



NetVanta 2000 Series Technical Note

How to Open SMTP, IMAP or POP3 traffic to an Email Server behind the NetVanta 2000 Series (Enhanced OS)



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

Feature/Application:

Manually opening Ports to allow Email traffic (SMTP, IMAP or POP3) 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: Create a Service Group

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 NetVanta 2000 Series unit 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.

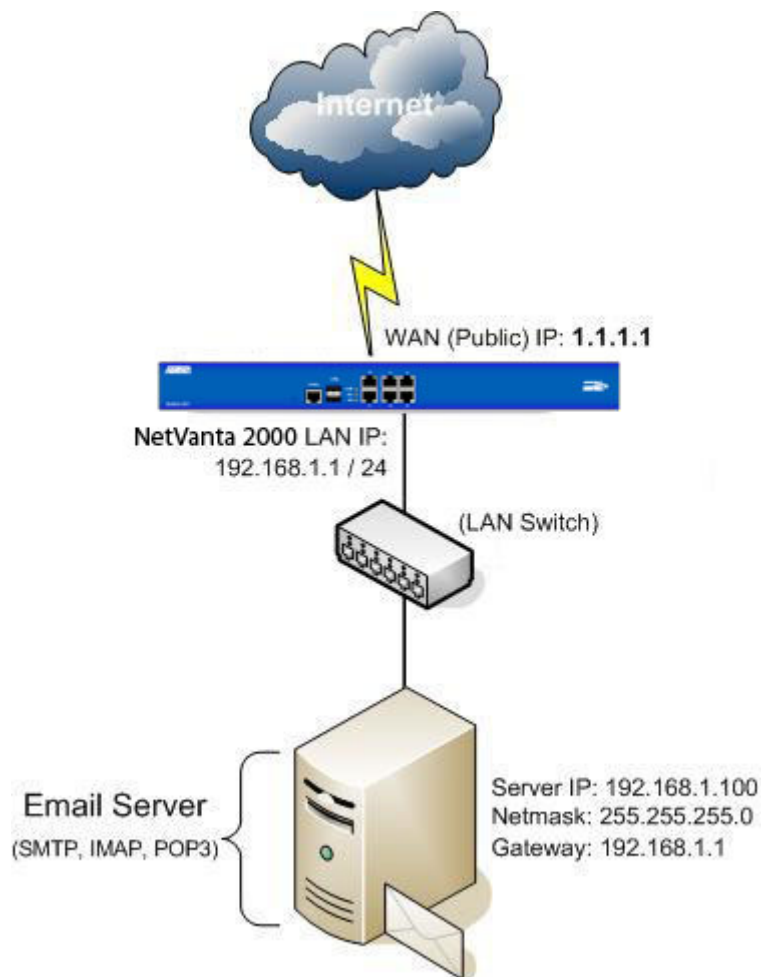
Scenario:

The following example covers allowing Email traffic (SMTP, IMAP or POP3) 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 Send emails to the Email Server behind the NetVanta 2000 Series UTM appliance through the **WAN (Public) IP** address **1.1.1.1**.



If you want to Open ports for OWA (Outlook Web Access), which is accessible on HTTP or HTTPS port then refer to ADTRAN Knowledge Base Article 3478.

Procedure:




Procedure:


In this example we have chosen to demonstrate using SMTP 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:

<p>Address Object for Server on LAN</p> <p>Name: MailServer Private</p> <p>Zone Assignment: LAN</p> <p>Type: Host</p> <p>IP Address: 192.168.1.100</p>	 <p>The screenshot shows a configuration dialog box for an ADTRAN Network Security Appliance. The title bar reads 'ADTRAN Network Security Appliance Protected by SonicWALL'. The dialog contains the following fields: 'Name' with the value 'MailServer Private', 'Zone Assignment' set to 'LAN', 'Type' set to 'Host', and 'IP Address' set to '192.168.1.100'. At the bottom, there is a 'Ready' status bar and two buttons: 'OK' and 'Cancel'.</p>
---	---

<p>Address Object for Server's Public IP</p> <p>Name: MailServer Public</p> <p>Zone Assignment: WAN</p> <p>Type: Host</p> <p>IP Address: 1.1.1.1</p>	 <p>The screenshot shows a configuration dialog box for an ADTRAN Network Security Appliance. The title bar reads 'ADTRAN Network Security Appliance Protected by SonicWALL'. The dialog contains the following fields: 'Name' with the value 'MailServer Public', 'Zone Assignment' set to 'WAN', 'Type' set to 'Host', and 'IP Address' set to '1.1.1.1'. At the bottom, there is a 'Ready' status bar and two buttons: 'OK' and 'Cancel'.</p>
---	--

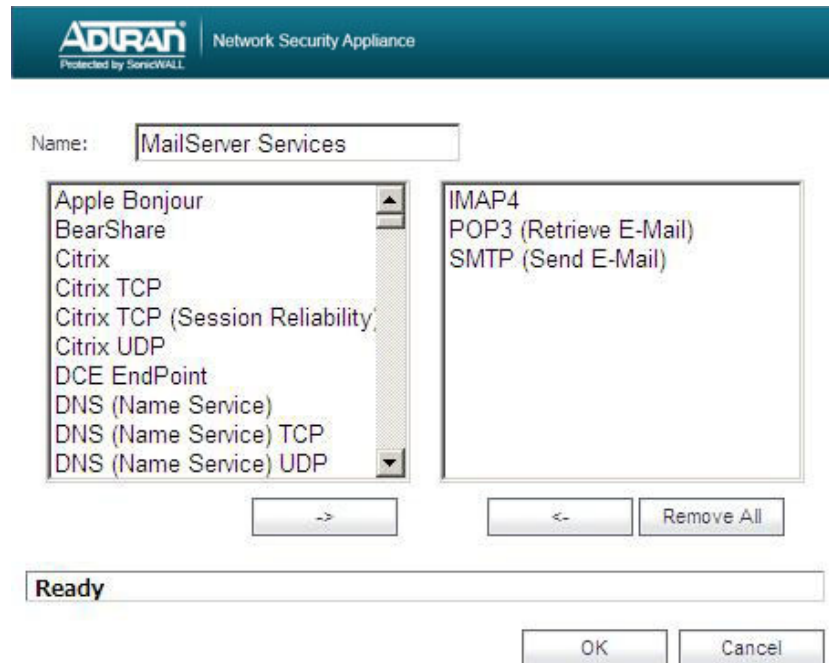
3. Click the **OK** button to complete creation of the new address objects.

Step 2: Create a Service Group

1. The Services page can be accessed either from **Firewall > Services** or **Network > Services**.
2. Click **Add Group**.
3. Select individual services from the list in the left column. Click - > to add the services to the group.

Procedure:

4. To remove services from the group, select individual services from the list in right column. Click < - to remove the services.



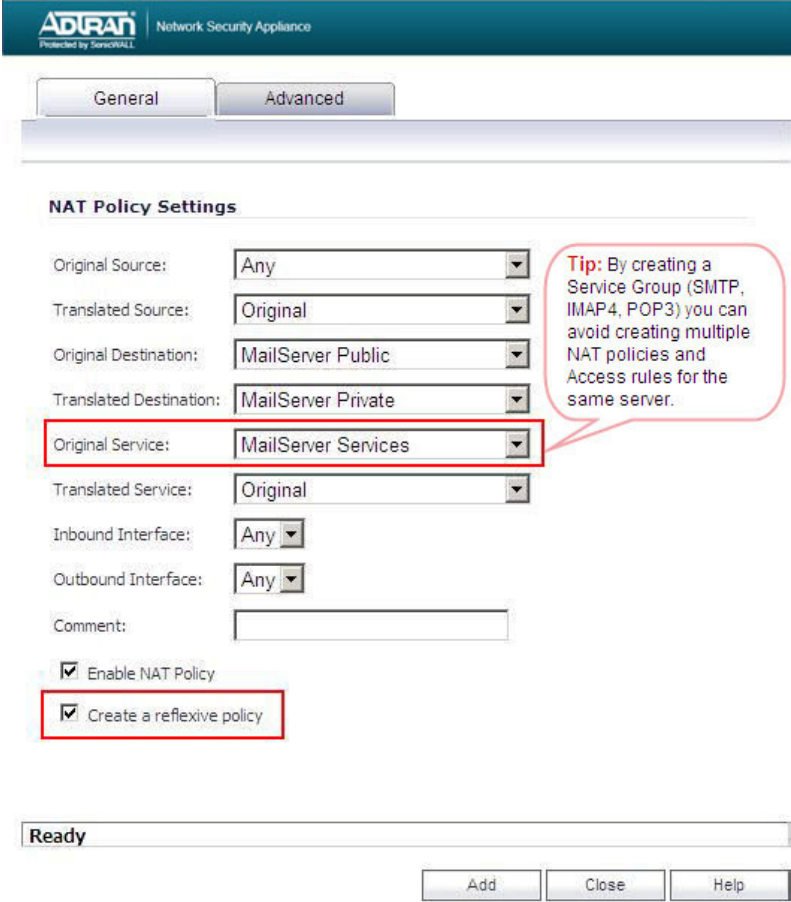
5. When you are finished, click **OK** to add the group to Custom Services Groups.

Step 3: Defining the appropriate NAT Policies

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

2. Click the **Add a new NAT Policy** button and choose 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.

<p>Adding appropriate NAT Policies</p> <p>Original Source: Any</p> <p>Translated Source: Original</p> <p>Original Destination: MailServer Public</p> <p>Translated Destination: MailServer Private</p> <p>Original Service: MailServer Services</p> <p>Translated Service: Original</p> <p>Inbound Interface: Any</p> <p>Outbound Interface: Any</p> <p>Comment: Webserver behind NetVanta 2000 Series.</p> <p>Enable NAT Policy: Checked</p> <p>Create a reflexive policy: Checked</p>	 <p>The screenshot shows the 'NAT Policy Settings' window in the ADTRAN Network Security Appliance. The 'Original Service' dropdown menu is selected and highlighted with a red box, showing 'MailServer Services'. Below it, the 'Create a reflexive policy' checkbox is checked and also highlighted with a red box. A red tip bubble on the right side of the window states: 'Tip: By creating a Service Group (SMTP, IMAP4, POP3) you can avoid creating multiple NAT policies and Access rules for the same server.'</p>
--	--

NOTE *Create a reflexive 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.*

Procedure:

3. Click the **Add** button.

Loopback Policy:

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

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

#	Source		Destination		Service		Interface		Priority	Comment	Enable	Configure		
	Original	Translated	Original	Translated	Original	Translated	Inbound	Outbound						
1	Firewalled Subnets	MailServer Public	MailServer Public	MailServer Private	MailServer Services	Original	Any	Any	11		<input checked="" type="checkbox"/>			
<input type="checkbox"/>	2	MailServer Private	MailServer Public	Any	Original	MailServer Services	Original	Any	X1	12	<input checked="" type="checkbox"/>			
<input type="checkbox"/>	3	Any	Original	MailServer Public	MailServer Private	MailServer Services	Original	Any	Any	13	<input checked="" type="checkbox"/>			

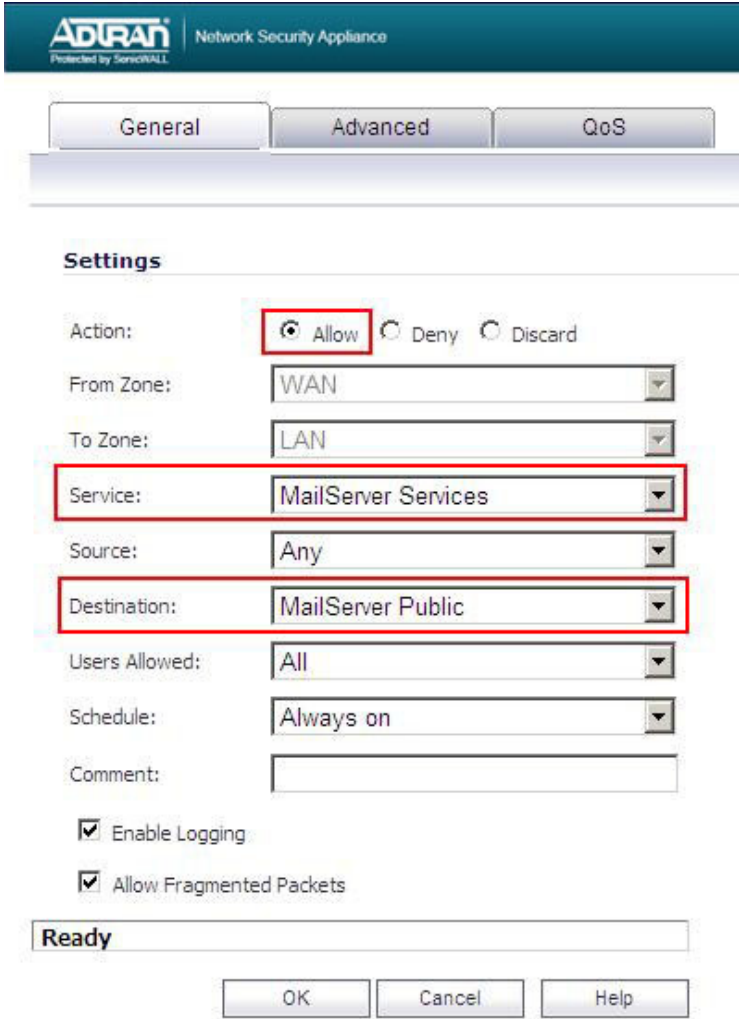
4. Upon completion under **Network > Nat Policies** tab the above **Inbound** and **Outbound** NAT policies will be created.

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:



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.

<p>Action: Allow</p> <p>From Zone: WAN</p> <p>To Zone: LAN</p> <p>Service: MailServer Services</p> <p>Source: Any</p> <p>Destination: MailServer Public</p> <p>Users Allowed: All</p> <p>Schedule: Always on</p> <p>Enable Logging: checked</p> <p>Allow Fragmented Packets: checked</p>	 <p>The screenshot shows the configuration window for a rule in the ADTRAN Network Security Appliance. The 'Settings' tab is selected. The configuration is as follows:</p> <ul style="list-style-type: none"> Action: <input checked="" type="radio"/> Allow, <input type="radio"/> Deny, <input type="radio"/> Discard From Zone: WAN To Zone: LAN Service: MailServer Services Source: Any Destination: MailServer Public Users Allowed: All Schedule: Always on Comment: (empty) <input checked="" type="checkbox"/> Enable Logging <input checked="" type="checkbox"/> Allow Fragmented Packets <p>The status bar at the bottom indicates 'Ready'. Buttons for 'OK', 'Cancel', and 'Help' are visible at the bottom right.</p>
--	---

5. Click **OK**.

How to Test:

- **Testing from within the private network:** Ensure that the Email Server is working from within the private network itself.
- **Testing from the Internet:** Go to www.mxtoolbox.com and enter your Email Server's Public IP address in the Domain Name field i.e **1.1.1.1**

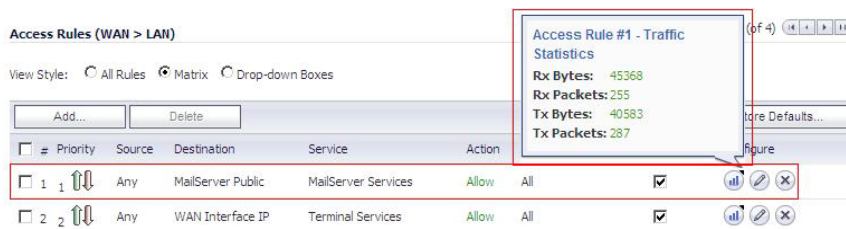


Troubleshooting:

- Ensure that the EmailServer's Default Gateway IP address is the NetVanta 2000 Series LAN IP address.
- Ensure that the Email Server is able to access the Internet.
- Try to reduce the MTU value on your the NetVanta 2000 Series appliance.
- **Displaying Access Rule Traffic Statistics:**

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. Move your mouse pointer over the **Graph** icon to display the following access rule receive (Rx) and transmit (Tx) traffic statistics:

- Rx Bytes
- Rx Packets
- Tx Bytes
- Tx Packets



- Ensure you do not have duplicate **NAT Policies** and **Firewall Access Rules** for your Email 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.