


[illegible]

Edit Firewall Rule

Action	Match		
	Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.		
Disabled	<input type="checkbox"/> Disable this rule Set this option to disable this rule without removing it from the list.		
Quick	<input type="checkbox"/> Apply the action immediately on match. Set this option to apply this action to traffic that matches this rule immediately.		
Interface	Any WAN LAN OPT1		
	Choose the interface(s) for this rule.		
Direction	any		
Address Family	IPv4		
	Select the Internet Protocol version this rule applies to.		
Protocol	TCP		
	Choose which IP protocol this rule should match.		

Source

Source	<input type="checkbox"/> Invert match	any	Source Address	/	
 Display Advanced					
The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any.					

Destination

Destination	<input type="checkbox"/> Invert match	any	Destination Address	/	
Destination Port Range	From	any	To	any	

☐ **Allow IP options** Allow packets with IP options to pass. Otherwise they are blocked by default. This is usually only seen with multicast traffic.

☐ **Disable reply-to** Disable auto generated reply to for this rule.

Tag
 A packet matching this rule can be marked and this mark used to match on other NAT/filter rules. It is called Policy filtering.

Tagged ☐ Invert Tagged
 Match a mark placed on a packet by a different rule with the Tag option. Check Invert to match packets which do not contain this tag.

Max. states
 Maximum state entries this rule can create.

Max. src nodes
 Maximum number of unique source hosts.

Max. connections
 Maximum number of established connections per host (TCP only).

Max. src. states
 Maximum state entries per host.

Max. src. conn. Rate
 Maximum new connections per host (TCP only).

Max. src. conn. Rates
 / per how many second(s) (TCP only)

State timeout
 State Timeout in seconds

TCP Flags

	FIN	SYN	RST	PSH	ACK	URG	ECN	CWR
set	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
out of	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ **Any flags.**
 Use this to choose TCP flags that must be set or cleared for this rule to match.

Firewall / Traffic Shaper / By Interface

☒ WAN
☐ LAN
☐ OPT1

Enable/Disable ☐ Enable/disable discipline and its children

Name lan

Scheduler Type HFSC
 Changing this changes all child queues! Beware information can be lost.

Bandwidth 100 Mbit/s

Queue Limit 3

TBR Size 16
 Adjusts the size, in bytes, of the token bucket regulator. If not specified, heuristics based on the interface bandwidth are used to determine the size.

In this lab, I learned how basic DDoS works and performs with ICMP and SYN floods. I also know how to perform these kinds of attacks, how to detect them using Wireshark, and how to prevent them with a firewall. Now, I know how to configure a firewall to prevent not only DDOS attack potential but also unknown traffic or traffic from suspected sources.