



## TECHNICAL SUPPORT NOTE

### Introduction to the Firewall Menu in the Web GUI

#### Featuring ADTRAN OS and the Web GUI

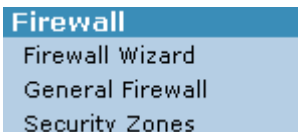
---

## Introduction

This Technical Support Note shows the different options available in the Firewall menu of the ADTRAN OS Web GUI.

### Firewall Menus

The NetVanta GUI Firewall menus allow you to quickly configure an initial firewall policy, change default protocol and traffic timeouts, and configure advanced firewall policies to control traffic going through the firewall.



### Firewall Wizard

The Firewall wizard can be used for the initial Firewall policy configuration. You can quickly enable Internet sharing (using NAT) by selecting the public interface and then selecting the private interfaces that will use the public interface for outbound traffic. Port forwarding can also be configured in the wizard if you have servers (web, e-mail, etc.) on your private network that need to be accessed from the Internet.

### General Firewall

The NetVanta Firewall can be enabled or disabled from the General Firewall screen. You can also override the default protocol timeouts for TCP, UDP, or ICMP in addition to setting timeouts on specific applications.

### Security Zones

The Security Zones screen can be used to configure advanced firewall options that cannot be configured in the firewall wizard. A security zone contains one or more policies and can be applied to interfaces to allow, discard, or NAT traffic as it enters the NetVanta.

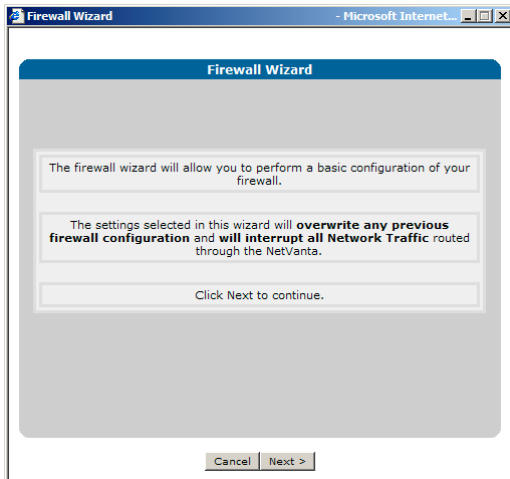
# Firewall Wizard

The Firewall Wizard enables the NetVanta firewall and allows you to perform a basic configuration of the firewall. The public interface connected to the Internet and the private interfaces that need access to the Internet can quickly be defined. You can also define servers on your private network that Internet users need to be able to access.

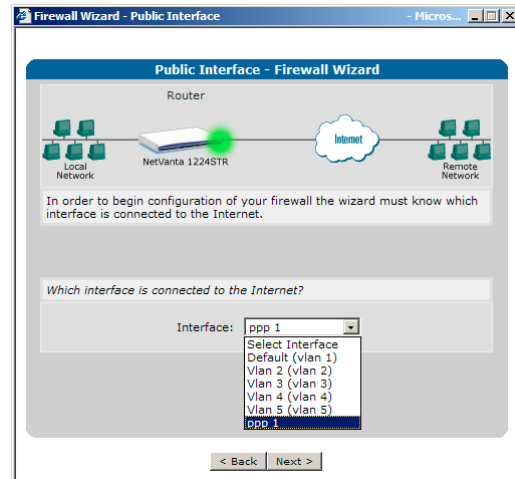
**WARNING!** - *The Firewall Wizard should only be used for the initial firewall configuration. It will overwrite any existing firewall policies and temporarily interrupt all Network Traffic. The Security Zones area of the firewall can be used to modify existing firewall policies.*

## Using the Firewall Wizard

1) After selecting the Firewall Wizard, click Next to confirm that you plan to overwrite any previous firewall configuration.

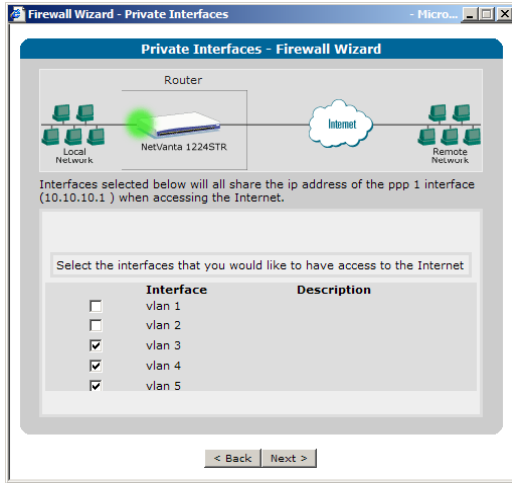


2) Choose the interface that is connected to the Internet. This will be the Public interface.

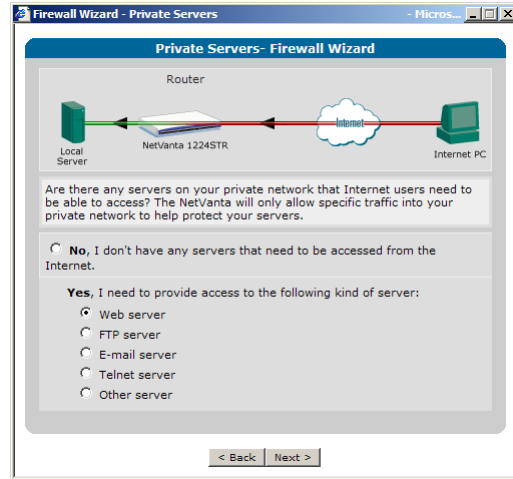


## Using the Firewall Wizard (Continued...)

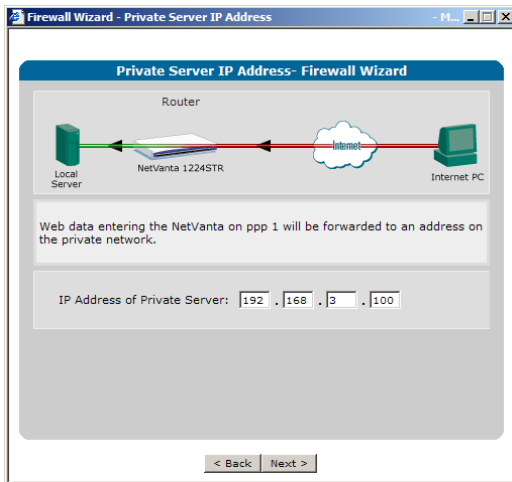
3) Select all the Private interfaces that will use the Public interface to get out to the Internet.



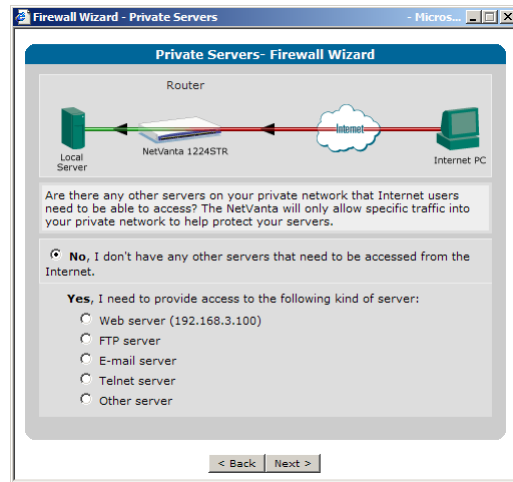
4) Specify the server (if any) on your Private network that you want to allow access to from the Internet.



5) Specify the IP address of the Private Server that will receive the forwarded traffic.

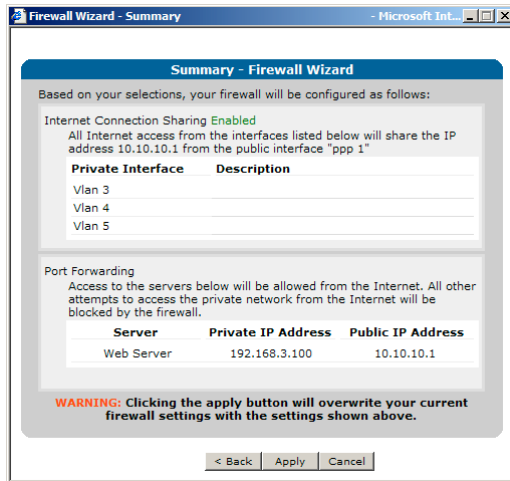


6) Identify any other servers that will be located on the Private network. (if any)

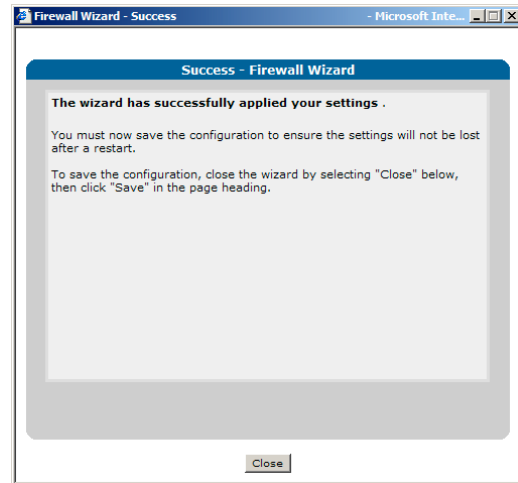


## Using the Firewall Wizard (Continued...)

7) One final warning that you will overwrite existing Firewall policies. Click Apply to create the defined Firewall policies.



8) You have successfully created and applied the Firewall policies. Close the window.



The firewall policies will be created and applied to the specified interfaces based on your selections. The following policy configuration was created based on the above selections:

```
ip access-list standard wizard-ics
 remark Internet Connection Sharing
 permit any
```

```
ip access-list extended self
 remark Traffic to NetVanta
 permit ip any any log
```

```
ip access-list extended wizard-pfwd-1
 remark Port Forward 1
 permit tcp any host 10.10.10.1 eq www log
```

```
ip policy-class Private
 allow list self self
 nat source list wizard-ics interface ppp 1 overload
```

```
ip policy-class Public
 nat destination list wizard-pfwd-1 address 192.168.3.100
```

```
interface vlan 3
 ip address 192.168.3.1 255.255.255.0
 access-policy Private
```

```
interface vlan 4
 ip address 192.168.4.1 255.255.255.0
 access-policy Private
```

```
interface vlan 5
 ip address 192.168.5.1 255.255.255.0
 access-policy Private
```

```
interface ppp 1
 ip address 10.10.10.1 255.255.255.252
 access-policy Public
```

\* *Partial output displayed*

\* Remember to save your configuration to ensure the settings will not be lost after a restart.

# General Firewall

The NetVanta Firewall can be enabled or disabled from the General Firewall screen. You can also customize timeout intervals for protocols (TCP, UDP, ICMP) or specific services by listing the particular port number.

The screenshot shows the NetVanta 1224STR configuration interface. On the left is a navigation menu with categories: System, Switch, Router / Bridge, Firewall, VPN, and Utilities. The 'Firewall' section is selected, showing 'General Firewall' as the active page. The main content area is divided into two sections:

- Configuration for Firewall:** This section allows enabling or disabling the firewall and setting default timeout intervals for TCP (600), UDP (60), and ICMP (60). Arrows point to the 'Enable' checkbox and the timeout input fields.
- Add / Modify / Delete IP Policy-Timeouts:** This section allows creating custom inactivity timeouts for specific protocols and ports. The 'Add an IP Policy-Timeout' form shows 'TCP' selected for the protocol and 'bgp (179)' for the port type. An arrow points to the 'Timeout' input field.

At the bottom of the 'Add / Modify / Delete IP Policy-Timeouts' section, there is a table for 'Delete Entries' with columns for Protocol, Port, and Timeout. A message below the table states: "There are no port timeouts, other than default, that are set."

## Default protocol timeouts for all services

- TCP - 600
- UDP - 60
- ICMP - 60

# Security Zones

The Security Zones screen can be used to configure advanced firewall options that cannot be configured in the firewall wizard. A security zone contains one or more policies and can be applied to interfaces to allow, discard, or NAT traffic as it enters the NetVanta.

**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
Default	<none>	Public
ppp 5	<none>	Private
ppp 6	<none>	test
ppp 7	<none>	<none>

Reset Assign

**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.

**Modify Security Zones**

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

Security Zone	Active Sessions	
<a href="#">test</a>	0	Rename
<a href="#">Public</a>	0	Rename
<a href="#">Private</a>	0	Rename
<a href="#">&lt;Unused Security Zone 4&gt;</a>	0	Rename
<a href="#">&lt;Unused Security Zone 5&gt;</a>	0	Rename

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.

The Public and Private Security Zone listed above were created with the Firewall Wizard

*A security zone that has no configured policies will allow all traffic to enter the interface.*

## Private Security Zone – Traffic to NetVanta Policy

The Private Security Zone was created with the Firewall Wizard. Two policies were created. The *Traffic to NetVanta* policy allows all traffic entering the Private interface to reach the NetVanta.

The screenshot shows the NetVanta 1224STR configuration interface. On the left is a navigation menu with categories: System, Switch, Router / Bridge, Firewall, VPN, and Utilities. The main content area is titled "Security Zones > Security Zone 'Private'".

**Configure Policies for Security Zone 'Private'**

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'**

Buttons: Add Policy to 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
▲ ▼	<a href="#">Traffic to NetVanta</a>	Advanced <a href="#">Delete</a>
▲ ▼	<a href="#">NAT list wizard-ics</a>	Advanced <a href="#">Delete</a>

Traffic not matching one of the policies above will be blocked.

← Add another Policy to this Security Zone

**Modify Traffic to NetVanta Policy**

**Configuration for Policy 'Traffic to NetVanta' in Security Zone 'Private'**

Policy Type: Advanced *Allows low-level configuration of all policy parameters.*

Policy Description:  *Optional description for this policy*

**Advanced Policy Data**

Policy Action:  *This is the action that will be taken if a packet matches the entries specified below.*

Destination Security Zone:  *This allows you to specify that this action will be taken only if the traffic is destined for this specific SecurityZone.*

NAT Type:  Source with Overloading *If Source is selected, replaces source address with NAT IP Address. Translates source port if port in use by another session. If Destination is selected, replaces destination address with NAT IP Address.*

Destination

NAT IP Address:  Specified  *Packets arriving from Security Zone 'Private' will have either their source or destination address replaced with this IP Address*

Interface

Buttons: Cancel, Apply

← Allow packets that match selector below

← Allow packets if they are directed to the NetVanta

**Add / Modify / Delete Policy Traffic Selectors**

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

**Add New Traffic Selector**

Buttons: Add New Traffic Selector..

**Modify/Delete Traffic Selector**

Priority Type	Protocol	Source Network/Ports	Dest Network/Ports
<a href="#">Permit</a>	any	any	any <a href="#">Delete</a>

← Permit any traffic from anywhere going anywhere

# Private Security Zone – Traffic to NetVanta Policy – Modify Traffic Selector

The default traffic selector added to the Traffic to NetVanta Policy will permit all traffic from anywhere going anywhere.

**NetVanta 1224STR** Save Logout

Security Zones > Security Zone 'Private' > Policy 'Traffic to NetVanta' > Modify Custom Policy Entry

### Modify 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: . . . .

**Source Ports (TCP/UDP Only):**  Any  Well Known  Specified

**Destination Data**

**Destination Host/Network:**  Any  IP Address  
Address: . . . .  
Mask: . . . .

**Destination Ports (TCP/UDP Only):**  Any  Well Known  Specified

Cancel Apply

Annotations:

- Permit filter
- Define source of traffic
- Define destination of traffic



## Private Security Zone – NAT list wizard-ics

The Private Security Zone was created with the Firewall Wizard. Two policies were created. The *NAT list wizard-ics* policy provides Network Address Translation of the private to public IP addresses and is shown below. With the configuration below, all hosts in the Private Security Zone will share the public IP address assigned to the WAN interface.

**NetVanta 1224STR** Save Logout

Security Zones > Security Zone 'Private'

**Configure Policies for Security Zone 'Private'**

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'**

Add Policy to 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
▲ ▼	<a href="#">Traffic to NetVanta</a>	Advanced <a href="#">Delete</a>
▲ ▼	<a href="#">NAT list wizard-ics</a>	Advanced <a href="#">Delete</a>

Traffic not matching one of the policies above will be blocked.

← Add another Policy to this Security Zone

**Modify NAT Policy**

**Configuration for Policy 'NAT list wizard-ics' in Security Zone 'Private'**

Policy Type: Advanced *Allows low-level configuration of all policy parameters.*

Policy Description:  *Optional description for this policy*

**Advanced Policy Data**

Policy Action:  *This is the action that will be taken if a packet matches the entries specified below.*

Destination Security Zone:  *This allows you to specify that this action will be taken only if the traffic is destined for this specific SecurityZone.*

NAT Type:  Source with Overloading *If Source is selected, replaces source address with NAT IP Address. Translates source port if port in use by another session. If Destination is selected, replaces destination address with NAT IP Address.*

Destination

NAT IP Address:  Specified *Packets arriving from Security Zone 'Private' will have either their source or destination address replaced with this IP Address*

Interface

← NAT Policy

← Specify that all hosts will share Public IP

← Specify public IP Address

← Public IP Address will be address assigned to the selected interface

**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
<a href="#">Permit</a>	any	any	any <a href="#">Delete</a>

← Defined rules for traffic that will use this policy

## Public Security Zone – Port Forward Policy

The Public Security Zone was created with the Firewall Wizard. A Port Forwarding policy was added to allow a server (web, e-mail, etc.) on the private network to be accessed from the Internet. All other inbound traffic will be blocked. With the configuration bellow, all traffic destined for the Public IP address 10.10.10.1, and port 80 (www), will be forwarded in to the Private IP address 192.168.3.100. Since this is the only policy in the Public Security Zone, all other traffic will be blocked.

The screenshot shows the NetVanta 1224STR web interface. The left sidebar contains navigation menus for System, Switch, Router / Bridge, Firewall, VPN, and Utilities. The main content area is titled "Configure Policies for Security Zone 'Public'". It includes an "Add Policy to Zone 'Public'" button and a table of existing policies. A dashed arrow labeled "Modify Policy" points from the "Port Forward 1" entry in the table to the "Configuration for Policy 'Port Forward 1' in Security Zone 'Public'" screen. This configuration screen shows the following details:

- Policy Type: Port Forward
- Policy Description: Port Forward 1
- Public IP Address: 10.10.10.1 (ppp 1)
- Private IP Address: 192 . 168 . 3 . 100
- Forwarding options:  Forward only traffic specified below,  Forward All Traffic (inbound 1:1 NAT)
- Protocols/Ports to Forward: tcp, www (80)

Annotations with arrows point to the "Add Policy to Zone 'Public'" button and the "Port Forwarding Policy" configuration details.

# Creating Your Own Security Zone

You can create and define your own Security Zone by selecting one of the Unused Security Zones in the **Edit Security Zones** field. When you select an unused security zone, you are prompted to give it a name, select a policy type, and define policy parameters for your new Security Zone.

**ADIRAN NetVanta 1224STR** Save Logout

**System**  
Getting Started  
System Summary  
Physical Interfaces  
Passwords  
IP Services  
DHCP Server  
Hostname / DNS  
LLDP

**Switch**  
Ports  
Port Security  
Storm Control  
Link Aggregation  
VLANs  
Spanning Tree  
MAC Forwarding  
Class of Service  
Stacking

**Router / Bridge**  
Default Gateway  
Routing  
Route Table  
IP Interfaces  
QOS Maps  
Bridging

**Firewall**  
Firewall Wizard  
General Firewall  
Security Zones

**VPN**  
VPN Wizard  
VPN Peers  
Certificates

**Utilities**  
Port Mirroring  
Configuration  
Firmware  
Reboot Unit  
Telnet To Unit

**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
Default	<none>	Public
ppp 5	<none>	Private
ppp 6	<none>	test
ppp 7	<none>	<none>

Reset Assign

**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.

**Modify Security Zones**

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

Security Zone	Active Sessions	
<a href="#">test</a>	0	Rename
<a href="#">Public</a>	0	Rename
<a href="#">Private</a>	0	Rename
<a href="#">&lt;Unused Security Zone 4&gt;</a>	0	Rename
<a href="#">&lt;Unused Security Zone 5&gt;</a>	0	Rename

1) Select Unused Security

**Configure Security Zone Name**

Name:

*This is a descriptive name for the security zone for easy reference later.*

Cancel Apply

2) Name the Security Zone

**Configure Policies for Security Zone 'DMZ'**

New policies can be added to Security Zone 'DMZ' 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 'DMZ'**

Add Policy to Zone 'DMZ'

**Modify/Delete Policies in Security Zone 'DMZ'**

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

Priority	Description	Action
	<a href="#">There are no configured policies; all traffic from Security Zone 'DMZ' will be blocked.</a>	

3) Click to add policy to Security Zone

## Creating Your Own Security Zone (Continued...)

After selecting the **Add Policy to Zone** <Zone Name>, select the policy type that you wish to create. A brief description of each policy type is displayed.

The screenshot shows the NetVanta 1224STR web interface. On the left is a navigation menu with categories: System, Switch, Router / Bridge, Firewall, VPN, and Utilities. The main content area is titled "Security Zones > Security Zone 'DMZ'".

The "Configure Policies for Security Zone 'DMZ'" section contains a text box explaining that new policies can be added by clicking the "Add Policy" button. Below this is a button labeled "Add Policy to Zone 'DMZ'".

The "Modify/Delete Policies in Security Zone 'DMZ'" section contains a table with columns for Priority, Description, and Action. The table is currently empty, with a message: "There are no configured policies; all traffic from Security Zone 'DMZ' will be blocked." A dashed arrow labeled "Add Policy" points from the button in the previous section to the "Add New Policy -- Select Policy Type" dialog box.

The "Add New Policy -- Select Policy Type" dialog box has a "Policy Type" dropdown menu set to "Select a policy type...". To the right of the dropdown is a note: "Select which policy type to create, then click Continue." Below this is a section titled "Policy Types Explained" with the following items:

- Port Forward:** Allows hosts from the 'DMZ' Security Zone to access all or selected ports on a private server in another Security Zone. Depending on the configuration, a Port Forward will NAT a public IP Address to a private IP Address for all protocols and ports or just a subset, like TCP/FTP and TCP/WWW. Typically used when Security Zone 'DMZ' is applied to interfaces connected to the Internet.
- Many:1 NAT:** Allows hosts from the 'DMZ' Security Zone to share a single public IP address for Internet access. Also known as Internet connection sharing. Typically used when Security Zone 'DMZ' is applied to interfaces connected to a private (local) network.
- Admin Access:** Used to allow administrative access to the NetVanta from hosts in the 'DMZ' Security Zone.
- Filter:** Blocks specified traffic from the 'DMZ' Security Zone from entering any other Security Zone.
- Allow:** Allows specified traffic from the 'DMZ' Security Zone to continue toward all other Security Zones unaffected.
- Advanced:** Allows low-level configuration of all policy parameters.

At the bottom of the dialog box is a note: "Note: A '1:1 NAT' may be emulated by configuring a Port Forward (of all ports) on the 'DMZ' Security Zone and a Many:1 NAT (with single private IP address) on the Security Zone in which the server is located." Below the note are "Cancel" and "Continue" buttons.

Annotations on the right side of the image:

- 4) Select the policy type that you wish to create (pointing to the Policy Type dropdown)
- 5) Assign policy parameters based to your new policy (pointing to the Policy Types Explained section)

## Policy Type – Port Forwarding

Allows hosts from the 'current' Security Zone to access all or selected ports on a private server in another Security Zone. Depending on the configuration, a Port Forward will NAT a public IP Address to a private IP Address for all protocols and ports or just a subset, like TCP/FTP and TCP/WWW. This is used when this Security Zone is applied to interfaces connected to the Internet.

The screenshot shows the configuration window for a Port Forwarding policy. The 'Policy Type' is set to 'Port Forward'. The 'Public IP Address' is 192.168.1.1 (eth 0/4). The 'Private IP Address' is 10.10.10.1. The 'Forward only traffic specified below' option is selected. The 'Protocols/Ports to Forward' table has one row with 'tcp' and 'www (80)'. The 'Apply' button is highlighted.

Protocol	Matching Ports
tcp	www (80)
< Add protocol/port >	<-- To add a row, select a protocol from the list.

## Policy Type – Many:1 / NATP

Allows hosts from the Security Zone that you are editing to share a single public IP address for Internet access. Also known as Internet connection sharing. Typically used when this Security Zone is applied to interfaces connected to a private (local) network.

The screenshot shows the configuration window for a Many:1 NATP policy. The 'Policy Type' is set to 'Many:1 NATP'. The 'Many:1 NATP Data' section has the 'Allow all hosts in the Private Security Zone to share the Public IP Address' option selected. The 'Public IP Address' is 192.168.1.1 (vlan 1). The 'Apply' button is highlighted.

## Policy Type – Admin Access

Used to allow administrative access to the NetVanta from hosts in this Security Zone.

**Add New Policy to Security Zone 'DMZ'**

Policy Type:  *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:  HTTP  SSH  
 HTTPS  SNMP *These are the methods used to access the NetVanta remotely.*  
 FTP  Telnet  
 Ping

## Policy Type – Filter

Blocks specified traffic from this Security Zone from entering any other Security Zone.

Policy Type:  *Blocks specified traffic from entering the Netvanta.*

Policy Description:  *Optional description for this policy*

**Filter Data**

Protocol:   *Protocol description*

Source IP Address/Mask:  Any  
 Specified *If specified, limits this filter to packets originating from matching IP addresses*

Address:  .  .  .   
Mask:  .  .  .

Filtered Ports (TCP and UDP only):  Any  
 Well Known   
 Specified *If specified, limits this filter to packets destined for the specified ports*

to

Destination IP Address/Mask:  Any  
 Specified *If specified, limits this filter to packets destined for matching IP addresses*

Address:  .  .  .   
Mask:  .  .  .

## Policy Type – Allow

Allows specified traffic from this Security Zone to continue toward all other Security Zones unaffected.

Policy Type: <input type="text" value="Allow"/>	<i>Allows specified traffic to continue toward its destination unaffected.</i>
Policy Description: <input type="text"/>	<i>Optional description for this policy</i>
<b>Allow Data</b>	
Source IP Address/Mask: <input type="radio"/> Any <input type="radio"/> Specified Address: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> Mask: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<i>If specified, only allows packets originating from matching IP addresses</i>
Destination IP Address/Mask: <input type="radio"/> Any <input type="radio"/> Specified Address: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> Mask: <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	<i>If specified, only allows packets destined for matching IP addresses</i>
Protocol: <input type="text" value="any"/> <input type="text"/>	<i>If specified, only allows packets that correspond to the specified protocol.</i>
Allowed Ports (TCP and UDP only): <input type="radio"/> Any <input type="radio"/> Well Known <input type="text"/> <input type="radio"/> Specified <input type="text"/> to <input type="text"/>	<i>If specified, only allows packets destined for the specified ports</i>
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	

## Policy Type – Advanced

Allows low-level configuration of all policy parameters.

<b>Add New Policy to Security Zone 'DMZ'</b>	
Policy Type: <input type="text" value="Advanced"/>	<i>Allows low-level configuration of all policy parameters.</i>
Policy Description: <input type="text"/>	<i>Optional description for this policy</i>
<b>Advanced Policy Data</b>	
Policy Action: <input type="text" value="Allow"/>	<i>This is the action that will be taken if a packet matches the entries specified below.</i>
Destination Security Zone: <input type="text" value="&lt;Any Security Zone&gt;"/>	<i>This allows you to specify that this action will be taken only if the traffic is destined for this specific SecurityZone.</i>
NAT Type: <input type="radio"/> Source with Overloading <input type="radio"/> Destination	<i>If Source is selected, replaces source address with NAT IP Address. Translates source port if port in use by another session. If Destination is selected, replaces destination address with NAT IP Address.</i>
NAT IP Address: <input type="radio"/> Specified <input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/> <input type="radio"/> Interface <input type="text" value="vlan 1"/>	<i>Packets arriving from Security Zone 'DMZ' will have either their source or destination address replaced with this IP Address</i>
<input type="button" value="Cancel"/> <input type="button" value="Apply"/>	