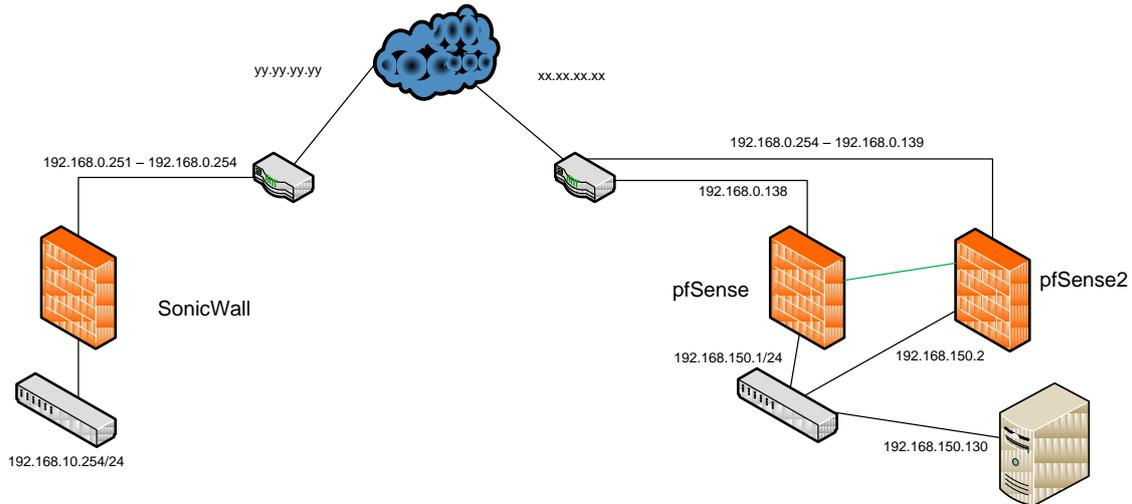


# pfSense : VPN with NAT

Test procedure on pfSense 2.0 β5 (I use it because I need to manage more than one network on IPsec Phase 2)



The link in green carry the network 10.138.1.0/30.

From the SonicWall, there's only one IP from the outer network.

192.168.150.0/24 is under NAT 10.138.1.1.

Only the HTTP access on 192.168.150.130 is seen from 192.168.10.0/24

## pfSense Firewall

I really need to add another interface, virtual IP doesn't helped me there.

Interfaces: OPT1



General configuration	
Enable	<input checked="" type="checkbox"/> <b>Enable Interface</b>
Description	<input type="text" value="OPT1"/> <small>Enter a description (name) for the interface here.</small>
Type	Static
MAC address	<input type="text"/> <small>This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections) Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank</small>
MTU	<input type="text"/> <small>If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.</small>
MSS	<input type="text"/> <small>If you enter a value in this field, then MSS damping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.</small>
Static IP configuration	
IP address	<input type="text" value="10.138.1.2"/> / <input type="text" value="30"/>
Gateway	<input type="text" value="None"/> <small>If this interface is an Internet connection, select an existing Gateway from the list or add a new one.</small>
Private networks	
<input type="checkbox"/> <b>Block private networks</b>	<small>When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.</small>
<input type="checkbox"/> <b>Block bogon networks</b>	<small>When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.</small>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

# pfSense : VPN with NAT

## Now let's place some rules

**Firewall: Rules** S L ?

Floating WAN LAN **OPT1** IPsec

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>	ICMP	10.138.1.1	*	10.138.1.2	*	*	none			
<input type="checkbox"/>	ICMP	10.138.1.1	*	192.168.10.1	*	*	none			
<input type="checkbox"/>	TCP	10.138.1.1	*	192.168.10.0/24	*	*	none			

pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled)

**Hint:**  
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

**Firewall: Rules** S L ?

Floating WAN LAN **OPT1** IPsec

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	
<input type="checkbox"/>	TCP	192.168.10.0/24	*	OPT1 net	80 (HTTP)	*	none		Pass TCP Isec HTTP	
<input type="checkbox"/>	ICMP	192.168.10.0/24	*	OPT1 net	*	*	none		Pass ICMP From IPsec	

pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled)

**Hint:**  
Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

## pfSense2 firewall

I place the IP address endpoint of the VPN:

**Interfaces: OPT1** S ?

**General configuration**

Enable  **Enable Interface**

Description   
Enter a description (name) for the interface here.

Type

MAC address   
Insert my local MAC address  
This field can be used to modify ("spoof") the MAC address of the WAN interface (may be required with some cable connections)  
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank

MTU   
If you leave this field blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary on some hardware.

MSS   
If you enter a value in this field, then MSS clamping for TCP connections to the value entered above minus 40 (TCP/IP header size) will be in effect.

**Static IP configuration**

IP address  /

Gateway   
If this interface is an Internet connection, select an existing Gateway from the list or add a new one.

**Private networks**

**Block private networks**  
When set, this option blocks traffic from IP addresses that are reserved for private networks as per RFC 1918 (10/8, 172.16/12, 192.168/16) as well as loopback addresses (127/8). You should generally leave this option turned on, unless your WAN network lies in such a private address space, too.

**Block bogon networks**  
When set, this option blocks traffic from IP addresses that are reserved (but not RFC 1918) or not yet assigned by IANA. Bogons are prefixes that should never appear in the Internet routing table, and obviously should not appear as the source address in any packets you receive.

## Routing

Just adding the gateway 10.138.1.2 of the first pfSense for the netmask 192.168.10.0/24.

# pfSense : VPN with NAT

## System: Gateways

Name	Interface	Gateway	Monitor IP	Description
GW_WAN (default)	WAN	192.168.0.254	192.168.0.254	Interface wan Static Gateway
GWIpsec1	OPT1	10.138.1.2	10.138.1.2	

## System: Static Routes

Network	Gateway	Interface	Description
192.168.10.0/24	GWIpsec1 - 10.138.1.2	OPT1	

**Note:** Do not enter static routes for networks assigned on any interface of this firewall. Static routes are only used for networks reachable via a different router, and not reachable via your default gateway.

## Firewall rules

### Firewall: Rules

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
*	*	*	*	LAN Address	22 80	*	*		Anti-Lockout Rule
	ICMP echoreq	192.168.10.0/24	*	10.138.1.1	*	*	none		
	ICMP echoreq	192.168.150.0/24	*	192.168.10.0/24	*	*	none		
	TCP	192.168.150.0/24	*	192.168.10.0/24	80 (HTTP)	*	none		

pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled)

**Hint:** Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

### Firewall: Rules

ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
	TCP	*	*	192.168.150.130	80 (HTTP)	*	none		NAT
	ICMP echoreq	192.168.10.0/24	*	10.138.1.1	*	*	none		
	TCP	192.168.10.0/24	*	LAN net	80 (HTTP)	*	none		

pass pass (disabled) block block (disabled) reject reject (disabled) log log (disabled)

**Hint:** Rules are evaluated on a first-match basis (i.e. the action of the first rule to match a packet will be executed). This means that if you use block rules, you'll have to pay attention to the rule order. Everything that isn't explicitly passed is blocked by default.

## Nat rules

Here, we define 10.138.1.1 port 80 is redirected to 192.168.150.130 port 80:

### Firewall: NAT: Port Forward

If	Proto	Src. addr	Src. ports	Dest. addr	Dest. ports	NAT IP	NAT Ports	Description
OPT1	TCP	*	*	OPT1 address	80 (HTTP)	192.168.150.130	80 (HTTP)	

pass linked rule

And use the interface OPT1 for packets from our LAN to the outer LAN:

# pfSense : VPN with NAT

**Firewall: NAT: Outbound**

Port Forward 1:1 Outbound

Mode:  Automatic outbound NAT rule generation (IPsec passthrough included)  Manual Outbound NAT rule generation (AON - Advanced Outbound NAT)

Mappings:

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
<input type="checkbox"/> OPT1	192.168.150.0/24	*	192.168.10.0/24	*	*	*	NO	

**Note:**  
If advanced outbound NAT is enabled, no outbound NAT rules will be automatically generated any longer. Instead, only the mappings you specify below will be used. With advanced outbound NAT disabled, a mapping is automatically created for each interface's subnet (except WAN). If you use target addresses other than the WAN interface's IP address, then depending on the way your WAN connection is setup, you may also need a Virtual IP.

## Testing

1. Ping from 192.168.150.130 to 192.168.10.1
2. HTTP communication from 192.168.150.130 to 192.168.10.1 (we verify the correct content)
3. Ping from 192.168.10.10 to 10.138.1.1
4. HTTP communication from 192.168.10.10 to 10.138.1.1 (we verify the correct content)

On the first pfSense :

**Status: System logs: Firewall**

System Firewall DHCP Portal Auth IPsec PPP VPN Load Balancer OpenVPN OpenNTPD Settings

Normal View | Dynamic View | Summary View

Last 4 firewall log entries. Max(50)

Act	Time	If	Source	Destination	Proto
<input checked="" type="checkbox"/>	Feb 7 15:53:43	OPT1	10.138.1.1	192.168.10.1	ICMP
<input checked="" type="checkbox"/>	Feb 7 15:53:46	OPT1	10.138.1.1:18275	192.168.10.1:80	TCP:S
<input checked="" type="checkbox"/>	Feb 7 15:53:50	enc0	192.168.10.10	10.138.1.1	ICMP
<input checked="" type="checkbox"/>	Feb 7 15:53:52	enc0	192.168.10.10:56972	10.138.1.1:80	TCP:S

TCP Flags: F - FIN, S - SYN, A or . - ACK, R - RST, P - PSH, U - URG, E - ECE, C - CWR

On the pfSense2 :

**Status: System logs: Firewall**

System Firewall DHCP Portal Auth IPsec PPP VPN Load Balancer OpenVPN OpenNTPD Settings

Normal View | Dynamic View | Summary View

Last 4 firewall log entries. Max(50)

Act	Time	If	Source	Destination	Proto
<input checked="" type="checkbox"/>	Feb 7 15:53:43	LAN	192.168.150.130	192.168.10.1	ICMP
<input checked="" type="checkbox"/>	Feb 7 15:53:46	LAN	192.168.150.130:56835	192.168.10.1:80	TCP:S
<input checked="" type="checkbox"/>	Feb 7 15:53:50	OPT1	192.168.10.10	10.138.1.1	ICMP
<input checked="" type="checkbox"/>	Feb 7 15:53:52	OPT1	192.168.10.10:56972	192.168.150.130:80	TCP:S

TCP Flags: F - FIN, S - SYN, A or . - ACK, R - RST, P - PSH, U - URG, E - ECE, C - CWR

## Conclusion

It's just a test case before pfSense 2.1.