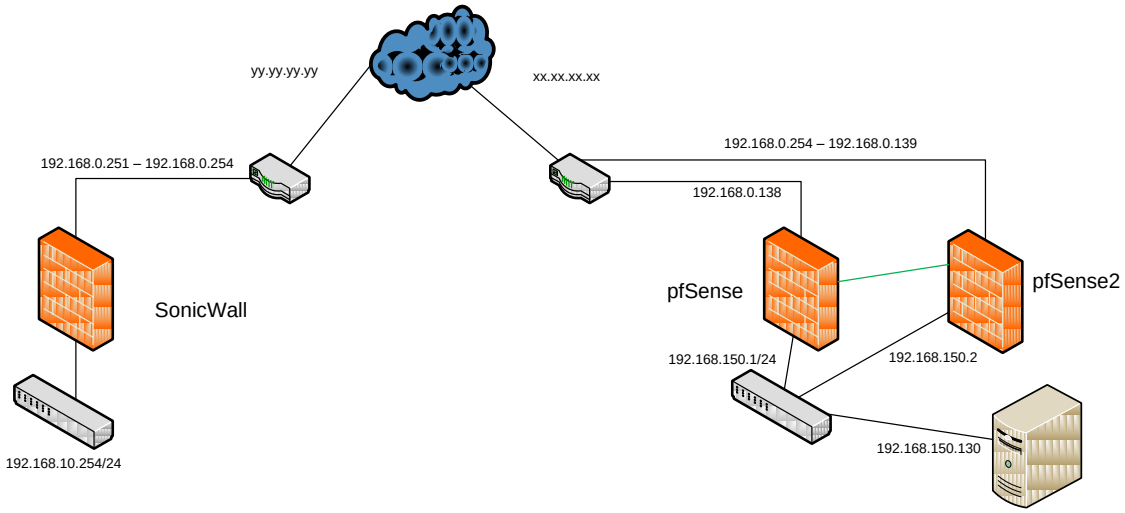
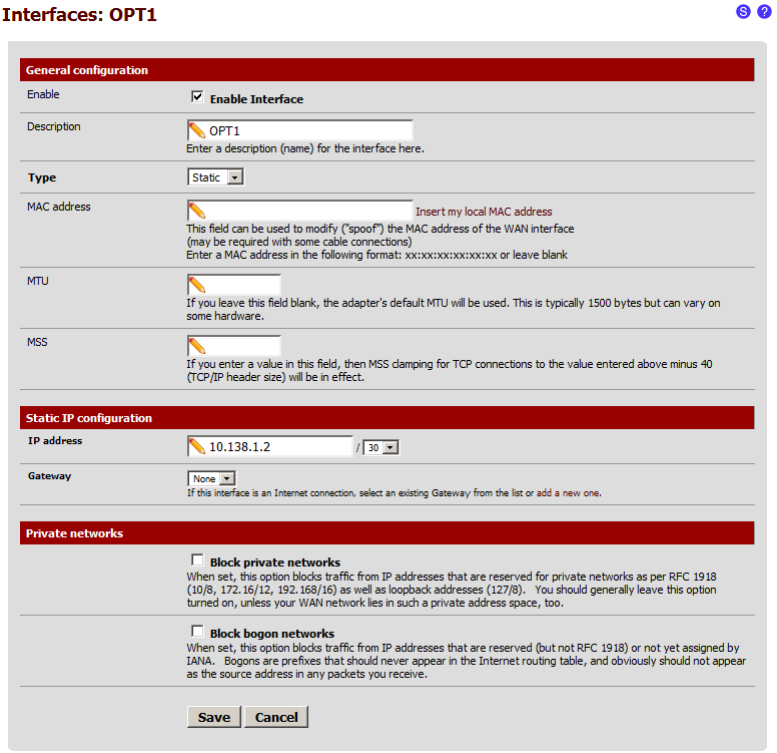
Test procedure on pfSense 2.0 β5 (I use it because I need to manage more than one network on IPsec Phase 2)



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.



Now let's place some rules

Firewall: Rules

Floating | WAN | LAN | OPT1 | IPsec

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		ICMP echoreq	10.138.1.1	*	10.138.1.2	*	*	none		
		ICMP echoreq	10.138.1.1	*	192.168.10.1	*	*	none		
		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

Floating | WAN | LAN | OPT1 | IPsec

	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description
		TCP	192.168.10.0/24	*	OPT1 net	80 (HTTP)	*	none		Pass TCP Ipsec HTTP
		ICMP echoreq	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

General configuration

Enable: Enable Interface

Description: OPT1
Enter a description (name) for the interface here.

Type: Static

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: 10.138.1.1 / 30

Gateway: None
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.

Save | Cancel

Routing

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

System: Gateways

Gateways | Routes | Groups

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

Gateways | Routes | Groups

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

Floating | WAN | LAN | OPT1

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

Floating | WAN | LAN | OPT1

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:

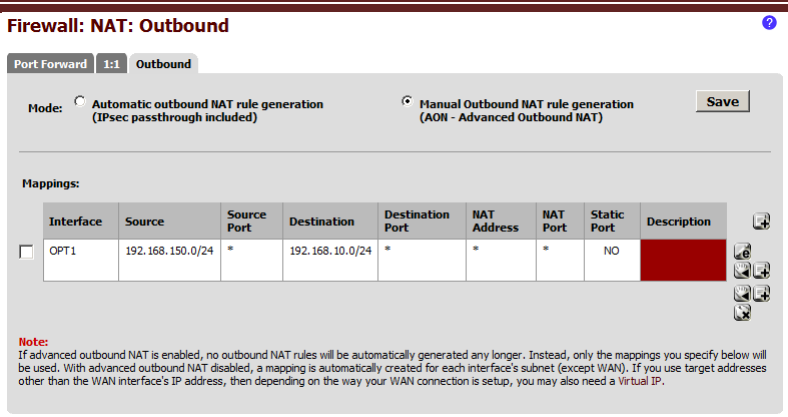
Firewall: NAT: Port Forward

Port Forward | 1:1 | Outbound

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

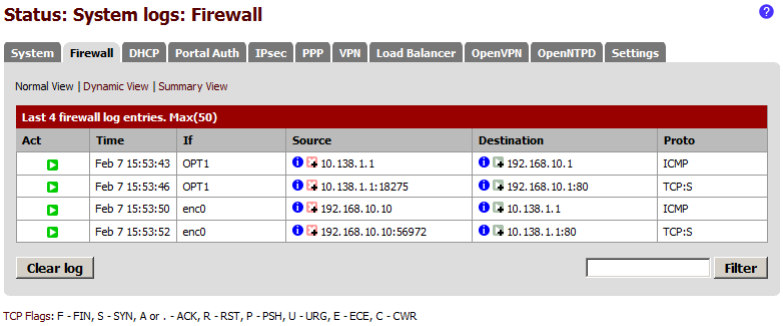
And use the interface OPT1 for packets from our LAN to the outer LAN:



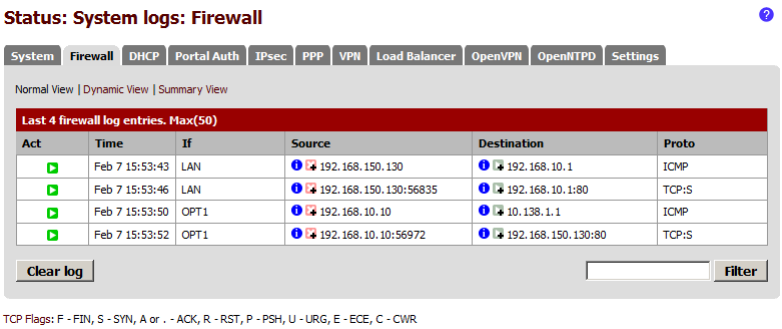
Testing

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 :



On the pfSense2 :



Conclusion

It’s just a test case before pfSense 2.1.