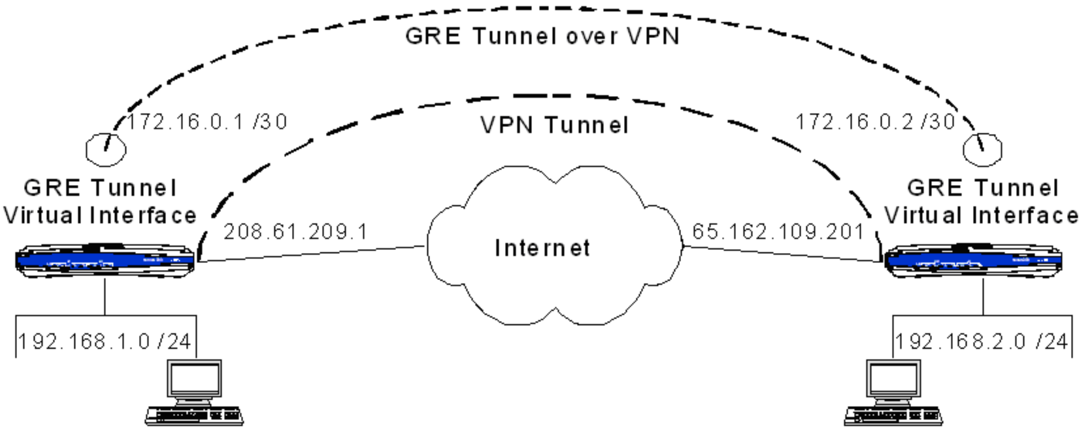
March 2008

Quick Configuration Guide
Configuring a GRE over IPSEC VPN Tunnel in AOS

Configuring a GRE over IPSEC VPN Tunnel in AOS



Introduction

To reduce the cost of point-to-point connections, the industry is moving away from dedicated circuits and towards IPSEC Virtual Private Network (VPN) tunnels. The problems with a standard VPN tunnel are that (1) all traffic that needs to traverse it must be specified in the configuration, (2) discontinuous subnets require separate tunnels, (3) it does not count as a routable interface, and (4) routing protocols cannot operate across it.

The best solution to simulate a dedicated point-to-point connection is a Generic Routing Encapsulation (GRE) tunnel. This kind of tunnel (1) by default has no limitations on the traffic that traverses it, (2) can route multiple subnets without multiple tunnels, (3) counts as a routable interface, and (4) can have routing protocols operate across it. However, the problem with GRE tunnels is that they are not secure.

The ultimate solution is to merge the two processes by protecting the GRE tunnel with a VPN tunnel. This solution would allow the GRE tunnel traffic to traverse the VPN tunnel, and all traffic limitations would take place in the GRE tunnel instead of the VPN tunnel. It also has the added benefit of creating a single IPSEC association regardless of how the GRE tunnel is utilized.

Hardware/Software Requirements

- Unit must be running at least AOS 9.1.
- Unit must be running the Enhanced Firmware Package (EFP).

Overview

To create a GRE over IPSEC VPN tunnel in AOS, the following will need to be configured:

1) VPN tunnel must be configured using the GRE tunnel endpoints as the selectors.
2) GRE tunnel must be configured.
3) Firewall must be setup on the GRE tunnel, if the firewall is running on the unit.
4) Routing settings must be configured to direct the desired traffic across the tunnel.

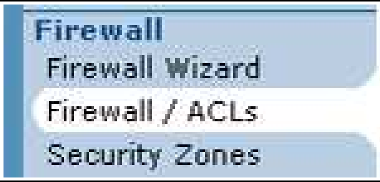
VPN Tunnel Configuration

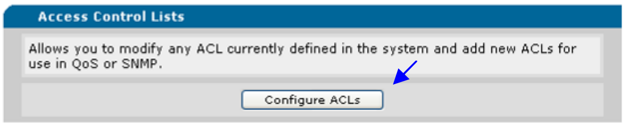
The first layer that must be configured is the VPN tunnel the GRE tunnel will ride above. This tunnel is configured identically to any other VPN tunnel in AOS except for the selector statement. This guide will not go into the overall configuration steps of a VPN tunnel since they are covered extensively in KB article #1973. This guide will instead center on the selector statement, which is the only difference from a traditional VPN.

The VPN tunnel selectors will consist of the endpoints of the GRE tunnel. Whatever kind of traffic traverses the GRE tunnel, after the GRE encapsulation it all looks like a GRE packet with a source address of the router and a destination address of the GRE peer. The selectors would have to reflect this GRE tunnel traffic. In the command line, it would look similar to the following:

```
ip access-list extended VPN-Selectors
  permit gre host <GRE Source IP Address> host <GRE Dest IP Address>
```

In the web interface, the selectors from an already built tunnel can be changed in the following manner:

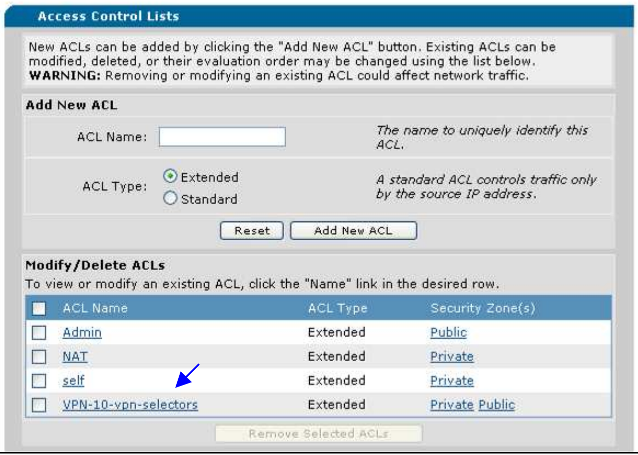
 Firewall Firewall Wizard Firewall / ACLs Security Zones	Browse to ‘Firewall / ACLs’. **** This may be called ‘General Firewall’ in some firmware revisions.*



Access Control Lists

Allows you to modify any ACL currently defined in the system and add new ACLs for use in QoS or SNMP.

Select ‘Configure ACLs’.



Access Control Lists

New ACLs can be added by clicking the "Add New ACL" button. Existing ACLs can be modified, deleted, or their evaluation order may be changed using the list below.
WARNING: Removing or modifying an existing ACL could affect network traffic.

Add New ACL

ACL Name: *The name to uniquely identify this ACL.*

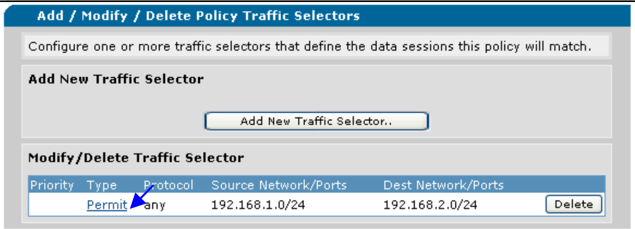
ACL Type: ● Extended ○ Standard *A standard ACL controls traffic only by the source IP address.*

Modify/Delete ACLs

To view or modify an existing ACL, click the "Name" link in the desired row.

□	ACL Name	ACL Type	Security Zone(s)
□	Admin	Extended	Public
□	NAT	Extended	Private
□	self	Extended	Private
□	VPN-10-vpn-selectors	Extended	Private Public

Configure the access-list that references the VPN in question.



Add / Modify / Delete Policy Traffic Selectors

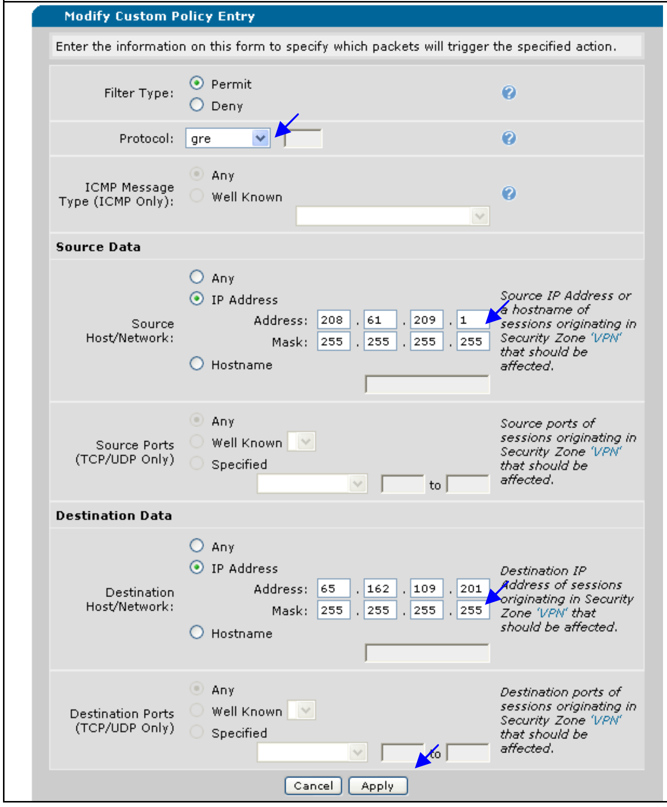
Configure one or more traffic selectors that define the data sessions this policy will match.

Add New Traffic Selector

Modify/Delete Traffic Selector

Priority	Type	Protocol	Source Network/Ports	Dest Network/Ports	
	Permit	any	192.168.1.0/24	192.168.2.0/24	Delete

Select the ‘Permit’ link to change the VPN selectors.



Modify Custom Policy Entry

Enter the information on this form to specify which packets will trigger the specified action.

Filter Type: ● Permit ○ Deny

Protocol: gre

ICMP Message Type (ICMP Only): ● Any ○ Well Known

Source Data

Source Host/Network: ○ Any ● IP Address
Address: 208 . 61 . 209 . 1
Mask: 255 . 255 . 255 . 255
○ Hostname
Source IP Address or a hostname of sessions originating in Security Zone 'VPN' that should be affected.

Source Ports (TCP/UDP Only): ● Any ○ Well Known ○ Specified ... to ...
Source ports of sessions originating in Security Zone 'VPN' that should be affected.

Destination Data

Destination Host/Network: ○ Any ● IP Address
Address: 65 . 162 . 109 . 201
Mask: 255 . 255 . 255 . 255
○ Hostname
Destination IP Address of sessions originating in Security Zone 'VPN' that should be affected.

Destination Ports (TCP/UDP Only): ● Any ○ Well Known ○ Specified ... to ...
Destination ports of sessions originating in Security Zone 'VPN' that should be affected.

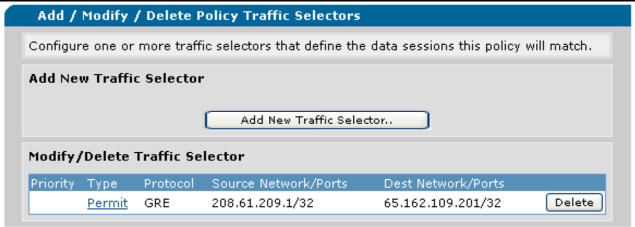
Change the Protocol to ‘gre’.

Change the Source IP Address to the source IP of the GRE tunnel, with a 255.255.255.255 mask.

Change the Destination IP Address to the destination IP of the GRE tunnel, with a 255.255.255.255 mask.

Click ‘Apply’.

**** The 255.255.255.255 subnet mask selects the IP address entered and that address only.*



Add / Modify / Delete Policy Traffic Selectors

Configure one or more traffic selectors that define the data sessions this policy will match.

Add New Traffic Selector

Modify/Delete Traffic Selector

Priority	Type	Protocol	Source Network/Ports	Dest Network/Ports	
	Permit	GRE	208.61.209.1/32	65.162.109.201/32	Delete

After applying, the VPN selectors will reflect the source and destination IP address of the GRE tunnel, and will only be selecting the GRE traffic type.

GRE Tunnel Configuration

The next step is to configure the GRE tunnel that will simulate the point-to-point connectivity. To configure a GRE tunnel:

1) Create the tunnel interface.

2) Specify the IP address & subnet mask of the tunnel endpoint.
   a) Since this is a routable interface, it requires an IP address. This IP address makes no difference to the subnet(s) behind the router, as they will usually be entirely unaware of its existence. These IP addresses should be determined by the network administrator, preferably in an organized and logical manner.
   b) If the GRE over IPSEC tunnel is replacing a dedicated circuit, the same or similar IP addressing scheme should be used.

3) Specify the source & destination IP addresses.
   a) These addresses are the public IP addresses of the routers at each end.

4) Specify the Maximum Transmission Unit (MTU).
   a) Both the GRE tunnel & the VPN encapsulation require additional overhead in the packet. This requires that the MTU of the GRE tunnel be small enough to account for the additional overhead so that the final packet that is created is not fragmented.
   b) In most typical scenarios, an MTU of 100 bytes less than the Internet connection is more than sufficient. 100 bytes is an easy-to-remember number, and given a typical Internet MTU of 1500, the GRE MTU would be 1400.
   c) If you are doing any type of special scenario where you are using additional GRE features, special-case VPNs, or need to maximize your GRE MTU for any reason, please look through the table below, and calculate the required MTU subtraction value you will need.

IPSec Transform Set Combination	Maximum IPSec Overhead (Bytes)
esp-(3des or des) esp-(sha or md5)-hmac	57
esp-(3des or des)	45
esp-aes-(128, 192, or 256) esp-(sha or md5)-hmac	73
esp-aes-(128, 192, or 256)	61
ah-(sha or md5)-hmac esp-(3des or des)	69
ah-(sha or md5)-hmac esp-aes-(128, 192, or 256)	85
ah-(sha or md5)-hmac	44

GRE Tunnel Feature	Addtional Overhead (Bytes)
Standard GRE Overhead	24
Tunnel Checksumming	4
Tunnel Sequencing	4
Tunnel Keying	4
All GRE Features (Worst-Case)	36

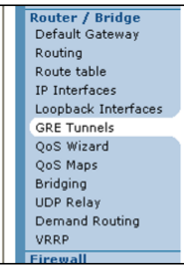
5) Specify the tunnel type as GRE.
    a) Currently in AOS, the only type selectable is GRE, although this may change in future firmware revisions.

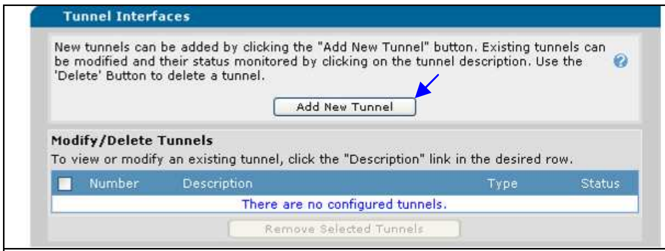
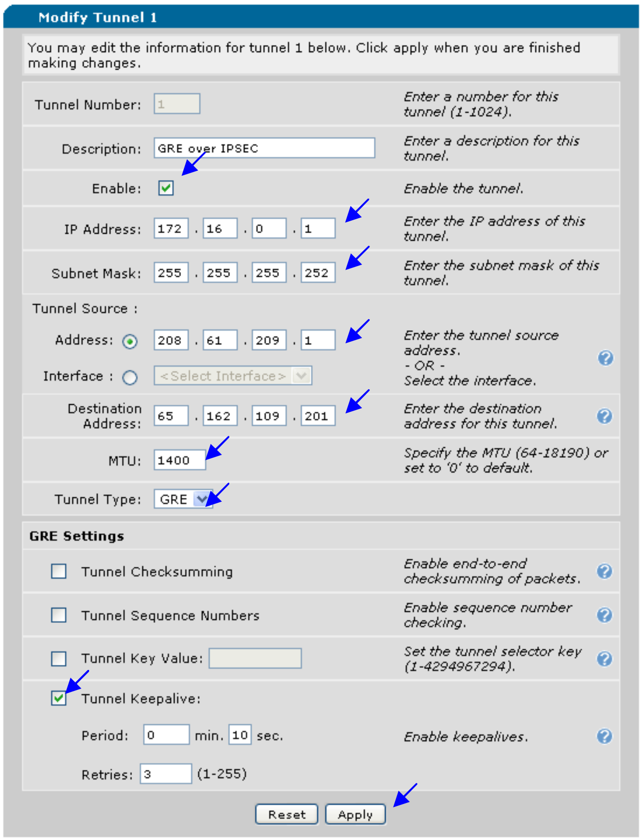
6) Turn on Keepalives.
    a) GRE tunnels have a built-in keepalive mechanism (default 10 seconds) that serves two purposes:
        i) Allows the tunnel to determine whether end-to-end communication is established. Without this feature the tunnel would always appear as UP, regardless of whether it was actually UP or DOWN.
        ii) Keeps a constant stream of traffic going across the tunnel to keep the GRE tunnel UP, and by extension the VPN tunnel UP.

In the command line, the GRE tunnel can be configured in the following manner:

```
interface tunnel 1
  ip address  172.16.0.1  255.255.255.252
  tunnel mode gre
  tunnel source 208.61.209.1
  tunnel destination 65.162.109.201
  keepalive
  mtu 1400
  no shutdown
```

In the web GUI, the GRE tunnel can be configured in the following manner:

	 Router / Bridge Default Gateway Routing Route table IP Interfaces Loopback Interfaces GRE Tunnels QoS Wizard QoS Maps Bridging UDP Relay Demand Routing VRRP Firewall	Browse to ‘GRE Tunnels’.

 **Tunnel Interfaces** New tunnels can be added by clicking the "Add New Tunnel" button. Existing tunnels can be modified and their status monitored by clicking on the tunnel description. Use the 'Delete' Button to delete a tunnel. **Modify/Delete Tunnels** To view or modify an existing tunnel, click the "Description" link in the desired row. □ Number · Description · Type · Status There are no configured tunnels. 	Select 'Add New Tunnel'.
 **Modify Tunnel 1** You may edit the information for tunnel 1 below. Click apply when you are finished making changes. Tunnel Number: 1 — *Enter a number for this tunnel (1-1024).* Description: GRE over IPSEC — *Enter a description for this tunnel.* Enable: ☑ — *Enable the tunnel.* IP Address: 172 . 16 . 0 . 1 — *Enter the IP address of this tunnel.* Subnet Mask: 255 . 255 . 255 . 252 — *Enter the subnet mask of this tunnel.* Tunnel Source : Address: ● 208 . 61 . 209 . 1 — *Enter the tunnel source address. - OR - Select the interface.* Interface : ○ <Select Interface> Destination Address: 65 . 162 . 109 . 201 — *Enter the destination address for this tunnel.* MTU: 1400 — *Specify the MTU (64-18190) or set to '0' to default.* Tunnel Type: GRE **GRE Settings** □ Tunnel Checksumming — *Enable end-to-end checksumming of packets.* □ Tunnel Sequence Numbers — *Enable sequence number checking.* □ Tunnel Key Value: — *Set the tunnel selector key (1-4294967294).* ☑ Tunnel Keepalive: Period: 0 min. 10 sec. — *Enable keepalives.* Retries: 3 (1-255) 	Configure the tunnel to the specifications required and as outlined in the above section. Click 'Apply' when finished.

GRE Tunnel Firewall Setup (Optional)

The GRE tunnel counts as a routable interface, and thus must have a firewall policy constructed for it. A uniquely-named policy-class (Security Zone) is recommended so that the firewall is able to distinguish the difference between interfaces in the same manner that the routing engine can, and it also makes it easier for the firewall administrator to understand in most cases.

This recommendation results in three policy-classes in the typical configuration:

- Private
    - Will be constructed to allow administrative access, allow all traffic through the GRE tunnel, and optionally NAT traffic to the public interface.

- Public
  - Will be constructed to allow the VPN tunnel traffic inbound, and allow administrative access.
- Tunnel
  - Will be constructed in most cases to allow all traffic.

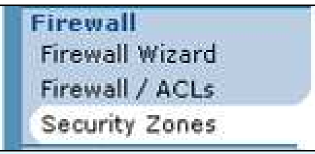
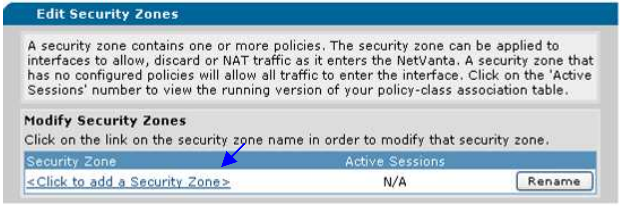
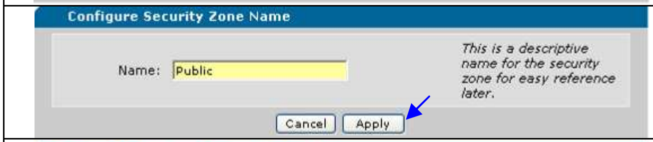
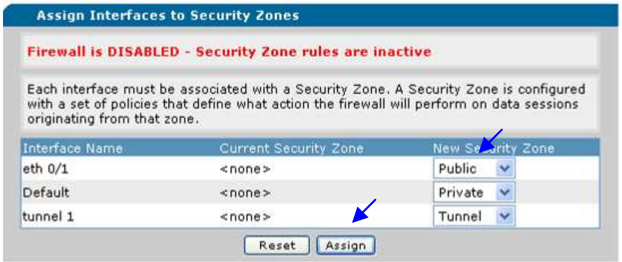
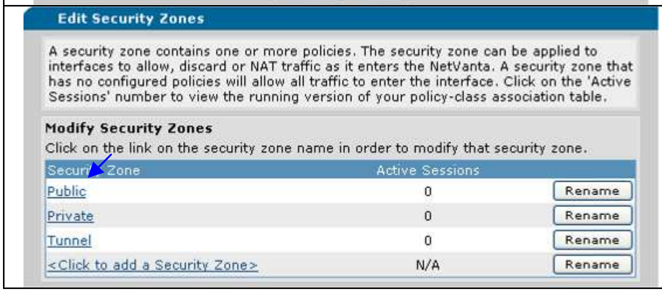
The firewall construction, as outlined in this document, will take advantage of a firewall function to specify the destination policy-class. This is designed to ease the administrative burden when traffic does not need to be filtered on the edge routers, only routed to another site where policing can be centrally enforced. This allows for the access-lists referenced by the firewall to be ‘match all’s, but be limited to what they will match based upon where the packet is routed.

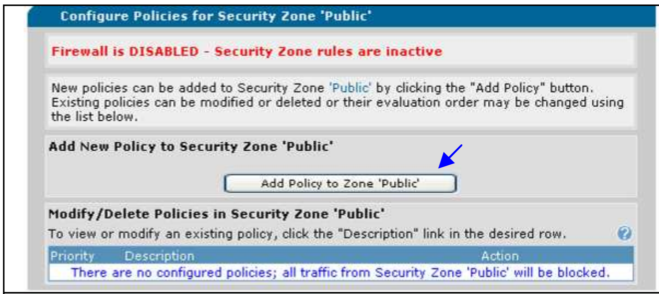
For further firewall configuration and understanding, refer to KB articles #1968 and #1543.

In the CLI, the firewall can be configured in the following manner:

```
ip firewall
!
interface <WAN Interface>
  access-policy Public
!
interface <LAN Interface>
  access-policy Private
!
interface tunnel 1
  access-policy Tunnel
!
ip access-list extended self
  remark Traffic to Netvanta
  permit ip any any
!
ip access-list extended tunnel
  remark Traffic to GRE Tunnel
  permit ip any any
!
ip access-list extended NAT
  remark NAT to the Internet
  permit ip any any
!
ip access-list extended AdminAccess
  remark Public Admin Access
  <Desired Admin Access>
!
ip access-list extended VPN-Selectors
  remark GRE Tunnel Selectors
  permit gre host 208.61.209.1 host 65.162.109.201
!
ip policy-class Private
  allow list self self
  allow list tunnel policy Tunnel
  nat source list NAT interface <WAN Interface> overload policy Public
!
ip policy-class Tunnel
  allow list self self
  allow list tunnel policy Private
!
ip policy-class Public
  allow reverse list VPN-Selectors stateless
  allow list AdminAccess self
```

In the web GUI, the firewall can be configured in the following manner:

 Firewall Firewall Wizard Firewall / ACLs Security Zones	Browse to 'Security Zones'.
 Edit Security Zones A security zone contains one or more policies. The security zone can be applied to interfaces to allow, discard or NAT traffic as it enters the NetVanta. A security zone that has no configured policies will allow all traffic to enter the interface. Click on the 'Active Sessions' number to view the running version of your policy-class association table. Modify Security Zones Click on the link on the security zone name in order to modify that security zone. Security Zone Active Sessions <Click to add a Security Zone> N/A Rename	Select 'Click to add a Security Zone'.
 Configure Security Zone Name Name: Public *This is a descriptive name for the security zone for easy reference later.* Cancel Apply	Create the zones 'Public', 'Private', and 'Tunnel'.
 Assign Interfaces to Security Zones Firewall is DISABLED - Security Zone rules are inactive Each interface must be associated with a Security Zone. A Security Zone is configured with a set of policies that define what action the firewall will perform on data sessions originating from that zone. Interface Name Current Security Zone New Security Zone eth 0/1 <none> Public Default <none> Private tunnel 1 <none> Tunnel Reset Assign	Assign the Security Zones to the appropriate interfaces.
 Edit Security Zones A security zone contains one or more policies. The security zone can be applied to interfaces to allow, discard or NAT traffic as it enters the NetVanta. A security zone that has no configured policies will allow all traffic to enter the interface. Click on the 'Active Sessions' number to view the running version of your policy-class association table. Modify Security Zones Click on the link on the security zone name in order to modify that security zone. Security Zone Active Sessions Public 0 Rename Private 0 Rename Tunnel 0 Rename <Click to add a Security Zone> N/A Rename	Select Security Zone 'Public'.



Configure Policies for Security Zone 'Public'

Firewall is DISABLED - Security Zone rules are inactive

New policies can be added to Security Zone 'Public' by clicking the "Add Policy" button. Existing policies can be modified or deleted or their evaluation order may be changed using the list below.

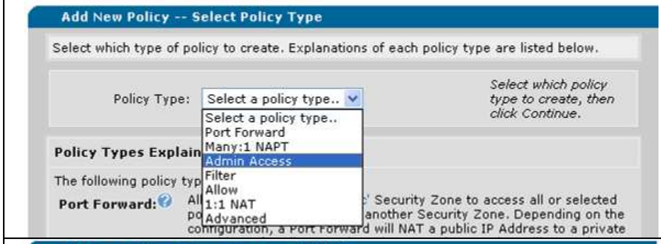
Add New Policy to Security Zone 'Public'

Modify/Delete Policies in Security Zone 'Public'

To view or modify an existing policy, click the "Description" link in the desired row.

Priority	Description	Action
There are no configured policies; all traffic from Security Zone 'Public' will be blocked.		

Select 'Add Policy to Zone Public'.



Add New Policy -- Select Policy Type

Select which type of policy to create. Explanations of each policy type are listed below.

Policy Type: Select a policy type..

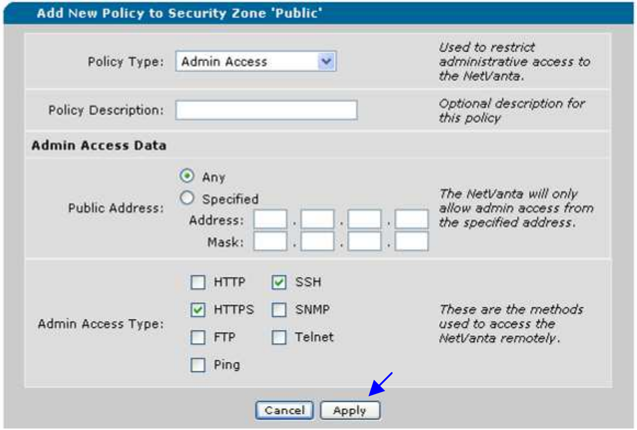
Select which policy type to create, then click Continue.

Policy Types Explain

The following policy typ

Port Forward: Al ' Security Zone to access all or selected po another Security Zone. Depending on the configuration, a Port Forward will NAT a public IP Address to a private

Select policy type 'Admin Access', click 'Continue'.



Add New Policy to Security Zone 'Public'

Policy Type: Admin Access — *Used to restrict administrative access to the NetVanta.*

Policy Description: — *Optional description for this policy*

Admin Access Data

Public Address: ● Any ○ Specified — *The NetVanta will only allow admin access from the specified address.*

Address: . . .

Mask: . . .

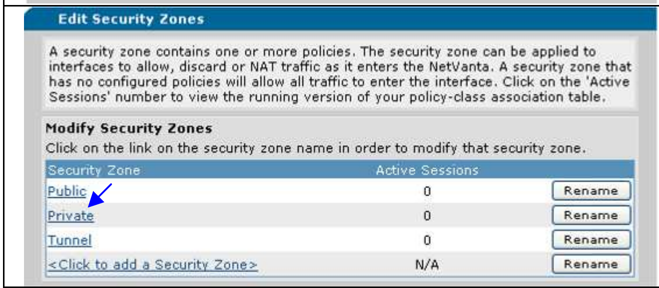
Admin Access Type: — *These are the methods used to access the NetVanta remotely.*

□ HTTP ☑ SSH
☑ HTTPS □ SNMP
□ FTP □ Telnet
□ Ping

The public address should be left to 'Any', or limited to the IP address range of the network administrator.

The type of remote access services that need to be allowed should be check marked. These should be determined by the network administrator and any relevant company-specific security policies.

Click 'Apply' when finished.



Edit Security Zones

A security zone contains one or more policies. The security zone can be applied to interfaces to allow, discard or NAT traffic as it enters the NetVanta. A security zone that has no configured policies will allow all traffic to enter the interface. Click on the 'Active Sessions' number to view the running version of your policy-class association table.

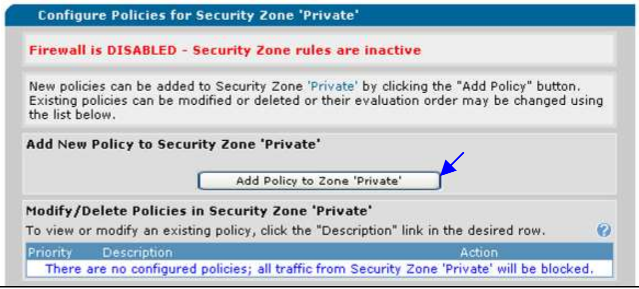
Modify Security Zones

Click on the link on the security zone name in order to modify that security zone.

Security Zone	Active Sessions	
Public	0	Rename
Private	0	Rename
Tunnel	0	Rename
<Click to add a Security Zone>	N/A	Rename

Browse back to 'Security Zones'.

Select Security Zone 'Private'.



Configure Policies for Security Zone 'Private'

Firewall is DISABLED - Security Zone rules are inactive

New policies can be added to Security Zone 'Private' by clicking the "Add Policy" button. Existing policies can be modified or deleted or their evaluation order may be changed using the list below.

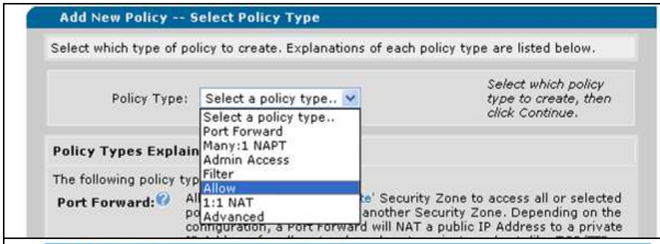
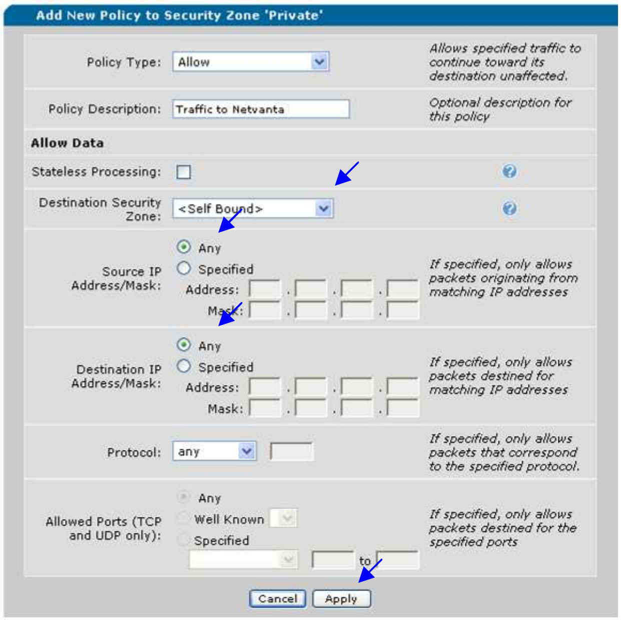
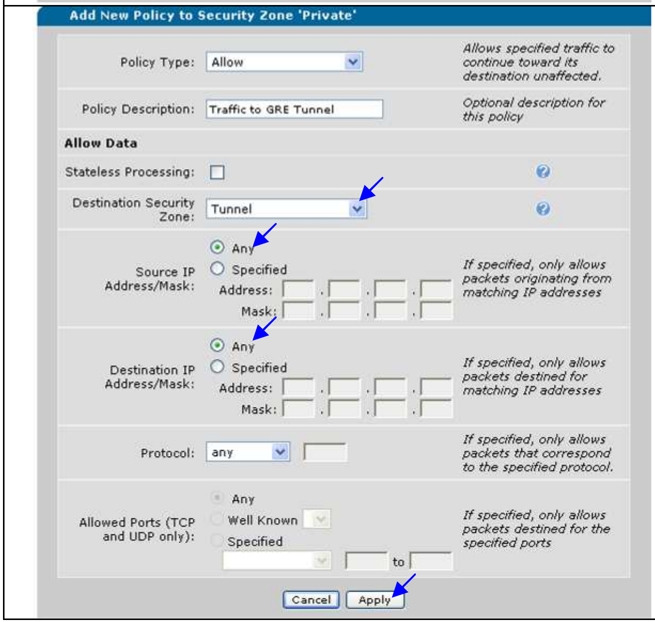
Add New Policy to Security Zone 'Private'

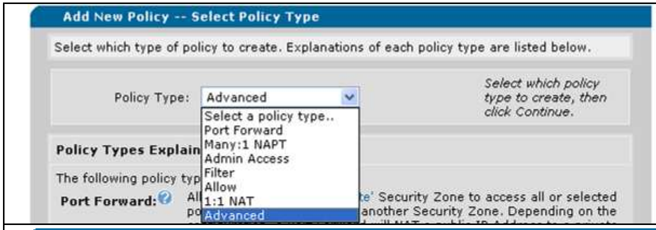
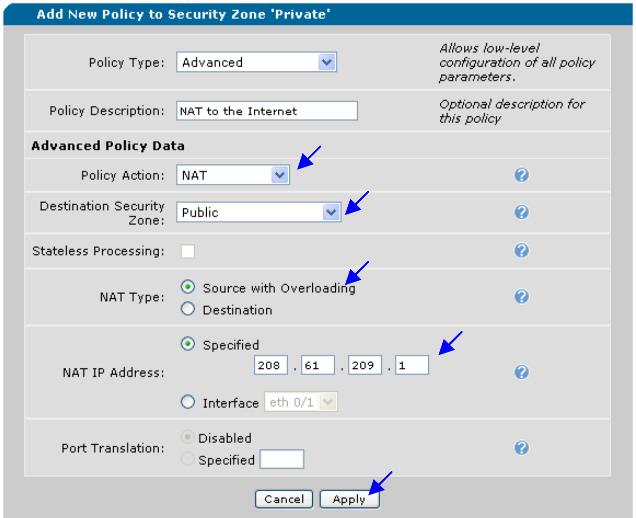
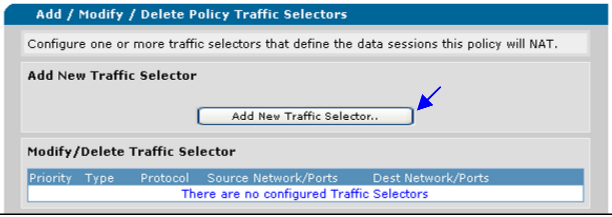
Modify/Delete Policies in Security Zone 'Private'

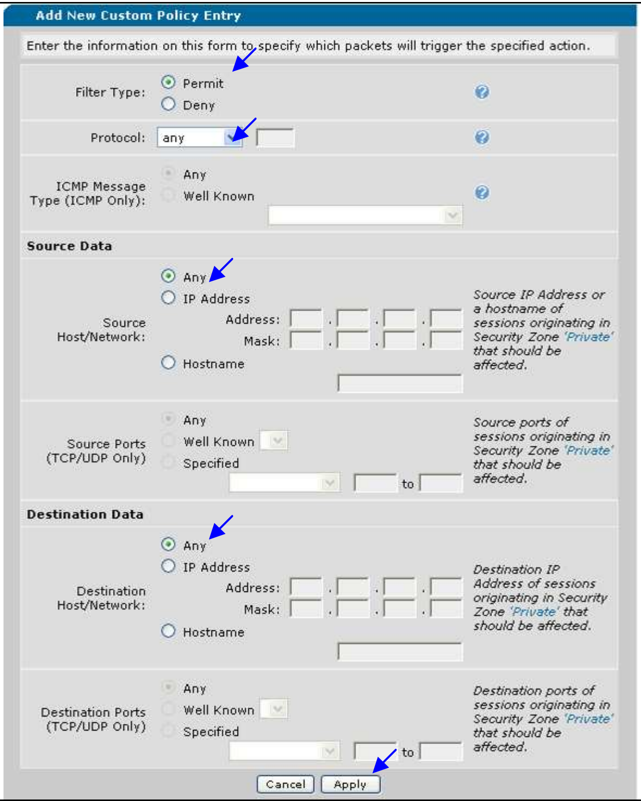
To view or modify an existing policy, click the "Description" link in the desired row.

Priority	Description	Action
There are no configured policies; all traffic from Security Zone 'Private' will be blocked.		

Select 'Add Policy to Zone Private'.

 Add New Policy -- Select Policy Type Select which type of policy to create. Explanations of each policy type are listed below. Policy Type: Select a policy type.. *Select which policy type to create, then click Continue.* Select a policy type.. Port Forward Many:1 NAPT Admin Access Filter Allow 1:1 NAT Advanced **Policy Types Explain** The following policy typ **Port Forward:** Al te' Security Zone to access all or selected po another Security Zone. Depending on the configuration, a Port Forward will NAT a public IP Address to a private	Select policy type 'Allow', click 'Continue'.
 Add New Policy to Security Zone 'Private' Policy Type: Allow — *Allows specified traffic to continue toward its destination unaffected.* Policy Description: Traffic to Netvanta — *Optional description for this policy* **Allow Data** Stateless Processing: □ Destination Security Zone: <Self Bound> Source IP Address/Mask: ● Any ○ Specified Address: Mask: — *If specified, only allows packets originating from matching IP addresses* Destination IP Address/Mask: ● Any ○ Specified Address: Mask: — *If specified, only allows packets destined for matching IP addresses* Protocol: any — *If specified, only allows packets that correspond to the specified protocol.* Allowed Ports (TCP and UDP only): ○ Any ○ Well Known ○ Specified to — *If specified, only allows packets destined for the specified ports* Cancel Apply	Select from 'any' to 'any', with a destination Security Zone of '<Self Bound>'. This will allow all traffic inbound to the Private Security Zone on any IP address owned by the router. Click 'Apply' when finished.
 Add New Policy to Security Zone 'Private' Policy Type: Allow — *Allows specified traffic to continue toward its destination unaffected.* Policy Description: Traffic to GRE Tunnel — *Optional description for this policy* **Allow Data** Stateless Processing: □ Destination Security Zone: Tunnel Source IP Address/Mask: ● Any ○ Specified Address: Mask: — *If specified, only allows packets originating from matching IP addresses* Destination IP Address/Mask: ● Any ○ Specified Address: Mask: — *If specified, only allows packets destined for matching IP addresses* Protocol: any — *If specified, only allows packets that correspond to the specified protocol.* Allowed Ports (TCP and UDP only): ○ Any ○ Well Known ○ Specified to — *If specified, only allows packets destined for the specified ports* Cancel Apply	Create a new 'Allow' policy in the 'Private' Security Zone. Select from 'any' to 'any', with a destination Security Zone of 'Tunnel'. This will allow all traffic inbound to the Private Security Zone that will be routed through the GRE tunnel. Click 'Apply' when finished.

 Add New Policy -- Select Policy Type Select which type of policy to create. Explanations of each policy type are listed below. Policy Type: Advanced Select which policy type to create, then click Continue. Select a policy type.. Port Forward Many:1 NAPT Admin Access Filter Allow 1:1 NAT Advanced Policy Types Explain The following policy typ Port Forward: Al te' Security Zone to access all or selected po another Security Zone. Depending on the	Create a new ‘Advanced’ policy in Zone ‘Private’.
 Add New Policy to Security Zone 'Private' Policy Type: Advanced — *Allows low-level configuration of all policy parameters.* Policy Description: NAT to the Internet — *Optional description for this policy* **Advanced Policy Data** Policy Action: NAT Destination Security Zone: Public Stateless Processing: □ NAT Type: ● Source with Overloading ○ Destination NAT IP Address: ● Specified 208 . 61 . 209 . 1 ○ Interface eth 0/1 Port Translation: ○ Disabled ○ Specified Cancel Apply	Set the policy action to ‘NAT’. Set the destination Security Zone to ‘Public’. Set the NAT type to ‘Source with Overloading’ Set the NAT IP Address to the public IP address of the router. Click ‘Apply’ when finished.
 Add / Modify / Delete Policy Traffic Selectors Configure one or more traffic selectors that define the data sessions this policy will NAT. **Add New Traffic Selector** Add New Traffic Selector.. **Modify/Delete Traffic Selector** Priority Type Protocol Source Network/Ports Dest Network/Ports There are no configured Traffic Selectors	Select ‘Add New Traffic Selector’.



Add New Custom Policy Entry

Enter the information on this form to specify which packets will trigger the specified action.

Filter Type:	● Permit ○ Deny	
Protocol:	any	
ICMP Message Type (ICMP Only):	○ Any ○ Well Known	

Source Data

Source Host/Network:	● Any ○ IP Address Address: . . . Mask: . . . ○ Hostname	Source IP Address or a hostname of sessions originating in Security Zone 'Private' that should be affected.
Source Ports (TCP/UDP Only)	○ Any ○ Well Known ○ Specified to	Source ports of sessions originating in Security Zone 'Private' that should be affected.

Destination Data

Destination Host/Network:	● Any ○ IP Address Address: . . . Mask: . . . ○ Hostname	Destination IP Address of sessions originating in Security Zone 'Private' that should be affected.
Destination Ports (TCP/UDP Only)	○ Any ○ Well Known ○ Specified to	Destination ports of sessions originating in Security Zone 'Private' that should be affected.

Select type 'Permit'.

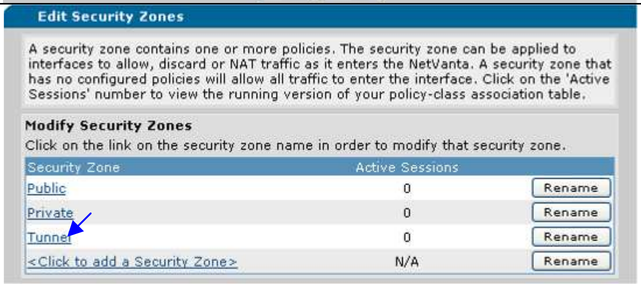
Select protocol 'any'.

Select source and destination 'any'.

Click 'Apply' when finished.

This policy will NAT all traffic to the internet (locally) for any traffic routed out the public interface.

**** This policy will have no effect if the default route is through the GRE tunnel. In this case, it would only take effect if the GRE tunnel was down and traffic failed-over to the local internet connection.*



Edit Security Zones

A security zone contains one or more policies. The security zone can be applied to interfaces to allow, discard or NAT traffic as it enters the NetVanta. A security zone that has no configured policies will allow all traffic to enter the interface. Click on the 'Active Sessions' number to view the running version of your policy-class association table.

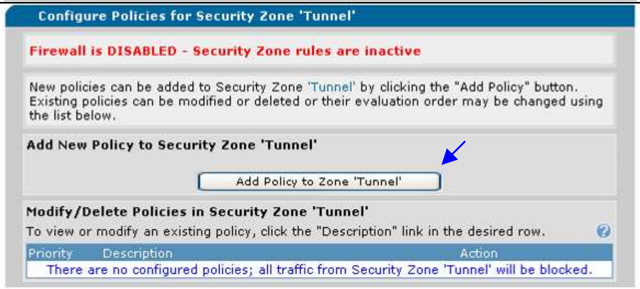
Modify Security Zones

Click on the link on the security zone name in order to modify that security zone.

Security Zone	Active Sessions	
Public	0	Rename
Private	0	Rename
Tunnel	0	Rename
<Click to add a Security Zone>	N/A	Rename

Browse back to 'Security Zones'.

Select Security Zone 'Tunnel'.



Configure Policies for Security Zone 'Tunnel'

Firewall is DISABLED - Security Zone rules are inactive

New policies can be added to Security Zone 'Tunnel' by clicking the "Add Policy" button. Existing policies can be modified or deleted or their evaluation order may be changed using the list below.

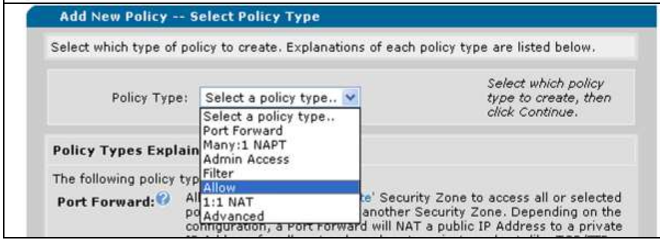
Add New Policy to Security Zone 'Tunnel'

Modify/Delete Policies in Security Zone 'Tunnel'

To view or modify an existing policy, click the "Description" link in the desired row.

Priority	Description	Action
	There are no configured policies; all traffic from Security Zone 'Tunnel' will be blocked.	

Select 'Add Policy to Zone Tunnel'.



Add New Policy -- Select Policy Type

Select which type of policy to create. Explanations of each policy type are listed below.

Policy Type: Select a policy type..

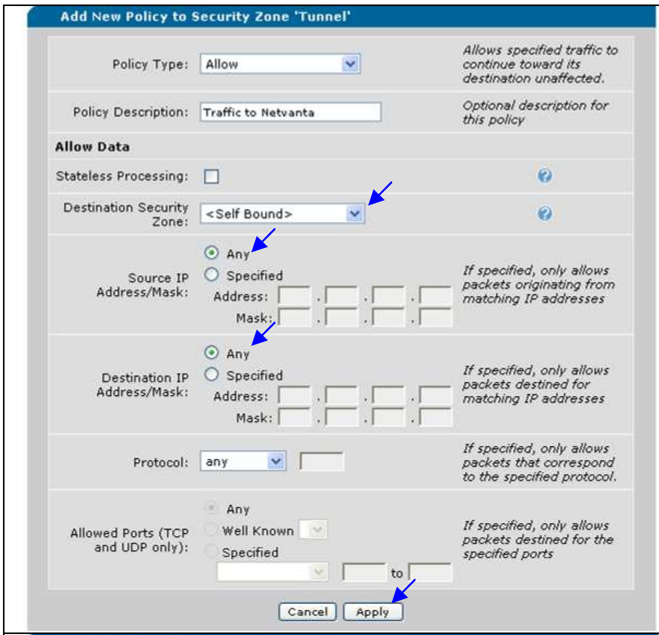
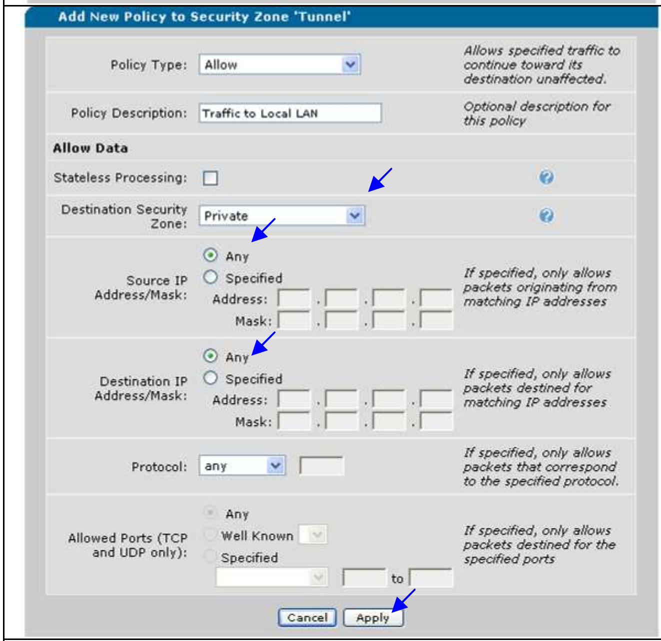
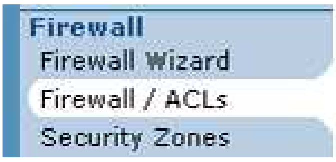
Select which policy type to create, then click Continue.

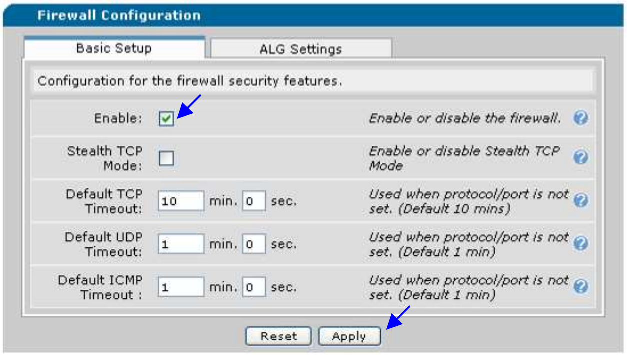
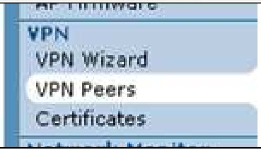
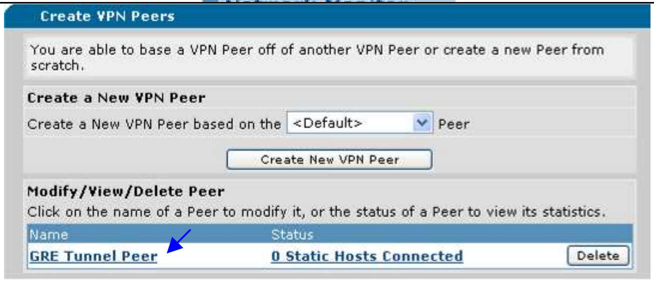
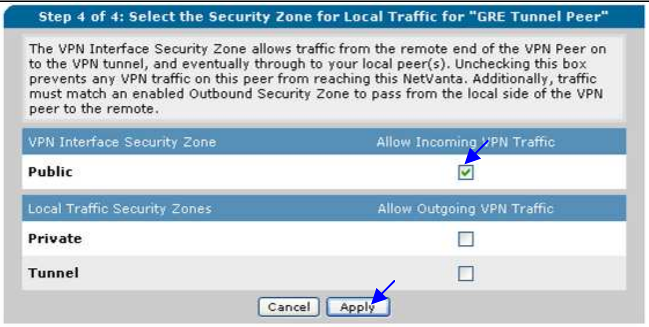
Policy Types Explain

The following policy typ

Port Forward: All ...te' Security Zone to access all or selected po... another Security Zone. Depending on the configuration, a Port Forward will NAT a public IP Address to a private

Select policy type 'Allow', click 'Continue'.

 Add New Policy to Security Zone 'Tunnel' Policy Type: Allow — Allows specified traffic to continue toward its destination unaffected. Policy Description: Traffic to Netvanta — Optional description for this policy **Allow Data** Stateless Processing: ☐ Destination Security Zone: <Self Bound> Source IP Address/Mask: ● Any ○ Specified Address: . . . Mask: . . . — If specified, only allows packets originating from matching IP addresses Destination IP Address/Mask: ● Any ○ Specified Address: . . . Mask: . . . — If specified, only allows packets destined for matching IP addresses Protocol: any — If specified, only allows packets that correspond to the specified protocol. Allowed Ports (TCP and UDP only): ○ Any ○ Well Known ○ Specified to — If specified, only allows packets destined for the specified ports Cancel Apply	Select from ‘any’ to ‘any’, with a destination Security Zone of ‘<Self Bound>’. This will allow all traffic inbound to the Tunnel Security Zone on any IP address owned by the router. Click ‘Apply’ when finished.
 Add New Policy to Security Zone 'Tunnel' Policy Type: Allow — Allows specified traffic to continue toward its destination unaffected. Policy Description: Traffic to Local LAN — Optional description for this policy **Allow Data** Stateless Processing: ☐ Destination Security Zone: Private Source IP Address/Mask: ● Any ○ Specified Address: . . . Mask: . . . — If specified, only allows packets originating from matching IP addresses Destination IP Address/Mask: ● Any ○ Specified Address: . . . Mask: . . . — If specified, only allows packets destined for matching IP addresses Protocol: any — If specified, only allows packets that correspond to the specified protocol. Allowed Ports (TCP and UDP only): ○ Any ○ Well Known ○ Specified to — If specified, only allows packets destined for the specified ports Cancel Apply	Create a new ‘Allow’ policy in the ‘Tunnel’ Security Zone. Select from ‘any’ to ‘any’, with a destination Security Zone of ‘Private’. This will allow all traffic inbound to the Tunnel Security Zone that will be routed to the local LAN Click ‘Apply’ when finished.
 Firewall Firewall Wizard Firewall / ACLs Security Zones	Browse to ‘Firewall / ACLs’. **** This may be called ‘General Firewall’ in some firmware revisions.*

 **Firewall Configuration** Basic Setup · ALG Settings Configuration for the firewall security features. Enable: ☑ — *Enable or disable the firewall.* Stealth TCP Mode: □ — *Enable or disable Stealth TCP Mode* Default TCP Timeout: 10 min. 0 sec. — *Used when protocol/port is not set. (Default 10 mins)* Default UDP Timeout: 1 min. 0 sec. — *Used when protocol/port is not set. (Default 1 min)* Default ICMP Timeout : 1 min. 0 sec. — *Used when protocol/port is not set. (Default 1 min)* 	Enable the firewall by check marking the 'Enable' box. Click 'Apply' when finished. **** This will immediately enable the firewall on all interfaces and may cause the current web session to be terminated.*
 	Browse to 'VPN Peers'.
 **Create VPN Peers** You are able to base a VPN Peer off of another VPN Peer or create a new Peer from scratch. **Create a New VPN Peer** Create a New VPN Peer based on the <Default> Peer **Modify/View/Delete Peer** Click on the name of a Peer to modify it, or the status of a Peer to view its statistics. Name: GRE Tunnel Peer — Status: 0 Static Hosts Connected 	Select the VPN policy for the GRE tunnel.
 **Step 4 of 4: Select the Security Zone for Local Traffic for "GRE Tunnel Peer"** The VPN Interface Security Zone allows traffic from the remote end of the VPN Peer on to the VPN tunnel, and eventually through to your local peer(s). Unchecking this box prevents any VPN traffic on this peer from reaching this NetVanta. Additionally, traffic must match an enabled Outbound Security Zone to pass from the local side of the VPN peer to the remote. VPN Interface Security Zone — Allow Incoming VPN Traffic **Public** ☑ Local Traffic Security Zones — Allow Outgoing VPN Traffic **Private** □ **Tunnel** □ 	Scroll down the page to Step 4 of 4 and check the box to 'Allow Incoming VPN Traffic' on the Public Security Zone. **** The outgoing GRE traffic will be sourced from the 'Self' Security Zone, and is always allowed.*

Routing Settings

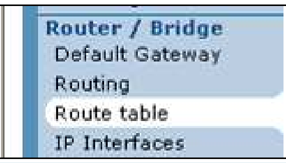
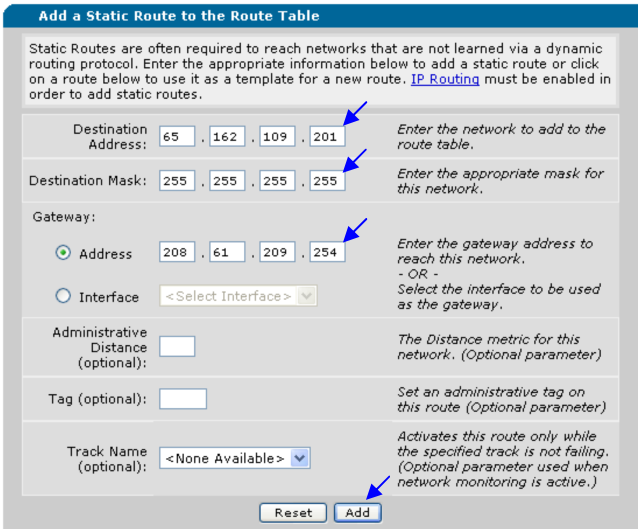
The firewall has been setup to take its cue from the routing engine, so a properly functioning routing table is critical. If the routing table is not setup correctly, especially in the case of funneling all Internet traffic through the GRE to a central location, recursive routing errors may occur.

The first step to avoid routing errors is to create a static route to the GRE tunnel peer. This will force the router to always use this path when accessing the GRE tunnel peer. If this route was not entered, and the default route was pointing through the GRE tunnel, the only way the router could get to the GRE tunnel peer would be to traverse the GRE tunnel, which results in a recursive routing error. Using the example configuration, the route would be configured in this manner in the command line:

```
ip route <GRE Tunnel Peer IP> 255.255.255.255 <Internet Gateway>

ip route 65.162.109.201 255.255.255.255 208.61.209.254
```

The route would be configured in this manner in the web GUI:

 Router / Bridge Default Gateway Routing Route table IP Interfaces	Browse to 'Route Table'
	Enter the GRE tunnel peer IP as the 'destination address'. Enter 255.255.255.255 as the 'destination mask'. Enter the internet connection gateway as the 'gateway'. Click 'Add' when finished

Add a Static Route to the Route Table

Static Routes are often required to reach networks that are not learned via a dynamic routing protocol. Enter the appropriate information below to add a static route or click on a route below to use it as a template for a new route. IP Routing must be enabled in order to add static routes.

Destination Address:	65 . 162 . 109 . 201	*Enter the network to add to the route table.*
Destination Mask:	255 . 255 . 255 . 255	*Enter the appropriate mask for this network.*
Gateway:		
● Address	208 . 61 . 209 . 254	*Enter the gateway address to reach this network.* *- OR -* *Select the interface to be used as the gateway.*
○ Interface	<Select Interface>	
Administrative Distance (optional):		*The Distance metric for this network. (Optional parameter)*
Tag (optional):		*Set an administrative tag on this route (Optional parameter)*
Track Name (optional):	<None Available>	*Activates this route only while the specified track is not failing. (Optional parameter used when network monitoring is active.)*

The next step will be to configure a routing protocol to use across the GRE tunnel, or add in static routes as needed. Routing protocols are covered in the following KB articles:

- RIP
  - KB article #1969
- OSPF
  - KB article #1625
- BGP
  - KB article #1618

A static route to the subnet across the GRE tunnel can be added in the following manner:

```
ip route <Peer Subnet> <Peer Subnet Mask> tunnel 1

ip route 192.168.2.0 255.255.255.0 tunnel 1
```

Route All Internet Traffic through the GRE Tunnel (Optional)

If the GRE tunnel is to be used to funnel all Internet traffic, it is probably a good idea to have the routing automatically fail-over to the local Internet connection in the event of a GRE tunnel failure. This way the users will lose connectivity to all the remote private subnets, but not Internet access. However, the downside is that the user’s traffic will be unrestricted by corporate firewalls and other security policies in place.

To setup the router to fail-over to the local Internet connection, a ‘floating’ static route (a route with a higher administrative distance) must be added. When the primary link goes down, the normal route that is statically set or learned by a dynamic routing protocol will be pulled out of the routing table due to the directly connected network associated with that interface no longer being available. At that point, the floating static route will be inserted in the routing table to direct traffic over the backup link.

The proper routing setup for funneling all traffic through the GRE tunnel, and failing back to the local Internet connection can be configured in the following manner:

```
ip route 0.0.0.0 0.0.0.0 tunnel 1
ip route 0.0.0.0 0.0.0.0 <Internet Gateway> <Administrative Distance>
ip route <GRE Tunnel Peer IP> 255.255.255.255 <Internet Gateway>
```

Application Overview

1) A packet destined for the remote VPN subnet arrives on the Private policy-class and is allowed through the firewall via an ‘Allow’ policy.

2) The destination IP address for this packet is checked with the routing table to determine the interface to send it out. The routing table lookup determines the tunnel 1 interface should be used from the static route specified in the configuration.

3) The tunnel interface configuration specifies the peer IP to use and sets the destination IP in the new IP header accordingly; this new IP header is inserted as part of the GRE encapsulation process.

4) The routing table is used again to determine where the GRE packet should be sent, which in this case is the Public interface.

5) The crypto map applied to the Public interface is activated because the VPN selector matches the traffic, in this case GRE traffic between the two hosts.

6) The crypto map also specifies the VPN peer IP address that should be used to direct the encrypted traffic to. Another new IP header is created with the destination IP

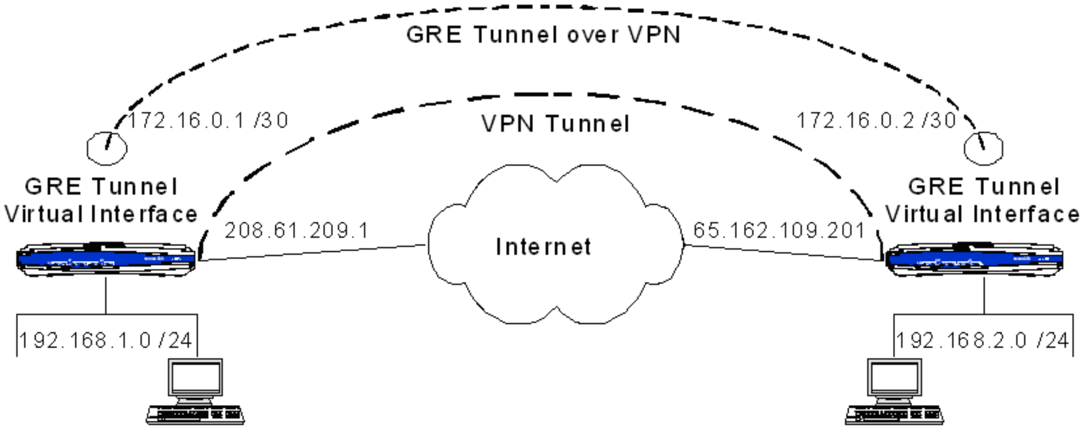
address set as the VPN peer IP from the crypto map peer statement; this new IP header is inserted as part of the VPN encapsulation process.

7) This final packet which has 3 IP headers [VPN | GRE | original] is routed out the Public interface and on to the Internet to reach the VPN peer.

8) The peer first terminates the VPN tunnel and peels that header off, then the GRE tunnel will be terminated with that header peeled off as well. Finally the original packet will be exposed and processed accordingly on the peer router.

Example Configuration

In the following example, a remote office for a company needs to route all traffic through the GRE over IPSEC tunnel to a central office for tracking and policing purposes. In the event that the main site or the GRE would ever go down, Internet access should still be allowed via the local Internet connection.



```
ip firewall
ip firewall fast-nat-failover
!
ip crypto
!
crypto ike policy 100
  initiate main
  respond main
  local-id address 208.61.209.1
  peer 65.162.109.201
  attribute 1
    encryption 3des
    hash md5
    authentication pre-share
!
crypto  ike  remote-id  address  65.162.109.201  preshared-key  adtran  ike-
policy 100 crypto map VPN 10 no-mode-config no-xauth
!
```

```
crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac
  mode tunnel
!
crypto map VPN 10 ipsec-ike
  description GRE Tunnel Peer
  match address VPN-Selectors
  set peer 65.162.109.201
  set transform-set esp-3des-esp-md5-hmac
  ike-policy 100
!
interface t1 1/1
  tdm-group 1 timeslots 1-24 speed 64
  no shutdown
!
interface ppp 1
  ip address 208.61.209.1 255.255.255.0
  access-policy Public
  crypto map VPN
  no shutdown
  cross-connect 1 t1 1/1 1 ppp 1
!
interface eth 0/1
  ip address 192.168.1.1 255.255.255.0
  access-policy Private
  no shutdown
!
interface tunnel 1
  ip address  172.16.0.1  255.255.255.252
  access-policy Tunnel
  tunnel mode gre
  tunnel source 208.61.209.1
  tunnel destination 65.162.109.201
  keepalive
  mtu 1400
  no shutdown
!
ip access-list extended self
  remark Traffic to Netvanta
  permit ip any any
!
ip access-list extended tunnel
  remark Traffic to GRE Tunnel
  permit ip any any
!
ip access-list extended NAT
  remark NAT to the Internet
  permit ip any any
!
ip access-list extended AdminAccess
  remark Public Admin Access
  permit tcp any any eq ssh
  permit tcp any any eq https
!
ip access-list extended VPN-Selectors
  remark GRE Tunnel Selectors
  permit gre host 208.61.209.1 host 65.162.109.201
!
```

```
ip policy-class Private
  allow list self self
  allow list tunnel policy Tunnel
  nat source list NAT interface ppp 1 overload policy Public
!
ip policy-class Tunnel
  allow list self self
  allow list tunnel policy Private
!
ip policy-class Public
  allow reverse list VPN-Selectors stateless
  allow list AdminAccess self

ip route 0.0.0.0 0.0.0.0 208.61.209.254
ip route 192.168.2.0 255.255.255.0 tunnel 1
ip route 65.162.109.201 255.255.255.255 208.61.209.254
```