Global Technology Associates, Inc.

Internet Firewall Developer since 1994

# Routing Services 1

Gateway Failover

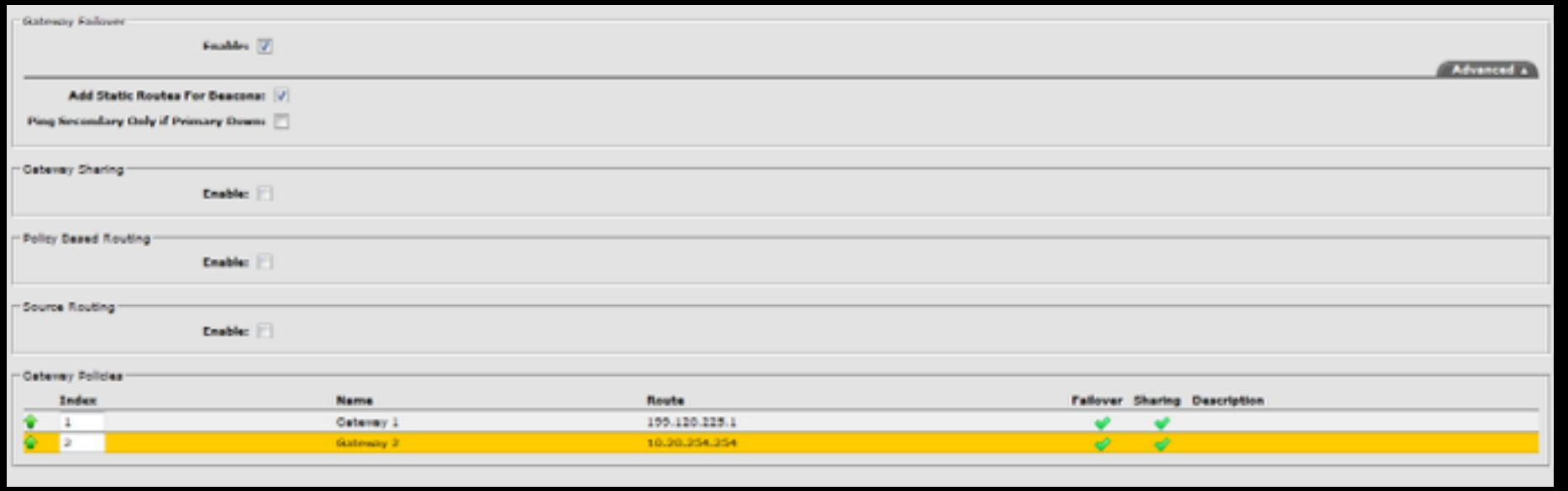
Policy Based Routes

Source Based Routes

Sharing

**Course # 2250**

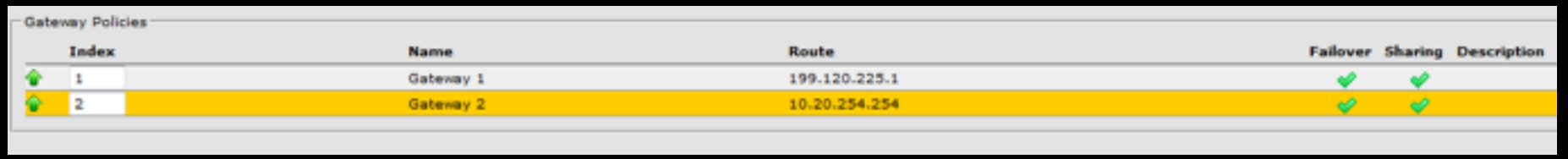
# Gateway Policies

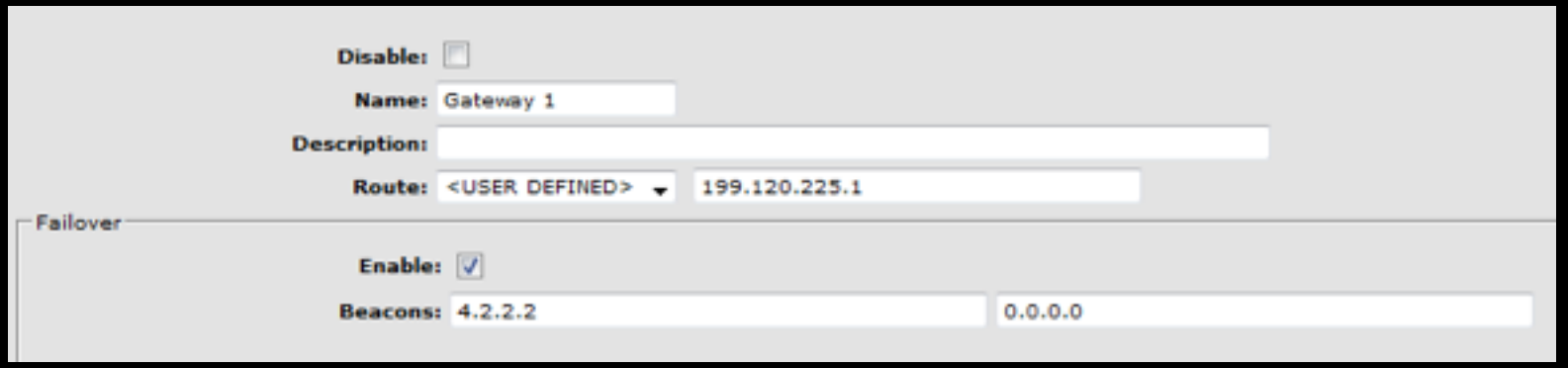



Gateway Policies consist of:

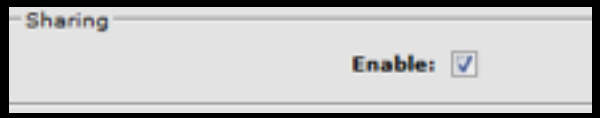
- Gateway Failover
- Gateway Sharing – Load balancing outbound
- Policy Based Routing - Outbound
- Source Based Routing - Inbound

# Gateways

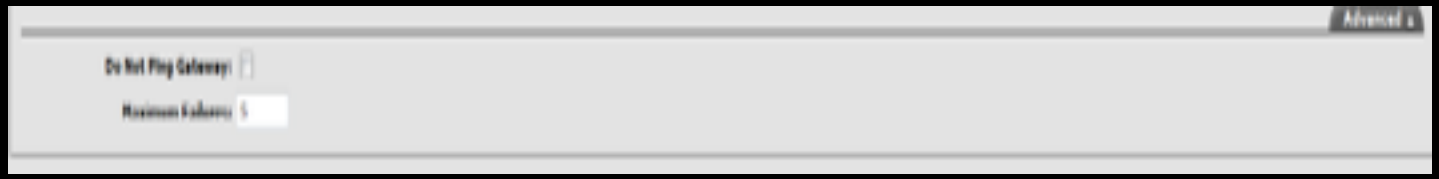



- Up to 20 gateways to the Internet can be configured.
- Number of gateways is NOT dependent on the number of firewall Interfaces.
- **Gateway**
  - Name – Used to reference in Security Policies.
  - Beacons – Used to ensure the path is patent for fail over
  - Sharing – Includes the interface in sharing when enabled.
  - Dynamic Gateways
    - Gateway learned via DHCP, PPP, PPPoE or PPTP
    - Route box will display the dynamic Interface name
    - Firewall will learn the dynamic route.

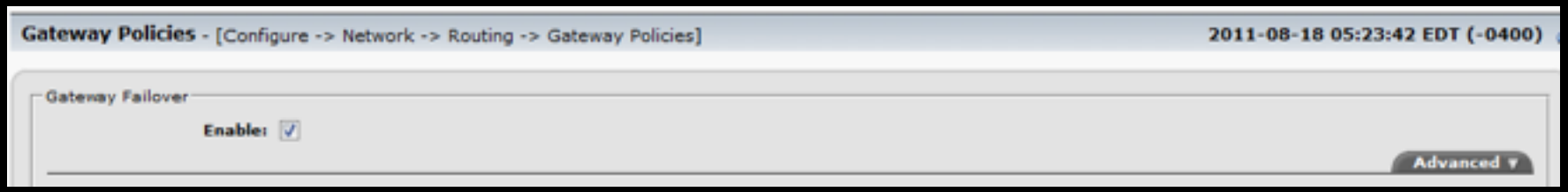


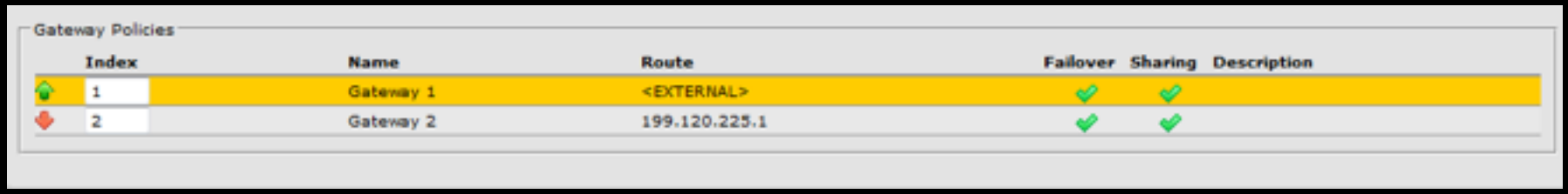
# Gateways Advanced



- Do not ping gateway – firewall will not use the gateway as a beacon.
- Maximum Failure –
  - number of failures to occur before gateway is considered down.
  - Firewall probes  (pings) beacons evey .5 seconds.

# Gateway Failover




- Allows the firewall to automatically fall over to redundant gateways and fall back. Ensures connectivity for local network.
- Requirements - Multiple routes to the Internet
- Gateway number 1 will become the firewall default route when Gateway failover is enabled.

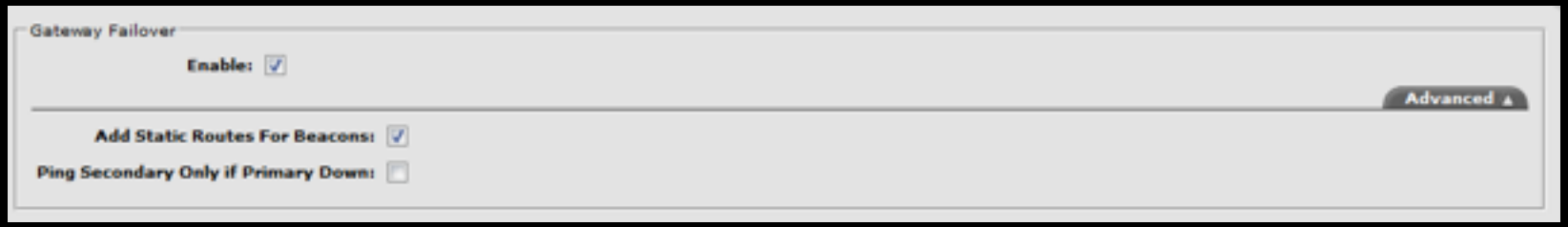
# Gateway Failover

- Beacons for fail over
- Failure of any beacon defined for a gateway results in a gateway failure condition.
- Beacons are checked every .5 seconds
- Fail back is automatic.

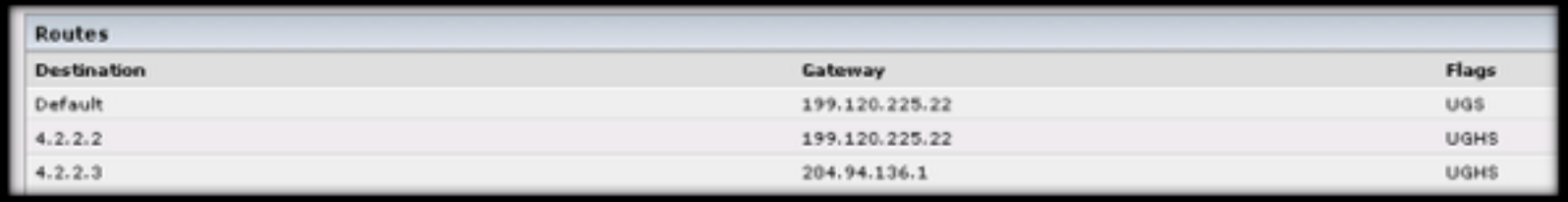
# Choosing Beacons

- Gateway is always consider a beacon and does not need to be added as a beacon.
- Best method to choose a beacon for primary gateway is to run a traceroute outbound from the firewall interface and choose the first two hops past the gateway.
- Secondary Interface beacons are little harder.  Usually run an inbound traceroute from remote site to secondary interface. Choosing the last two before the gateway.

# Gateway Failover Advanced Options




- Add Static Routes for Beacons address to the routing table

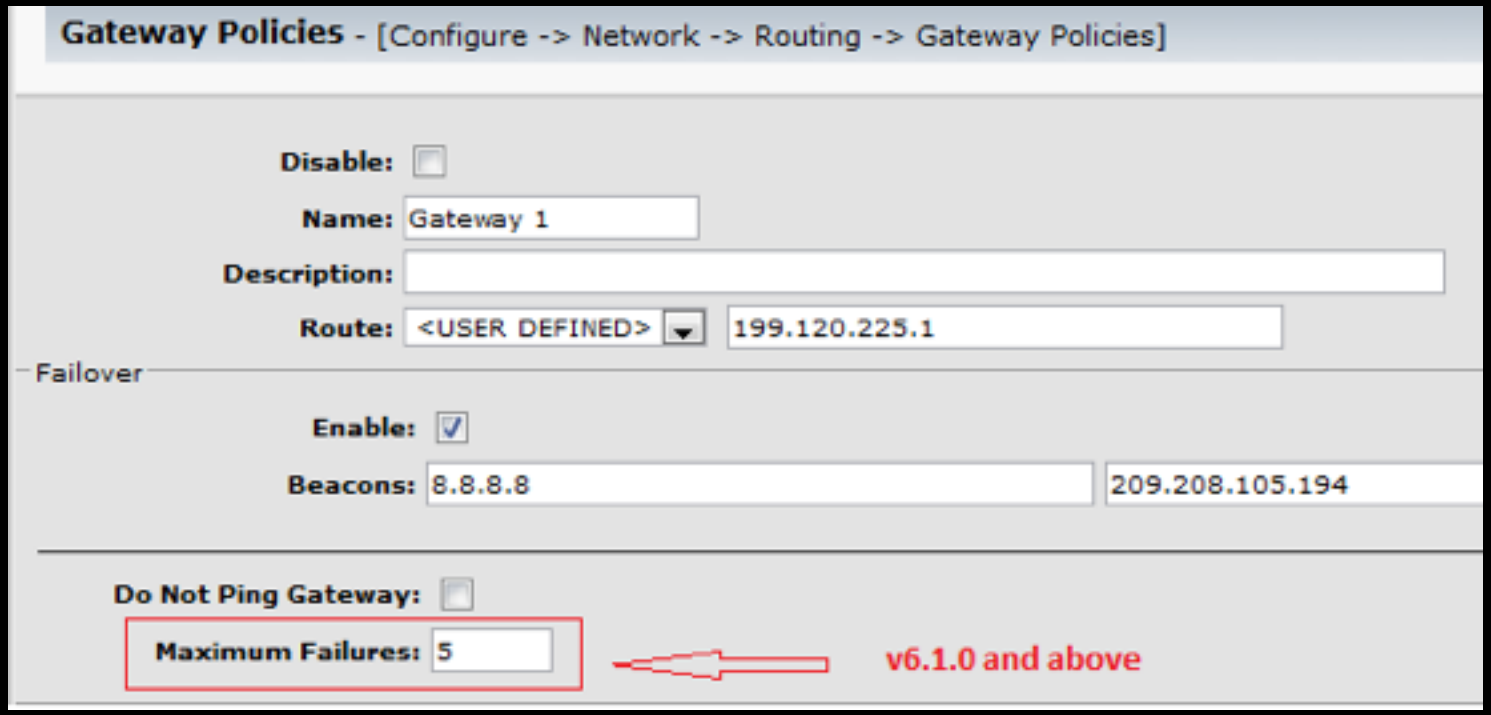


Routes

| Destination | Gateway | Flags |
|---|---|---|
| Default | 199.120.225.22 | UGS |
| 4.2.2.2 | 199.120.225.22 | UGHS |
| 4.2.2.3 | 204.94.136.1 | UGHS |

- Used only in cases where your secondary gateway is on demand.

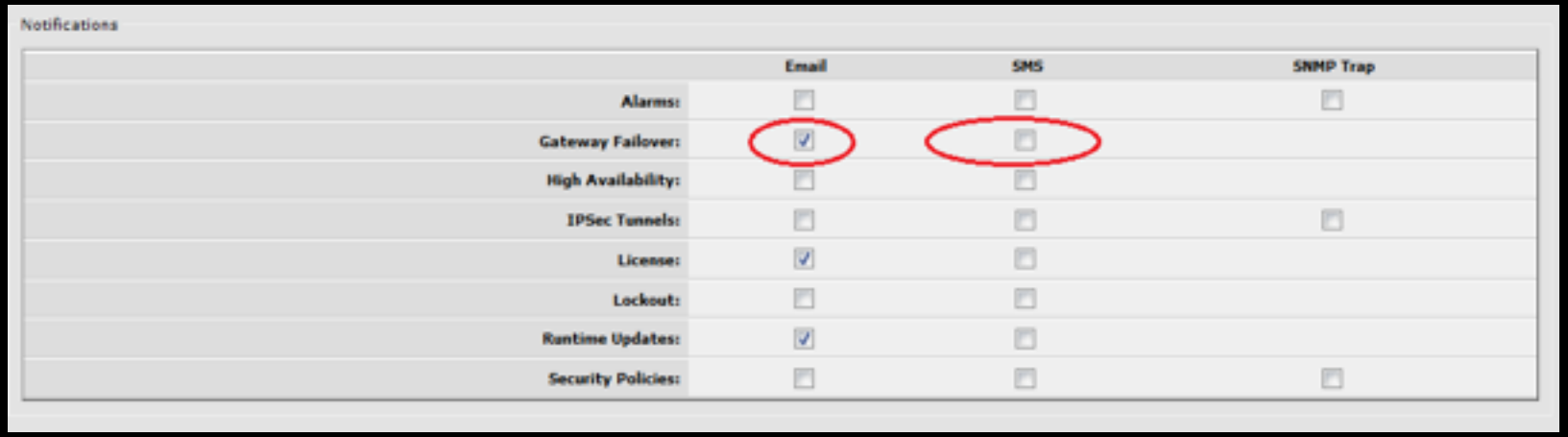
# Gateway Failover Advanced Options




Do Not Ping Gateway when enabled the firewall will not use the firewalls own gateway as a beacon. Used when local router or modem does not respond to pings.

Maximum Failures: Sets the number of dropped probes responses before gateway is determined to be down.

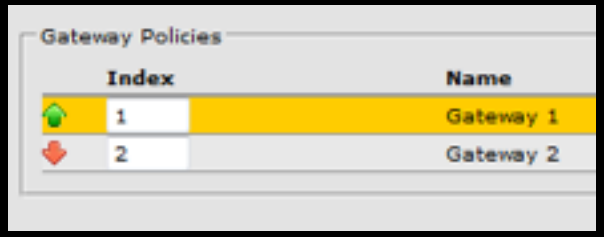
# Notification




- Gateway down Alerts is configured in [Configure -> System -> Notifications]
- Sends via email or SMS

# Trouble Shooting Gateway Failover

- Gateway does not respond to pings.
  - Use the Advanced option to not ping gateway.
- Gateway Status Indicator is red
  - Indicates the route is down and a possible problem.
  - Check gateway is up and responding.
  - Check all beacons for gateway.



# Gateway Sharing

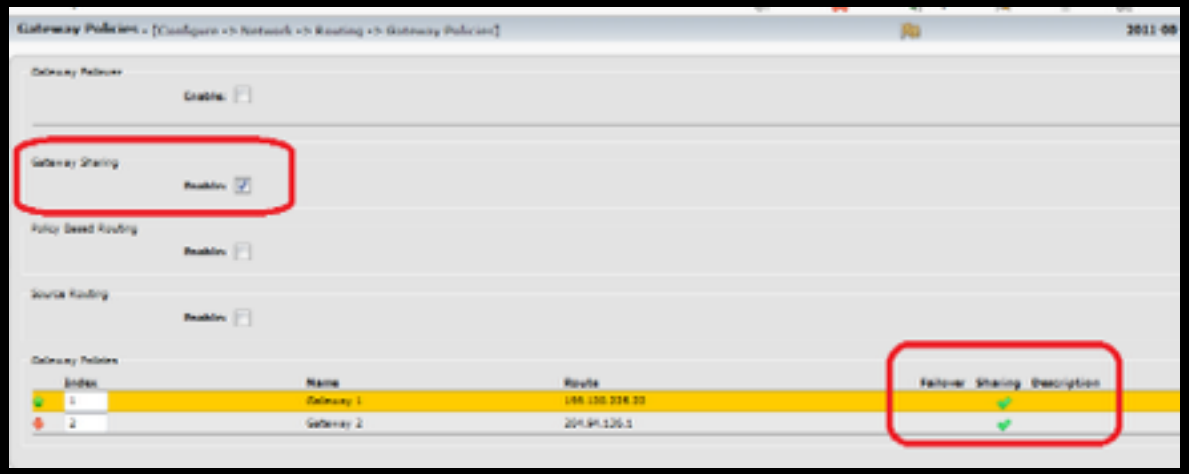
- Shares connections over more than one route. Allows full utilizations of Internet connections.
- Uses a round robin approach to sending packets.
- Requirements -
  - 3.7.0 or later.
  - Two or more connections to the Internet.
  - Knowledge of TCP/IP and routing.
  - Basic understanding of filtering concepts.
- 3 Simple Steps to configure
  - Configure your alternate gateway under Gateway Policies -> Gateways
  - Enable Gateway Sharing
  - Create/configure an Outbound Policy referencing the route "**Sharing**".

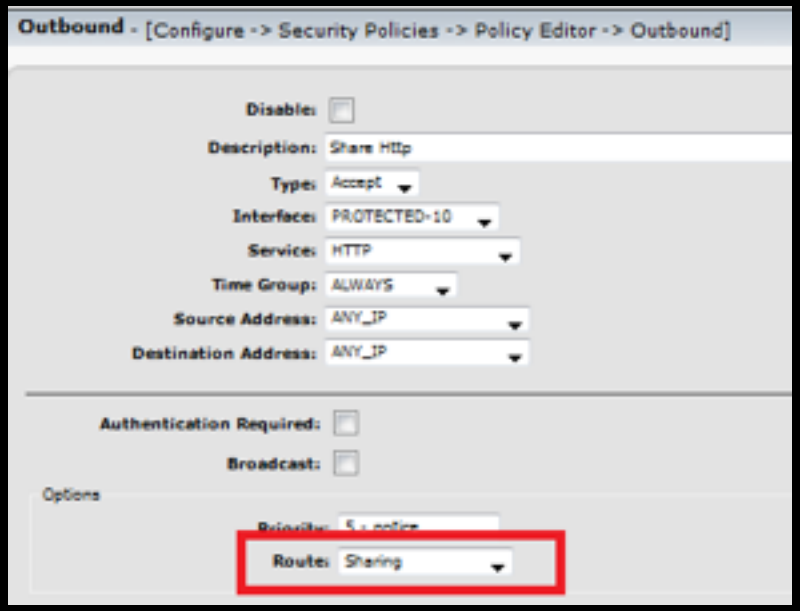
# Why Use Sharing or Not Use Sharing?

- Load Balance connections over multiple lines.
  - Recommend being specific on the connections shared.  Do not share all protocols.
  - Example Share http connections.
- Do not share VPN connections through a firewall.  VPN's use UDP 500/4500 and ESP.  This could break a VPN.

# Sharing Configuration

- Enable Sharing
- Configure each gateway sharing will be used on.

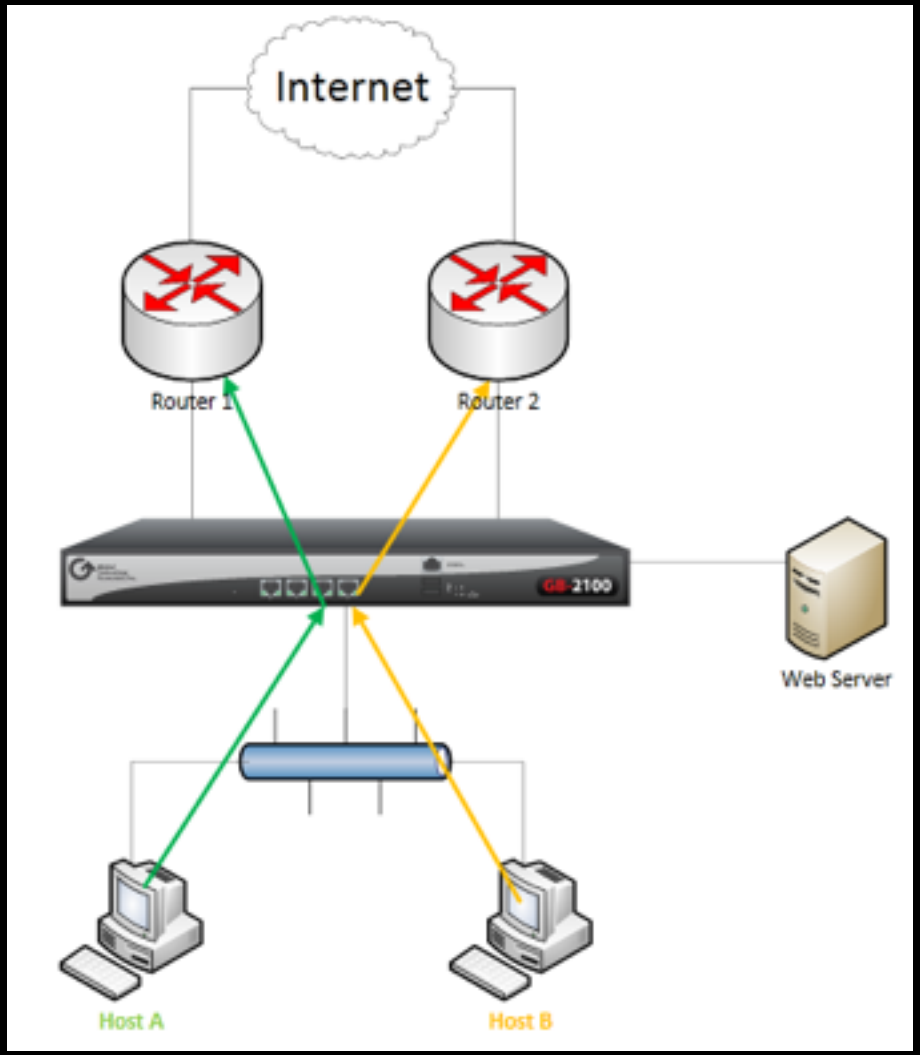


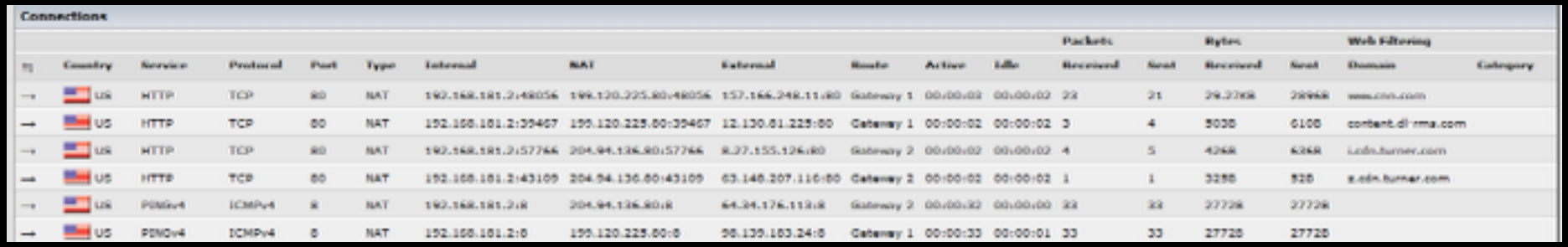

- Configure an outbound policy to use sharing in the advanced section of the policy.

# Sharing Example

- An http request from Host A is processed and sent via router 1.
- Next request is from Host B and is sent via Router 2.
- Subsequent request from A or B will round robin through each defined gateway.



# Monitor Display of Sharing

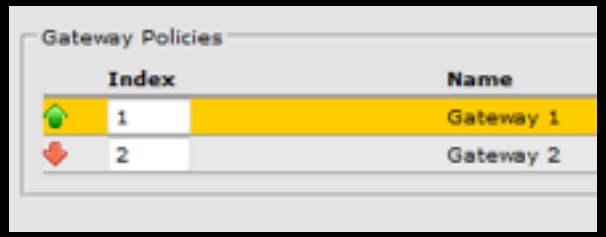


Connections

| | | | | | | | | | | | | Packets | | Bytes | | Web Filtering | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Country | Service | Protocol | Port | Type | Internal | NAT | External | Route | Active | Idle | Received | Sent | Received | Sent | Domain | Category |
| → | US | HTTP | TCP | 80 | NAT | 192.168.181.2:48056 | 199.120.225.80:48056 | 157.166.248.11:80 | Gateway 1 | 00:00:03 | 00:00:02 | 22 | 21 | 29.2KB | 28KB | www.cnn.com | |
| → | US | HTTP | TCP | 80 | NAT | 192.168.181.2:39467 | 199.120.225.80:39467 | 12.130.61.225:80 | Gateway 1 | 00:00:01 | 00:00:02 | 3 | 4 | 5038 | 6108 | content.dl-rma.com | |
| → | US | HTTP | TCP | 80 | NAT | 192.168.181.2:57766 | 204.94.136.80:57766 | 8.27.155.126:80 | Gateway 2 | 00:00:02 | 00:00:02 | 4 | 5 | 4268 | 4268 | i.cdn.turner.com | |
| → | US | HTTP | TCP | 80 | NAT | 192.168.181.2:43109 | 204.94.136.80:43109 | 63.148.207.116:80 | Gateway 2 | 00:00:02 | 00:00:02 | 1 | 1 | 328 | 328 | s.cdn.turner.com | |
| → | US | PING/v4 | ICMPv4 | 8 | NAT | 192.168.181.2:8 | 204.94.136.80:8 | 64.34.176.113:8 | Gateway 2 | 00:00:32 | 00:00:00 | 33 | 33 | 27720 | 27720 | | |
| → | US | PING/v4 | ICMPv4 | 8 | NAT | 192.168.181.2:8 | 199.120.225.80:8 | 50.135.183.24:8 | Gateway 1 | 00:00:33 | 00:00:01 | 33 | 33 | 27720 | 27720 | | |

# Trouble Shooting Sharing

- Confirm all gateways are up
  - Indicates the route is down and a possible problem.
  - Check gateway is up and responding.
  - Check all beacons for gateway.




- Confirm the gateways are correctly configured for sharing.
- Check the outbound policy with sharing enabled is being matched by the connection.
- Some web sites will fail with gateway sharing. Usually these web sites require additional connections be from the same address –
  - Example: https://secure.insightfinancialcu.com/scripts/ibank.dll
  - Work Around –
    - Description: # Do not share connection

    Type: Accept Interface: ANY protocol: TCP Route: Gateway_1 From: <ANY_IP> to 205.245.63.88 Port: 443

# Policy Based Routing

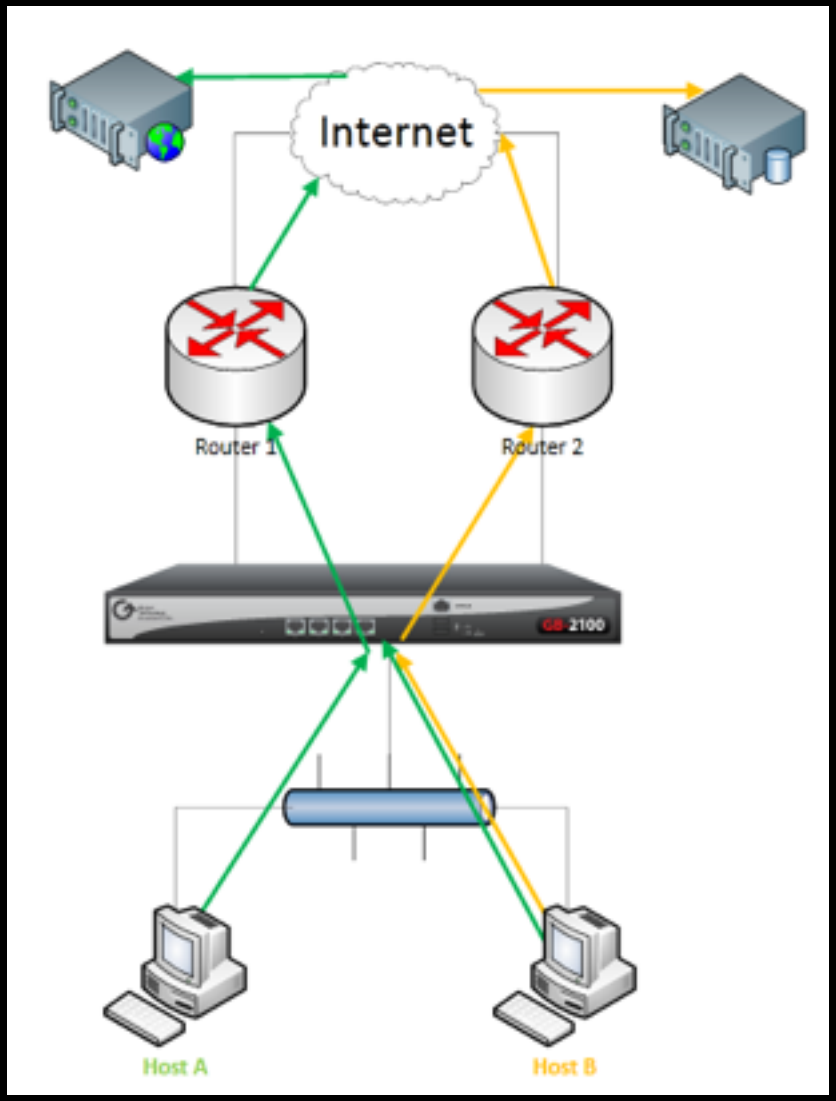
- Allows the administrator to specify alternate gateways based on:
  - Source IP/Subnet
  - Destination IP/Subnet
  - Protocol
  - Protocol and port number
- 3 Simple Steps to configure
  - Configure your alternate gateway under Gateway Policies -> Gateways
  - Enable the Policy Based Routing
  - Create/configure an Outbound filter referencing alternate gateway.
- Requirements:
  - 3.7.0 or later.
  - Two or more connections to connections to the Internet.
  - Knowledge of TCP/IP and routing.
  - Basic understanding of filtering concepts.

# Why Use Policy Based Routing?

- Force specific traffic to use a certain route. For example – customer has a T1 and a cable modem. Primary route is the T1. Secondary route is the cable modem. Force all http traffic through the cable modem.
- Dedicate one internet connection for specific traffic. For example connections to remote database.

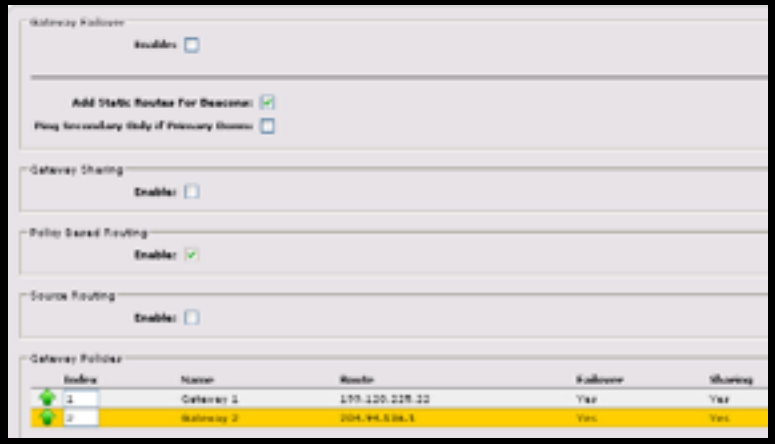
# Policy Based Route Example

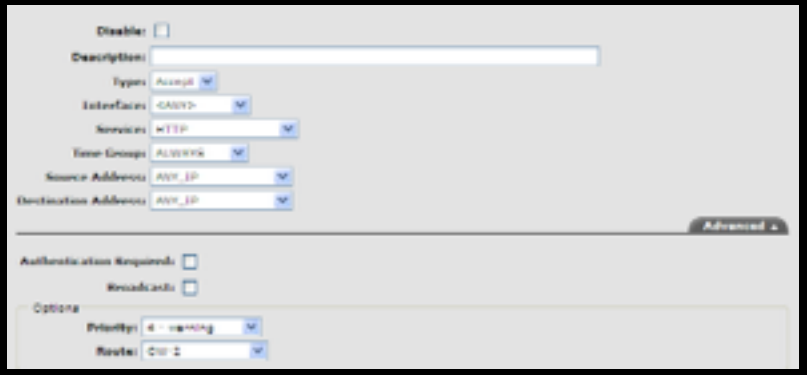
- In policy based to the right. All Web Connections (Green) go via Router 1.
- All connections to the remote database are via Router 2.



# Policy Based Routing

- Enable Policy based routing
- Configure the gateways to use
- Create a Security Policy using the selected gateway.



# Policy Based Route Connection

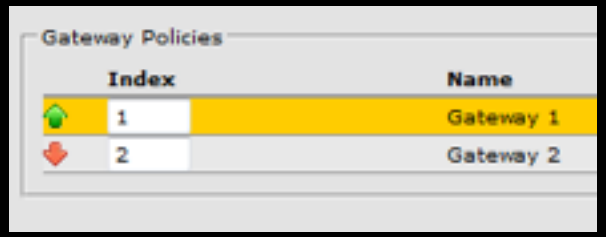
Connections

| | Protocol | Internal | NAT | External | Route | Active | Idle | Packets Received | Packets Sent | Bytes Received | Bytes Sent |
|---|---|---|---|---|---|---|---|---|---|---|---|
| --> | TCP | 10.10.1.163:3736 | 204.94.136.201:3736 | 209.85.165.99:80 | Gateway 2 | 00:00:10 | 00:00:10 | 2 | 1 | 207 | 40 |
| --> | TCP | 10.10.1.163:3737 | 204.94.136.201:3737 | 209.85.165.99:80 | Gateway 2 | 00:00:10 | 00:00:10 | 3 | 4 | 251 | 960 |
| --> | ICMP | 10.10.1.79:26368 | VPN | 192.168.172.1:26368 | | 00:00:09 | 00:00:09 | 0 | 1 | 0 | 104 |
| --> | TCP | 10.10.1.163:3738 | 199.120.225.81:3738 | 24.50.20.221:443 | | 00:00:07 | 00:00:06 | 11 | 9 | 2600 | 1200 |

- All http connections are via Gateway 2

# Trouble Shooting Policy Based Routing

- Confirm all gateways are up
  - Indicates the route is down and a possible problem.
  - Check gateway is up and responding.
  - Check all beacons for gateway.




- Check the outbound policy with sharing enabled is being matched by the connection.
- Order is important – check that the policy with the Route enabled is being matched.

# Source Based Routing

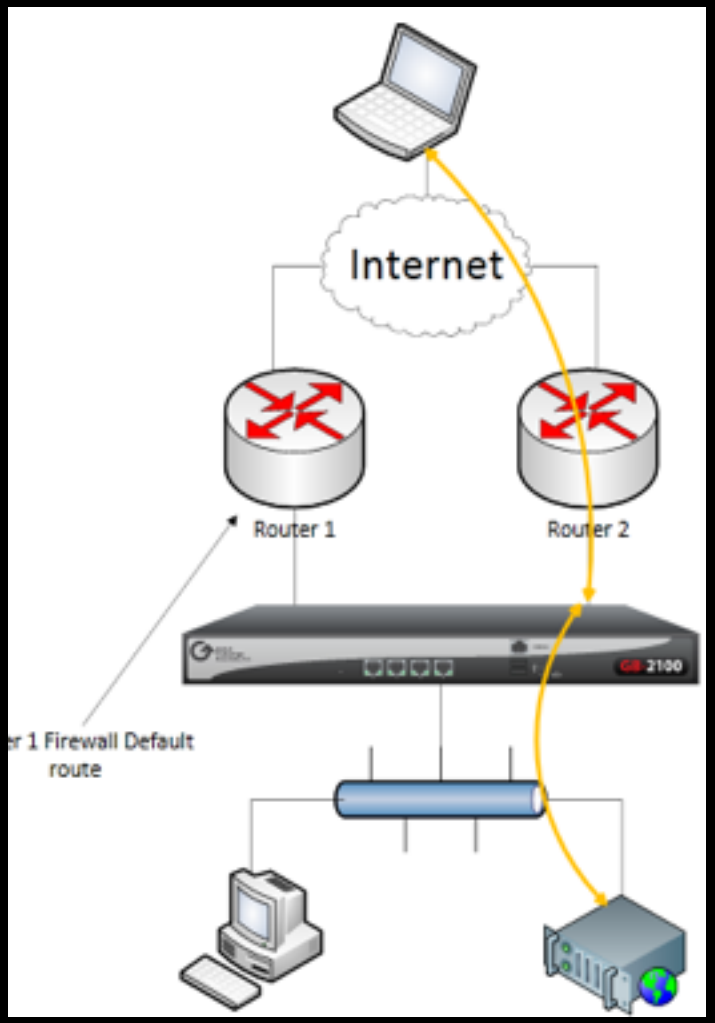
- Packet arrives on an interface  from a router.  The response packets follow the same path.
- Global option
- Source based routing does not apply to services on the firewall
  - Service on firewall
    - ICMP responses by firewall
    - Email Proxy
    - DNS server
- Requirements
  - 3.7.0 or later.
  - Two or more connections to the Internet.
  - Knowledge of TCP/IP and routing.
- Steps
  - Enable Source based routing under Routing -> Gateway Policies.

# Why Use Source Routing?

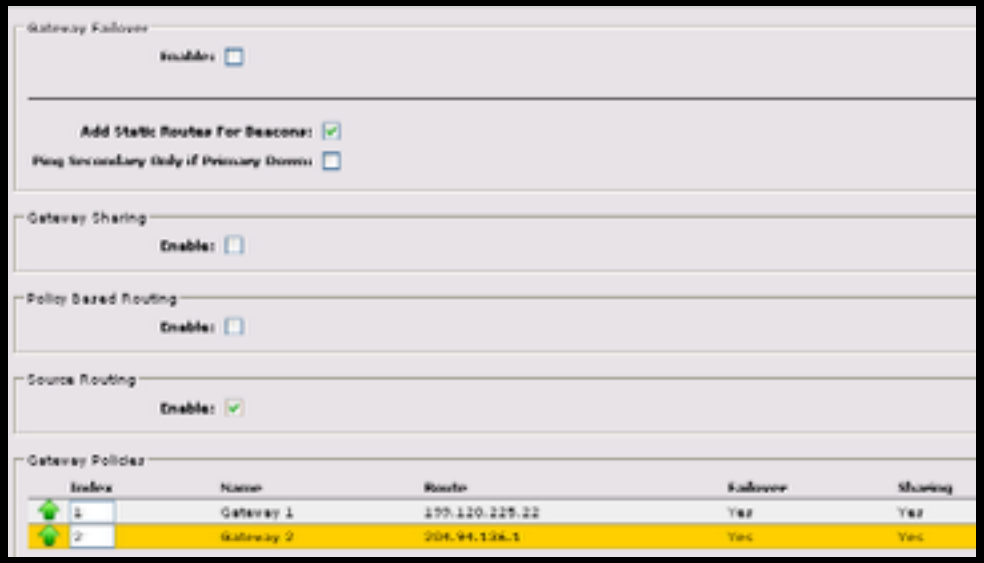
- Allows one to fully utilize multiple inbound Internet connections from different providers.
- Redundancy to servers.
- Transition to a new Internet connection.
  - Configure two up and functional connections
  - Web server and email server DNS changes are allowed time to propagate while both connections are up.

# Source Based Routing Example

- Packet for the web server arrives via secondary gateway inbound.
- Firewall keeps track of the MAC address of the local router and routes response back via gateway.

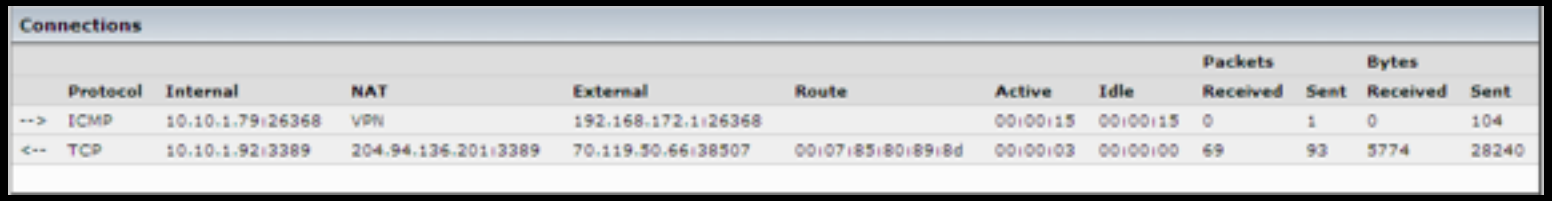


# Sourced based Routing




- Enable Sourced based routing
- Configure the gateways to use

# Source Based Route Connections



Connections

| | Protocol | Internal | NAT | External | Route | Active | Idle | Packets Received | Packets Sent | Bytes Received | Bytes Sent |
|---|---|---|---|---|---|---|---|---|---|---|---|
| --> | ICMP | 10.10.1.79:26368 | VPN | 192.168.172.1:26368 | | 00:00:15 | 00:00:15 | 0 | 1 | 0 | 104 |
| <-- | TCP | 10.10.1.92:3389 | 204.94.136.201:3389 | 70.119.50.66:38507 | 00:07:85:80:89:8d | 00:00:03 | 00:00:00 | 69 | 93 | 5774 | 28240 |

- Connection will display the MAC address of the router/gateway the packet came through.
- Return/response packets will follow the same path.

# Trouble Shooting Source Based Routing

- Test all gateways to ensure there is no failure along either path.
- Not supported for services – such as Mail Sentinel, VPN's, DNS server, etc..
- Check in the active connections table that the packets are using the correct gateway.
- Test the route to ensure there is no failure along its path.

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

# References


- GTA Online Documentation - http://www.gta.com/support/documents