Interconexión de redes

Juan Sebastián Giraldo Adames

Daniel Esteban Charria Suarez

Universidad Cooperativa de Colombia

Infraestructura de Red IPv6 con Servicios Centrales y Firewall Perimetral en GNS3.

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El crecimiento de las redes empresariales y la adopción de nuevas tecnologías de comunicación IPv6 hacen necesario el diseño y la simulación de infraestructuras de red que reflejen las condiciones reales de operación en las organizaciones. Este proyecto se enfoca en la implementación y análisis de una topología de red multi-sede, con el propósito de comprender su funcionamiento, optimizar su rendimiento y fortalecer los principios de seguridad y segmentación. La simulación se desarrolla sobre un entorno que integra tres sedes interconectadas, administradas mediante un router core que simula la conexión a una red MPLS, replicando el comportamiento de redes corporativas reales. Cada sede cuenta con segmentación por VLANs, ruteo IPv6 implementado con OSPFv3, y gestión de seguridad a través de pfSense como firewall perimetral. Adicionalmente, se configuró un servidor local que brinda servicios internos a los usuarios autorizados, aplicando políticas y normativas de seguridad que limitan el acceso según los roles y permisos definidos en la red. Esta integración permite una evaluación completa del tráfico, la seguridad y la interoperabilidad entre las sedes, reforzando las competencias técnicas en administración de redes modernas y seguras.

1.1 OBJETIVO

Diseñar, implementar y analizar una topología de red multi-sede basada en direccionamiento IPv6 y segmentación por VLANs, utilizando protocolos de ruteo dinámico y mecanismos de seguridad perimetral, con el fin de simular el funcionamiento de una infraestructura corporativa real que garantice conectividad eficiente, administración centralizada y control seguro del acceso a los recursos internos.

1.2 ALCANCE

El presente proyecto abarca el diseño, configuración y análisis de una topología de red multi-sede simulada, basada en direccionamiento IPv6 y segmentación mediante VLANs, con el fin de reproducir el funcionamiento de una infraestructura empresarial real. Las actividades desarrolladas incluyen la implementación de enrutamiento dinámico OSPFv3 entre las sedes, el despliegue de un firewall pfSense para el control de acceso y seguridad perimetral, y la instalación de un servidor interno destinado a proporcionar servicios locales a los usuarios autorizados.

El proyecto contempla además la verificación de conectividad, la aplicación de políticas de seguridad y la validación de la interoperabilidad entre los componentes de la red. No se considera dentro del alcance la integración con servicios de nube, balanceo de carga avanzado, monitoreo automatizado, ni configuración de alta disponibilidad; sin embargo, la infraestructura queda preparada para permitir futuras ampliaciones. Este alcance permite evaluar el comportamiento operativo de una red empresarial moderna, fortaleciendo la comprensión de sus procesos de administración y seguridad.

2. DESCRIPCIÓN DE LA RED

La red diseñada corresponde a una infraestructura multi-sede basada en direcciones IPv6, donde se estableció un esquema de comunicación completo entre diferentes ciudades (BOGOTÁ, BARRANQUILLA, CALI y MEDELLIN), asegurando conectividad extremo a extremo y acceso controlado a servicios internos.

Se emplearon routers interconectados mediante enlaces punto a punto utilizando direcciones IPv6 global unicast del bloque 2001:db8:acad::/48. Para permitir la comunicación dinámica entre las sedes y garantizar convergencia automática ante cambios topológicos, se configuró el protocolo de enrutamiento OSPFv3, encargado de distribuir las rutas IPv6 en toda la red troncal.

En la sede de BARRANQUILLA, CALI y MEDELLIN, se implementó un firewall pfSense, el cual cumple varias funciones:

Servidor DHCPv6, RA, DNS, filtración de tráfico y VLANs, para la asignación automática de direcciones IPv6 y parámetros de red a los equipos finales como máquinas virtuales Linux Mint.

Gateway de salida hacia router de sede y posteriores comunicaciones con el exterior.

Dentro de la LAN de cada sede se diseñó una segmentación mediante VLANs, con el objetivo de separar usuarios y servicios según su rol. Cada VLAN cuenta con su propio prefijo IPv6 /64, garantizando compatibilidad con autoconfiguración DHCPv6. Adicionalmente, se implementaron reglas de firewall por VLAN en pfSense para restringir o permitir el tráfico entre segmentos o acceso a servidor principal HTTP, aumentando la seguridad interna y evitando accesos no autorizados hacia el servidor web.

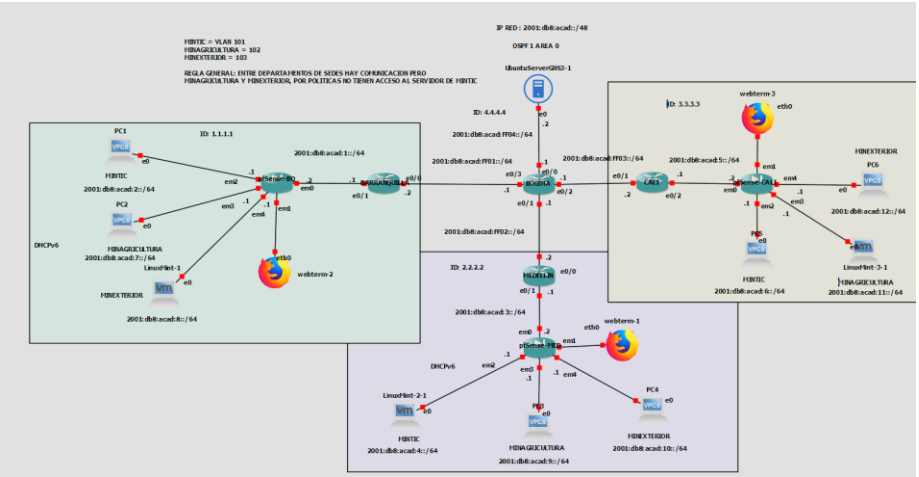
Finalmente, se habilitó un servidor DNS dentro de la misma sede y servidor local HTTP en BOGOTA, accesible únicamente desde las VLANs autorizadas y desde las sedes remotas por medio de OSPFv3. Esta estructura permite una red organizada, escalable, segura y totalmente basada en tecnologías modernas IPv6.

3. CONFIGURACIÓN DE LA RED

3.1 TOPOLOGIA Y PLANO LOGICO

La topología utilizada en este proyecto es una malla parcial jerárquica combinada con estrella extendida. A nivel de backbone, los routers están interconectados con enlaces punto a punto desde un nodo central (BOGOTA), lo que permite una comunicación eficiente entre sedes simuladas y facilita el enrutamiento jerárquico. Esta estructura imita una red WAN simplificada y organizada. A nivel local, cada router está conectado a un switch que distribuye la red a los dispositivos finales en una topología de estrella, segmentada por VLANs. Esta combinación fue elegida por su escalabilidad, facilidad de administración, control del tráfico y adecuación al escenario bancario propuesto en el proyecto.

3.1.1 IMAGEN 1 TOPOLOGIA



3.2 SEGMENTACION DE RED

A continuación, se presenta la segmentación de la red en los enlaces punto a punto entre routers y así mismo como trabaja la conexión del router central al servidor DHCP en Ubuntu:

ENLACE WAN	SUCURSAL (ROUTER)	INTERFAZ	DIRECCION IP	ID OSPF
BOGOTA - BARRANQUILLA	BOGOTA	FastEthernet0/3	2001:db8:acad:FF01::1/64	4.4.4.4
	BARRANQUILLA	FastEthernet0/0	2001:db8:acad:FF01::2/64	1.1.1.1
BOGOTA - MEDELLIN	BOGOTA	FastEthernet0/1	2001:db8:acad:FF02::1/64	4.4.4.4
	MEDELLIN	FastEthernet0/0	2001:db8:acad:FF02::2/64	2.2.2.2
BOGOTA - CALI	BOGOTA	FastEthernet0/2	2001:db8:acad:FF03::1/64	4.4.4.4
	CALI	FastEthernet0/1	2001:db8:acad:FF03::2/64	3.3.3.3
BOGOTA - HTTP	BOGOTA	FastEthernet0/0	2001:db8:acad:FF04::1/64	4.4.4.4
	HTTP	Ethernet0	2001:db8:acad:FF04::2/64	4.4.4.4

Una vez comprendida la forma en que se interconectan los routers a través de enlaces WAN, se procede a analizar la distribución de VLANs mediante el uso de un firewall simulado de código abierto como pfSense. Para ello, usamos una imagen nativa de los servidores de GNS3 y de una imagen ISO que permite su fácil instalación y configuración. Este firewall actúa como identificador lógico del tráfico, lo que permite que analizar, filtrar, aceptar, denegar tráfico proveniente de sus interfaces ethernet (LAN) y que así mismo funciona para el enrutamiento hacia su vecino más cercano el router que permite el enrutamiento hacia las demás redes.

Para esto es necesario la creación de VLANS que nos faciliten la creación de un firewall que logre identificar y filtrara correctamente el tráfico, tomando decisiones asociadas con las políticas de la sede.

A continuación, se presenta la creación de las VLANS, segmentación LAN y asignación de DHCPv6:

VLAN	MINISTERIO	INTERFAZ PFSENSE	SUCURSAL	RANGO DHCPv6
101	MINTIC	Ethernet2	BARRANQUILLA	2001:db8:acad:2::10/64 - 2001:db8:acad:2::20/64
			MEDELLIN	2001:db8:acad:4::10/64 - 2001:db8:acad:4::20/64
			CALI	2001:db8:acad:6::10/64 - 2001:db8:acad:6::20/64
102	MINAGRICULTURA	Ethernet3	BARRANQUILLA	2001:db8:acad:7::10/64 - 2001:db8:acad:7::20/64
			MEDELLIN	2001:db8:acad:9::10/64 - 2001:db8:acad:9::20/64
			CALI	2001:db8:acad:11::10/64 - 2001:db8:acad:11::20/64
103	MINEXTERIOR	Ethernet4	BARRANQUILLA	2001:db8:acad:8::10/64 - 2001:db8:acad:8::20/64
			MEDELLIN	2001:db8:acad:10::10/64 - 2001:db8:acad:10::20/64
			CALI	2001:db8:acad:12::10/64 - 2001:db8:acad:12::20/64

4. PROCEDIMIENTO DE CONFIGURACIÓN DE ENRUTAMIENTO

Se describe la configuración aplicada en los equipos de red (routers) para la correcta comunicación inter-sede, usando el protocolo de enrutamiento OSPFv3, además se adjuntan los comandos usan con su pertinente explicación.

4.1 CONFIGURACIÓN DE INTERFACES

Para permitir la comunicación entre los diferentes router punto a punto y comunicaciones router-pfSense usaremos los siguientes comandos:

4.1.1 TABLA DE COMANDOS ROUTERS

Configuración de todos los routers	Explicación
BARRANQUILLA ////////////////////// ROUTER ////////////////////// conf t ipv6 router ospf 1 router-id 1.1.1.1 redistribute static exit conf t ipv6 unicast-routing interface e0/1 description Conexion a pfSense-BQ ipv6 address 2001:db8:acad:1::1/64 ipv6 ospf 1 area 0 no shutdown exi conf t interface e0/0 description Conexion a BOGOTA ipv6 address 2001:db8:acad:FF01::2/64 ipv6 ospf 1 area 0 no shutdown end wr show ipv6 interface brief show ipv6 route ipv6 route 2001:db8:acad:2::/64 2001:db8:acad:1::2	Configuración de interfaces con su respectiva asignación de ID router, área, proceso ospf, IPv6 adresses y una breve descripción de la función de cada interfaz. Por otro lado, se usa enrutamiento estático para comunicación entre routers y pfSense quien será gestor de las redes LAN de cada sede.

ipv6 route 2001:db8:acad:7::/64 2001:db8:acad:1::2

ipv6 route 2001:db8:acad:8::/64 2001:db8:acad:1::2

MEDELLIN

////////////////////// ROUTER
//////////////////////

conf t

ipv6 router ospf 1

router-id 2.2.2.2

redistribute static

exit

conf t

ipv6 unicast-routing

interface e0/1

description Conexion a pfSense-MED

ipv6 address 2001:db8:acad:3::1/64

ipv6 ospf 1 area 0

no shutdown

exi

conf t

interface e0/0

description Conexion a BOGOTA

ipv6 address 2001:db8:acad:FF02::2/64

ipv6 ospf 1 area 0

no shutdown

end

wr

ipv6 route 2001:db8:acad:4::/64 2001:db8:acad:3::2

ipv6 route 2001:db8:acad:9::/64 2001:db8:acad:3::2

ipv6 route 2001:db8:acad:10::/64 2001:db8:acad:3::2

CALI

////////////////////// ROUTER
//////////////////////

conf t

ipv6 router ospf 1

router-id 3.3.3.3

redistribute static

exit

conf t

ipv6 unicast-routing

interface e0/2

description Conexion a pfSense-CALI

ipv6 address 2001:db8:acad:5::1/64

ipv6 ospf 1 area 0

no shutdown

exi

conf t

interface e0/1

description Conexion a BOGOTA

ipv6 address 2001:db8:acad:FF03::2/64

ipv6 ospf 1 area 0

no shutdown

end

wr

ipv6 route 2001:db8:acad:6::/64 2001:db8:acad:5::2

ipv6 route 2001:db8:acad:11::/64 2001:db8:acad:5::2

ipv6 route 2001:db8:acad:12::/64 2001:db8:acad:5::2

BOGOTA

////////////////////// ROUTER
//////////////////////

conf t

ipv6 unicast-routing

ipv6 router ospf 1

router-id 4.4.4.4

redistribute static

exit

conf t

interface e0/3

description Conexion a BARRANQUILLA

ipv6 address 2001:db8:acad:FF01::1/64

ipv6 ospf 1 area 0

no shutdown interface e0/1 description Conexion a MEDELLIN ipv6 address 2001:db8:acad:FF02::1/64 ipv6 ospf 1 area 0 no shutdown interface e0/2 description Conexion a CALI ipv6 address 2001:db8:acad:FF03::1/64 ipv6 ospf 1 area 0 no shutdown conf t interface e0/0 description CONEXION A HTTP ipv6 address 2001:db8:acad:FF04::1/64 ipv6 ospf 1 area 0	

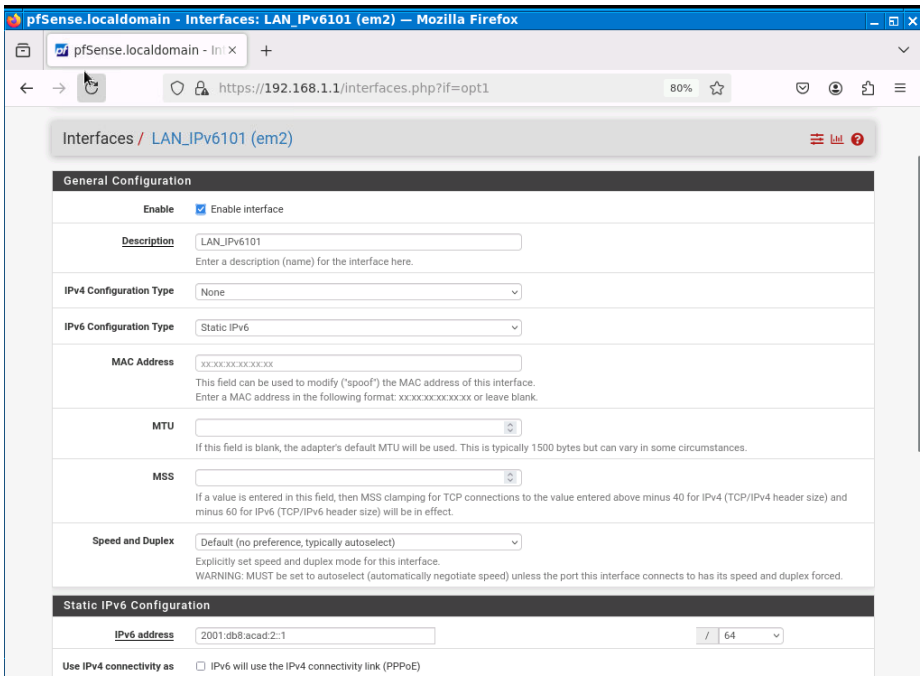
4.1.3 TABLA DE COMANDOS SERVIDOR HTTP

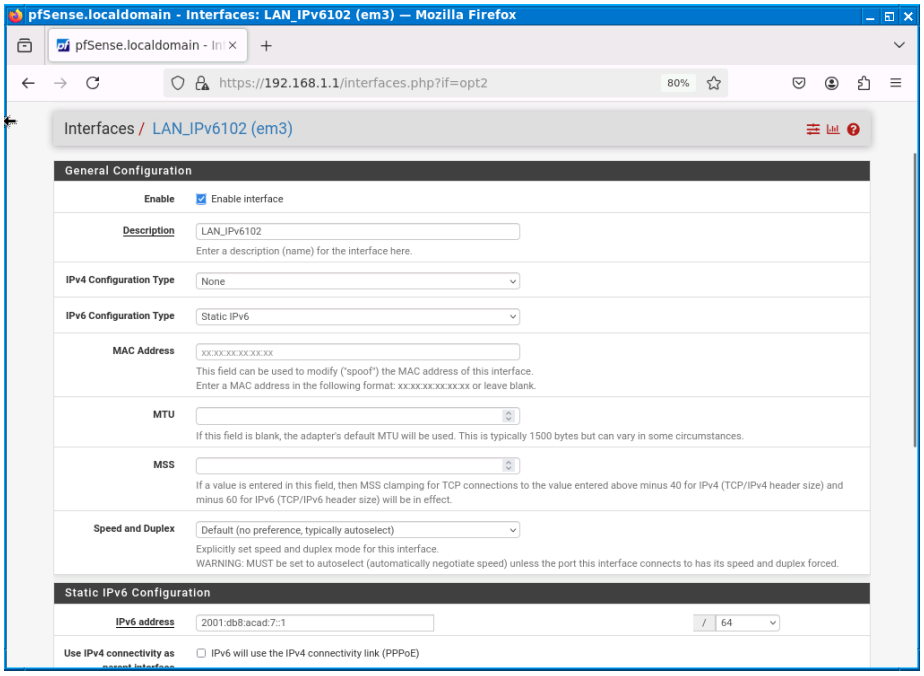
sudo apt update sudo apt install nginx -y sudo systemctl enable nginx sudo systemctl start nginx sudo systemctl status nginx sudo nano /etc/netplan/00-installer-config.yaml network: version: 2 renderer: networkd ethernets: ens33: dhcp4: true dhcp6: no addresses: - 2001:db8:acad:FF04::2/64 gateway6: 2001:db8:acad:FF04::1	1. Se obtiene y actualiza los paquetes de drives/ configuraciones más recientes para la versión. (tener presente hacer esto antes de colocar la VM en GNS3) 2. Se instala la dependencia nginx el cual nos ayuda como motor de servidor http. Se habilita y se verifica que quede en estado running. 3. Se configura una ip estática en la interfaz de red correcta, dentro del segmento asignado para BOGOTA con esa conexión y se apunta hacia el Gateway de la interfaz. 4. Se aplican los cambios de la configuración de la tarjeta de red. 5. Se valida que la salida de este servicio sea por el puerto 80 TCP para HTTP. 6. Se valida que la ejecución de la página sea dentro de un HTML posteriormente configurado. 7. Se establece / permite la recepción y envió de información a través del

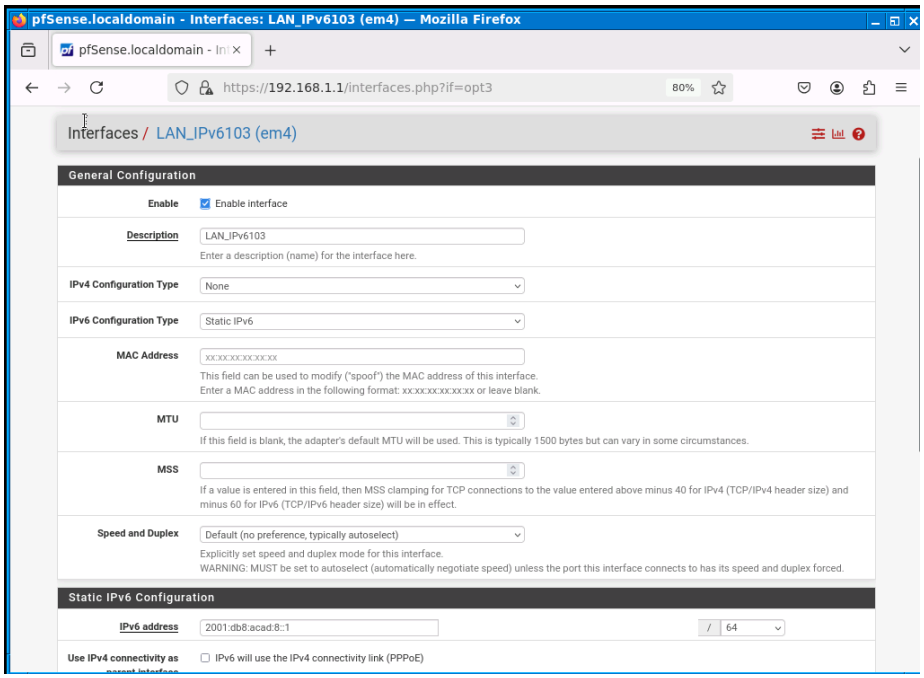
sudo netplan apply
 	
sudo nano /etc/nginx/sites-available/default
 	
server {
listen 80 default_server;
listen [::]:80 default_server;
 	
root /var/www/html;
index index.html index.htm;
 	
server_name _;
 	
location / {
try_files $uri $uri/ =404;
}
}
 	
sudo nginx -t
sudo systemctl restart nginx
 	
sudo ufw allow 80/tcp
sudo ufw allow from any to any proto tcp port 80
sudo ufw enable
sudo ufw status
	puerto 80 TCP sin que el firewall por default lo bloquee.
	8. Se reinicia el servicio nginx para que tome los cambios aplicados.

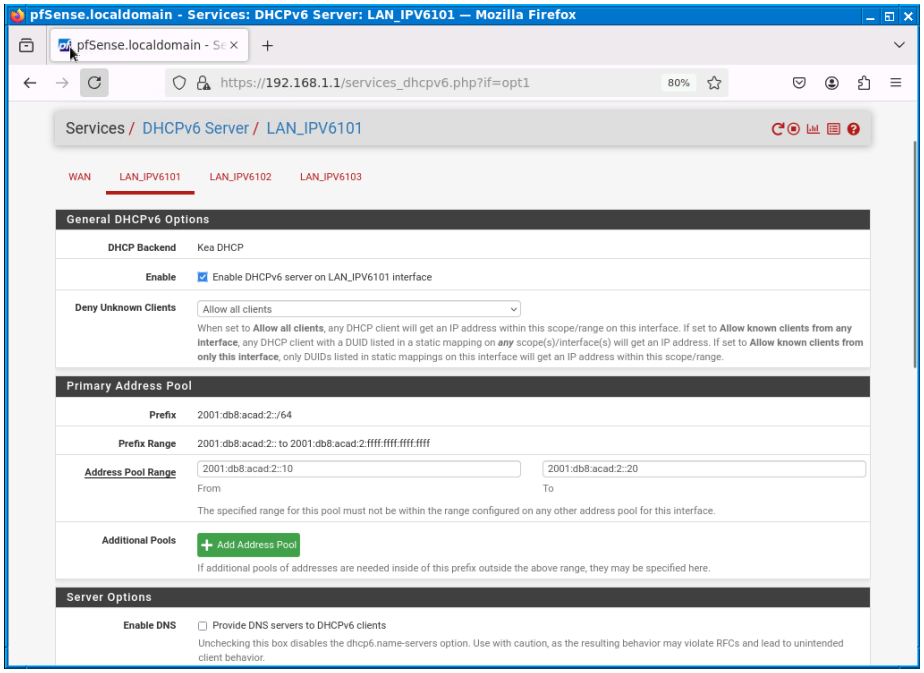
4.1.4 CONFIGURACIÓN PFSENSE (DNS, DHCPV6, FIREWALL)

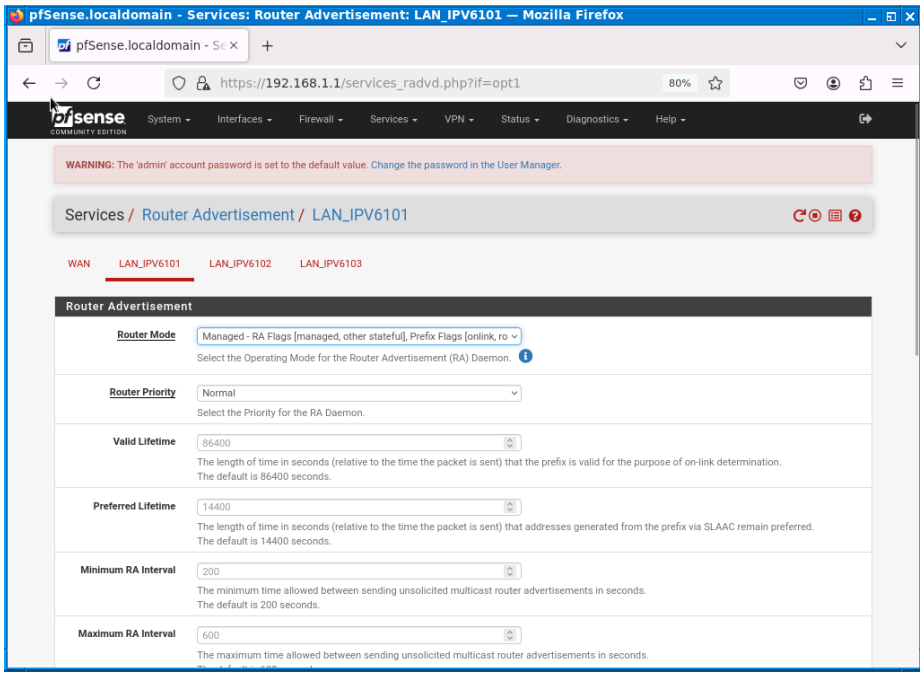
1. **DHCPv6:**
   Cada VLAN (101, 102, 103) representa un segmento lógico distinto (MINTIC, MINAGRICULTURA, MINEXTERIOR), aislando el tráfico dentro de cada grupo, así como su asignación.


pfSense.localdomain - Interfaces: LAN_IPv6101 (em2) — Mozilla Firefox
pfSense.localdomain - In
https://192.168.1.1/interfaces.php?if=opt1
80%
Interfaces / LAN_IPv6101 (em2)
General Configuration
Enable
Enable interface
Description
LAN_IPv6101
Enter a description (name) for the interface here.
IPv4 Configuration Type
None
IPv6 Configuration Type
Static IPv6
MAC Address
xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv6 Configuration
IPv6 address
2001:db8:acad:2::1
/ 64
Use IPv4 connectivity as
IPv6 will use the IPv4 connectivity link (PPPoE)


pfSense.localdomain - Interfaces: LAN_IPv6102 (em3) — Mozilla Firefox
pfSense.localdomain - In
https://192.168.1.1/interfaces.php?if=opt2
80%
Interfaces / LAN_IPv6102 (em3)
General Configuration
Enable
Enable interface
Description
LAN_IPv6102
Enter a description (name) for the interface here.
IPv4 Configuration Type
None
IPv6 Configuration Type
Static IPv6
MAC Address
xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv6 Configuration
IPv6 address
2001:db8:acad:7::1
/ 64
Use IPv4 connectivity as
IPv6 will use the IPv4 connectivity link (PPPoE)

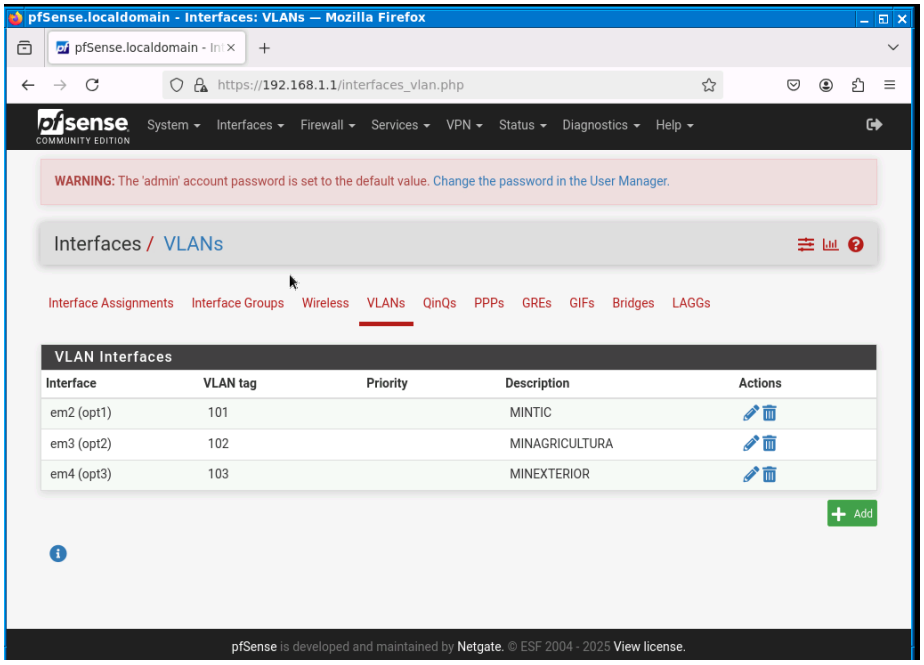

pfSense.localdomain - Interfaces: LAN_IPv6103 (em4) — Mozilla Firefox
pfSense.localdomain - Int
https://192.168.1.1/interfaces.php?if=opt3
80%
Interfaces / LAN_IPv6103 (em4)
General Configuration
Enable
Enable interface
Description
LAN_IPv6103
Enter a description (name) for the interface here.
IPv4 Configuration Type
None
IPv6 Configuration Type
Static IPv6
MAC Address
xx:xx:xx:xx:xx:xx
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS
If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex
Default (no preference, typically autoselect)
Explicitly set speed and duplex mode for this interface.
WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.
Static IPv6 Configuration
IPv6 address
2001:db8:acad:8::1
/ 64
Use IPv4 connectivity as
IPv6 will use the IPv4 connectivity link (PPPoE)


pfSense.localdomain - Services: DHCPv6 Server: LAN_IPV6101 — Mozilla Firefox
pfSense.localdomain - Se
https://192.168.1.1/services_dhcpv6.php?if=opt1
80%
Services / DHCPv6 Server / LAN_IPV6101
WAN
LAN_IPV6101
LAN_IPV6102
LAN_IPV6103
General DHCPv6 Options
DHCP Backend
Kea DHCP
Enable
Enable DHCPv6 server on LAN_IPV6101 interface
Deny Unknown Clients
Allow all clients
When set to Allow all clients, any DHCP client will get an IP address within this scope/range on this interface. If set to Allow known clients from any interface, any DHCP client with a DUID listed in a static mapping on any scope(s)/interface(s) will get an IP address. If set to Allow known clients from only this interface, only DUIDs listed in static mappings on this interface will get an IP address within this scope/range.
Primary Address Pool
Prefix
2001:db8:acad:2::/64
Prefix Range
2001:db8:acad:2:: to 2001:db8:acad:2:ffff:ffff:ffff:ffff
Address Pool Range
2001:db8:acad:2::10
From
2001:db8:acad:2::20
To
The specified range for this pool must not be within the range configured on any other address pool for this interface.
Additional Pools
Add Address Pool
If additional pools of addresses are needed inside of this prefix outside the above range, they may be specified here.
Server Options
Enable DNS
Provide DNS servers to DHCPv6 clients
Unchecking this box disables the dhcp6.name-servers option. Use with caution, as the resulting behavior may violate RFCs and lead to unintended client behavior.



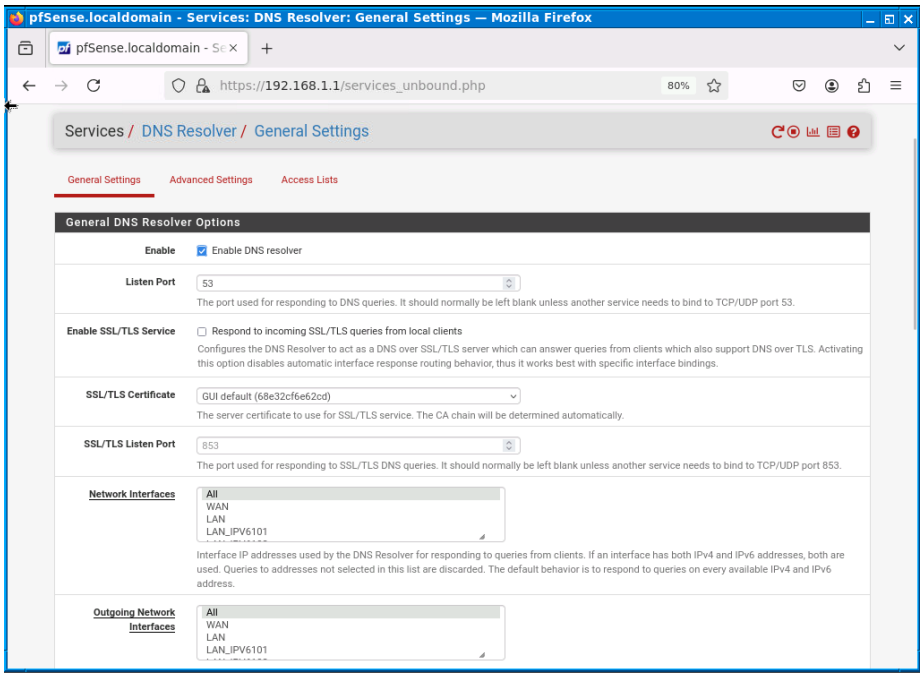
2. **VLANs:**

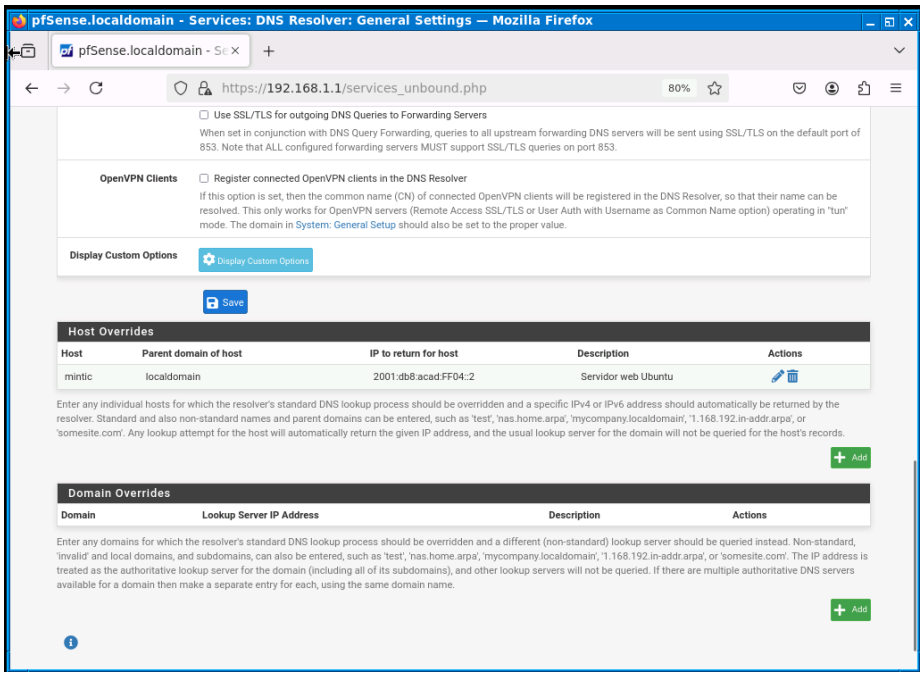
Asignación de VLANs a puertos de acceso de cada ministerio:



3. **DNS:**

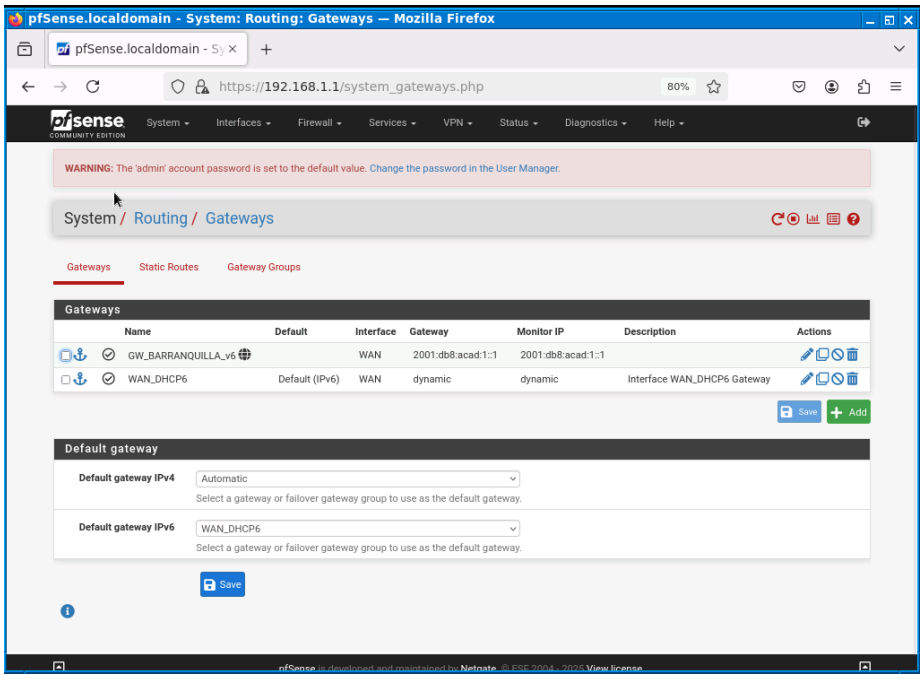
Servicio que permite la resolución de dominio del servidor principal HTTP con dominio mintic.localdomain (2001:db8:acad:FF04::2)

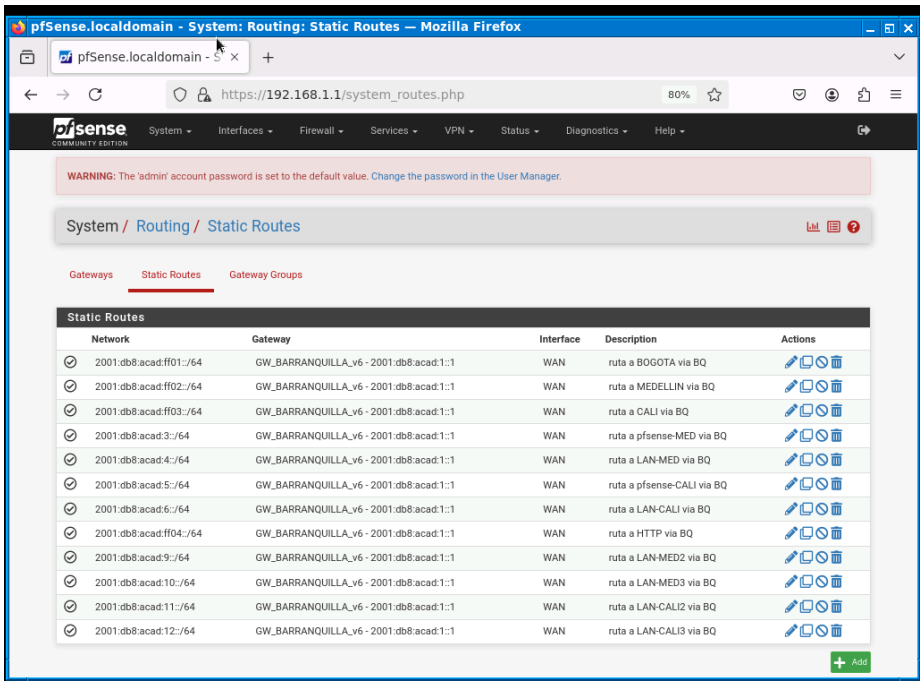




4. **Enrutamiento entre VLANs:**

Enrutamiento estático al gateway de router de sede para que permita la comunicación en una extranet.





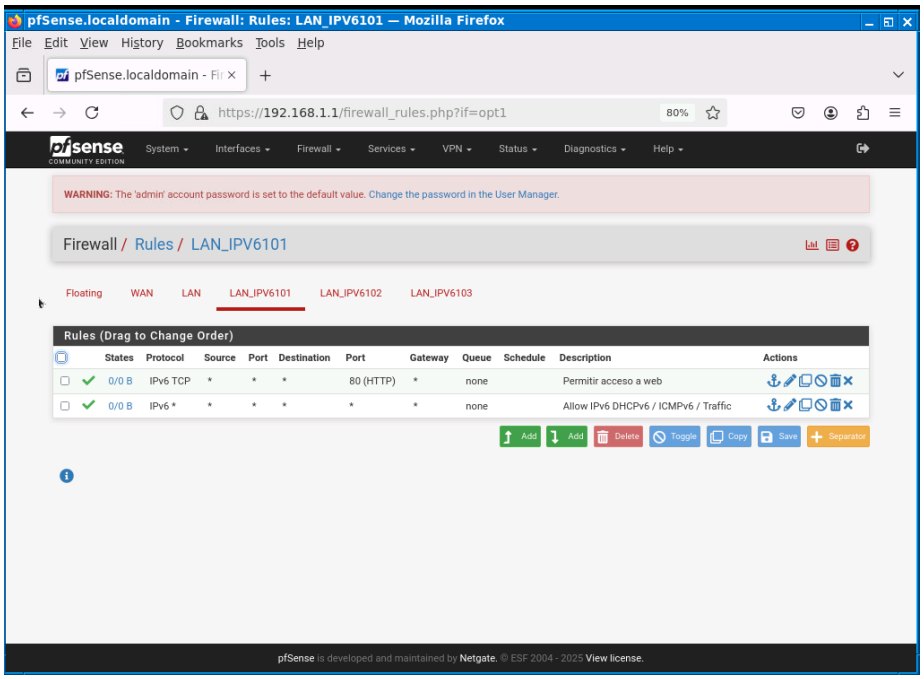
5. **Firewall:**

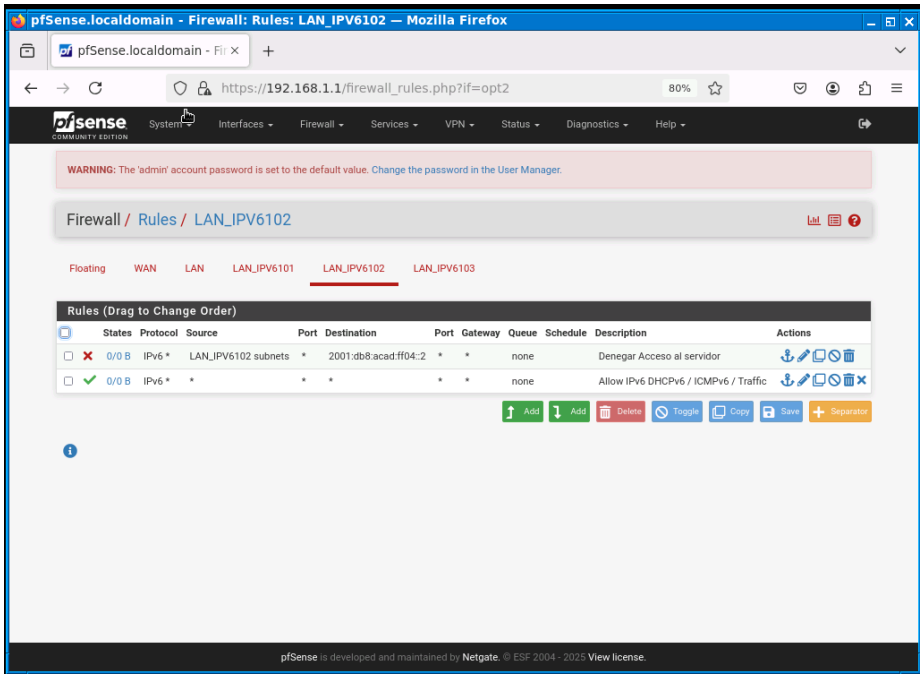
Asignación de políticas de comunicación y acceso de la siguiente forma:

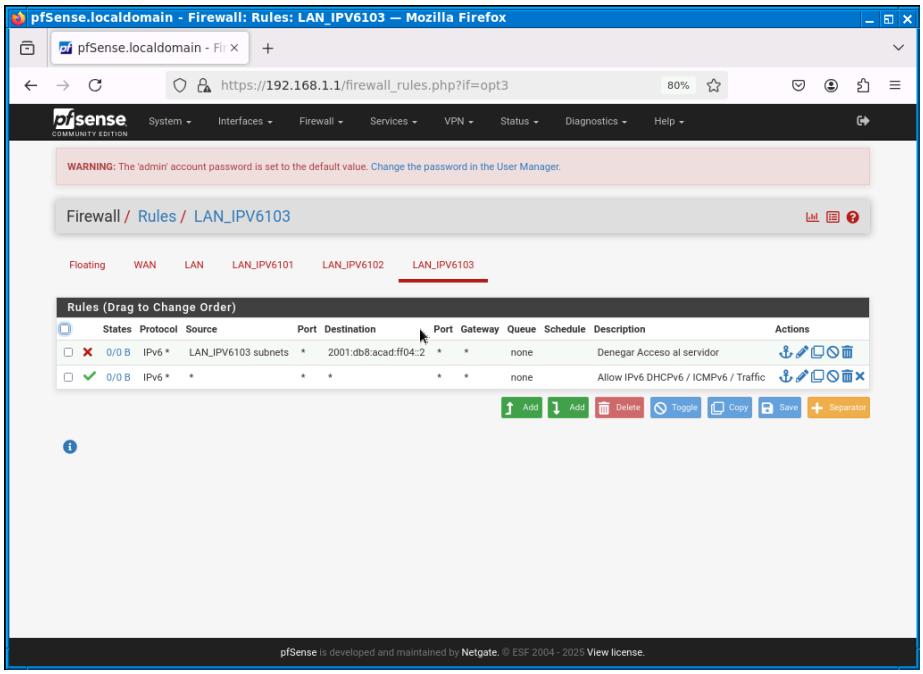
VLAN 101 (MINTIC) puede acceder al servidor y cualquier otra red.

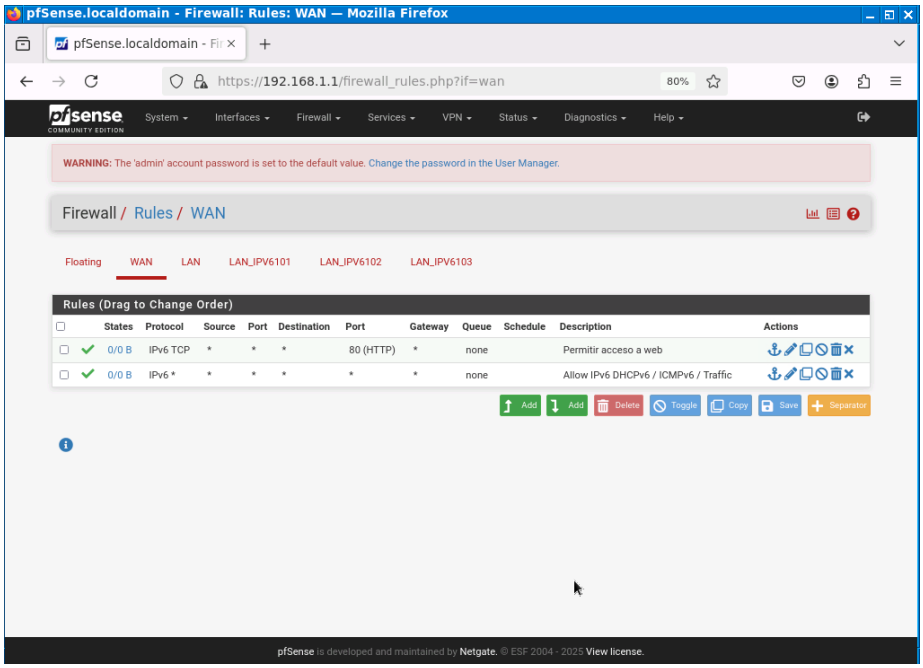
VLAN 102 (MINAGRICULTURA) no puede acceder al servidor, pero si comunicarse con las demás redes

VLAN 103 (MINEXTERIOR) no puede acceder al servidor, pero si comunicarse con las demás redes


pfSense.localdomain - Firewall: Rules: LAN_IPV6101 — Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://192.168.1.1/firewall_rules.php?if=opt1
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / LAN_IPV6101
Floating WAN LAN LAN_IPV6101 LAN_IPV6102 LAN_IPV6103
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
0/0 B IPv6 TCP * * * 80 (HTTP) * none Permitir acceso a web
0/0 B IPv6 * * * * * * none Allow IPv6 DHCPv6 / ICMPv6 / Traffic
Add Add Delete Toggle Copy Save Separator
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.


pfSense.localdomain - Firewall: Rules: LAN_IPV6102 — Mozilla Firefox
https://192.168.1.1/firewall_rules.php?if=opt2
System Interfaces Firewall Services VPN Status Diagnostics Help
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.
Firewall / Rules / LAN_IPV6102
Floating WAN LAN LAN_IPV6101 LAN_IPV6102 LAN_IPV6103
Rules (Drag to Change Order)
States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions
0/0 B IPv6 * LAN_IPV6102 subnets * 2001:db8:acad:ff04::2 * * none Denegar Acceso al servidor
0/0 B IPv6 * * * * * * none Allow IPv6 DHCPv6 / ICMPv6 / Traffic
Add Add Delete Toggle Copy Save Separator
pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 View license.





5. EVIDENCIAS DE PRUEBAS Y OPERATIVIDAD

PRUEBAS DE CONECTIVIDAD (PING):

Se ejecutaron comandos `ping` y `traza` desde varias estaciones hacia otras estaciones y servidor, verificando la conectividad entre VLANs y confirmando el correcto enrutamiento de la red. Prueba de comunicación entre VLAN permitidas por el FIREWALL, Asignacion del Servidor DHCP en las distintas

redes, Funcionamiento de las Maquinas virtuales de las diferentes VLANS y Validacion de acceso a servidor HTTP.

Pings y trazas desde el punto más lejano de cada VLAN asegurando el correcto funcionamiento de la red:

ROUTER BOGOTA (CORE)

ENRUTAMIENTO DINAMICO OSPFv3:

```
BOGOTA#show ipv6 interface brief
Ethernet0/0            [up/up]
    FE80::A8BB:CCFF:FE00:200
    2001:DB8:ACAD:FF04::1
Ethernet0/1            [up/up]
    FE80::A8BB:CCFF:FE00:210
    2001:DB8:ACAD:FF02::1
Ethernet0/2            [up/up]
    FE80::A8BB:CCFF:FE00:220
    2001:DB8:ACAD:FF03::1
Ethernet0/3            [up/up]
    FE80::A8BB:CCFF:FE00:230
    2001:DB8:ACAD:FF01::1
```

```
BOGOTA#show ipv6 route
IPv6 Routing Table - default - 21 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       H - NHRP, I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       IS - ISIS summary, D - EIGRP, EX - EIGRP external, NM - NEMO
       ND - ND Default, NDp - ND Prefix, DCE - Destination, NDr - Redirect
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2, la - LISP alt
       lr - LISP site-registrations, ld - LISP dyn-eid, a - Application
O   2001:DB8:ACAD:1::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:400, Ethernet0/3
OE2 2001:DB8:ACAD:2::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:400, Ethernet0/3
O   2001:DB8:ACAD:3::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:300, Ethernet0/1
OE2 2001:DB8:ACAD:4::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:300, Ethernet0/1
O   2001:DB8:ACAD:5::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:110, Ethernet0/2
OE2 2001:DB8:ACAD:6::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:110, Ethernet0/2
OE2 2001:DB8:ACAD:7::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:400, Ethernet0/3
OE2 2001:DB8:ACAD:8::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:400, Ethernet0/3
OE2 2001:DB8:ACAD:9::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:300, Ethernet0/1
OE2 2001:DB8:ACAD:10::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:300, Ethernet0/1
OE2 2001:DB8:ACAD:11::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:110, Ethernet0/2
OE2 2001:DB8:ACAD:12::/64 [110/20]
     via FE80::A8BB:CCFF:FE00:110, Ethernet0/2
C   2001:DB8:ACAD:FF01::/64 [0/0]
     via Ethernet0/3, directly connected
L   2001:DB8:ACAD:FF01::1/128 [0/0]
     via Ethernet0/3, receive
C   2001:DB8:ACAD:FF02::/64 [0/0]
     via Ethernet0/1, directly connected
L   2001:DB8:ACAD:FF02::1/128 [0/0]
     via Ethernet0/1, receive
C   2001:DB8:ACAD:FF03::/64 [0/0]
     via Ethernet0/2, directly connected
L   2001:DB8:ACAD:FF03::1/128 [0/0]
     via Ethernet0/2, receive
C   2001:DB8:ACAD:FF04::/64 [0/0]
     via Ethernet0/0, directly connected
L   2001:DB8:ACAD:FF04::1/128 [0/0]
     via Ethernet0/0, receive
L   FF00::/8 [0/0]
     via Null0, receive
BOGOTA#
```

```
BOGOTA#show ospfv3 database

          OSPFv3 1 address-family ipv6 (router-id 4.4.4.4)

               Router Link States (Area 0)

ADV Router       Age         Seq#        Fragment ID  Link count  Bits
 1.1.1.1         17          0x80000003  0            1           E
 2.2.2.2         1948        0x80000002  0            1           E
 3.3.3.3         1948        0x80000002  0            1           E
 4.4.4.4         1947        0x80000002  0            3           None

               Net Link States (Area 0)

ADV Router       Age         Seq#        Link ID     Rtr count
 4.4.4.4         1947        0x80000001  4           2
 4.4.4.4         1947        0x80000001  5           2
 4.4.4.4         1947        0x80000001  6           2

               Link (Type-8) Link States (Area 0)

ADV Router       Age         Seq#        Link ID     Interface
 1.1.1.1         17          0x80000003  3           Et0/3
 4.4.4.4         1982        0x80000002  6           Et0/3
 3.3.3.3         1983        0x80000002  4           Et0/2
 4.4.4.4         1982        0x80000002  5           Et0/2
 2.2.2.2         1983        0x80000002  3           Et0/1
 4.4.4.4         1982        0x80000002  4           Et0/1
 4.4.4.4         1982        0x80000002  3           Et0/0

               Intra Area Prefix Link States (Area 0)

ADV Router       Age         Seq#        Link ID     Ref-lstype  Ref-LSID
 1.1.1.1         17          0x80000003  0           0x2001      0
 2.2.2.2         1948        0x80000002  0           0x2001      0
 3.3.3.3         1948        0x80000002  0           0x2001      0
 4.4.4.4         1947        0x80000002  0           0x2001      0
 4.4.4.4         1947        0x80000001  4096        0x2002      4
 4.4.4.4         1947        0x80000001  5120        0x2002      5
 4.4.4.4         1947        0x80000001  6144        0x2002      6

               Type-5 AS External Link States

ADV Router       Age         Seq#        Prefix
 1.1.1.1         17          0x80000002  2001:DB8:ACAD:8::/64
 1.1.1.1         17          0x80000002  2001:DB8:ACAD:7::/64
 1.1.1.1         17          0x80000002  2001:DB8:ACAD:2::/64
 2.2.2.2         1988        0x80000001  2001:DB8:ACAD:10::/64
 2.2.2.2         1988        0x80000001  2001:DB8:ACAD:9::/64
 2.2.2.2         1988        0x80000001  2001:DB8:ACAD:4::/64
 3.3.3.3         1988        0x80000001  2001:DB8:ACAD:12::/64
 3.3.3.3         1988        0x80000001  2001:DB8:ACAD:11::/64
 3.3.3.3         1988        0x80000001  2001:DB8:ACAD:6::/64
BOGOTA#
```

PRUEBAS PING:

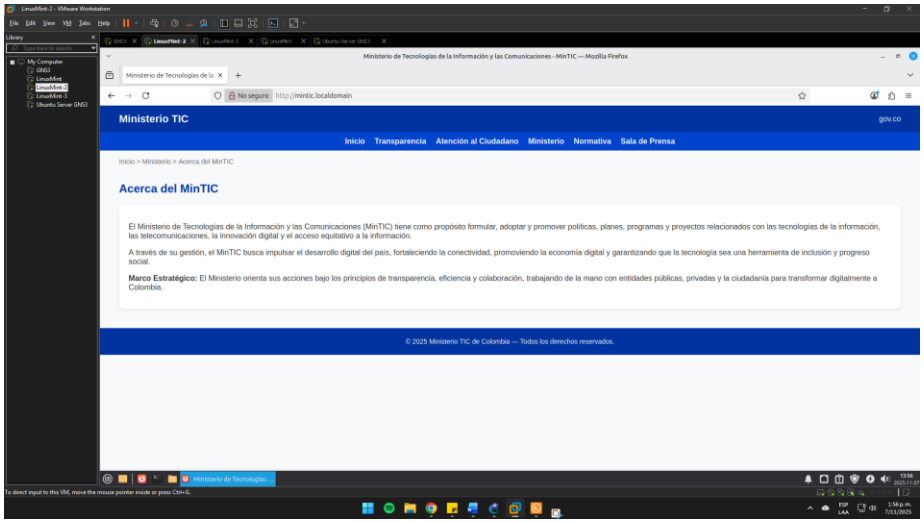
ENTRE SEDES

```
BOGOTA#ping 2001:db8:acad:FF01::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:FF01::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/20 ms
BOGOTA#ping 2001:db8:acad:FF02::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:FF02::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/17 ms
BOGOTA#ping 2001:db8:acad:FF03::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:FF03::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/4/18 ms
BOGOTA#ping 2001:db8:acad:FF04::2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2001:DB8:ACAD:FF04::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/8 ms
BOGOTA#
```

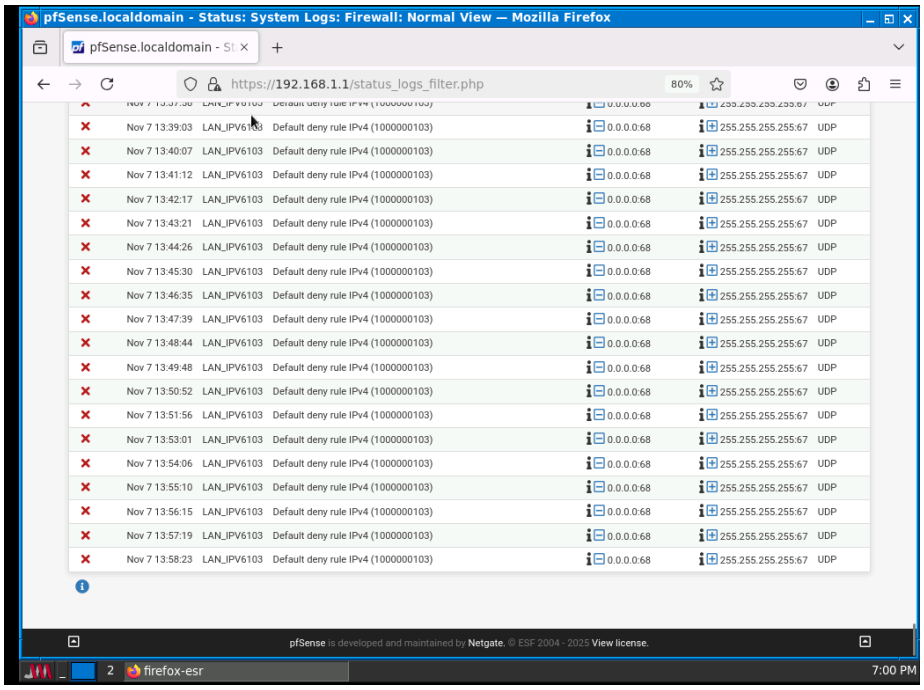
CLIENTES FINALES:

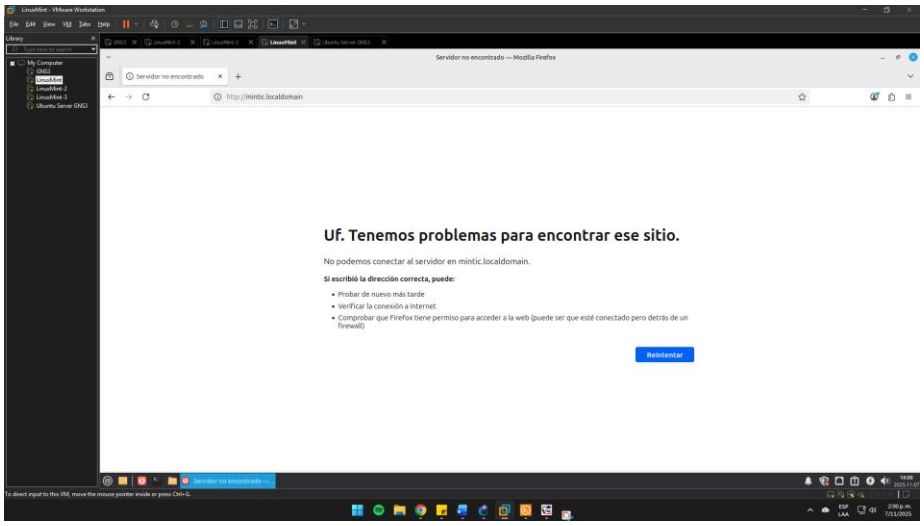
CLIENTES FINALES A SERVIDOR HTTP (mintic.localdomain)

VLAN 101 (SEDE MEDELLIN)

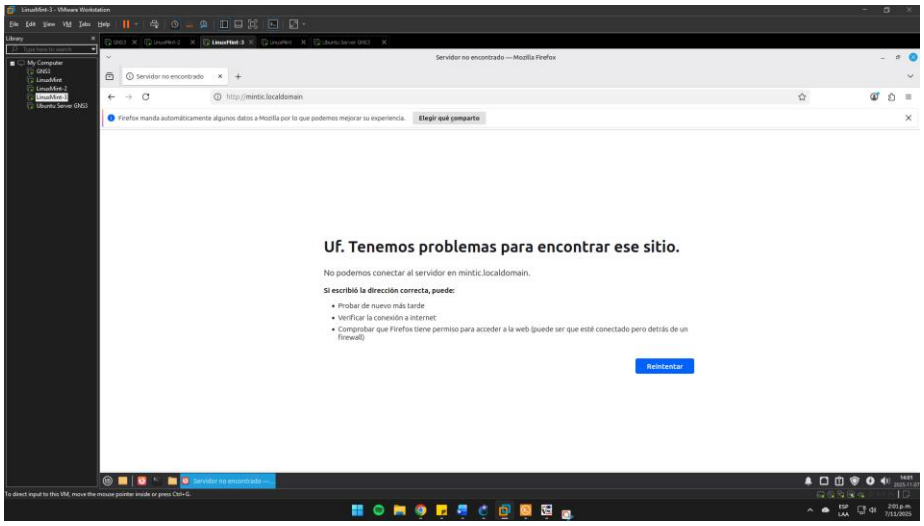


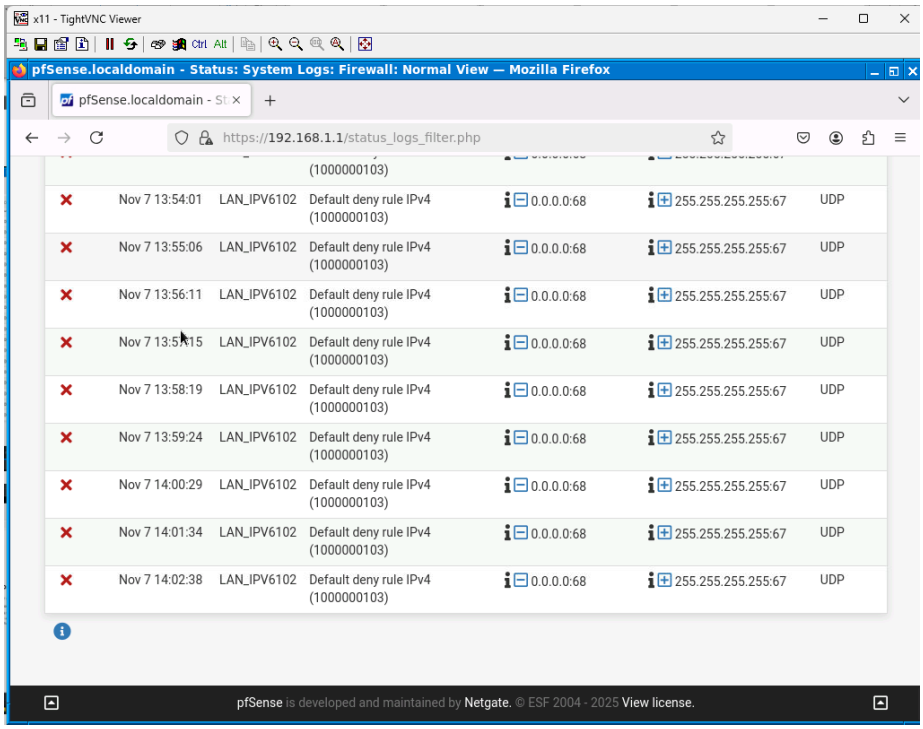
VLAN 103 (SEDE BARRANQUILLA)





VLAN 102 (SEDE CALI)





COMUNCACION INTERSEDE (CLIENTES FINALES)

```
fniel@PC1-Mint:~$ ping6 2001:db8:acad:11::10
PING 2001:db8:acad:11::10 (2001:db8:acad:11::10) 56 data bytes
64 bytes from 2001:db8:acad:11::10: icmp_seq=1 ttl=59 time=3.58 ms
64 bytes from 2001:db8:acad:11::10: icmp_seq=2 ttl=59 time=3.16 ms
64 bytes from 2001:db8:acad:11::10: icmp_seq=3 ttl=59 time=3.31 ms
64 bytes from 2001:db8:acad:11::10: icmp_seq=4 ttl=59 time=2.96 ms
^C
--- 2001:db8:acad:11::10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 2.964/3.253/3.579/0.225 ms
fniel@PC1-Mint:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:fc:b8:ce brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet6 2001:db8:acad:8::10/128 scope global dynamic noprefixroute
       valid_lft 6116sec preferred_lft 3416sec
    inet6 fe80::71fe:e1c4:e4ff:8f3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
fniel@PC1-Mint:~$
```

PRUEBAS DE SERVICIO HTTP:

```
fniel@mintic:~$ sudo systemctl status nginx
● nginx.service - A high performance web server and a reverse proxy server
     Loaded: loaded (/lib/systemd/system/nginx.service; enabled; vendor preset: enabled)
     Active: active (running) since Fri 2025-11-07 18:14:32 UTC; 52min ago
       Docs: man:nginx(8)
    Process: 1035 ExecStartPre=/usr/sbin/nginx -t -q -g daemon on; master_process on; (code=exited,
    Process: 1116 ExecStart=/usr/sbin/nginx -g daemon on; master_process on; (code=exited, status=0
   Main PID: 1128 (nginx)
      Tasks: 3 (limit: 4550)
     Memory: 9.1M
     CGroup: /system.slice/nginx.service
             ├─1128 nginx: master process /usr/sbin/nginx -g daemon on; master_process on;
             ├─1129 nginx: worker process
             └─1130 nginx: worker process

nov 07 18:14:31 mintic systemd[1]: Starting A high performance web server and a reverse proxy serve
nov 07 18:14:32 mintic systemd[1]: Started A high performance web server and a reverse proxy server.

fniel@mintic:~$ _
```

6. INFORME TÉCNICO DEL PROYECTO

6.1 JUSTIFICACION DEL DISEÑO LÓGICO Y FÍSICO

El diseño lógico y físico de la red se fundamenta en la necesidad de integrar múltiples sedes mediante una infraestructura escalable, organizada y segura, que permita la comunicación estable entre los distintos segmentos y servicios internos. A nivel lógico, la red se estructuró utilizando direccionamiento IPv6 global unicast, lo que facilita la expansión de subredes y asegura compatibilidad con tecnologías modernas. La elección del protocolo OSPFv3 se justifica por su capacidad para distribuir rutas dinámicamente, garantizar convergencia eficiente ante cambios en la topología y soportar nativamente IPv6, lo que resulta fundamental en entornos empresariales distribuidos.

La segmentación mediante VLANs se implementó para separar grupos de trabajo y servicios según criterios de función y seguridad. Esto no solo mejora la administración de la red, sino que también reduce el dominio de broadcast, optimizando el rendimiento. Para el control perimetral y la asignación interna de direcciones y servicios, se utilizó pfSense como firewall y servidor, debido a su flexibilidad, soporte para DHCPv6, DNS y filtrado de tráfico, permitiendo aplicar reglas y políticas diferenciales entre sedes y VLANs, garantizando que solo los usuarios autorizados accedan a los recursos internos.

Finalmente, la inclusión de un servidor web interno con acceso restringido fortalece la representación de un entorno corporativo real, donde la información crítica es protegida mediante políticas centralizadas de seguridad y control de acceso. En conjunto, el diseño adoptado equilibra escalabilidad, eficiencia, seguridad y coherencia con prácticas modernas de infraestructura de red empresarial.

6.2 CONCLUSIONES

A través de la implementación de esta topología multi-sede basada en direccionamiento IPv6 y segmentación por VLANs, se comprobó la viabilidad y eficiencia de una infraestructura de red corporativa moderna. Se logró establecer comunicación confiable entre sedes mediante OSPFv3, lo que permitió una convergencia automática y una distribución estructurada del enrutamiento.

El uso de pfSense como firewall perimetral demostró ser una solución efectiva para la administración del tráfico interno y la aplicación de políticas de seguridad diferenciadas por VLAN, permitiendo controlar el acceso a servicios críticos como el servidor web interno. Asimismo, la implementación del servidor HTTP reforzó la comprensión de los procesos de provisión de servicios locales, resolución DNS e interacción entre cliente–servidor en un entorno realista.

En general, el proyecto permitió integrar conceptos clave de redes como direccionamiento IPv6, enrutamiento dinámico, segmentación lógica, seguridad y servicios internos en una infraestructura funcional y coherente. Esto fortaleció las competencias técnicas necesarias para la administración y el diseño de redes avanzadas en entornos empresariales.

6.3 POSIBLES MEJORAS

1. Alta disponibilidad (HA): Implementar redundancia tanto en firewalls como en routers para asegurar continuidad del servicio ante fallas.

2. Balanceo de carga: Incluir mecanismos que distribuyan de manera inteligente el tráfico hacia servicios internos para mejorar el rendimiento.

3. Monitoreo y alertamiento: Integrar herramientas como Zabbix, Grafana o PRTG para la supervisión en tiempo real de los recursos y enlaces.

4. Políticas de seguridad más estrictas: Implementar inspección profunda de paquetes (DPI) y segmentación con Zero Trust para aumentar el nivel de protección.

5. Integración con servicios en a la nube: Migrar el servidor interno a una arquitectura hibrida controlada, lo que permitiría mayor escalabilidad y disponibilidad remota.

7. BIBLIOGRAFÍA

1.Agregar switch/router Cisco C3725 a proyecto GNS3 y configuración inicial» Proyecto A. (2022, May 8). *Proyecto A »*

2. Tutoriales nuevas tecnologías y código fuente. https://proyectoa.com/agregar-switch-router-cisco-c3725-a-proyecto-gns3-y-configuracion-inicial/

3. Charria. (2025, May 15). *UbuntuServer20_04: Servidor Web con Ubuntu Server 20.04 LTS*. https://github.com/Fniel88/UbuntuServer20_04.git

4. Marcelo. (2019, August 30). *Enrutamiento Intra VLAN (Entre Subredes de Distintas VLANs)*. CCNA Desde Cero. https://ccnadesdecero.com/curso/enrutamiento-intra-vlan/

5. Network Warriors. (2024a, August 12). *APRENDE a Instalar y Configurar Servidor DHCP Real (Ubuntu Server)*. YouTube. https://www.youtube.com/watch?v=4bBHymdw3fU

6. Network Warriors. (2024b, August 26). *GNS3: Conectar con REDES Remotas Servidor DHCP en Ubuntu server 22.04 - Red de Computadoras*. YouTube. https://www.youtube.com/watch?v=MUr9R0cHRK0