NetVanta 2000 Series Technical Note

How to Open HTTP or HTTPS traffic to a webserver behind the NetVanta 2000 Series unit (Enhanced OS)

NOTE *This document is applicable to NetVanta 2600 series, 2700 series, and 2800 series units.*

Feature/Application:

Manually opening Ports to allow Webserver traffic (HTTP or HTTPS) from Internet to a server behind the NetVanta 2000 Series unit in the Enhanced OS involves the following steps:

Step 1: Creating the necessary Address Objects

Step 2: Defining the appropriate NAT Policies (Inbound, Outbound and Loopback)

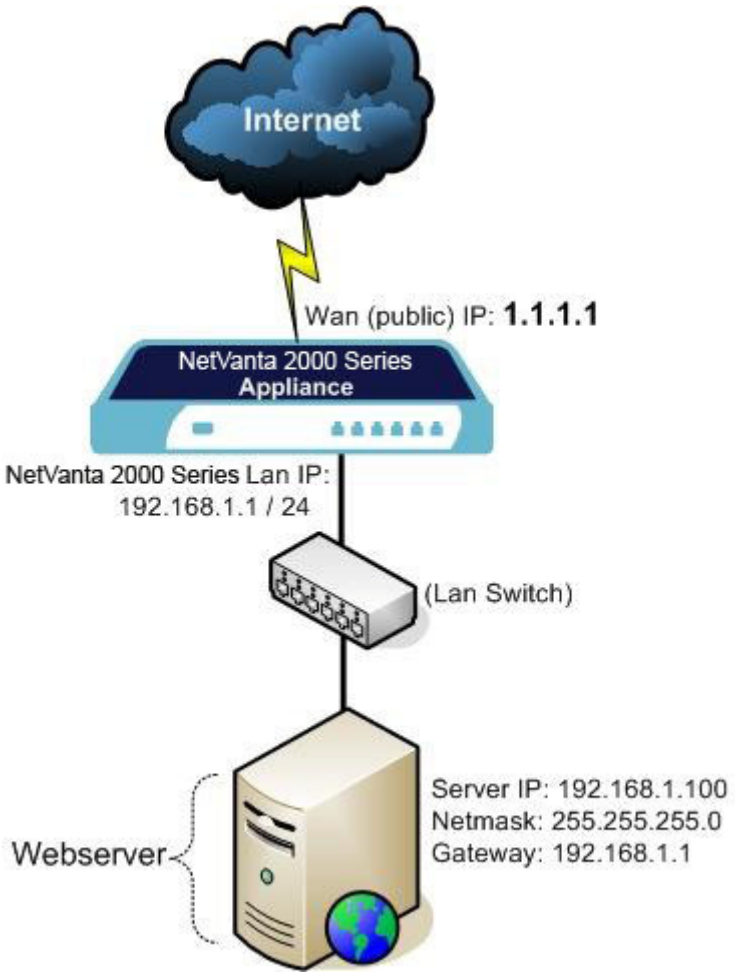
Step 3: Creating the necessary WAN > Zone Access Rules for public access

Recommendation: The Public Server Wizard quickly configure your the NetVanta 2000 Series to provide public access to an internal server. The Public Server Wizard is the most ambitious and functional wizard developed to date. It simplifies the complex process of creating a publicly and internally accessible server resource by automating above mentioned steps.

Alert: The NetVanta 2000 Series security appliance can be managed using HTTP (Port 80) or HTTPS (443) and a Web browser. Both HTTP and HTTPS are enabled by default. If you are using the NetVanta 2000 Series WAN IP address for HTTP or HTTPS port forwarding to a server, then the **default Management port** must be changed to another unused port number (e.g. 8080, 444, 4443, etc.). You can change this under the **System > Administration** page.

Scenario:

The following example covers allowing **HTTP (webserver)** service from the Internet to a server on the LAN with private IP address as **192.168.1.100**. Once the configuration is complete, Internet users can access the HTTP (webserver) service behind the NetVanta 2000 Series UTM appliance through the **WAN (Public) IP** address **1.1.1.1**.



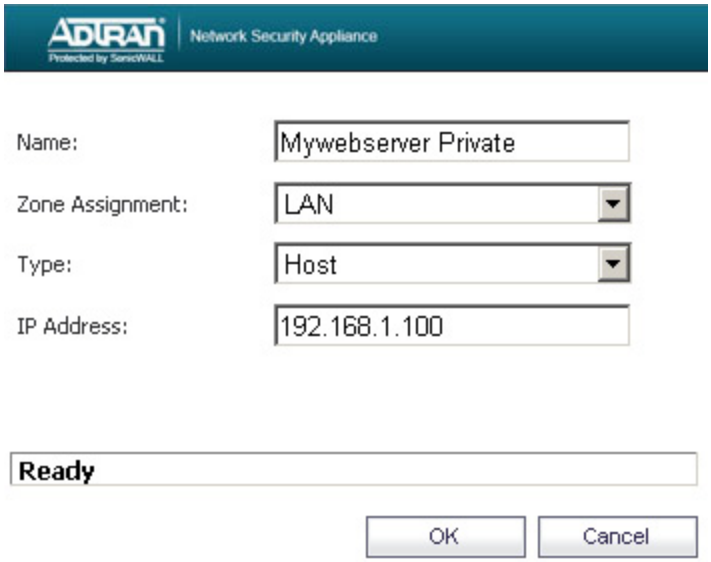
Procedure:

In this example we have chosen to demonstrate using HTTP service, however the following steps apply to any service you wish to use (like HTTPS, SMTP, FTP, Terminal Services, SSH, etc).

Step 1: Creating the necessary Address Objects

1. Select **Network > Address Objects**.

2. Click the **Add a new address object** button and create two address objects one for **Server IP on LAN** and another for **Public IP** of the server:

Address Object for Server on LAN Name: **Mywebserver Private** Zone Assignment: **LAN** Type: **Host** IP Address: **192.168.1.100**	

Address Object for Server's Public IP Name: **Mywebserver Public** Zone Assignment: **WAN** Type: **Host** IP Address: **1.1.1.1**	

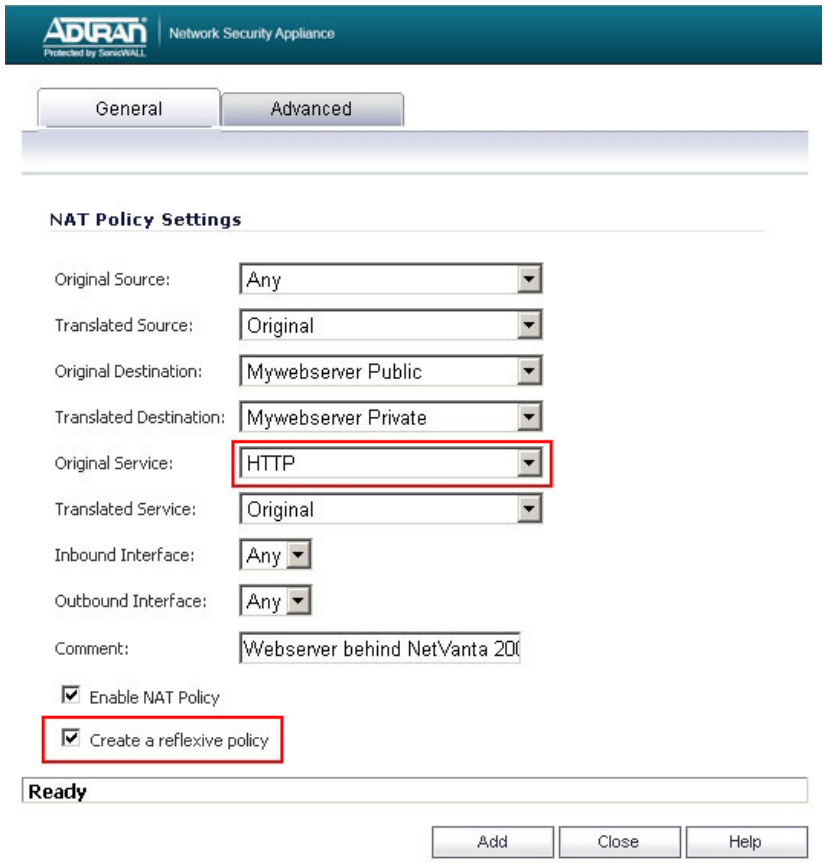
3. Click the **OK** button to complete creation of the new address objects.

Step 2: Defining the appropriate NAT Policies

1. Select **Network > NAT Policies**.

2. Click the **Add a new NAT Policy** button and chose the following settings from the drop-down menu:

Understanding how to use NAT policies starts with the construction of an IP packet. Every packet contains addressing information that allows the packet to get to its destination, and for the destination to respond to the original requester. The packet contains (among other things) the requester's IP address, the protocol information of the requestor, and the destination's IP address. The NAT Policies engine in SonicOS Enhanced can inspect the relevant portions of the packet and can dynamically rewrite the information in specified fields for incoming, as well as outgoing traffic.

Adding appropriate NAT Policies Original Source: **Any** Translated Source: **Original** Original Destination: **Mywebserver Public** Translated Destination: **Mywebserver Private** Original Service: **HTTP** Translated Service: **Original** Inbound Interface: **Any** Outbound Interface: **Any** Comment: Webserver behind NetVanta 2000 Series. Enable NAT Policy: **Checked** Create a reflexive policy: **Checked**	

If you have more than WAN interface on your UTM device, you will want to specify it (e.g., X1, X2, etc.) as the Inbound Interface in your inbound NAT Policy.

> ***Create a reflective policy:*** *When you check this box, a mirror outbound or inbound NAT policy for the NAT policy you defined in the Add NAT Policy window is automatically created.*

3. Click the **Add** button.

Loopback Policy:

If you wish to access this server from other internal zones using the Public IP address Http://1.1.1.1 consider creating a **Loopback NAT Policy** else go to next step:

- **Original Source:** Firewalled Subnets
- **Translated Source:** Mywebserver Public
- **Original Destination:** Mywebserver Public
- **Translated Destination:** Mywebserver Private
- **Original Service:** HTTP
- **Translated Service:** Original
- **Inbound Interface:** Any
- **Outbound Interface:** Any
- **Comment:** Loopback policy
- **Enable NAT Policy:** Checked
- **Create a reflexive policy:** unchecked

4. Upon completion under **Network > Nat Policies** tab the above **Inbound** and **Outbond NAT** policies will be created.

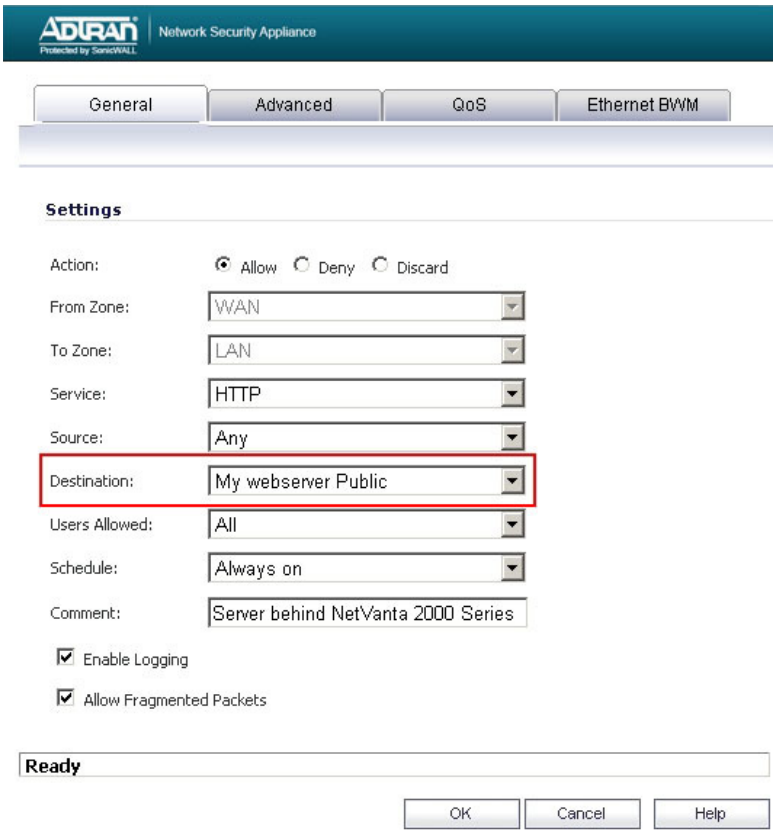
Step 3: Creating Firewall Access Rules

1. Click **Firewall > Access Rules** tab.

2. Select the type of view in the **View Style** section and go to **WAN to LAN** access rules.

3. Click **Add a new entry** and create the rule by entering the following into the fields:

> **CAUTION** *The ability to define network access rules is a very powerful tool. Using custom access rules can disable firewall protection or block all access to the Internet. Use caution when creating or deleting network access rules.*

Action: **Allow** From Zone: **WAN** To Zone: **LAN** Service: **HTTP** Source: **Any** Destination: **My webserver Public** Users Allowed: **All** Schedule: **Always on** Enable Logging: **checked** Allow Fragmented Packets: **checked**	

4. Under the **Advanced** tab, you can leave the "**Inactivity Timeout in Minutes**" at 15 minutes. Some protocols, such as Telnet, FTP, SSH, VNC and RDP can take advantage of longer timeouts where increased values like 30 or 60 minutes can be tried with caution in those cases. Longer timeout values will not help at all for HTTP or HTTPS.

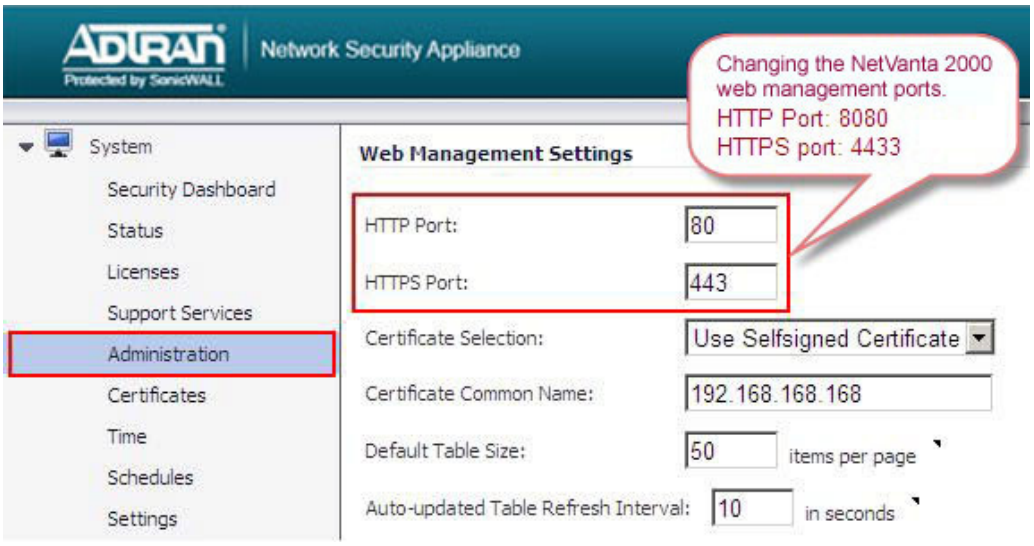
5. Click **OK**.

How to Test:

- **Testing from within the private network:** Try to access the webserver through its private IP address (Http://192.168.1.100) to ensure it is working from within the private network itself.
- From the Webserver, access the following website Http://www.whatismyip.com to verify the webserver's Public IP address.
- **Testing from the Internet:** Login to a computer on the Internet and try to access the web-server by entering the public IP (Http://1.1.1.1) in the Browser address bar.

Troubleshooting:

- Ensure that the Webserver's Default Gateway IP address is the NetVanta 2000 Series's LAN IP address.
- Ensure that the Webserver is able to access the Internet.
- **Changing the NetVanta 2000 Series web management port:** the NetVanta 2000 Series security appliance can be managed using HTTP port: 80 or HTTPS port: 443 and a Web browser. Both HTTP and HTTPS are enabled by default, but you can configure access through another port. Type the number of the desired port in the **Port field** on the **System > Administration** page and click **Accept**. However, if you configure another port for HTTP management, you must include the port number when you use the IP address to log into the NetVanta 2000 Series appliance, For example, if you configure the port to be 8080, then you must type <LAN IP Address>:8080 into the Web browser, i.e. Http://192.168.1.1:8080.



- Ensure you do not have duplicate **NAT Policies** and **Firewall Access Rules** for your web-server.
- For further troubleshooting go to the NetVanta 2000 Series Logs under **Log > View** page and check for Alerts, Denied IP's, Dropped messages, etc.

