

Firewall

- NAT Rules
- Security Rules

NAT Rules

Inbound NAT Translation

3	Inbound Guacamole	none	 untrusted	 untrusted	ethernet1/1	any	 14.202.159.252	any	none	destination-translation address: 10.99.8.8
---	-------------------	------	---	---	-------------	-----	--	-----	------	---

Outbound NAT for internet access in DMZ

8	Outbound Guacamole NAT	none	 dmz	 untrusted	ethernet1/1	 10.99.8.8	any	any	dynamic-ip-and-port ethernet1/1 TPG Fibre Public IP	none	363036	2023-07-31 15:59:07	2023-07-03 11:49:17	2023-07-03 11:51:53	2023-07-03 11:49:11
---	------------------------	------	---	---	-------------	---	-----	-----	---	------	--------	---------------------	---------------------	---------------------	---------------------

Security Rules

Given Guac sits in DMZ, with outbound internet access and internal network access, we need to be very careful around what we can allow the server access to.

The server has restrictive access to the internal LAN, as well as external internet.

Guac to Outbound

Internal LAN to Guac:

Only allows SSH and SSL access to the server, as well as ping sends and built-in Guac profile

4	allow, guac	none	universal	trusted vpn	any	any	any	oniz	10.99.8.8	any	apache guacamole pfig  ssh tel	any	Allow	none	11	2139	2023-07-31 15:47:04	2023-06-29 16:44:41	4
---	-------------	------	-----------	--	-----	-----	-----	--	---	-----	--	-----	---	------	--	------	---------------------	---------------------	---

Guac to Inbound:

Allows RDP SSH and VNC to specified servers

Also allows internal DNS access to DC's.

7	guc_broked	none	universal	img	10.99.8.8	any	any	trusted	192.168.126.125 192.168.134.2	any	ms-dp vch vnc	any	Allow	none	1	37366	2023-07-31 15:09:33	2023-06-30 14:40:47	2
8	guc_allowedns	none	universal	img	10.99.8.6	any	any	trusted	10.1.6.90 10.1.6.91	any	✓ dns	application-d...	Allow	none	1	0	-	-	-