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 disable 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.

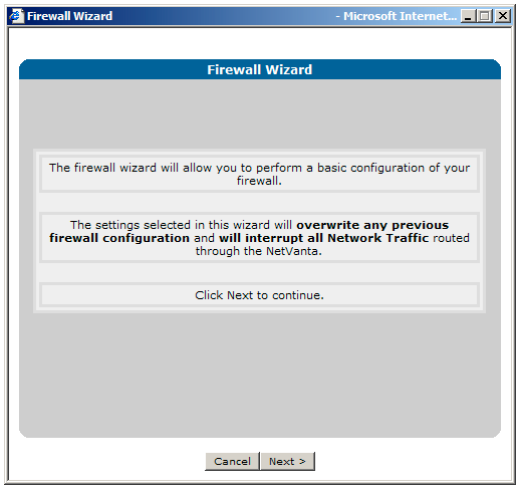
Firewall Wizard

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.

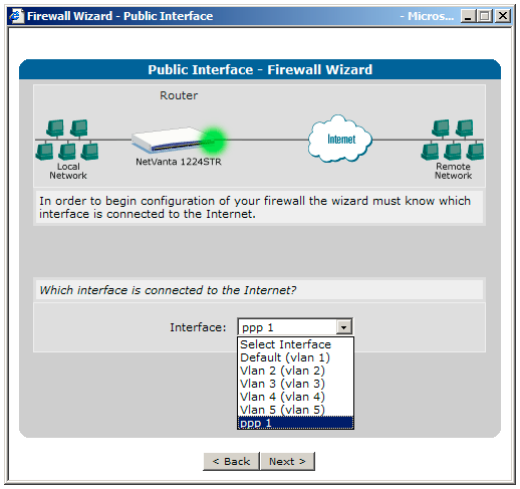
WARNING! - *The Firewall Wizard should only be used for the initial firewall configuration. It will overwrite any existing firewall policies and temporarily interrupt all Network Traffic. The Security Zones area of the firewall can be used to modify existing firewall policies.*

Using the Firewall Wizard

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

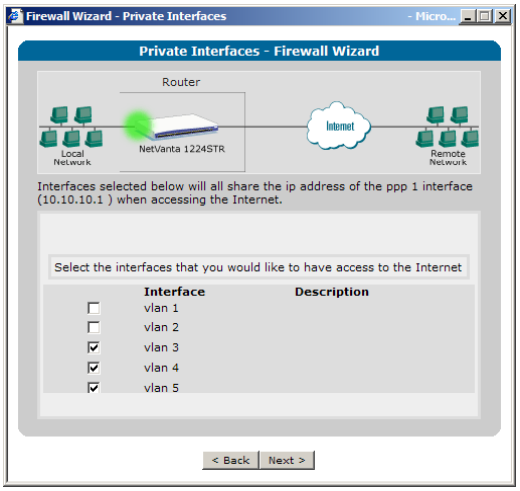


2) Choose the interface that is connected to the Internet. This will be the Public interface.

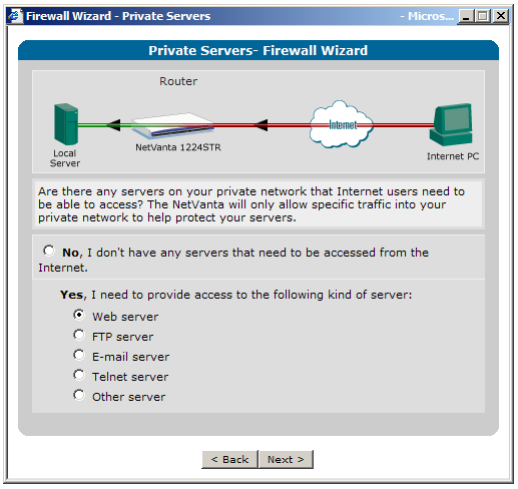


Using the Firewall Wizard (*Continued*…)

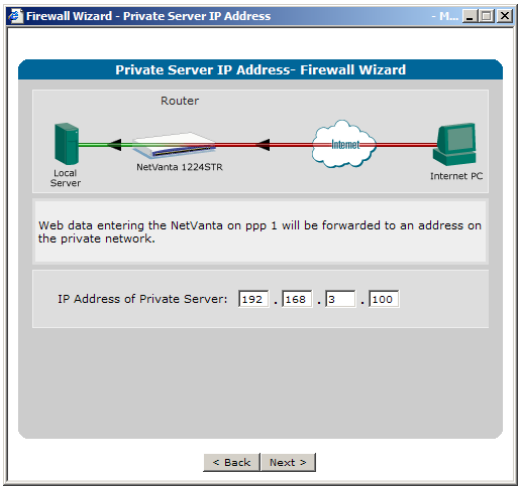
3) Select all the Private interfaces that will use the Public interface to get out to the Internet.



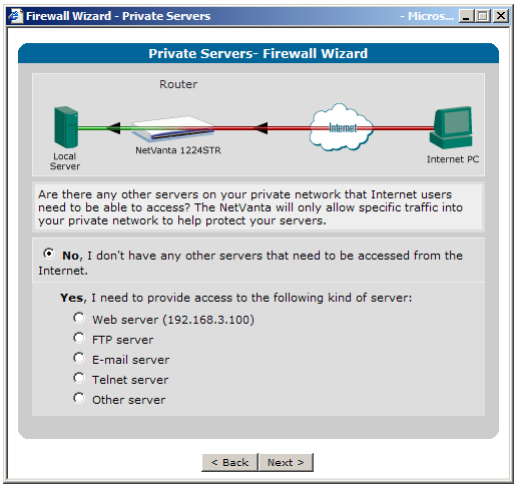
4) Specify the server (if any) on your Private network that you want to allow access to from the Internet.



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

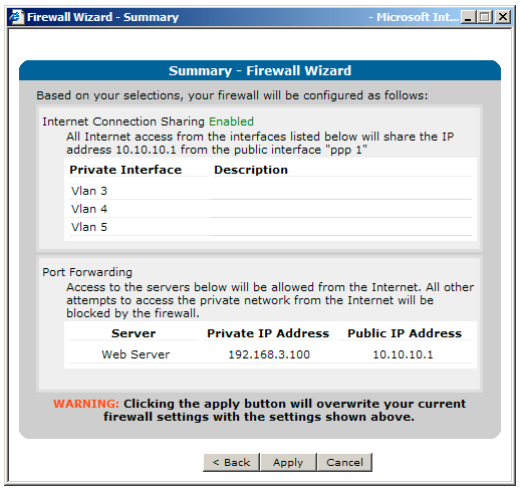


6) Identify any other servers that will be located on the Private network. (if any)

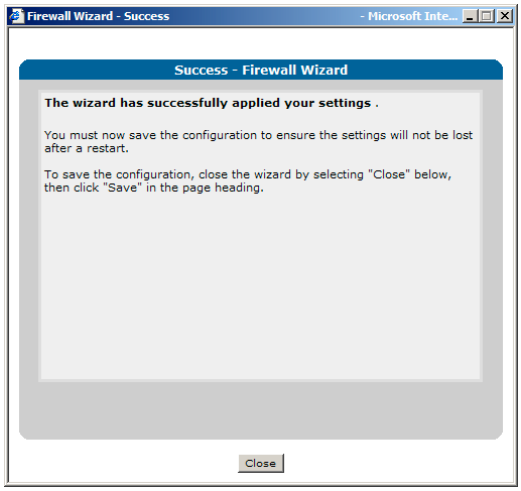


Using the Firewall Wizard (*Continued…*)

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:

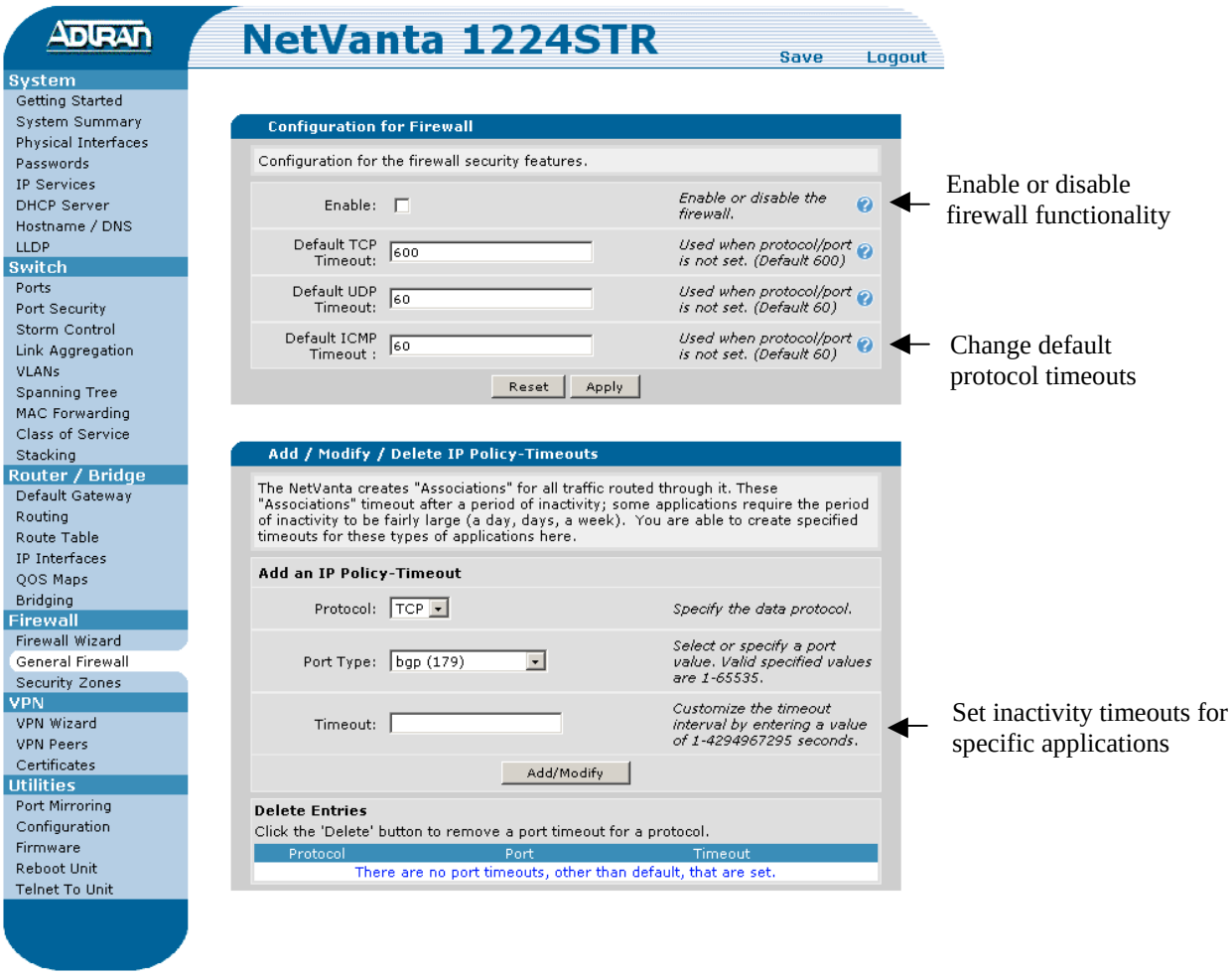
```
ip access-list standard wizard-ics
  remark Internet Connection Sharing
  permit any

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 disable 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.

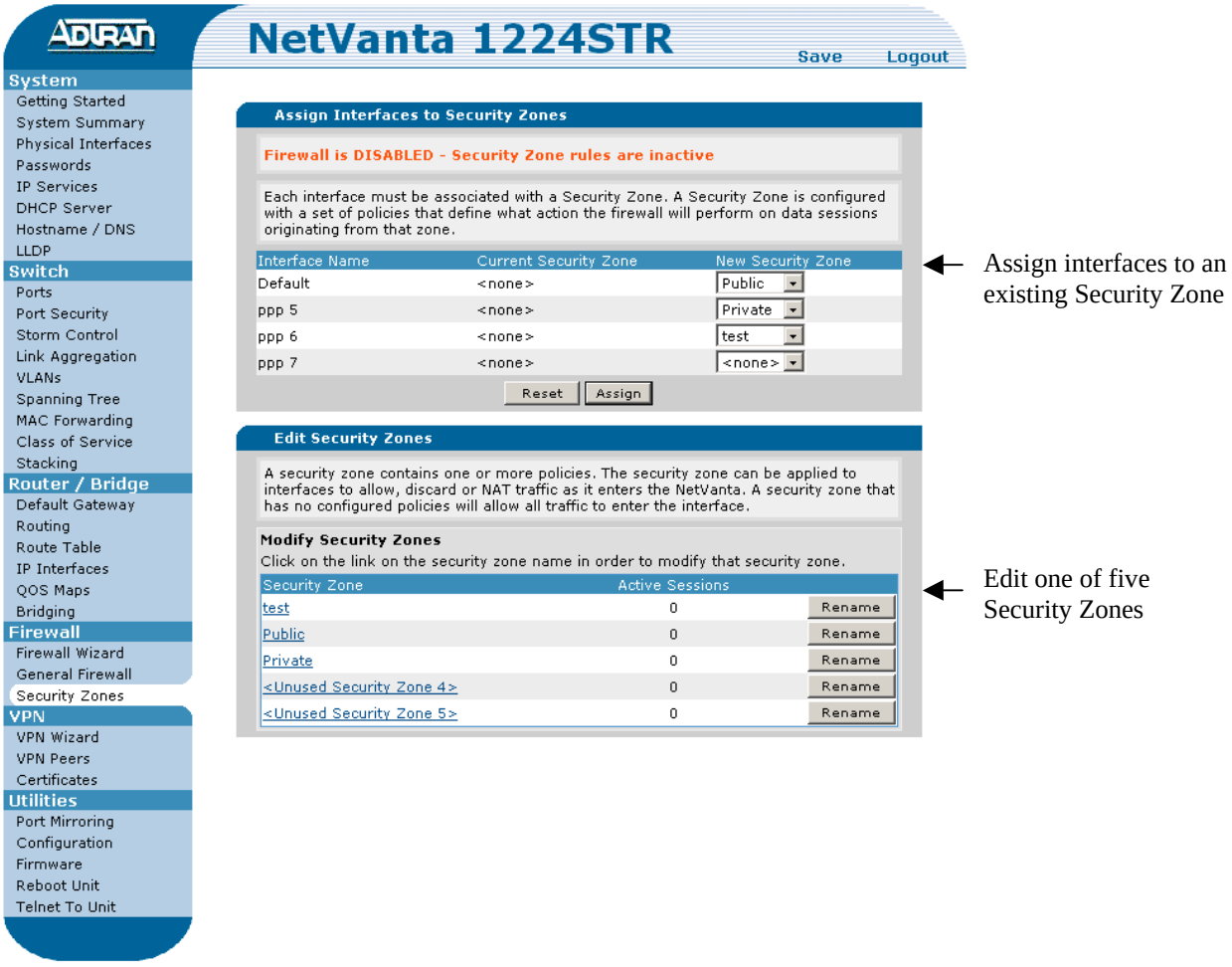


Default protocol timeouts for all services

- 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.



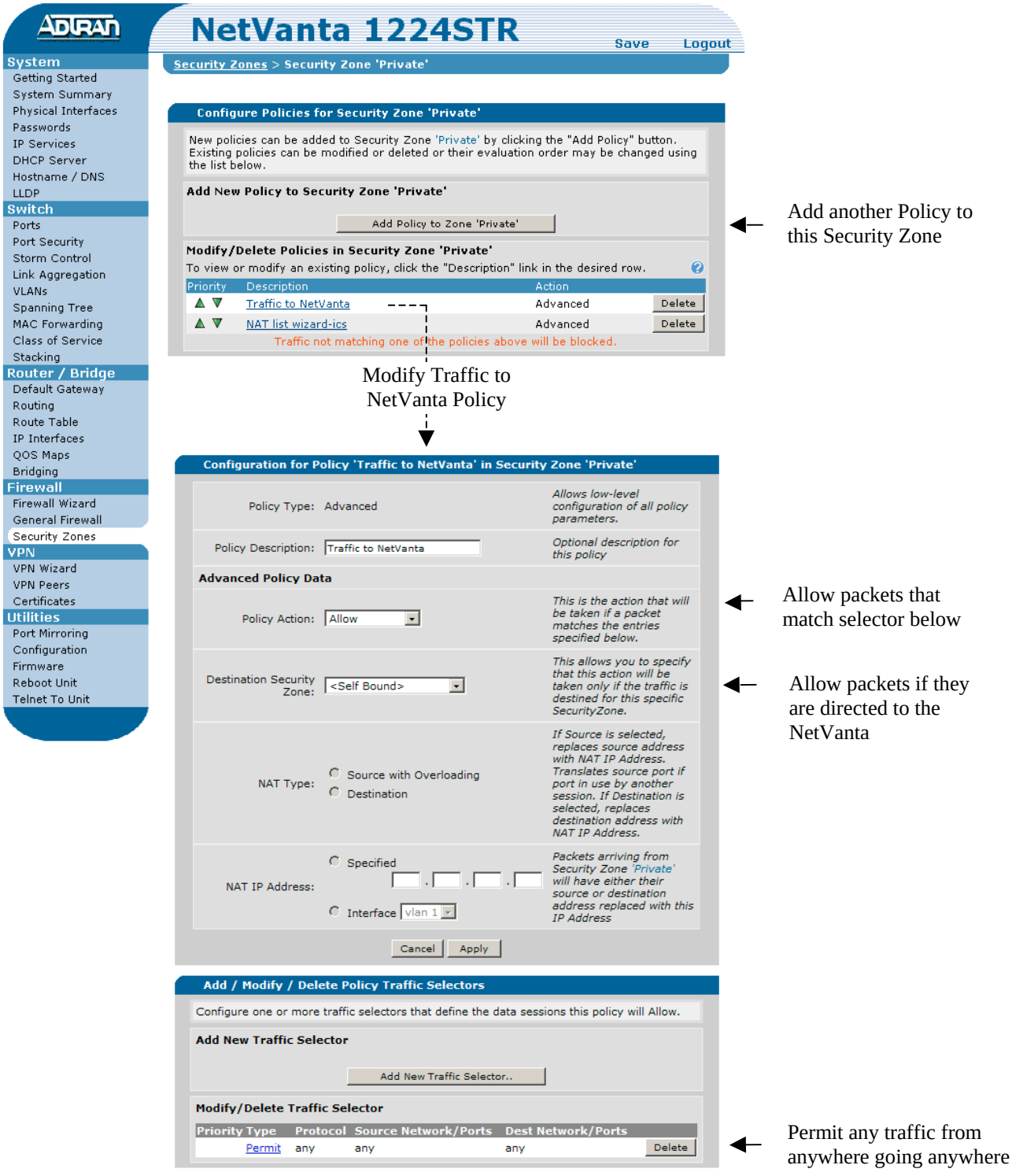
Each interface must be associated with a Security Zone. A Security Zone is configured with a set of policies that define what action the firewall will perform on data sessions **originating** from that zone.

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.



Add another Policy to this Security Zone

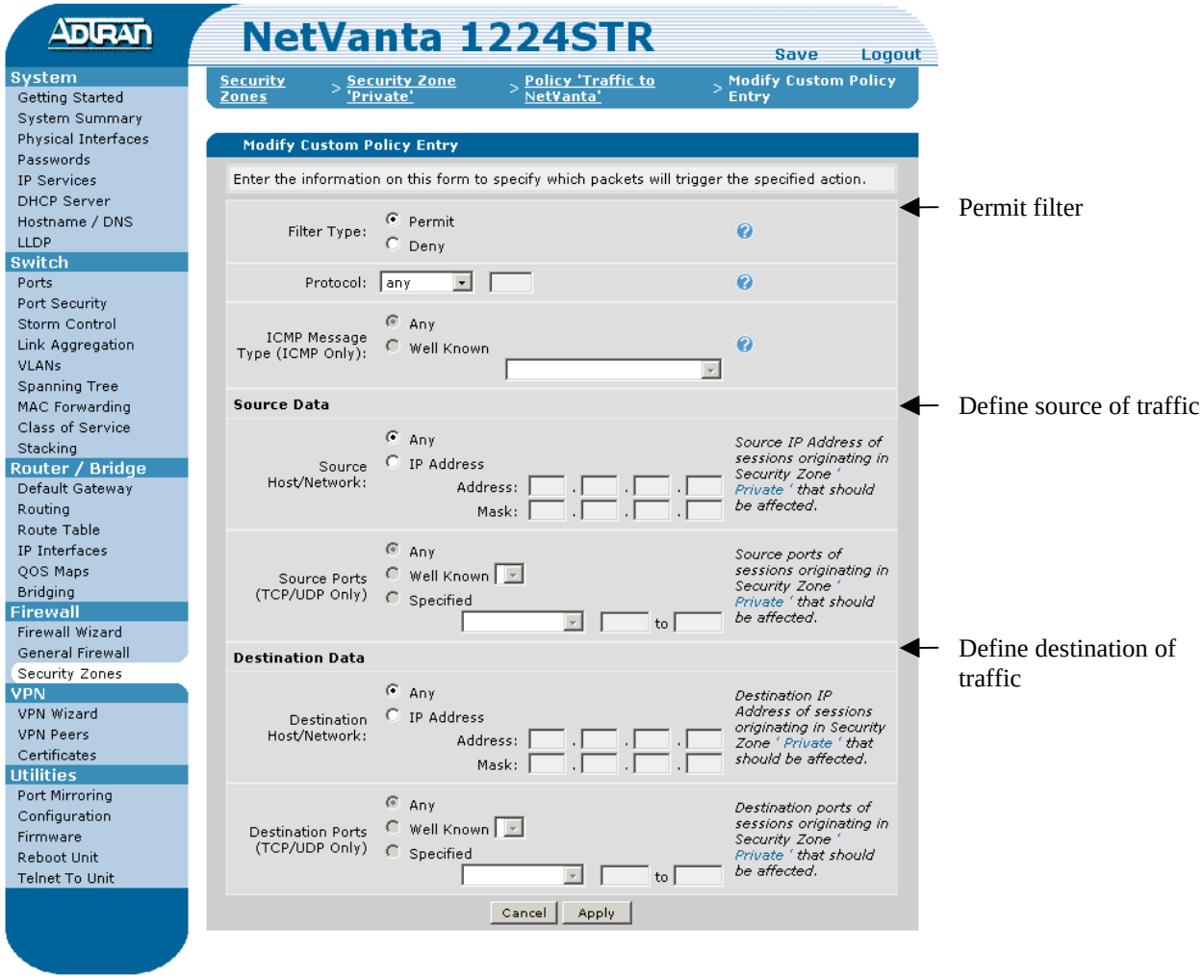
Allow packets that match selector below

Allow packets if they are directed to the NetVanta

Permit any traffic from anywhere going anywhere

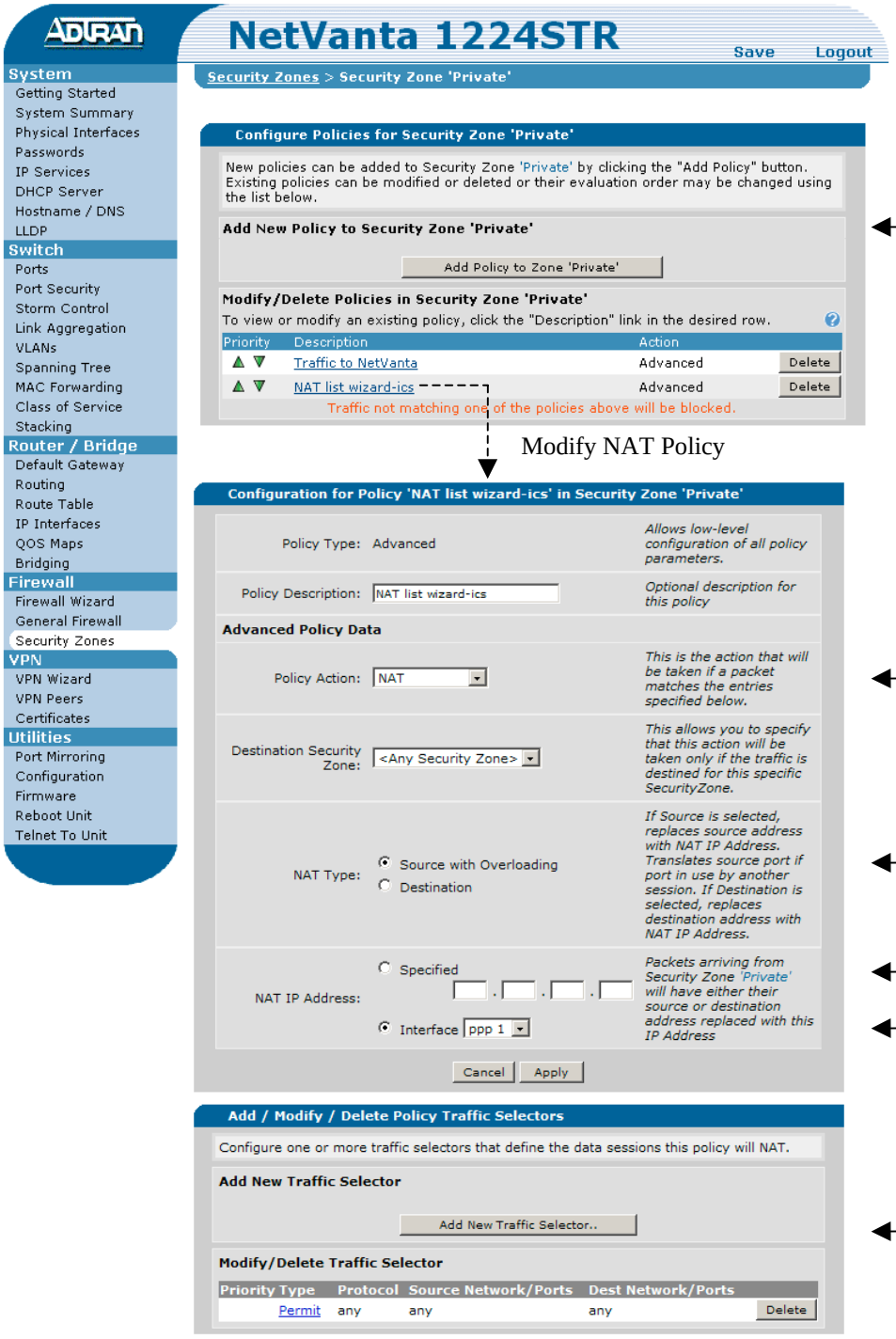
Private Security Zone – *Traffic to NetVanta Policy – Modify Traffic Selector*

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



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.



← Add another Policy to this Security Zone

← NAT Policy

← Specify that all hosts will share Public IP

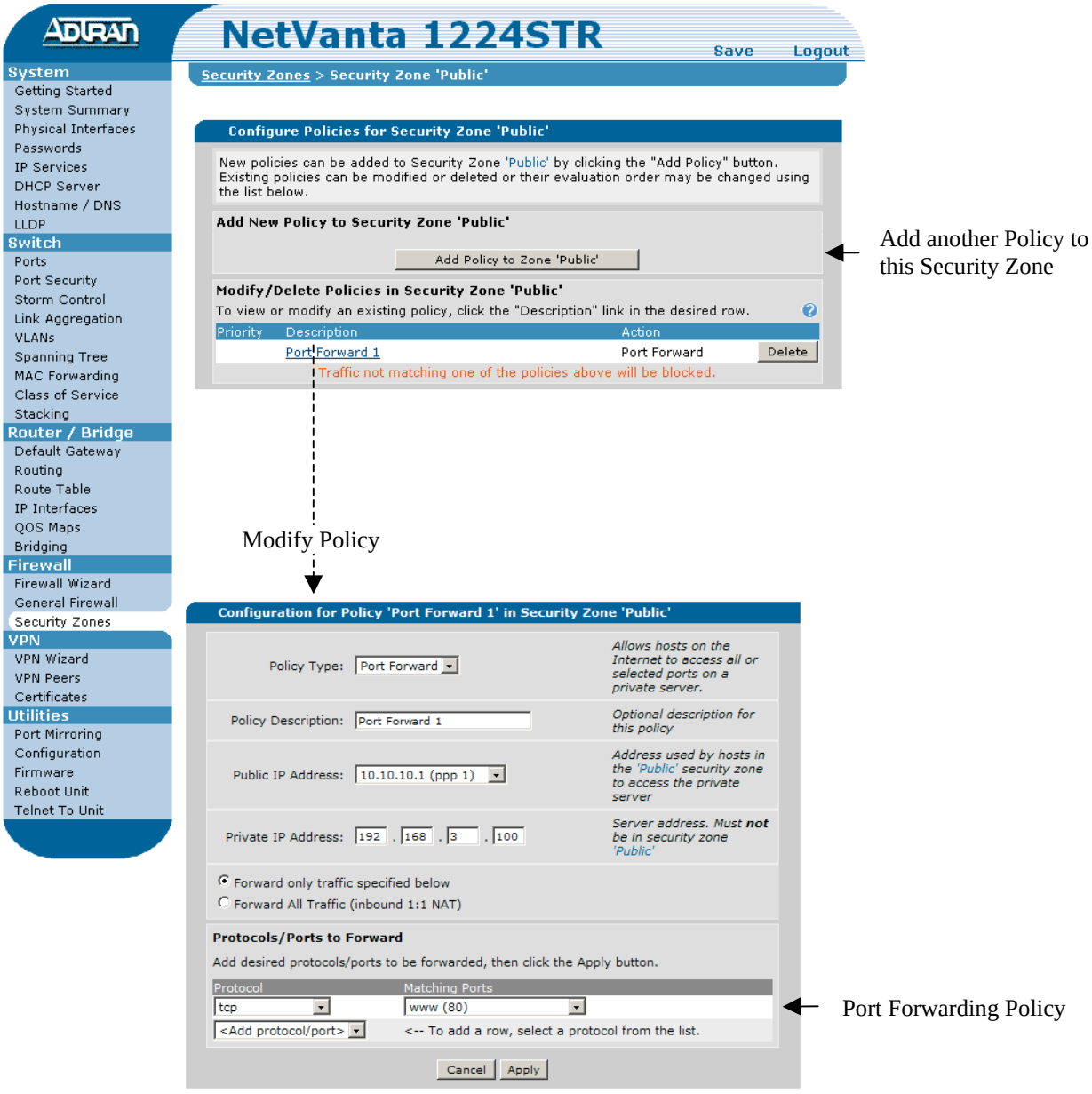
← Specify public IP Address

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

← Defined rules for traffic that will use this policy

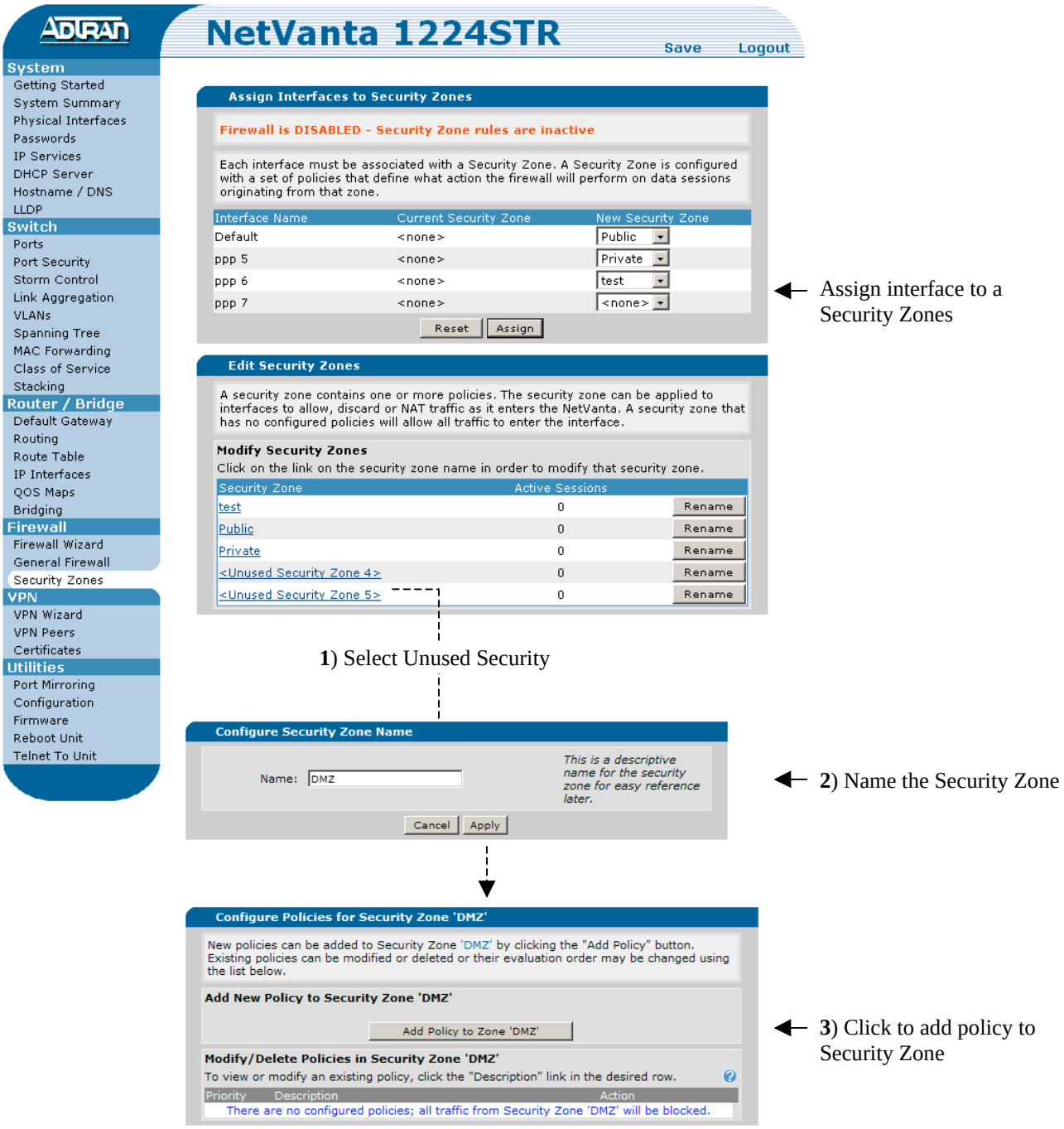
Public Security Zone – *Port Forward Policy*

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 otther traffic will be blocked.



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.



Assign interface to a Security Zones

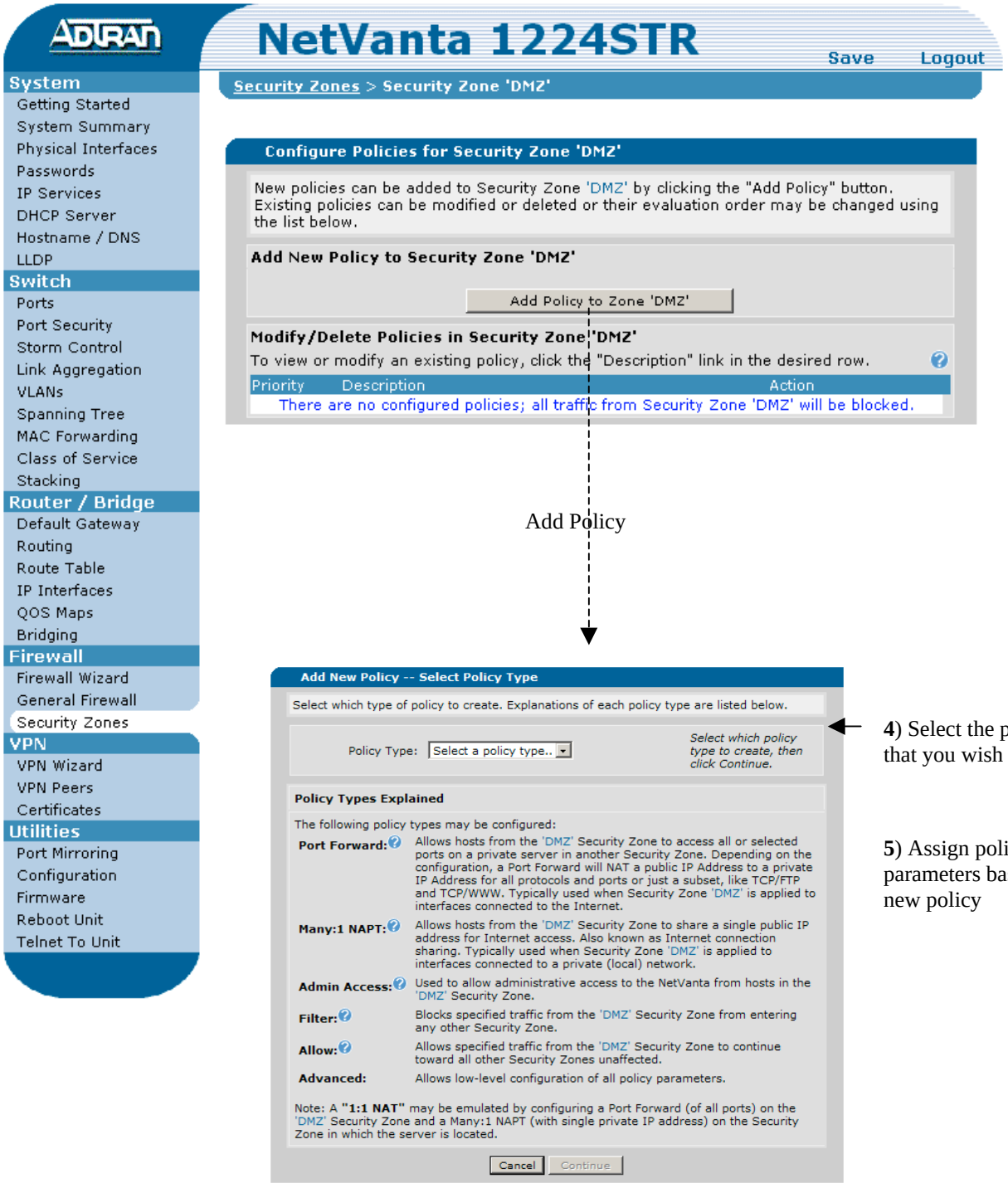
1) Select Unused Security

2) Name the Security Zone

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.

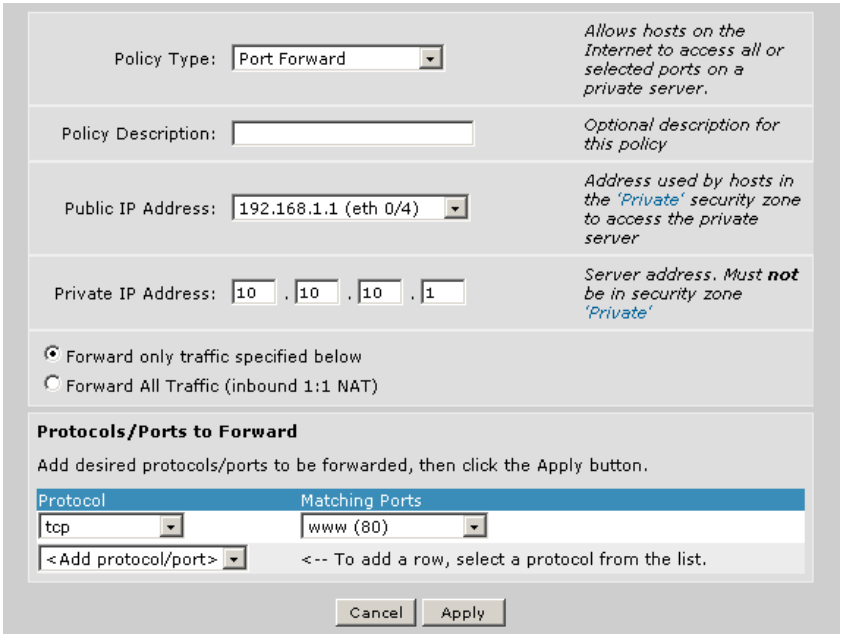


4) Select the policy type that you wish to create

5) Assign policy parameters based to your new policy

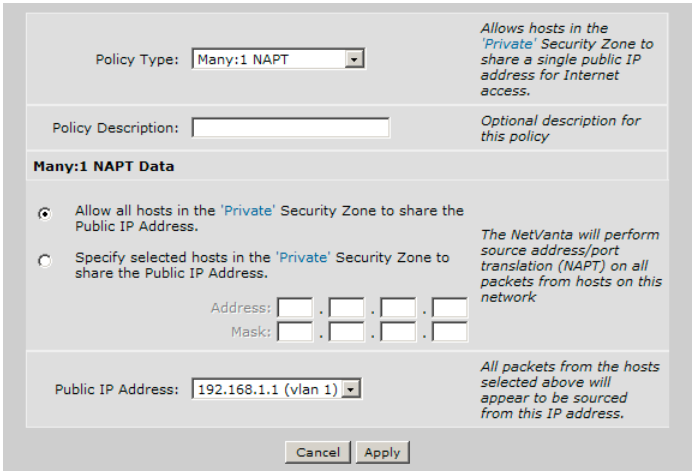
Policy Type – Port Forwarding

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.



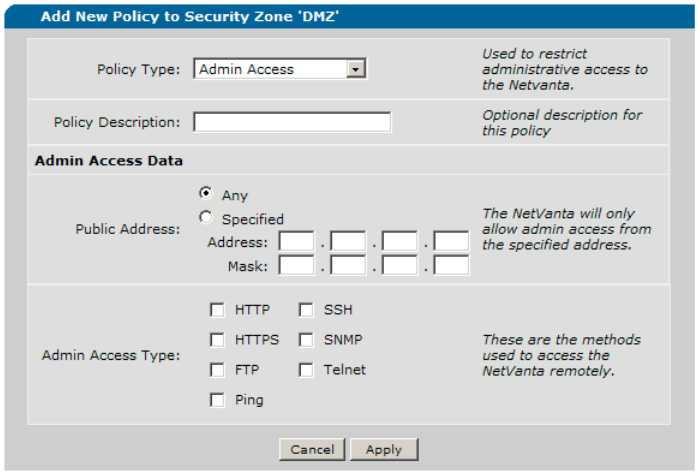
Policy Type – Many:1 / NAPT

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.



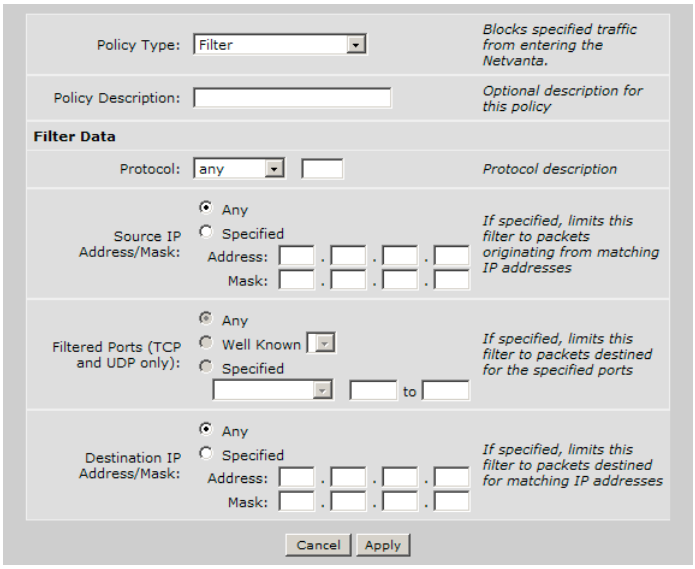
Policy Type – Admin Access

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



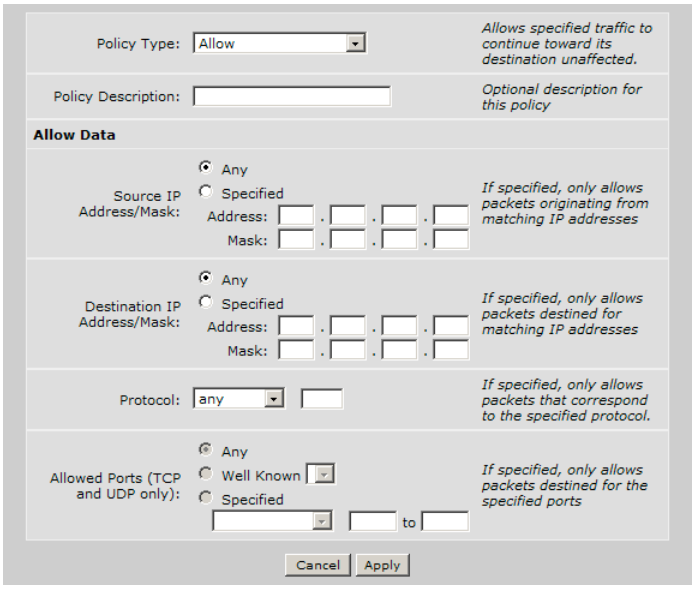
Policy Type – Filter

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



Policy Type – Allow

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



Policy Type – Advanced

Allows low-level configuration of all policy parameters.