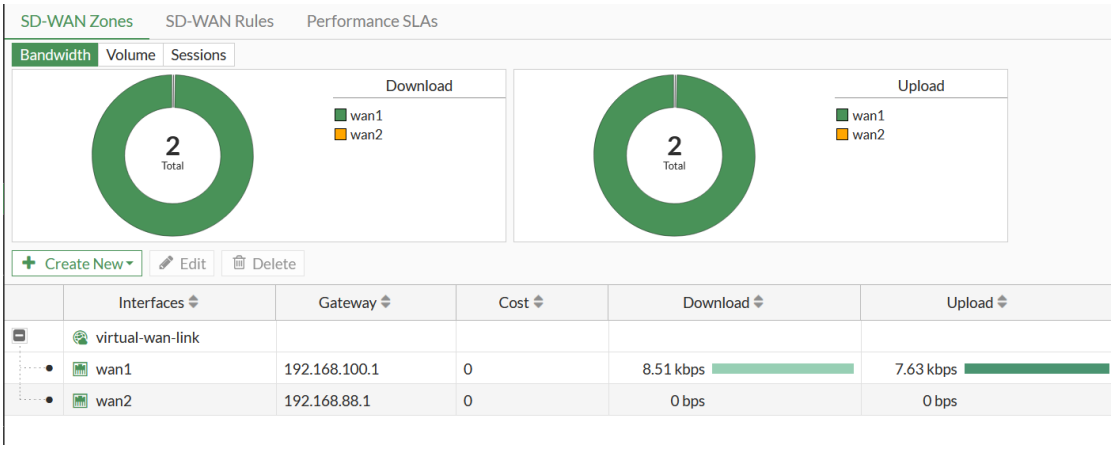


Figura 5.13-7: Miembros agregados en zona SD-WAN.

Paso 2: Agregamos la ruta por defecto hacia mediando la zona SD-WAN que hemos creado, para esto nos vamos al menú ***Network > Static Routes*** y creamos una nueva.

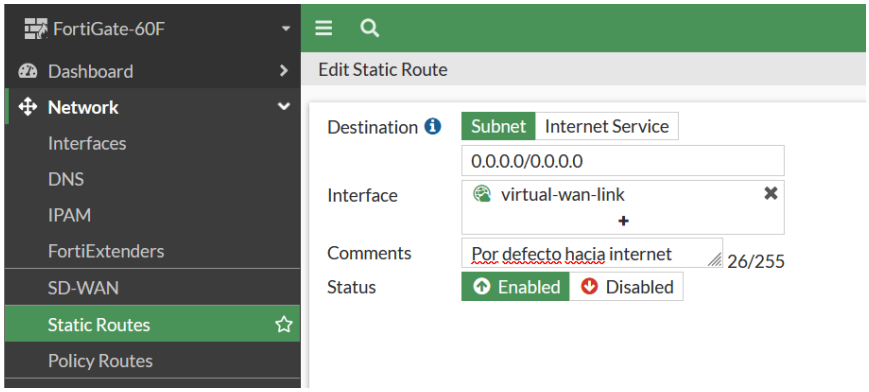


Figura 5.13-8: Ruta estática por la zona SD-WAN.

Paso 3: Creamos una política de firewall desde nuestra LAN conectada al puerto 1 hacia la zona SD-WAN, esto nos hará que la regla permita el tráfico por ambos miembros de la zona.

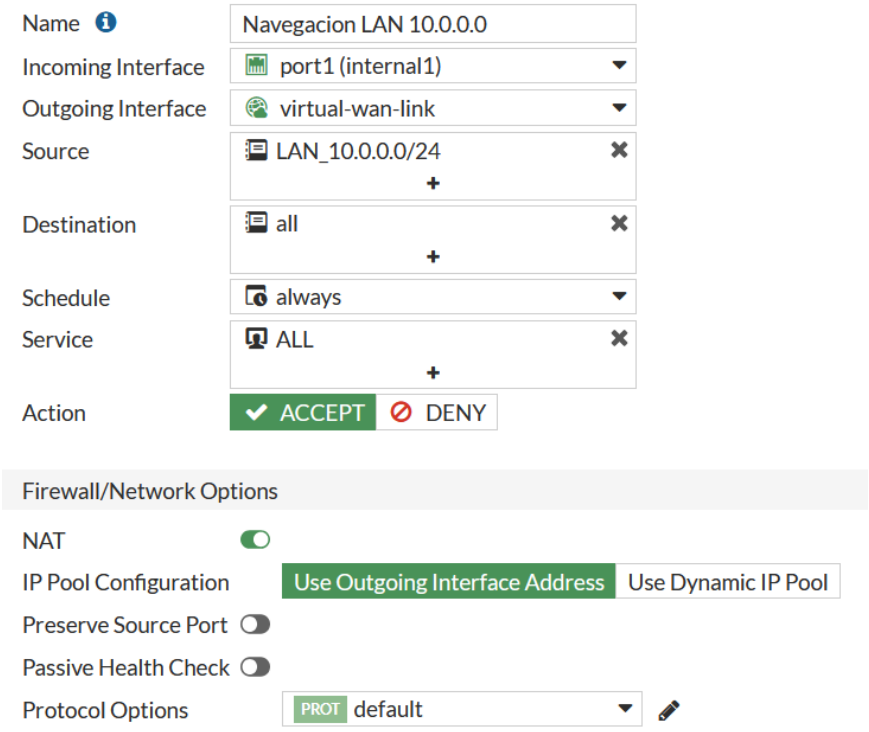


Figura 5.13-9: Política de firewall para la zona SD-WAN.

Configuración de *"Performance SLA"*

Los Performances SLA son sensores que nos permite saber la salud de nuestros miembros SD-WAN y en base al estado que tengan tomar decisiones.

Paso 1: Para crear un ***Performance SLA*** nos vamos al menú ***Network > SD-WAN*** y creamos uno nuevo.

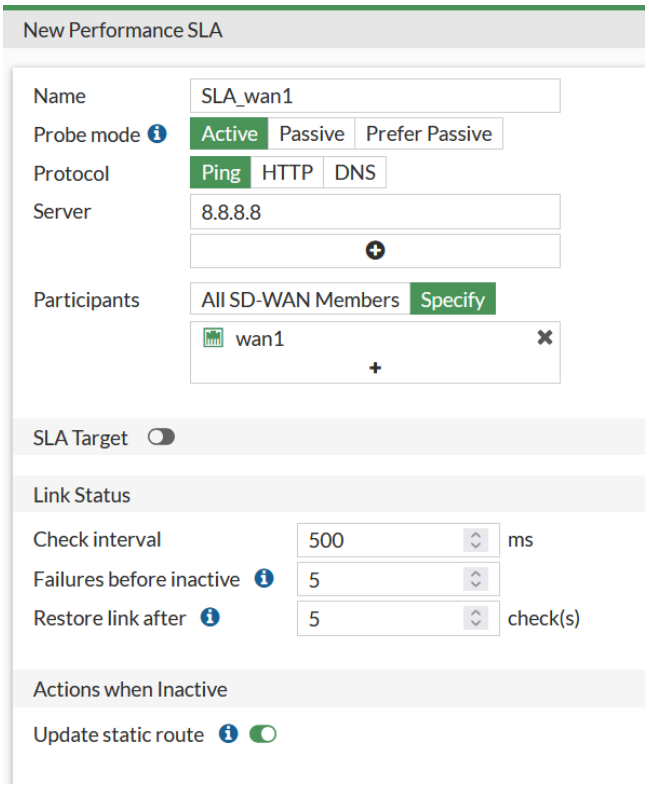


Figura 5.13-10: Performances SLA para wan1.

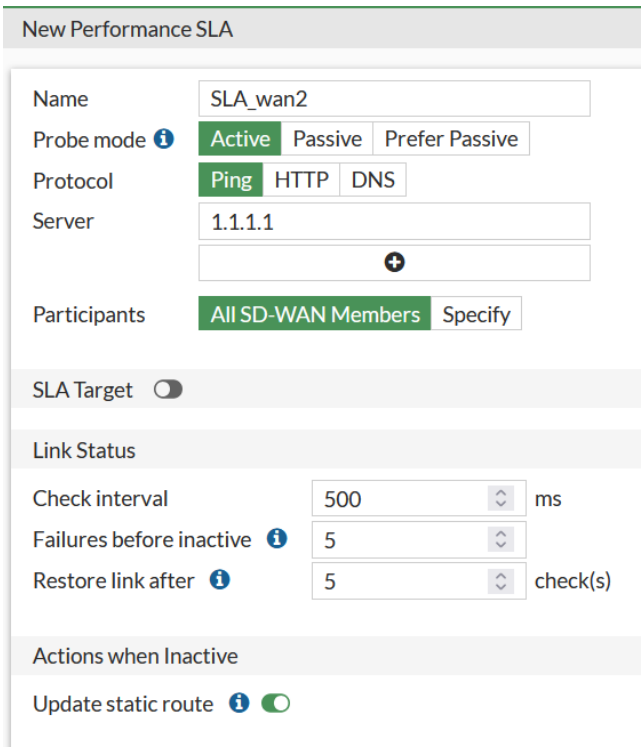


Figura 5.13-11: Performances SLA para wan2.

Ahora podremos monitorear el estado de los enlaces de internet desde las gráficas que nos general el FortiGate, las variables que podemos medir son:

- Perdida de paquetes
- Latencia
- Jitter

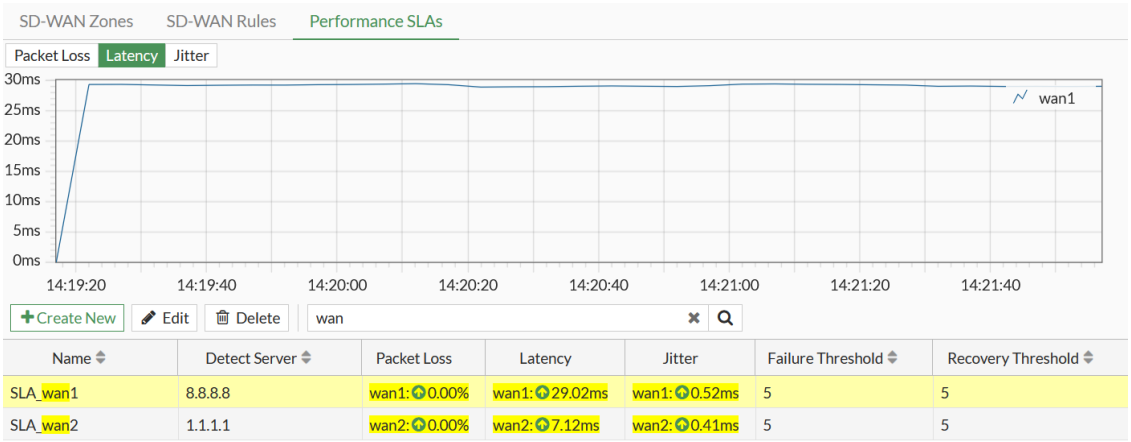


Figura 5.13-12: Estado de los enlaces de internet.

Configuración de *"SD-WAN rules"*

Las reglas nos sirven para manipular tráfico y enrutarlo por los miembros que nosotros decidamos en base a la salud o capacidad de estos.

Paso 1: Nos vamos al menú ***Network > SD-WAN*** y en la pestaña de SD-WAN rules creamos una nueva para forzar todo el tráfico que se genere en LAN hacia Gmail por la wan2.

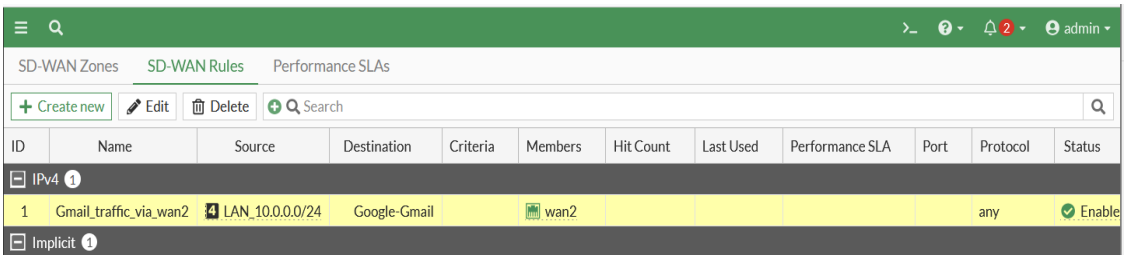


Figura 5.13-13: Regla para forzar tráfico de Gmail por wan2.

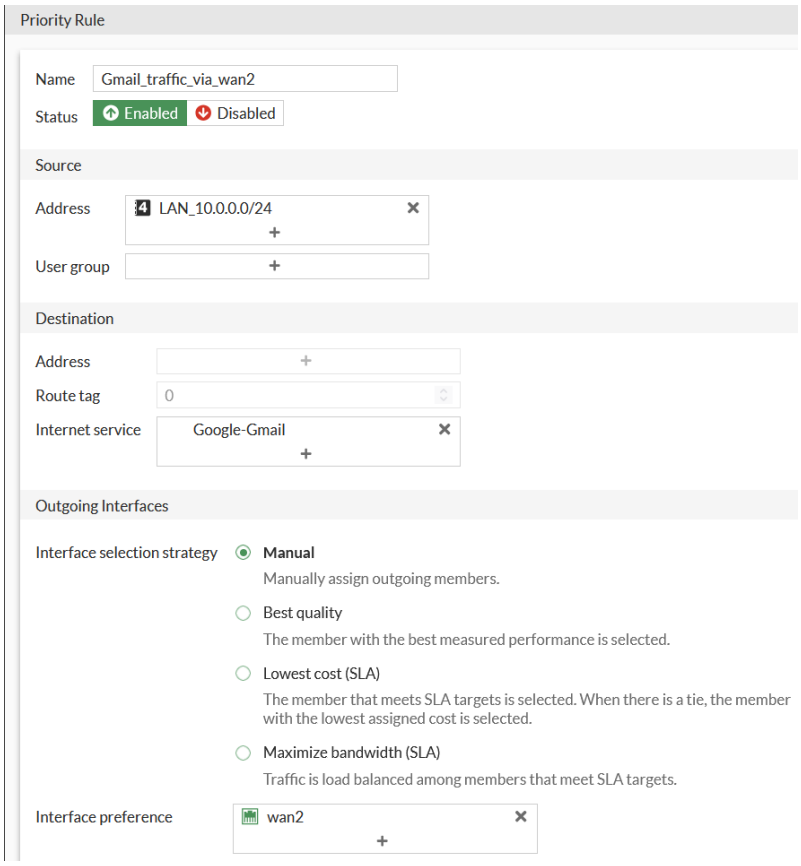


Figura 5.13-14: Detalle de SD-WAN rule.

Monitoreo

Para monitorear el consumo de ancho de banda podemos usar el menú ***Network > SD-WAN*** y en la pestaña ***SD-WAN Zones*** podremos visualizar la utilización de nuestros enlaces.

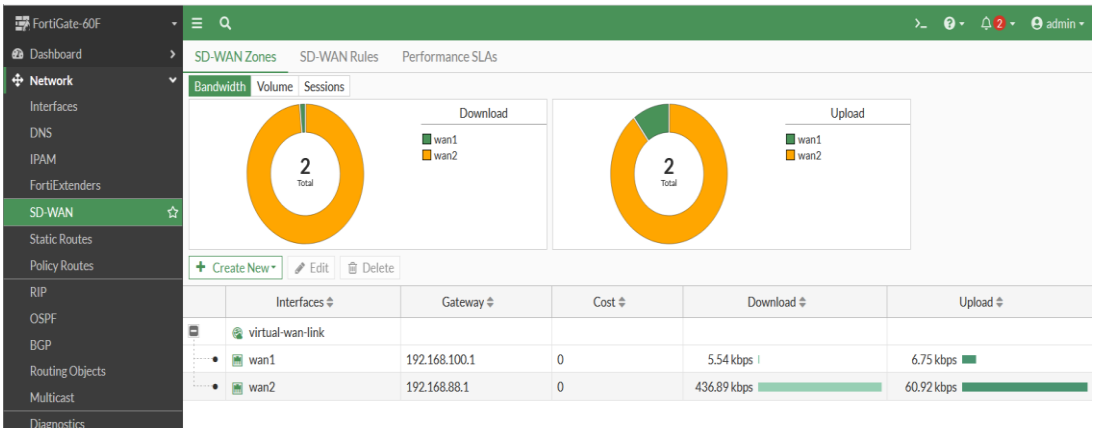


Figura 5.13-15: Monitoreo de utilización de enlaces.

También en el Dashboard de FortiView para SD-WAN podremos ver si tenemos alarmas.

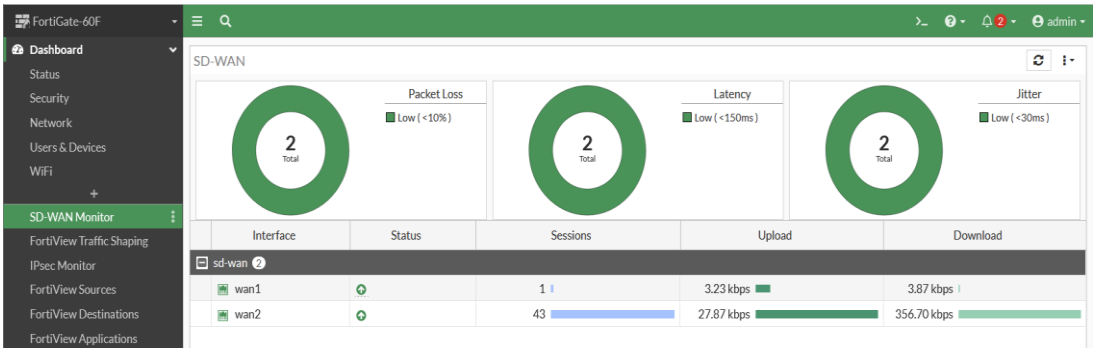


Figura 5.13-16: Monitoreo de SD-WAN desde FortiView.

Pruebas

Prueba 1: Alta disponibilidad de internet

Además de el balanceo de enlaces con SD-WAN también logramos alta disponibilidad, para realizar esta prueba vamos a desconectar la WAN2 y nuestra conexión a internet en la LAN debe mantenerse y en el FortiGate debe alarmarse el miembro.

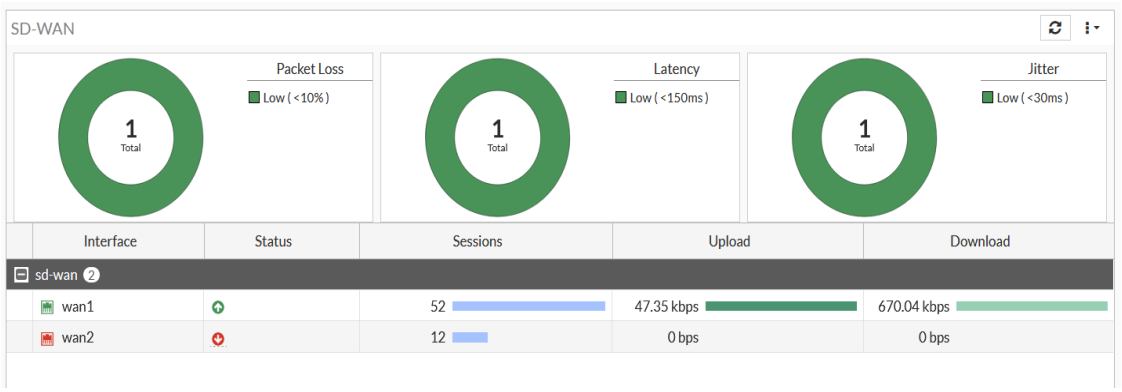


Figura 5.13-17: Alarma activa en wan2 luego de la falla.

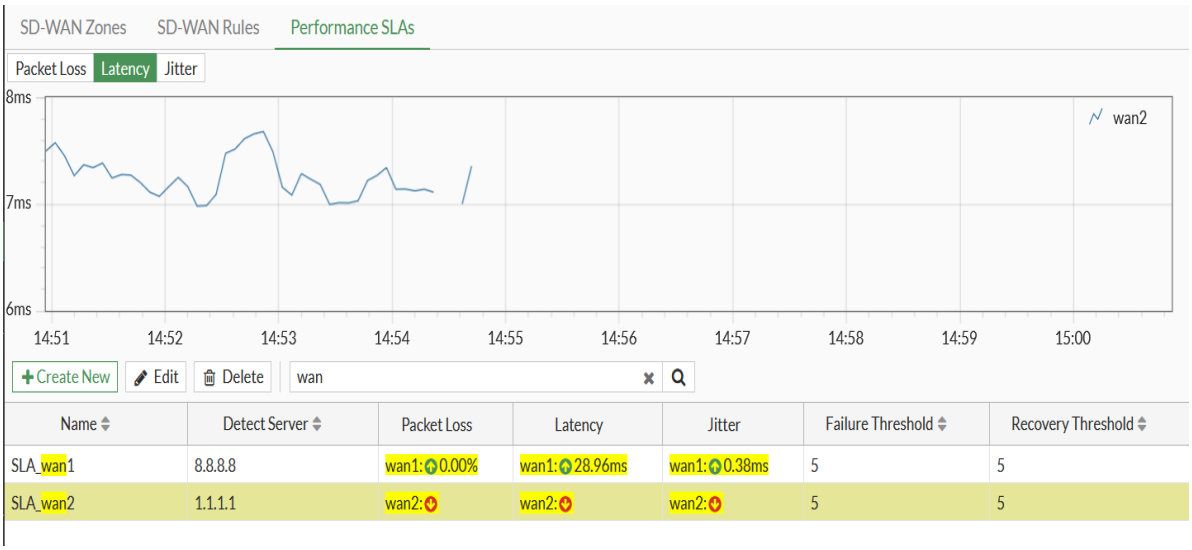


Figura 5.13-18: Monitoreo de SLA alarmado.

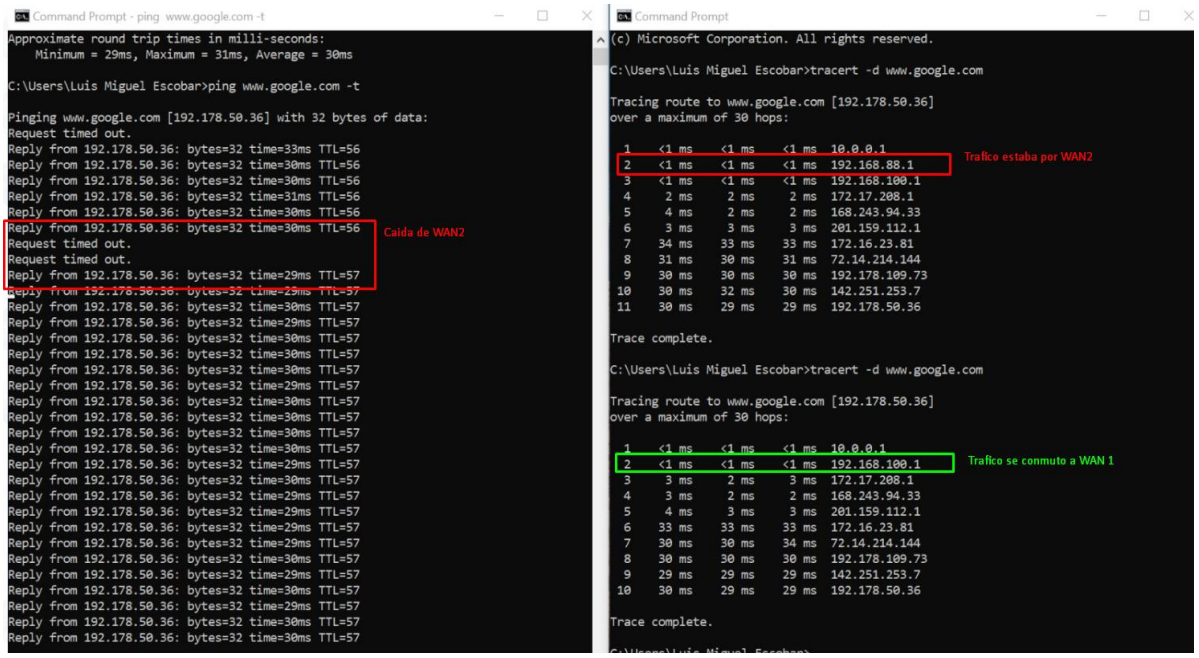


Figura 5.13-19: Análisis de alta disponibilidad.

Como apreciamos en la Figura 5.13-19 luego de analizar la traza tomada en la computadora conectada en la LAN podemos apreciar como el tráfico que estaba por la wan2 se conmuta hacia la wan1 luego de la falla.

Conclusiones

- Se detalló el proceso de creación y configuración de balanceo de tráfico usando SDWAN, se concluye tras la implementación que el protocolo no solo sirve como balanceador saliente si no también proporciona alta disponibilidad de enlace.

- Se manipuló tráfico exitosamente luego de forzar las peticiones hacia Gmail usando las reglas de SDWAN.

- Luego de medir la salud de los miembros de la zona SD-WAN concluimos que es posible medir latencia, jitter y perdida de paquetes.

CONCLUSIONES

- *Evaluación de alternativas de sistemas de seguridad perimetral para empresas del sector eléctrico y telecomunicaciones (Objetivo General):* Se analizaron diversas soluciones de seguridad perimetral enfocadas en la protección de redes críticas dentro del sector eléctrico y de telecomunicaciones. Se concluyó que los firewalls de nueva generación (NGFW) ofrecen ventajas significativas en términos de inspección profunda de paquetes, segmentación de redes y detección de amenazas en tiempo real. Además, se identificó que la elección del sistema de seguridad debe basarse en factores como escalabilidad, facilidad de administración, costos y compatibilidad con los sistemas de control industrial (ICS) utilizados en estas infraestructuras.

- *Investigación de opciones de diseños de seguridad perimetral para redes de gestión y monitoreo de empresas del sector eléctrico y telecomunicaciones (Objetivo Específico 1):* Se exploraron diferentes enfoques de diseño de seguridad perimetral, considerando tanto arquitecturas tradicionales basadas en firewalls como estrategias avanzadas que incorporan segmentación de redes, zonas desmilitarizadas (DMZ) y mecanismos de detección de intrusiones (IDS/IPS). Asimismo, se compararon diferentes marcas de firewalls para evaluar sus capacidades en cuanto a seguridad, rendimiento y facilidad de integración en infraestructuras críticas. Se concluyó que la implementación de un modelo de defensa en profundidad es esencial para reducir la superficie de ataque y proteger los sistemas de gestión y monitoreo de infraestructuras críticas. Adicionalmente, se destacó la importancia de integrar soluciones de seguridad perimetral con sistemas de monitoreo en tiempo real para detectar y responder eficazmente a amenazas emergentes.

- *Desarrollo de políticas de seguridad perimetral orientadas a la segregación de dispositivos y aplicaciones (Objetivo Específico 2):* Se establecieron políticas de seguridad enfocadas en la segregación de dispositivos y aplicaciones dentro de redes industriales y empresariales. Se concluyó que la segmentación basada en zonas de seguridad y la implementación de listas de control de acceso (ACL) son estrategias efectivas para reducir el riesgo de ataques laterales y accesos no autorizados. Asimismo, se determinó que el uso de autenticación multifactor (MFA)

y cifrado de datos en tránsito son prácticas recomendadas para reforzar la seguridad perimetral en entornos críticos.

- *Sugerencia de planes de formación en materia de ciberseguridad utilizando el sistema operativo FortiOS orientado al sector eléctrico (Objetivo Específico 3):* Se propuso un plan de formación basado en el sistema operativo FortiOS, con el objetivo de capacitar a estudiantes en la gestión de firewalls y la configuración de medidas de seguridad perimetral. Se concluyó que la formación práctica a través de laboratorios permite una mejor comprensión de las funciones de seguridad, como la configuración de reglas de firewall, la inspección profunda de paquetes y la detección de amenazas.

- *Documentación del procedimiento para gestionar, instalar y administrar el equipo que será donado al laboratorio de telemática de la Escuela de Ingeniería Eléctrica (Objetivo Específico 4):* Se elaboró una guía detallada que documenta el proceso de instalación, configuración y administración del firewall FortiGate 60F, el cual será donado al laboratorio de telemática de la Escuela de Ingeniería Eléctrica. Se concluyó que esta documentación servirá como material de referencia para los estudiantes y docentes, facilitando el aprendizaje sobre la gestión de seguridad perimetral en entornos académicos. Además, se determinó que la implementación de este equipo en el laboratorio permitirá realizar pruebas y simulaciones de seguridad, enriqueciendo la formación en ciberseguridad de los futuros profesionales.

En resumen, esta investigación ha permitido evaluar alternativas de seguridad perimetral aplicables al sector eléctrico y de telecomunicaciones, proporcionando un enfoque práctico y académico para mejorar la protección de infraestructuras críticas. La integración de políticas de seguridad, planes de formación y documentación técnica contribuirá significativamente a la capacitación de profesionales y a la mejora de la seguridad en redes industriales y empresariales.

REFERENCIAS

- Udemy. (n.d.). Introduction to Network Security. https://www.udemy.com/course/introduction-to-network-security/
- Fortinet. (n.d.). FortiGate / FortiWiFi 60F series data sheet. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/pdf/fortigate-fortiwifi-60f-series.pdf
- Iqbal, O. (2020). FortiGate Next-Generation Firewall Cookbook. Packt Publishing.
- King, P. M. (2019). Mastering FortiGate Firewalls. Packt Publishing.
- Barker, K., & Gilmore, D. (2016). Network Security with FortiGate: Implementing the FortiGate Security Appliances. Pearson.
- Fortinet. (n.d.). Fortinet Technical Documentation. https://docs.fortinet.com/
- Fortinet. (n.d.). *Fortinet Network Security Expert (NSE) Training Institute*. https://training.fortinet.com/
- Fortinet. (n.d.). *Fortinet Learning Center*. https://www.fortinet.com/training
- Fortinet. (n.d.). *FortiGate Essentials: Free Online Training*. https://www.fortinet.com/training
- Fortinet. (n.d.). *Fortinet official YouTube channel*. https://www.youtube.com/user/fortinet
- edX. (n.d.). Cybersecurity Fundamentals. https://www.edx.org/course/cybersecurity-fundamentals
- Open Security Training. (n.d.). Security Training. http://opensecuritytraining.info/
- Fortinet. (n.d.). Gartner Magic Quadrants. Fortinet. https://www.fortinet.com/lat/solutions/gartner-magic-quadrants
- Burns, R. (2019). Critical infrastructure protection and resilience: The state of cybersecurity in the electric sector. Cybersecurity Press.

- Brown, J., Davis, L., & Wang, Q. (2020). Ransomware and critical infrastructure: Impact and defense mechanisms. Journal of Cybersecurity, 45(3), 123-135. https://doi.org/10.1016/j.jocs.2020.03.005
- Chauhan, S., & Bedi, P. (2015). VPN-based security for enterprises: A review. International Journal of Network Security, 19(4), 474-484.
- Fruhlinger, J. (2019). What is phishing? CSO Online. https://www.csoonline.com/article/3248837/what-is-phishing.html
- Fortinet. (2020). FortiGate 60F series: Next-generation firewall solutions. https://www.fortinet.com/
- Garcia, L., & Martin, C. (2021). Automated cybersecurity: Implementing SIEM and SOAR solutions in large networks. Security Technology Journal, 12(2), 87-102.
- Kim, J., & Kankanhalli, M. (2014). Intrusion detection systems: A survey. International Journal of Computer Science and Information Security, 12(8), 22-31.
- Kindervag, J. (2010). No more trust: Zero Trust security. Forrester Research.
- Kaspersky. (2020). The state of cybersecurity in critical infrastructure. Kaspersky Lab. https://www.kaspersky.com/
- Mogull, R. (2021). How to defend against data exfiltration. Security Information. https://www.securityinfo.com/
- NIST. (2020). NIST Cybersecurity Framework (CSF). National Institute of Standards and Technology. https://www.nist.gov/cyberframework
- Panda, M., Singh, R., & Arora, N. (2020). Cloud security: A new frontier for cybersecurity solutions. International Journal of Cloud Computing, 5(3), 112-126.
- Pfleeger, C., & Pfleeger, S. (2012). Security in computing (4th ed.). Pearson Education.
- Raman, G. (2020). Machine learning for cybersecurity. Journal of Cyber Defense, 9(4), 67-84.
- Shostack, A. (2014). Threat modeling: Designing for security. Wiley.

- Symantec. (2020). Internet Security Threat Report. https://www.symantec.com/security-center/threat-report
- U.S. Department of Energy. (2020). Cybersecurity for the energy sector. https://www.energy.gov/
- Zhou, Y., Smith, L., & Davis, T. (2018). Securing remote access in critical infrastructure networks. Telecommunications Journal, 10(2), 45-59.

GLOSARIO

Ciberataques: Ataques maliciosos a sistemas informáticos o redes.

IoT (Internet de las cosas): Dispositivos físicos que se conectan y intercambian datos a través de Internet.

PYMEs (Pequeñas y Medianas Empresas): Empresas con un número limitado de empleados y bajos ingresos.

Vulnerabilidad: Debilidad en un sistema que puede ser explotada por una amenaza.

Integridad de datos: Mantenimiento y garantía de la exactitud y consistencia de los datos.

Disponibilidad de datos: Asegurar que los datos sean accesibles y utilizables bajo demanda.

Confidencialidad de datos: Protección de datos sensibles contra accesos no autorizados.

Seguridad perimetral: Estrategias de seguridad para proteger la red interna de una organización de amenazas externas.

Firewall: Sistema de seguridad de red que monitorea y controla el tráfico de red entrante y saliente. Intrusión: Acceso no autorizado a un sistema o red.

Firewall de última generación (NGFW): Firewall avanzado que incluye inspección profunda de paquetes y prevención de intrusiones.

Phishing: Intento fraudulento de obtener información sensible haciéndose pasar por una entidad confiable.

Exfiltración de datos: Transferencia no autorizada de datos desde un sistema.

VPN (Red privada virtual): Extensión segura de una red privada a través de una red pública como Internet.

SD-WAN (Red de área amplia definida por software): Tecnología que simplifica la gestión y operación de una WAN al desacoplar el hardware de su mecanismo de control.

Zero Trust (Confianza Cero): Modelo de seguridad que requiere estricta verificación de identidad para cada persona y dispositivo que intenta acceder a los recursos en una red privada.

Machine learning (aprendizaje automático): Subcampo de la IA que permite a las máquinas aprender de los datos sin ser explícitamente programadas.

SIEM (Gestión de eventos e información de seguridad): Enfoque de la seguridad que combina SIM (gestión de información de seguridad) y SEM (gestión de eventos de seguridad).

SOAR (Orquestación, automatización y respuesta de seguridad): Tecnologías que permiten la automatización de tareas de seguridad.

FortiGate: Plataforma de seguridad de red desarrollada por Fortinet.

FortiOS: Sistema operativo de seguridad de red de Fortinet.

GUI (Interfaz gráfica de usuario): Interfaz que permite a los usuarios interactuar con dispositivos electrónicos a través de iconos y representaciones visuales.

CLI (Interfaz de línea de comandos): Interfaz que permite a los usuarios interactuar con un sistema operativo o aplicación introduciendo comandos de texto.

LAN (Red de área local): Red que conecta computadoras y dispositivos en un área local.

WAN (Red de área amplia): Red que cubre un área geográfica extensa.

DMZ (Zona desmilitarizada): Subred que expone los servicios de una organización a una red no confiable más grande, usualmente Internet.

USB (Bus serie universal): Estándar de la industria para cables, conectores y protocolos para conexión, comunicación y fuente de alimentación entre computadoras y dispositivos electrónicos.

IP (Protocolo de Internet): Conjunto de reglas para direccionar y enrutar paquetes de datos a través de una red.

TFTP (Protocolo de transferencia de archivos trivial): Protocolo simple de transferencia de archivos, similar a una versión simplificada de FTP.

VLAN (Red de área local virtual): Red lógica de dispositivos que se comportan como si estuvieran conectados al mismo dominio de difusión.

FTP (Protocolo de transferencia de archivos): Protocolo estándar de red utilizado para la transferencia de archivos entre un cliente y un servidor en una red informática.

VDOM (Dominio virtual): Método para dividir un único dispositivo FortiGate en múltiples unidades virtuales que funcionan como dispositivos independientes.

OSPF (Abrir el camino más corto primero): Protocolo de enrutamiento para redes de Protocolo de Internet.

NAT (Traducción de direcciones de red): Método de reasignar un espacio de direcciones IP a otro creando una o más direcciones IP públicas en un espacio de direcciones IP privado.

SNAT (Traducción de direcciones de red de origen): Proceso de modificar la dirección IP de origen en los encabezados de paquetes IP mientras están en tránsito a través de un enrutador o firewall.

IP Pool (Grupo de direcciones IP): Conjunto de direcciones IP que pueden ser asignadas o utilizadas para un propósito específico.

ARP (Protocolo de resolución de direcciones): Protocolo de red utilizado para convertir una dirección IP en una dirección física (MAC).

DNAT (Traducción de direcciones de red de destino): Técnica de cambiar la dirección IP de destino de los paquetes en tránsito a través de un enrutador.

DHCP (Protocolo de configuración dinámica de host): Protocolo de gestión de red utilizado en redes IP mediante el cual un servidor DHCP asigna automáticamente direcciones IP y otra información de configuración de red a cada dispositivo en la red.

DNS (Sistema de nombres de dominio): Sistema de nomenclatura jerárquico descentralizado para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

IPSec (Seguridad del protocolo de Internet): Conjunto de protocolos de seguridad de red que autentican y cifran los paquetes de datos para proporcionar comunicación segura a través de redes IP.

Traffic Shaping (Conformación del tráfico): Técnica de gestión de ancho de banda en redes informáticas que retrasa algunos paquetes para cumplir con un objetivo de rendimiento.

SD-WAN (Red de área amplia definida por software): Conexión WAN que utiliza software y tecnologías basadas en la nube para simplificar la gestión y operación de WANs.

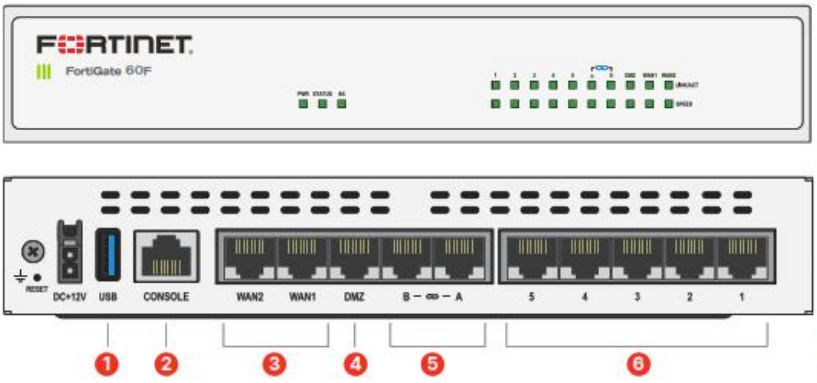
ANEXOS

ANEXO A: FICHA TÉCNICA FORTINET 60 F

Hardware

FortiGate FortiWiFi 60F/61F

SoC4 | DESKTOP | a/b/g/n/ac-W2 | 128GB



Interfaces

1. 1 x USB Port
2. 1 x Console Port
3. 2 x GE RJ45 WAN Ports
4. 1 x GE RJ45 DMZ Port
5. 2 x GE RJ45 FortiLink Ports
6. 5 x GE RJ45 Internal Ports

Specifications

	FORTIGATE 60F	FORTIGATE 61F	FORTIWIFI 60F	FORTIWIFI 61F
Operating Environment and Certifications				
Power Rating	12Vdc, 3A			
Power Required	Powered by External DC Power Adapter, 100–240V AC, 50/60 Hz			
Maximum Current	100Vac/1.0A, 240Vac/0.6A			
Power Consumption (Average / Maximum)	10.17 W / 12.43 W	17.2 W / 18.7 W	17.2 W / 18.7 W	17.5 W / 19.0 W
Heat Dissipation	42.4 BTU/hr	42.4 BTU/hr	63.8 BTU/hr	64.8 BTU/hr
Operating Temperature	32°F to 104°F (0°C to 40°C)			
Storage Temperature	-31°F to 158°F (-35°C to 70°C)			
Humidity	10% to 90% non-condensing			
Noise Level	Fanless 0 dBA			
Operating Altitude	Up to 7400 ft (2250 m)			
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB			
Certifications	USGv6/IPv6			
Radio Specifications				
Multiple User (MU) MIMO	—	—	3×3	
Maximum Wi-Fi Speeds	—	—	1300 Mbps @ 5 GHz, 450 Mbps @ 2.4 GHz	
Maximum Tx Power	—	—	20 dBm	
Antenna Gain	—	—	3.5 dBi @ 5 GHz, 5 dBi @ 2.4 GHz	

ANEXO B: PRACTICAS DE CONTINGENCIA

Práctica 14: Recuperación del sistema operativo con servidor TFTP.

Introducción

En la presente practica se explica el proceso para recuperar el sistema operativo a partir de una imagen cargada en un servidor TFTP.

Objetivo general

- Instalar el FortiOS a partir de una imagen cargada en un servidor TFTP.

Objetivos específicos

- Configurar un servidor TFTP.
- Formatear de fábrica el dispositivo cuando no tenemos las credenciales para autenticarnos.

Desarrollo:

El desarrollo de esta práctica nos permitirá realizar el proceso de booteo del dispositivo remotamente, esto es útil cuando no sabemos las credenciales de un equipo y no tenemos forma entrar al sistema operativo, también cuando un sistema operativo haya sido corrompido.

Paso 1: Descargamos y configuramos un servidor TFTP, para el desarrollo lo haremos con el programa tftpd64[15] disponible para Windows.

Paso 2: Desde el programa ubicamos la carpeta donde tenemos la imagen del sistema operativo en la opción **Browse**. Para el ejemplo la ubicación del archivo es en la carpeta Downloads\FortiOS for Fortigate 60F.

[15] El proceso de descargar de este software no se explica, el programa está disponible gratuitamente en la página https://pjo2.github.io/tftpd64/

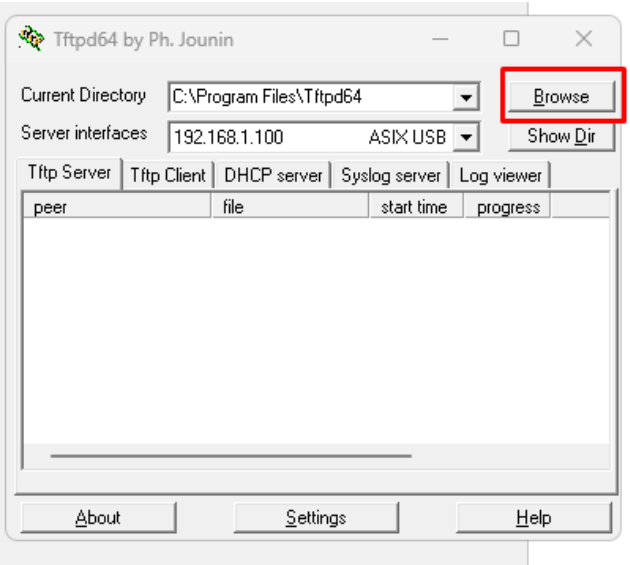


Figura 1: Interfaz del TFTPD64.

Paso 3: Opcionalmente podemos cambiarle nombre el firmware por el siguiente nombre **image.out** al firmware, esto se realiza debido a que es el nombre que por defecto tiene el firewall para su arranque, sin embargo, en el menú del boot veremos que podemos colocar el nombre exacto del archivo que tenemos en nuestra carpeta.

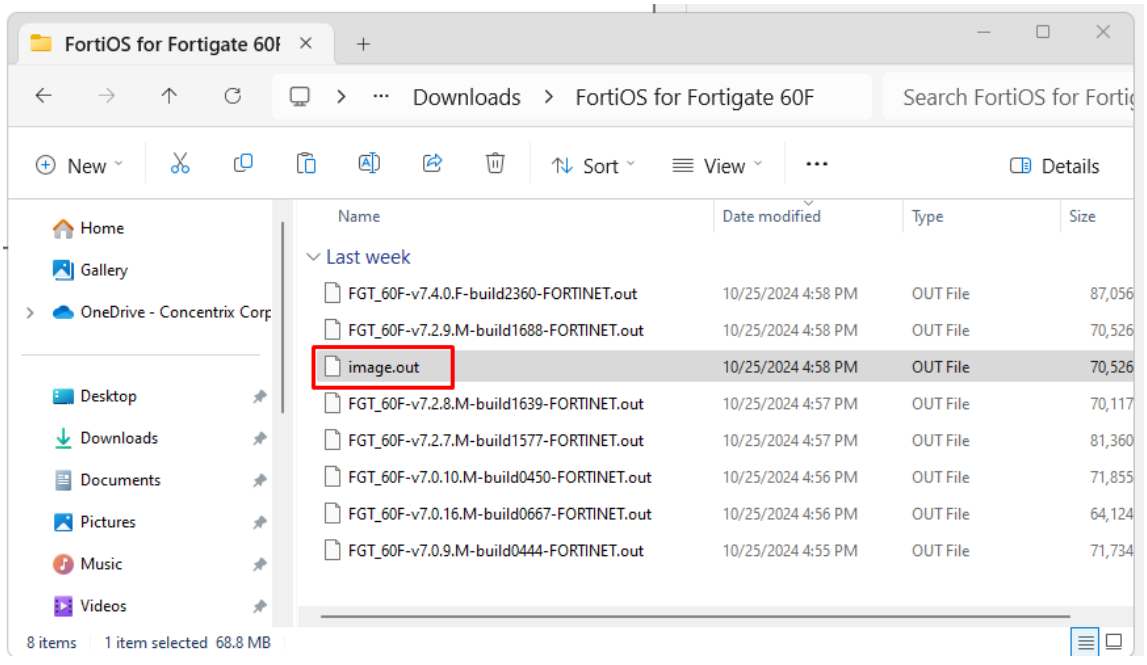


Figura 2: Cambio de nombre al archivo del sistema operativo.

Para la práctica se hizo una copia de la versión 7.2.9 y se le cambio nombre.

Paso 4: Conectarse al firewall por consola usando Putty

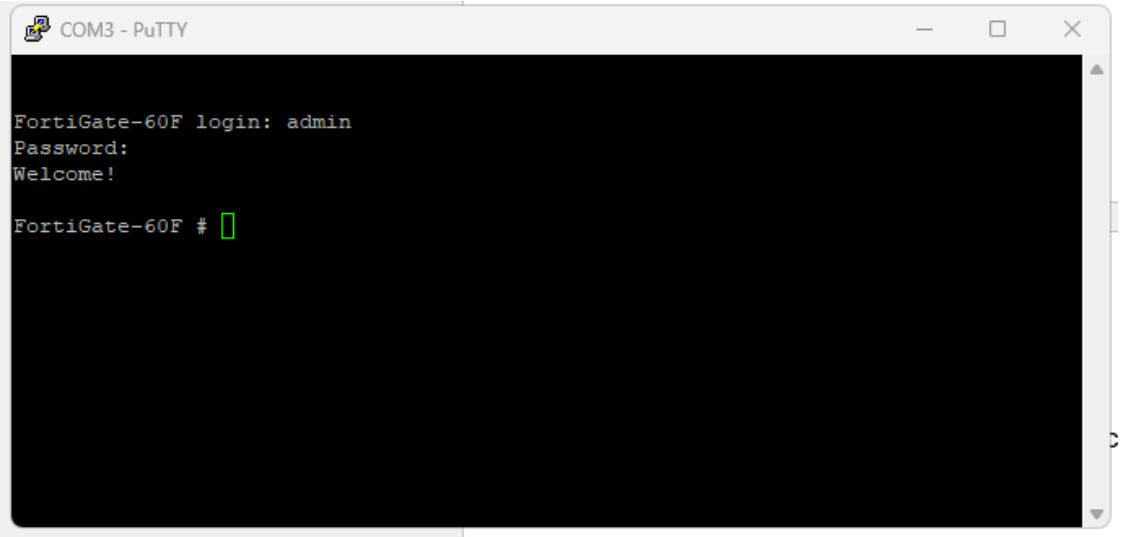


Figura 3: Conexión por consola al firewall.

Paso 5: Se procede a reiniciar el equipo para que vuelva a cargar y hacer el proceso de interrupción.

Paso 6: Cuando el firewall este cargando nos saldrá por unos segundos lo que se muestra en la figura 4, ahí debemos presionar cualquier tecla para interrumpir el boot.

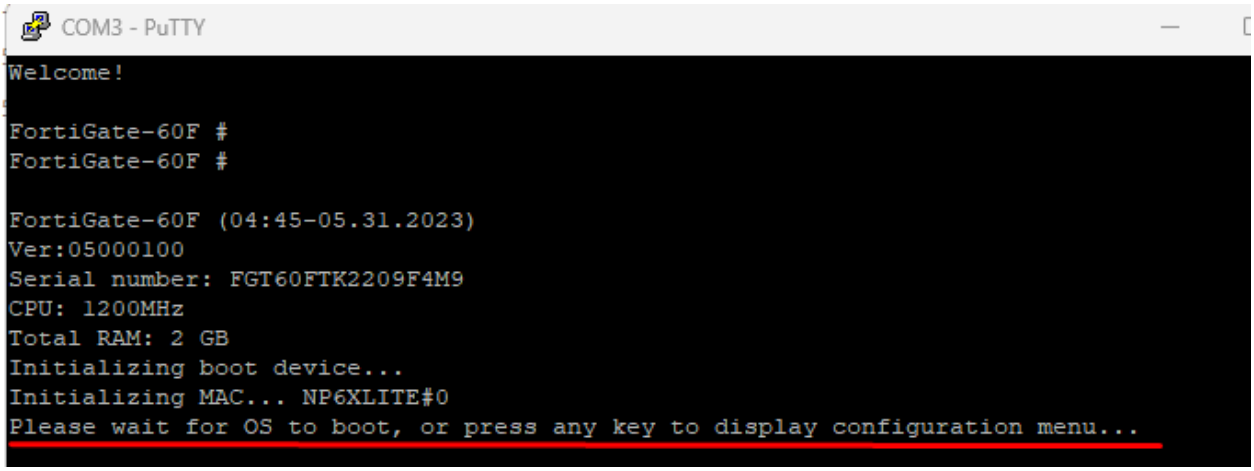


Figura 4: Mensaje de interrupción.

Si nos aparece el menú como el de la figura 5 significa que el proceso de interrupción fue exitoso.

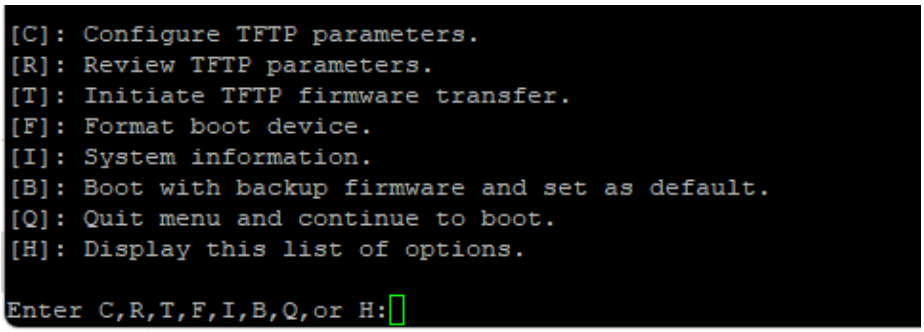


Figura 5: Menú principal de boot del firewall.

Paso 7: En el menú presionamos la letra **C** para configurar los parámetros del TFTP server, se nos desplegará un nuevo menú como el de la figura 6.

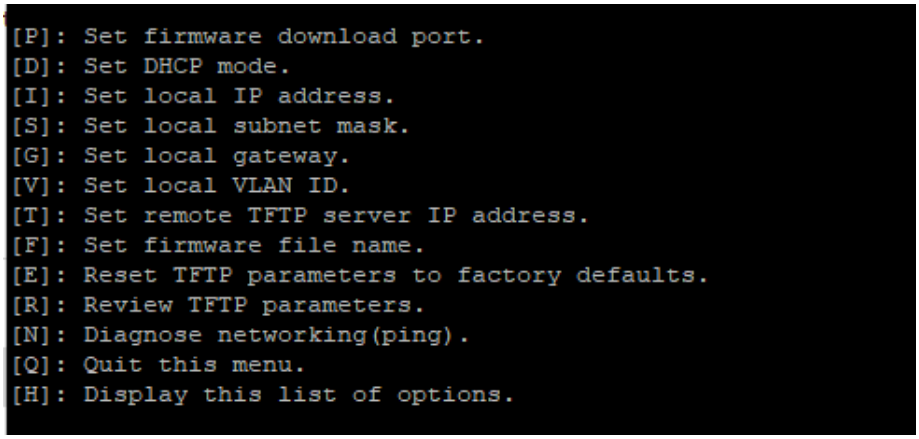


Figura 6: Menú para establecer los parámetros del TFTP *Server.*

Paso 8: A continuación, presionamos la letra **T** para establecer la dirección IP del servidor TFTP que en este caso es nuestra computadora con IP 192.168.1.100.

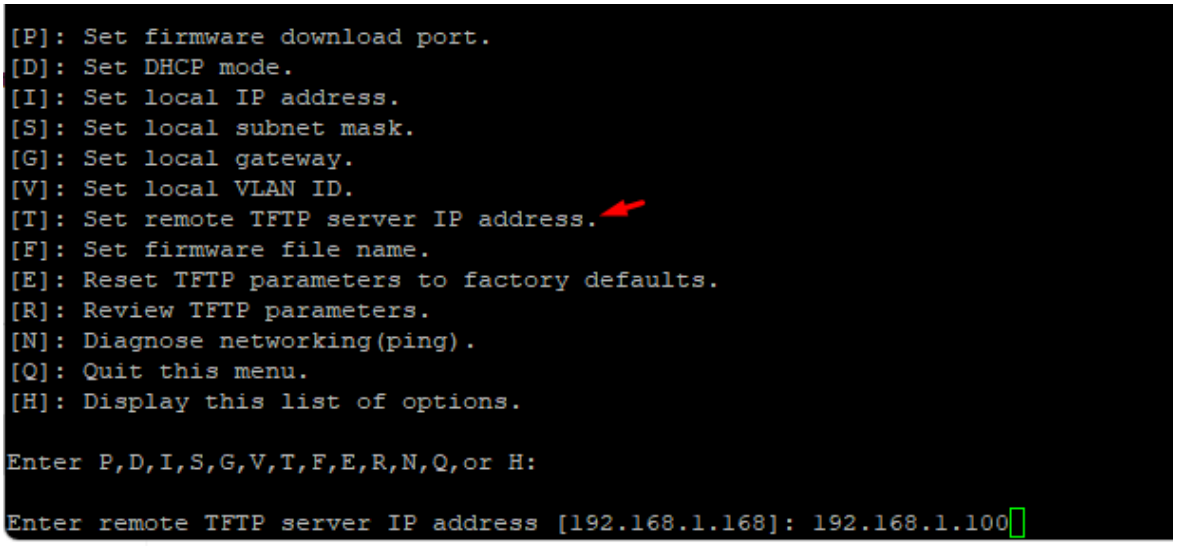


Figura 7: Configuración IP del servidor TFTP.

Paso 9: Luego presionamos la letra **P** y nos saldrá el menú de la figura 8 en el cual establecemos el puerto por el que estamos conectados al firewall desde nuestra computadora, en nuestro caso estamos conectados en el puerto 1 por eso presionamos el número **0.**

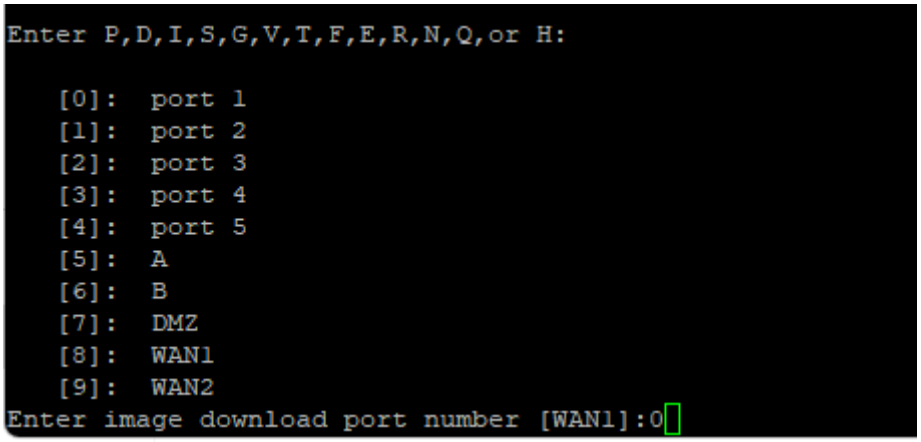


Figura 8: Configuración del puerto de conexión entre firewall y computadora.

Paso 9: Posteriormente presionamos la letra **F** para establecer el nombre el archivo que queremos ir a buscar al servidor para transferir, en nuestro caso vamos a pasar el archivo FGT_60F-v7.4.0.F-build2360-FORTINET.out

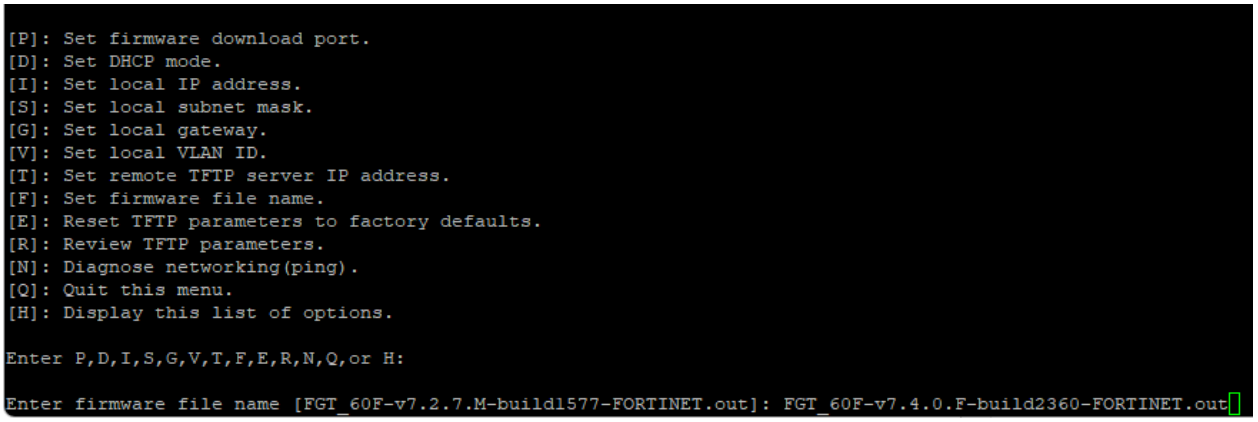


Figura 9: Nombre del archivo que trasferiremos.

Paso 10: Ahora verificamos que los parámetros que hemos configurado estén correctamente aplicados, para esto presionamos la letra **R**.

Image download port: port 1
TFTP server IP address: 192.168.1.100
Firmware file name: FGT_60F-v7.4.0.F-build2360-FORTINET.out

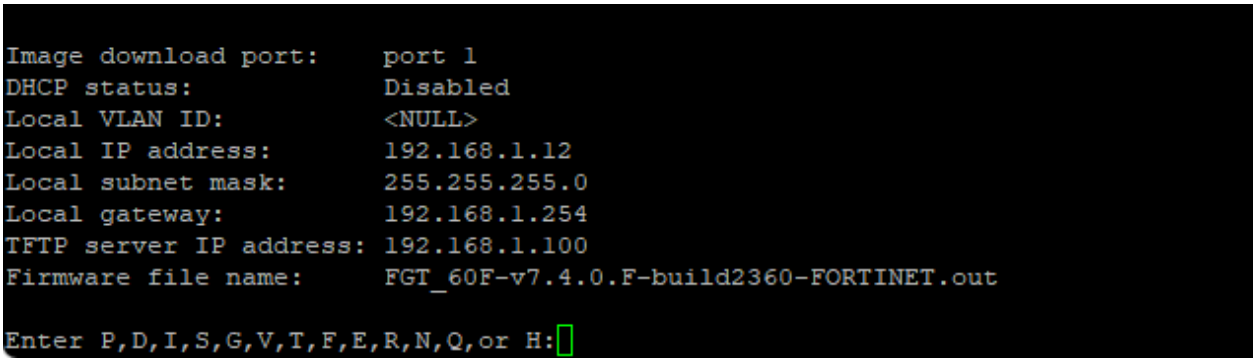


Figura 10: Parámetros del servidor TFTP configurados.

Paso 11: Luego presionamos la letra **Q** para volver al menú principal.

Paso 12: Ya en el menú principal presionamos la letra T para iniciar la transferencia del firmware.

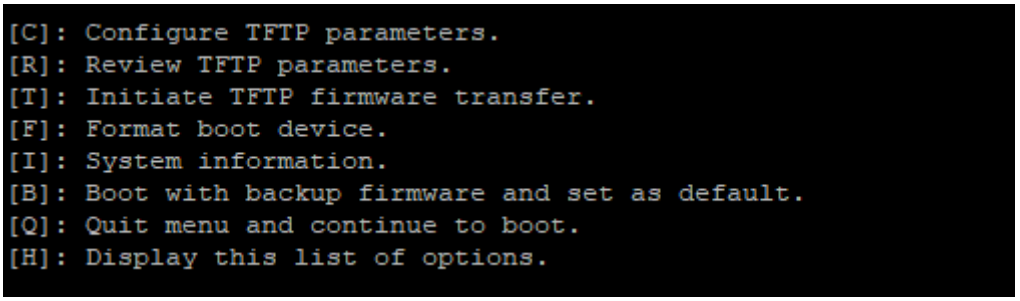


Figura 11: Menú principal listo para iniciar la transferencia.

Paso 13: Luego de iniciada la transferencia nos aparecerá en el servidor TFTP el progreso como se muestra en la figura 12.

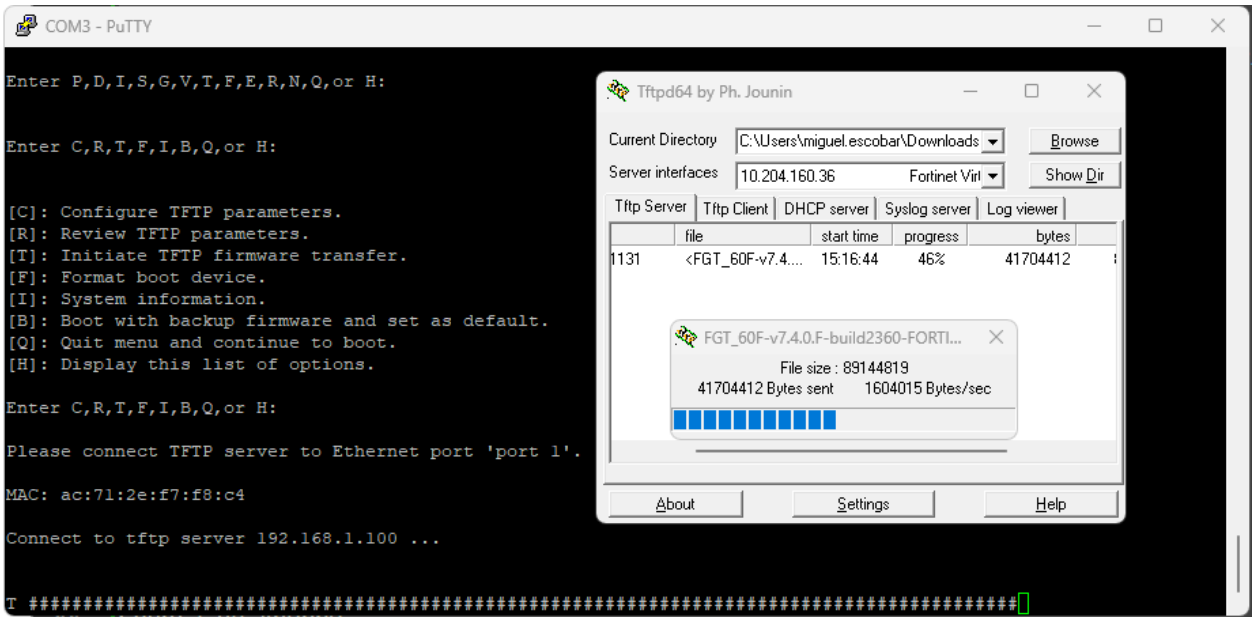


Figura 12: Progreso de la transferencia del firmware.

Paso 14: Una vez finalizada la transferencia nos preguntara *(Save as Default firmware/Backup firmware/Run image without saving:[D/B/R]?)* si queremos arrancar el sistema operativo. Para el caso de la práctica solo subiremos el firmware como backup (por eso presionamos **B**), ya que nos enfocaremos en las siguientes prácticas en la versión 7.2.8.

Si quisiéramos cargar la imagen 7.4.0 en esta parte debemos presionar D o R.

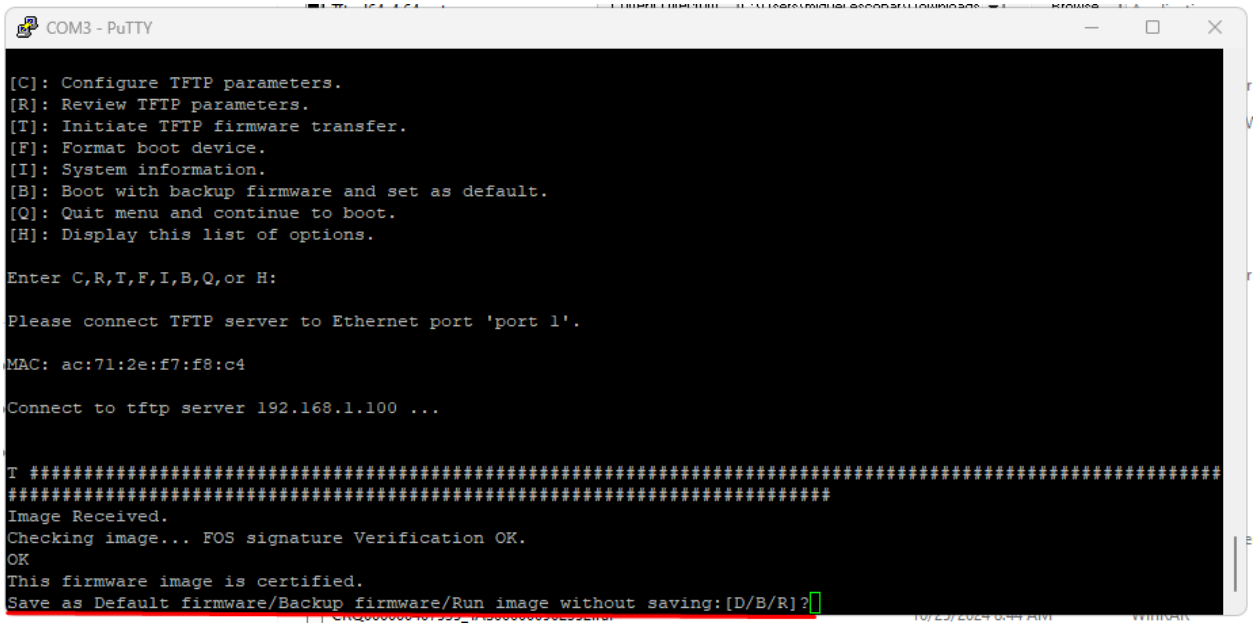


Figura 13: Opciones de arranque cuando carga el nuevo firmware.

Paso 14: Cuando le indicamos al firewall que deje la imagen como respaldo, el sistema procede al arranque con el sistema operativo por defecto.

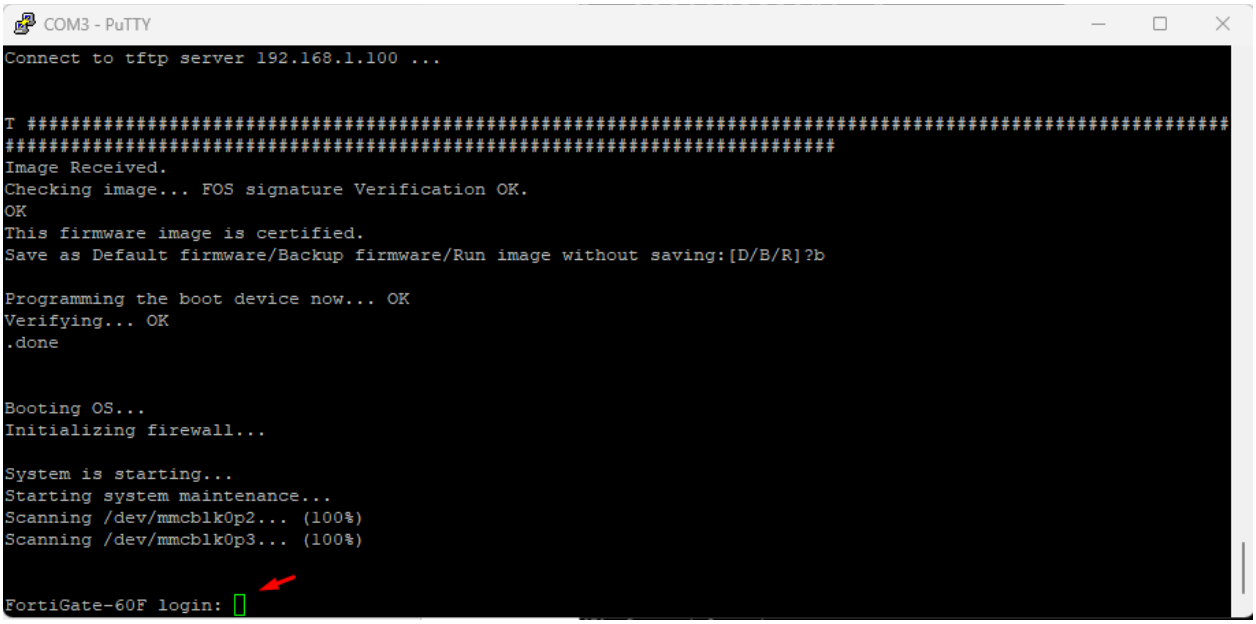


Figura 14: Arranque del sistema operativo.

Conclusiones

- Se comprobó que es posible instalar el sistema operativo en un firewall desde usando un servidor remoto siempre que se tenga conectividad capa 3 con el firewall.

- Es posible configurar un servidor TFTP de una manera sencilla en Windows

- Es posible reinstalar el sistema operativo en un FortiGate a pesar que no tengamos las credenciales del sistema.

Práctica 15: Enrutamiento dinámico.

Introducción

En la presente práctica se explicará el proceso configurar enrutamiento dinámico entre dos vdom, este proceso es útil para no que las redes se aprendan de manera dinámica y no sea necesario colocar manualmente rutas estáticas.

El concepto se puede extrapolar para configurar enrutamiento dinámico con cualquier otra tecnología siempre y cuando cumplan con la configuración correcta del estándar que se esté aplicando.

Objetivo general

- Configurar el protocolo estándar OSPF para intercambiar rutas entre dos dominios virtuales.

Objetivos específicos

- Aprender a revisar la tabla de enrutamiento para identificar cuando se está corriendo un protocolo dinámico.
- Realizar pruebas de conectividad en capa 3.

Desarrollo

Tomando como referencia la topología de la práctica anterior vamos a configurar el protocolo OSPF en cada vdom para que exista comunicación entre ambas redes.

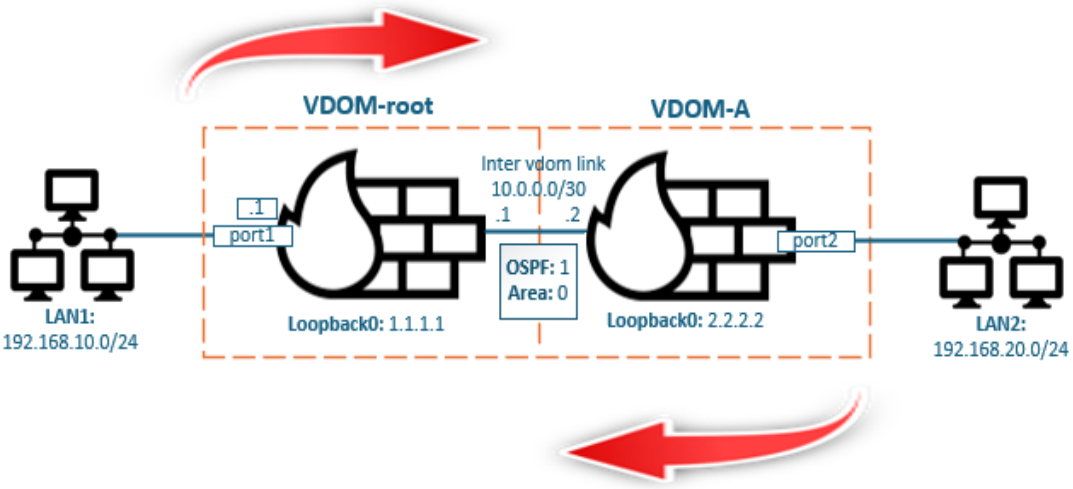


Figura 1. Topología para configurar enrutamiento dinámico.

Vamos a partir de la topología previamente configurada en la practica 7 de enrutamiento estático y nos centraremos en configurar el protocolo dinámico.

Configuración de OSPF en vdom root.

Paso 1: Agregamos una interfaz loopback que nos servirá para anunciar nuestra LAN_1, debido a que es un ambiente de laboratorio y las interfaces físicas no tienen nada conectado necesitamos crear esta interfaz lógica que siempre este activa para que el proceso OSPF converja, para esto nos vamos al menú ***Network > Interfaces*** y damos click en *Create New > Interface.*

Name: Loopback0
Alias: RouterID
Type: Loopback Interface
Virtual domain: root
Role: LAN
IP/Netmask: 192.168.10.1/24
Administrative Access: PING

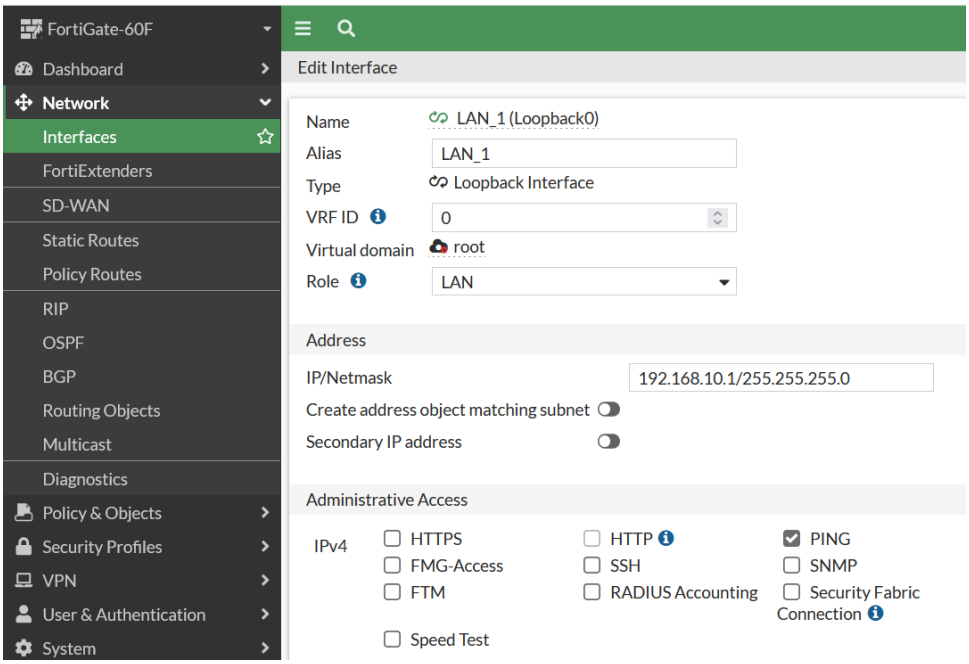


Figura 2. Configuración de interfaz loopback en vdom root.

Paso 2: Por defecto el enrutamiento avanzado no viene activado por lo que debemos activarlo en el menú ***System > Feature Visibility*** y activamos la opción de ***Advance Routing.***

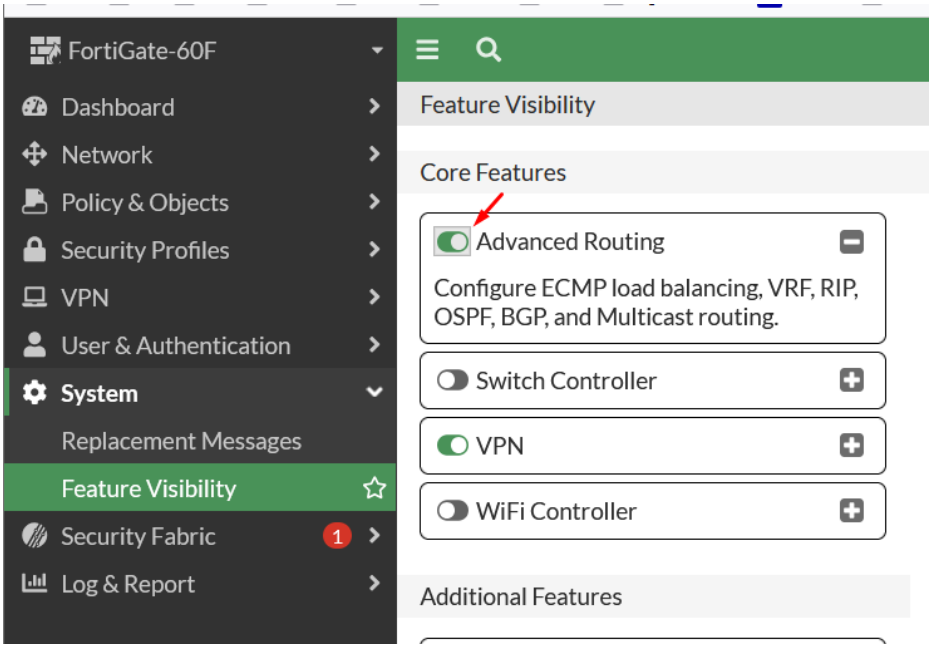


Figura 3. Activación de enrutamiento avanzado en vdom root.

Paso 3: Ahora que ya nos aparecen los protocolos dinámicos de enrutamiento seleccionamos OSPF y configuramos lo siguiente.

Router ID: 1.1.1.1

Areas: Creare New

Area ID: 0.0.0.0

Type: Regular

Authentication: None

Networks: Create New (se deben agregar las 2 redes)

Area: 0.0.0.0

IP/Netmask: 192.168.10.0/24

IP/Netmask: 10.0.0.0/30

Interfaces: Create New

Name: Router1

Interface: vdomlink0

IP: 0.0.0.0

Prefix length: 0 (default)

Cost: 0 (default)

Priority: 1 (default)

Authentication: None (default)

BFD: Global (default)

Network type: Broadcast (default)

Timers:

Hello interval: 10

Dead interval: 40

Todos los otros parámetros se dejan por defecto y se aplican los cambios.

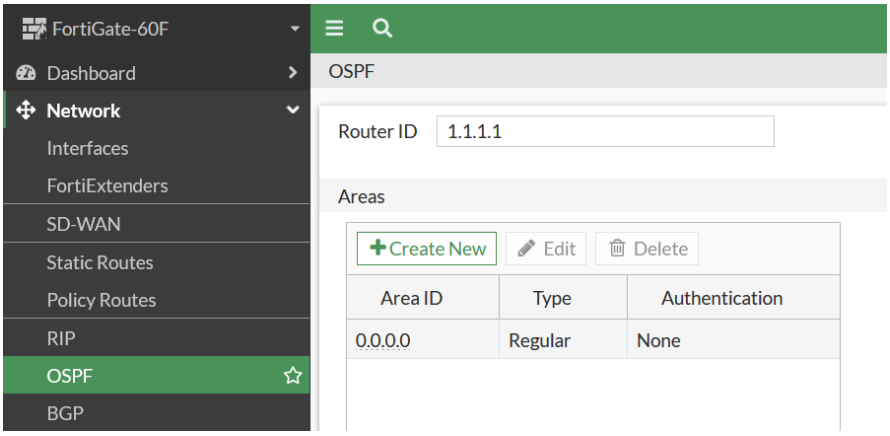


Figura 4. Configuración de *Router ID y Areas* en vdom root.

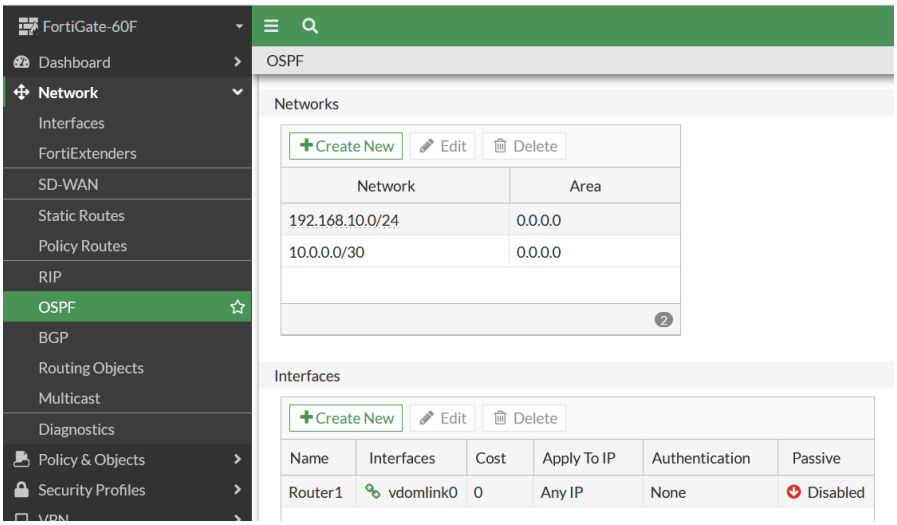


Figura 5. Configuración de *Interfaces y Networks* en vdom root.

Paso 4: Revisión de configuración usando la CLI

```
FortiGate-60F (root) # config router ospf

FortiGate-60F (ospf) # show
config router ospf
    set router-id 1.1.1.1
    config area
        edit 0.0.0.0
        next
    end
    config ospf-interface
        edit "Router1"
            set interface "vdomlink0"
            set dead-interval 40
            set hello-interval 10
            set network-type point-to-point
        next
    end
    config network
        edit 1
            set prefix 192.168.10.0 255.255.255.0
        next
        edit 2
            set prefix 10.0.0.0 255.255.255.252
        next
    end
    config redistribute "connected"
    end
    config redistribute "static"
    end
    config redistribute "rip"
    end
    config redistribute "bgp"
    end
    config redistribute "isis"
    end
end
```

Figura 6. Revisión de configuraciones de OSPF en vdom root usando la CLI.

Configuración de OSPF en vdom A

Paso 1: Agregamos una interfaz loopback que nos servirá para anunciar nuestra LAN_2, debido a que es un ambiente de laboratorio y las interfaces físicas no tienen nada conectado necesitamos crear esta interfaz lógica que siempre este activa para que el proceso OSPF converja, para esto nos vamos al menú ***Network > Interfaces*** y damos click en *Create New > Interface*

Name: Loopback1
Alias: LAN_2
Type: Loopback Interface
Virtual domain: VDOM-A
Role: LAN
IP/Netmask: 192.168.20.1/24

Administrative Access: PING

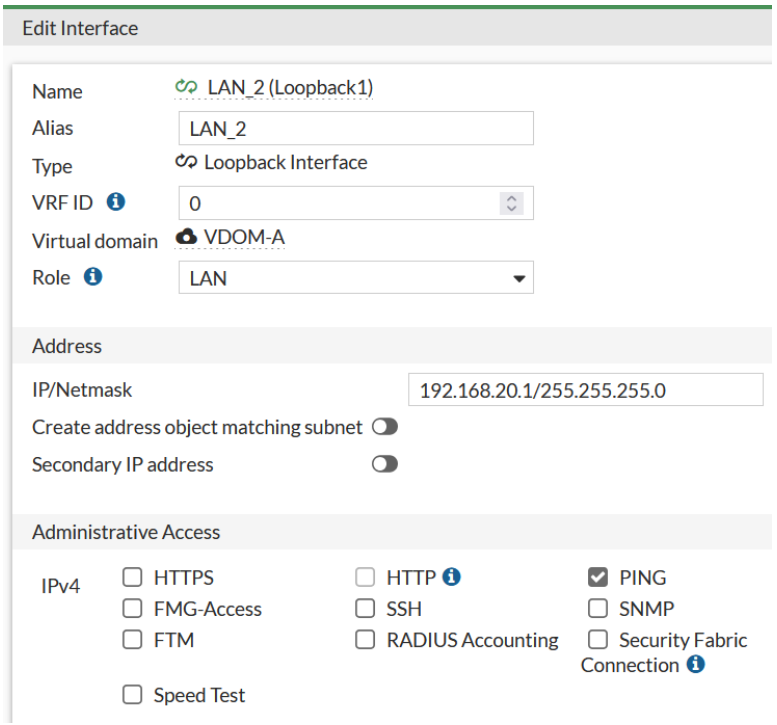


Figura 7. Configuración de interfaz loopback en vdom A.

Paso 2: Por defecto el enrutamiento avanzado no viene activado por lo que debemos activarlo en el menú ***System > Feature Visibility*** y activamos la opción de ***Advance Routing.***

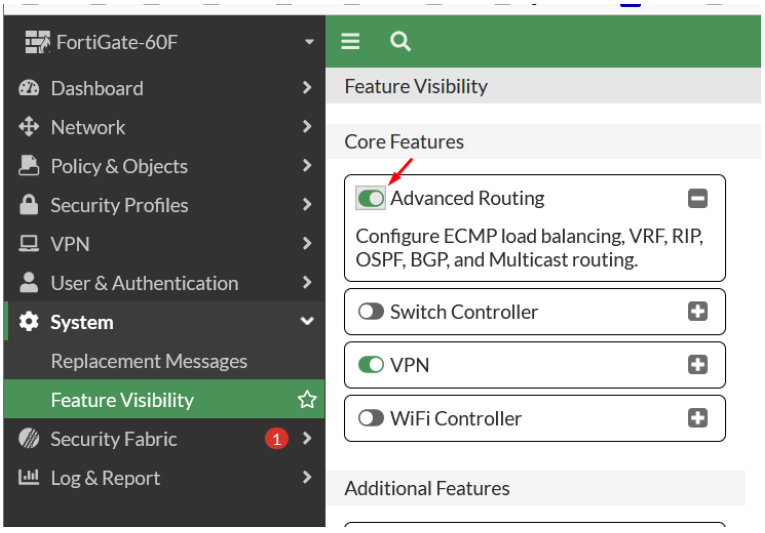


Figura 8. Activación de enrutamiento avanzado en vdom A.

Paso 3: Ahora que ya nos aparecen los protocolos dinámicos de enrutamiento seleccionamos OSPF y configuramos lo siguiente.

Router ID: 2.2.2.2
Areas: Creare New
Area ID: 0.0.0.0
Type: Regular
Authentication: None
Networks: Create New
Area: 0.0.0.0
IP/Netmask: 192.168.20.0/24
IP/Netmask: 10.0.0.0/30
Interfaces: Create New
Name: Router2
Interface: vdomlink1
IP: 0.0.0.0
Prefix length: 0 (default)
Cost: 0 (default)
Priority: 1 (default)
Authentication: None (default)
BFD: Global (default)
Network type: Broadcast (default)
Timers:
Hello interval: 10
Dead interval: 40

Todos los otros parámetros se dejan por defecto y se aplican los cambios.

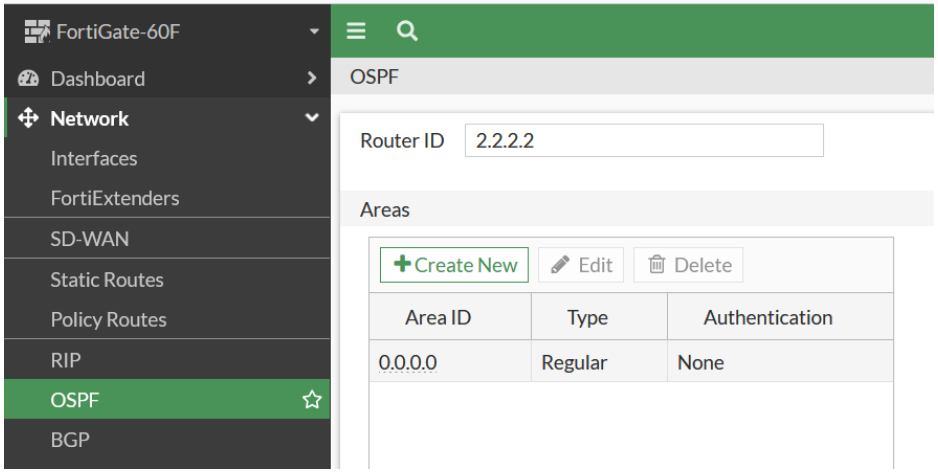


Figura 9. Configuración de *Router ID y Areas* en vdom A.

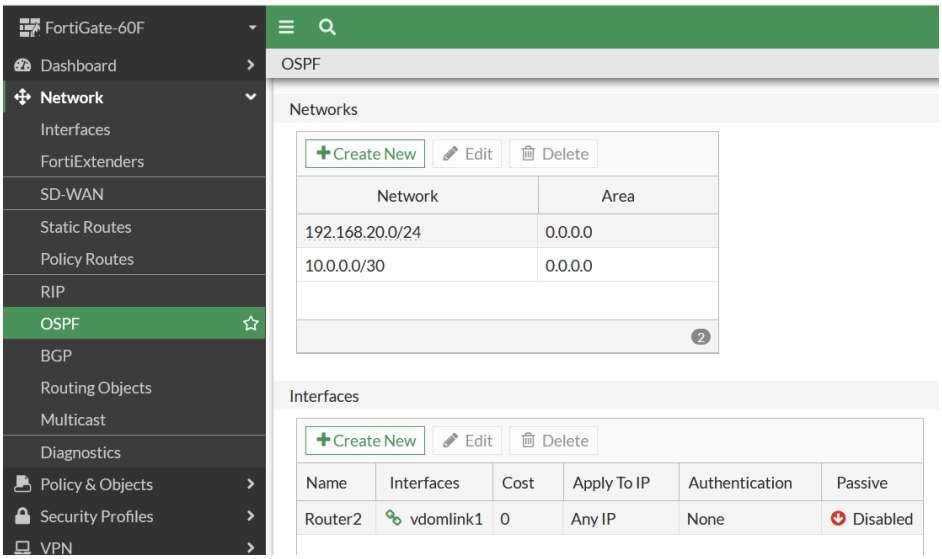


Figura 10. Configuración de *Interfaces y Networks* en vdom A.

Paso 4: Revisión de configuración usando la CLI

```
FortiGate-60F (VDOM-A) # config router ospf

FortiGate-60F (ospf) # show
config router ospf
    set router-id 2.2.2.2
    config area
        edit 0.0.0.0
        next
    end
    config ospf-interface
        edit "Router2"
            set interface "vdomlink1"
            set dead-interval 40
            set hello-interval 10
            set network-type point-to-point
        next
    end
    config network
        edit 1
            set prefix 192.168.20.0 255.255.255.0
        next
        edit 2
            set prefix 10.0.0.0 255.255.255.252
        next
    end
    config redistribute "connected"
    end
    config redistribute "static"
    end
    config redistribute "rip"
    end
    config redistribute "bgp"
    end
    config redistribute "isis"
    end
end
```

Figura 11. Revisión de configuraciones de OSPF en vdom A usando la CLI.

Creación de políticas de seguridad

Paso 1: Crear una política en el vdom root que permita el tráfico que se origina en la red 192.168.10.0/24 con destino 192.168.20.0/24

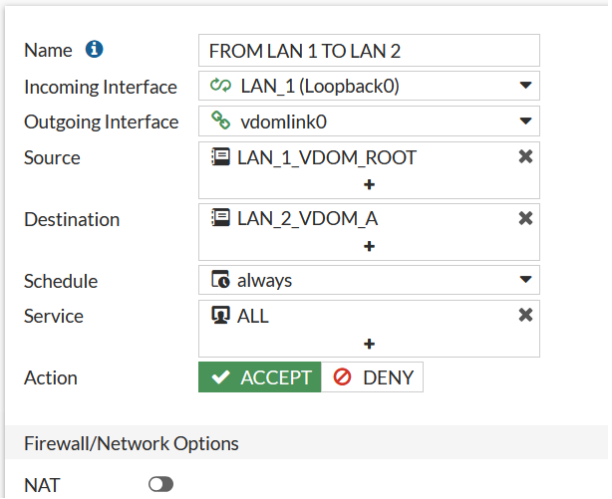


Figura 12. Política en vdom root desde LAN_1 hacia LAN_2.

Paso 2: Crear una política en el vdom root que permita el tráfico que se origina en la red 192.168.20.0/24 con destino 192.168.10.0/24

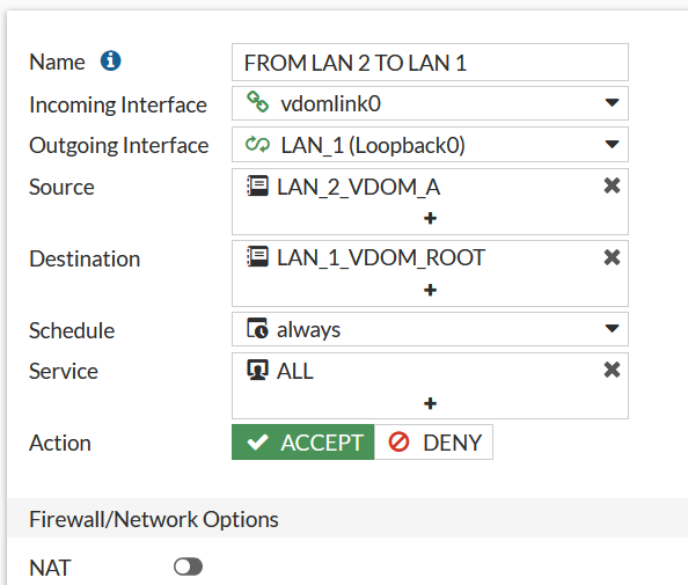


Figura 13. Política en vdom root desde LAN_1 hacia LAN_2.

Paso 3: Crear una política en el vdom A, que permita el tráfico que se origina en la red 192.168.20.0/24 con destino 192.168.10.0/24

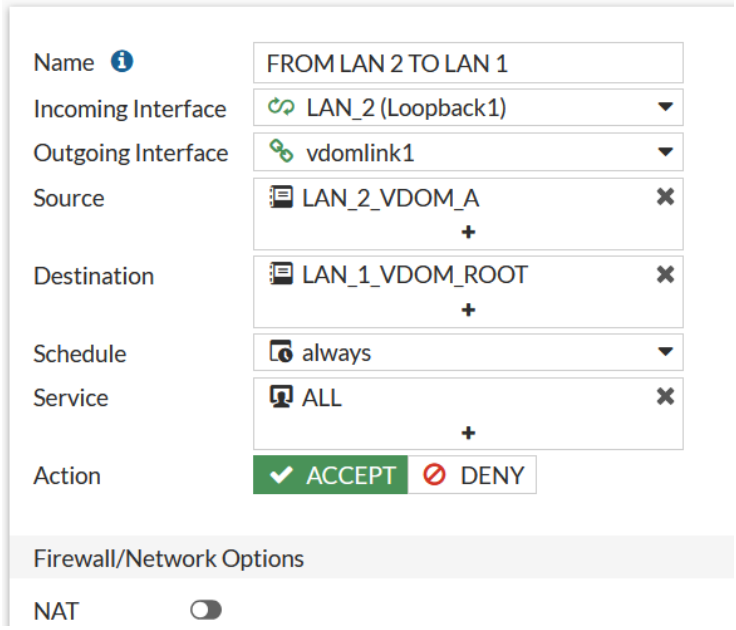


Figura 14. Política en vdom A desde LAN_1 hacia LAN_2.

Paso 4: Crear una política en el vdom A, que permita el tráfico que se origina en la red 192.168.10.0/24 con destino 192.168.20.0/24

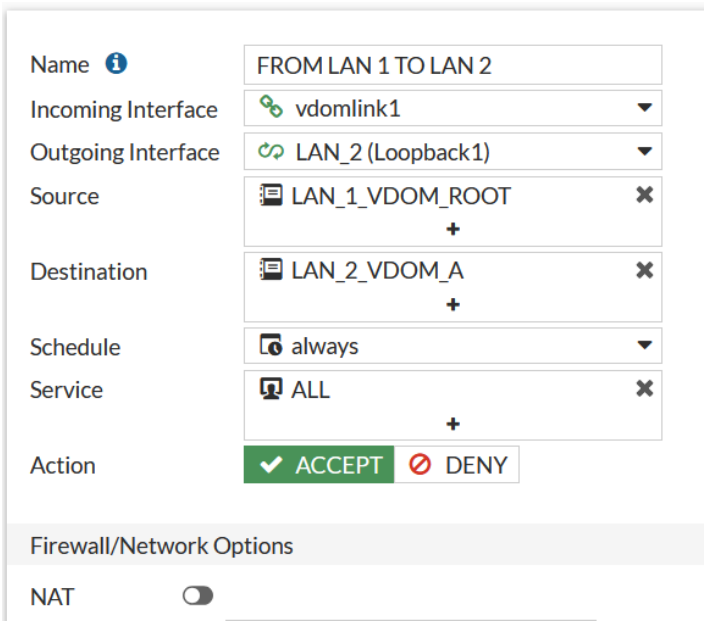


Figura 15. Política en vdom roAot desde LAN_1 hacia LAN_2.

Comandos de revisiones y pruebas

Paso 1: Revisar vecinos con los que se haya establecido adyacencia en el proceso OSPF.

get router info ospf neighbor

```
FortiGate-60F (root) # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2           1   Full/ -         00:00:40    10.0.0.2        vdomlink0
```

Figura 16. Revisión de tabla de vecinos en vdom root.

```
FortiGate-60F (VDOM-A) # get router info ospf neighbor
OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address         Interface
1.1.1.1           1   Full/ -         00:00:35    10.0.0.1        vdomlink1
```

Figura 17. Revisión de tabla de vecinos en vdom A.

Paso 2: Revisar la tabla de enrutamiento para el destino especifico en cada vdom.

get router info routing-table details [IP ESPECIFICA]

```
FortiGate-60F (root) # get router info routing-table details 192.168.20.1

Routing table for VRF=0
Routing entry for 192.168.20.1/32
  Known via "ospf", distance 110, metric 200, best
  Last update 03:30:26 ago
  * vrf 0 10.0.0.2, via vdomlink0
```

Figura 18. Revisión de tabla de enrutamiento para el destino 192.168.20.1

```
FortiGate-60F (VDOM-A) # get router info routing-table details 192.168.10.1

Routing table for VRF=0
Routing entry for 192.168.10.1/32
  Known via "ospf", distance 110, metric 200, best
  Last update 03:30:46 ago
  * vrf 0 10.0.0.1, via vdomlink1
```

Figura 19. Revisión de tabla de enrutamiento para el destino 192.168.10.1.

Como puede apreciarse en las figuras 18 y 19 las redes remotas respectivas se conocen mediante el protocolo OSPF con una distancia 110 por la interfaz ***vdomlink***

Paso 3: Pruebas de conectividad

```
FortiGate-60F (root) # execute ping-options source 192.168.10.1

FortiGate-60F (root) # exe ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1): 56 data bytes
64 bytes from 192.168.20.1: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 192.168.20.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 192.168.20.1: icmp_seq=4 ttl=255 time=0.1 ms

--- 192.168.20.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.2 ms
```

Figura 20. Prueba de conectividad desde el LAN1 hacia LAN2.

```
FortiGate-60F (VDOM-A) # execute ping-options source 192.168.20.1

FortiGate-60F (VDOM-A) # execute ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1): 56 data bytes
64 bytes from 192.168.10.1: icmp_seq=0 ttl=255 time=0.2 ms
64 bytes from 192.168.10.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=255 time=0.0 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=255 time=0.1 ms

--- 192.168.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.2 ms
```

Figura 21. Prueba de conectividad desde el LAN2 hacia LAN1.

Conclusiones

- Con la elaboración de la práctica se concluye que configurar un protocolo dinámico de enrutamiento se necesita de un conocimiento más avanzado en redes pero que es la forma es la que se pueden elaborar soluciones escalables.

- Se configuro el protocolo de enrutamiento dinámico OSPF para comunicar dos redes remotas que pertenecen a un diferente dominio virtual.

- Se aprendieron comandos que permiten la revisión de la tabla de enrutamiento y hacer pruebas de conectividad de capa 3 entre firewall.

Práctica 16: Regla de DNAT

Introducción

En la presente práctica se explicará el proceso para una regla de ***Destinación NAT*** para publicar un servicio interno hacia una red externa.

Objetivo general

- Publicar un servicio interno protegido por el FortiGate en el perímetro

Objetivos específicos

- Acceder desde una red externa a servicio web activo en la red interna

- Asociar reglas de *port-fordwarding* con políticas de seguridad

Desarrollo

En esta práctica se debe aplicar una regla en el firewall con la cual podamos publicar el puerto 80 del servidor web con IP 10.10.10.10 para que sea alcanzado externamente por la IP 192.168.100.210 por el mismo puerto 80 desde la PC externa con IP 192.168.100.4.

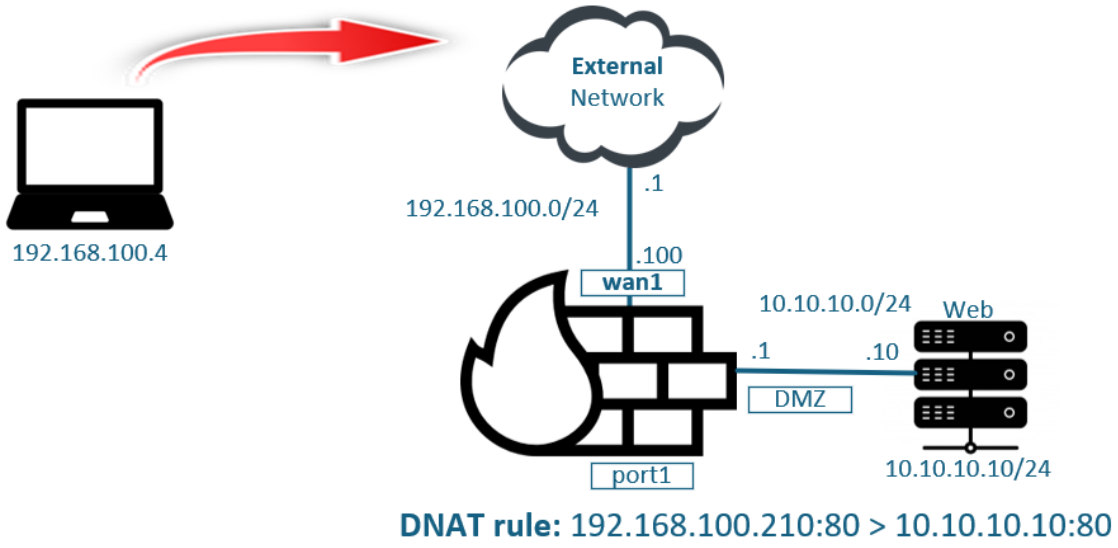


Figura 1. Topología para DNAT.

En la tabla 1 se muestra la regla que debemos aplicar:

IP externa	Puerto externo	IP interna	Puerto interno
192.168.100.210	80	10.10.10.10	80

Tabla 1. Detalle de la regla DNAT

Configuración de DNAT

Paso 1: Para crear el objeto de NAT o Virtual IP nos vamos al menú ***Policy & Object > Virtual IPs*** y creamos uno nuevo con las siguientes configuraciones.

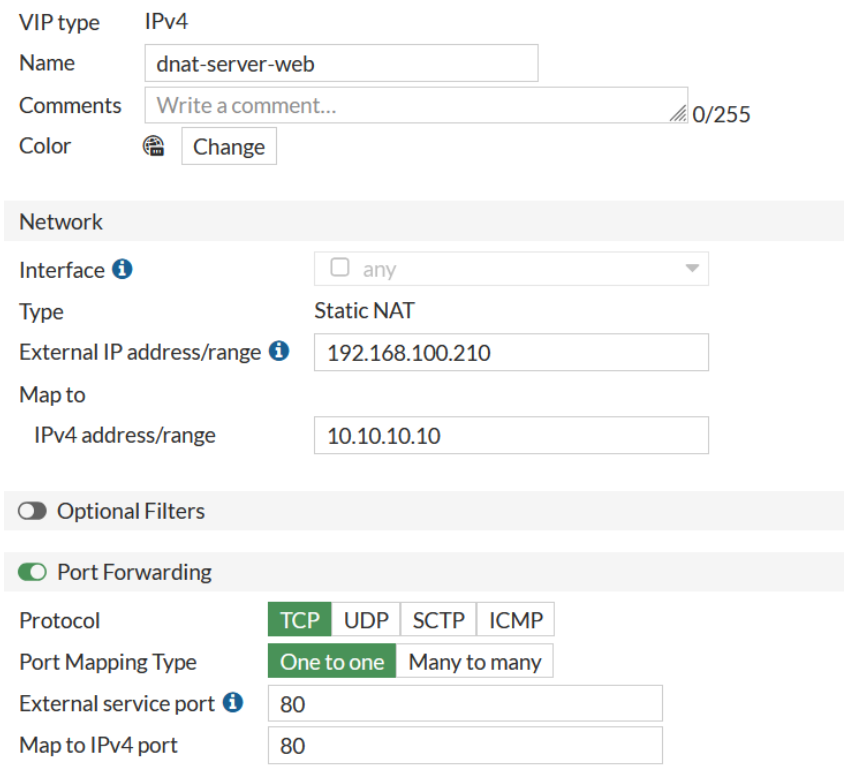


Figura 2. Virtual IP para la publicación del servicio.

Como observamos en la figura 2 se configuró como dirección externa la que nos especifican en la tabla 1 la cual esta mapeada a la IP real del servidor 10.10.10.10

Configuración de política

Paso 1: Ahora procederemos a crear la política para esto nos vamos a ***Policy & Object > Firewall Policy*** y creamos una nueva.

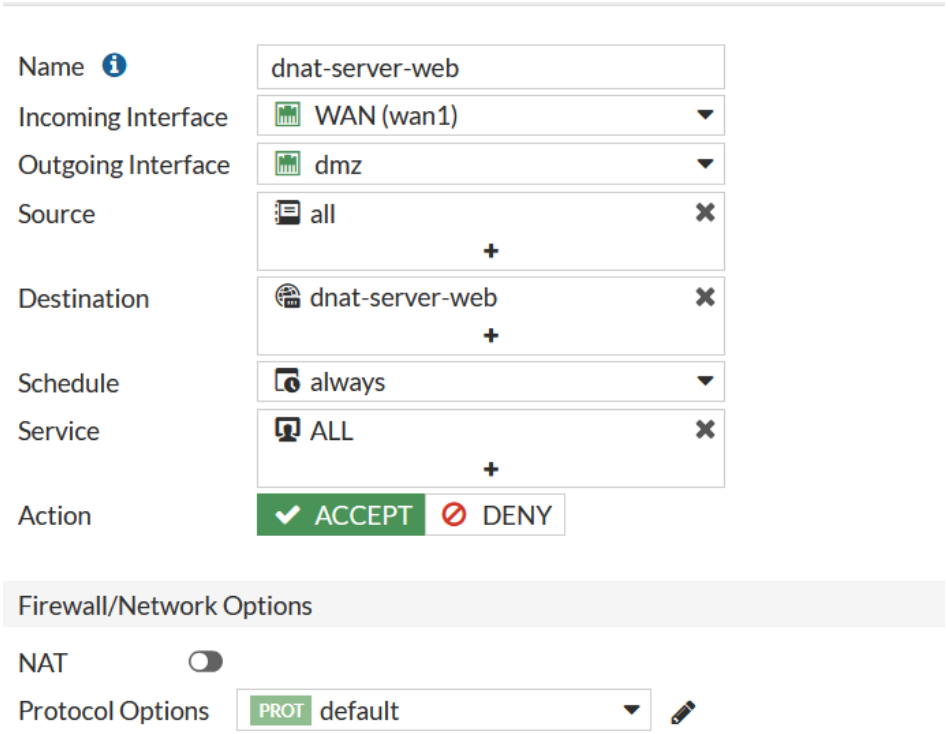


Figura 3. Política de seguridad para el DNAT.

Se ha establecido el objecto de Virtual IP que creamos anteriormente como el destino en la política de seguridad, esto nos permite realizar la traslación de IP.

Pruebas

Prueba 1: Cargar el index por defecto del servidor web:

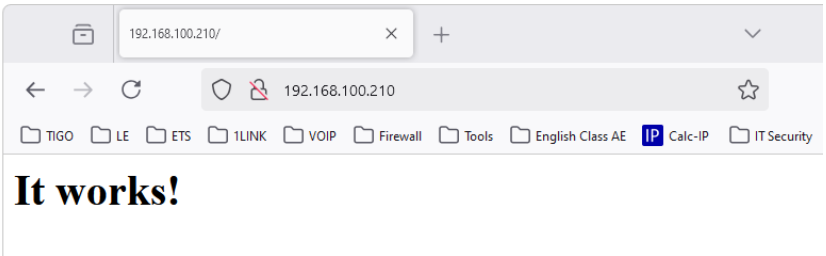


Figura 4. Index por defecto del servidor web.

Prueba 2: Montar una página web en el servidor Apache y cargarla mediante la IP externa.

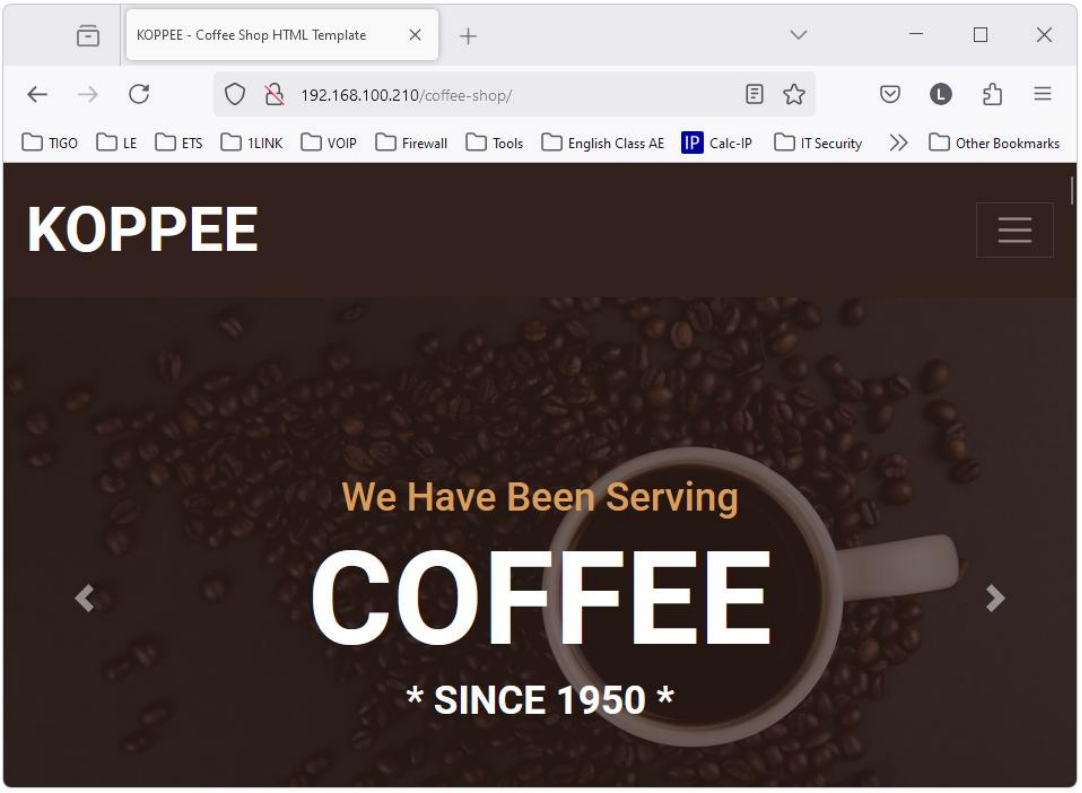


Figura 5. Página web especifica dentro del servidor.

Prueba 3: Usar nmap para escanear los puertos que tiene publicas el servidor web 10.10.10.10

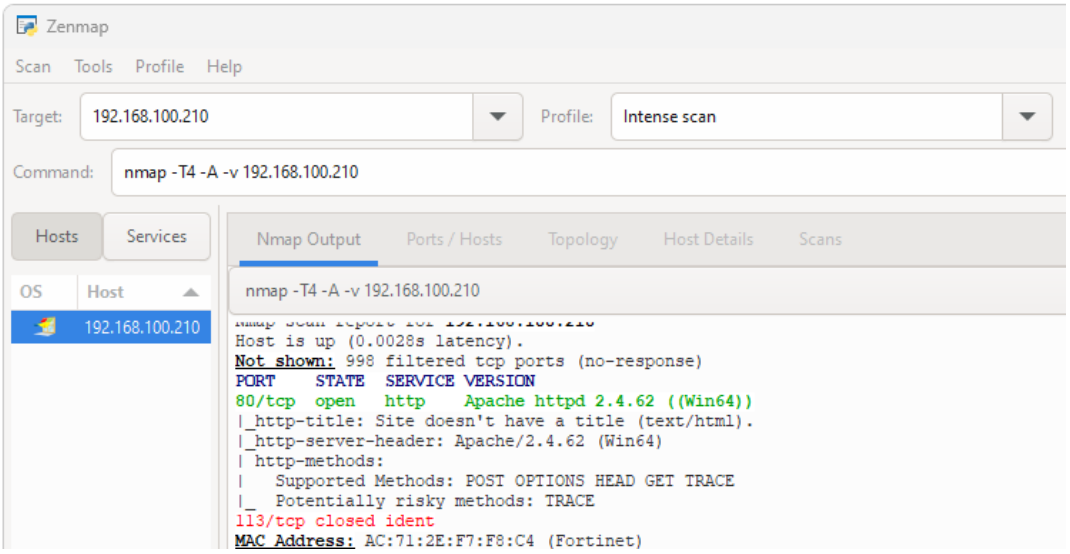


Figura 6. Escaneo de puertos del servidor web.

Como se muestra en la figura 6, el resultado del escaneo fue que encontró un servicio de Apache corriendo sobre el puerto 80.

Prueba 4: Revisión de logs en FortiGate en el menú ***Log & Report > Forward traffic***

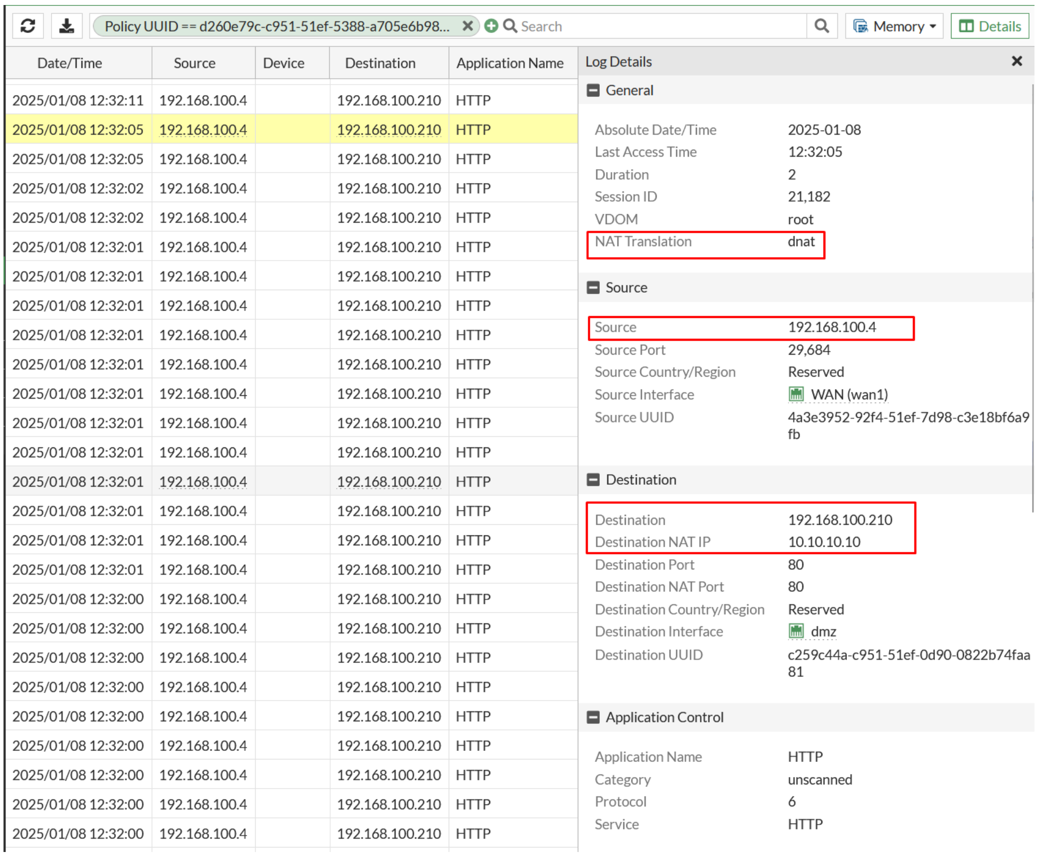


Figura 7. Revisión de logs

Conclusiones

- Se publicó exitosamente el servicio www de un servidor interno para que pueda ser alcanzado externamente, este concepto se puede extender cuando hacemos esta publicación a través de internet por medio de una dirección IP pública.

- Usando una PC externa fue posible cargar los servicios web internos esto debido que el Firewall permite las peticiones, pero es posible delimitar el origen y tipo de tráfico que requerimos permitir en la política de seguridad.

Práctica 17: Concentrador VPN.

Introducción

En la presente práctica se configurará un concentrador VPN que nos permitirá conectarnos remotamente usando un cliente VPN a la infraestructura de red interna de una corporación.

Esta topología de red es muy importante cuando queremos implementar soluciones de Teletrabajo en la cual los clientes pueden estar en cualquier parte del mundo y por internet conectarse a la red interna de la empresa.

Objetivo general

- Configurar un concentrador VPN que autentique con la base de datos de usuarios locales en el FortiGate.

Objetivos específicos

- Instalar y configurar el cliente VPN de Fortinet
- Crear una base de datos de usuarios locales en el FortiGate
- Establecer una conexión segura entre el cliente remoto y el servidor web mediante IPSec.

Desarrollo

Como se muestra en la figura 1 se debe configurar la topología de red en la cual en el port1 del FortiGate esté conectado el servidor web con IP 10.0.0.10 y el FortiGate a su vez actúe como concentrador VPN y acepte conexiones remotas autenticadas en su WAN 192.168.100.100.

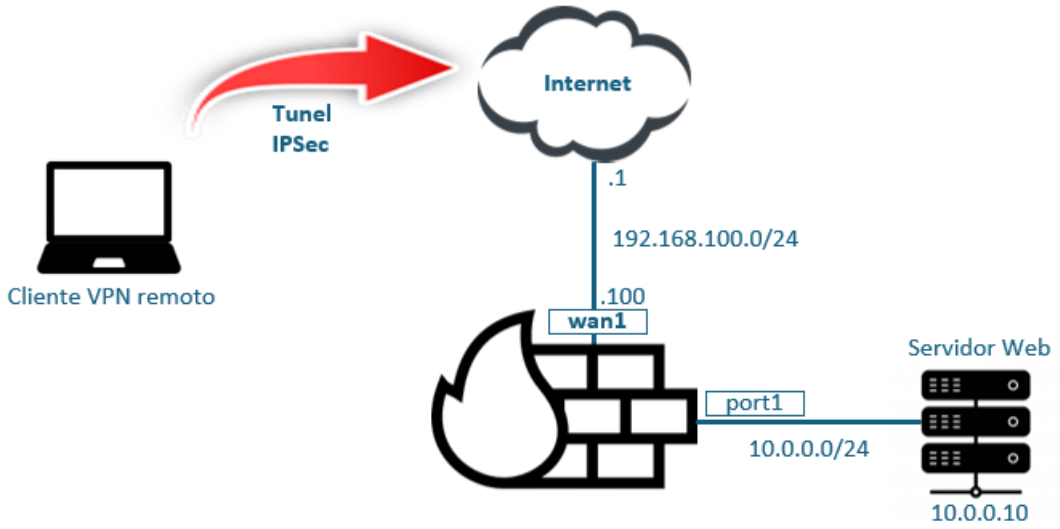


Figura 1. Topología de red para el concentrado VPN.

Configuración de base de datos de usuarios

Paso 1: Nos iremos al menú ***User & Authentication > User Definition*** y configuramos la siguiente base de datos de usuarios, damos click en Create New.

Usuario	Contraseña
RemoteUser1	VPNPassword1
RemoteUser2	VPNPassword2
RemoteUser3	VPNPassword3
RemoteUser4	VPNPassword4

Tabla 1. Base de datos de usuarios.

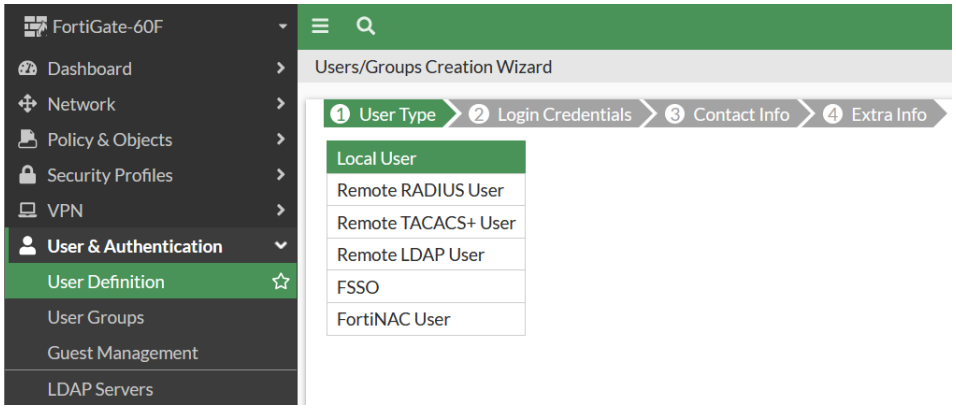


Figura 2. Selección del tipo de usuario.

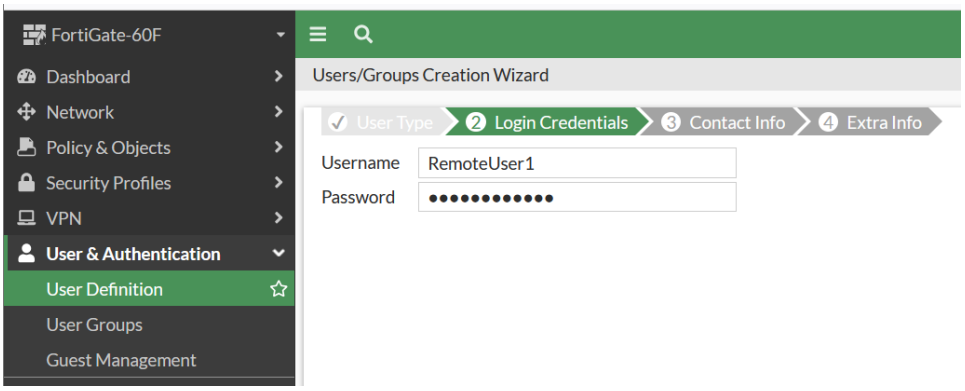


Figura 3. Establecimiento de credenciales.

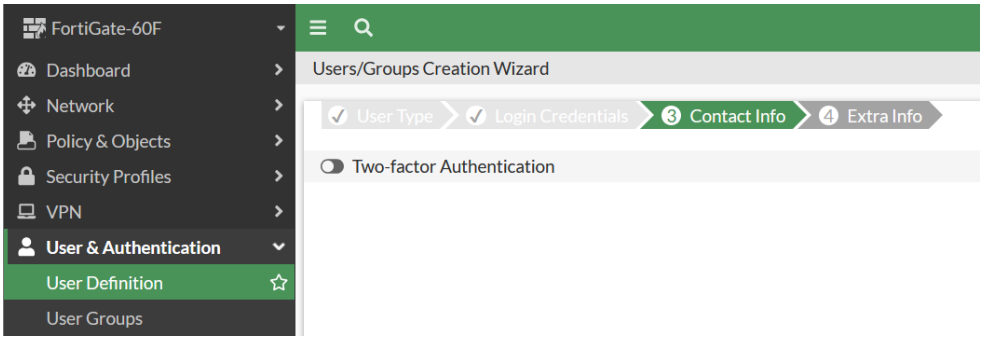


Figura 4. Parámetros adicionales del usuario.

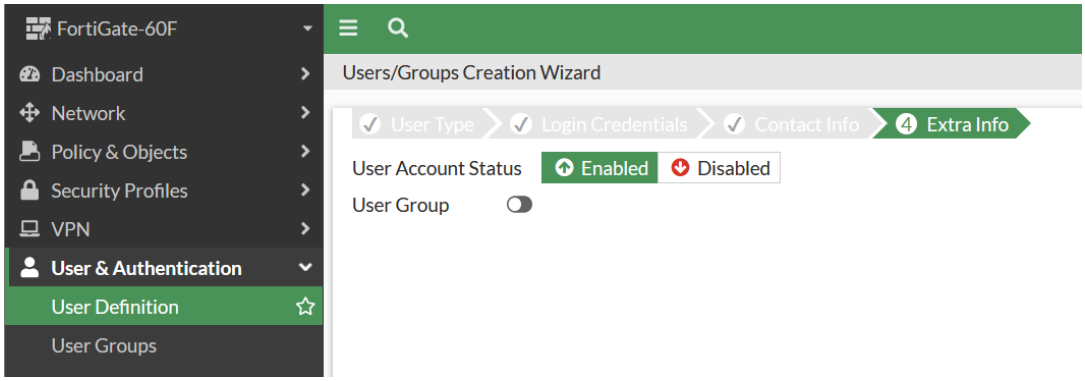


Figura 5. Estado del usuario (activo por defecto).

En la figura 5 nos percatamos que podemos asignarlo a un grupo, pero debido a que aún no hemos creado ningún grupo dejamos esa opción desactivada.

Paso 2: Ahora nos vamos al menú ***User & Authentication > User Groups*** y crearemos un grupo nuevo.

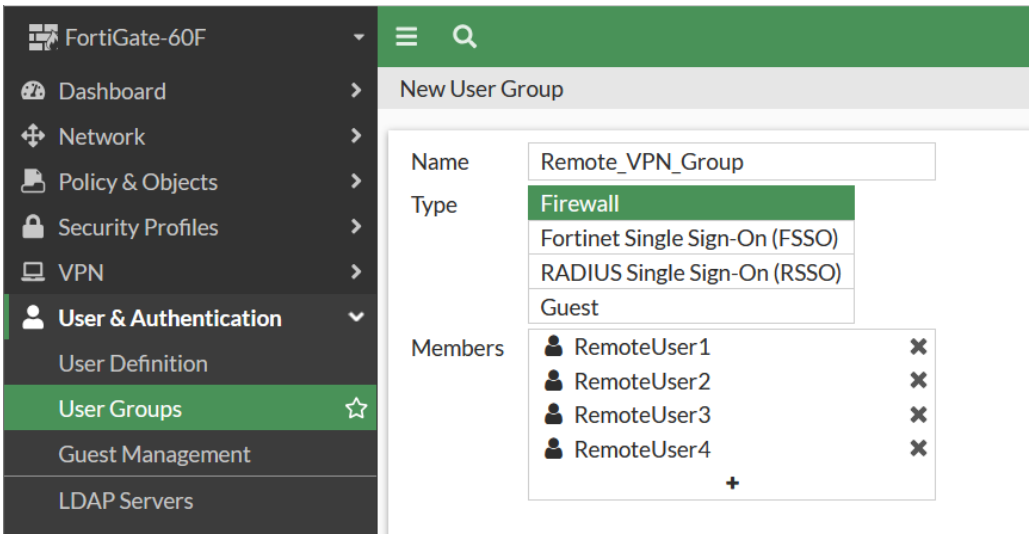


Figura 6. Grupo de usuarios que autenticará el concentrado VPN.

Configuración de concentrador VPN

Paso 1: Procederemos a configurar el concentrador VPN para esto nos vamos a ***VPN > IPSec Tunnels*** y creamos uno nuevo de tipo IPSec Tunnel. Debemos seleccionar el tipo de conexión como ***Remote Access*** y basada en el cliente de Fortinet.

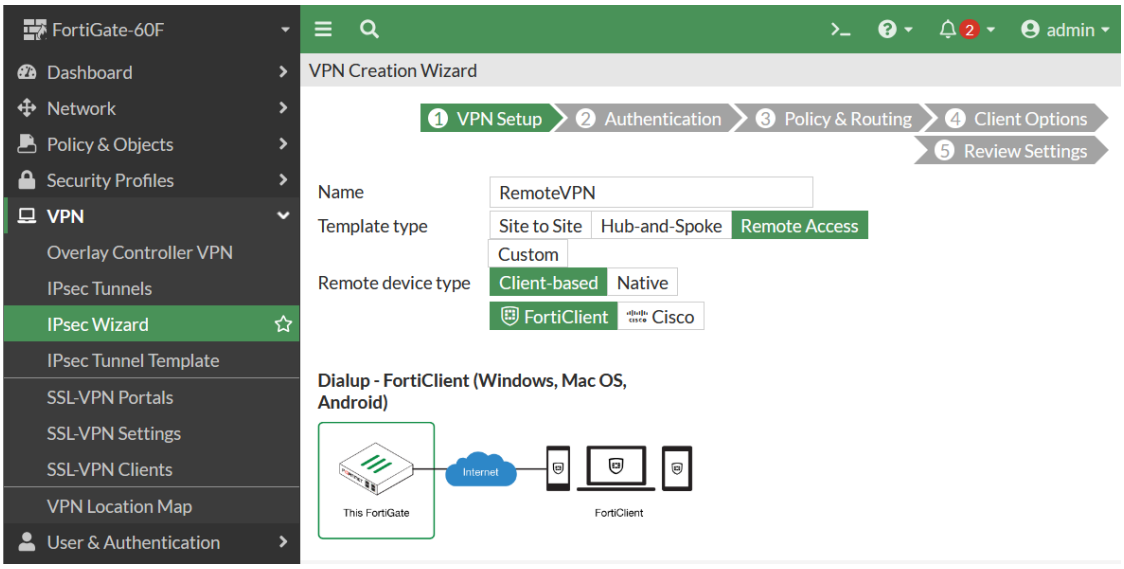


Figura 7. Tipo de configuración IPSec.

Paso 2: En el segundo paso nos pide configurar el tipo de autenticación, para nuestro concentrador usaremos ***Pre-shared key*** que es una clave pre compartida es decir que sabe el cliente o usuario remoto.

En ***User Group*** usamos el grupo de usuarios que creamos anteriormente.

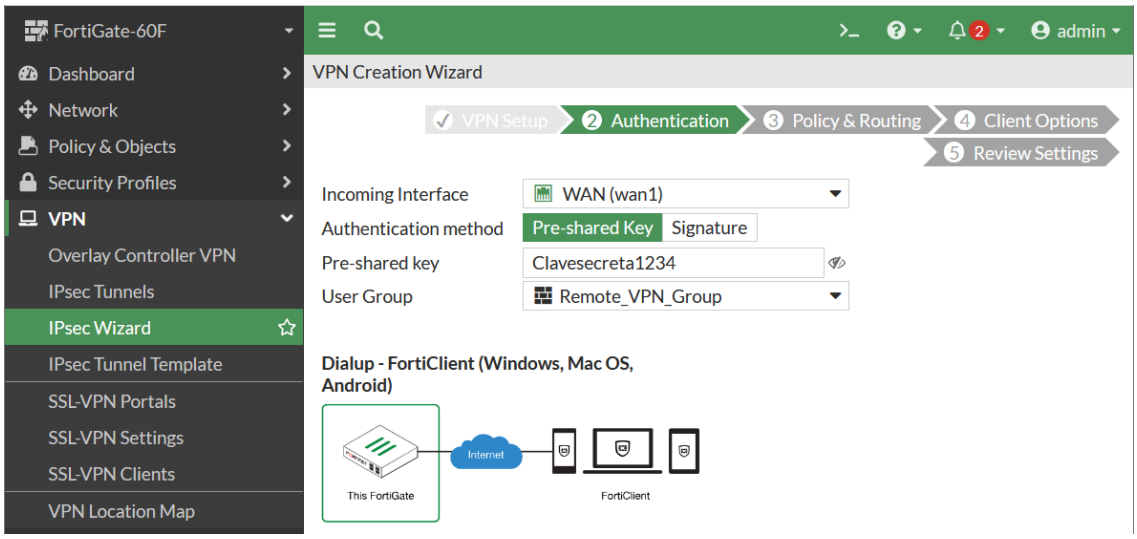


Figura 8. Tipo de autenticación en el concentrador VPN.

Paso 3: Ahora configuramos la red que enrutaremos por el túnel para este caso tenemos 2 opciones:

- **Full Tunnel:** Se enruta todo por el túnel
- **Split Tunnel:** Solo se enruta la red o IP especifica que definamos

Como nosotros solo queremos alcanzar una dirección IP especifica, dejaremos activado el ***IPV4 Split tunnel*** y en el ***Local Address*** estableceremos la dirección IP que requerimos sea alcanzable por el tunnel.

En la parte de ***Client Address Range*** establecemos el direccionamiento que se asignara en el cliente VPN y debe estar dimensionado en base a la cantidad de conexiones o clientes que tendremos en el concentrado VPN, para nuestra practica tomamos la red 10.200.50.0/24

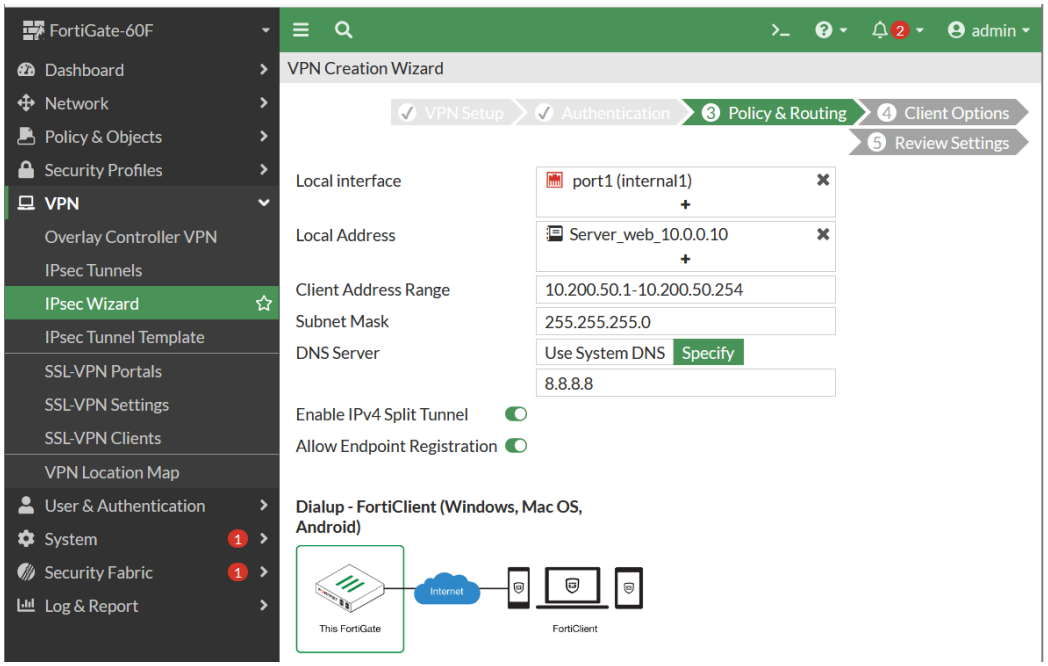


Figura 9. Asignación de direccionamiento IP en túnel.

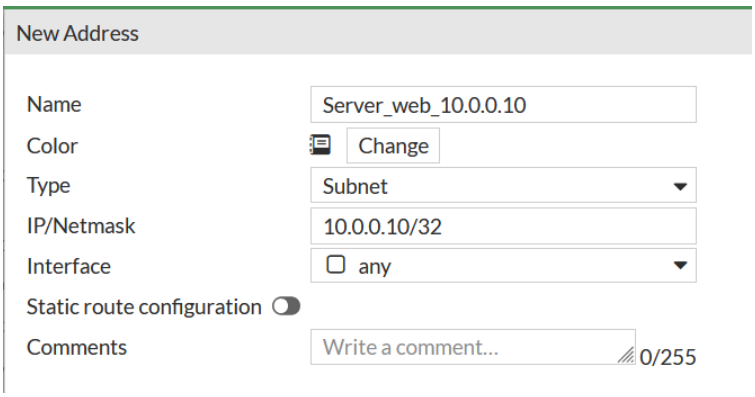


Figura 10. Creación de objeto para el servidor web.

Paso 4: En el paso 4 dejamos las opciones por defecto.

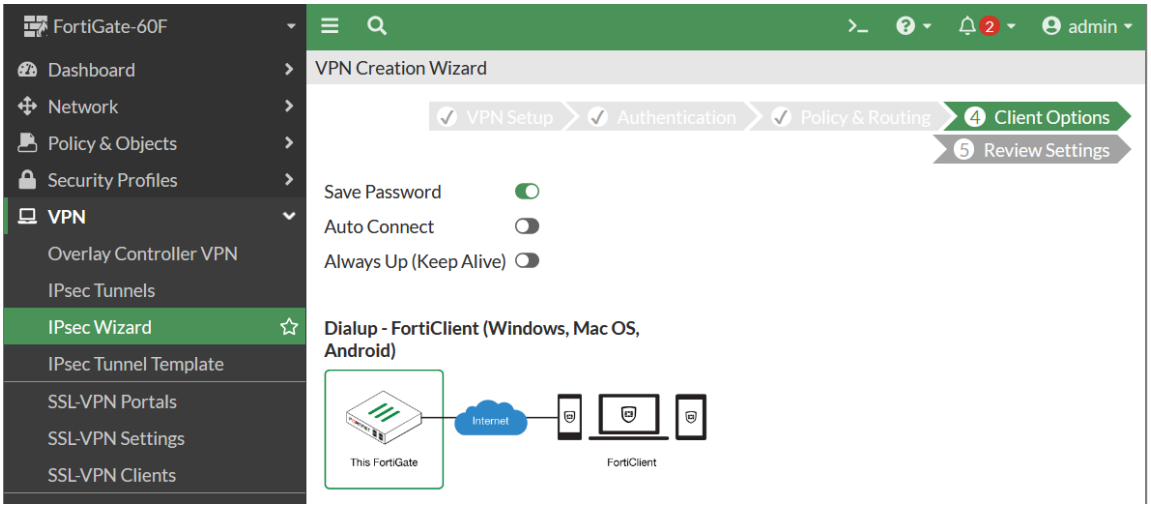


Figura 11. Opciones que se permitirán en el cliente VPN.

Paso 5: El último paso solo es una revisión de los parámetros que hemos configurado.

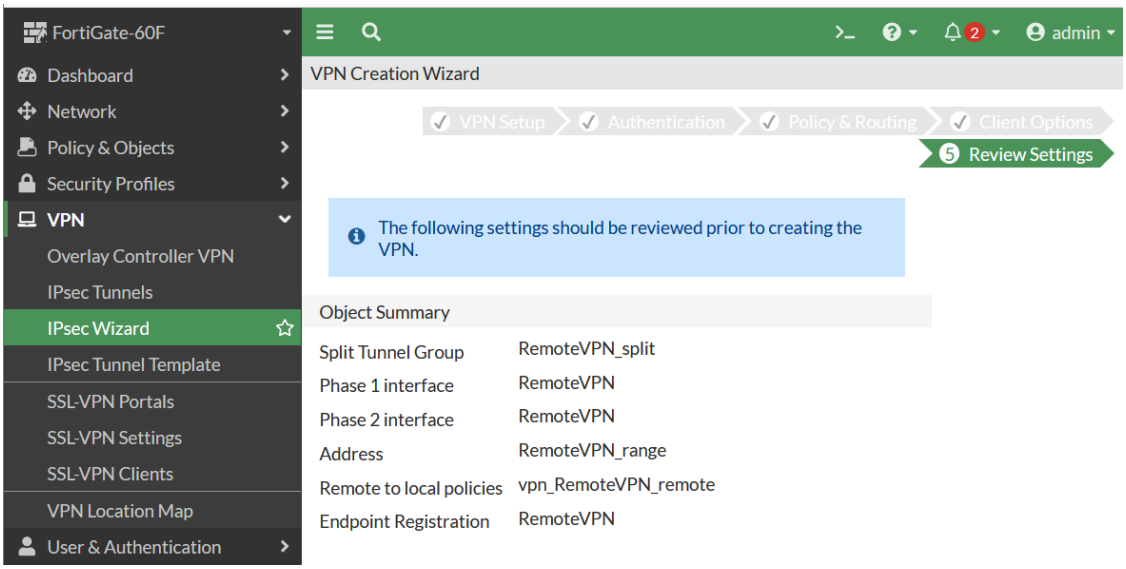


Figura 12. Revisión de parámetros configurados en el concentrador VPN.

Paso 6: Ahora procedemos a revisar que el túnel ya nos aparezca en el menú ***VPN > IPSec Tunnels*** nos aparecerá como inactivo debido a que no tenemos ninguna conexión.

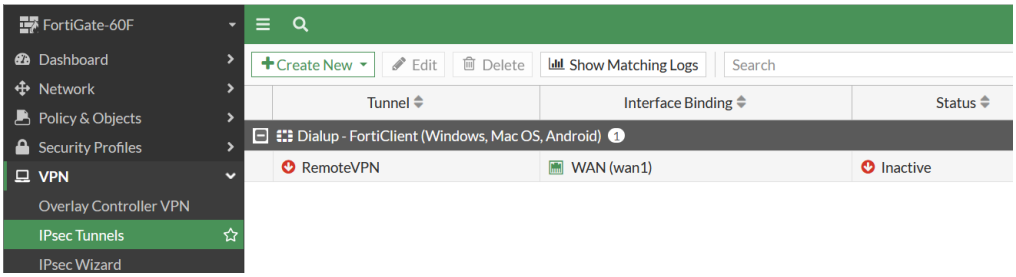


Figura 13. Estado de los túneles IPSec.

Paso 7: Lo siguiente es revisar la política de acceso que creo el asistente por defecto y desactivarle el NAT, nos vamos a **Policy & Object > Firewall Policy**

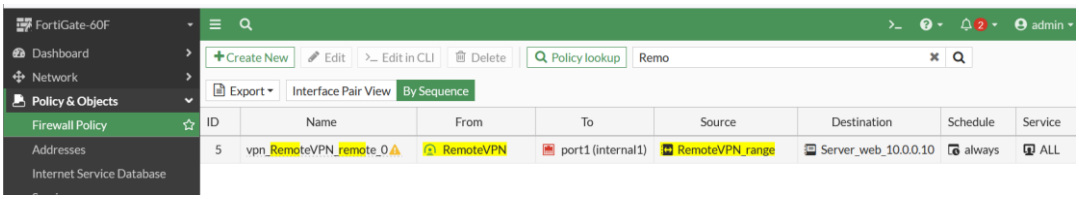


Figura 14. Política de acceso.

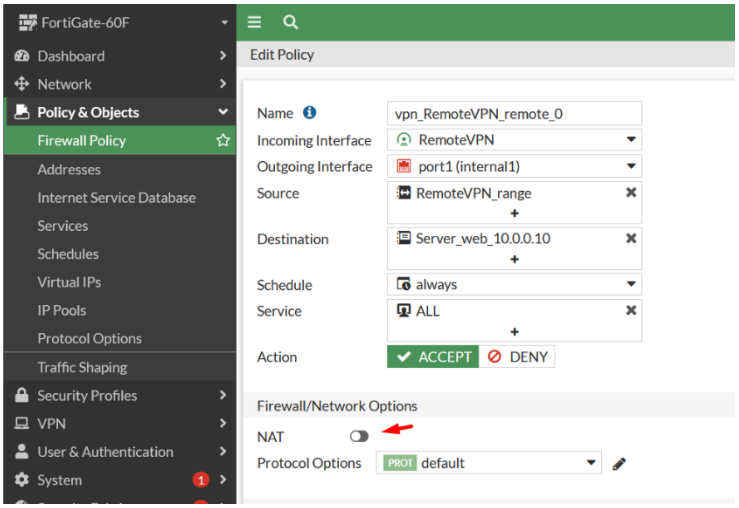


Figura 15. Modificación de política.

Observar que el **Incoming interface** en la política es una interface virtual que se origina en el FortiGate cuando creamos el túnel IPSec.

Instalación de cliente VPN FortiClient

Paso 1: Nos vamos al sitio oficial del fabricante para descargar el software gratuitamente del siguiente enlace.
https://www.fortinet.com/lat/support/product-downloads

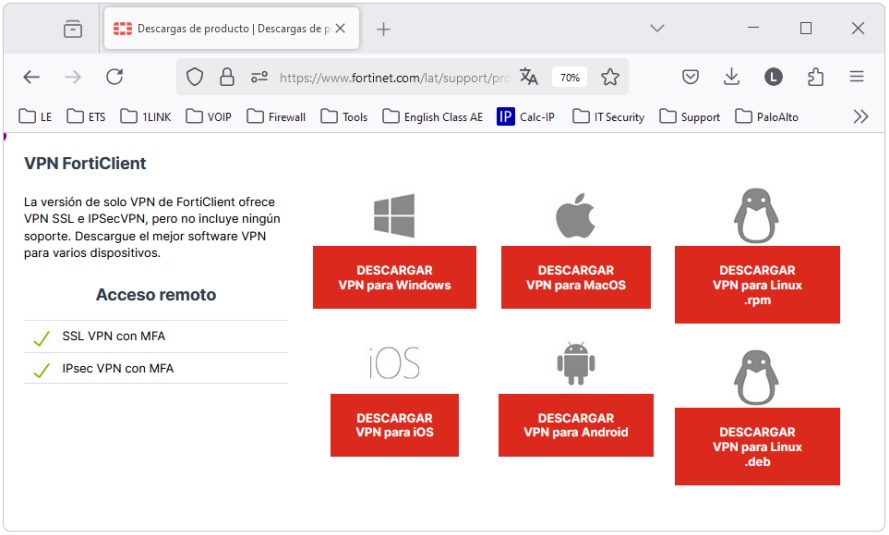


Figura 16. Descarga del cliente VPN FortiClient.

Ahora en la parte de “**Acceso Remoto**” y descargamos el correspondiente al sistema operativo del dispositivo remoto, para la práctica se realizará la conexión desde un dispositivo Windows.

Paso 2: Una vez descargado e instalado el cliente VPN procedemos a configurarlo, para esto agregamos una nueva conexión de tipo IPSec con los siguientes parámetros.

VPN Type: IPSec
Connection Name: Cualquier nombre que identifique la conexión
Remote Gateway: IP de la WAN del FortiGate
Preshared key: La clave que establecimos cuando configuramos la VPN

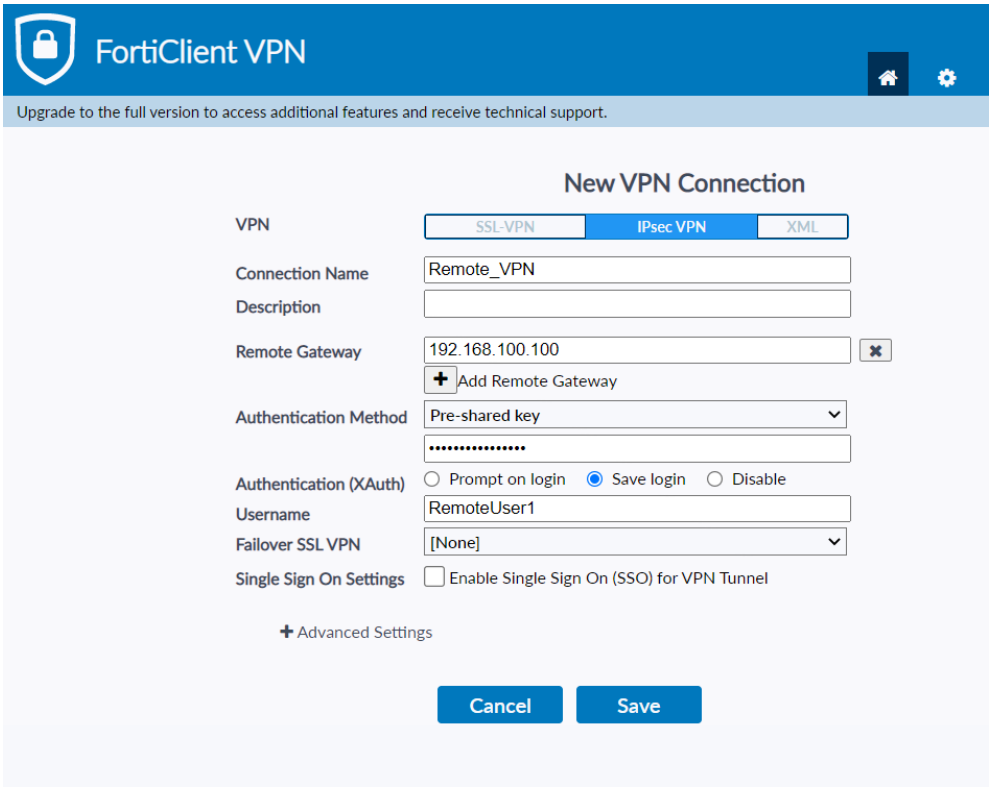


Figura 17. Configuración de cliente VPN.

Paso 3: Luego de guardar los cambios procedemos a introducir las credenciales de un usuario valido de los que creamos y asignamos al grupo de autenticación.

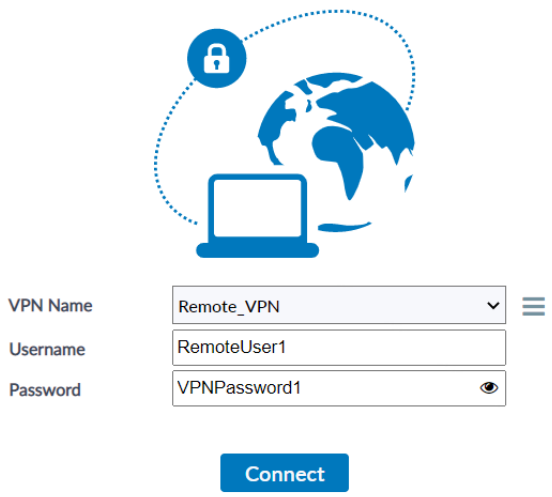


Figura 18. Ingreso de credenciales en FortiClient.

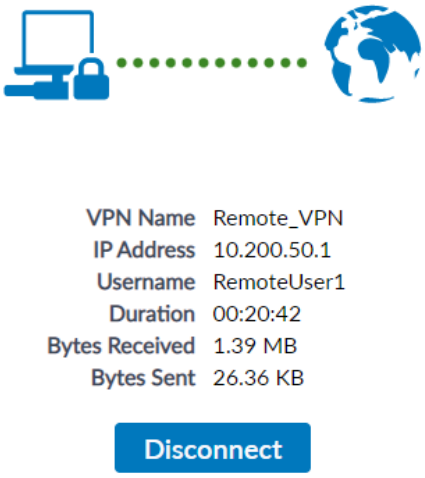


Figura 19. Conexión establecida.

Pruebas

Prueba 1: Desde la computadora que se conectó a la VPN abrir un navegador y cargar el servidor web 10.0.0.10. Como se aprecia en la figura 20 el servidor web cargo mediante su dirección IP interna sin necesidad de publicarlo con un DNAT.

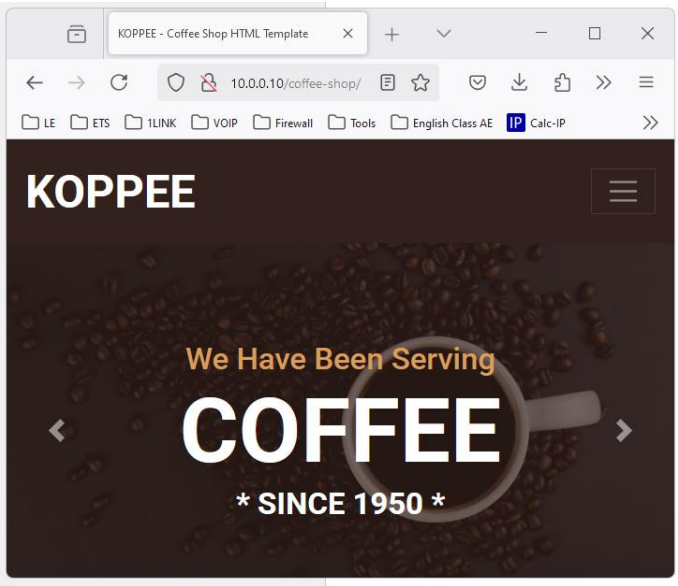


Figura 20. Sitio web cargado a través de la VPN.

Prueba 2: Revisar el estado del túnel en el firewall y los usuarios que se han conectado.

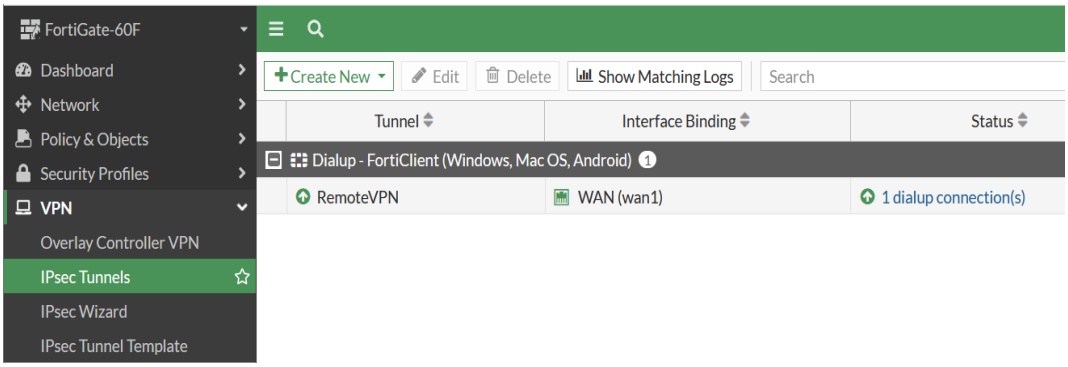


Figura 21. Estado del túnel IPSec.

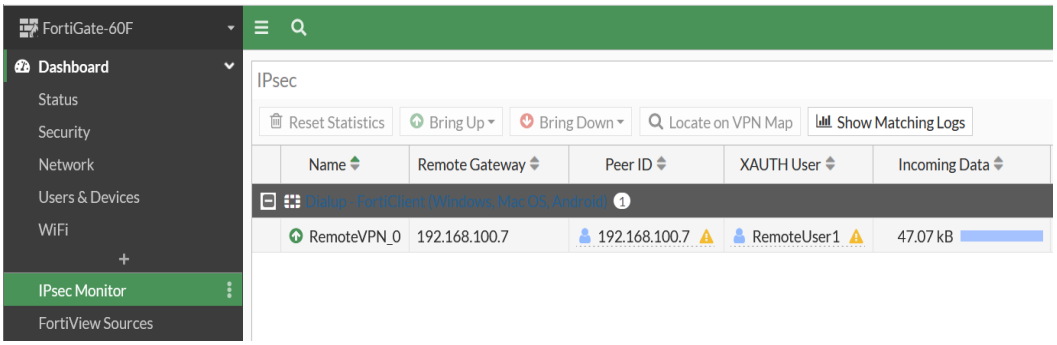


Figura 22. Usuarios conectados a la VPN.

Prueba 3: Revisar los LOG en el FortiGate.

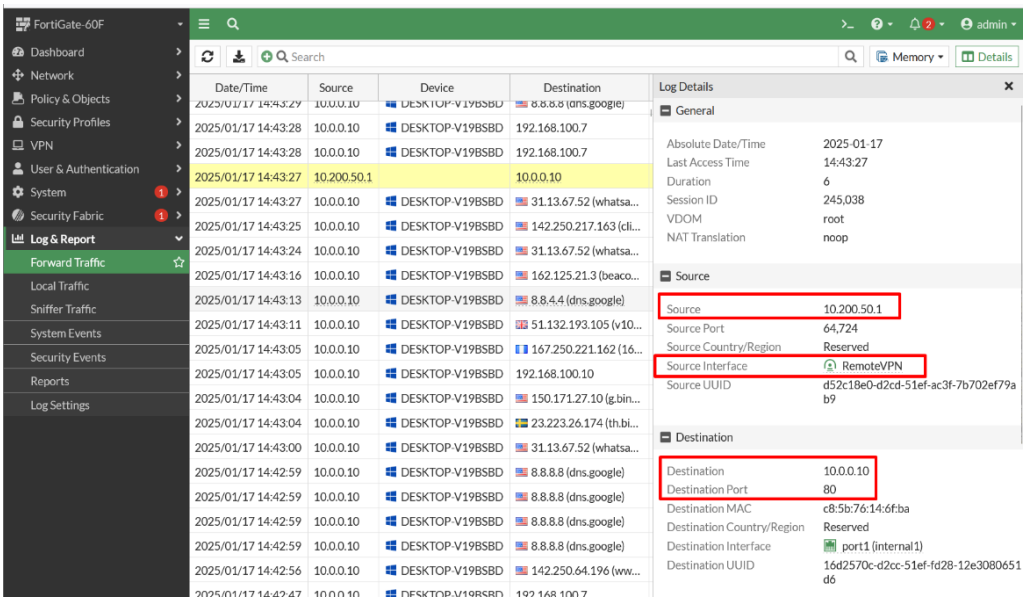


Figura 23. Logs relacionados al tráfico web.

Conclusiones

- Se configuró exitosamente el concentrador VPN con una base de datos de usuarios locales. En las implementaciones corporativas el FortiGate está integrado con el directorio activo y la autenticación se realiza con usuarios de dominio.

- Se instaló y configuró el cliente VPN y se estableció la conexión segura hacia el concentrador VPN.

- Se concluye que la conexión segura es posible por la interfaz virtual ***"RemoteVPN"*** creada en el FortiGate para recibir las conexiones remotas.