A03 – Firewall Troubleshooting

10 points
Turn in a Word or PDF document to the D2L Dropbox

Overview

In this lab you will be auditing and troubleshooting firewall rules in a pfSense firewall. You'll be reconfiguring the rules as necessary to meet certain business requirements.

Credentials

- pfSense
  - admin
  - pfsense
- Linux Servers
  - root
  - Password1!
- Windows Machines
  - DSU
  - Password1!

Network Overview

The network has the following machines:

- LAN
  FSD_Admin: Configured with DHCP
- DMZ
  - **FSD_Server1:** 64.42.152.100
  - **FSD_Server2:** 64.42.152.101
- WAN
  - **Internet**: 24.220.182.100

The interfaces on pfSense are configured as follows:

- em0: WAN: 24.220.182.102/24
- em1: LAN: 64.42.99.1/24
- em2: DMZ: 64.42.152.1/24

Your Task

- Analyze the firewall rules already in place. Make a determination if the rule should be modified in any way to fit the requirements below.
  - Fill out the table below to provide comments on the existing rules. Make notes of what the rule does, what is wrong with it if anything, and why it should be kept as is, modified, or deleted completely.
- Fix the firewall rules on the three interfaces to fit the requirements below. Note that a single requirement may not necessarily equate to a single firewall rule.

Deliverable

Submit the following screenshots in a Word or PDF document

- The table below with your comments and descriptions on the existing rules
- Three screenshots showing the firewall rules from each interface

Firewall Requirements

- Allow Internet to Server1 HTTP
- Allow LAN to Server2 HTTP
- Deny LAN to Server2 RDP
- Allow LAN to Server1 HTTP
- Allow LAN to Server1 RDP
- Prevent Servers from sending anything else not explicitly specified here outbound
- Allow LAN out to the internet on only HTTP, HTTPS, and DNS
- Allow Servers and LAN to ping anywhere, but don't allow the Internet to ping

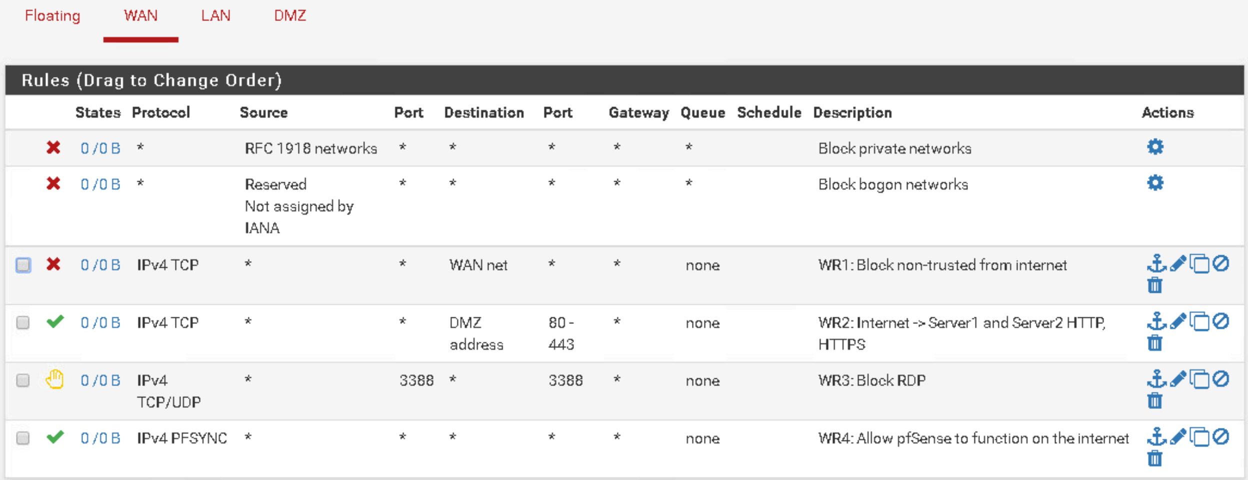
Rule ID	**Keep/Modify/Remove**	**Reasons**
WR1	remove	this rule is preventing the internet from accessing itself. useless.
WR2	modify	separate rules for each service (http, https, dns) and only to Serv.1
WR3	remove	dont want internet to rdp in
WR4	remove	protocol used to sync redundant firewalls
LR1	keep	need dns to both zones as precursor for http/https
LR2	modify	Change IGMP>ICMP echo,Change from drop to pass
LR3	keep/remove	not necessary according to reqmnts. not sure if removingwill break smthing
LR4	modify	separate rules for each service (http>dmz, rdp>server1)
LR5	remove	modifications to LR4 make this redundant
DR1	remove	rules to allow internet in don't belong on this interface
DR2	Modify	Remove the !! (inversions), change ipv4-TCP to ipv4+ipv6-ANY
DR3	Modify	ICMP any > ICMP echo request, Move to above DR2 (block all rule), and Change Destination address to *

Link to WAN Rules Screencap:
https://gyazo.com/26b11f6b1af2055138ee7f6625638be9

Link to LAN Rules Screencap:
https://gyazo.com/3c4a8a3ddf67301cf1a247649d6ebfe9

Link to DMZ Rules Screencap:
https://gyazo.com/a9e820f47bceb7c9fcaf4b761997c838

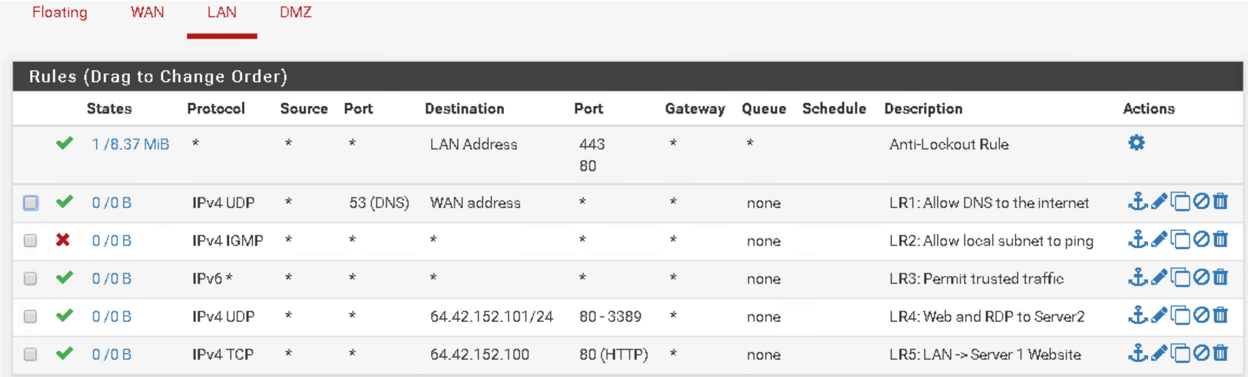
Original Rules



Floating WAN LAN DMZ

Rules (Drag to Change Order)

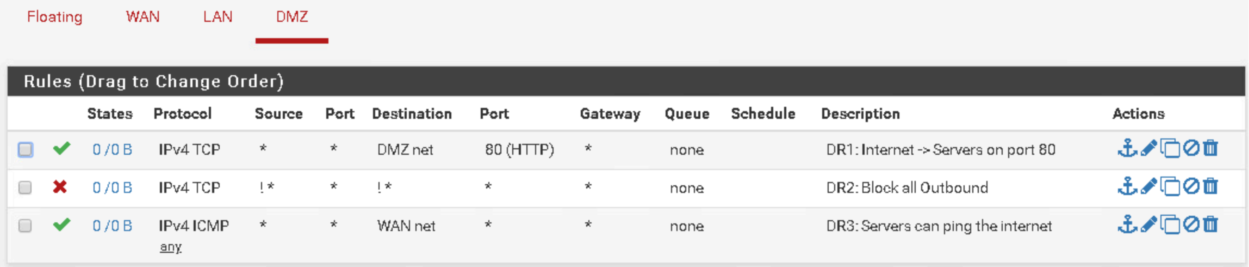
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗	0 /0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	⚙
	✗	0 /0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	⚙
□	✗	0 /0 B	IPv4 TCP	*	*	WAN net	*	*	none		WR1: Block non-trusted from internet	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0 /0 B	IPv4 TCP	*	*	DMZ address	80 - 443	*	none		WR2: Internet -> Server1 and Server2 HTTP, HTTPS	⚓ ✎ ⧉ ⊘ 🗑
□	✋	0 /0 B	IPv4 TCP/UDP	*	3388	*	3388	*	none		WR3: Block RDP	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0 /0 B	IPv4 PFSYNC	*	*	*	*	*	none		WR4: Allow pfSense to function on the internet	⚓ ✎ ⧉ ⊘ 🗑



Floating WAN LAN DMZ

Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	1 /8.37 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙
□	✓	0 /0 B	IPv4 UDP	*	53 (DNS)	WAN address	*	*	none		LR1: Allow DNS to the internet	⚓ ✎ ⧉ ⊘ 🗑
□	✗	0 /0 B	IPv4 IGMP	*	*	*	*	*	none		LR2: Allow local subnet to ping	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0 /0 B	IPv6 *	*	*	*	*	*	none		LR3: Permit trusted traffic	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0 /0 B	IPv4 UDP	*	*	64.42.152.101/24	80 - 3389	*	none		LR4: Web and RDP to Server2	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0 /0 B	IPv4 TCP	*	*	64.42.152.100	80 (HTTP)	*	none		LR5: LAN -> Server 1 Website	⚓ ✎ ⧉ ⊘ 🗑



Floating WAN LAN DMZ

Rules (Drag to Change Order)

		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0 /0 B	IPv4 TCP	*	*	DMZ net	80 (HTTP)	*	none		DR1: Internet -> Servers on port 80	⚓ ✎ ⧉ ⊘ 🗑
□	✗	0 /0 B	IPv4 TCP	! *	*	! *	*	*	none		DR2: Block all Outbound	⚓ ✎ ⧉ ⊘ 🗑
□	✓	0 /0 B	IPv4 ICMP any	*	*	WAN net	*	*	none		DR3: Servers can ping the internet	⚓ ✎ ⧉ ⊘ 🗑