Global Technology Associates, Inc.

Internet Firewall Developer since 1994

IP Pass Through

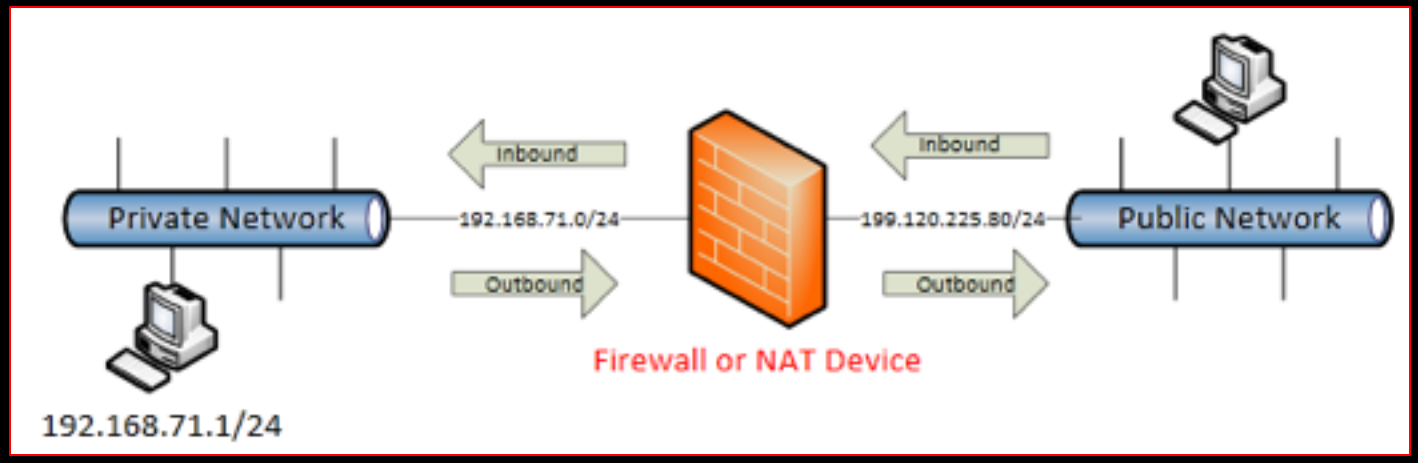
Removing Network Address Translation

Course #2221

Overview

- What is NAT?
- What is IP Pass Through?
- Why Use IP Pass Through?
- Configuring IP Pass Through
- IP Pass Through Examples

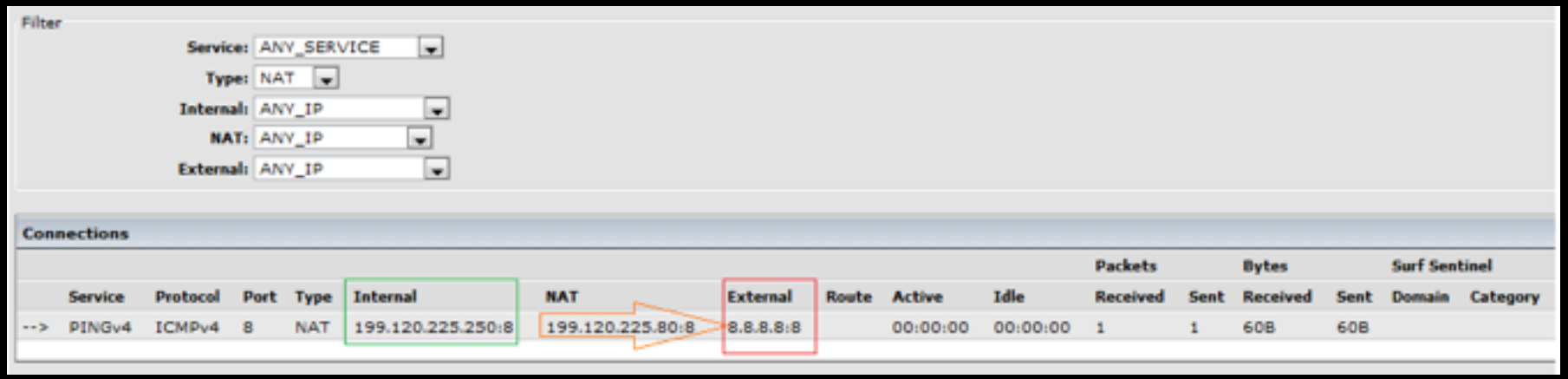
Network Address Translation



Network Address Translation (NAT) translates an IP address behind the firewall to the IP address of the external network interface, disguising the original IP address. Using NAT makes it possible to use a non-registered IP address within protected networks and PSNs, while still presenting a registered IP address to the external network (typically the Internet).

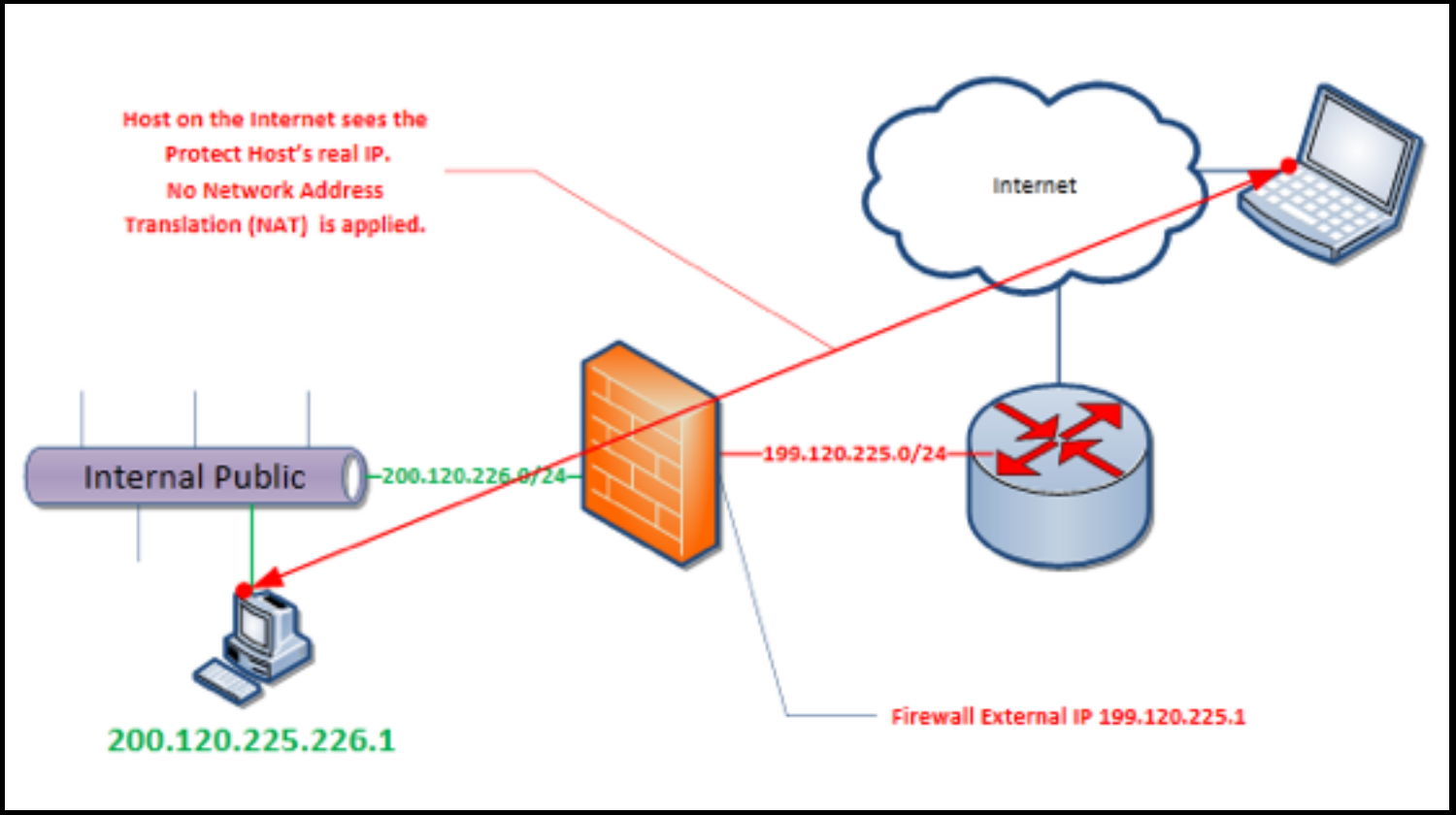
- **NAT is active by default on all GTA firewalls.**
- **NAT is applied to outbound packets from:**
  - A protected network to an external network
  - A protected network to a PSN
  - A PSN to an external network
  - A protected network to another protected network
- NAT can be used with both IPv6 and IPv4 Networks.

Active Connection Through Firewall With NAT



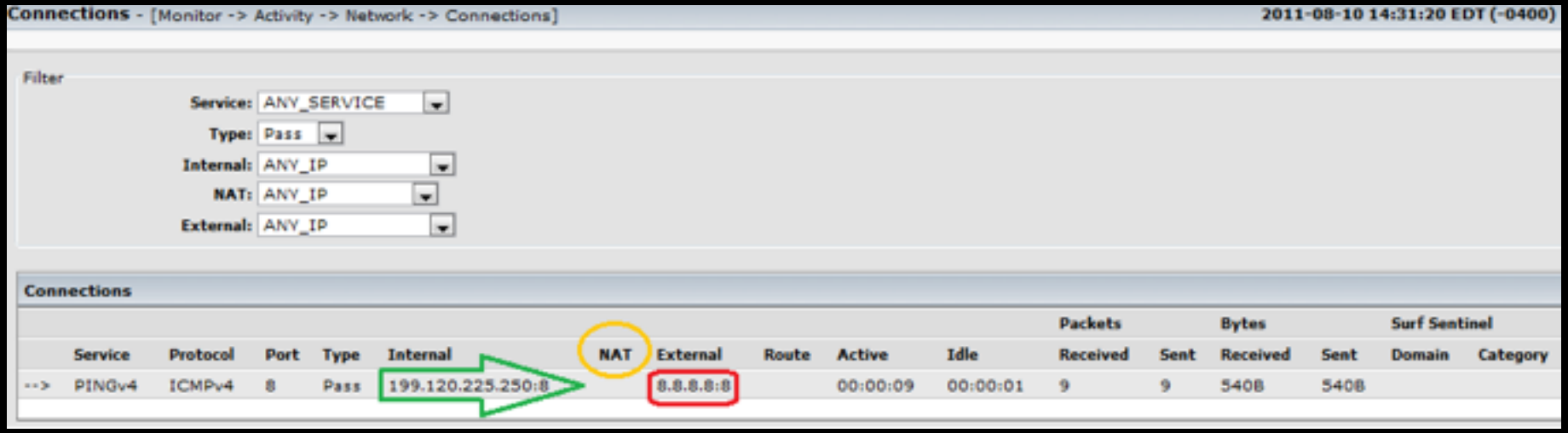
The NAT column shows an IP address that the internal host is translated to.

What is IP Pass Through?



IP Pass Through is simply no Network Address Translation or No NAT.

Active Connection Through the Firewall With IP Pass Through



No NAT entry in the active connection table.

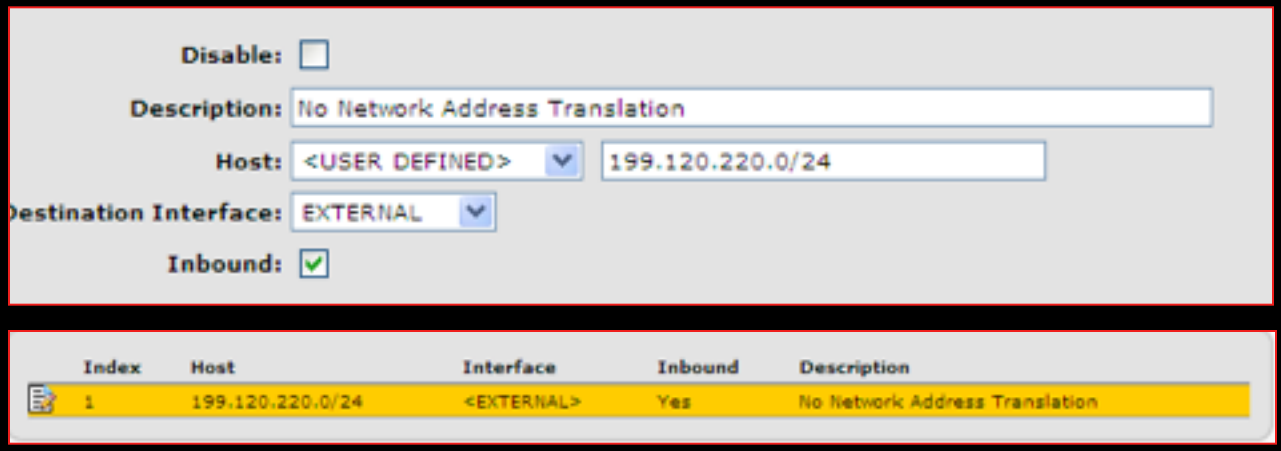
Why use IP Pass Through?

- Public IP Address behind the firewall needs NAT removed.
- Intranet firewall that does not require or need Network Address Translation.
- Application in use does not allow the use of NAT.
- Connections are from
  - From a Protected to PSN network and NAT is not required or needed.
  - Or from One Protected Network to another Protected Network.
  - Or from one PSN to Another PSN.

IP Pass Through

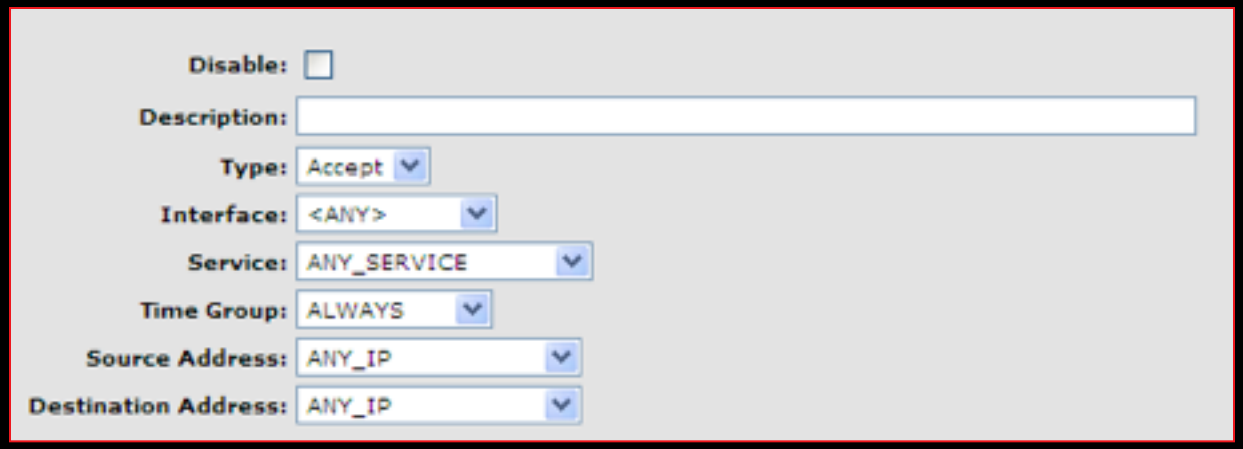
- **No Network Address translation**
  - NAT is removed ***exiting*** an interface.
  - Applied to single hosts or networks
- **Requirements**
  - Each interface is on a different logical subnet
  - If destination is the Internet a public IP address is needed.
  - In some cases a route will need to be added to a router pointing to the firewall as the gateway to the Pass Through network.
- **Configured in**
  - **[Configure -> Network -> Pass Through -> Hosts/Networks]– remove NAT**
  - **[Configure -> Security Policies -> Policy Editor -> Pass Through] – control access in and out.**
- **Conditions where you can define IP Pass Through (Internal host or network going outbound)**
  - Protected network/host to another Protected Network
  - Protected network/host to a PSN
  - Protected network/host to an External network
  - PSN network/host to another PSN
  - PSN network/host to an External Network

IP Pass Through



- Description – user defined
- Host –
  - Object
  - User Defined
- Interface – Interface the packets will exit and have NAT removed.
  - Selecting ANY will match all Interfaces.
- Inbound – check if inbound connections are allowed
  - No incoming packets are allowed if not checked.
  - Virtual cracks for services such as ftp will not be opened if inbound is not checked.

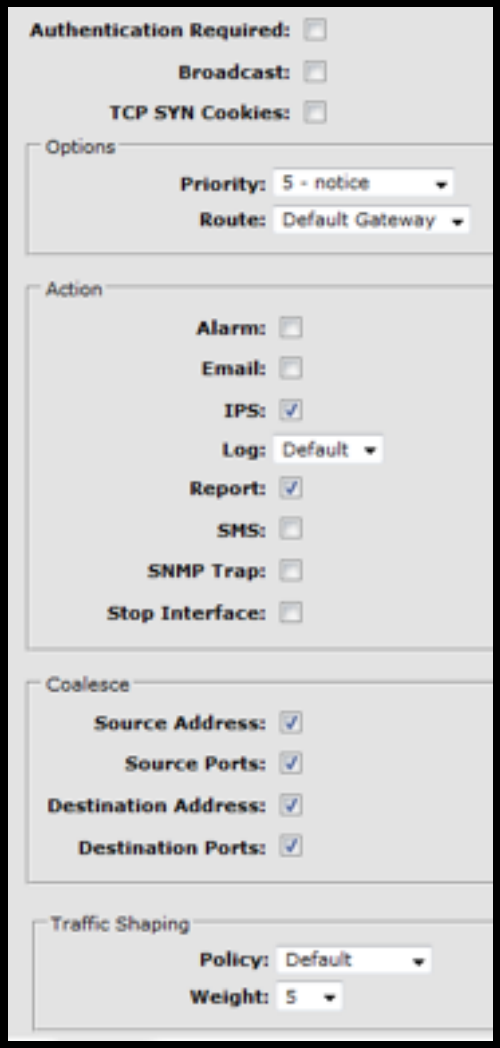
[Configure -> Security Policies -> Policy Editor -> Pass Through]



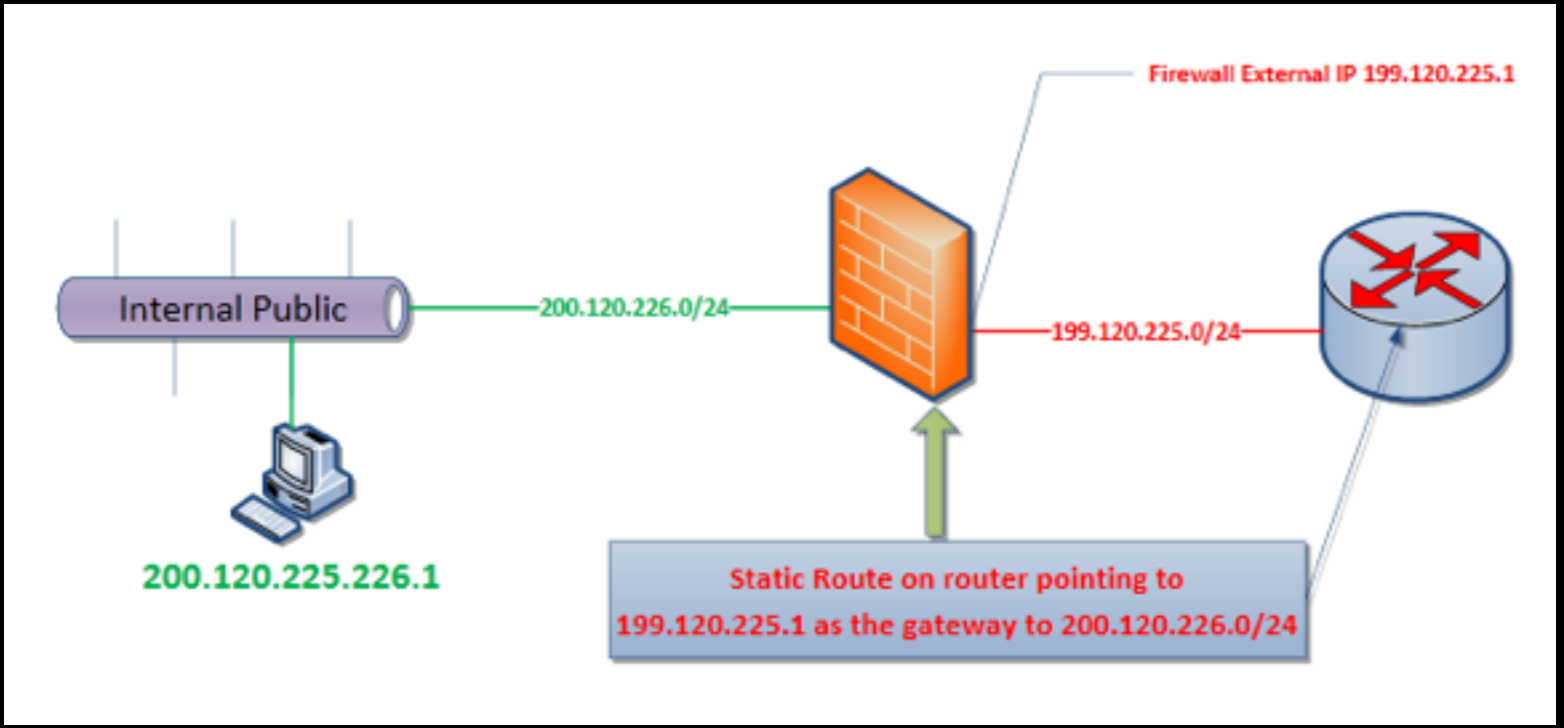
- When an IP Pass Through Host/Networks is defined
  - Inbound and Outbound access is controlled by IP Pass Through Policies
  - Policies need to be configure for the source and destination addresses.

Pass Through Policies Advanced

- Advanced options are same as most other policies.
- Depending type accept or deny different options will display.



Pass Through Protected or PSN to EXTERNAL

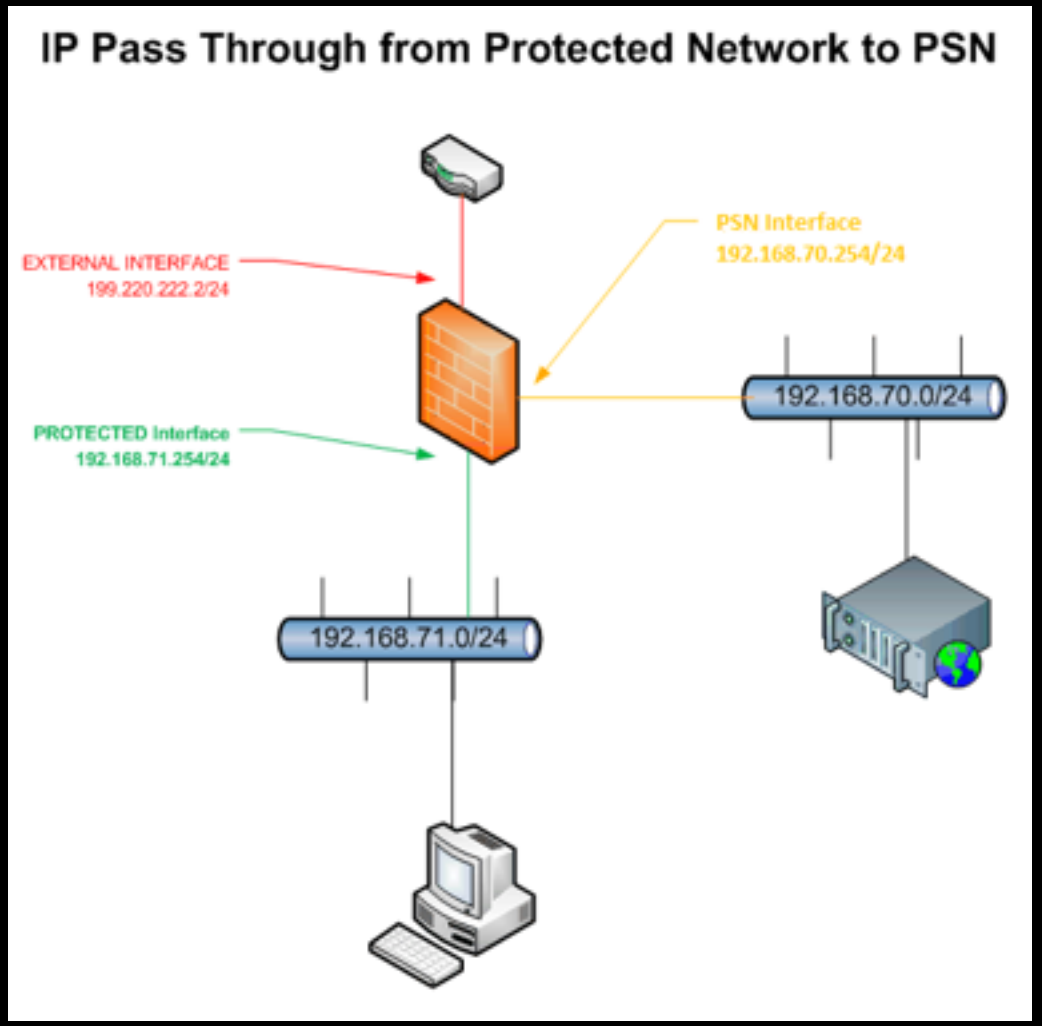


In example above the an internal host has NAT removed exiting the external interface.

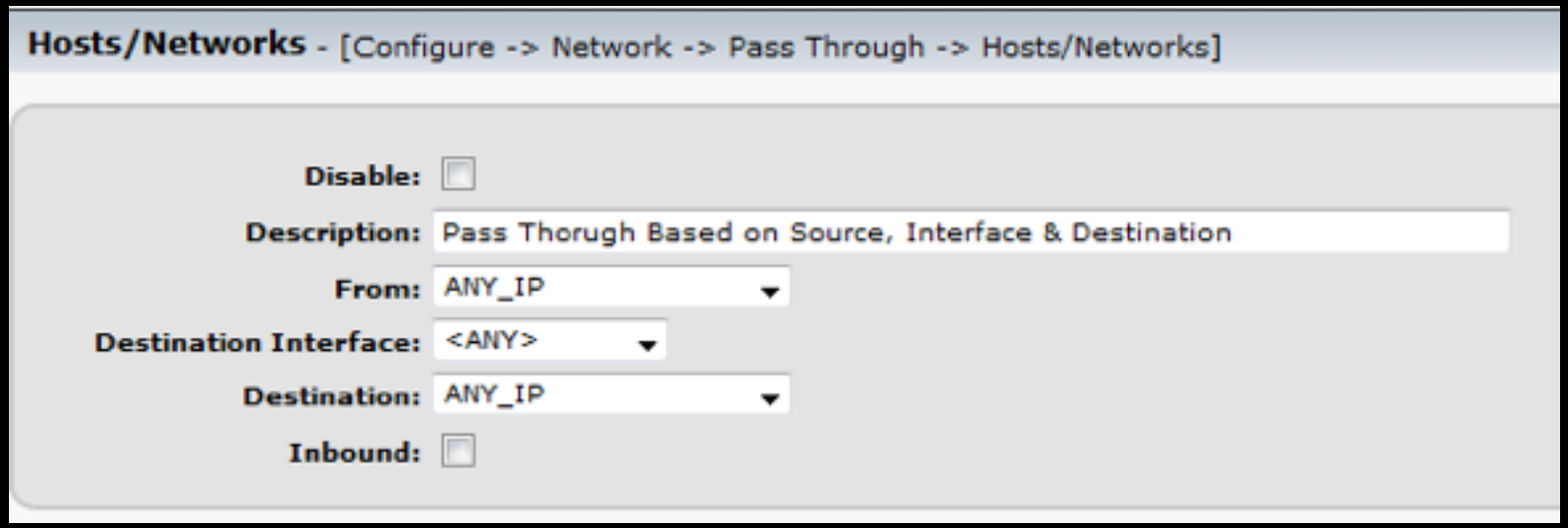
The route needs a route entry for the internal network.

Pass Through Protected to PSN

In the example to the left NAT is removed going to the PSN. While host is still NAT'ed to the External side.



Pass Through Based on Destination



Trouble Shooting & Pass Through Errors

- Defined using an External interface which is the Internet and using a private address
  - Results in loss of Internet Access
- Defined from an External network to an internal network.
  - IP Pass Through is always internal going out.
  - External is external to Protected and PSN networks.
  - PSN is external to a Protected network.
- NAT is still applied to the internal hosts.
  - Check that there are no stale connections. You may need to flush the active connections matching the IP Pass Through.
  - No host Networks defined for the Pass Through Networks.
- No Pass Through Security Policy to allow a connection displays the log message below -
  - Aug 10 14:30:06 pri=4 pol_type=PTP pol_action=block count=1 msg="Block PTP" rule=5 proto=icmpV4 src=199.120.225.250 srcport=8 dst=8.8.8.8 dstport=8 interface="PROTECTED-192" attribute="alarm,report"
- No routes in place for the network being passed through. A route is usually required on routers pointing to the interface of the firewall as the gateway to the internal network.

IP Pass Through vs. Bridge

- Pass Through each interface must be on a logically different network.
  - EXTERNAL – 199.120.225.1/25
  - Protected – 199.120.225.254/25

Logical Interfaces

Index	Name	Type	Zone	IP Address	NIC	Options	Description
1	EXTERNAL	Standard	External	199.120.225.1/25	eth1		External Interface
2	Protected	Standard	Protected	199.120.225.254/25	eth0		

- Bridge one network/IP addresses is shared on many interfaces
  - EXTERNAL – 199.120.225.1/24
    - Protected-Bridge – Use Same IP

Logical Interfaces

Index	Name	Type	Zone	IP Address	NIC	Options	Description
1	EXTERNAL Protected-Bridge	Bridge -----	External Protected	199.120.225.80/24 -----	eth2 eth0	-----	

If you require additional assistance or have additional questions please contact GTA Technical Support.

- Customer Email: support @gta.com
- Support Line Phone: 1.407.482.6925
- Normal Hours – 0830-1900 EST U.S.
- Free User Support – http://forum.gta.com