



Avaya Solution and Interoperability Test Lab

How to Configure the Juniper NetScreen 5GT to Support Avaya H.323 IP Telephony – Issue 1.0

Abstract

These Application Notes describe how to configure the Juniper NetScreen 5GT to support Avaya H.323 IP Telephony. The sample configuration presented in these Application Notes illustrates how a Juniper NetScreen 5GT firewall can be configured to protect Avaya C-LANs and Media Processor boards using security policies which only allow H.323 signaling, RTP, and H.248 traffic to pass through the firewall.

1. Introduction

These Application Notes describe how to configure the Juniper NetScreen 5GT to support Avaya H.323 IP Telephony. The sample configuration presented in these Application Notes illustrates how a Juniper NetScreen 5GT firewall can be configured to protect Avaya C-LANs and Media Processor boards using security policies which only allow H.323 signaling, RTP, and H.248 traffic to pass through the firewall.

The Juniper NetScreen-5GT appliance integrates multiple security functions - Stateful and Deep Inspection firewall, IPSec VPN (Virtual Private Network), denial of service protection, anti-virus and Web filtering. The focus of these Application Notes is on using the Juniper NetScreen 5GT as an “interior firewall”, within the enterprise network, to protect the Avaya C-LAN and Media Processor boards.

The Juniper NetScreen 5GT has five Ethernet interfaces. One of the five Ethernet interfaces was configured for the public or “untrust” security zone. The C-LAN and Media Processors were connected to the other four interfaces which were configured for the private or “trust” security zone.

Each security zone is assigned to its own virtual router, “untrust-vr” for the “untrust” security zone and “trust-vr” for the “trust” security zone. This allows the Juniper NetScreen 5GT device to maintain two separate routing tables and to conceal the routing information in one virtual router from the other. A static route is configured for the trust-vr virtual router to define the untrust-vr as the next hop to allow traffic to pass between the two security zones.

In the configuration tested in these Application Notes:

- The H.323 Application Layer Gateway (ALG) was disabled.
- The Juniper NetScreen 5GT firewall was configured in “route” mode so Network Address Translation (NAT) is not used.
- The security policies defined were limited to traffic flows to and from the Avaya C-LAN and Media Processor boards.

The following items were tested when the Avaya C-LAN and Media Processor boards were placed behind the Juniper NetScreen 5GT firewall:

- Ability of the Avaya IP Telephones to register successfully and place calls
- Ability of the Avaya G350 Media Gateway to register successfully
- Ability of the Avaya Enterprise Survivable Server (ESS) to register successfully and participate in calls
- Ability of the Avaya S8300 Media Server in Local Survivable Processor (LSP) mode to register successfully
- File synchronization to successfully occur between the primary Avaya S8720 Media Servers and the ESS and LSP servers
- Shuffled and non-shuffled H.323 calls
- Failover from the primary Avaya S8720 Media Servers to the ESS and LSP servers and recovery back to the primary Media Servers

Table 2 lists the ports that were opened on the Juniper NetScreen 5GT to support the configuration shown in **Figure 1**. For more information regarding these ports, refer to [1] in Section 7.

From	TCP/UDP Port or Protocol	To	TCP/UDP Port or Protocol	Notes
Any endpoint	UDP any	Any C-LAN	UDP 1719	For endpoint registration (RAS).
Any endpoint	TCP any	Any C-LAN	TCP 1720	For H.225 call signaling.
Any endpoint	UDP any	Any MedPro	UDP 2048-3327 (UDP port range on the IP Network Region form)	To facilitate RTP/RTCP audio streams between MedPros and endpoints.
G700/G350/G250	TCP any	Any C-LAN	TCP 1039	For encrypted H.248 signaling between the Avaya G700 or G350 Media Gateway and call server.
G700/G350/G250	TCP any	Any C-LAN	TCP 2945	For unencrypted H.248 signaling between the Avaya G700 or G350 Media Gateway and call server.
Any endpoint	ICMP any	Any C-LAN and Any MedPro	ICMP any	For diagnostic purposes.

Table 1 – TCP/UDP Ports

Figure 1 illustrates the configuration that was used to verify these Application Notes.

***Note:** The administration of the network infrastructure shown in **Figure 1** is not the focus of these Application Notes and will not be covered. Instead, the focus of these Application Notes is on configuring the Juniper NetScreen 5GT as an “interior firewall”.*

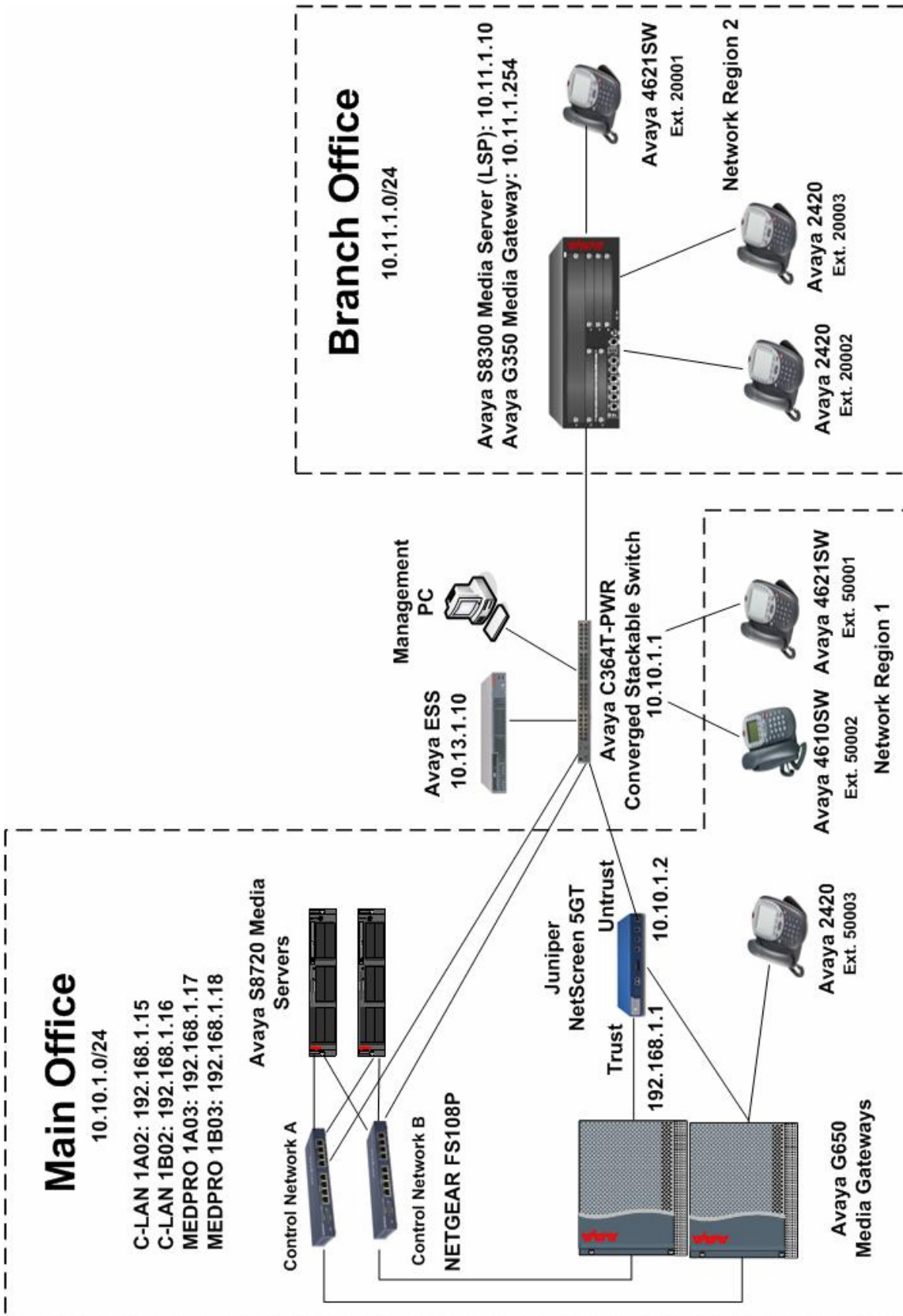


Figure 1 – Network Configuration Diagram

Table 1 lists the IP address assignment for the equipment shown in **Figure 1**.

Equipment	IP Network/Mask	Description
S8720 Media Server – 1		
Ethernet 0	1.1.1.1/24	Control Network A
Ethernet 1	192.11.13.6/30	Services Port
Ethernet 2	192.11.13.13/30	Server Duplication Link
Ethernet 3	2.2.2.1/24	Control Network B
Ethernet 4	10.10.1.11/24	Corporate LAN
Active Server	10.10.1.10/24	Active server address for Corporate Network
Gateway	10.10.1.1/24	Gateway address
S8720 Media Server – 2		
Ethernet 0	1.1.1.2/24	Control Network A
Ethernet 1	192.11.13.6/30	Services Port
Ethernet 2	192.11.13.14/30	Server Duplication Link
Ethernet 3	2.2.2.2/24	Control Network B
Ethernet 4	10.10.1.12/24	Corporate LAN
Active Server	10.10.1.10/24	Active server address for Corporate Network
Gateway	10.10.1.1/24	Gateway address
IPSI – A	1.1.1.3/24	IPSI connected to Control Network A
Gateway	1.1.1.254/24	Gateway address
IPSI – B	2.2.2.3/24	IPSI connected to Control Network B
Gateway	2.2.2.254/24	Gateway address
C-LAN – A	192.168.1.15/24	C-LAN in Avaya G650 A carrier
Gateway	192.168.1.1/24	Gateway address
C-LAN – B	192.168.1.16/24	C-LAN in Avaya G650 B carrier
Gateway	192.168.1.1/24	Gateway address
MedPro – A	192.168.1.17/24	Media Processor in Avaya G650 A carrier
Gateway	192.168.1.1/24	Gateway address
MedPro – B	192.168.1.18/24	Media Processor in Avaya G650 B carrier
Gateway	192.168.1.1/24	Gateway address
ESS (S8500)	10.13.1.10/24	Enterprise Survivable Server
LSP (S8300)	10.11.1.10/24	Local Survivable Processor
G350 (GW)	10.11.1.254/24	Avaya G350 Media Gateway
G350 (WAN)	10.12.1.2	Avaya G350 WAN interface
Avaya C364T-PWR	10.10.1.1	Router interface connected to Juniper NetScreen 5GT
Juniper NetScreen 5GT	10.10.1.2	Public interface address
	192.168.1.1	Private interface address

Table 2 – IP Address Assignment

2. Equipment and Software Validated

The following hardware and software versions were used for this configuration:

Equipment	Version
Avaya S8710 Media Server	3.1.1 Load 628.7 and Service Pack 11640
Avaya G650 Media Gateway Avaya TN2312BP IPSI Avaya TN799DP C-LAN Avaya TN2602AP MEDPRO	HW12 FW030 HW01 FW017 HW20 FW108
Avaya S8500 Media Server (ESS)	3.1.1 Load 628.7 and Service Pack 11640
Avaya S8300 Media Server (LSP)	3.1.1 Load 628.7 and Service Pack 11640
Avaya C364T-PWR Converged Stackable Switch	4.5.14
Avaya G350 Media Gateway	25.23.0
Avaya 4610SW IP Telephone	2.4
Avaya 4621SW IP Telephone	2.4
Avaya 2420 Digital Telephone	---
Avaya 6408D+ Digital Telephone	---
Avaya 6211 Analog Telephone	---
Juniper NetScreen 5GT	5.3.0r2.0

Table 3 – Equipment and Version Validated

3. Juniper NetScreen 5GT Configuration

The following section describes the Juniper NetScreen 5GT configuration to support H.323 registration for Avaya IP telephones and Media Gateways.

3.1. Log in to the Juniper NetScreen 5GT Management Interface

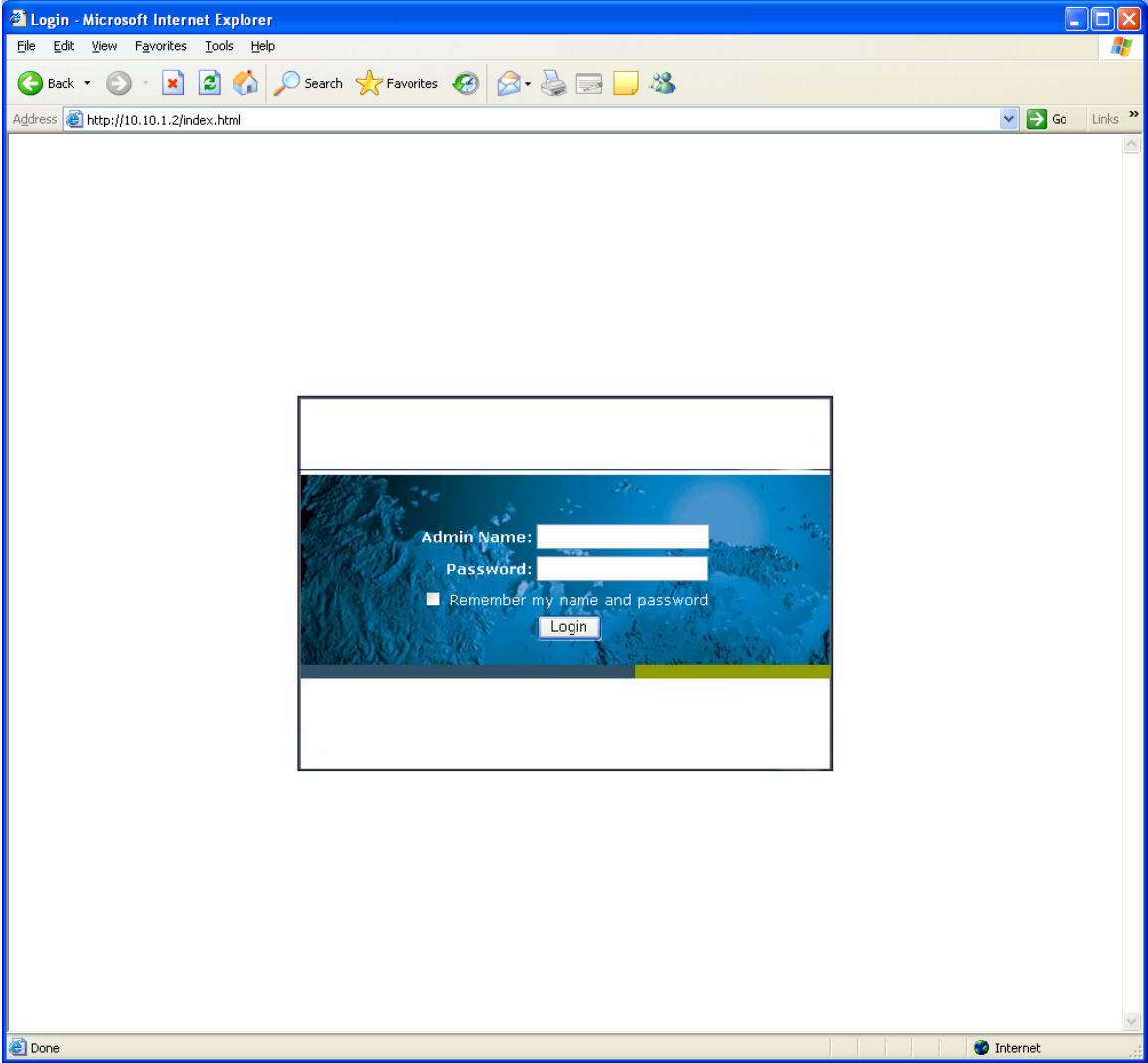
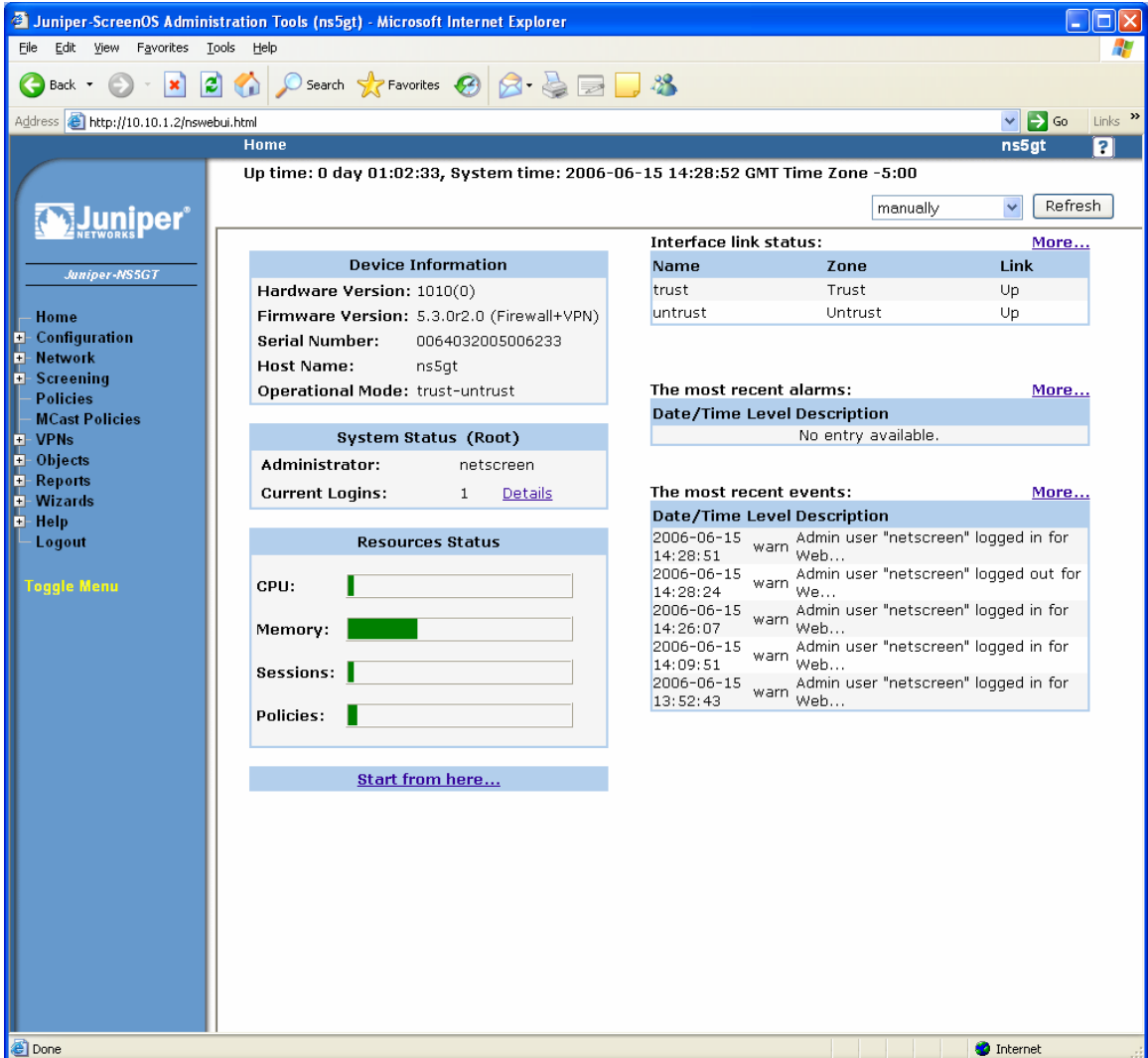
Step	Description
1.	<p>Enter the URL of the Juniper NetScreen 5GT management interface (e.g., <a href="http://<ip address of the Juniper NetScreen 5GT>">http://<ip address of the Juniper NetScreen 5GT>) in a browser window and the login screen shown in Figure 2 will appear. Log in using the appropriate credentials.</p> 

Figure 2 – Juniper NetScreen 5GT Login Screen

Step	Description
2.	<p>The screen shown in Figure 3 will be displayed after successful login.</p>  <p>Figure 3 – Juniper NetScreen 5GT Home Page</p>

3.2. Globally Disable the H.323 Application Layer Gateway

The required ports will be defined using the Juniper NetScreen 5GT security policies instead of using the H.323 Application Layer Gateway feature.

Step	Description
1.	From the navigation menu on the left, select Configuration → Advanced → ALG → Configure .
2.	Uncheck the H.323 check box to globally disable the H.323 Application Layer Gateway as shown in Figure 4 . Click Apply .

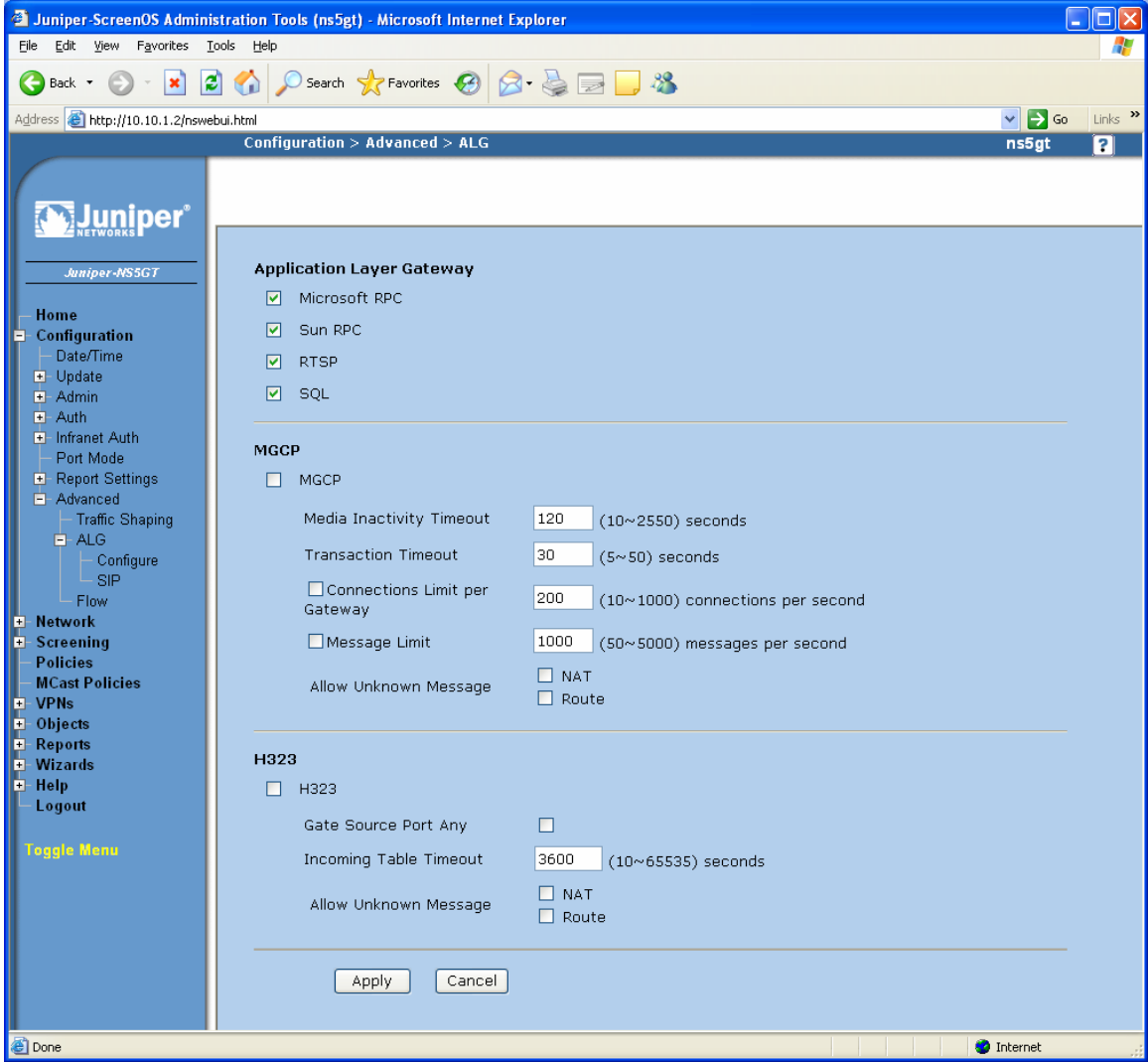
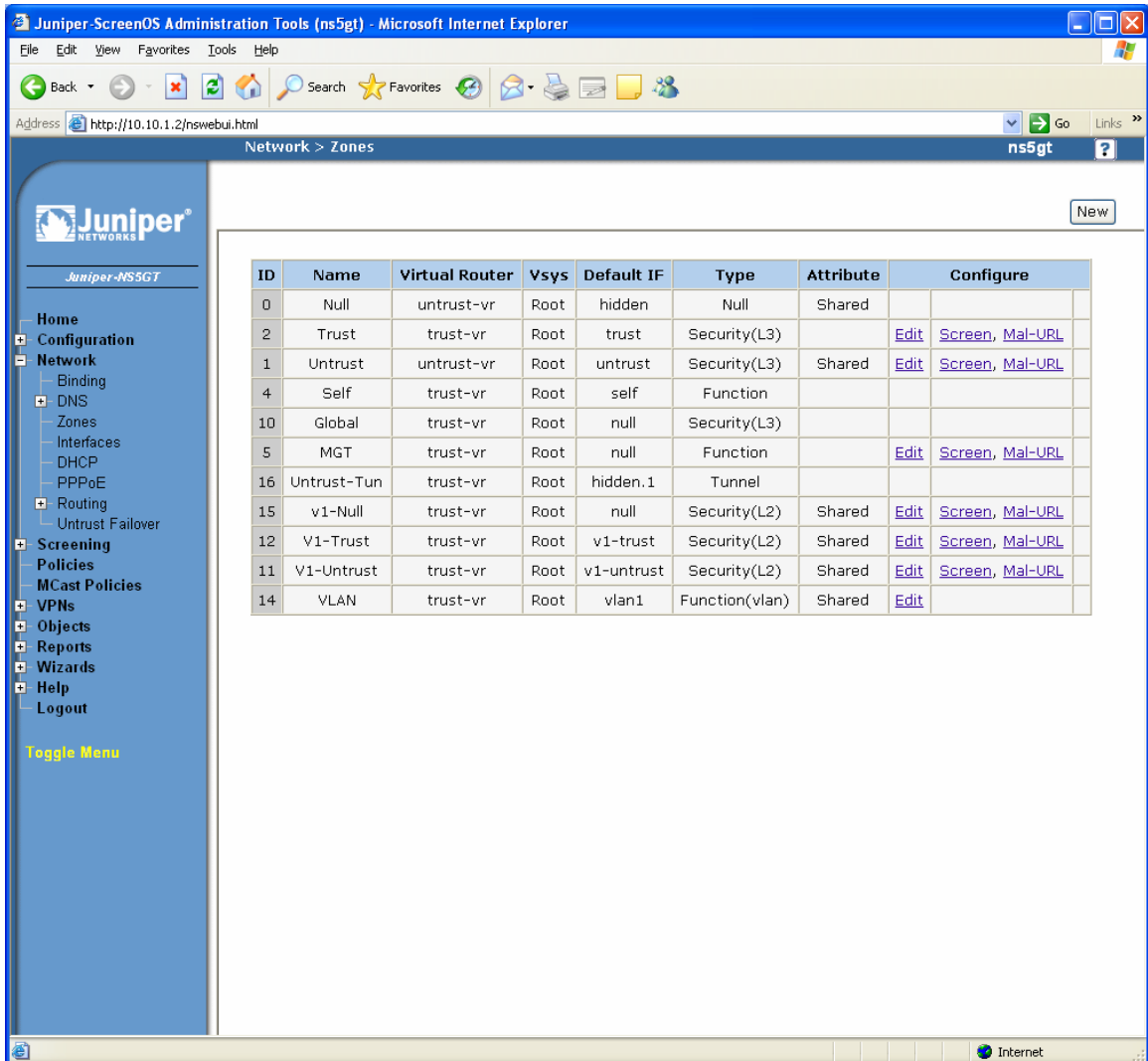


Figure 4 – ALG Configuration

3.3. Configure Security Zones

The steps in this section assigns virtual router name “trust-vr” to the “trust” or private security zone and “untrust-vr” to the “untrust” or public security zone.

Step	Description
1.	From the navigation menu on the left, select Network → Zones to view the network security zones of the Juniper NetScreen 5GT as shown in Figure 5 .



ID	Name	Virtual Router	Vsys	Default IF	Type	Attribute	Configure
0	Null	untrust-vr	Root	hidden	Null	Shared	
2	Trust	trust-vr	Root	trust	Security(L3)		Edit Screen , Mal-URL
1	Untrust	untrust-vr	Root	untrust	Security(L3)	Shared	Edit Screen , Mal-URL
4	Self	trust-vr	Root	self	Function		
10	Global	trust-vr	Root	null	Security(L3)		
5	MGT	trust-vr	Root	null	Function		Edit Screen , Mal-URL
16	Untrust-Tun	trust-vr	Root	hidden.1	Tunnel		
15	v1-Null	trust-vr	Root	null	Security(L2)	Shared	Edit Screen , Mal-URL
12	V1-Trust	trust-vr	Root	v1-trust	Security(L2)	Shared	Edit Screen , Mal-URL
11	V1-Untrust	trust-vr	Root	v1-untrust	Security(L2)	Shared	Edit Screen , Mal-URL
14	VLAN	trust-vr	Root	vlan1	Function(vlan)	Shared	Edit

Figure 5 – Network Zones

Figure 5 – Network Zones

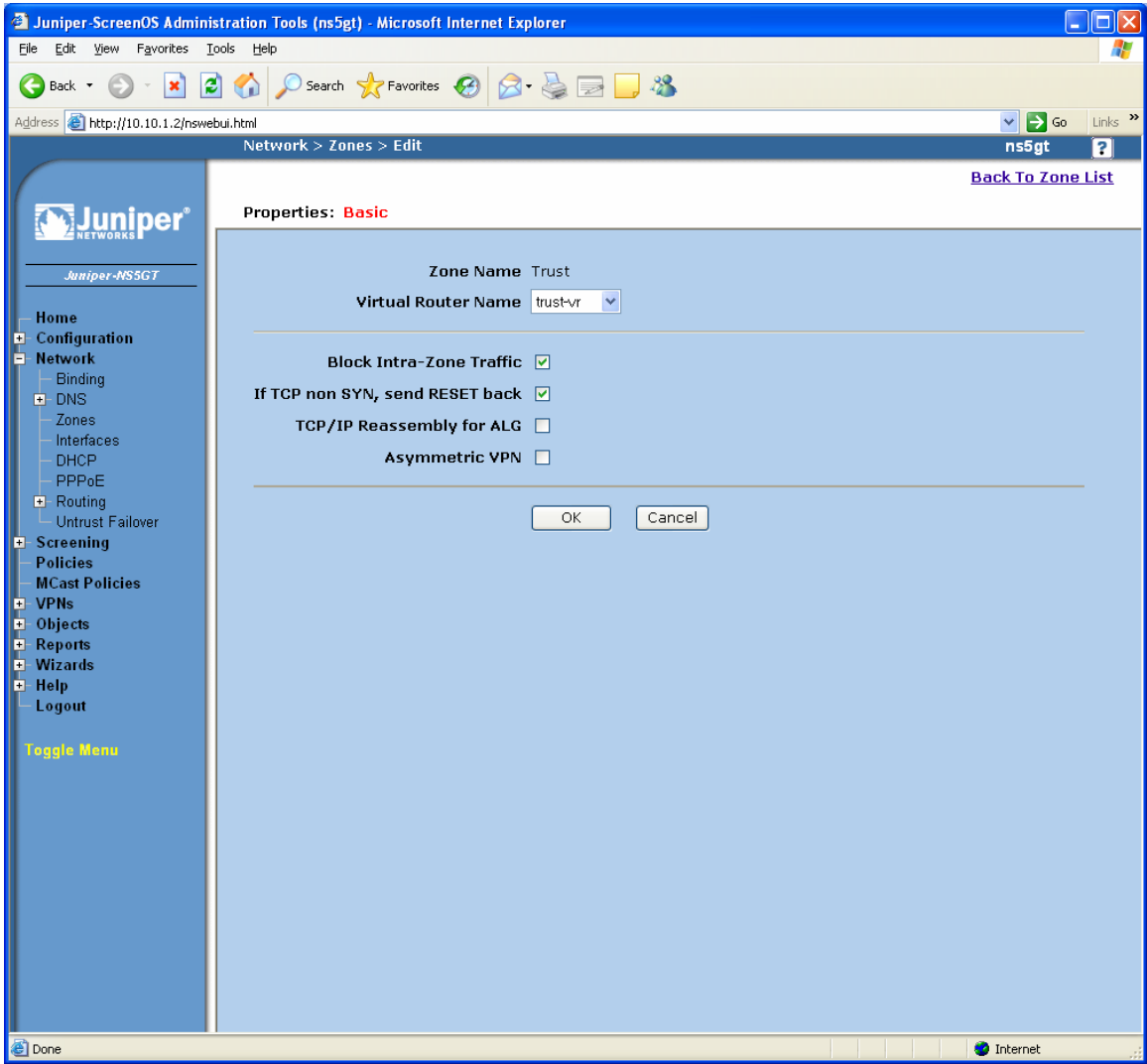
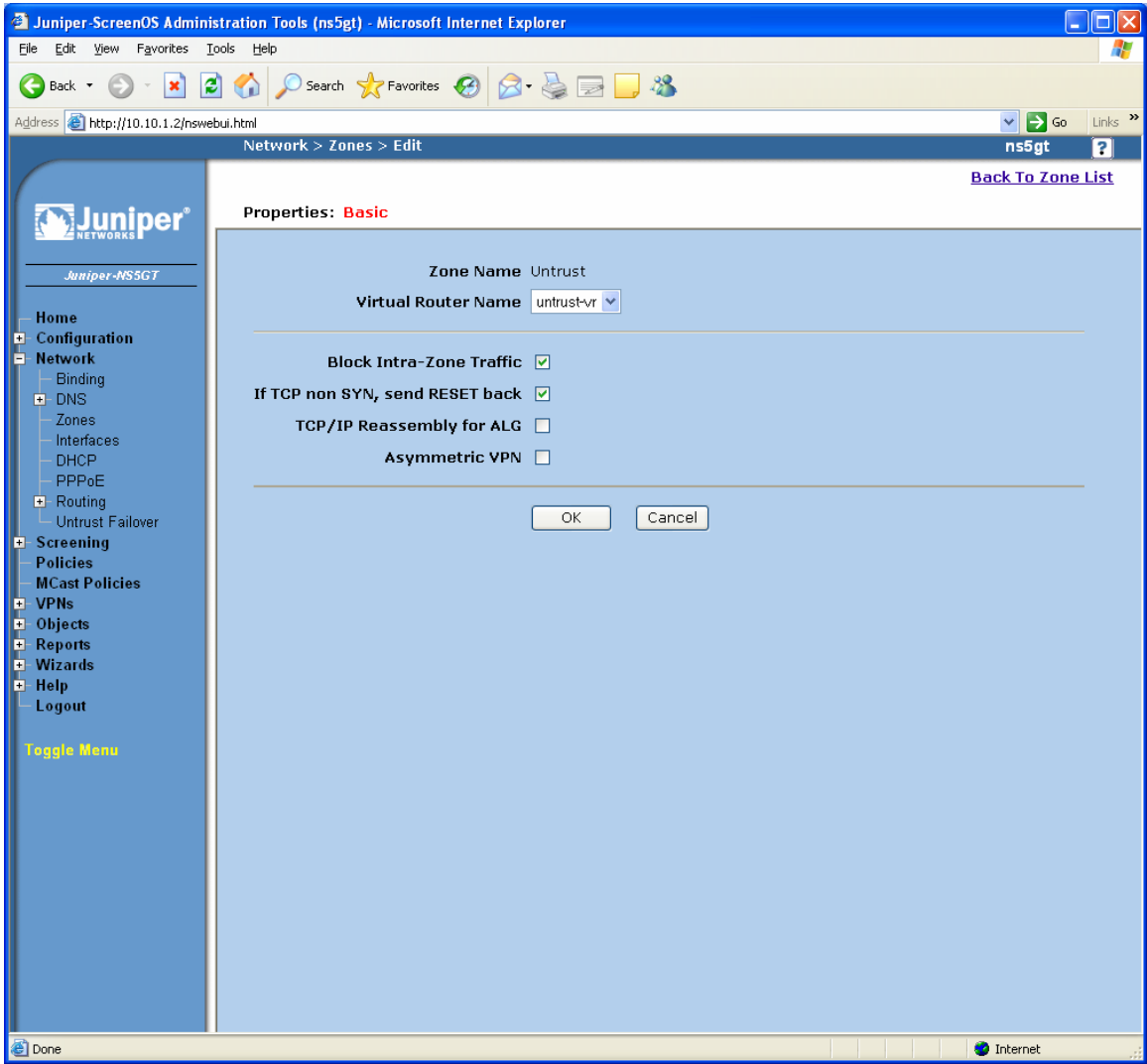
Step	Description
2.	<p>Click Edit on the row corresponding to “Trust” in Figure 5 to view the properties for the Trust security zone. Select trust-vr from the drop-down list for the Virtual Router Name as shown in Figure 6. Accept the other default settings. Click OK.</p> 

Figure 6 – Trust Zone Properties

Step	Description
3.	<p>Click Edit on the row corresponding to “Untrust” in Figure 5 to view the properties for the Untrust security zone. Select untrust-vr from the drop-down list for the Virtual Router Name as shown in Figure 7. Accept the other default settings. Click OK.</p>  <p style="text-align: center;">Figure 7 – Trust Zone Properties</p>

3.4. Configuring Interfaces

The steps in this section assign an IP address to the interfaces for the “trust” and “untrust” security zone. Each interface will operate in “route” mode and function as a separate router. A static route is configured for the trust-vr virtual router to define the untrust-vr as the next hop to allow traffic to pass between the “trust” and “untrust” security zones.

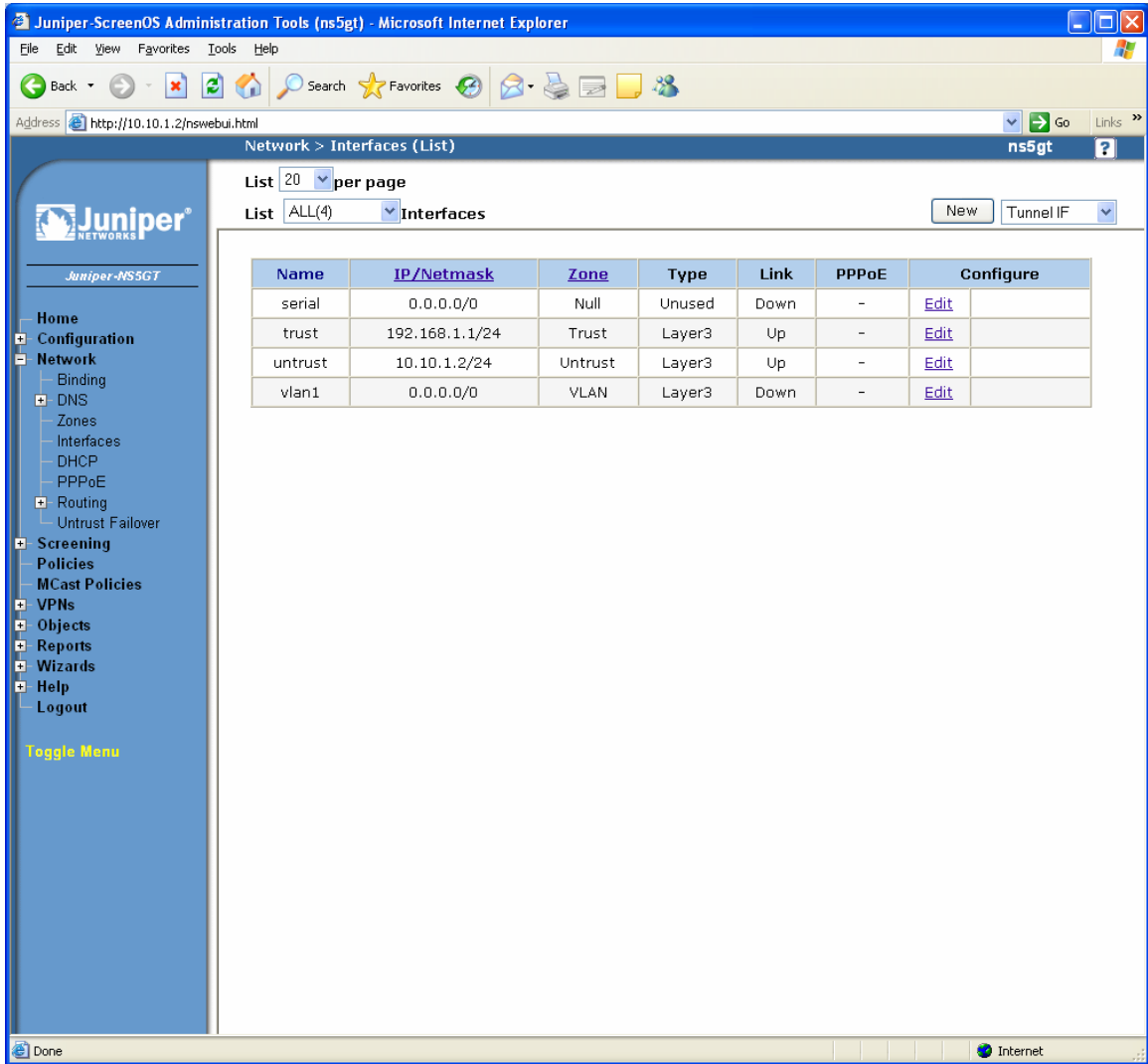
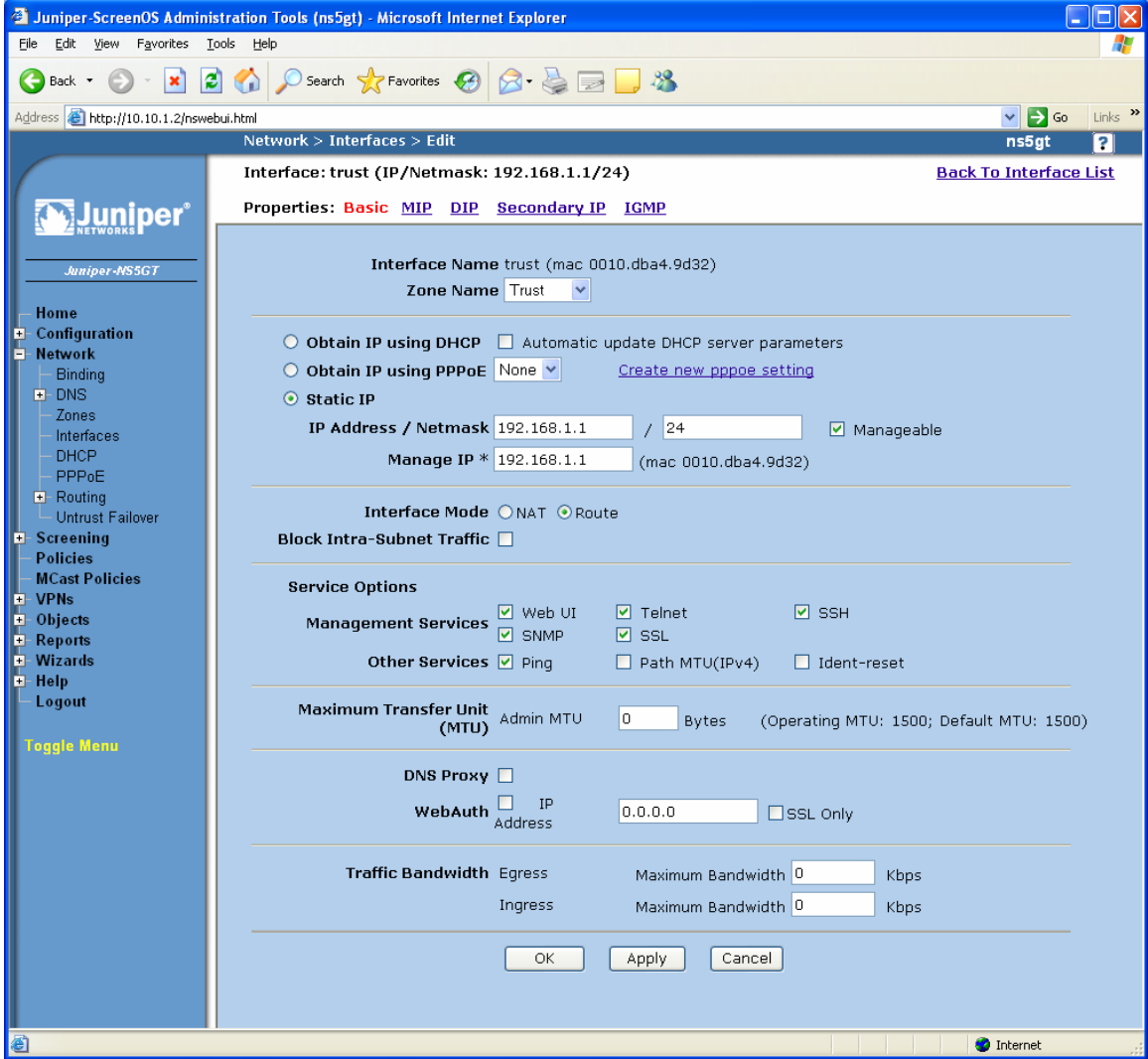
Step	Description																																			
1.	<p>From the navigation menu on the left, select Network → Interfaces to view the network interfaces of the Juniper NetScreen 5GT as shown in Figure 8.</p>  <table><tr><th>Name</th><th>IP/Netmask</th><th>Zone</th><th>Type</th><th>Link</th><th>PPPoE</th><th>Configure</th></tr><tr><td>serial</td><td>0.0.0.0/0</td><td>Null</td><td>Unused</td><td>Down</td><td>-</td><td>Edit</td></tr><tr><td>trust</td><td>192.168.1.1/24</td><td>Trust</td><td>Layer3</td><td>Up</td><td>-</td><td>Edit</td></tr><tr><td>untrust</td><td>10.10.1.2/24</td><td>Untrust</td><td>Layer3</td><td>Up</td><td>-</td><td>Edit</td></tr><tr><td>vlan1</td><td>0.0.0.0/0</td><td>VLAN</td><td>Layer3</td><td>Down</td><td>-</td><td>Edit</td></tr></table>	Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure	serial	0.0.0.0/0	Null	Unused	Down	-	Edit	trust	192.168.1.1/24	Trust	Layer3	Up	-	Edit	untrust	10.10.1.2/24	Untrust	Layer3	Up	-	Edit	vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit
Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure																														
serial	0.0.0.0/0	Null	Unused	Down	-	Edit																														
trust	192.168.1.1/24	Trust	Layer3	Up	-	Edit																														
untrust	10.10.1.2/24	Untrust	Layer3	Up	-	Edit																														
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit																														

Figure 8 – Network Interfaces

Step	Description
2.	<p>Click Edit on the row corresponding to Trust in Figure 8 to view the interface configuration for the Trust security zone. Enter the following information on the screen shown in Figure 9:</p> <ul style="list-style-type: none"> • Zone Name: Select Trust from the drop-down list. • IP Address / Netmask: Enter the IP address for the Trust interface. • Interface Mode: Select Route Mode. • Service Options: Select the desired options for this interface. <p>Click OK.</p> 
	<p align="center">Figure 9 – Trust Network Interface</p>

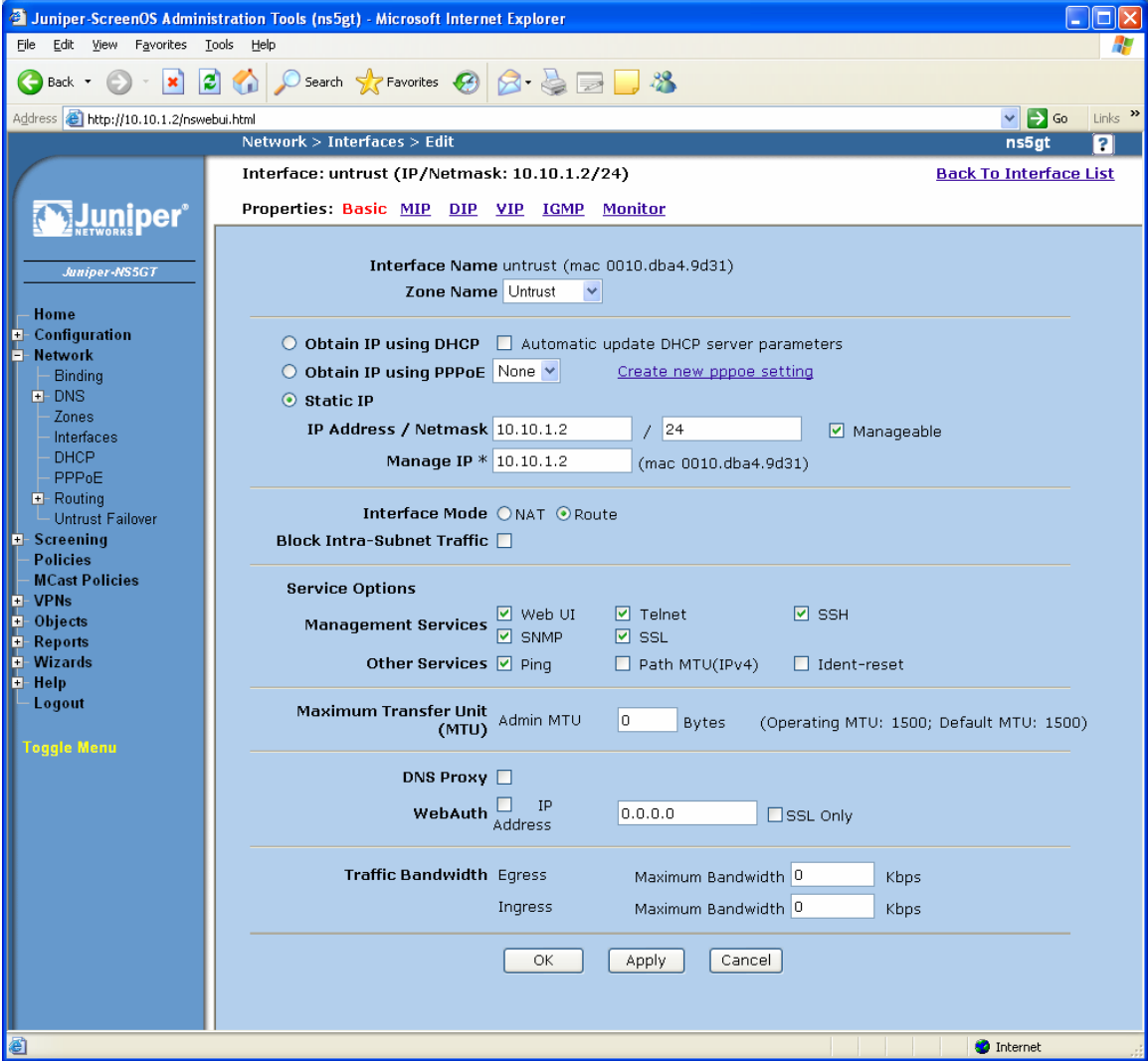
Step	Description
3.	<p>Click Edit on the row corresponding to Untrust in Figure 8 to view the interface configuration for the Untrust security zone. Enter the following information on the screen shown in Figure 10:</p> <ul style="list-style-type: none"> • Zone Name: Select Untrust from the drop-down list. • IP Address / Netmask: Enter the IP address for the Untrust interface. • Interface Mode: Select Route Mode. • Service Options: Select the desired options for this interface. <p><i>Note: The Manageable and Telnet checkbox was enabled for the “untrust” interface for ease of administration of the Juniper NetScreen 5GT from PCs located in the “untrust” security zone. These options do not have to be enabled.</i></p> <p>Click OK.</p>  <p>The screenshot shows the 'Edit' page for the 'untrust' interface in the Juniper-ScreenOS Administration Tools. The interface is configured with the following settings:</p> <ul style="list-style-type: none"> Interface Name: untrust (mac 0010.dba4.9d31) Zone Name: Untrust Obtain IP using DHCP: <input type="radio"/> (Automatic update DHCP server parameters: <input type="checkbox"/>) Obtain IP using PPPoE: <input type="radio"/> None (Create new pppoe setting: Create new pppoe setting) Static IP: <input checked="" type="radio"/> <ul style="list-style-type: none"> IP Address / Netmask: 10.10.1.2 / 24 (Manageable: <input checked="" type="checkbox"/>) Manage IP *: 10.10.1.2 (mac 0010.dba4.9d31) Interface Mode: <input type="radio"/> NAT <input checked="" type="radio"/> Route Block Intra-Subnet Traffic: <input type="checkbox"/> Service Options: <ul style="list-style-type: none"> Management Services: <input checked="" type="checkbox"/> Web UI, <input checked="" type="checkbox"/> SNMP, <input checked="" type="checkbox"/> Telnet, <input checked="" type="checkbox"/> SSH, <input checked="" type="checkbox"/> SSL Other Services: <input checked="" type="checkbox"/> Ping, <input type="checkbox"/> Path MTU(IPv4), <input type="checkbox"/> Ident-reset Maximum Transfer Unit (MTU): Admin MTU: 0 Bytes (Operating MTU: 1500; Default MTU: 1500) DNS Proxy: <input type="checkbox"/> WebAuth: <input type="checkbox"/> IP Address: 0.0.0.0 <input type="checkbox"/> SSL Only Traffic Bandwidth: <ul style="list-style-type: none"> Egress: Maximum Bandwidth: 0 Kbps Ingress: Maximum Bandwidth: 0 Kbps <p>Buttons at the bottom: OK, Apply, Cancel.</p>

Figure 10 – Untrust Network Interface

Step	Description
4.	<p>Configure a static route for the trust-vr virtual router to define the untrust-vr interface as the next hop to allow traffic to pass between the “trust” and “untrust” security zones. From the navigation menu on the left, select Network → Routing → Destination. Click New to create a static route for the Trust virtual router as shown in Figure 11. Enter the Destination Network IP Address (e.g., 10.0.0.0) and the Netmask (e.g., 8) for the “untrust” zone. Select Gateway and select the untrust interface from the drop-down list. Enter the Gateway IP address (e.g., 10.10.1.1) of the next hop router and accept the other default settings. In the configuration shown in Figure 1, the next hop router is the Avaya C364T-PWR connected directly to the Juniper NetScreen 5GT. Click OK.</p>

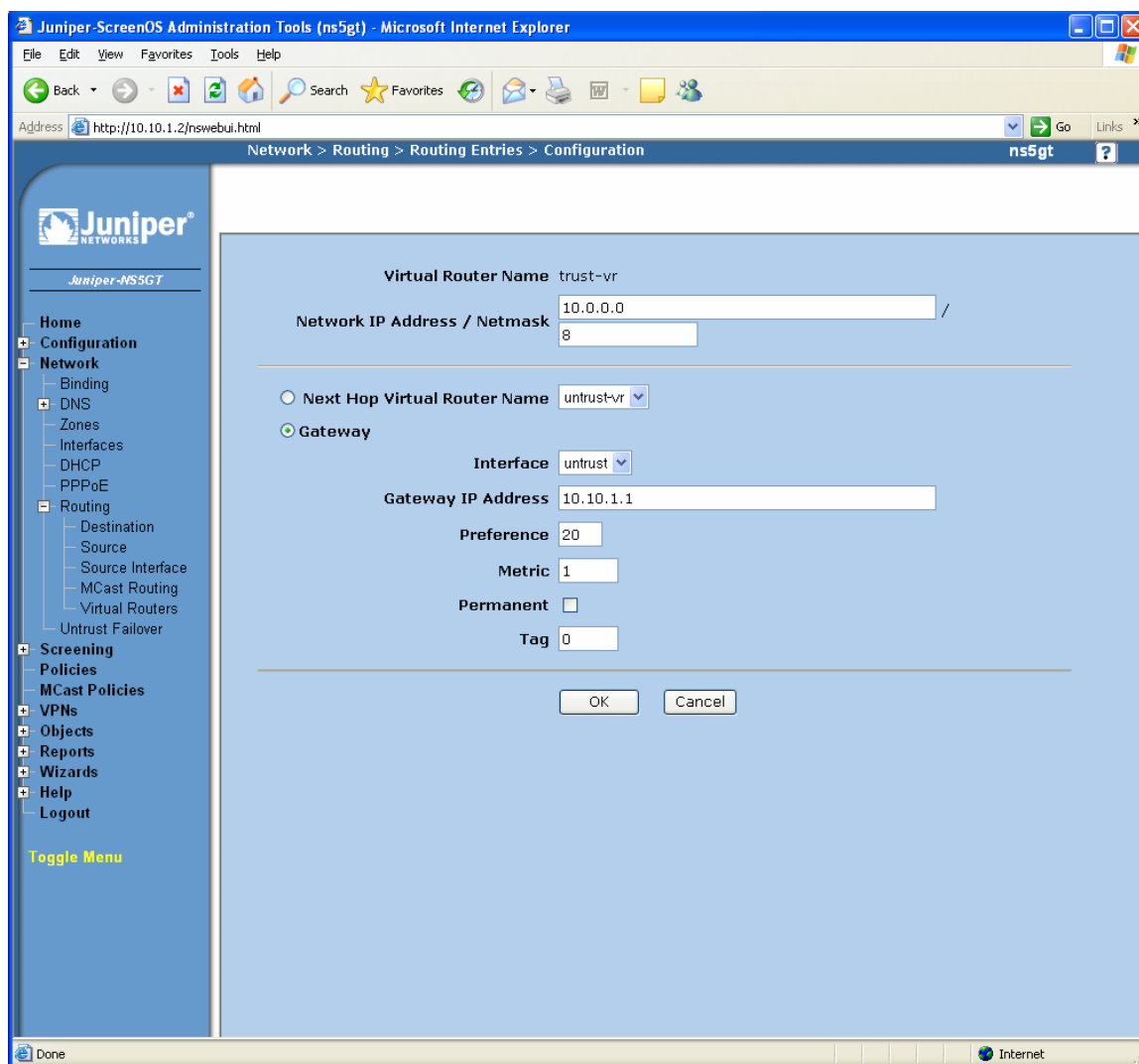


Figure 11 – Static Route for trust-vr

3.5. Create Address Book Entries

Address book entries are used to define resources referenced by security policies. Network addresses are used to specify the subnets of the Main and Branch Office. Individual IP addresses are specified for the Avaya ESS, C-LANs and Media Processors.

Step	Description
1.	<p>From the navigation menu on the left, select Objects → Addresses → List. The address list page is displayed. Click the New button on top right corner of page to create a new address book entry for the range of IP addresses used by equipment at the Main Office. Enter the following information on the screen shown in Figure 12:</p> <ul style="list-style-type: none">• Address Name: Avaya Main Office• IP Address/Netmask: IP address and subnet mask of the Main Office network• Zone: Select Untrust from the drop down list <p>Click OK.</p>

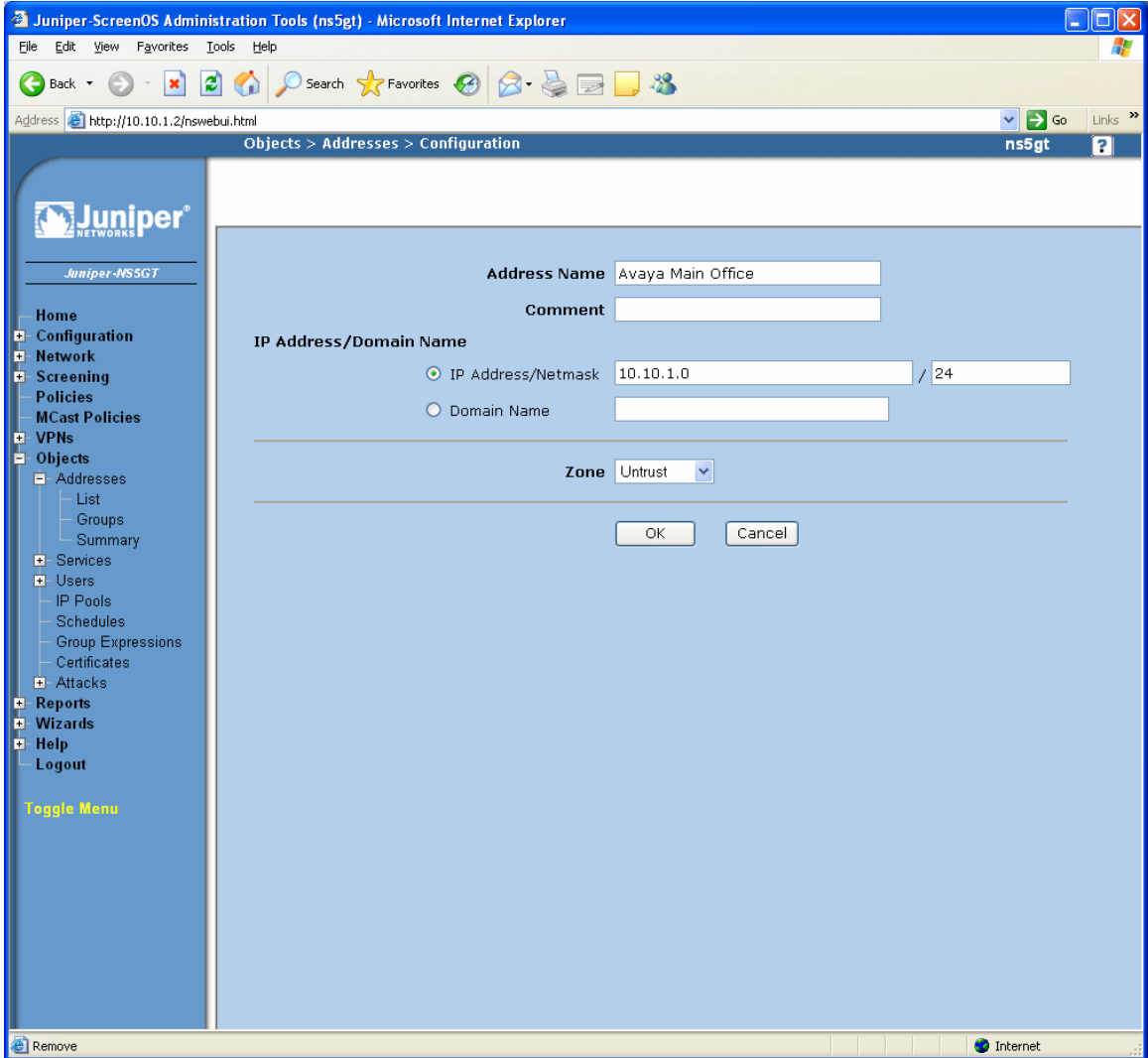


Figure 12 – Avaya Main Office Address Book Entry

Step	Description
2.	<p>From the navigation menu on the left, select Objects → Addresses → List. The address list page is displayed. Click the New button on top right corner of page to create a new address book entry. Enter the following information on the screen shown in Figure 13:</p> <ul style="list-style-type: none"> • Address Name: Avaya Branch Office • IP Address/Netmask: IP address and subnet mask of the Branch Office network • Zone: Select Untrust from the drop down list <p>Click OK.</p>

Juniper-ScreenOS Administration Tools (ns5gt) - Microsoft Internet Explorer

Address: http://10.10.1.2/nswebui.html

Objects > Addresses > Configuration

Juniper NETWORKS

Juniper-NS5GT

Home

Configuration

Network

Screening

Policies

MCast Policies

VPNs

Objects

Addresses

List

Groups

Summary

Services

Users

IP Pools

Schedules

Group Expressions

Certificates

Attacks

Reports

Wizards

Help

Logout

Toggle Menu

Address Name: Avaya Branch Office

Comment:

IP Address/Domain Name

☒ IP Address/Netmask: 10.11.1.0 / 24

☐ Domain Name:

Zone: Untrust

OK Cancel

Figure 13 – Avaya Branch Office Address Book Entry

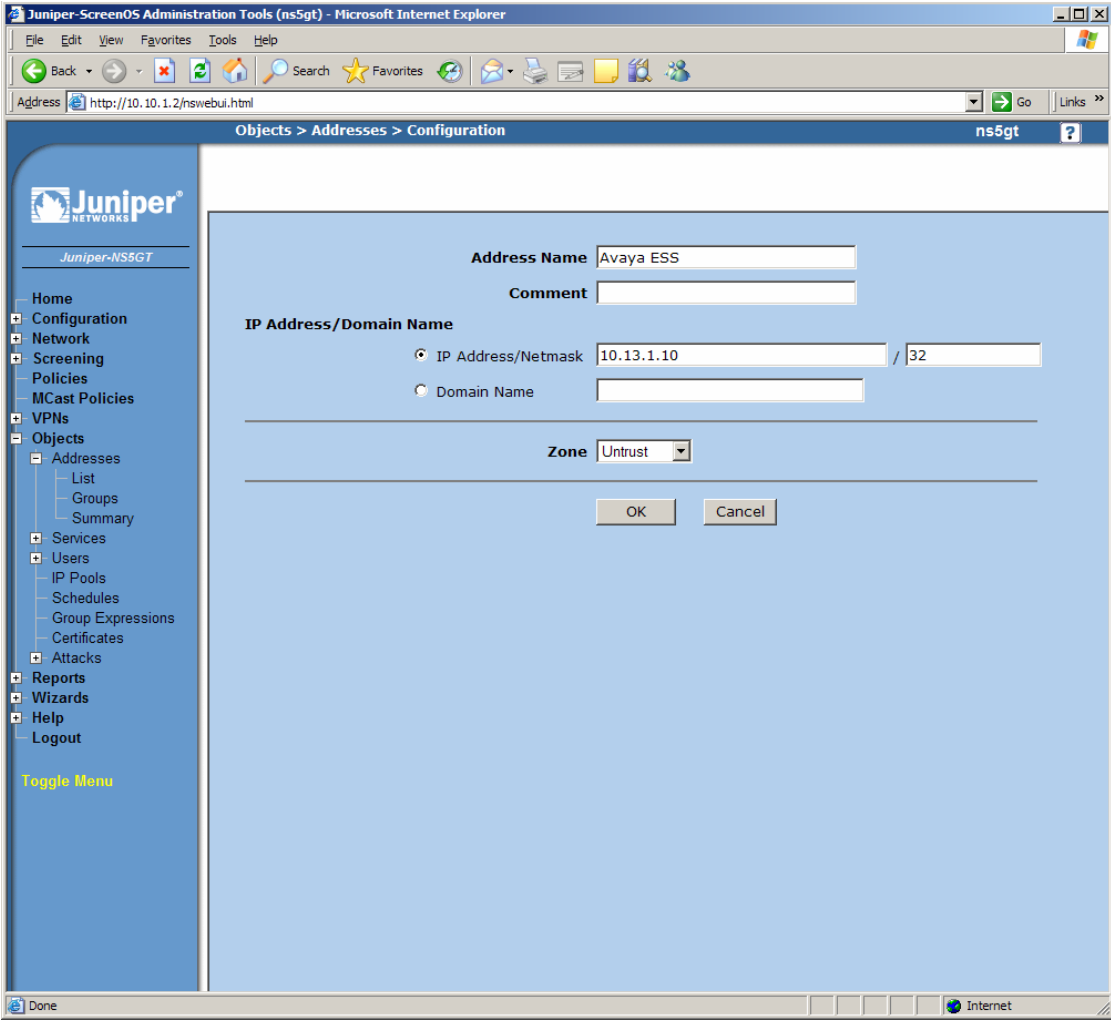
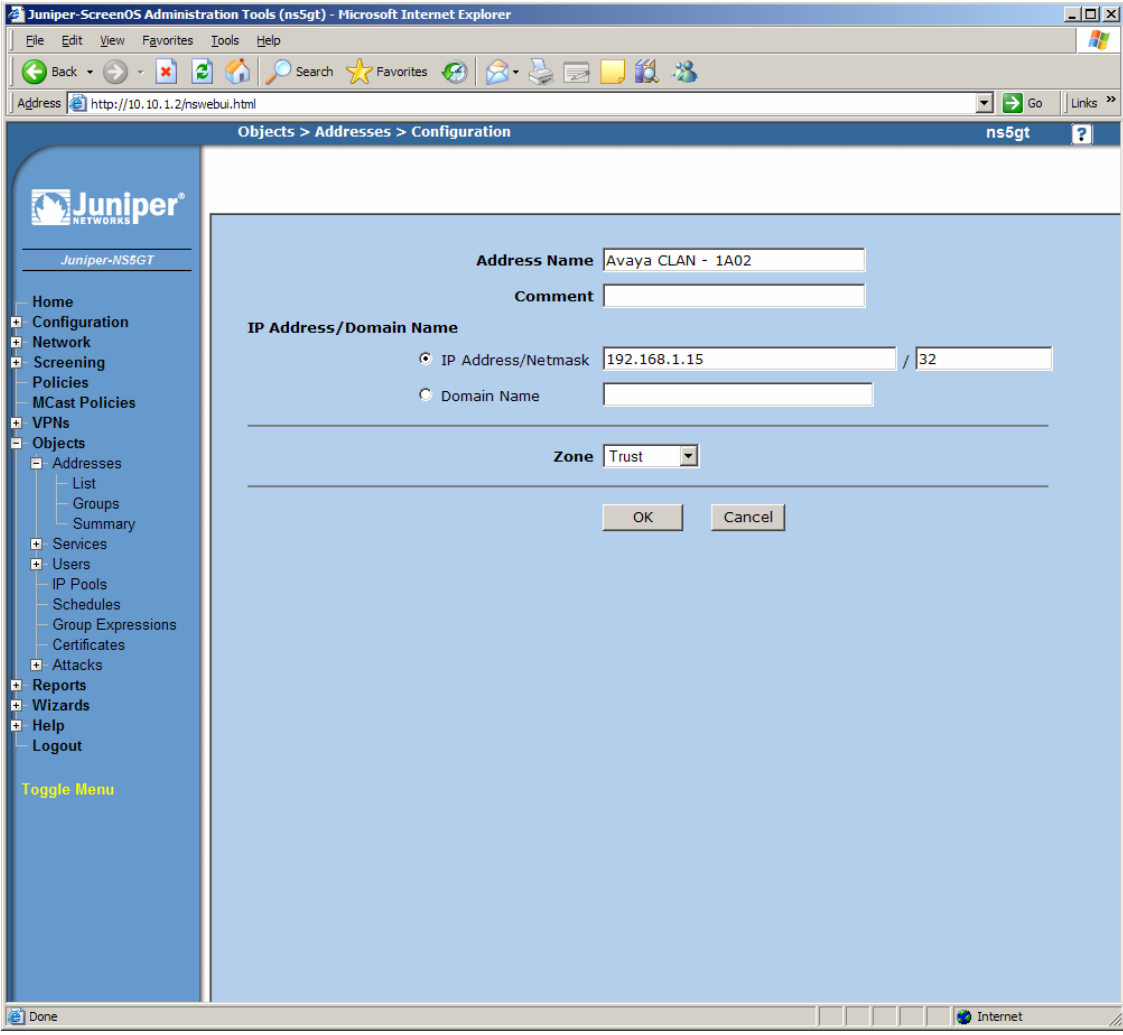
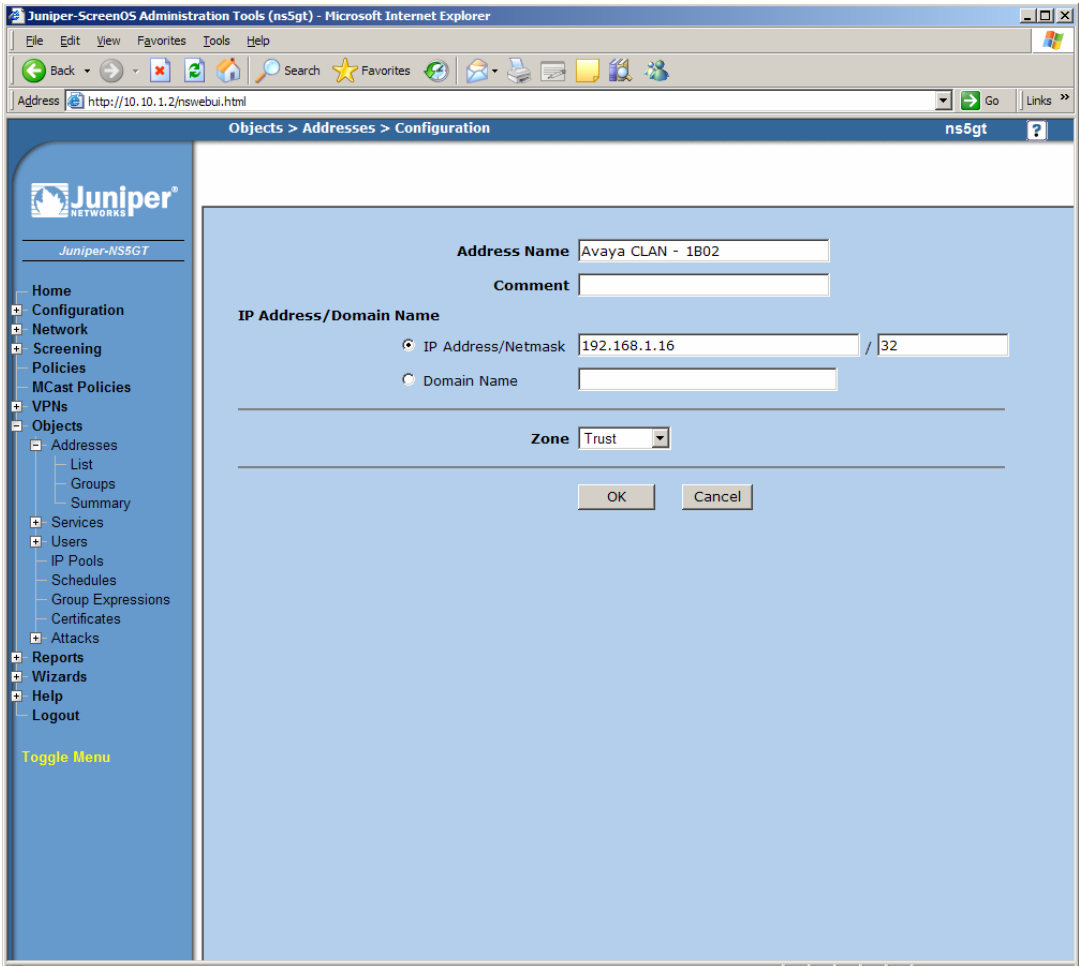
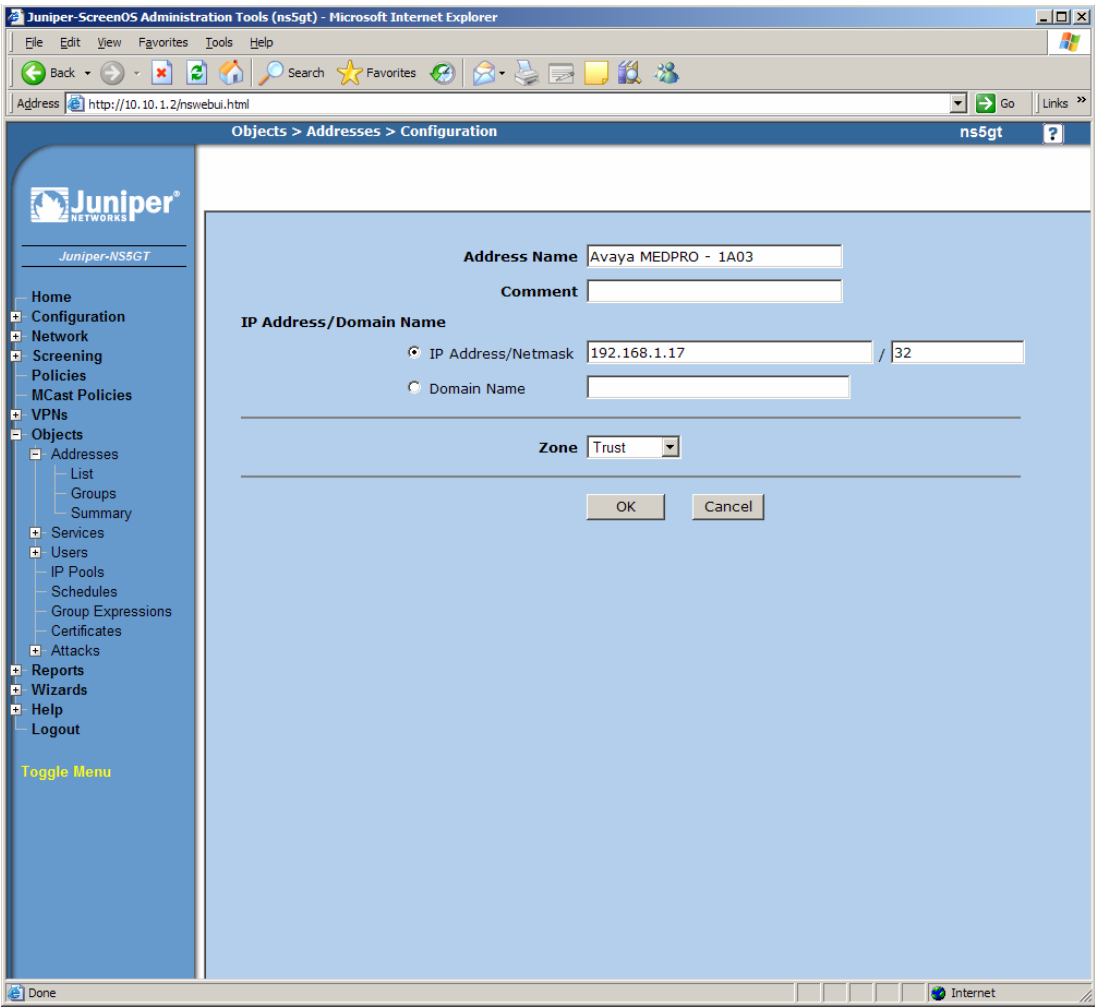
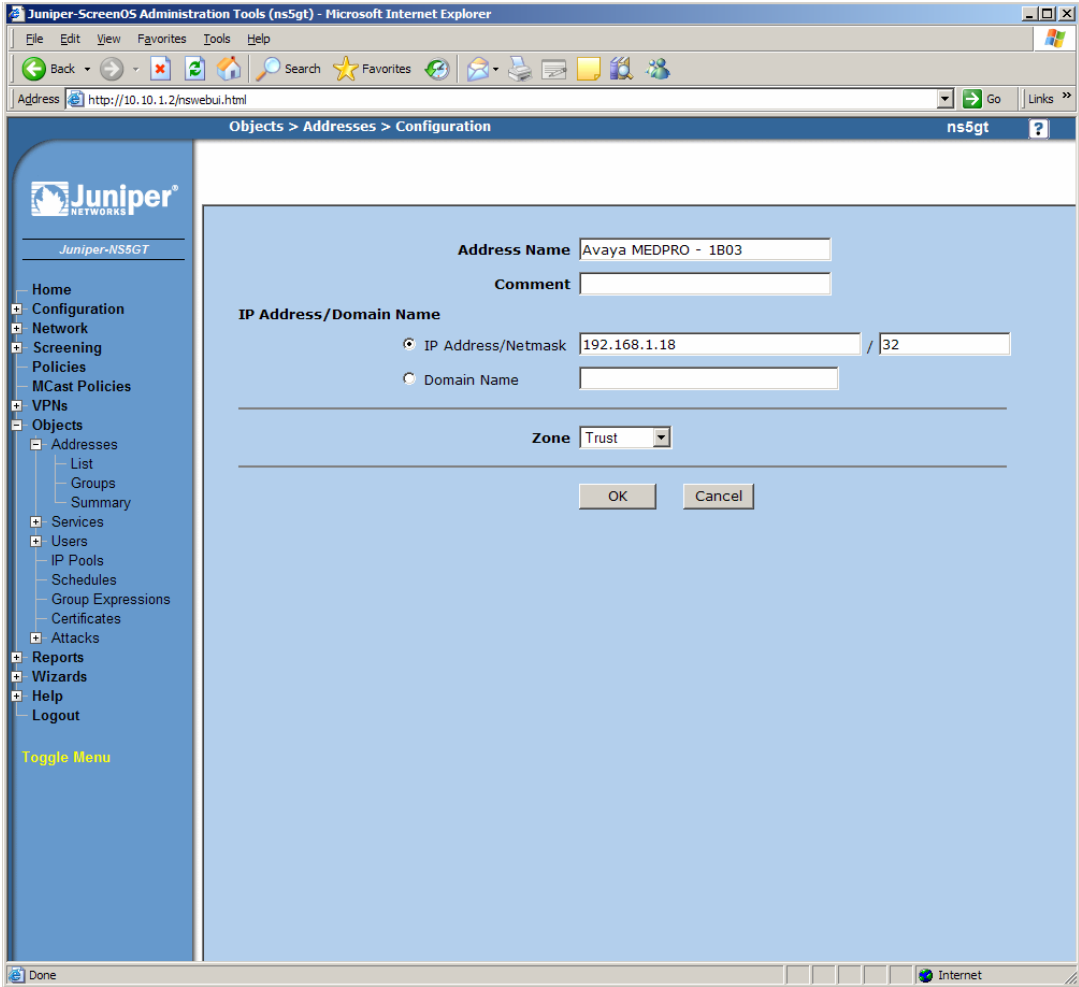
Step	Description
3.	<p>From the navigation menu on the left, select Objects → Addresses → List. The address list page is displayed. Click the New button on top right corner of page to create a new address book entry. Enter the following information on the screen shown in Figure 14:</p> <ul style="list-style-type: none"> • Address Name: Avaya ESS • IP Address/Netmask: IP address and subnet mask of the ESS • Zone: Select Untrust from the drop down list <p>Click OK.</p> 

Figure 14 – Avaya ESS Address Book Entry

Step	Description
4.	<p>From the navigation menu on the left, select Objects → Addresses → List. The address list page is displayed. Click the New button on top right corner of page to create a new address book entry. Enter the following information on the screen shown in Figure 15:</p> <ul style="list-style-type: none"> • Address Name: Avaya CLAN – 1A02 • IP Address/Netmask: IP address and subnet mask of the C-LAN in slot 1A02 • Zone: Select Trust from the drop down list <p>Click OK.</p> 
	<p align="center">Figure 15 – Avaya CLAN-1A02 Address Book Entry</p>

Step	Description
5.	<p>From the navigation menu on the left, select Objects → Addresses → List. The address list page is displayed. Click the New button on top right corner of page to create a new address book entry. Enter the following information on the screen shown in Figure 16:</p> <ul style="list-style-type: none"> • Address Name: Avaya CLAN – 1B02 • IP Address/Netmask: IP address and subnet mask of the C-LAN in slot 1B02 • Zone: Select Trust from the drop down list <p>Click OK.</p>  <p style="text-align: center;">Figure 16 – Avaya CLAN-1A02 Address Book Entry</p>

Step	Description
6.	<p>From the navigation menu on the left, select Objects → Addresses → List. The address list page is displayed. Click the New button on top right corner of page to create a new address book entry. Enter the following information on the screen shown in Figure 17:</p> <ul style="list-style-type: none"> • Address Name: Avaya MEDPRO – 1A03 • IP Address/Netmask: IP address and subnet mask of the MEDPRO located in slot 1A03 • Zone: Select Trust from the drop down list <p>Click OK.</p>  <p style="text-align: center;">Figure 17 – Avaya MEDPRO – 1A03 Address Book Entry</p>

Step	Description
7.	<p>From the navigation menu on the left, select Objects → Addresses → List. The address list page is displayed. Click the New button on top right corner of page to create a new address book entry. Enter the following information on the screen shown in Figure 18:</p> <ul style="list-style-type: none"> • Address Name: Avaya MEDPRO – 1B03 • IP Address/Netmask: IP address and subnet mask of the MEDPRO located in slot 1B03 • Zone: Select Trust from the drop down list <p>Click OK.</p> 
	<p>Figure 18 – Avaya MEDPRO – 1B03 Address Book Entry</p>

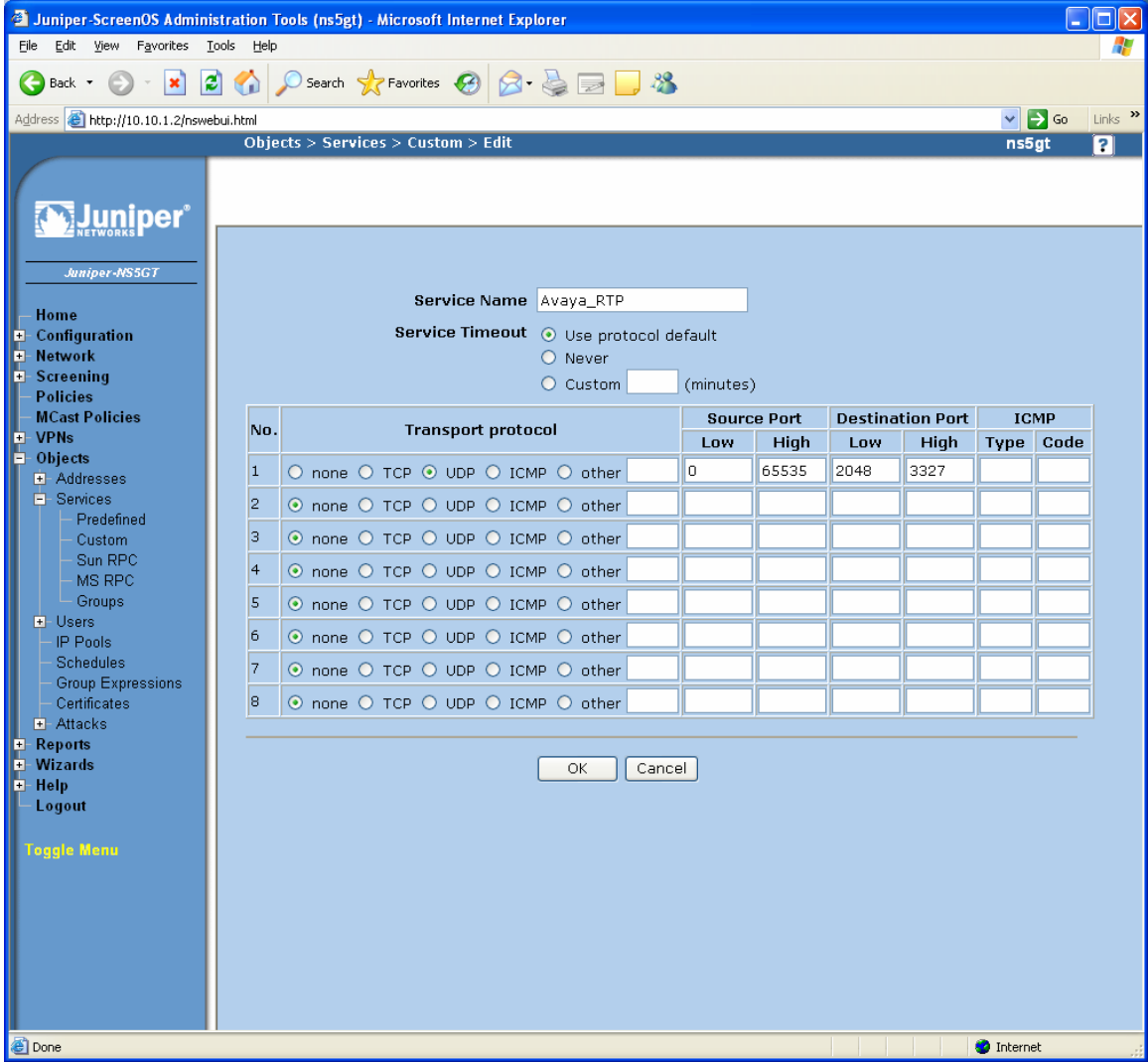
3.6. Configuring Custom Service

Custom services allow for the specification of protocols that are not pre-defined on the NetScreen. Three custom services are defined in this section. The first custom service is used to support Avaya H.323 signaling. The second custom service is used to support RTP traffic. The third custom service is used to support H.248 signaling between the C-LAN and Media Gateway.

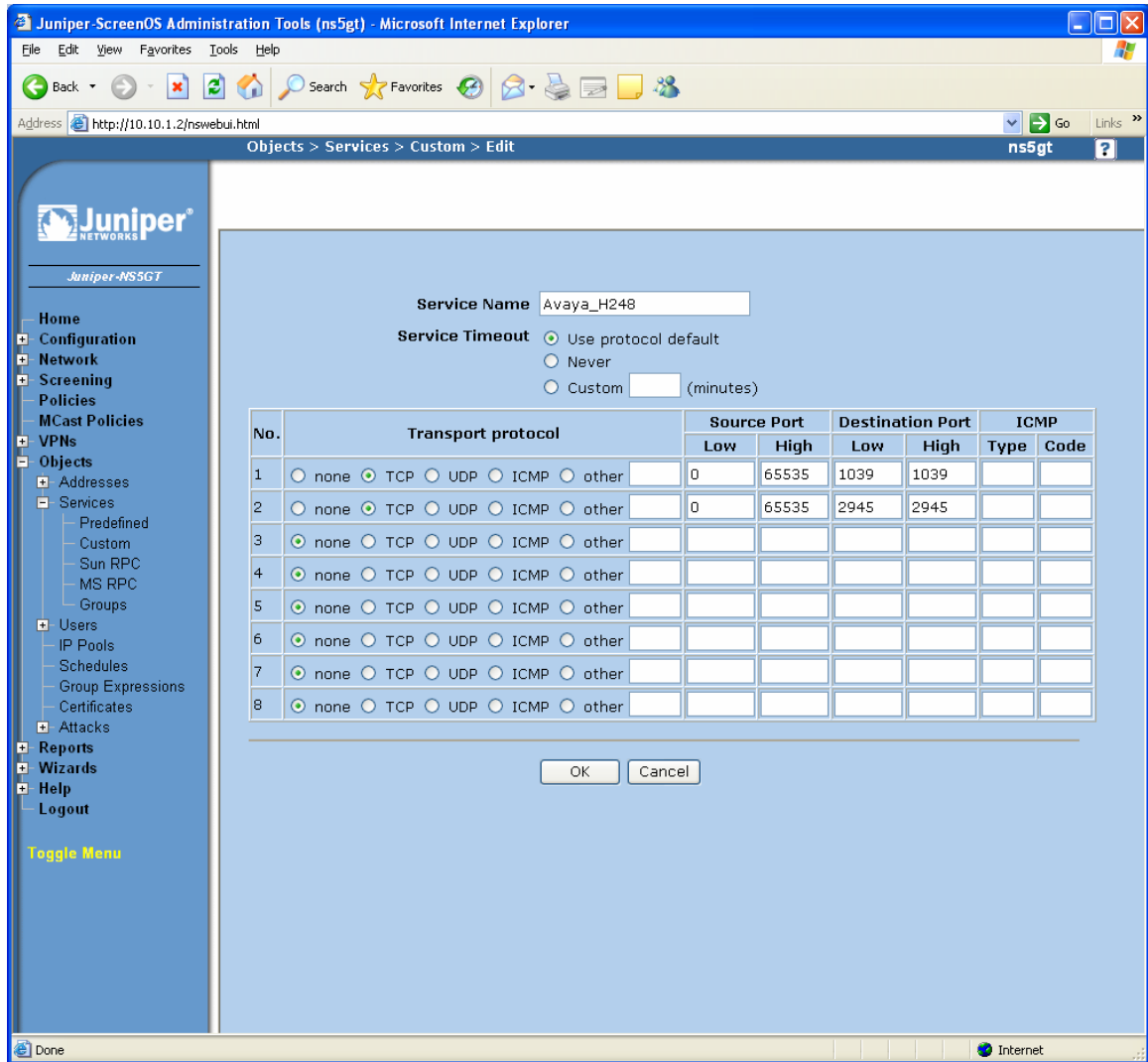
Step	Description
1.	<p>From the navigation menu on the left, select Objects → Services → Custom. The Custom Services page is displayed. Click the New button on top right corner of page to create a new custom service. Enter the following information in the screen shown in Figure 19.</p> <ul style="list-style-type: none"> • Service Name: Avaya_H323 • Service Timeout: Use protocol default. This is the default setting. <p>The UDP and TCP ports specified are described in Table 1. Click OK.</p>

No.	Transport protocol	Source Port		Destination Port		ICMP	
		Low	High	Low	High	Type	Code
1	<input type="radio"/> none <input type="radio"/> TCP <input checked="" type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> other	0	65535	1719	1719		
2	<input type="radio"/> none <input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> other	0	65535	1720	1720		
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						

Figure 19 – Avaya H323 Custom Service

Step	Description
2.	<p>From the navigation menu on the left, select Objects → Services → Custom. The Custom Services page is displayed. Click the New button on top right corner of page to create a new custom service. Enter the following information in the screen shown in Figure 20.</p> <ul style="list-style-type: none"> • Service Name: Avaya_RTP • Service Timeout: Use protocol default. This is the default setting. <p>The UDP ports specified are described in Table 1. The Destination Port range corresponds to the UDP port range specified on the IP Network Region form in Figure 30. Click OK.</p>  <p style="text-align: center;">Figure 20 – Avaya RTP Custom Service</p>

Step	Description
3.	<p>From the navigation menu on the left, select Objects → Services → Custom. The Custom Services page is displayed. Click the New button on top right corner of page to create a new custom service. Enter the following information in the screen shown in Figure 21.</p> <ul style="list-style-type: none">• Service Name: Avaya_H248• Service Timeout: Use protocol default. This is the default setting. <p>The TCP ports specified are described in Table 1. Click OK.</p>



Juniper-ScreenOS Administration Tools (ns5gt) - Microsoft Internet Explorer

Address: http://10.10.1.2/nswebui.html

Objects > Services > Custom > Edit ns5gt

Juniper NETWORKS

Juniper-NS5GT

Home

Configuration

Network

Screening

Policies

MCast Policies

VPNs

Objects

Addresses

Services

Predefined

Custom

Sun RPC

MS RPC

Groups

Users

IP Pools

Schedules

Group Expressions

Certificates

Attacks

Reports

Wizards

Help

Logout

Toggle Menu

Service Name: Avaya_H248

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	0	65535	1039	1039		
2	<input type="radio"/> none <input checked="" type="radio"/> TCP <input type="radio"/> UDP <input type="radio"/> ICMP <input type="radio"/> other	0	65535	2945	2945		
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 Internet

Figure 21 – Avaya H248 Custom Service

Figure 21 – Avaya H248 Custom Service

3.7. Creating Security Policies

Two security policies must be created on the Juniper NetScreen 5GT to allow traffic to flow between the “trust” and the “untrust” zones. The security policy created in Section 3.7.1 allows all traffic to flow from the “trust” zone to the “untrust” zone. The security policy created in Section 3.7.2 only allows ICMP and traffic defined by the custom services in Section 3.6 to flow from the “untrust” zone to the “trust” zone.

3.7.1. Trust to Untrust Policy

Step	Description
1.	<p>From the navigation menu on the left, select Policies. On the top of the Policies page, select Trust on the From drop-down list and Untrust on the To drop-down list. Click the New button on the top right corner of the page to create a new security policy. Enter the following information in the screen shown in Figure 22:</p> <ul style="list-style-type: none">• Name: Avaya Private-to-Public• Source Address: See Step 2 below.• Destination Address: See Step 3 below.• Service: Select ANY from the drop-down list.• Application: Select None from the the drop-down list.• Action: Select Permit from the drop-down list.• Logging: Enable logging by checking the box to see events in the Juniper NetScreen 5GT log.

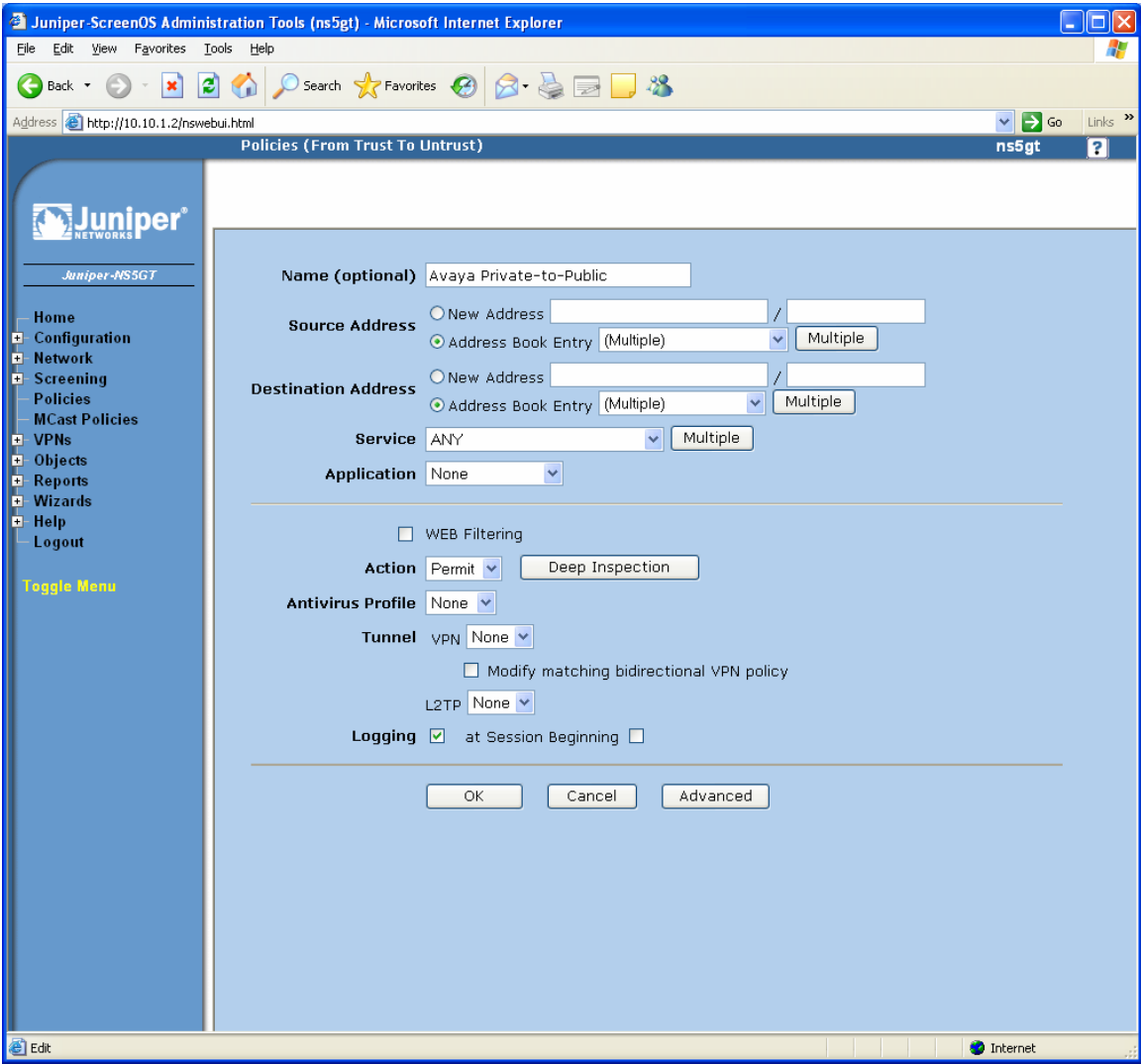
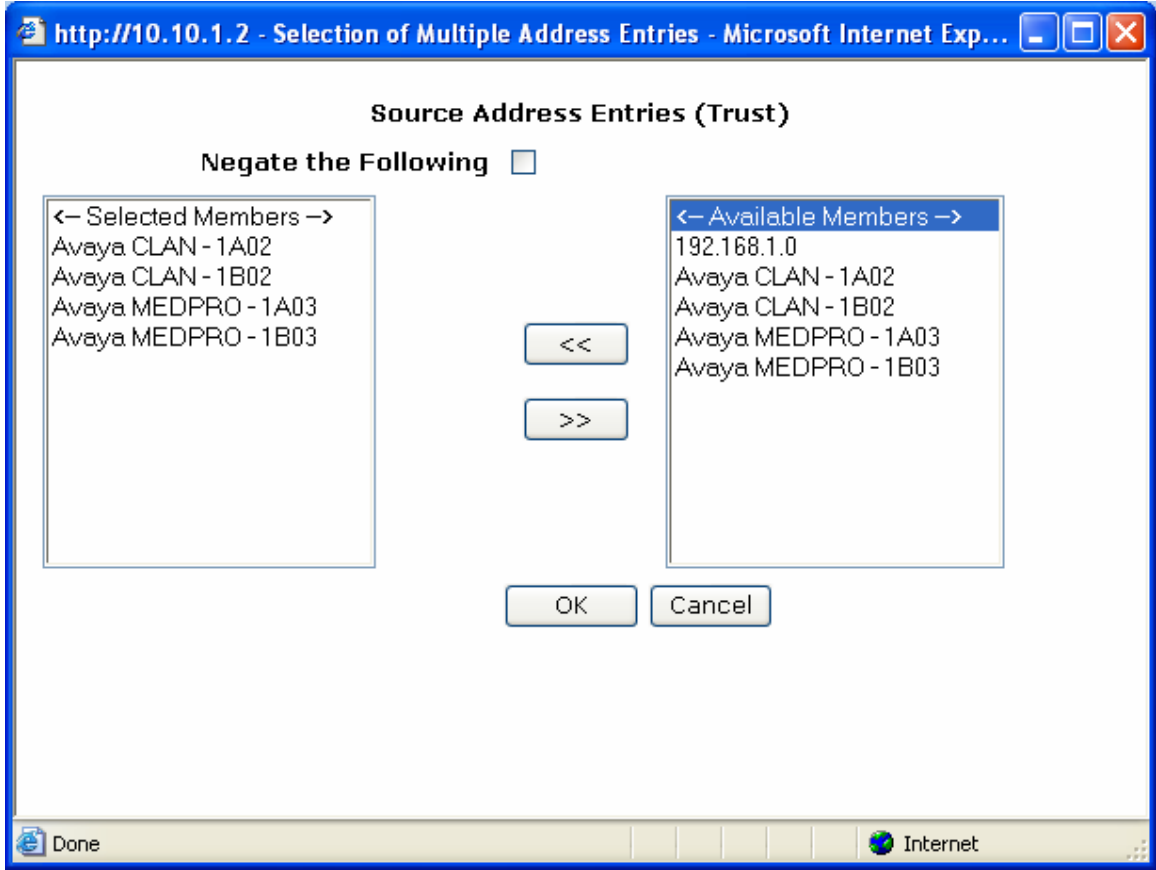
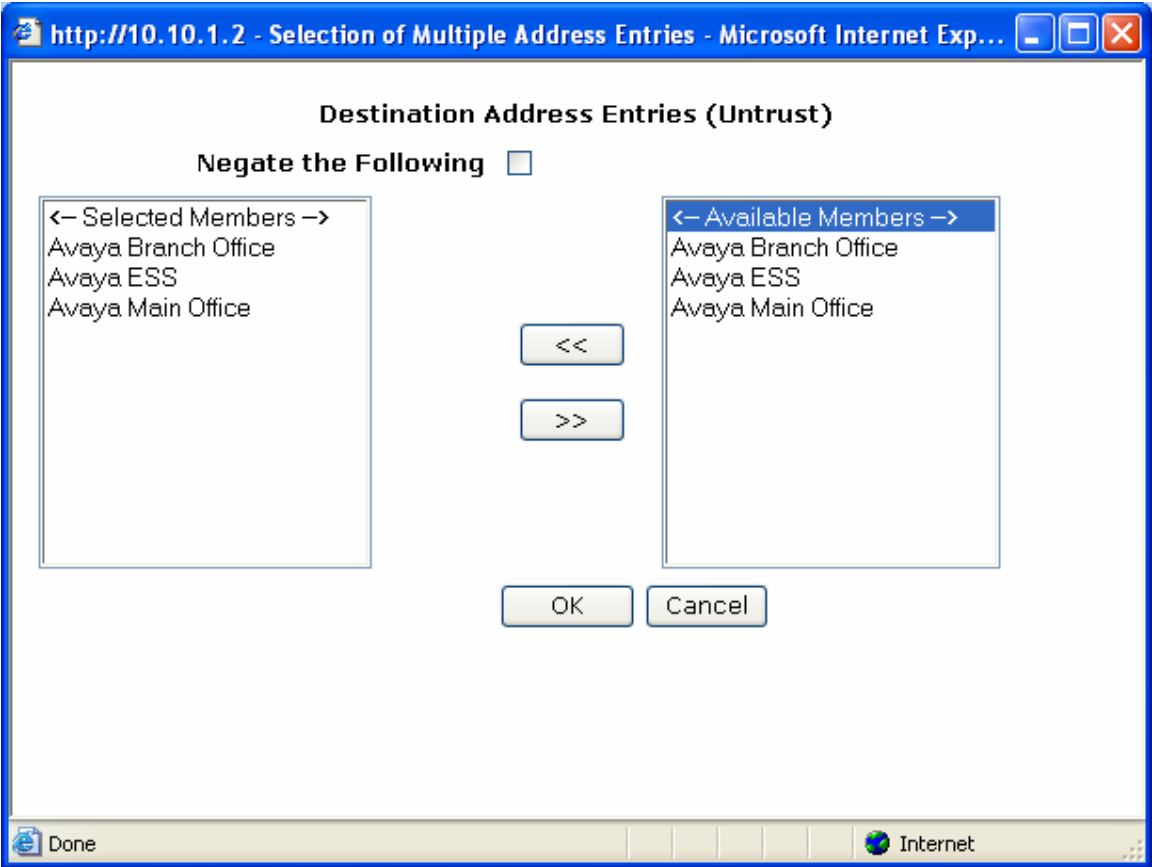
Step	Description
	 <p>The screenshot displays the Juniper-ScreenOS Administration Tools (ns5gt) web interface in Microsoft Internet Explorer. The browser's address bar shows 'http://10.10.1.2/nswebui.html'. The page title is 'Policies (From Trust To Untrust)'. On the left, a navigation menu includes links for Home, Configuration, Network, Screening, Policies, MCast Policies, VPNs, Objects, Reports, Wizards, Help, and Logout. The main content area is for configuring a policy. The 'Name (optional)' field contains 'Avaya Private-to-Public'. The 'Source Address' and 'Destination Address' are both configured with 'Address Book Entry (Multiple)'. The 'Service' is set to 'ANY' and the 'Application' is set to 'None'. Under the 'Action' section, 'Permit' is selected, and a 'Deep Inspection' button is visible. The 'Antivirus Profile' is set to 'None'. In the 'Tunnel' section, 'VPN None' is selected, and there is a checkbox for 'Modify matching bidirectional VPN policy'. The 'Logging' section has a checked box for 'at Session Beginning'. At the bottom of the configuration area are buttons for 'OK', 'Cancel', and 'Advanced'.</p>

Figure 22 – Trust to Untrust Policy

Step	Description
2.	<p>From the Policies (Trust to Untrust) screen in Figure 22, select Address Book Entry for the Source Address and click the Multiple button. Select the Address Book entries created for the C-LAN and MEDPRO boards from the Available Members window and move these over to the Selected Members window as shown in Figure 23. Click OK.</p>  <p style="text-align: center;">Figure 23 – Source Address Entries (Trust)</p>

Step	Description
3.	<p>From the Policies (Trust to Untrust) screen in Figure 22, select Address Book Entry for the Destination Address and click the Multiple button. Select the Address Book entries created for the Branch Office, ESS, and Main Office from the Available Members window and move these over to the Selected Members window as shown in Figure 24. Click OK to continue.</p> <p>Click OK to save the Trust to Untrust policy.</p>  <p>Figure 24 – Destination Address Entries (Untrust)</p>

3.7.2. Untrust to Trust Policy

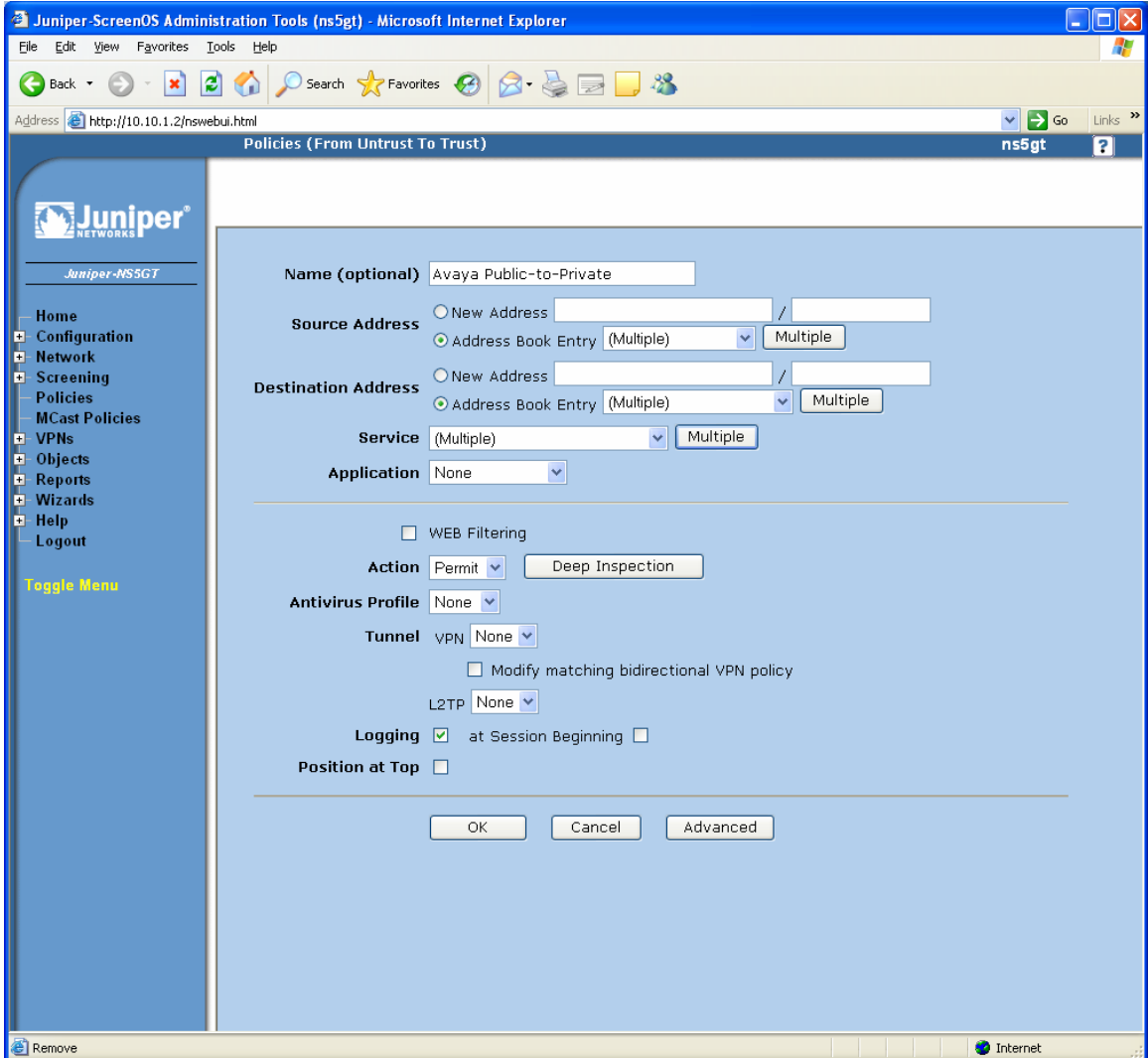
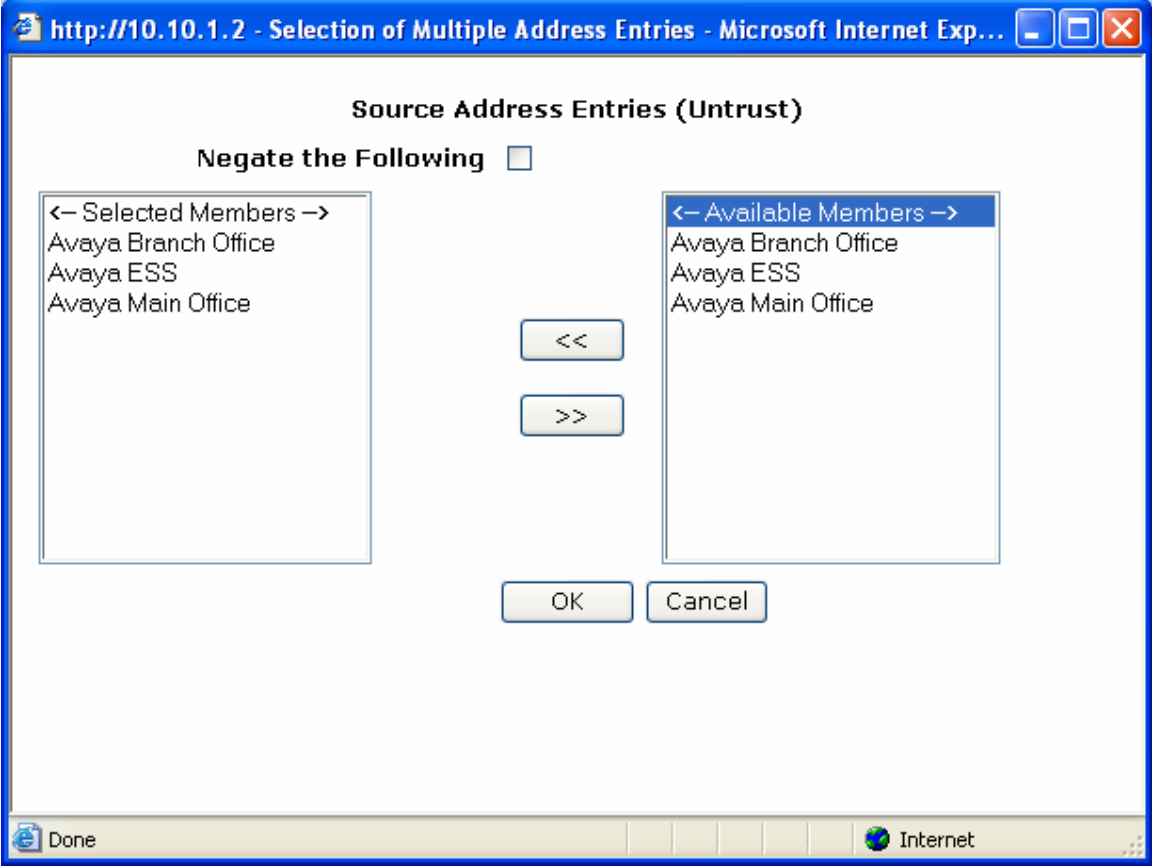
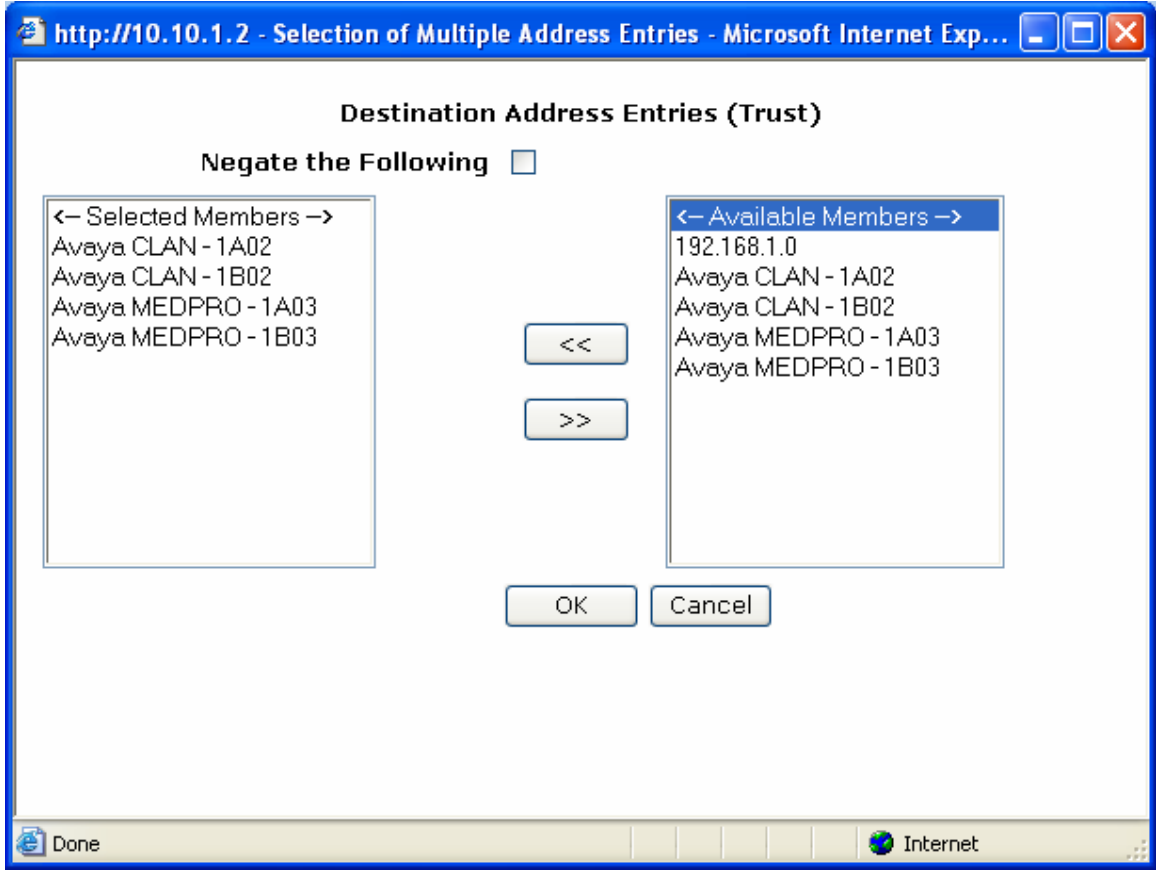
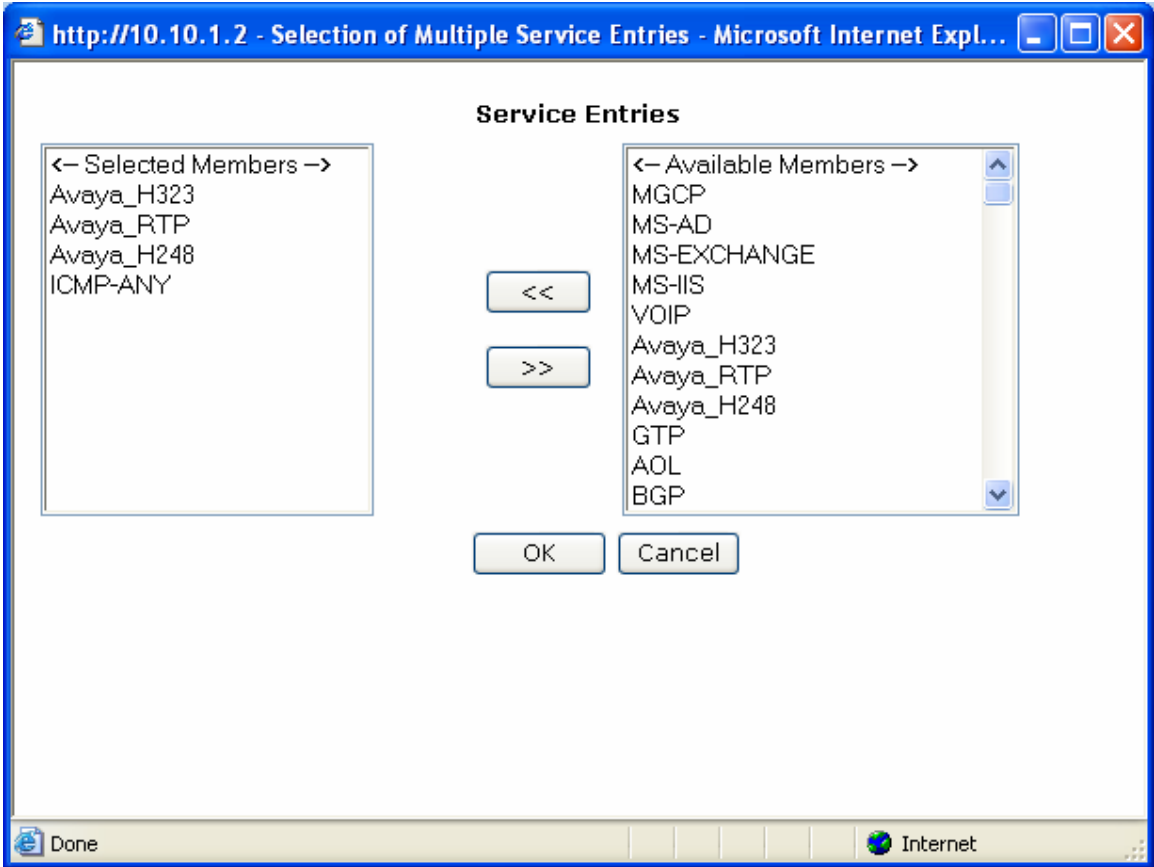
Step	Description
1.	<p>From the navigation menu on the left, select Policies. On the top of the Policies page, select Untrust on the From drop-down list and Trust on the To drop-down list. Click the New button on the top right corner of the page to create a new security policy. Enter the following information in the screen shown in Figure 25:</p> <ul style="list-style-type: none"> • Name: Avaya Public-to-Private • Source Address: See Step 2 below. • Destination Address: See Step 3 below. • Service: See Step 4 below. • Application: Select None from the drop-down list. • Action: Select Permit from the drop-down list. • Logging: Enable logging by checking the box to see events in the NetScreen log. <p>Click OK.</p> 

Figure 25 – Trust to Untrust Policy

Step	Description
2.	<p>From the Policies (Untrust to Trust) screen in Figure 25, select Address Book Entry for the Source Address and click the Multiple button. Select the Address Book entries created for the Branch Office, ESS, and Main Office from the Available Members window and move these over to the Selected Members window as shown in Figure 26. Click OK.</p>  <p style="text-align: center;">Figure 26 – Source Address Entries (Untrust)</p>

Step	Description
3.	<p>From the Policies (Untrust to Trust) screen in Figure 25, select Address Book Entry for the Destination Address and click the Multiple button. Select the Address Book entries created for the C-LAN and MEDPRO boards from the Available Members window and move these over to the Selected Members window as shown in Figure 27. Click OK.</p>  <p style="text-align: center;">Figure 27 – Source Address Entries (Untrust)</p>

Step	Description
4.	<p>From the Policies (Untrust to Trust) screen in Figure 25, click the Multiple button for Service. Select the Custom Services created in Section 3.6 from the Available Members window and move these over to the Selected Members window as shown in Figure 28. Click OK to continue.</p> <p>Click OK to save the Untrust to Trust policy.</p>  <p style="text-align: center;">Figure 28 – Service Entries</p>

3.7.3. Summary of Security Policies to Support Avaya IP Telephony

From the Juniper NetScreen 5GT Home Page, click **Policies** to display the two security policies created in Sections 3.7.1 and 3.7.2.

Juniper-ScreenOS Administration Tools (ns5gt) - Microsoft Internet Explorer

Address: http://10.10.1.2/nswebui.html

Policies (From All zones To All zones) ns5gt

List 20 per page

From All zones To All zones Go

Search New

From Trust To Untrust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
1	Avaya CLAN - 1A02	Avaya Branch Office	ANY	Allow		Edit Clone Remove	<input checked="" type="checkbox"/>	↓ →

From Untrust To Trust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
2	Avaya Branch Office	Avaya CLAN - 1B02	Avaya_H248 Avaya_H323 Avaya_RTP ICMP-ANY	Allow		Edit Clone Remove	<input checked="" type="checkbox"/>	↓ →

Figure 29 – Service Entries

4. Avaya Communication Manager Configuration

From the System Access Terminal (SAT), enter the “**change ip-network-region n**” command, where n represents the region number. Enter the UDP port range (minimum and maximum) under **Media Parameters** as shown in **Figure 30** for Network Region 1. This port range must match the Custom Service port range used in Step 2 of Section 3.6. The Main Office uses Network Region 1 and the Branch Office (not shown) uses Network Region 2. The same UDP port range is specified for each Network Region.

change ip-network-region 1		Page 1 of 19
19		
IP NETWORK REGION		
Region: 1		
Location: 1	Authoritative Domain:	
Name:		
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3327		
DIFFSERV/TOS PARAMETERS	RTCP Reporting Enabled? y	
Call Control PHB Value: 46	RTCP MONITOR SERVER PARAMETERS	
Audio PHB Value: 46	Use Default Server Parameters? y	
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5	AUDIO RESOURCE RESERVATION PARAMETERS	
H.323 IP ENDPOINTS	RSVP Enabled? n	
H.323 Link Bounce Recovery? y		
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

Figure 30 – IP Network Region Form

5. Verification Steps

The following steps can be performed to verify that the Juniper NetScreen 5GT can support Avaya IP Telephones, Avaya Media Gateways, Avaya Enterprise Survivable Servers, and Avaya Local Survivable Processors:

Step	Description
1.	<p>From the System Access Terminal (SAT), use the “list registered-ip-stations” command to verify that the Juniper NetScreen 5GT configuration allows the Avaya IP Telephones (e.g., 20001, 50001-50002) to register to a C-LAN.</p> <div> <pre>list registered-ip-stations</pre> <pre> REGISTERED IP STATIONS Station Set Product Prod Station Net Orig Gatekeeper TCP Ext Type ID Rel IP Address Rgn Port IP Address Skt 20001 4621 IP_Phone 2.400 10.11.1.21 2 192.168.1.15 y 50001 4621 IP_Phone 2.400 10.10.1.51 1 192.168.1.15 y 50002 4610 IP_Phone 2.400 10.10.1.52 1 192.168.1.15 y </pre> </div> <p>Figure 31 – Registered IP Stations</p>
2.	<p>From the System Access Terminal (SAT), use the “list media-gateway” command to verify that the Juniper NetScreen 5GT configuration allows the Avaya G350 Media Gateway to register to a C-LAN.</p> <div> <pre>list media-gateway</pre> <pre> MEDIA-GATEWAY REPORT Num Name Serial No/ IP Address/ Type NetRgn Reg? FW Ver/HW Vint Cntrl IP Addr RecRule 1 g350 05IS35724296 10 .11 .1 .254 g350 2 y 25 .23 .0 /1 192.168.1 .15 1 </pre> </div> <p>Figure 32 – Media-Gateway Report</p>

Step	Description																																				
3.	<div><p>From the System Access Terminal (SAT), use the “status ess clusters” command to verify that the Juniper NetScreen 5GT configuration allows both Cluster 1 (Primary Servers) and Cluster 2 (ESS Server) to register.</p><div><pre>status ess clusters</pre><table><tr><td colspan="2">Cluster ID</td><td colspan="2">1</td><td colspan="4">ESS CLUSTER INFORMATION</td></tr><tr><td>Cluster ID</td><td>Enabled?</td><td>Active Server ID</td><td>Registered?</td><td colspan="2">Translations Updated</td><td colspan="2">Software Version</td></tr><tr><td>1</td><td>y</td><td>1</td><td>y</td><td colspan="2">22:00 7/4/2006</td><td colspan="2">R013x.01.1.628.7</td></tr><tr><td>2</td><td>y</td><td>3</td><td>y</td><td colspan="2">22:00 7/4/2006</td><td colspan="2">R013x.01.1.628.7</td></tr></table></div><p>Figure 33 – ESS Cluster Information</p></div>	Cluster ID		1		ESS CLUSTER INFORMATION				Cluster ID	Enabled?	Active Server ID	Registered?	Translations Updated		Software Version		1	y	1	y	22:00 7/4/2006		R013x.01.1.628.7		2	y	3	y	22:00 7/4/2006		R013x.01.1.628.7					
Cluster ID		1		ESS CLUSTER INFORMATION																																	
Cluster ID	Enabled?	Active Server ID	Registered?	Translations Updated		Software Version																															
1	y	1	y	22:00 7/4/2006		R013x.01.1.628.7																															
2	y	3	y	22:00 7/4/2006		R013x.01.1.628.7																															
4.	<div><p>From the System Access Terminal (SAT), use the “list survivable-processor” command to verify that the Juniper NetScreen 5GT configuration allows both the Avaya S8300 (g350-lsp) and the Avaya S8500 (8500-ess) to register. File synchronization is working properly because both servers have the same time and date in the Translations Updated field.</p><div><pre>list survivable-processor</pre><table><tr><td colspan="2"></td><td colspan="4">SURVIVABLE PROCESSORS</td><td colspan="2"></td><td></td></tr><tr><td>Name</td><td>Type</td><td colspan="2">IP Address</td><td>Reg</td><td>LSP Act</td><td colspan="2">Translations Updated</td><td>Net Rgn</td></tr><tr><td>g350-lsp</td><td>LSP</td><td>10</td><td>.11 .1 .10</td><td>y</td><td>n</td><td colspan="2">22:00 7/4/2006</td><td>2</td></tr><tr><td>8500-ess</td><td>ESS</td><td>10</td><td>.13 .1 .10</td><td>y</td><td></td><td colspan="2">22:00 7/4/2006</td><td>1</td></tr></table></div><p>Figure 34 – ESS Cluster Information</p></div>			SURVIVABLE PROCESSORS							Name	Type	IP Address		Reg	LSP Act	Translations Updated		Net Rgn	g350-lsp	LSP	10	.11 .1 .10	y	n	22:00 7/4/2006		2	8500-ess	ESS	10	.13 .1 .10	y		22:00 7/4/2006		1
		SURVIVABLE PROCESSORS																																			
Name	Type	IP Address		Reg	LSP Act	Translations Updated		Net Rgn																													
g350-lsp	LSP	10	.11 .1 .10	y	n	22:00 7/4/2006		2																													
8500-ess	ESS	10	.13 .1 .10	y		22:00 7/4/2006		1																													
5.	Verify shuffled and non-shuffled calls can be placed successfully when a primary media server is active from the Avaya IP Telephones at both the Main and Branch Offices.																																				
6.	Verify shuffled and non-shuffled calls can be placed successfully when the ESS server is active from the Avaya IP Telephones at both the Main and Branch Offices.																																				

6. Conclusion

These Application Notes describe how to configure the Juniper NetScreen 5GT to support Avaya H.323 IP Telephony. The sample configuration presented in these Application Notes illustrated how a Juniper NetScreen 5GT firewall can be configured to protect Avaya C-LANs and Media Processor boards using security policies which only allow H.323 signaling, RTP, and H.248 traffic to pass through the firewall.

7. Additional References

The following Avaya product documentation can be found at <http://support.avaya.com>.

- [1] *Avaya Application Solutions: IP Telephony Deployment Guide*, Issue 4.2, February 2006, Document ID: 555-245-600.
- [2] *Configuring the Juniper NetScreen Firewall Security Policies to support Avaya IP Telephony*, Issue 1.0.

The following Juniper NetScreen documentation can be found at <http://www.juniper.net>.

- [3] *NetScreen Concepts & Examples, ScreenOS Reference Guide, Volume 2: Fundamentals*, ScreenOS 5.0.0 P/N 093-1345-000, Rev. A.

© 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 and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabinotes@list.avaya.com