



**Avaya Solution & Interoperability Test Lab**

---

## **Configuring the Juniper NetScreen Firewall Security Policies to support Avaya IP Telephony – Issue 1.0**

### **Abstract**

These Application Notes describes a procedure for configuring the security policies of a Juniper NetScreen-50 firewall to support Avaya H.323 IP Telephones. These security policies accommodate networks where the H.323 Application Layer Gateway functionality of the NetScreen firewall must be disabled.

# TABLE OF CONTENTS

<b>1.</b>	<b>INTRODUCTION.....</b>	<b>3</b>
<b>2.</b>	<b>SCOPE .....</b>	<b>3</b>
<b>3.</b>	<b>NETWORK TOPOLOGY .....</b>	<b>3</b>
3.1.	RTP TRAVERSAL.....	3
3.2.	LOGICAL NETWORK .....	4
3.3.	PHYSICAL NETWORK.....	5
<b>4.</b>	<b>SECURITY POLICY .....</b>	<b>5</b>
<b>5.</b>	<b>EQUIPMENT AND SOFTWARE VALIDATED.....</b>	<b>7</b>
<b>6.</b>	<b>JUNIPER NETSCREEN CONFIGURATION .....</b>	<b>8</b>
6.1.	ACCESS JUNIPER NETSCREEN-50 FIREWALL.....	8
6.2.	GLOBALLY DISABLE H.323 ALG .....	10
6.3.	CONFIGURE SECURITY ZONES .....	11
6.4.	CONFIGURING INTERFACES .....	14
6.5.	CREATE ADDRESS BOOK ENTRIES.....	18
6.6.	CONFIGURING CUSTOM SERVICE .....	22
6.7.	CREATING SECURITY POLICY .....	25
6.7.1.	<i>Trust to Untrust policy.....</i>	<i>25</i>
6.7.2.	<i>Untrust to Trust policy.....</i>	<i>29</i>
6.7.3.	<i>Summary of Avaya IP Telephone Security Policies .....</i>	<i>34</i>
<b>7.</b>	<b>AVAYA COMMUNICATION MANAGER CONFIGURATION.....</b>	<b>35</b>
<b>8.</b>	<b>CONCLUSION.....</b>	<b>35</b>
<b>9.</b>	<b>REFERENCES.....</b>	<b>36</b>

# 1. Introduction

Avaya Communication Manager and Media Gateways are security hardened network appliances with built in protection mechanisms to ward off various malicious attack scenarios. Some enterprises, however, require an added level of protection for network appliances providing mission critical services to the enterprise, such as Avaya Communication Manager. These Application Notes describe the configuration of the Juniper Networks NetScreen firewall to provide this added level of protection.

Although not tested, the configuration steps described in these Application Notes for the Juniper NetScreen-50 Firewall also apply to other Juniper NetScreen platforms.

## 2. Scope

The following items outline the scope of these application notes.

- The security policies defined in these application notes reflect the H.323 Application Layer Gateway (ALG) being disabled.
- An “Interior Firewall” design was used for these Application Notes for the implementation of the NetScreen firewall.
- The NetScreen firewall is configured in Routed Mode - No Network Address Translation (NAT).
- The Security Policies defined in these Application Notes are limited to Avaya IP Telephones and Avaya Communications Manager IP traffic flows.

## 3. Network Topology

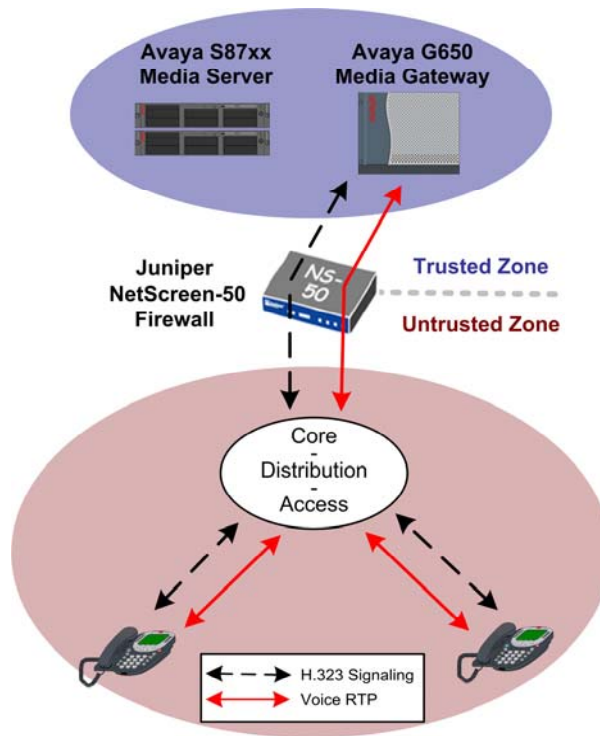
The network design presented in these application notes consists of an Avaya Communication Manager implementation with the NetScreen firewall deployed in an interior firewall configuration. An interior firewall design consists of a firewall placed within the core of the enterprise network, as opposed to at the perimeter. Interior firewalls protect critical internal resources, such as Avaya Communication Manager, from internal attack, possibly by improperly configured internal equipment or disgruntled employees.

### 3.1. RTP Traversal

Consideration must be taken for the load IP Telephony traffic will place on a firewall. This traffic could impact the performance of the firewall which will create delay, degrading voice quality for existing calls and preventing new calls from being established. A good network design, upfront planning and appropriate sizing of network elements, such as firewalls, will accommodate high volumes of RTP voice traffic and allow media gateways to be placed behind the firewall in the Trusted security zone as shown in **Figure 1**.

## 3.2. Logical Network

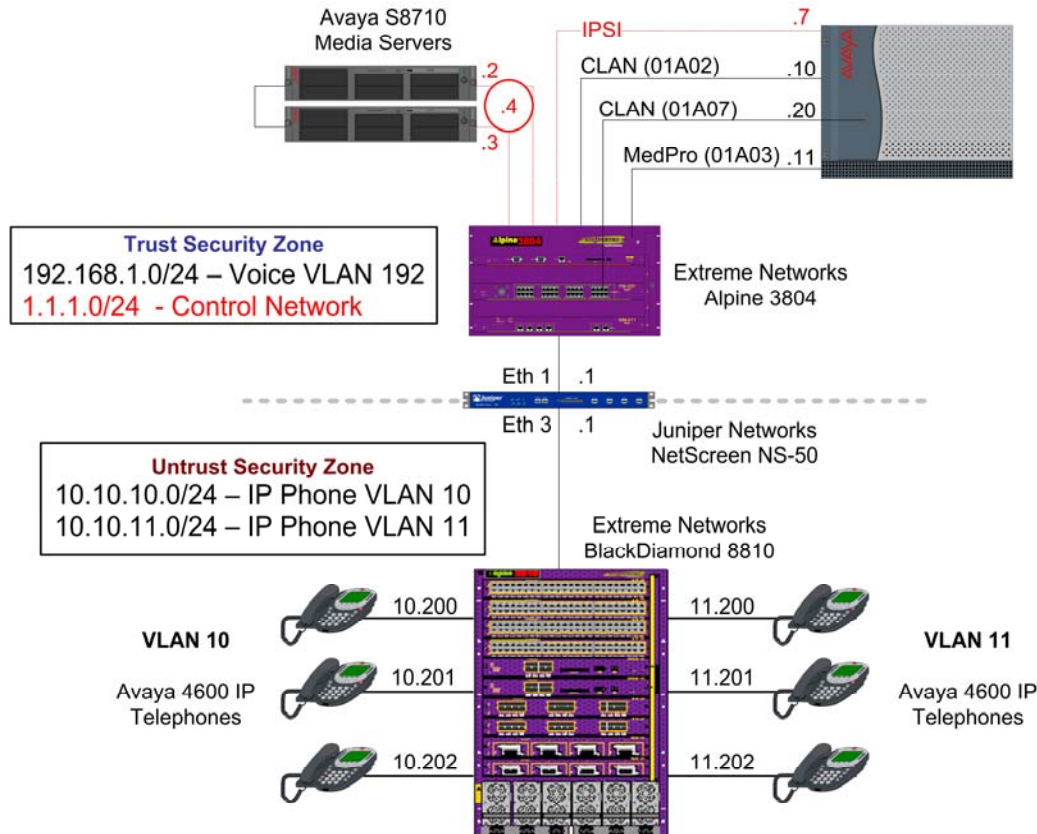
**Figure 1** shows a logical diagram of the Juniper NetScreen firewall separating Trusted and Untrusted security zones and shows H.323 signaling and RTP voice traffic flows which need to traverse the firewall.



**Figure 1: Logical Network View**

### 3.3. Physical Network

The physical network implemented for these Application Notes is shown in **Figure 2**.

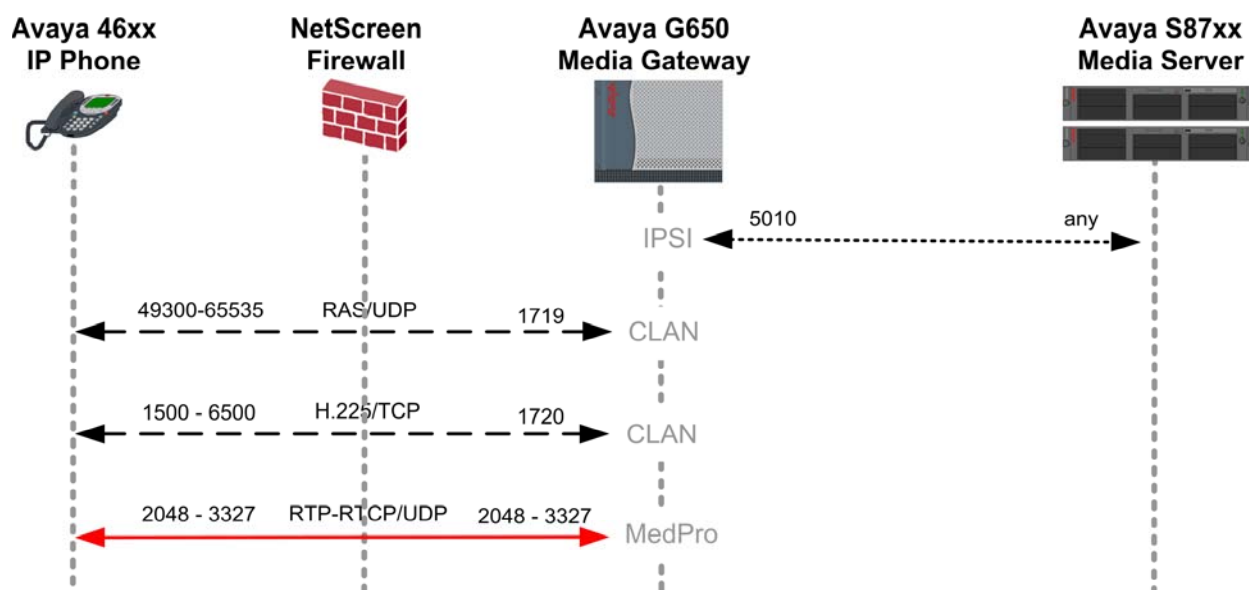


### Figure 2: Physical Network

## 4. Security Policy

Security policies specify the types of traffic permitted or denied between two Security Zones.

**Figure 3** provides a view of the Avaya H.323 signaling and RTP voice traffic flows required to traverse the firewall. Security policies must be created to accommodate this traffic. The details of these flows are presented in **Table 1**.



**Figure 3: Traffic Flow**

**Note:** The RTP / RTCP port range of the firewall policy must match the RTP port range defined in Avaya Communication Manager **ip-network-region** form for each configured region. UDP ports 2048 – 3327 are the default range as of Avaya Communication Manager release 3.1.

From (Sender)	Source Port	To (Listener)	Destination Port	Purpose
C-LAN	UDP 1719	Avaya IP Telephone	UDP 49300 - 65535	RAS - IP phone Registration
Avaya IP Telephone	UDP 49300 - 65535	C-LAN	UDP 1719	RAS - IP phone Registration
C-LAN	TCP 1720	Avaya IP Telephone	TCP 1500 - 6500	H.225 call signaling
Avaya IP Telephone	TCP 1500 - 6500	C-LAN	TCP 1720	H.225 call signaling
MedPro	UDP 2048 – 3327	Avaya IP Telephone	UDP 2048 – 3327	RTP / RTCP voice media
Avaya IP Telephone	UDP 2048 – 3327	MedPro	UDP 2048 – 3327	RTP / RTCP voice media

**Table 1 – UDP/TCP Ports**

## 5. Equipment and Software Validated

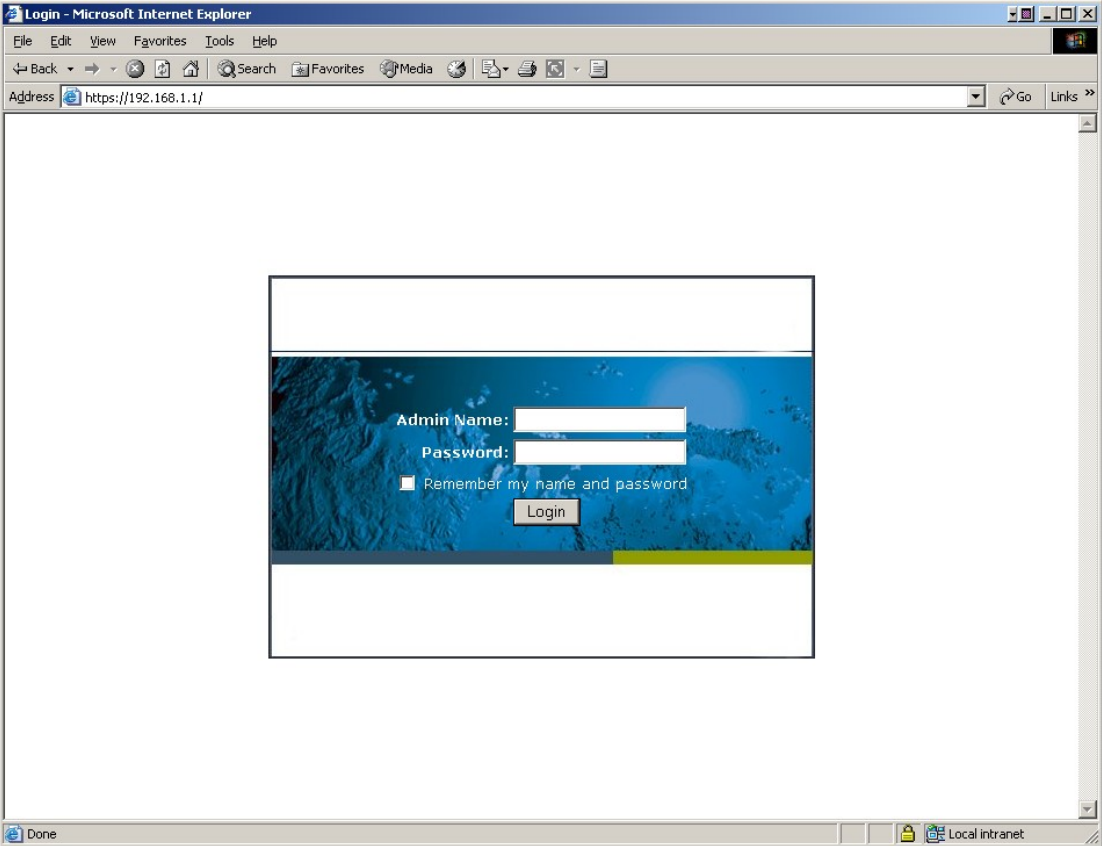
**Table 2** lists the equipment and software/firmware versions used in the sample configuration provided.

Device Description	Versions Tested
Avaya S8710 Media Server	Avaya Communication Manager R3.1 (R013x. 01.0.628.6)
Avaya G650 Media Gateway	-
TN2312BP IPSI	FW 22
TN799DP C-LAN	FW 16
TN2302AP IP MedPro	FW 108
Avaya 4602SW IP Telephones	R2.3 – Application (a02d01b2_3.bin)
Avaya 4610SW IP Telephones	R2.3 – Application (a10d01b2_3.bin)
Avaya 4620SW IP Telephones	R2.3 – Application (a20d01b2_3.bin)
Avaya 4625SW IP Telephones	R2.5 – Application (a25d01a2_5.bin)
Juniper Networks NetScreen-50	ScreenOS 5.3.0r2.0

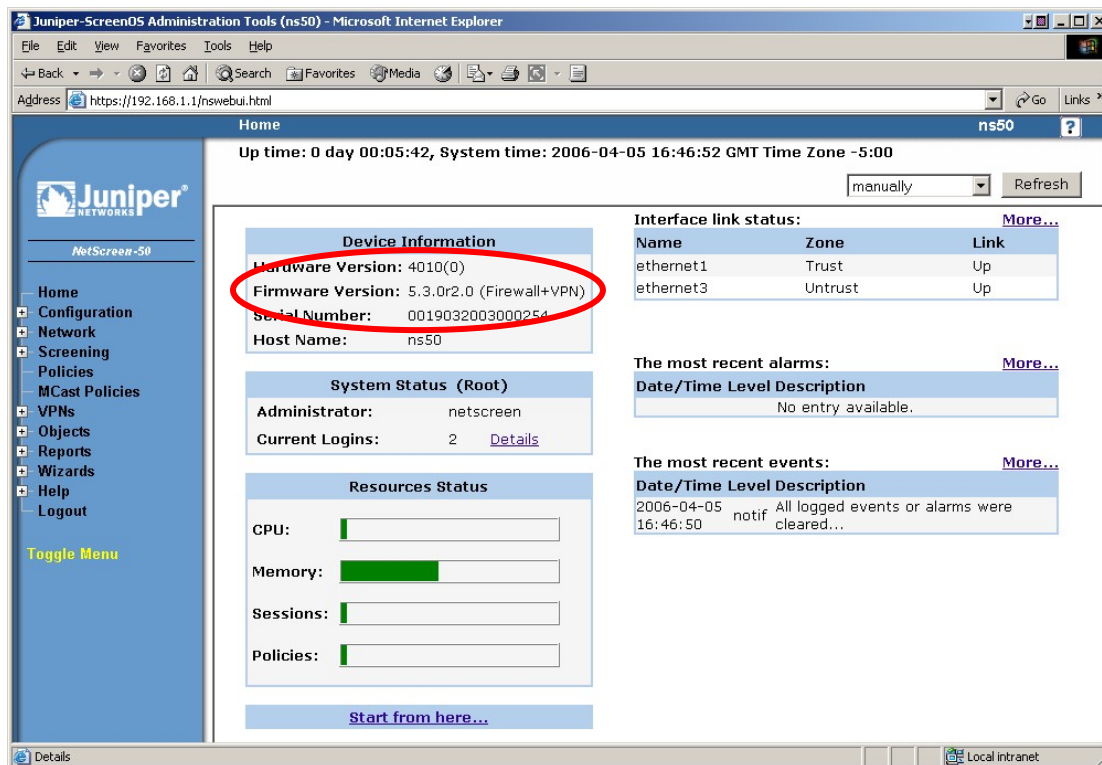
**Table 2 – Equipment and Software Validated**

## 6. Juniper NetScreen Configuration

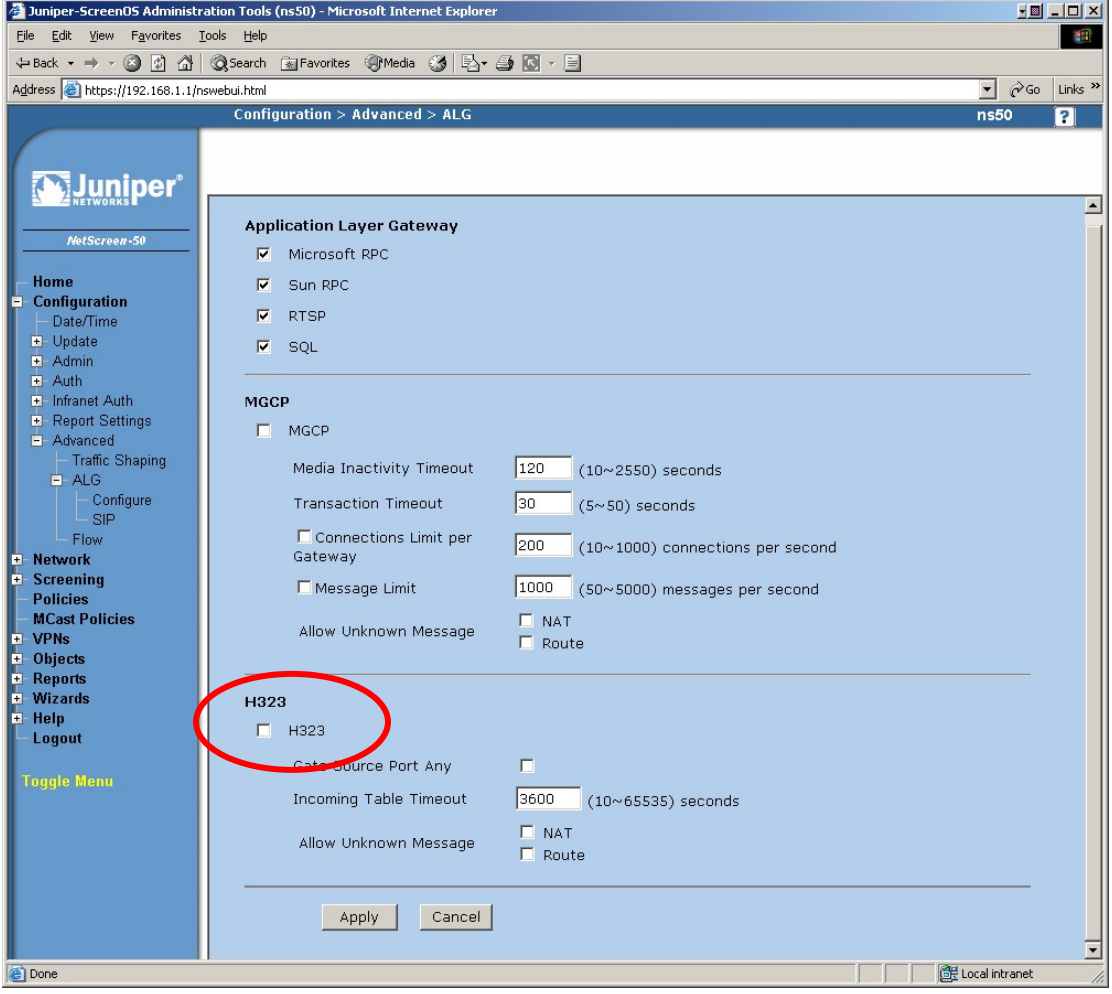
### 6.1. Access Juniper NetScreen-50 Firewall

Step	Description
1.	<p>Access to the NetScreen-50 Firewall management GUI is done through a web browser. Enter the URL of the NetScreen management interface, <a href="https://&lt;IP address of NetScreen&gt;">https://&lt;IP address of NetScreen&gt;</a> and the following login screen appears. Log in using a user name with administrative privileges.</p> 



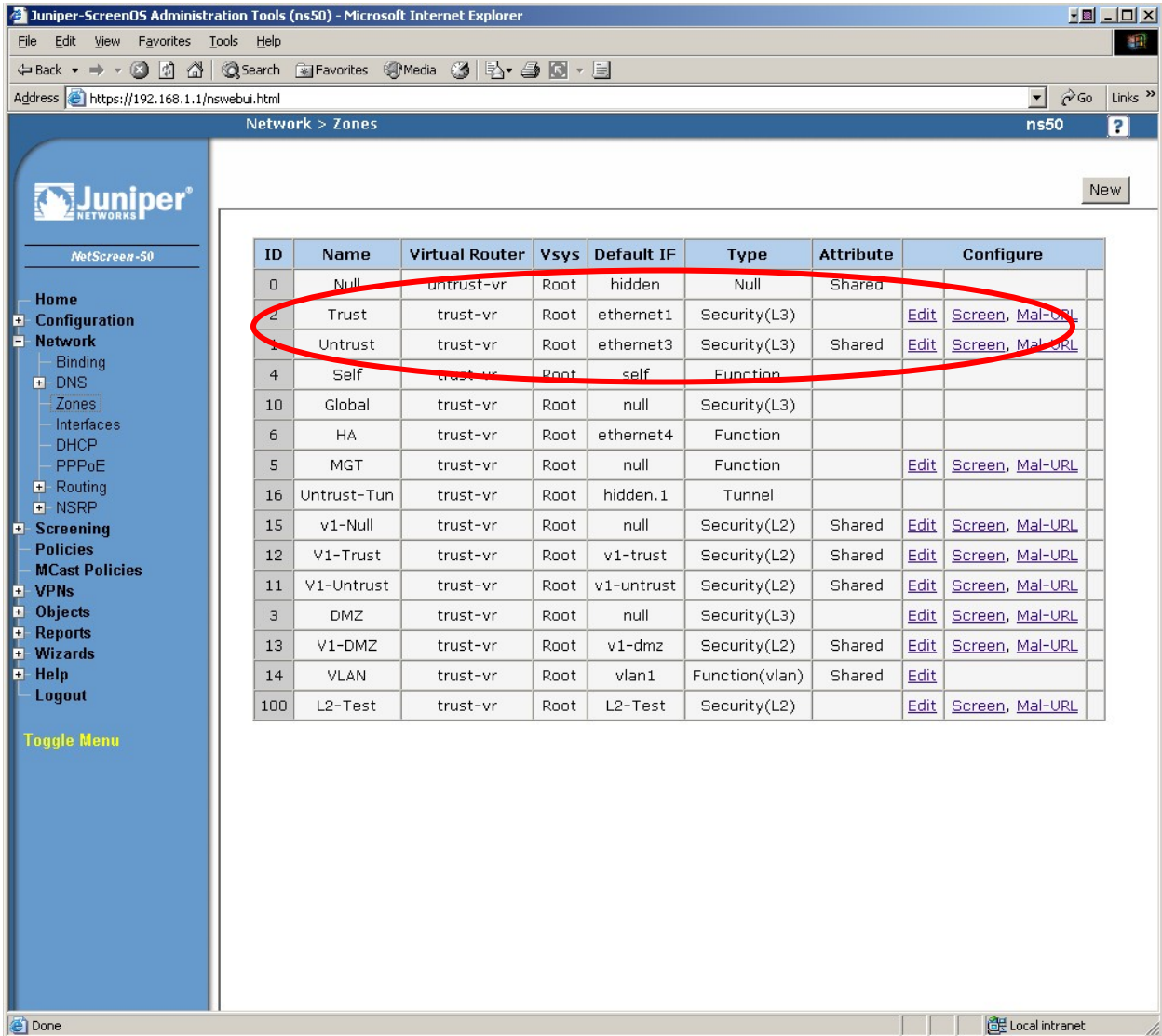
Step	Description
2.	<p>A NetScreen Web administration page similar to the one below appears upon successful login. Note the ScreenOS Firmware version in the Device Information pane.</p>  <p>The screenshot displays the Juniper-NetScreen-50 Administration Tools web interface. The page is titled 'Juniper-NetScreen-50 Administration Tools (ns50) - Microsoft Internet Explorer'. The address bar shows 'https://192.168.1.1/nswebui.html'. The page content includes a sidebar with navigation links (Home, Configuration, Network, Screening, Policies, MCast Policies, VPNs, Objects, Reports, Wizards, Help, Logout) and a main content area. The main content area is divided into several sections: 'Device Information' (highlighted with a red circle), 'System Status (Root)', 'Resources Status', 'Interface link status', 'The most recent alarms', and 'The most recent events'. The 'Device Information' section shows 'Hardware Version: 4010(0)', 'Firmware Version: 5.3.0r2.0 (Firewall+VPN)', 'Serial Number: 0019032003000254', and 'Host Name: ns50'. The 'System Status (Root)' section shows 'Administrator: netscreen' and 'Current Logins: 2'. The 'Resources Status' section shows 'CPU', 'Memory', 'Sessions', and 'Policies' with corresponding progress bars. The 'Interface link status' section shows a table with columns 'Name', 'Zone', and 'Link'. The 'The most recent alarms' and 'The most recent events' sections show 'No entry available' and 'All logged events or alarms were cleared...' respectively.</p>

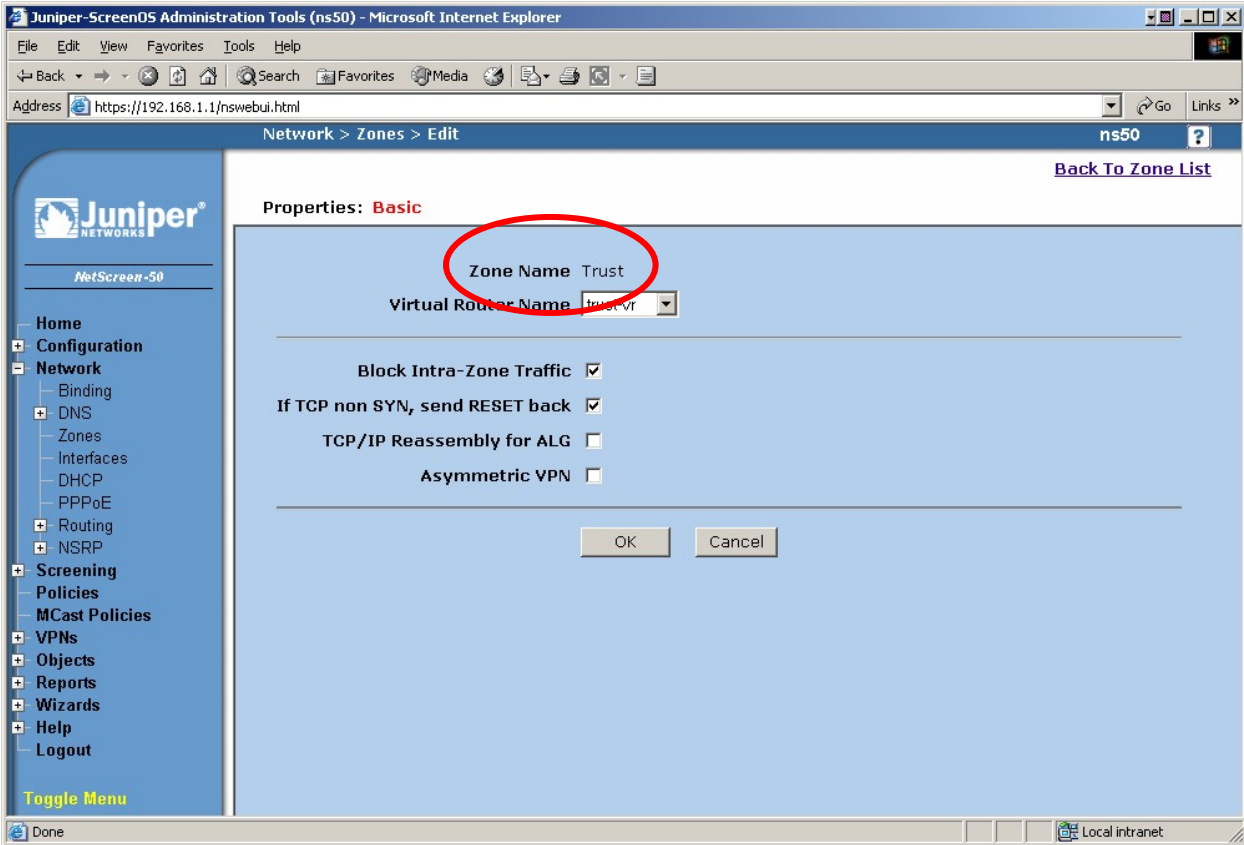
## 6.2. Globally Disable H.323 ALG

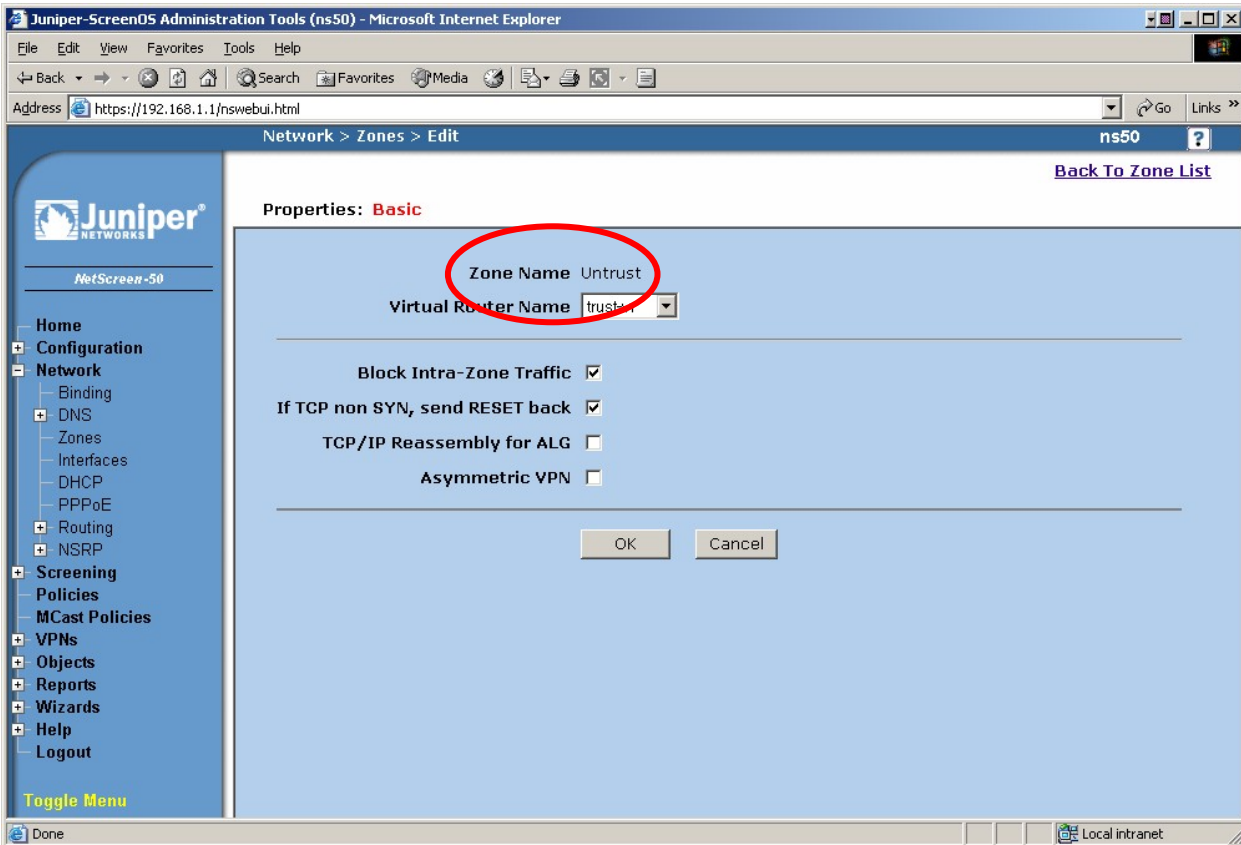
Step	Description
1.	From the left navigation menu, select <b>Configuration</b> → <b>Advanced</b> → <b>ALG</b> → <b>Configure</b> .
2.	<p>Un-Check the H323 check box to globally disable the H.323 Application Layer Gateway.</p> 

### 6.3. Configure Security Zones

A Security Zone is used to divide a network into logical segments. Two security zones are required at a minimum. Juniper NetScreen firewalls come with several predefined security zones. The Trust and Untrust predefined security zones are used in these Application Notes.

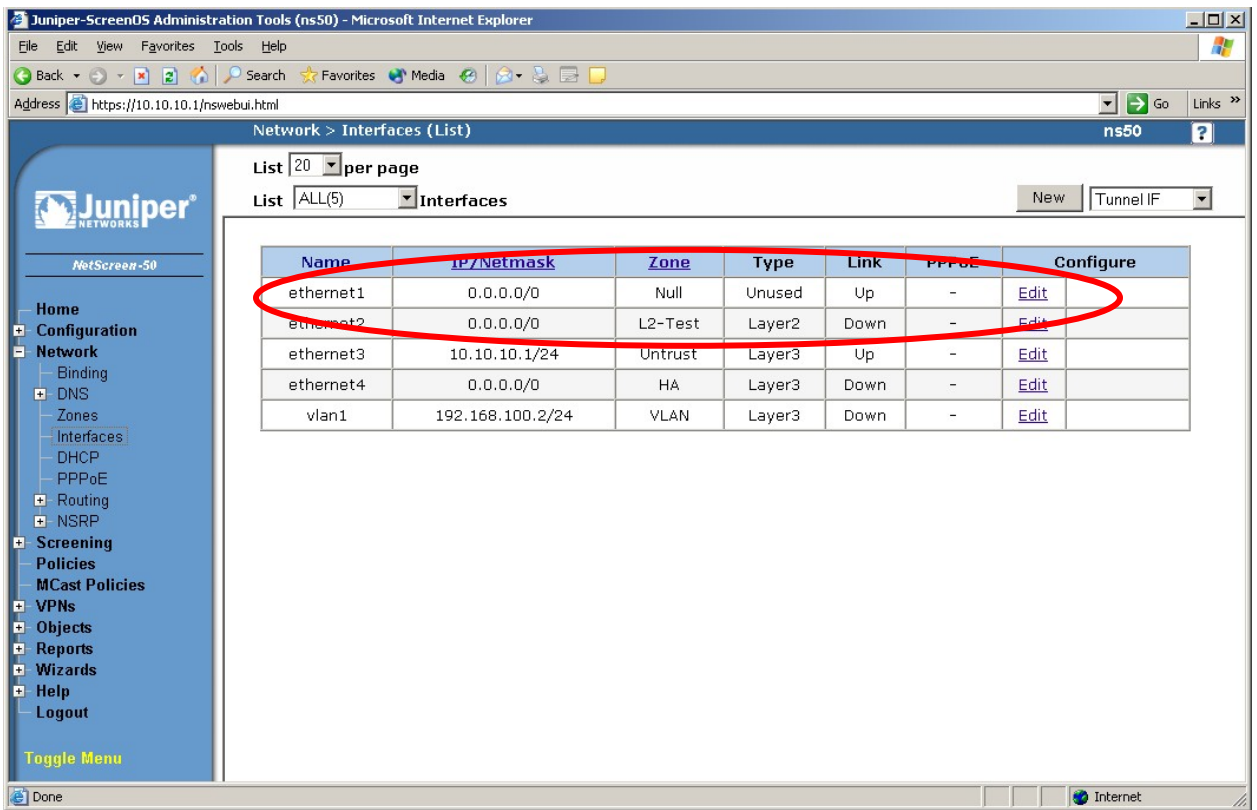
Step	Description																																																																																																																																
1.	<p>To view these security zones and verify configurations, select <b>Configuration → Zones</b> from the left navigation menu. A page similar to the one below appears displaying all the configured security zones.</p>  <table><thead><tr><th>ID</th><th>Name</th><th>Virtual Router</th><th>Vsys</th><th>Default IF</th><th>Type</th><th>Attribute</th><th>Configure</th></tr></thead><tbody><tr><td>0</td><td>Null</td><td>untrust-vr</td><td>Root</td><td>hidden</td><td>Null</td><td>Shared</td><td></td></tr><tr><td>2</td><td>Trust</td><td>trust-vr</td><td>Root</td><td>ethernet1</td><td>Security(L3)</td><td></td><td><a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a></td></tr><tr><td>1</td><td>Untrust</td><td>trust-vr</td><td>Root</td><td>ethernet3</td><td>Security(L3)</td><td>Shared</td><td><a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a></td></tr><tr><td>4</td><td>Self</td><td>trust-vr</td><td>Root</td><td>self</td><td>Function</td><td></td><td></td></tr><tr><td>10</td><td>Global</td><td>trust-vr</td><td>Root</td><td>null</td><td>Security(L3)</td><td></td><td></td></tr><tr><td>6</td><td>HA</td><td>trust-vr</td><td>Root</td><td>ethernet4</td><td>Function</td><td></td><td></td></tr><tr><td>5</td><td>MGT</td><td>trust-vr</td><td>Root</td><td>null</td><td>Function</td><td></td><td><a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a></td></tr><tr><td>16</td><td>Untrust-Tun</td><td>trust-vr</td><td>Root</td><td>hidden.1</td><td>Tunnel</td><td></td><td></td></tr><tr><td>15</td><td>v1-Null</td><td>trust-vr</td><td>Root</td><td>null</td><td>Security(L2)</td><td>Shared</td><td><a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a></td></tr><tr><td>12</td><td>V1-Trust</td><td>trust-vr</td><td>Root</td><td>v1-trust</td><td>Security(L2)</td><td>Shared</td><td><a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a></td></tr><tr><td>11</td><td>V1-Untrust</td><td>trust-vr</td><td>Root</td><td>v1-untrust</td><td>Security(L2)</td><td>Shared</td><td><a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a></td></tr><tr><td>3</td><td>DMZ</td><td>trust-vr</td><td>Root</td><td>null</td><td>Security(L3)</td><td></td><td><a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a></td></tr><tr><td>13</td><td>V1-DMZ</td><td>trust-vr</td><td>Root</td><td>v1-dmz</td><td>Security(L2)</td><td>Shared</td><td><a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a></td></tr><tr><td>14</td><td>VLAN</td><td>trust-vr</td><td>Root</td><td>vlan1</td><td>Function(vlan)</td><td>Shared</td><td><a href="#">Edit</a></td></tr><tr><td>100</td><td>L2-Test</td><td>trust-vr</td><td>Root</td><td>L2-Test</td><td>Security(L2)</td><td></td><td><a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a></td></tr></tbody></table>	ID	Name	Virtual Router	Vsys	Default IF	Type	Attribute	Configure	0	Null	untrust-vr	Root	hidden	Null	Shared		2	Trust	trust-vr	Root	ethernet1	Security(L3)		<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>	1	Untrust	trust-vr	Root	ethernet3	Security(L3)	Shared	<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>	4	Self	trust-vr	Root	self	Function			10	Global	trust-vr	Root	null	Security(L3)			6	HA	trust-vr	Root	ethernet4	Function			5	MGT	trust-vr	Root	null	Function		<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>	16	Untrust-Tun	trust-vr	Root	hidden.1	Tunnel			15	v1-Null	trust-vr	Root	null	Security(L2)	Shared	<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>	12	V1-Trust	trust-vr	Root	v1-trust	Security(L2)	Shared	<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>	11	V1-Untrust	trust-vr	Root	v1-untrust	Security(L2)	Shared	<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>	3	DMZ	trust-vr	Root	null	Security(L3)		<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>	13	V1-DMZ	trust-vr	Root	v1-dmz	Security(L2)	Shared	<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>	14	VLAN	trust-vr	Root	vlan1	Function(vlan)	Shared	<a href="#">Edit</a>	100	L2-Test	trust-vr	Root	L2-Test	Security(L2)		<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>
ID	Name	Virtual Router	Vsys	Default IF	Type	Attribute	Configure																																																																																																																										
0	Null	untrust-vr	Root	hidden	Null	Shared																																																																																																																											
2	Trust	trust-vr	Root	ethernet1	Security(L3)		<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>																																																																																																																										
1	Untrust	trust-vr	Root	ethernet3	Security(L3)	Shared	<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>																																																																																																																										
4	Self	trust-vr	Root	self	Function																																																																																																																												
10	Global	trust-vr	Root	null	Security(L3)																																																																																																																												
6	HA	trust-vr	Root	ethernet4	Function																																																																																																																												
5	MGT	trust-vr	Root	null	Function		<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>																																																																																																																										
16	Untrust-Tun	trust-vr	Root	hidden.1	Tunnel																																																																																																																												
15	v1-Null	trust-vr	Root	null	Security(L2)	Shared	<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>																																																																																																																										
12	V1-Trust	trust-vr	Root	v1-trust	Security(L2)	Shared	<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>																																																																																																																										
11	V1-Untrust	trust-vr	Root	v1-untrust	Security(L2)	Shared	<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>																																																																																																																										
3	DMZ	trust-vr	Root	null	Security(L3)		<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>																																																																																																																										
13	V1-DMZ	trust-vr	Root	v1-dmz	Security(L2)	Shared	<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>																																																																																																																										
14	VLAN	trust-vr	Root	vlan1	Function(vlan)	Shared	<a href="#">Edit</a>																																																																																																																										
100	L2-Test	trust-vr	Root	L2-Test	Security(L2)		<a href="#">Edit</a> <a href="#">Screen</a> <a href="#">Mal-URL</a>																																																																																																																										

Step	Description
2.	<p>To view the Trust security zone configuration, select <b>Edit</b> on the row with the name Trust. A page similar to the one below appears displaying the Trust Security zone default configuration.</p>  <p>The screenshot shows the Juniper-ScreenOS Administration Tools (ns50) web interface in Microsoft Internet Explorer. The browser address bar shows 'https://192.168.1.1/nswebui.html'. The page title is 'Juniper-ScreenOS Administration Tools (ns50) - Microsoft Internet Explorer'. The breadcrumb navigation shows 'Network &gt; Zones &gt; Edit'. The page has a blue header with the Juniper logo and 'ns50' on the right. A left sidebar contains a navigation menu with options: Home, Configuration, Network (expanded), Binding, DNS, Zones, Interfaces, DHCP, PPPoE, Routing, NSRP, Screening, Policies, MCast Policies, VPNs, Objects, Reports, Wizards, Help, and Logout. The main content area is titled 'Properties: Basic' and shows the configuration for the 'Trust' security zone. The 'Zone Name' field is circled in red and contains the text 'Trust'. Below it, the 'Virtual Router Name' dropdown menu is set to 'Trust vr'. There are four checkboxes: 'Block Intra-Zone Traffic' (checked), 'If TCP non SYN, send RESET back' (checked), 'TCP/IP Reassembly for ALG' (unchecked), and 'Asymmetric VPN' (unchecked). At the bottom of the configuration area are 'OK' and 'Cancel' buttons. The status bar at the bottom of the browser shows 'Done' and 'Local intranet'.</p>

Step	Description
3.	<p>To view the Untrust security zone configuration, select <b>Edit</b> on the row with the name Untrust. A page similar to the one below appears displaying the Untrust Security zone default configuration.</p> 

## 6.4. Configuring Interfaces

The physical interfaces of the NetScreen firewall must be bound to a security zone before an IP address can be assigned. As show in **Figure 2: Physical Network**, the NetScreen Ethernet 1 interface is bound to the Trust security zone and the Ethernet 3 interface is bound to the Untrust zone.

Step	Description																																										
1.	<p>To configure interface <b>Ethernet 1</b>, select <b>Network → Interfaces</b> from the left navigation menu. A page similar to the one below appears displaying all the network interfaces available on the NetScreen. The highlighted area below shows Ethernet 1 with no IP address or security zone assigned.</p>  <table><thead><tr><th>Name</th><th>IP/Netmask</th><th>Zone</th><th>Type</th><th>Link</th><th>PPPoE</th><th>Configure</th></tr></thead><tbody><tr><td>ethernet1</td><td>0.0.0.0/0</td><td>Null</td><td>Unused</td><td>Up</td><td>-</td><td><a href="#">Edit</a></td></tr><tr><td>ethernet2</td><td>0.0.0.0/0</td><td>L2-Test</td><td>Layer2</td><td>Down</td><td>-</td><td><a href="#">Edit</a></td></tr><tr><td>ethernet3</td><td>10.10.10.1/24</td><td>Untrust</td><td>Layer3</td><td>Up</td><td>-</td><td><a href="#">Edit</a></td></tr><tr><td>ethernet4</td><td>0.0.0.0/0</td><td>HA</td><td>Layer3</td><td>Down</td><td>-</td><td><a href="#">Edit</a></td></tr><tr><td>vlan1</td><td>192.168.100.2/24</td><td>VLAN</td><td>Layer3</td><td>Down</td><td>-</td><td><a href="#">Edit</a></td></tr></tbody></table>	Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure	ethernet1	0.0.0.0/0	Null	Unused	Up	-	<a href="#">Edit</a>	ethernet2	0.0.0.0/0	L2-Test	Layer2	Down	-	<a href="#">Edit</a>	ethernet3	10.10.10.1/24	Untrust	Layer3	Up	-	<a href="#">Edit</a>	ethernet4	0.0.0.0/0	HA	Layer3	Down	-	<a href="#">Edit</a>	vlan1	192.168.100.2/24	VLAN	Layer3	Down	-	<a href="#">Edit</a>
Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure																																					
ethernet1	0.0.0.0/0	Null	Unused	Up	-	<a href="#">Edit</a>																																					
ethernet2	0.0.0.0/0	L2-Test	Layer2	Down	-	<a href="#">Edit</a>																																					
ethernet3	10.10.10.1/24	Untrust	Layer3	Up	-	<a href="#">Edit</a>																																					
ethernet4	0.0.0.0/0	HA	Layer3	Down	-	<a href="#">Edit</a>																																					
vlan1	192.168.100.2/24	VLAN	Layer3	Down	-	<a href="#">Edit</a>																																					



Step	Description
2.	<p>Select <b>Edit</b> on the row with the name <b>Ethernet 1</b>. A screen appears offering several configuration options for the Ethernet 1 interface.</p> <p>Key configuration options are highlighted below:</p> <ul style="list-style-type: none"> <li>• <b>Zone Name:</b> Select the <b>Trust</b> zone from the drop down list. This binds the Ethernet 1 interface with the Trust zone.</li> <li>• <b>IP address:</b> Assigns the Ethernet 1 interface an IP address</li> <li>• <b>Interface Mode:</b> Select <b>Route mode</b></li> <li>• <b>Service Options :</b> Select the appropriate options for the network environment</li> </ul>

Juniper-ScreenOS Administration Tools (ns50) - Microsoft Internet Explorer

Address: https://192.168.1.1/nswebui.html

Network > Interfaces > Edit

Interface: ethernet1 (IP/Netmask: 192.168.1.1/24) [Back To Interface List](#)

Properties: **Basic** MIP DIP Secondary IP IGMP Monitor

Interface Name: ethernet1 (mac 0010.db3f.c850)

As member of group: none

Zone Name: Trust

Obtain IP using DHCP ☐ Automatic update DHCP server parameters

Obtain IP using PPPoE: None [Create new pppoe setting](#)

Static IP ☒

IP Address: 192.168.1.1 / 24 ☒ Manageable

Manage IP #: 192.168.1.1 (mac 0010.db3f.c850)

Interface Mode: NAT ☐ Route ☒

Block Intra-subnet Traffic ☐

Service Options

Management Services: ☒ Web UI ☒ Telnet ☒ SSH

Other Services: ☒ SNMP ☒ SSL ☐ Path MTU(IPv4) ☐ Ident-reset

Maximum Transfer Unit(MTU) Admin MTU: 0 Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy ☐

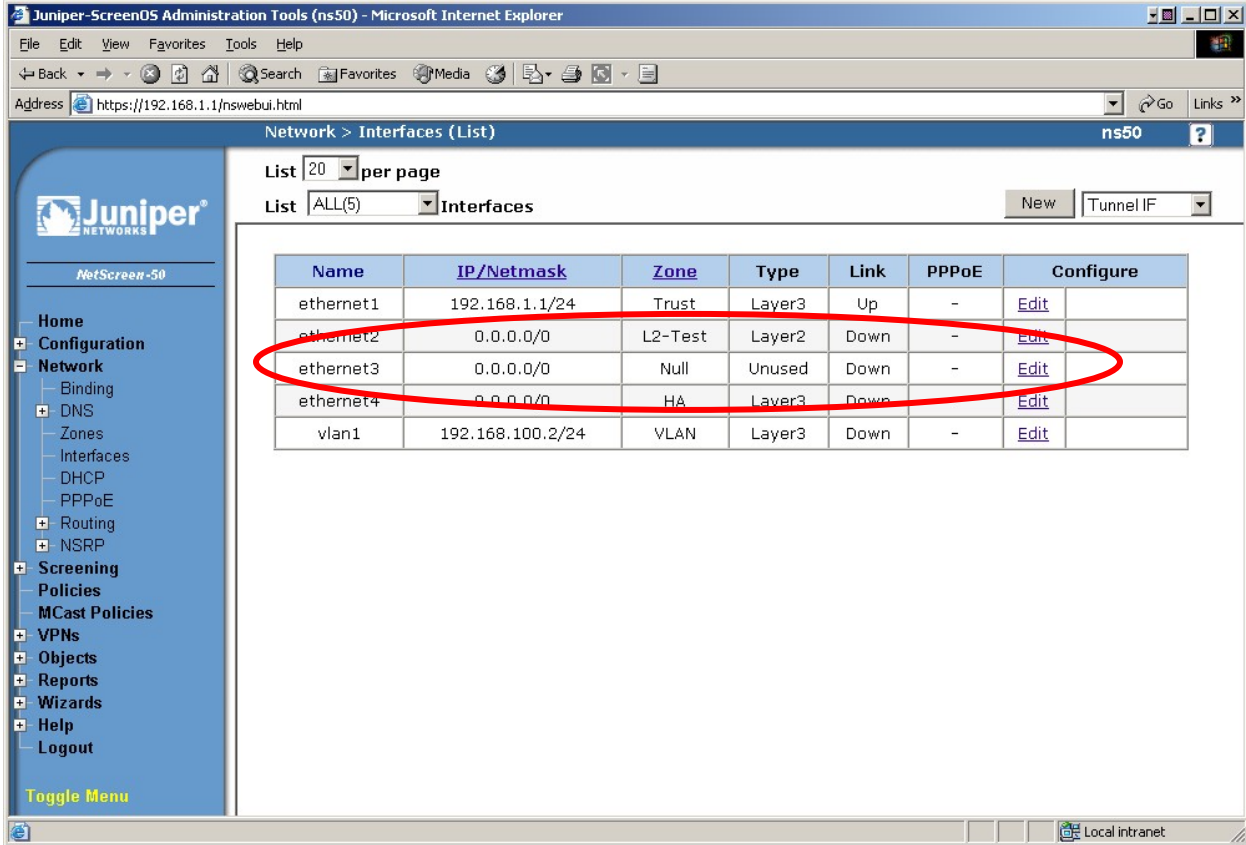
WebAuth ☐ IP Address: 0.0.0.0 ☐ SSL Only

Traffic Bandwidth

Egress: Maximum Bandwidth: 0 Kbps

Ingress: Maximum Bandwidth: 0 Kbps

OK Apply Cancel

Step	Description																																										
3.	<p>To configure interface <b>Ethernet 3</b>, select <b>Network → Interfaces</b> from the left navigation menu. A page similar to the one below appears displaying all the network interfaces available on the NetScreen. The highlighted area below shows Ethernet 3 with no IP address or security zone assigned.</p>  <table><thead><tr><th>Name</th><th>IP/Netmask</th><th>Zone</th><th>Type</th><th>Link</th><th>PPPoE</th><th>Configure</th></tr></thead><tbody><tr><td>ethernet1</td><td>192.168.1.1/24</td><td>Trust</td><td>Layer3</td><td>Up</td><td>-</td><td><a href="#">Edit</a></td></tr><tr><td>ethernet2</td><td>0.0.0.0/0</td><td>L2-Test</td><td>Layer2</td><td>Down</td><td>-</td><td><a href="#">Edit</a></td></tr><tr><td>ethernet3</td><td>0.0.0.0/0</td><td>Null</td><td>Unused</td><td>Down</td><td>-</td><td><a href="#">Edit</a></td></tr><tr><td>ethernet4</td><td>0.0.0.0/0</td><td>HA</td><td>Layer3</td><td>Down</td><td>-</td><td><a href="#">Edit</a></td></tr><tr><td>vlan1</td><td>192.168.100.2/24</td><td>VLAN</td><td>Layer3</td><td>Down</td><td>-</td><td><a href="#">Edit</a></td></tr></tbody></table>	Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure	ethernet1	192.168.1.1/24	Trust	Layer3	Up	-	<a href="#">Edit</a>	ethernet2	0.0.0.0/0	L2-Test	Layer2	Down	-	<a href="#">Edit</a>	ethernet3	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>	ethernet4	0.0.0.0/0	HA	Layer3	Down	-	<a href="#">Edit</a>	vlan1	192.168.100.2/24	VLAN	Layer3	Down	-	<a href="#">Edit</a>
Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure																																					
ethernet1	192.168.1.1/24	Trust	Layer3	Up	-	<a href="#">Edit</a>																																					
ethernet2	0.0.0.0/0	L2-Test	Layer2	Down	-	<a href="#">Edit</a>																																					
ethernet3	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>																																					
ethernet4	0.0.0.0/0	HA	Layer3	Down	-	<a href="#">Edit</a>																																					
vlan1	192.168.100.2/24	VLAN	Layer3	Down	-	<a href="#">Edit</a>																																					



Step	Description
4.	<p>Select <b>Edit</b> on the row with the name <b>Ethernet 3</b>. A screen appears offering several configuration options for the Ethernet 1 interface.</p> <p>Key configuration options are highlighted below:</p> <ul style="list-style-type: none"> <li>• <b>Zone Name:</b> Select the <b>Untrust</b> zone from the drop down list. This binds the Ethernet 3 interface with the Untrust zone.</li> <li>• <b>IP address:</b> Assigns the Ethernet 3 interface an IP address.</li> <li>• <b>Interface Mode:</b> Select <b>Route mode</b>.</li> <li>• <b>Service Options :</b> Select the appropriate options for the network environment.</li> </ul>

Juniper-ScreenOS Administration Tools (ns50) - Microsoft Internet Explorer

Address: https://192.168.1.1/nswebui.html

Network > Interfaces > Edit

Interface: ethernet3 (IP/Netmask: 10.10.10.1/24) [Back To Interface List](#)

Properties: **Basic** MIP DIP VIP IGMP Monitor

Interface Name: ethernet3 (mac 0010.db3f.c856)

As member of group: none

Zone Name: Untrust

Obtain IP using DHCP ☐ Automatic update DHCP server parameters

Obtain IP using PPPoE: None [Create new pppoe setting](#)

Static IP ☒

IP Address: 10.10.10.1 / 24 ☒ Manageable

Manage IP #: 10.10.10.1 (mac 0010.db3f.c856)

Interface Mode: ☐ NAT ☒ Route

Block Intra-subnet Traffic ☐

Service Options

Management Services: ☐ Web UI ☐ Telnet ☐ SSH

Other Services: ☐ SNMP ☐ SSL ☐ Ping ☐ Path MTU(IPv4) ☐ Ident-reset

Maximum Transfer Unit(MTU) Admin MTU: 0 Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy ☐

WebAuth ☐ IP Address: 0.0.0.0 ☐ SSL Only

Traffic Bandwidth

Egress: Maximum Bandwidth: 0 Kbps

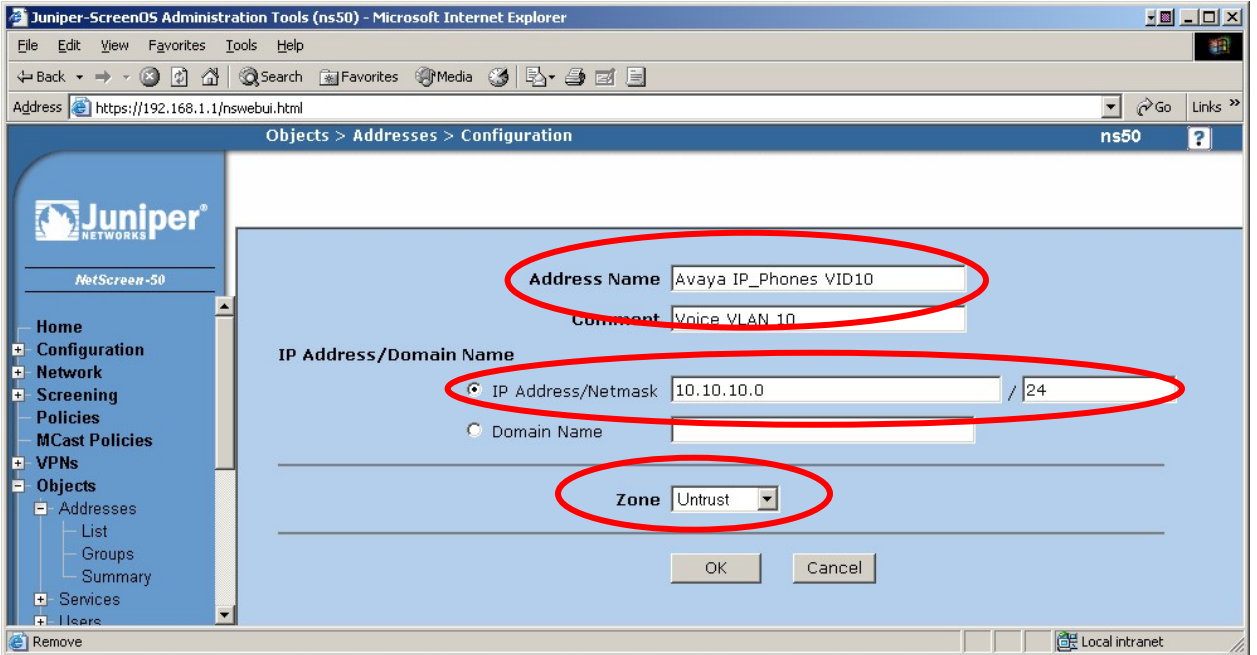
Ingress: Maximum Bandwidth: 0 Kbps


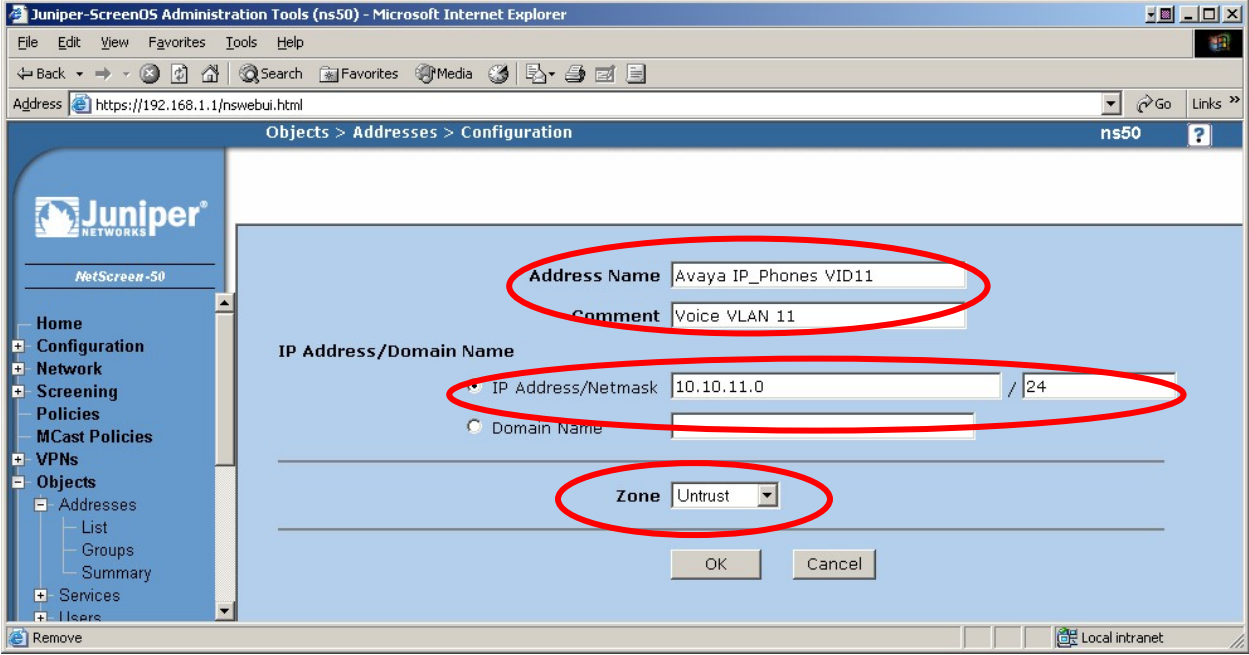
OK Apply Cancel


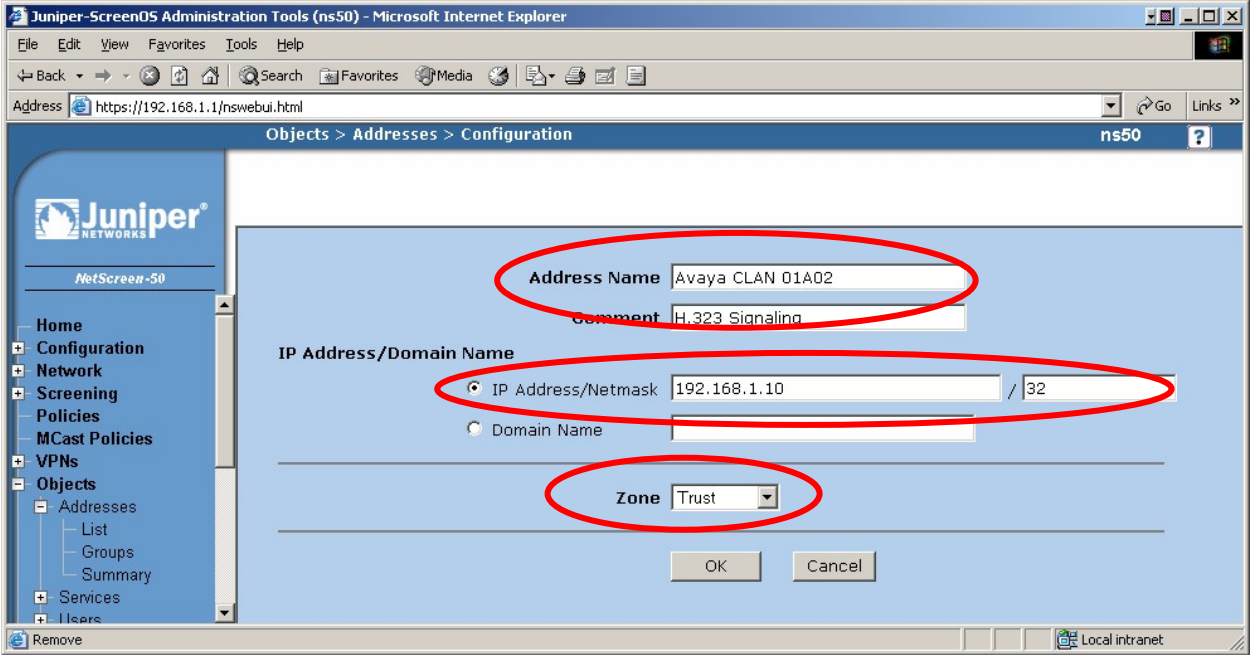
## 6.5. Create Address Book Entries


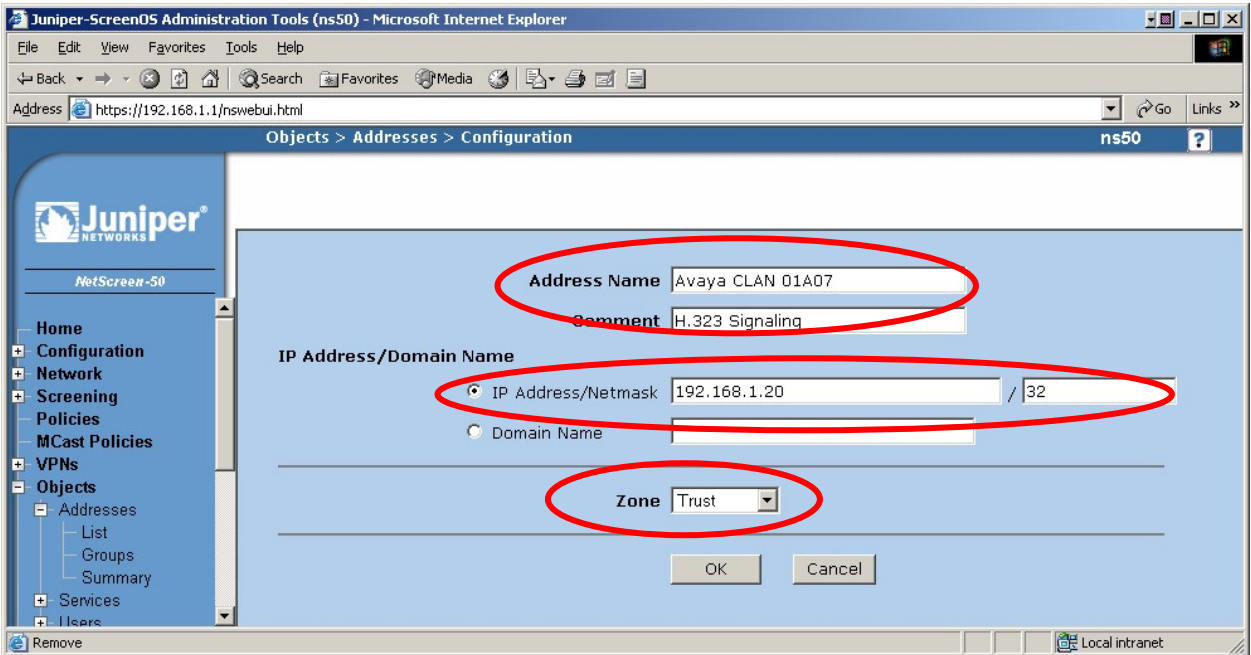
As shown in **Figure 2: Physical Network**, the Avaya IP Telephones are located in the Untrust security zone in dedicated IP telephone VLANs. This simplifies the IP telephone IP addressing scheme for entry into the **NetScreen Address Book**. The IP phone network addresses are entered, rather than entering each individual IP phone address.


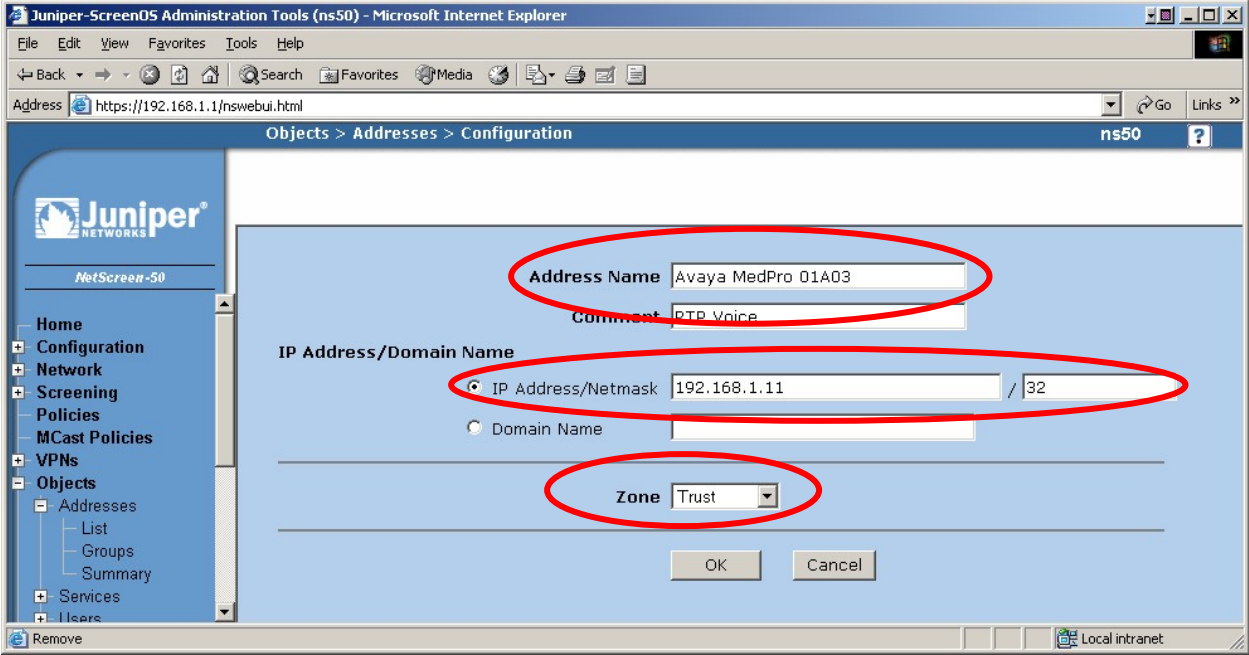
**NetScreen Address Book** entries for the Trust security zone consist of Avaya CLAN and Medpro IP addresses.

Step	Description
1.	<p><b>IP Phone VLAN 10 IP address entry – Untrust Zone:</b></p> <p>From the left navigation menu, select <b>Objects → Addresses → List</b>. The address list page is displayed. Select the <b>New</b> button on top right corner of page to create a new address book entry. Enter the following information for IP phone network VLAN 10:</p> <ul style="list-style-type: none"><li>• <b>Address Name:</b> Name to reference this address book entry by.</li><li>• <b>Comment:</b> Description of entry</li><li>• <b>IP Address/Netmask:</b> IP address and subnet mask of IP phone network</li><li>• <b>Zone:</b> Select <b>Untrust</b> from drop down list</li></ul> 

Step	Description
2.	<p data-bbox="289 237 1008 268"><b>IP Phone VLAN 11 IP address entry – Untrust Zone:</b></p> <p data-bbox="289 306 1477 432">From the left navigation menu, select <b>Objects → Addresses → List</b>. The address list page is displayed. Select the  button on top right corner of page to create a new address book entry. Enter the following information for IP phone network VLAN 11:</p> <ul data-bbox="337 478 1305 625" style="list-style-type: none"> <li>• <b>Address Name:</b> Name to reference this address book entry by.</li> <li>• <b>Comment:</b> Description of entry</li> <li>• <b>IP Address/Netmask:</b> IP address and subnet mask of IP phone network</li> <li>• <b>Zone:</b> Select <b>Untrust</b> from drop down list</li> </ul> 

Step	Description
3.	<p data-bbox="289 241 901 277"><b>CLAN 01A02 IP address entry – Trust Zone:</b></p> <p data-bbox="289 310 1477 436">From the left navigation menu, select <b>Objects → Addresses → List</b>. The address list page is displayed. Select the  button on top right corner of page to create a new address book entry. Enter the following information for CLAN 01A02:</p> <ul data-bbox="337 478 1307 630" style="list-style-type: none"> <li>• <b>Address Name:</b> Name to reference this address book entry by.</li> <li>• <b>Comment:</b> Description of entry</li> <li>• <b>IP Address/Netmask:</b> IP address and subnet mask of IP phone network</li> <li>• <b>Zone:</b> Select <b>Trust</b> from drop down list</li> </ul> 

Step	Description
4.	<p><b>CLAN 01A07 IP address entry – Trust Zone:</b></p> <p>From the left navigation menu, select <b>Objects → Addresses → List</b>. The address list page is displayed. Select the  button on top right corner of page to create a new address book entry. Enter the following information for CLAN 01A07:</p> <ul style="list-style-type: none"> <li>• <b>Address Name:</b> Name to reference this address book entry by.</li> <li>• <b>Comment:</b> Description of entry</li> <li>• <b>IP Address/Netmask:</b> IP address and subnet mask of IP phone network</li> <li>• <b>Zone:</b> Select <b>Trust</b> from drop down list</li> </ul> 

Step	Description
5.	<p data-bbox="289 237 930 268"><b>MedPro 01A03 IP address entry – Trust Zone:</b></p> <p data-bbox="289 310 1477 436">From the left navigation menu, select <b>Objects → Addresses → List</b>. The address list page is displayed. Select the  button on top right corner of page to create a new address book entry. Enter the following information for MedPro 01A03:</p> <ul data-bbox="337 478 1307 630" style="list-style-type: none"> <li>• <b>Address Name:</b> Name to reference this address book entry by.</li> <li>• <b>Comment:</b> Description of entry</li> <li>• <b>IP Address/Netmask:</b> IP address and subnet mask of IP phone network</li> <li>• <b>Zone:</b> Select <b>Trust</b> from drop down list</li> </ul> 


## 6.6. Configuring Custom Service

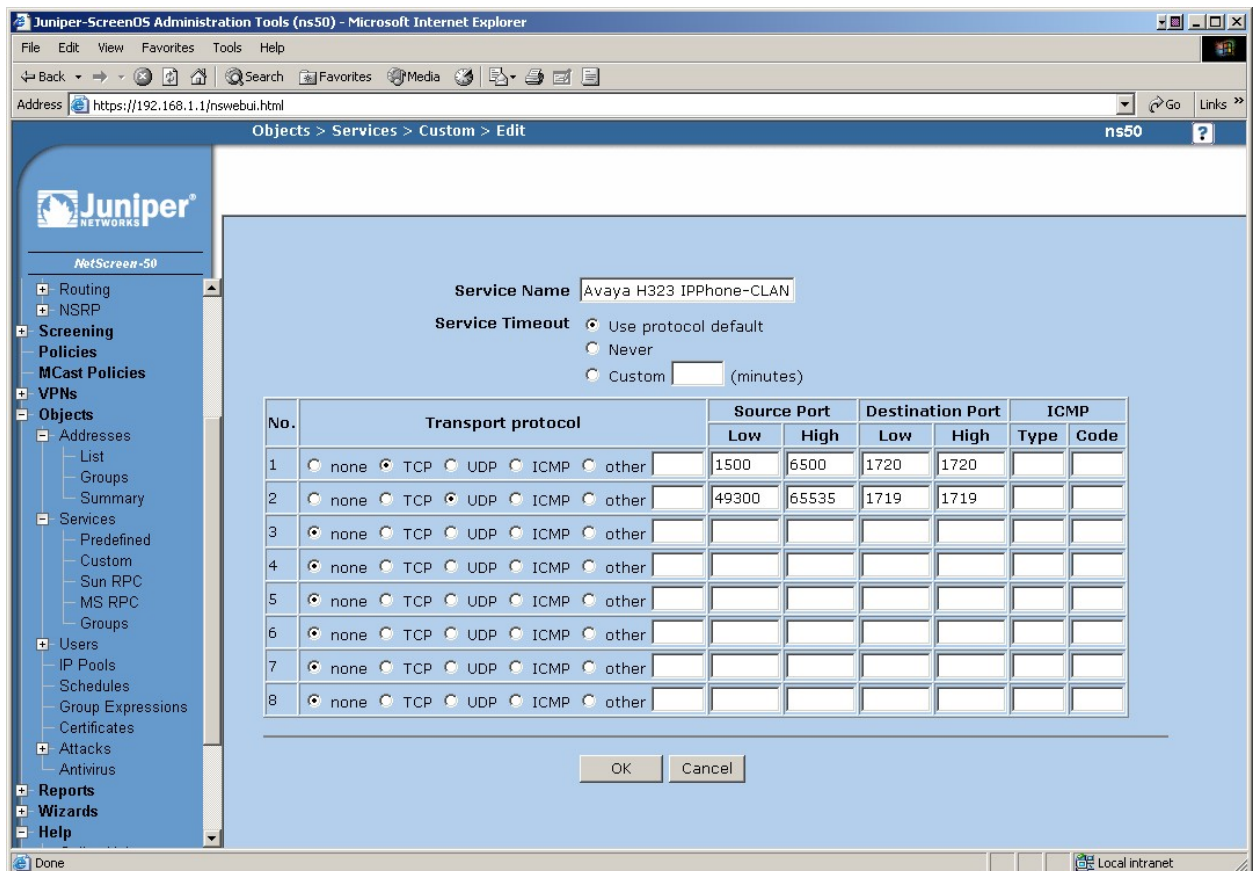
The Juniper NetScreen firewall is pre-configured with over thirty pre-defined Services. A Service has several defining properties that tell the firewall how to identify traffic, i.e. transport protocol and port range. When a security policy is created, a service must be referenced for that policy.

The NetScreen firewall supports the creation of Custom Services. Custom Services are created by an Administrator to either support a protocol not on the pre-defined list or to allow for a tighter match of the properties of a pre-defined protocol.



The steps below create two custom services specific to Avaya Communication Manager traffic flows. One custom service accommodating the H.323 signaling flows and the other accommodating the RTP voice flows. These custom services are a tight match on the transport protocols (UDP/TCP) and port ranges used by Avaya Communications Manager and Avaya IP Telephones.

Step	Description
1.	From the left navigation menu, select <b>Objects → Services → Custom</b> . The custom services page is displayed. Select the  button on top right corner of page to create a new custom service.
2.	Create the <b>Avaya H323 IPPhone-CLAN</b> Custom Service defining the ports and transport protocols used between Avaya IP Telephones and CLAN interfaces for H.323 signaling. Select the <b>Use protocol default</b> option for <b>Service Timeout</b> .



Juniper-ScreenOS Administration Tools (ns50) - Microsoft Internet Explorer

Address: https://192.168.1.1/nswebui.html

Objects > Services > Custom > Edit ns50

Juniper  
NetScreen-50

- Routing
- NSRP
- Screening
  - Policies
  - MCast Policies
- VPNs
- Objects
  - Addresses
    - List
    - Groups
    - Summary
  - Services
    - Predefined
    - Custom
    - Sun RPC
    - MS RPC
    - Groups
  - Users
    - IP Pools
    - Schedules
    - Group Expressions
    - Certificates
  - Attacks
  - Antivirus
- Reports
- Wizards
- Help

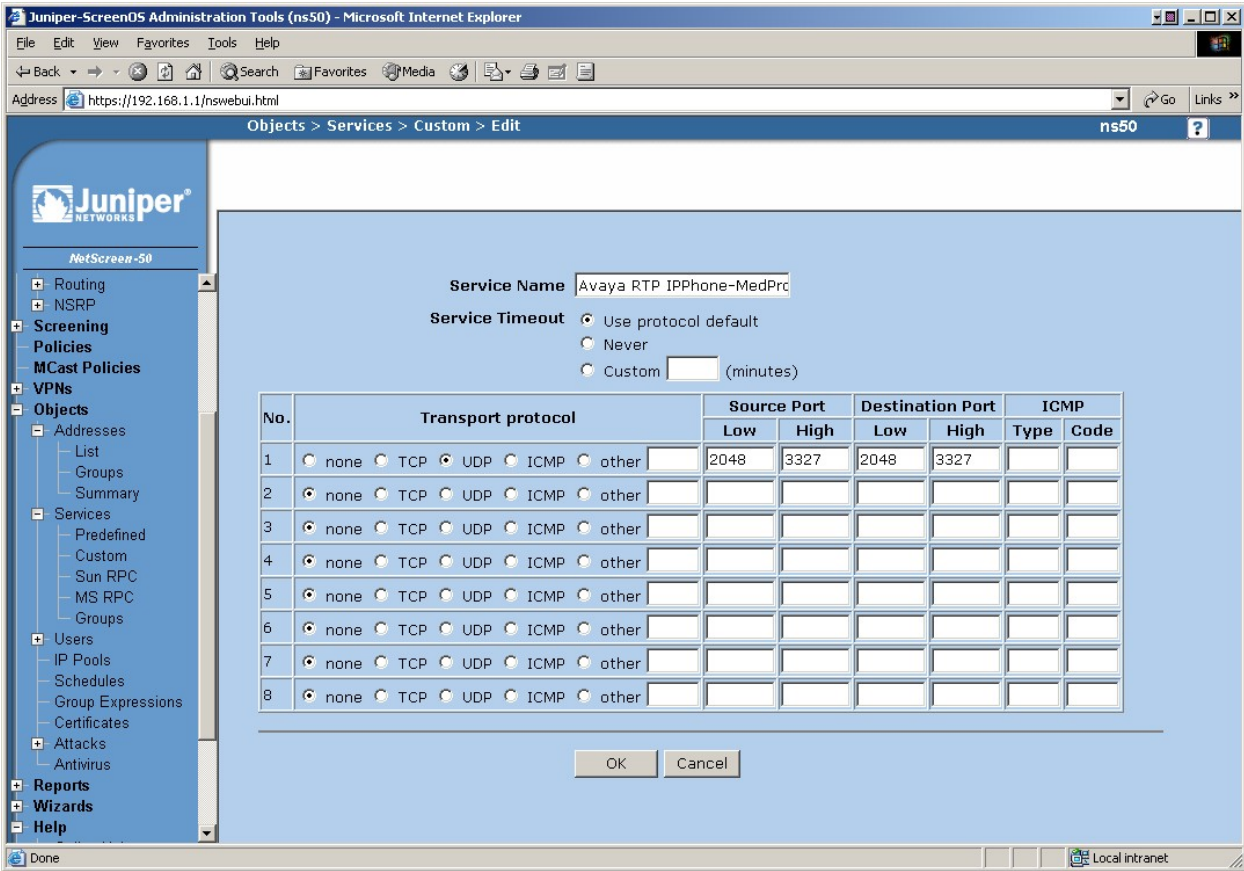
Service Name: Avaya H323 IPPhone-CLAN

Service Timeout:
 ☒ Use protocol default
 ☐ Never
 ☐ Custom  (minutes)

No.	Transport protocol	Source Port		Destination Port		ICMP	
		Low	High	Low	High	Type	Code
1	<input type="radio"/> none <input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> other	1500	6500	1720	1720		
2	<input type="radio"/> none <input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> other	49300	65535	1719	1719		
3	<input checked="" type="radio"/> none <input type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> other						
4	<input checked="" type="radio"/> none <input type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> other						
5	<input checked="" type="radio"/> none <input type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> other						
6	<input checked="" type="radio"/> none <input type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> other						
7	<input checked="" type="radio"/> none <input type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> other						
8	<input checked="" type="radio"/> none <input type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> other						

OK Cancel

Done Local intranet

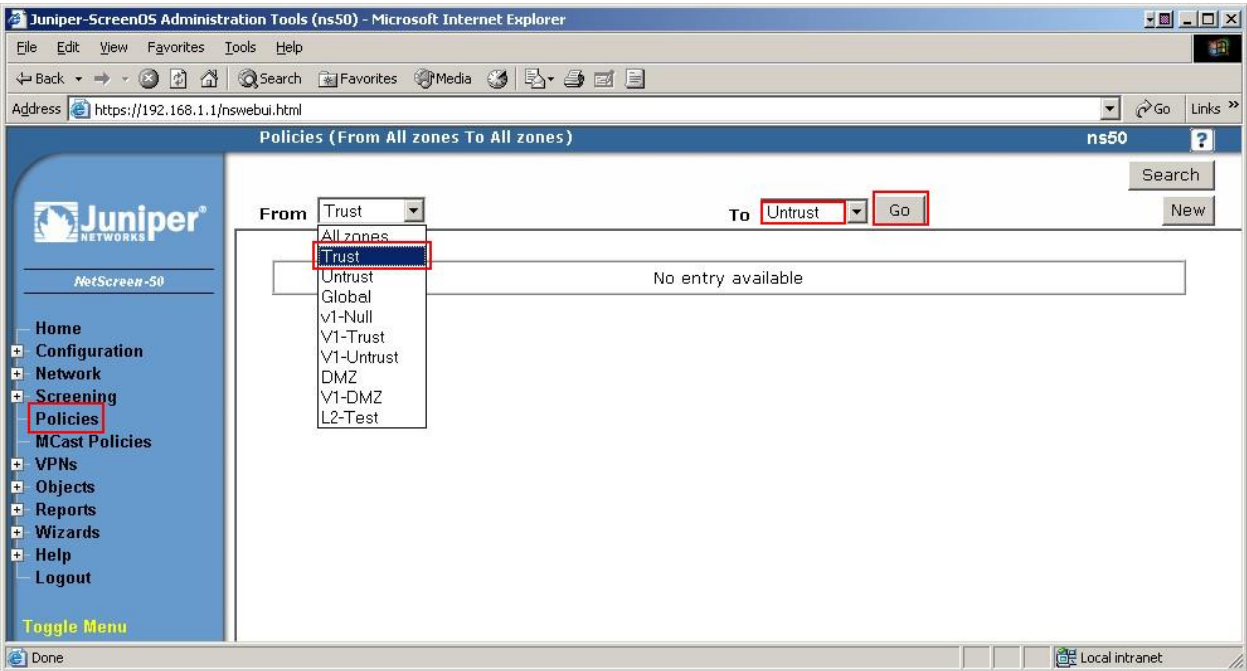
Step	Description
3.	<p>Create the <b>Avaya RTP IPPhone-MedPro</b> Custom Service defining the port range used for voice RTP packets between Avaya IP Telephones and MedPro interfaces. This port range must match the range defined in the <b>ip-network-region</b> form.</p>  <p>The screenshot displays the Juniper-ScreenOS Administration Tools (ns50) web interface. The browser window title is "Juniper-ScreenOS Administration Tools (ns50) - Microsoft Internet Explorer". The address bar shows "https://192.168.1.1/nswebui.html". The navigation pane on the left includes sections like Routing, NSRP, Screening, Policies, MCast Policies, VPNs, Objects, Addresses, Services, Users, IP Pools, Schedules, Group Expressions, Certificates, Attacks, Antivirus, Reports, Wizards, and Help. The "Services" section is expanded, and "Custom" is selected. The main content area shows the "Edit" page for a service named "Avaya RTP IPPhone-MedPro". The "Service Timeout" is set to "Use protocol default". Below this is a table with 8 rows for defining service rules. Row 1 is selected, showing "Transport protocol" as UDP, "Source Port" range 2048-3327, and "Destination Port" range 2048-3327. The table has columns for "No.", "Transport protocol", "Source Port" (Low, High), "Destination Port" (Low, High), and "ICMP" (Type, Code). The "OK" and "Cancel" buttons are at the bottom.</p>

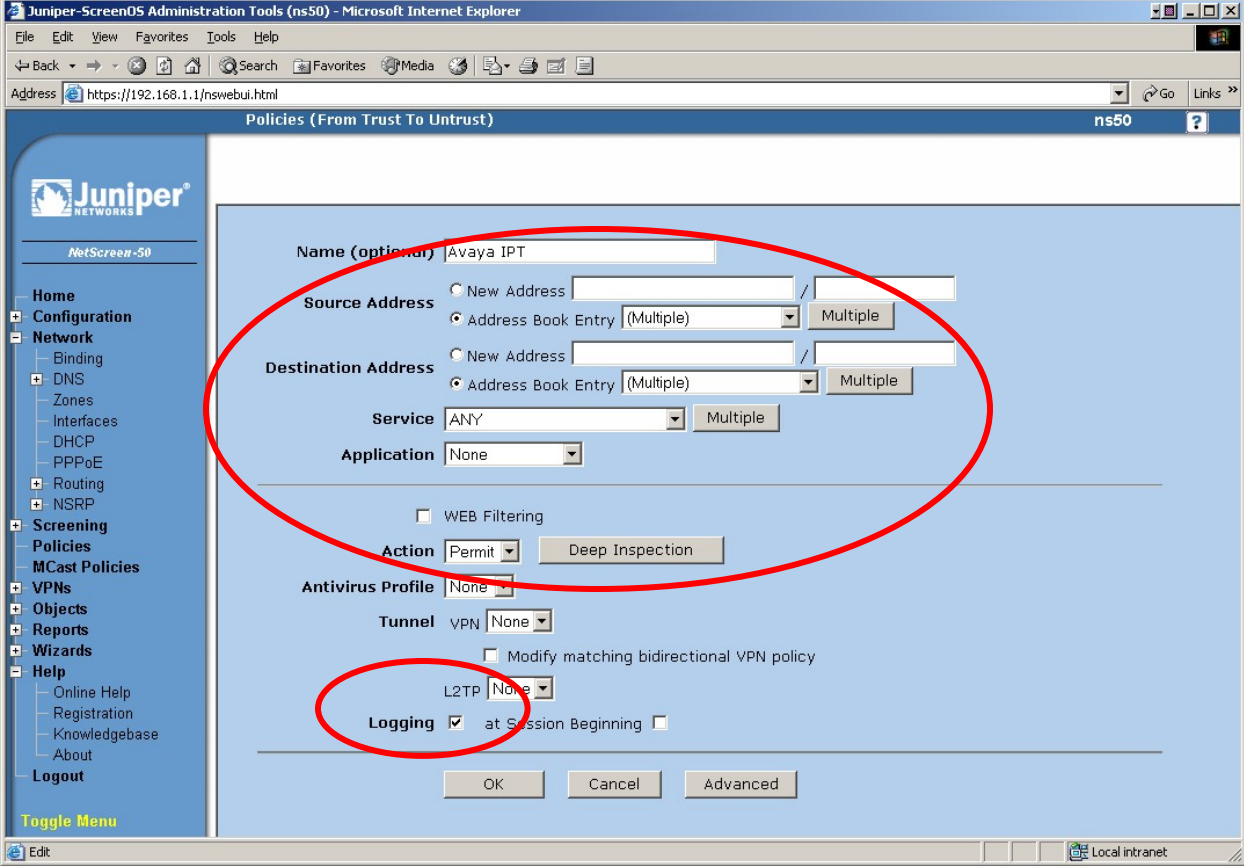


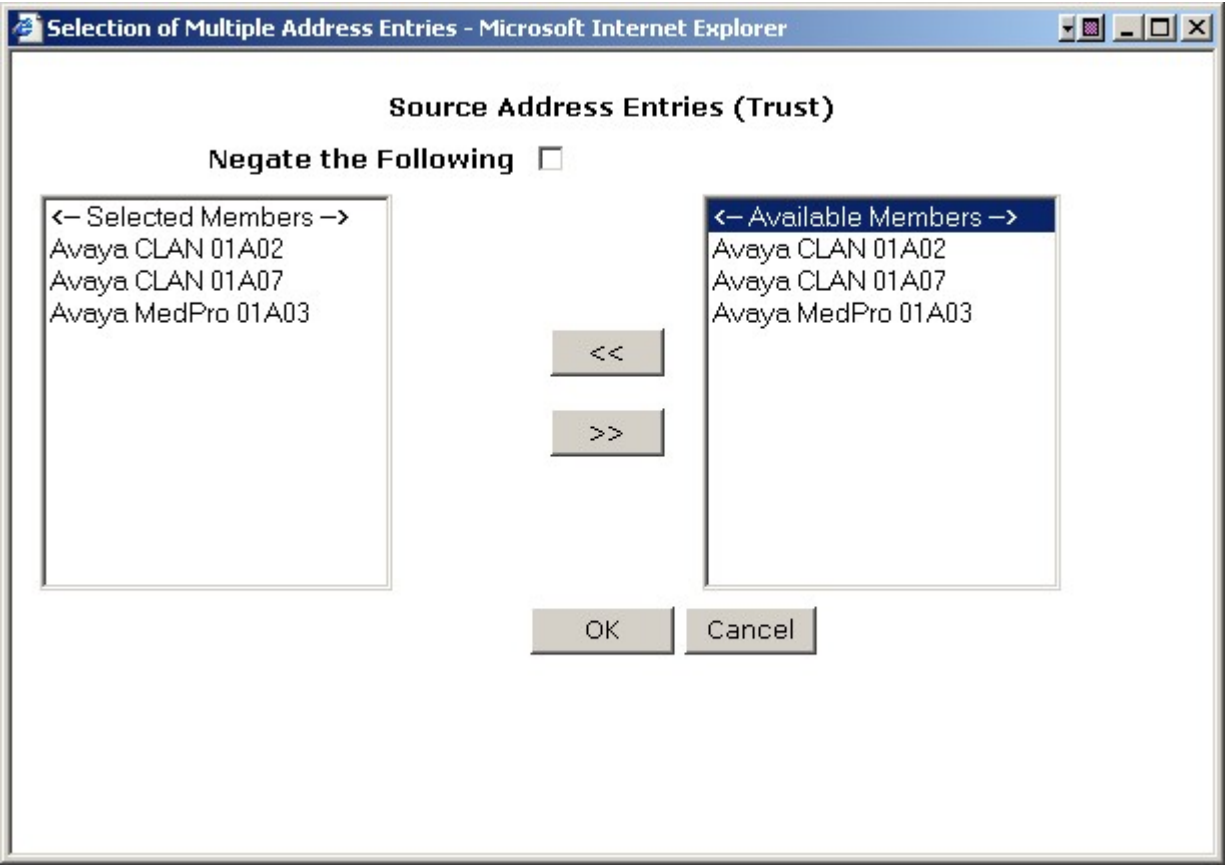
## 6.7. Creating Security Policy

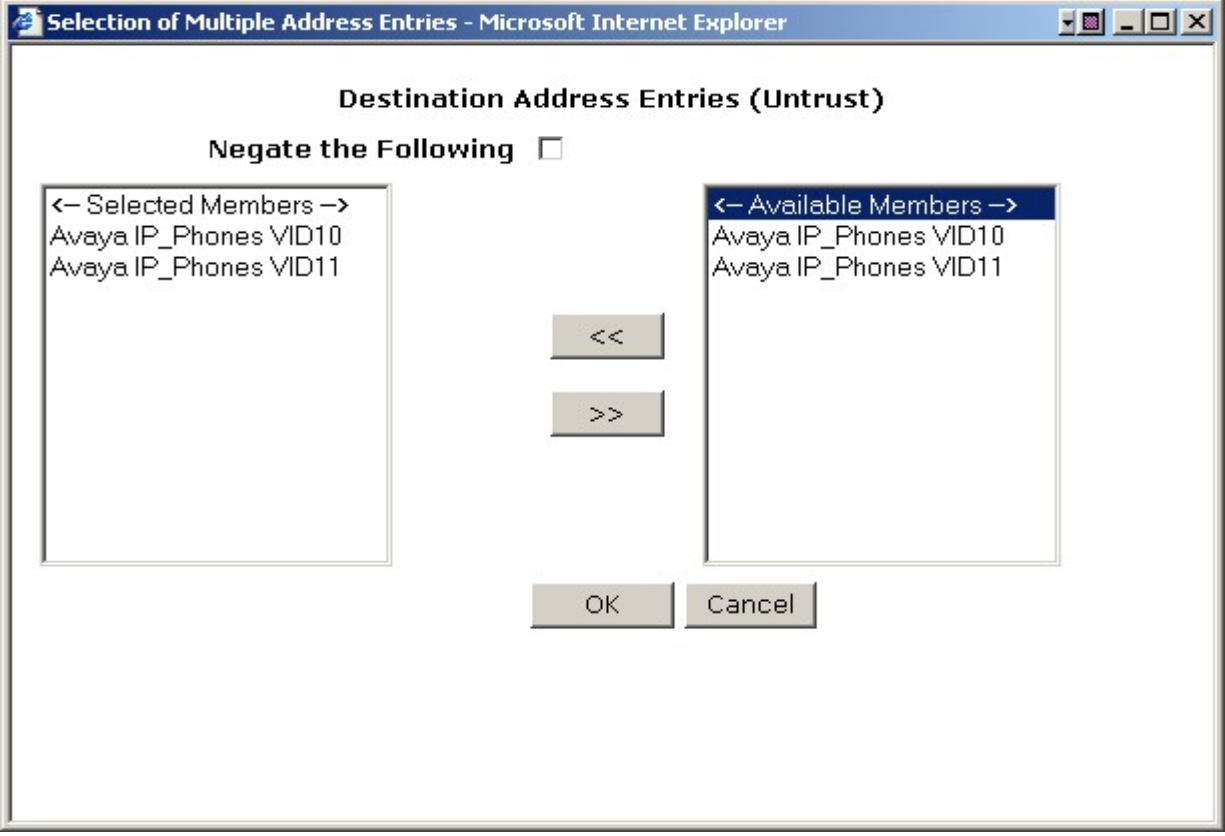
Two Security Policies must be created; one for traffic flowing from the Trust zone to the Untrust zone and the other for traffic flowing from the Untrust zone to the Trust zone. The following steps create these policies.

### 6.7.1. Trust to Untrust policy

Step	Description
1.	From the left navigation menu select <b>Policies</b> . Any currently configured security policies are displayed.
2.	Create a security policy for traffic flowing from the Trust zone, Avaya CLAN and MedPro traffic, to the Untrust zone, Avaya IP Telephones. On the top of the <b>Policies</b> page select <b>Trust</b> on the <b>From</b> drop down list and <b>Untrust</b> on the <b>To</b> drop down list. Select the <b>GO</b> button on top right corner of page to create a new security policy. 

Step	Description
3.	<p>A screen similar the one below appears offering several configuration options for this new policy.</p> <p>Key configuration options highlight below:</p> <ul style="list-style-type: none"> <li>• <b>Name (Optional):</b> Avaya IPT.</li> <li>• <b>Source Address:</b> (Multiple) See <b>Source Address Entries (Trust)</b> in <b>Step 4</b> below.</li> <li>• <b>Destination Address:</b> (Multiple) See <b>Destination Address Entries (Untrust)</b> in <b>Step 5</b> below.</li> <li>• <b>Service:</b> Enter the server of <b>ANY</b> to allow all application types</li> <li>• <b>Application :</b> None</li> <li>• <b>Action:</b> Select <b>Permit</b> from the drop down list.</li> <li>• <b>Logging:</b> enabled (checked) to see this policy events in the local NetScreen log or with syslog.</li> </ul> 

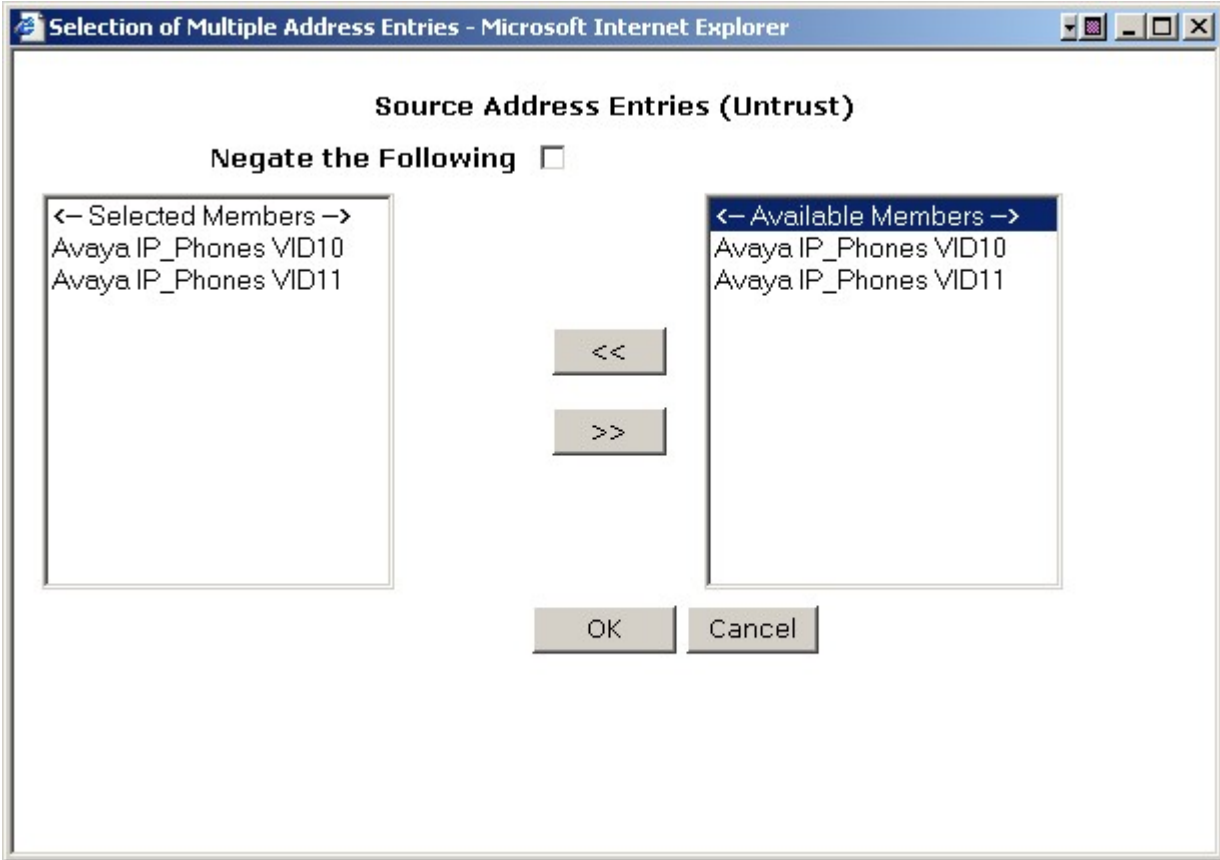
Step	Description
4.	<p>From the <b>Policies (From Trust to Untrust)</b> screen above, select <b>Source Address → Address Book Entry → Multiple</b> button. A screen similar to the one below appears. The CLAN and MedPro Address Book entries from <b>6.5 Create Address Book Entries</b> appear in the <b>Available Members</b> list.</p> <ul style="list-style-type: none"> <li>• Select the MedPro and CLAN entries from the <b>Available Members</b> list so they appear in the <b>Selected Members</b> list.</li> <li>• Select the <b>OK</b> button</li> </ul> 

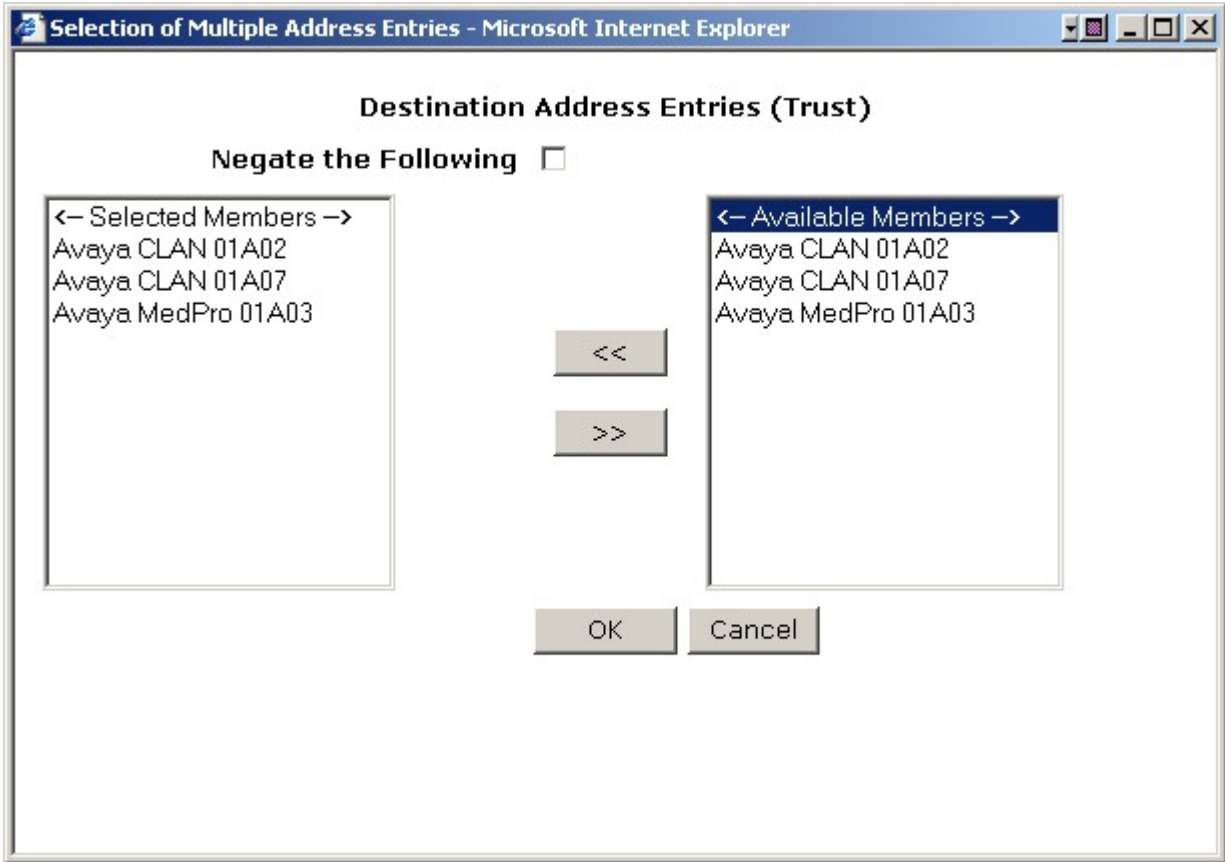
Step	Description
5.	<p>From the <b>Policies (From Trust to Untrust)</b> screen above, select <b>Destination Address → Address Book Entry → Multiple</b> button. A screen similar to the one below appears. The Avaya IP Telephone Address Book entries from <b>6.5 Create Address Book Entries</b> appear in the <b>Available Members</b> list.</p> <ul style="list-style-type: none"> <li>• Select the Avaya IP Telephone entries from the <b>Available Members</b> list so they appear in the <b>Selected Members</b> list.</li> <li>• Select the <b>OK</b> button</li> </ul> 
6.	<p>Select the OK button from the <b>Policies (From Trust to Untrust)</b> screen to complete the creation of the <b>Trust to Untrust policy</b> with the name <b>Avaya IPT</b>.</p>

### 6.7.2. Untrust to Trust policy

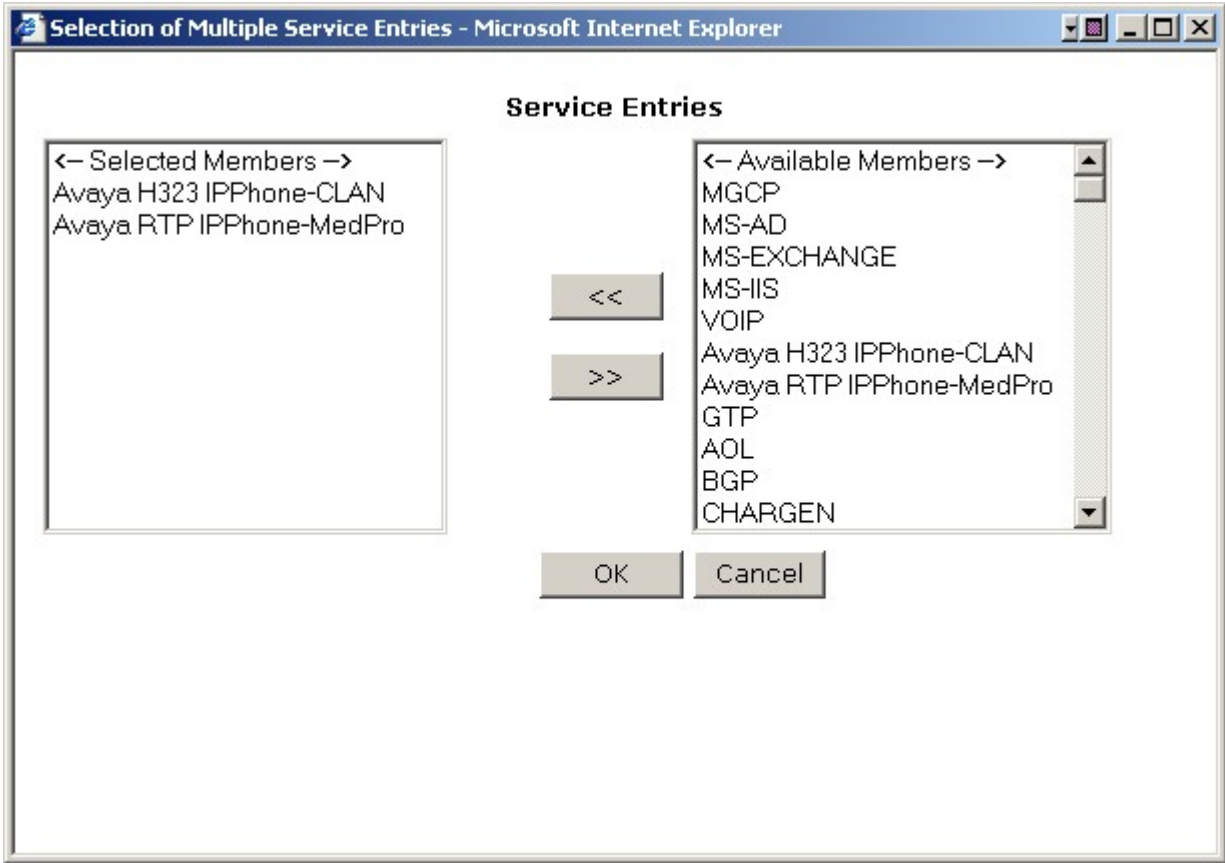
Step	Description
1.	Create a security policy for traffic flowing from the Untrust zone, Avaya IP Telephone traffic, to the Trust zone, Avaya CLAN and MedPro. On the top of the <b>Policies</b> page select <b>Untrust</b> on the <b>From</b> drop down list and <b>Trust</b> on the <b>To</b> drop down list. Select the <b>GO</b> button on top right corner of page to create a new security policy.
2.	<p>A screen similar the one below appears offering several configuration options for this new policy.</p> <p>Key configuration options highlight below:</p> <ul style="list-style-type: none"><li>• <b>Name (Optional):</b> Avaya IP Phones.</li><li>• <b>Source Address:</b> (Multiple) See <b>Source Address Entries (Untrust)</b> in <b>Step 3</b> below.</li><li>• <b>Destination Address:</b> (Multiple) See <b>Destination Address Entries (Trust)</b> in <b>Step 4</b> below.</li><li>• <b>Service:</b> (Multiple) See <b>Service Entries</b> in <b>Step 5</b> below.</li><li>• <b>Application :</b> None</li><li>• <b>Action:</b> Select <b>Permit</b> from the drop down list.</li><li>• <b>Logging:</b> enabled (checked) to see this policy events in the local NetScreen log or with syslog.</li></ul>

Step	Description

Step	Description
3.	<p>From the <b>Policies (From Untrust to Trust)</b> screen above, select <b>Source Address → Address Book Entry → Multiple</b> button. A screen similar to the one below appears. The Avaya IP Telephone Address Book entries from <b>6.5 Create Address Book Entries</b> appear in the <b>Available Members</b> list.</p> <ul style="list-style-type: none"> <li>• Select the Avaya IP Telephone entries from the <b>Available Members</b> list so they appear in the <b>Selected Members</b> list.</li> <li>• Select the <b>OK</b> button.</li> </ul> 

Step	Description
4.	<p>From the <b>Policies (From Untrust to Trust)</b> screen above, select <b>Destination Address → Address Book Entry → Multiple</b> button. A screen similar to the one below appears. The CLAN and MedPro Address Book entries from <b>6.5 Create Address Book Entries</b> appear in the <b>Available Members</b> list.</p> <ul style="list-style-type: none"> <li>• Select the CLAN and MedPro entries from the <b>Available Members</b> list so they appear in the <b>Selected Members</b> list.</li> <li>• Select the <b>OK</b> button</li> </ul> 



Step	Description
5.	<p>From the <b>Policies (From Untrust to Trust)</b> screen above, select <b>Service → Multiple</b> button. A screen similar to the one below appears. The Avaya H.323 and Avaya RTP customer service entries from <b>6.6 Configuring Custom services</b> appear in the <b>Available Members</b> list.</p> <ul style="list-style-type: none"> <li>• Select the <b>Avaya H.323 IPPhone-CLAN</b> and <b>Avaya RTP IPPhone-MedPro</b> entries from the <b>Available Members</b> list so they appear in the <b>Selected Members</b> list.</li> <li>• Select the <b>OK</b> button</li> </ul> 
6.	<p>Select the <b>OK</b> button from the <b>Policies (From Trust to Untrust)</b> screen to complete the creation of the <b>Untrust to Trust</b> policy with the name <b>Avaya IP Phones</b>.</p>

### 6.7.3. Summary of Avaya IP Telephone Security Policies

Step	Description
1.	<p>From the left navigation menu select <b>Policies</b>. The new security policies created in <b>Sections 6.7.1</b> and <b>6.7.2</b> will be displayed as well as any previously configured security policies.</p> <p>The green check icon the Action column indicates the policy is active. The icon in the Options column indicates logging for this policy is enabled.</p>

Juniper-ScreenOS Administration Tools (ns50) - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Search Favorites Media Print Mail Print Mail

Address https://192.168.1.1/nswebui.html Go Links

Policies (From All zones To All zones) ns50

List 20 per page

From All zones To All zones Go

Search New

Juniper NETWORKS

NetScreen-50

Home

Configuration

Network

- Binding
- DNS
- Zones
- Interfaces
- DHCP
- PPPoE
- Routing
- NSRP

Screening

- Policies
- MCast Policies

VPNs

Objects

Reports

Wizards

Help

- Online Help
- Registration
- Knowledgebase
- About

Logout

Toggle Menu

From Trust To Untrust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
1	Avaya CLAN 01A02 Avaya CLAN 01A07 Avaya MedPro 01A03	Avaya IP_Phones VID10 Avaya IP_Phones VID11	ANY			<a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Remove</a>	<input checked="" type="checkbox"/>	

From Untrust To Trust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
2	Avaya IP_Phones VID10 Avaya IP_Phones VID11	Avaya CLAN 01A02 Avaya CLAN 01A07 Avaya MedPro 01A03	Avaya H323 IPPhone-CLAN Avaya RTP IPPhone-MedPro			<a href="#">Edit</a> <a href="#">Clone</a> <a href="#">Remove</a>	<input checked="" type="checkbox"/>	

Local intranet

## 7. Avaya Communication Manager Configuration

Avaya Communication Manager allows the RTP/RTCP port range to be configurable through the **ip-network-region** form. UDP ports 2048 – 3327 are the default range as of Avaya Communication Manager Release 3.1. The following steps modify the **ip-network-region 1** RTP port range.

Step	Description
1.	<p>From the System Access Terminal (SAT), enter the change <b>ip-network-region x</b> command where x is the region number to modify. Under Media Parameters, enter the UDP Port Min: (which must be an even number) and UDP Port Max: (which must be an odd number). This port range must match the Custom Service port range created in section 6.6 Configuring Custom Service.</p> <pre>change ip-network-region 1                                     Page 1 of 19 IP NETWORK REGION Region: 1 Location: Authoritative Domain: avaya.com Name: MEDIA PARAMETERS   Codec Set: 1   UDP Port Min: 2048   UDP Port Max: 3327 DIFFSERV/TOS PARAMETERS   Call Control PHB Value: 46   Audio PHB Value: 46   Video PHB Value: 26 802.1P/Q PARAMETERS   Call Control 802.1p Priority: 6   Audio 802.1p Priority: 6   Video 802.1p Priority: 5 H.323 IP ENDPOINTS   H.323 Link Bounce Recovery? y   Idle Traffic Interval (sec): 20   Keep-Alive Interval (sec): 5   Keep-Alive Count: 5 Intra-region IP-IP Direct Audio: yes Inter-region IP-IP Direct Audio: yes IP Audio Hairpinning? y RTCP Reporting Enabled? y RTCP MONITOR SERVER PARAMETERS Use Default Server Parameters? y AUDIO RESOURCE RESERVATION PARAMETERS RSUP Enabled? n ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh</pre>
2.	Enter the <b>save translation all</b> command to save.

## 8. Conclusion

These Application Notes describe the steps necessary to implement a Juniper NetScreen Firewall as an interior firewall protecting critical components of Avaya Communication Manager platform. The security policies are tightly implemented to accommodate the H.323 Application Layer Gateway (ALG) being disabled.

## 9. References

1. **Juniper Networks: Concepts & Examples ScreenOS Reference Guide; Volume 6: Voice-over-Internet Protocol** *Release 5.3.0, Rev. B*, <http://www.juniper.net>
2. Cameron R., Cantrell C., Killion D., Russell K., Tam K. (2005) **Configuring NetScreen Firewalls**. Rockland: Syngress Publishing, Inc., <http://www.juniper.net>
3. Additional Avaya Application Notes and Resources are available, <http://avaya.com/gcm/master-usa/en-us/resource/>

---

**©2006 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at [interoplabnotes@list.avaya.com](mailto:interoplabnotes@list.avaya.com)