TrustGate –Basic PortForwarding

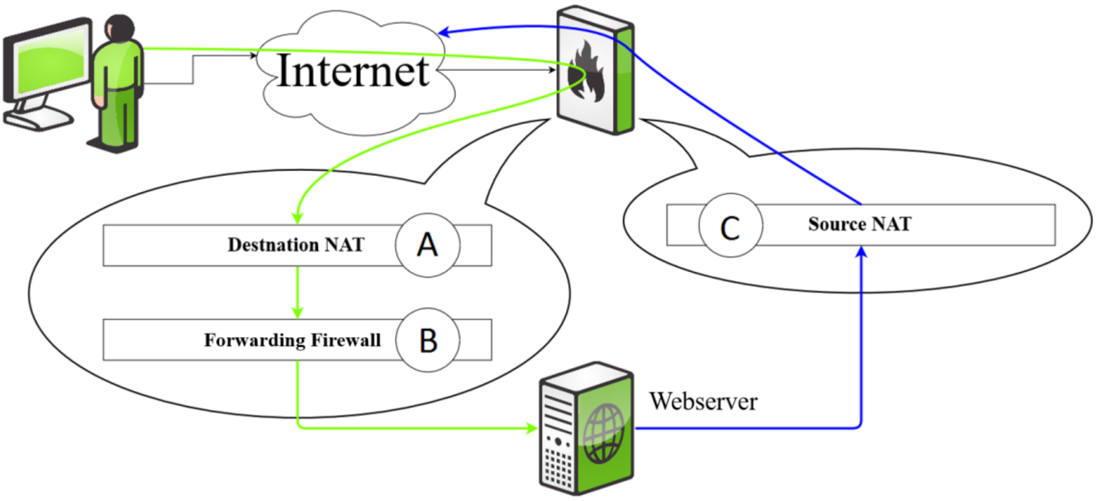
Prerequisites:
- Any TrustGate (TrustGate SoftClient not included)

A. Understanding forwarding.

a. When a packet is arriving at a TrustGate, the first list it goes through, is the Destination NAT. if your packet match any of the filter, it will apply to the actions set in that particular rule.

b. Afterwards, your packet will arrive at the Forwarding Firewall. Here, it will search through the filters to see if your packet is allowed (or blocked) to access the requested interfaces.

c. Source NAT is normally used when you are going from the inside (LAN / DMZ) to the outside WAN / VPN). It will look through the Source NAT filter, and if it matches any, it will apply to the actions given in that rule.



B. Setting up Destination NAT

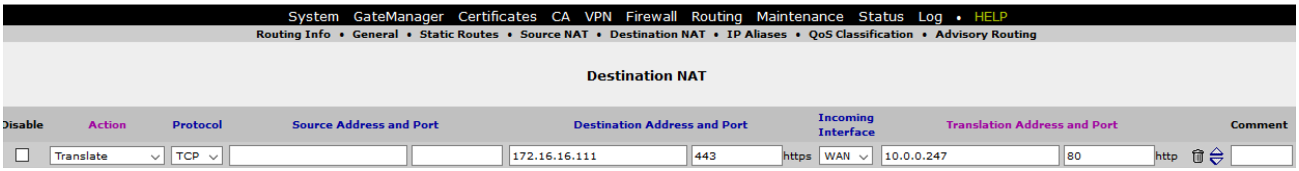
a. Log on to your TrustGate Management interface, go to "Routing" -> "Destination NAT".

b. The "Action" dropdown should be set to Translate. The Protocol dropdown should be set to the protocol that you want to use. (If you are trying to port forward a webserver this should be set to TCP). Blank means "any protocol".

c. The "Source Address and Port" should be set to the address that you want to gain access to the inside of your network. If left blank then everyone will gain access. (In This case we are setting up a webserver)

d. The "Destination Address and Port" is usually the WAN address of your TrustGate. This is where we are specifying what IP address and port should be applied for filtering this packet. If port is left blank then all ports will be translated to the "Translation port". Incoming interface is used to define on what interface this rule is applied to.

e. "Translation Address and port" is the device that you want to gain access to from the outside. In this case our Web server.


System GateManager Certificates CA VPN Firewall Routing Maintenance Status Log • HELP
Routing Info • General • Static Routes • Source NAT • Destination NAT • IP Aliases • QoS Classification • Advisory Routing

Destination NAT

Disable	Action	Protocol	Source Address and Port		Destination Address and Port		Incoming Interface	Translation Address and Port		Comment
☐	Translate	TCP			172.16.16.111	443 https	WAN	10.0.0.247	80 http	

C. Setting up Forwarding Firewall

a. When a package arrives at the Forwarding Firewall, the package has already been translated to the IP that was stated in “Destination NAT”.

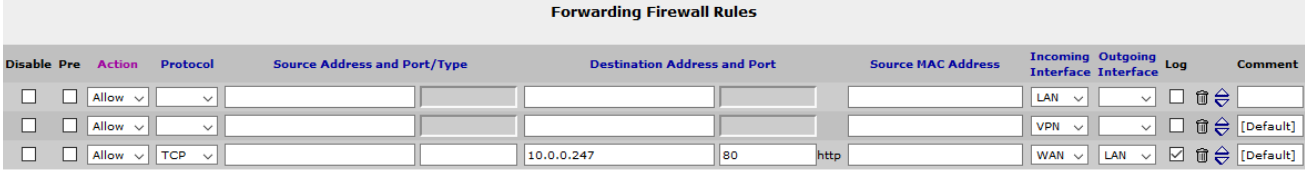
b. Action settings should be set to allow your packages to gain access to the internal network, and protocol should be set to the standard that fits your needs. Blank means “any protocol”.

c. “Source Address and port” should be set to the address that you want to allow access from, into your internal network. If set to blank, all addresses have access to the destination that you determine in the next field.

d. “Destination address and port” is the device that you want to gain access to from the outside. In this case our Web server.

e. “Source MAC” is used if you have only a specific device that must gain access to the destination address.

f. Incoming and Outgoing interface is used to determine from where and to this rule should be applied.



Forwarding Firewall Rules

Disable	Pre	Action	Protocol	Source Address and Port/Type		Destination Address and Port		Source MAC Address	Incoming Interface	Outgoing Interface	Log	Comment
□	□	Allow							LAN		□	
□	□	Allow							VPN		□	[Default]
□	□	Allow	TCP			10.0.0.247	80 http		WAN	LAN	☑	[Default]