P7 - VPN

Luis Carlos Leaño Martin – 744732

Diego Gutiérrez Aldrete - 745359

ITESO, Universidad Jesuita de Guadalajara

Ruteo Avanzado

21/11/2024

Introduction

A VPN (Virtual Private Network) is a technology that allows creating a secure and encrypted connection between two or more devices through a public network like the internet. This enables users to remotely access resources of a private network securely.

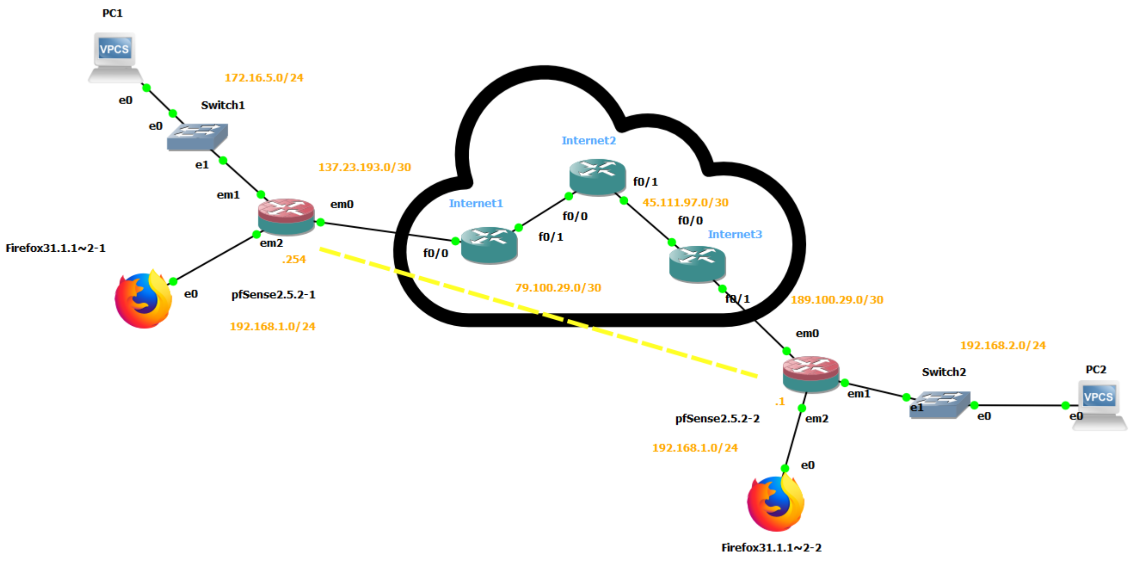
IPsec (Internet Protocol Security) is one of the main protocols used to establish and maintain VPN connections. IPsec operates at the network level, which means it encrypts and authenticates data packets as they move between the VPN endpoints.

Specifically, IPsec uses two modes of operation:

- Transport Mode: IPsec only encrypts the content of IP packets, leaving the IP header intact. This allows the packets to be routed normally through the internet.

- Tunnel Mode: IPsec encrypts both the content and the IP header of the packets. This creates a virtual "tunnel" through the internet, completely obscuring the original communication.

In the diagram used for the practice, the VPN communication between the Pfsense firewalls utilizes the Tunnel mode of IPsec. This means that all traffic between the PC1 and PC2 networks travels in an encrypted manner through this virtual tunnel, providing a high level of security and privacy.



Development

For the development of this practice, the first step was researching how to integrate pfSense firewalls and their respective Firefox configurations to enable HTTP configuration. When running these two tools, we had to add an additional interface to the firewalls for the Firefox browsers, as they originally came with only two ports: one for WAN and one for LAN. Through this interface, we connected via HTTP outside the LAN using a different network, and we restricted access to only allow HTTP connections. This ensured no other ports were open, creating a more secure and professional design.

Once everything was set up according to the practice diagram, we proceeded to configure the corresponding IP addressing. We set up the EIGRP routing protocol between Internet routers 1 to 3.

Next, in pfSense, we changed the WAN and LAN interface addresses to the ones corresponding to each pfSense. We also added the static route with its next hop: towards Internet 1 from pfSense1 (R2) and towards Internet 3 from pfSense2 (R4), using a default route of 0.0.0.0/0.

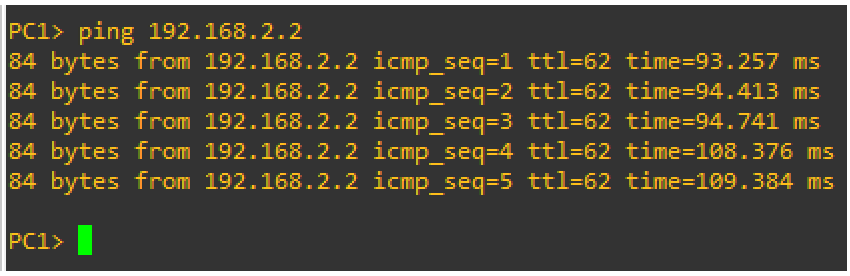
With this completed, we moved on to configuring the VPN with IPsec. We created the first phase of the VPN with key exchange using IKEv2 on the WAN interface. The remote gateway was set to the IP of the WAN interface of the other firewall. For authentication, we used mutual PSK with a pre-shared key configured identically on both firewalls. For the encryption algorithm, we used AES256-GCM with 128-bit SHA256 and DH group14 with 2048 bits.

In phase 2 of the VPN, we set the local network as the LAN subnet and the remote network as the LAN network on the other side. We used the ESP (Encapsulating Security Payload) protocol and selected AES256-GCM with 128-bit encryption and DH group14 with 2048 bits. The automatic host ping was directed to the LAN IP of the other side.

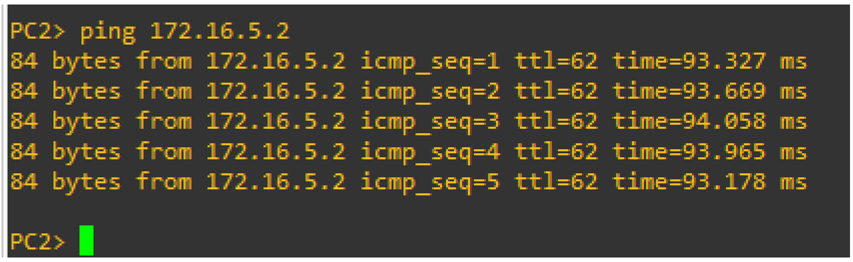
Finally, we set up rules for the WAN interface, adding two: one to allow ICMP (ping) traffic from any source to any destination and another for UDP traffic on port 500 (ISAKMP) for the VPN. On the LAN interface, we kept the default rules. On OPT1, we created a rule for HTTP connections. In the IPsec interface, we created a rule to allow traffic from the LAN on the other side to pass through to our LAN network. This configuration was mirrored for both firewalls.

Evidence

Ping PC1 a PC2

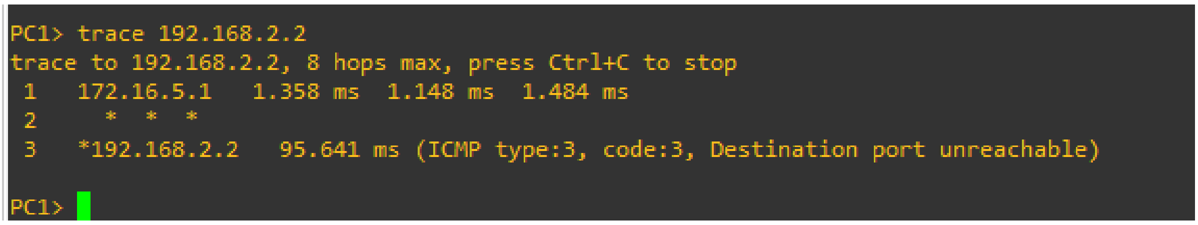


```
PC1> ping 192.168.2.2
84 bytes from 192.168.2.2 icmp_seq=1 ttl=62 time=93.257 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=62 time=94.413 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=62 time=94.741 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=62 time=108.376 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=62 time=109.384 ms

PC1>
```

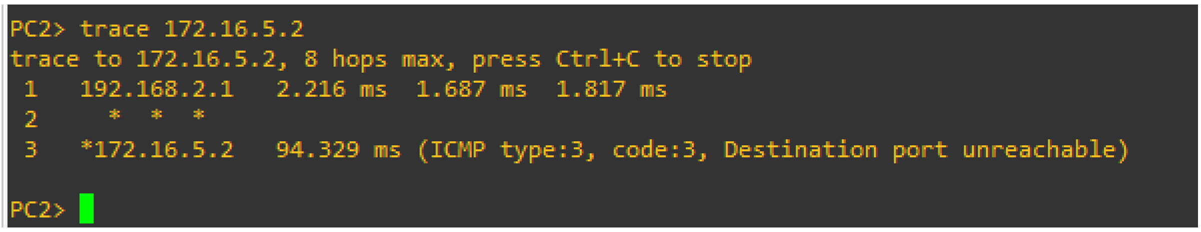


```
PC2> ping 172.16.5.2
84 bytes from 172.16.5.2 icmp_seq=1 ttl=62 time=93.327 ms
84 bytes from 172.16.5.2 icmp_seq=2 ttl=62 time=93.669 ms
84 bytes from 172.16.5.2 icmp_seq=3 ttl=62 time=94.058 ms
84 bytes from 172.16.5.2 icmp_seq=4 ttl=62 time=93.965 ms
84 bytes from 172.16.5.2 icmp_seq=5 ttl=62 time=93.178 ms

PC2>
```

Traceroute de PC1 a PC2

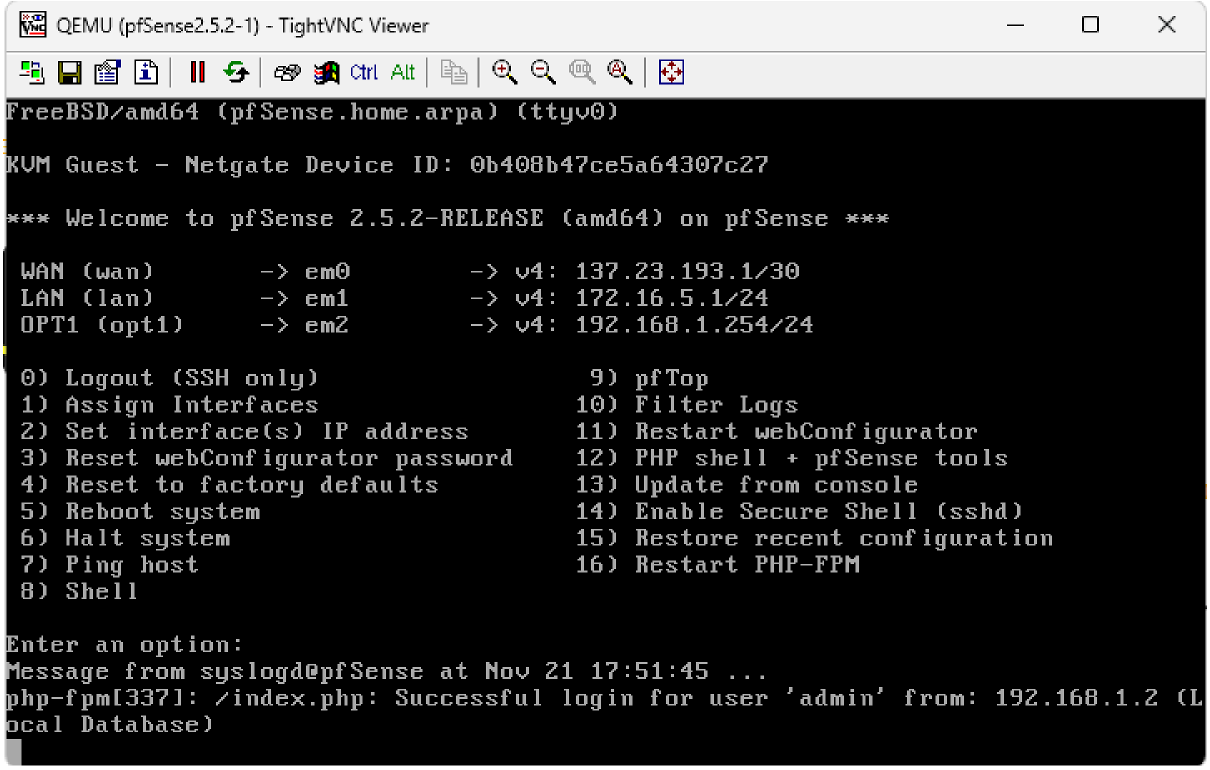


```
PC1> trace 192.168.2.2
trace to 192.168.2.2, 8 hops max, press Ctrl+C to stop
 1   172.16.5.1   1.358 ms  1.148 ms  1.484 ms
 2     *  *  *
 3   *192.168.2.2   95.641 ms (ICMP type:3, code:3, Destination port unreachable)

PC1>
```

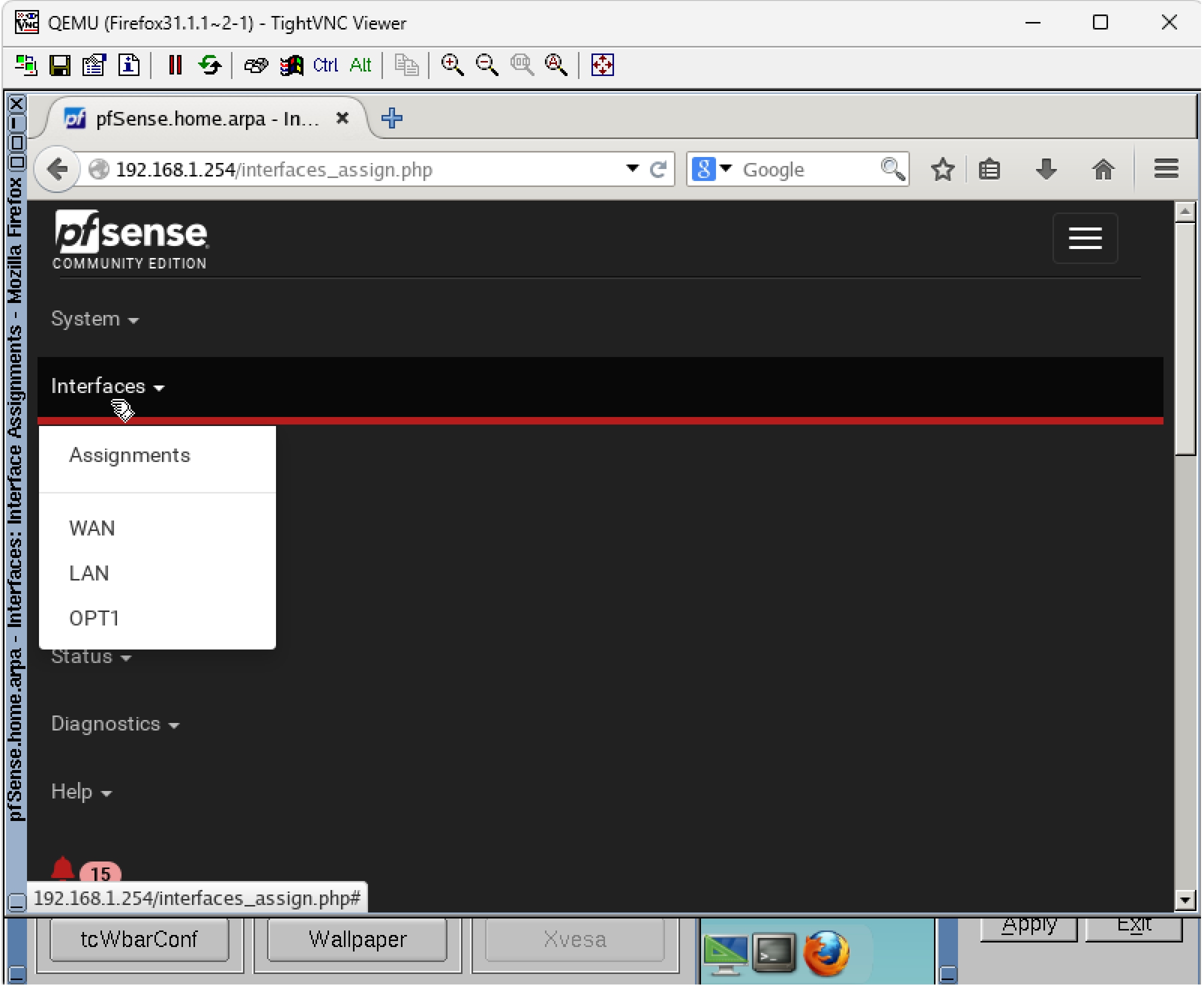


```
PC2> trace 172.16.5.2
trace to 172.16.5.2, 8 hops max, press Ctrl+C to stop
 1   192.168.2.1   2.216 ms  1.687 ms  1.817 ms
 2     *  *  *
 3   *172.16.5.2   94.329 ms (ICMP type:3, code:3, Destination port unreachable)

PC2>
```

Pfsense 1

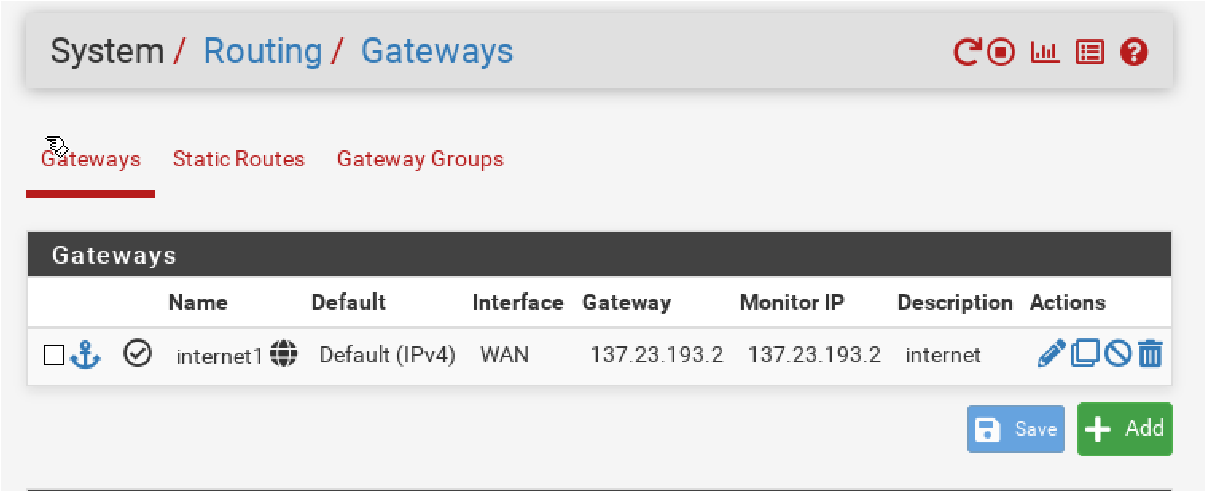


```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

KVM Guest - Netgate Device ID: 0b408b47ce5a64307c27

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

 WAN (wan)        -> em0        -> v4: 137.23.193.1/30
 LAN (lan)        -> em1        -> v4: 172.16.5.1/24
 OPT1 (opt1)      -> em2        -> v4: 192.168.1.254/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
Message from syslogd@pfSense at Nov 21 17:51:45 ...
php-fpm[337]: /index.php: Successful login for user 'admin' from: 192.168.1.2 (L
ocal Database)
```



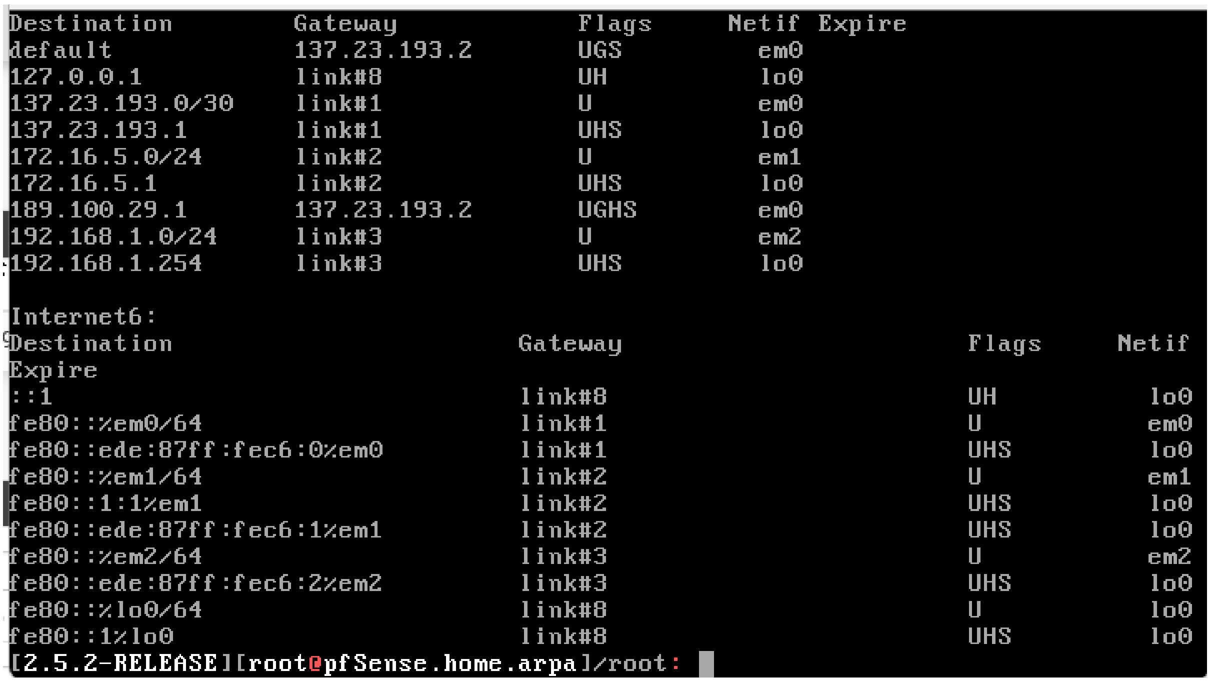
QEMU (Firefox31.1.1~2-1) - TightVNC Viewer
Ctrl Alt
pfSense.home.arpa - Interfaces: Interface Assignments - Mozilla Firefox
pfSense.home.arpa - In...
192.168.1.254/interfaces_assign.php
Google
pfsense
COMMUNITY EDITION
System
Interfaces
Assignments
WAN
LAN
OPT1
Status
Diagnostics
Help
15
192.168.1.254/interfaces_assign.php#
tcWbarConf
Wallpaper
Xvesa
Apply
Exit

Default route



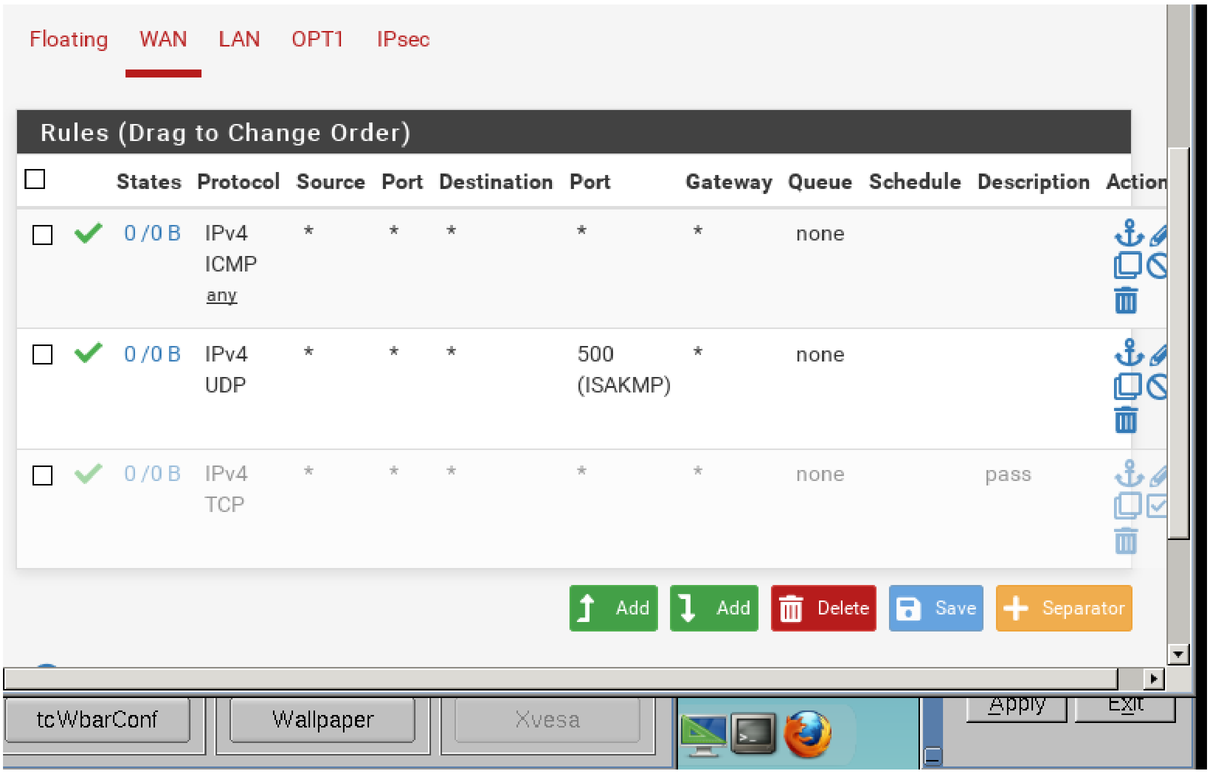
Gateways

	Name	Default	Interface	Gateway	Monitor IP	Description	Actions
□ ⚓ ✓	internet1 🌐	Default (IPv4)	WAN	137.23.193.2	137.23.193.2	internet	



```
Destination        Gateway            Flags     Netif Expire
default            137.23.193.2       UGS         em0
127.0.0.1          link#8             UH          lo0
137.23.193.0/30    link#1             U           em0
137.23.193.1       link#1             UHS         lo0
172.16.5.0/24      link#2             U           em1
172.16.5.1         link#2             UHS         lo0
189.100.29.1       137.23.193.2       UGHS        em0
192.168.1.0/24     link#3             U           em2
192.168.1.254      link#3             UHS         lo0

Internet6:
Destination                       Gateway                       Flags     Netif
Expire
::1                               link#8                        UH          lo0
fe80::%em0/64                     link#1                        U           em0
fe80::ede:87ff:fec6:0%em0         link#1                        UHS         lo0
fe80::%em1/64                     link#2                        U           em1
fe80::1:1%em1                     link#2                        UHS         lo0
fe80::ede:87ff:fec6:1%em1         link#2                        UHS         lo0
fe80::%em2/64                     link#3                        U           em2
fe80::ede:87ff:fec6:2%em2         link#3                        UHS         lo0
fe80::%lo0/64                     link#8                        U           lo0
fe80::1%lo0                       link#8                        UHS         lo0
[2.5.2-RELEASE][root@pfSense.home.arpa]/root:
```

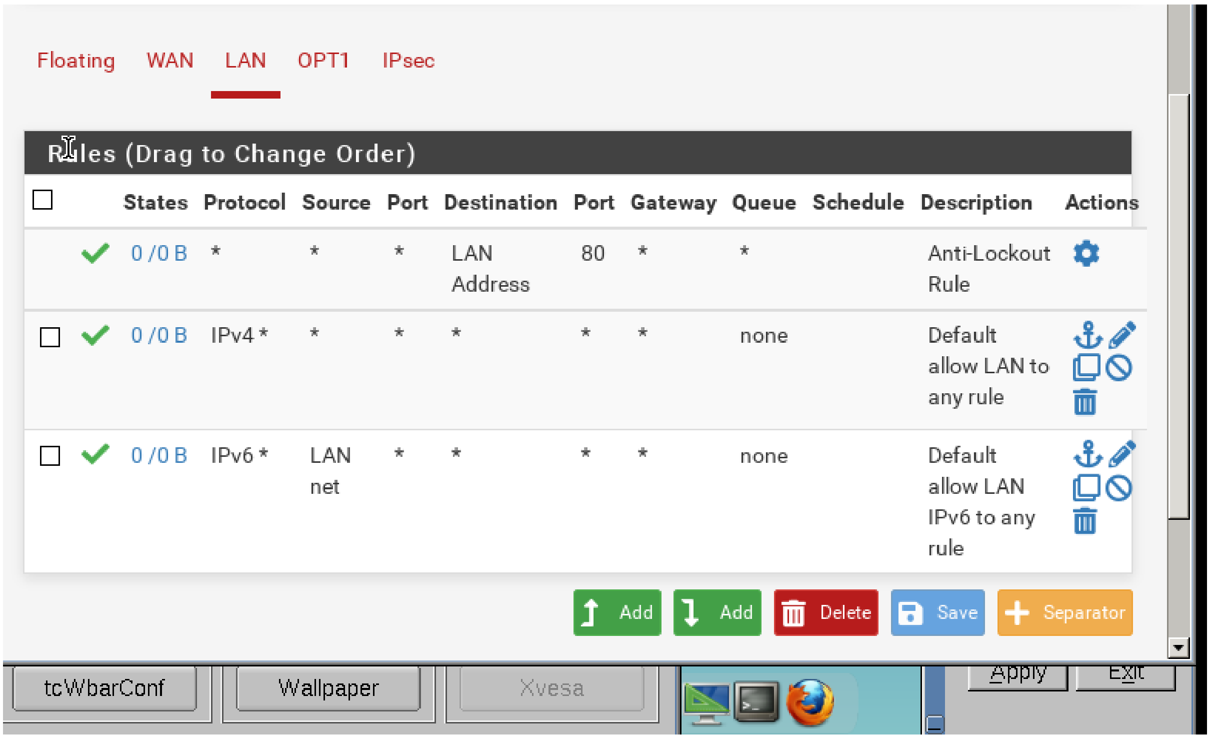
Rules WAN



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Action
□	✓	0 /0 B	IPv4 ICMP any	*	*	*	*	*	none			
□	✓	0 /0 B	IPv4 UDP	*	*	*	500 (ISAKMP)	*	none			
□	✓	0 /0 B	IPv4 TCP	*	*	*	*	*	none		pass	

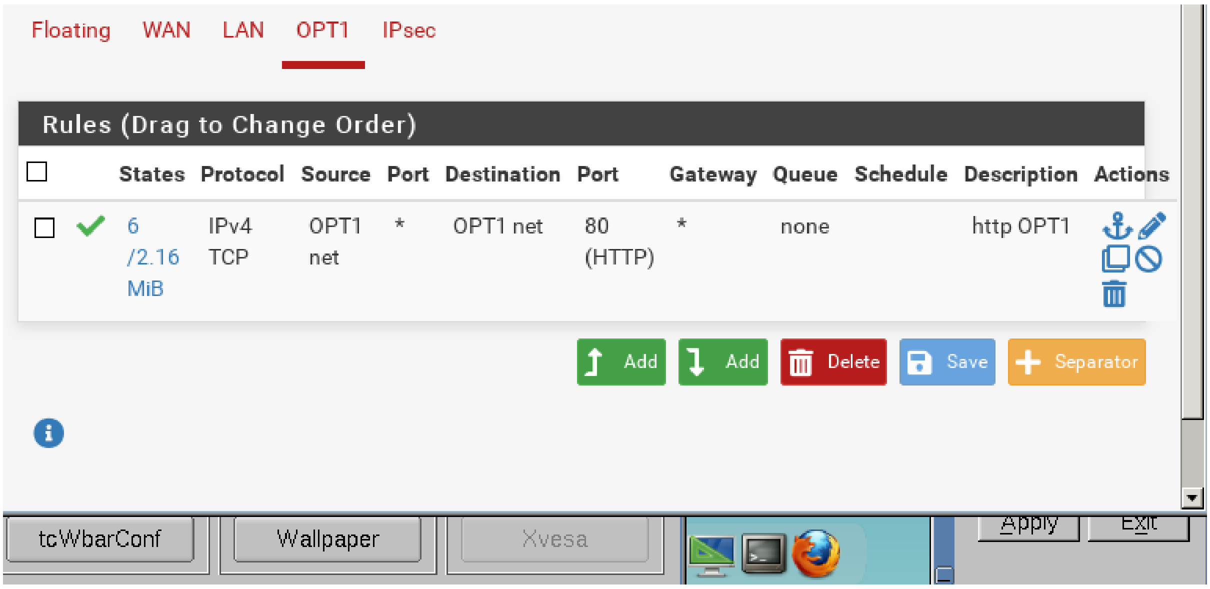
Rules LAN



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0 /0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
□	✓	0 /0 B	IPv4 *	*	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

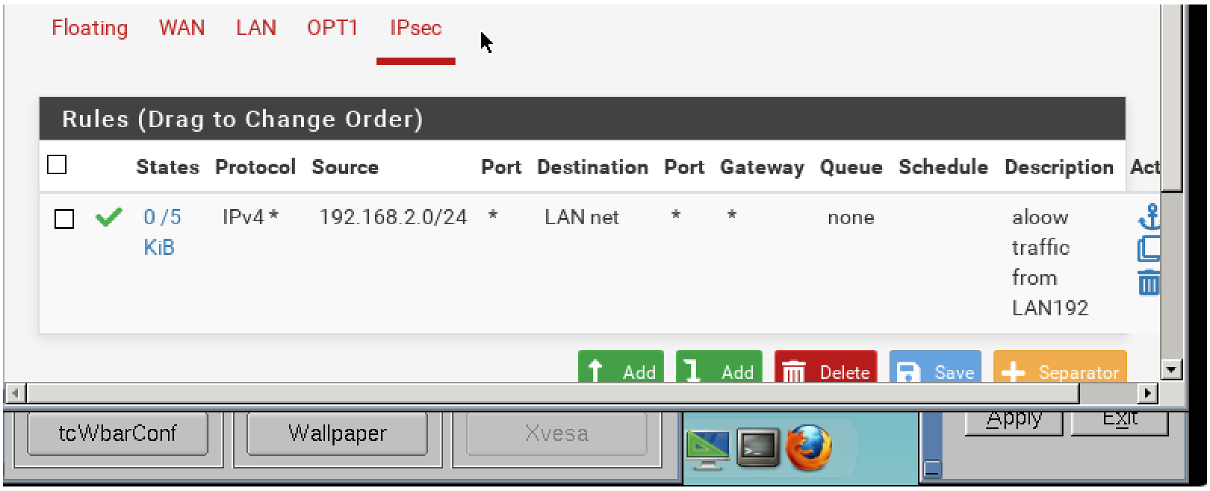
Rules OPT1



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	6 /2.16 MiB	IPv4 TCP	OPT1 net	*	OPT1 net	80 (HTTP)	*	none		http OPT1	

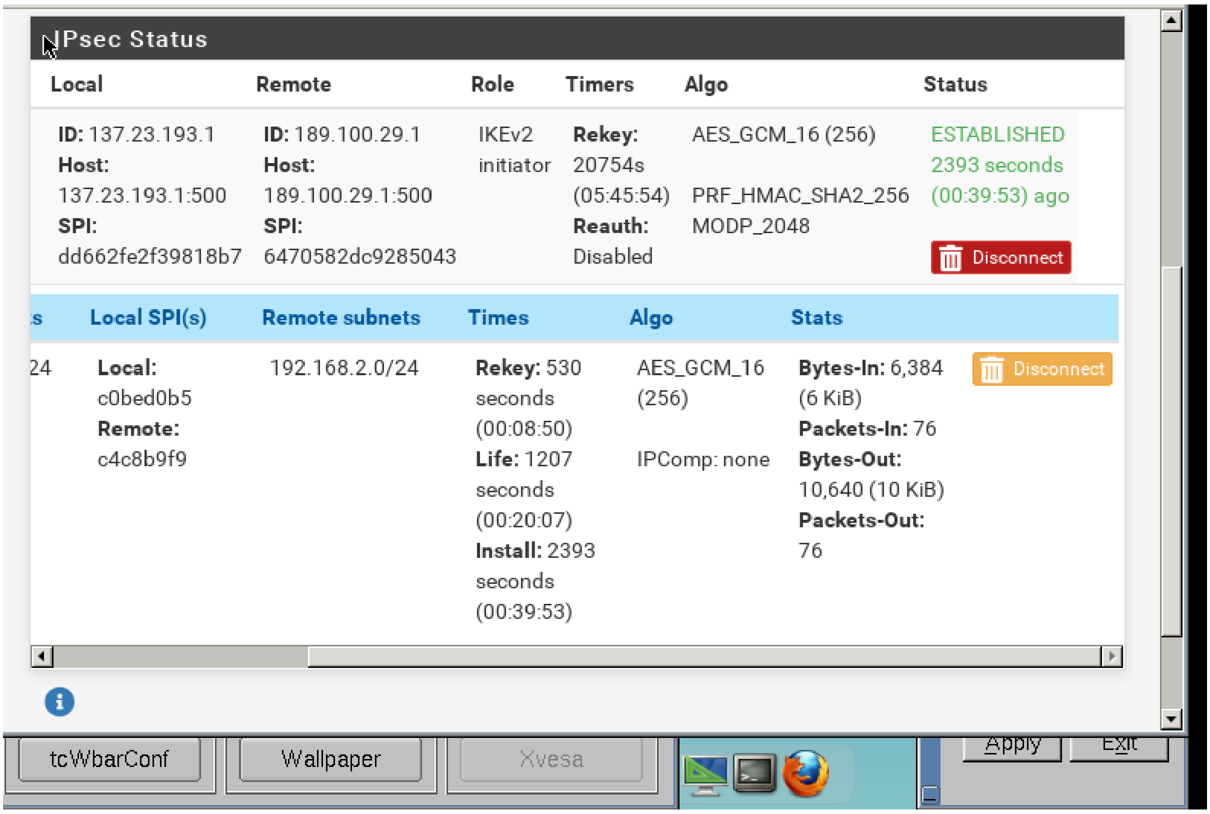
Rules IPsec



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Act
□	✓	0 /5 KiB	IPv4 *	192.168.2.0/24	*	LAN net	*	*	none		aloow traffic from LAN192	

Status IPsec

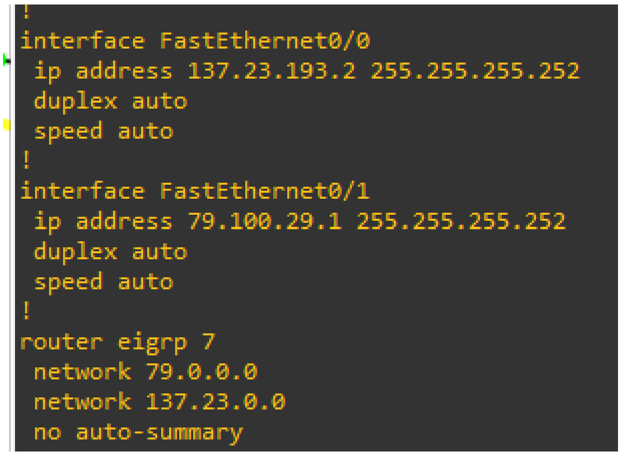


IPsec Status

Local	Remote	Role	Timers	Algo	Status
ID: 137.23.193.1 **Host:** 137.23.193.1:500 **SPI:** dd662fe2f39818b7	**ID:** 189.100.29.1 **Host:** 189.100.29.1:500 **SPI:** 6470582dc9285043	IKEv2 initiator	**Rekey:** 20754s (05:45:54) **Reauth:** Disabled	AES_GCM_16 (256) PRF_HMAC_SHA2_256 MODP_2048	ESTABLISHED 2393 seconds (00:39:53) ago Disconnect

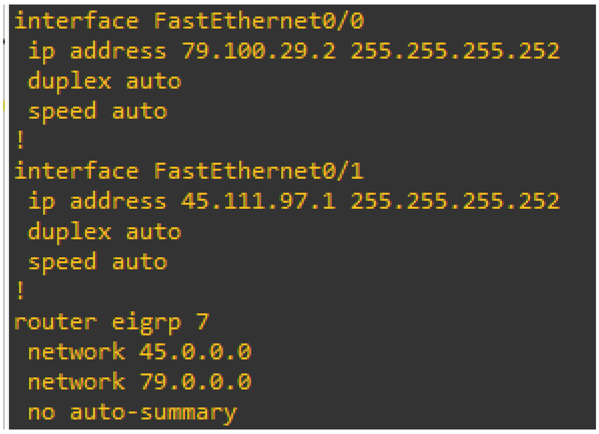
s	Local SPI(s)	Remote subnets	Times	Algo	Stats	
24	**Local:** c0bed0b5 **Remote:** c4c8b9f9	192.168.2.0/24	**Rekey:** 530 seconds (00:08:50) **Life:** 1207 seconds (00:20:07) **Install:** 2393 seconds (00:39:53)	AES_GCM_16 (256) IPComp: none	**Bytes-In:** 6,384 (6 KiB) **Packets-In:** 76 **Bytes-Out:** 10,640 (10 KiB) **Packets-Out:** 76	Disconnect

Internet 1



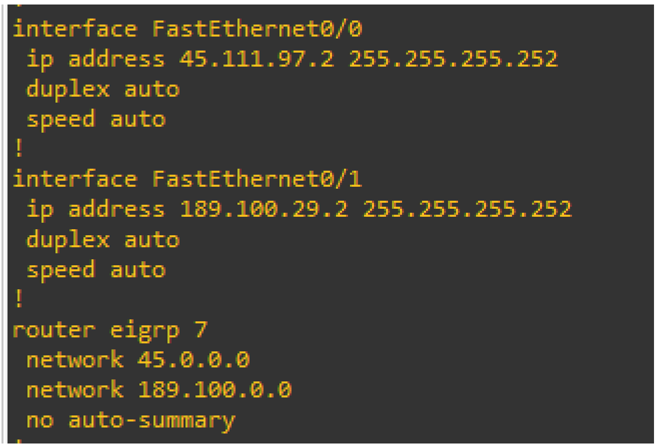
```
!
interface FastEthernet0/0
 ip address 137.23.193.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 79.100.29.1 255.255.255.252
 duplex auto
 speed auto
!
router eigrp 7
 network 79.0.0.0
 network 137.23.0.0
 no auto-summary
```

Internet 2



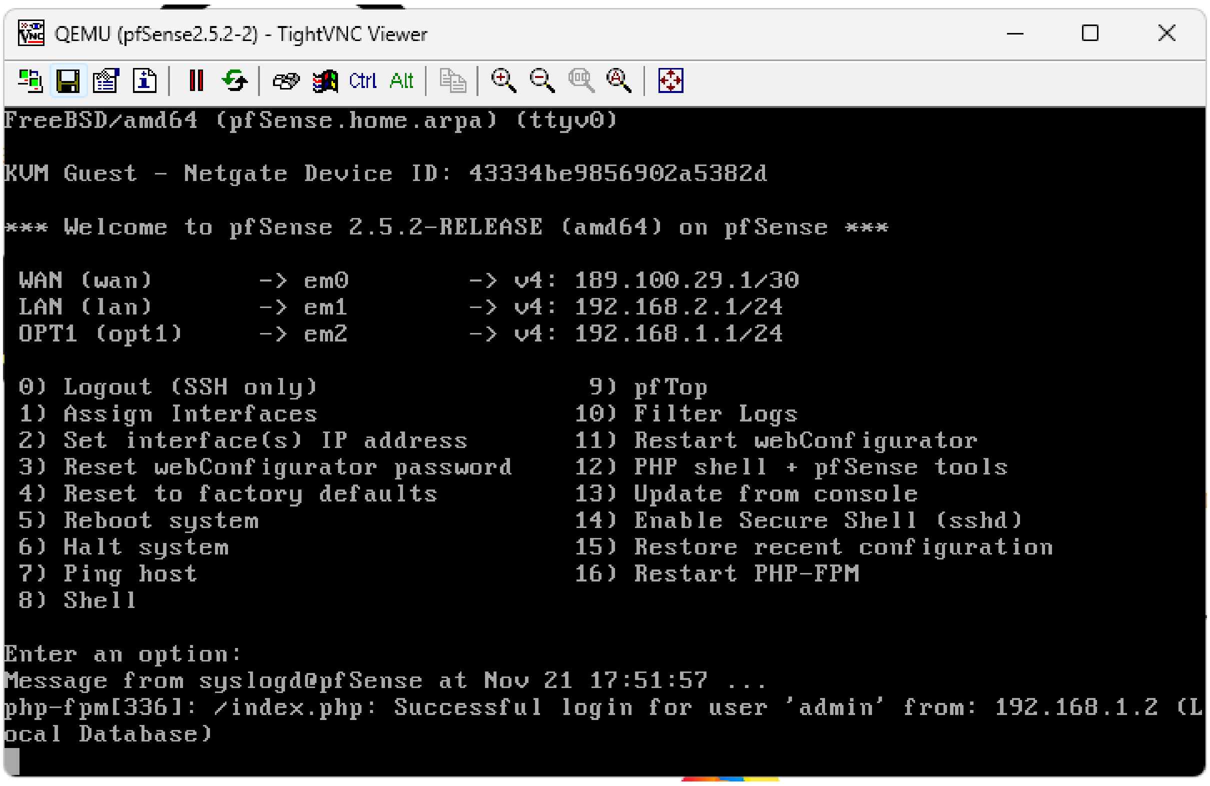
```
interface FastEthernet0/0
 ip address 79.100.29.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 45.111.97.1 255.255.255.252
 duplex auto
 speed auto
!
router eigrp 7
 network 45.0.0.0
 network 79.0.0.0
 no auto-summary
```

Internet 3



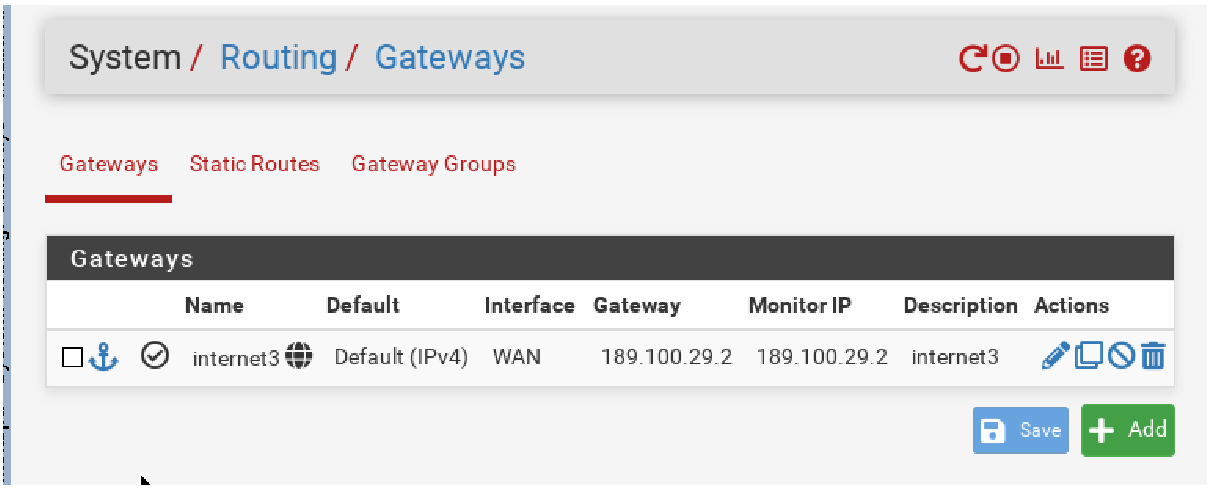
```
interface FastEthernet0/0
 ip address 45.111.97.2 255.255.255.252
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 189.100.29.2 255.255.255.252
 duplex auto
 speed auto
!
router eigrp 7
 network 45.0.0.0
 network 189.100.0.0
 no auto-summary
```

Pfsense 2



```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)

KVM Guest - Netgate Device ID: 43334be9856902a5382d

*** Welcome to pfSense 2.5.2-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4: 189.100.29.1/30
 LAN (lan)       -> em1        -> v4: 192.168.2.1/24
 OPT1 (opt1)     -> em2        -> v4: 192.168.1.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
Message from syslogd@pfSense at Nov 21 17:51:57 ...
php-fpm[336]: /index.php: Successful login for user 'admin' from: 192.168.1.2 (L
ocal Database)
```

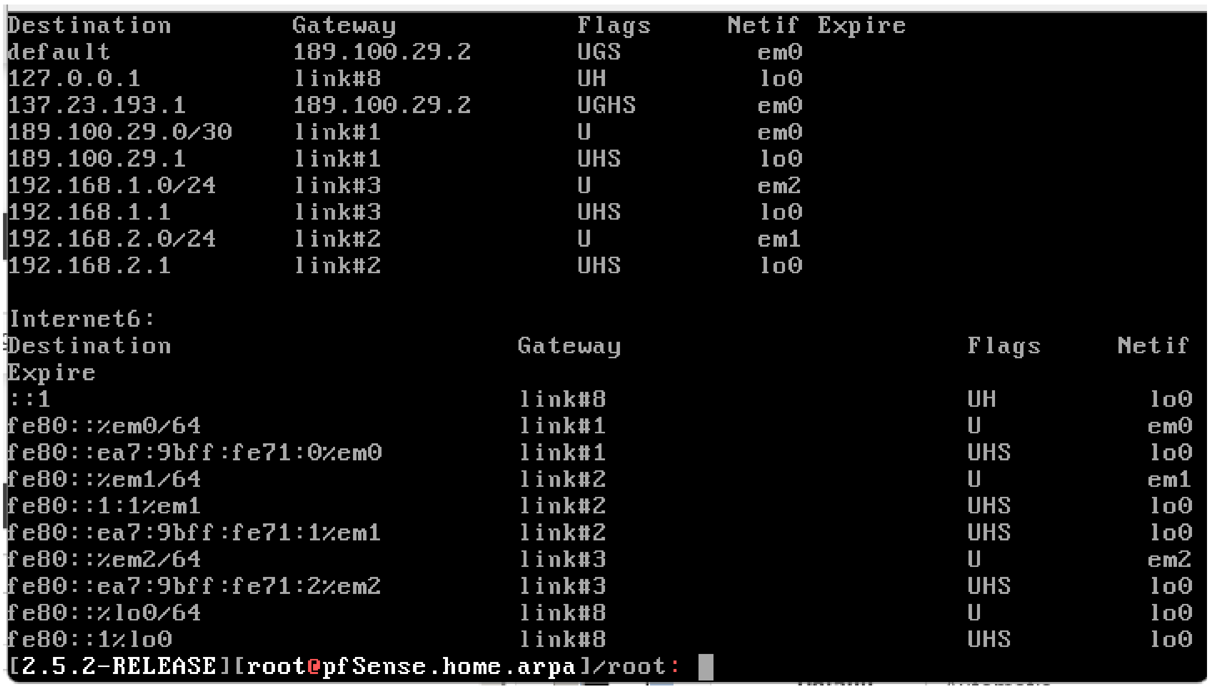
Default route



System / Routing / Gateways

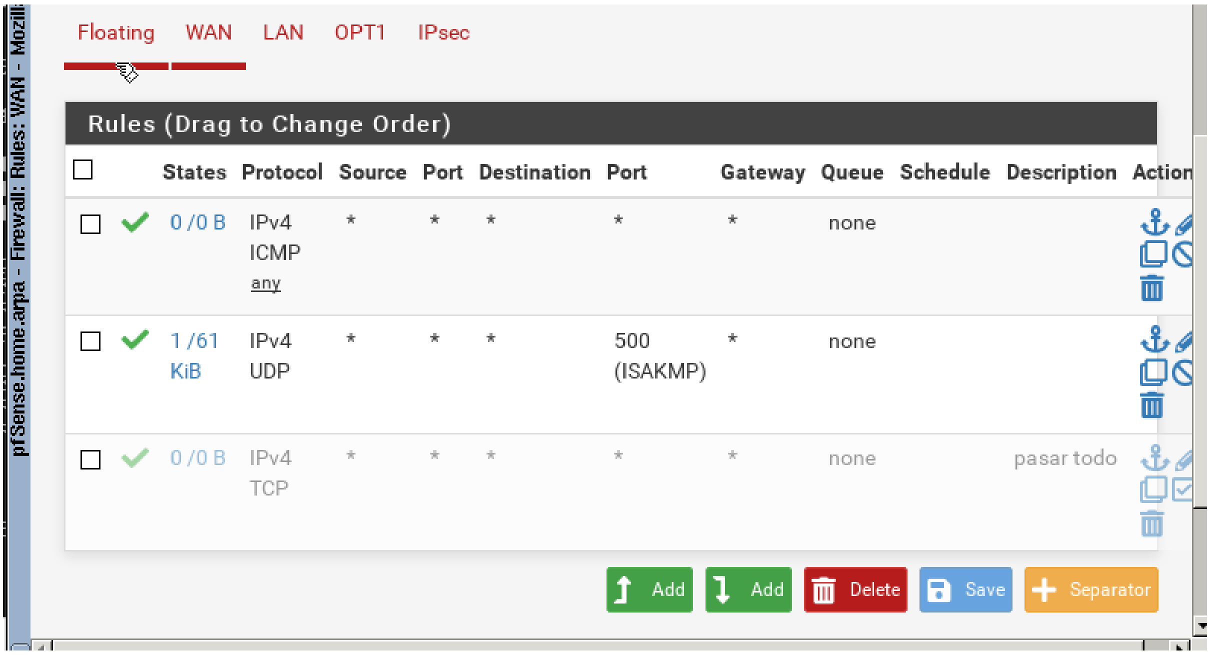
Gateways

		Name	Default	Interface	Gateway	Monitor IP	Description	Actions
□ ⚓	✓	internet3 🌐	Default (IPv4)	WAN	189.100.29.2	189.100.29.2	internet3	



```
Destination        Gateway            Flags     Netif Expire
default            189.100.29.2       UGS         em0
127.0.0.1          link#8             UH          lo0
137.23.193.1       189.100.29.2       UGHS        em0
189.100.29.0/30    link#1             U           em0
189.100.29.1       link#1             UHS         lo0
192.168.1.0/24     link#3             U           em2
192.168.1.1        link#3             UHS         lo0
192.168.2.0/24     link#2             U           em1
192.168.2.1        link#2             UHS         lo0

Internet6:
Destination                       Gateway                       Flags     Netif
Expire
::1                               link#8                        UH          lo0
fe80::%em0/64                     link#1                        U           em0
fe80::ea7:9bff:fe71:0%em0         link#1                        UHS         lo0
fe80::%em1/64                     link#2                        U           em1
fe80::1:1%em1                     link#2                        UHS         lo0
fe80::ea7:9bff:fe71:1%em1         link#2                        UHS         lo0
fe80::%em2/64                     link#3                        U           em2
fe80::ea7:9bff:fe71:2%em2         link#3                        UHS         lo0
fe80::%lo0/64                     link#8                        U           lo0
fe80::1%lo0                       link#8                        UHS         lo0
[2.5.2-RELEASE][root@pfSense.home.arpa]/root:
```

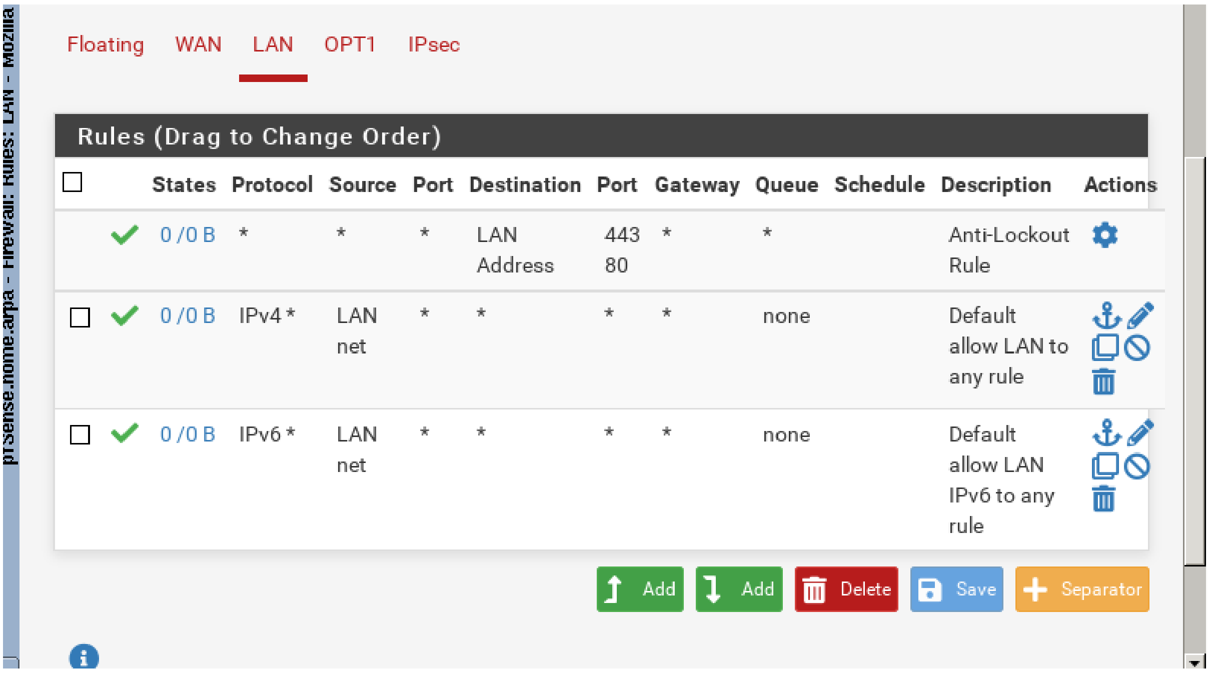
Rules WAN



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Action
□	✓	0 /0 B	IPv4 ICMP any	*	*	*	*	*	none			
□	✓	1 /61 KiB	IPv4 UDP	*	*	*	500 (ISAKMP)	*	none			
□	✓	0 /0 B	IPv4 TCP	*	*	*	*	*	none		pasar todo	

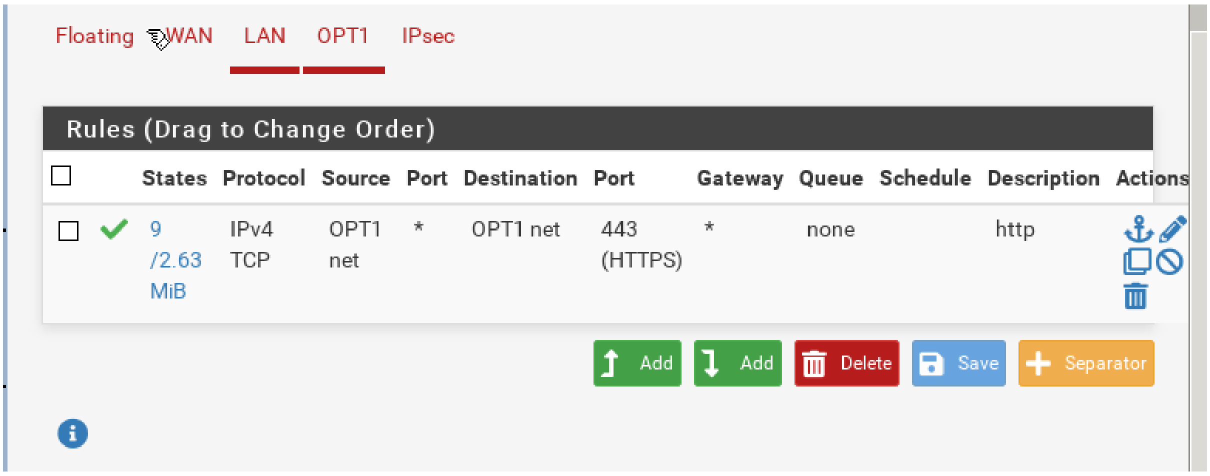
Rules LAN



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	0 /0 B	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
□	✓	0 /0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
□	✓	0 /0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

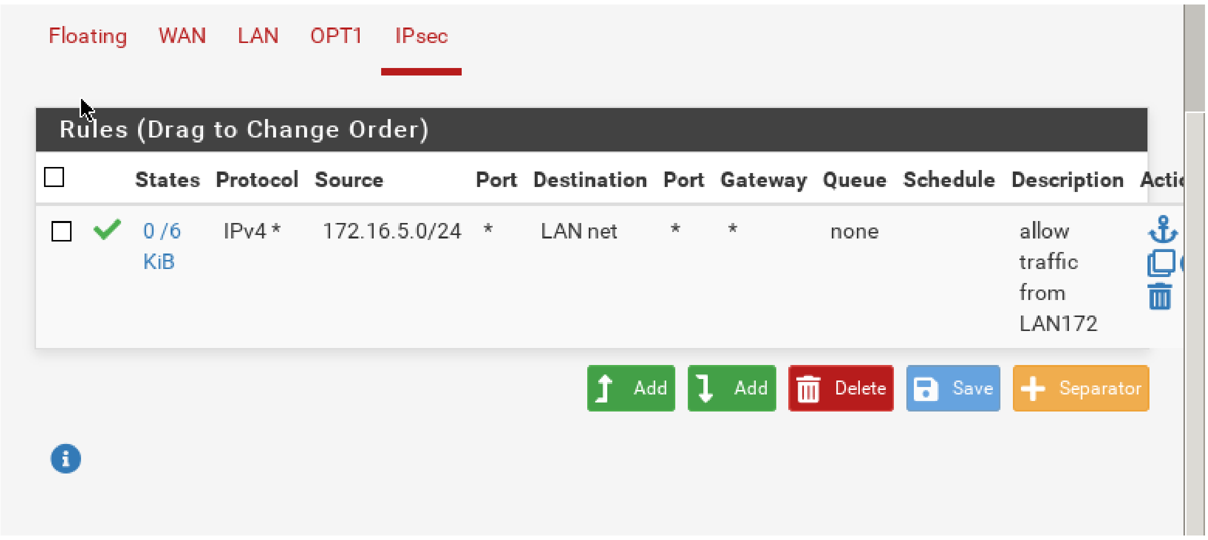
Rules OPT1



Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
☐	✓	9 /2.63 MiB	IPv4 TCP	OPT1 net	*	OPT1 net	443 (HTTPS)	*	none		http	

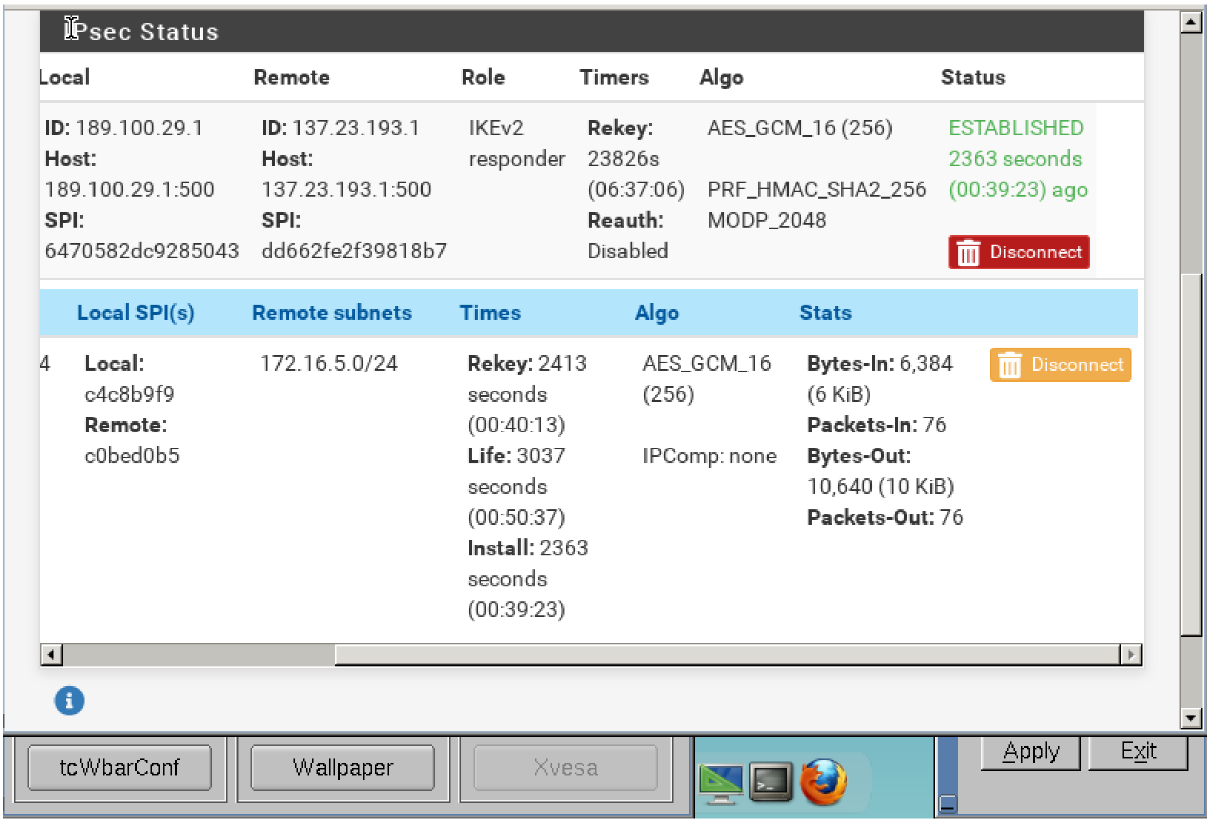
Rules IPsec



Rules (Drag to Change Order)

☐		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Acti
☐	✓	0 /6 KiB	IPv4 *	172.16.5.0/24	*	LAN net	*	*	none		allow traffic from LAN172	

Status IPsec



IPsec Status

Local	Remote	Role	Timers	Algo	Status
ID: 189.100.29.1 **Host:** 189.100.29.1:500 **SPI:** 6470582dc9285043	**ID:** 137.23.193.1 **Host:** 137.23.193.1:500 **SPI:** dd662fe2f39818b7	IKEv2 responder	**Rekey:** 23826s (06:37:06) **Reauth:** Disabled	AES_GCM_16 (256) PRF_HMAC_SHA2_256 MODP_2048	ESTABLISHED 2363 seconds (00:39:23) ago Disconnect

	Local SPI(s)	Remote subnets	Times	Algo	Stats	
4	**Local:** c4c8b9f9 **Remote:** c0bed0b5	172.16.5.0/24	**Rekey:** 2413 seconds (00:40:13) **Life:** 3037 seconds (00:50:37) **Install:** 2363 seconds (00:39:23)	AES_GCM_16 (256) IPComp: none	**Bytes-In:** 6,384 (6 KiB) **Packets-In:** 76 **Bytes-Out:** 10,640 (10 KiB) **Packets-Out:** 76	Disconnect

Conclusions

Luis Carlos:
My conclusion from this work is that I learned a lot, especially because we implemented it with a firewall interface, which is the most common setup in companies today. This gives a more advanced focus to the practices, which is very useful for us to be able to apply this knowledge in a professional setting with ease, as we now have the experience.

We encountered an issue with the VPN but managed to resolve it. The problem was that we had not configured the same parameters on both firewalls, so they didn't match and wouldn't connect. Once we fixed it, everything worked perfectly.

I found this to be one of the practices where I learned new knowledge that is widely used in the industry today. Additionally, we are applying security to the connections, which aligns closely with our field as cybersecurity engineers.

Diego Gutiérrez:
In conclusion, the existence of VPNs is very useful, since through their operation we can create links from one point to another as if the devices were within the same network. Specifically regarding IPsec, it's good that different types of VPNs exist because if the medium (Internet) is not under our control, it's reassuring to know that you can guarantee the confidentiality of your connection by encrypting it.

I believe it was correct to attempt completing the practice using firewalls, since in everyday situations, these will be the starting point VPN tools that companies use. Although they won't be Pfsense, it's important to understand the operation and rule declarations that must be made to complete a proper configuration and correctly allow the interesting traffic.

Sources

- Diogo, Tânia. "What Is IPsec and How Does It Work?" Devopedia, 13 Apr. 2020, https://devopedia.org/ipsec.