pfSense Firewall
Firewall Features - Considerations

Prior to diving into firewall rules and configuration, we'll look at some considerations for best results in firewall deployment.

We'll discuss:

- **Rules and Rulesets**
- **Stateful Filtering**
- **Blocking vs. Rejecting Traffic**
- **Ingress vs. Egress**

Rules and Rulesets

Firewalls process traffic and permit, take action on, or deny it based on Rules. You can group sets of related rules into Rulesets if your configuration is complex enough to warrant that.

Once you create a rule, you assign it to an interface or to interfaces. You also specify the direction on the interface.

Rules are read from top to bottom and traffic is processed based on the first match observed in the rules or ruleset.

If you have a rule that is likely to be used often, it is best to have it higher in the list of rules. This will reduce the processing load on your system. The firewall won't have to go through a rule or rules that don't apply to get to the one that does as often if the common traffic is processed first.

For example, if you use HTTPS a lot, and SSH only a little, and you want to have rules to allow both, it makes sense to check for HTTPS first, then SSH.

Stateful Filtering

You'll see this referred to as Stateful Packet Inspection or SPI by some firewall vendors such as Cisco.

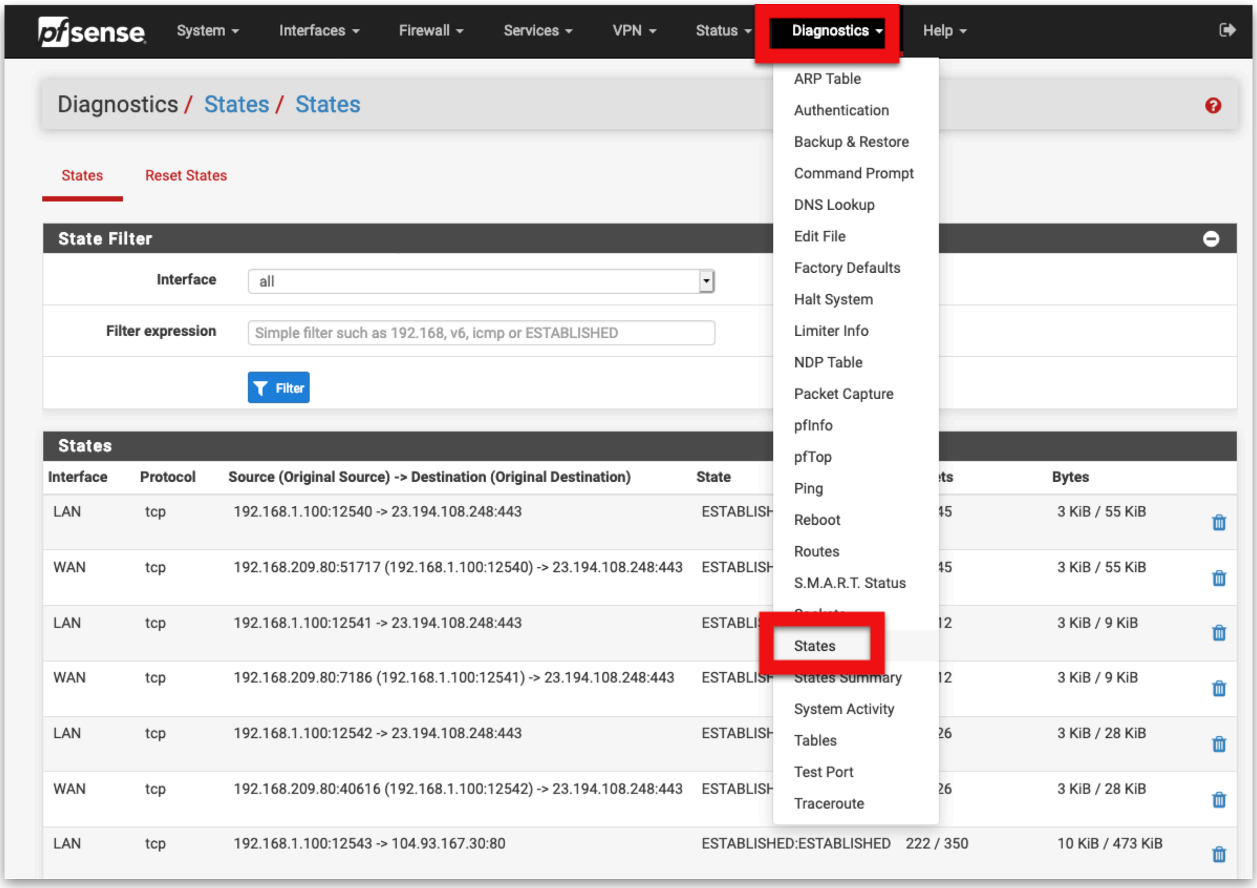
You want your firewall to keep track of information going out, and you want it to let the return traffic back in to the requestor.

However you don't want to let unrequested traffic or potentially malicious into your network.

You don't want to have to define all return traffic, because you likely don't know ahead of time what your users or even you will have to have access in advance.

The firewall keeps track of outbound requests and listens for and processes related replies in a State Table. The state table records the source, destination, protocol, ports, and the state of the connection as well as the interface involved.

You can see the state table on your pfSense Firewall at any time by clicking on Diagnostics and choosing States from the menu.



Diagnostics / States / States

State Filter

Interface: all

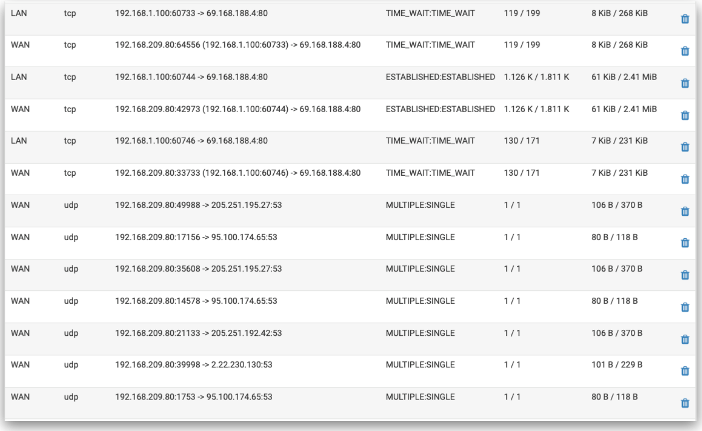
Filter expression: Simple filter such as 192.168, v6, icmp or ESTABLISHED

States

Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	ts	Bytes
LAN	tcp	192.168.1.100:12540 -> 23.194.108.248:443	ESTABLISH	45	3 KiB / 55 KiB
WAN	tcp	192.168.209.80:51717 (192.168.1.100:12540) -> 23.194.108.248:443	ESTABLISH	45	3 KiB / 55 KiB
LAN	tcp	192.168.1.100:12541 -> 23.194.108.248:443	ESTABLI	12	3 KiB / 9 KiB
WAN	tcp	192.168.209.80:7186 (192.168.1.100:12541) -> 23.194.108.248:443	ESTABLISH	12	3 KiB / 9 KiB
LAN	tcp	192.168.1.100:12542 -> 23.194.108.248:443	ESTABLISH	26	3 KiB / 28 KiB
WAN	tcp	192.168.209.80:40616 (192.168.1.100:12542) -> 23.194.108.248:443	ESTABLISH	26	3 KiB / 28 KiB
LAN	tcp	192.168.1.100:12543 -> 104.93.167.30:80	ESTABLISHED:ESTABLISHED	222 / 350	10 KiB / 473 KiB

Some examples of state types are ESTABLISHED for active connections, and FIN_WAIT_2 for a connection that is or is expected to be closing. States are shown as pairs separated by a colon.

ESTABLISHED:ESTABLISHED means the connection is established from the perspective of the sender and receiver as far as the firewall can tell.



LAN	tcp	192.168.1.100:60733 -> 69.168.188.4:80	TIME_WAIT:TIME_WAIT	119 / 199	8 KiB / 268 KiB
WAN	tcp	192.168.209.80:64556 (192.168.1.100:60733) -> 69.168.188.4:80	TIME_WAIT:TIME_WAIT	119 / 199	8 KiB / 268 KiB
LAN	tcp	192.168.1.100:60744 -> 69.168.188.4:80	ESTABLISHED:ESTABLISHED	1.126 K / 1.811 K	61 KiB / 2.41 MiB
WAN	tcp	192.168.209.80:42973 (192.168.1.100:60744) -> 69.168.188.4:80	ESTABLISHED:ESTABLISHED	1.126 K / 1.811 K	61 KiB / 2.41 MiB
LAN	tcp	192.168.1.100:60746 -> 69.168.188.4:80	TIME_WAIT:TIME_WAIT	130 / 171	7 KiB / 231 KiB
WAN	tcp	192.168.209.80:33733 (192.168.1.100:60746) -> 69.168.188.4:80	TIME_WAIT:TIME_WAIT	130 / 171	7 KiB / 231 KiB
WAN	udp	192.168.209.80:49988 -> 205.251.195.27:53	MULTIPLE:SINGLE	1 / 1	106 B / 370 B
WAN	udp	192.168.209.80:17156 -> 95.100.174.65:53	MULTIPLE:SINGLE	1 / 1	80 B / 118 B
WAN	udp	192.168.209.80:35608 -> 205.251.195.27:53	MULTIPLE:SINGLE	1 / 1	106 B / 370 B
WAN	udp	192.168.209.80:14578 -> 95.100.174.65:53	MULTIPLE:SINGLE	1 / 1	80 B / 118 B
WAN	udp	192.168.209.80:21133 -> 205.251.192.42:53	MULTIPLE:SINGLE	1 / 1	106 B / 370 B
WAN	udp	192.168.209.80:39998 -> 2.22.230.130:53	MULTIPLE:SINGLE	1 / 1	101 B / 229 B
WAN	udp	192.168.209.80:1753 -> 95.100.174.65:53	MULTIPLE:SINGLE	1 / 1	80 B / 118 B

TCP is connection oriented so sessions can be established.

UDP is connectionless so state is kind of simulated or set up for the purpose of knowing what may be expected in association with UDP traffic being sent.

You will see states like SINGLE:MULTIPLE, and MULTIPLE:SINGLE for UDP.

Other protocols like Internet Control Message Protocol (ICMP) will have states as well.

Any outbound request that is expecting a reply must have an entry in the state table.

Blocking vs. Rejecting

Blocking traffic silently drops it, not notifying the sender in any way. Your device looks like it is turned off.

Rejecting traffic sends an appropriate reply to the requestor to let them know the device is there, but the connection is not allowed.

In general, it is good practice to have Internet exposed devices block unwanted traffic and internal devices reject traffic that is not allowed.

Blocking theoretically makes it more difficult for an attacker to know a device is even there, and rejecting reduces the wait times associated with unanswered requests.

Ingress vs. Egress

Ingress and Egress from the firewall's perspective, if it's a device between your home or business and the Internet refers to traffic into or out of your home or business network.

If you want to go to google.com from a browser on your computer, the request from your computer to the nearest Google presence is considered Egress traffic.

If you have a web server hosted in a DMZ off of the Opt port on your pfSense Firewall, requests to that would be Ingress traffic.

Considering that the Internet is a wild and crazy place with automated scanners and manual hackers constantly scouring any exposure for weaknesses, you will typically want to disallow all Ingress traffic with very rare, highly secure exceptions like Virtual Private Networking (VPN) connections.

If your network isn't too complex, or maybe even if it is, you may want to consider Egress filtering as well. You would start by allowing protocols you know you'll use all the time like HTTP and HTTPS for web browsing, SSH for remotely accessing any servers you have on the Internet, if you have any, and making sure updates still work for your computers and Internet of Things (IoT) devices. Hopefully, those IoT things use HTTP or HTTPS, so they should not have to have other ports open.

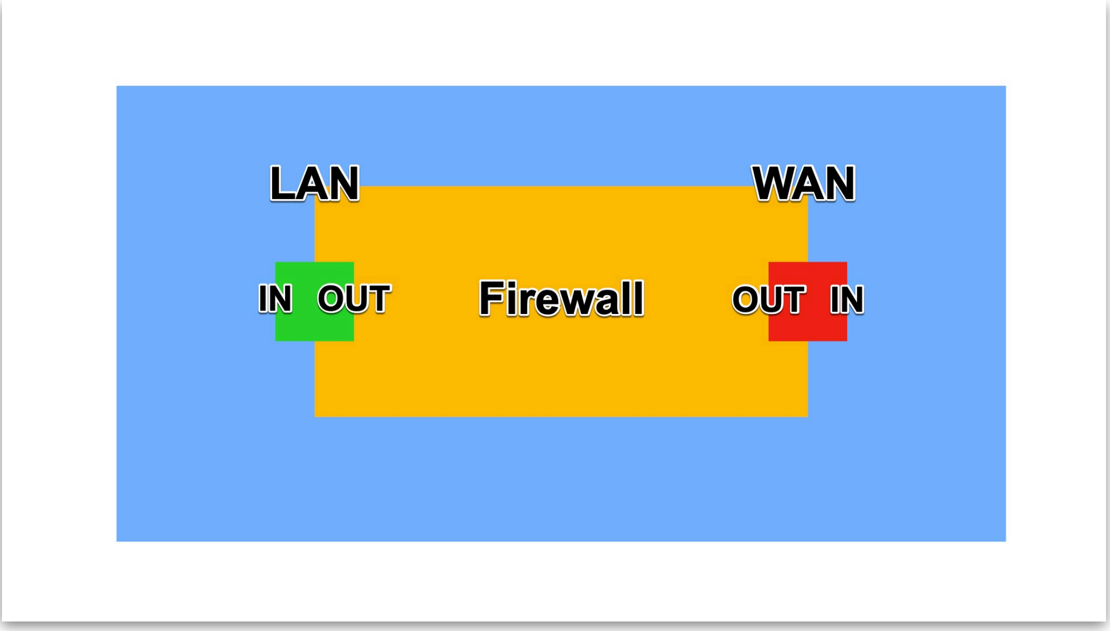
You would also want to allow Domain Name System (DNS) queries from all of your computers, or at least from your internal DNS forwarders or resolvers so name resolution can occur.

For your home network, this can be a great way to see what's going on.

For work, you'll want to have a pretty firm grasp on what other protocols are needed for your employees to do their work before denying traffic.

We'll cover some strategies for doing this with minimal chance of breaking things in an upcoming lesson.

Try to mentally put yourself in the position of the firewall when deciding whether traffic is Ingress or Egress from its perspective.



Traffic Into the LAN Interface would be Egress traffic from the network's perspective. Traffic going from the Firewall Out on the WAN Interface would also be Egress.

Traffic coming Into the WAN Interface would be Ingress. Traffic going Out from the Firewall toward the LAN on the LAN interface would also be Ingress. I hope the following table will make this clearer.

LAN		WAN	
In	Egress	In	Ingress
Out	Ingress	Out	Egress

In this lesson, you learned about:

- **Rules and Rulesets**
- **Stateful Filtering**
- **Blocking vs. Rejecting Traffic**
- **Ingress vs. Egress**

Next, we'll have a look at Whitelisting vs. Blacklisting approaches to firewalling.

References
pfSense book - 12.1 Firewalling Fundamentals
https://docs.netgate.com/manuals/pfsense/en/latest/the-pfsense-book.pdf