Avaya Solution & Interoperability Test Lab

Sample Configuration for Route-Based Site-to-Site VPN Tunnel using Juniper Networks Secure Services Gateway to support an Avaya Distributed Office Branch – Issue 1.0

Abstract

These Application Notes describe the steps for configuring a Route-Based Site-to-Site VPN Tunnel between two Juniper Networks Secure Services Gateways to support an Avaya Distributed Office branch location. Unlike a policy-based Site-to-Site VPN, the decision of whether network traffic should go through the VPN tunnel is based on information in the routing table.

1. Introduction

These Application Notes describe a solution for configuring a Route-Based Site-to-Site VPN tunnel using Juniper Networks Secure Services Gateway (SSG) to support a branch location connected through an unsecured network.).

1.1. Overview

The sample network consists of three locations, HQ, Branch-2, and Branch-7. Avaya Distributed Office is deployed in each branch location to provide local telephony support. An Avaya Communication Manager and Avaya SIP Enablement Services (SES) are located in HQ and are responsible for providing local telephony as well as call routing for Avaya Distributed Office among branches. Reference [2] provides additional information on how to configure SIP private networking. All IP addresses are administered via Dynamic Host Configuration Protocol. A mix of SIP, H.323, Digital, and analog telephones are used in the sample network. Branch-7 is connected to a simulated Internet network and communicates with HQ via a Route-Based Site-to-Site VPN connection between a Juniper SSG5 and a Juniper SSG520 at HQ. Dynamic routing is enabled for the VPN tunnel interface to populate the routing table for all routers.

2. Configuration

Figure 1 illustrates the configuration used in these Application Notes.

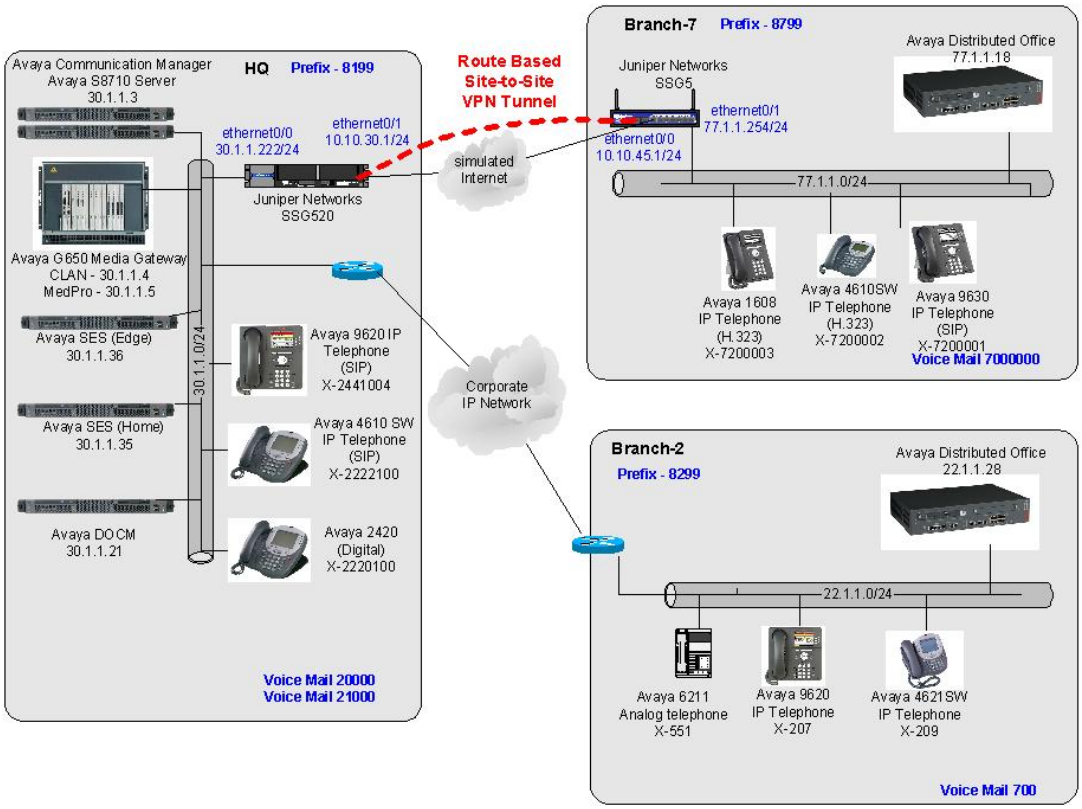


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

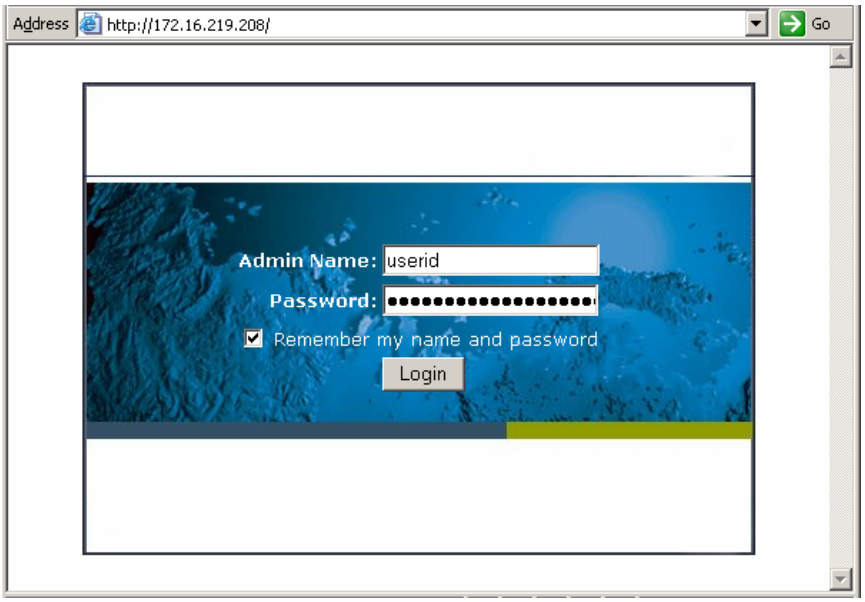
The following equipment and software/firmware were used for the sample configuration:

DEVICE DESCRIPTION	VERSION TESTED
Avaya Distributed Office i40	1.1.1_41.03
Avaya S8710 Server with G650 Gateway	R015x.00.0.825.4
Avaya 6211 Telephone	N/A
Avaya 1608 IP Telephone	1.024
Avaya 4610SW IP Telephone (H.323)	2.8
Avaya 4621SW IP Telephone (H.323)	2.8
Avaya 9620 IP Telephone (SIP)	1.0.2.2
Avaya 9630 IP Telephone (SIP)	1.0.2.2
Juniper Networks SSG520	ScreenOS 6.0R3
Juniper Networks SSG5	ScreenOS 6.0R3

4. Configure Juniper Networks SSG 520

This section describes the configuration for the SSG 520 in **Figure 1**. It is assumed that basic configuration has been performed to allow for IP and WebUI connectivity into the SSG 520. All steps in this section are performed using the Web User Interface (WebUI) of the SSG 520. The complete SSG520 command line configuration is shown in **Section 7** for reference.

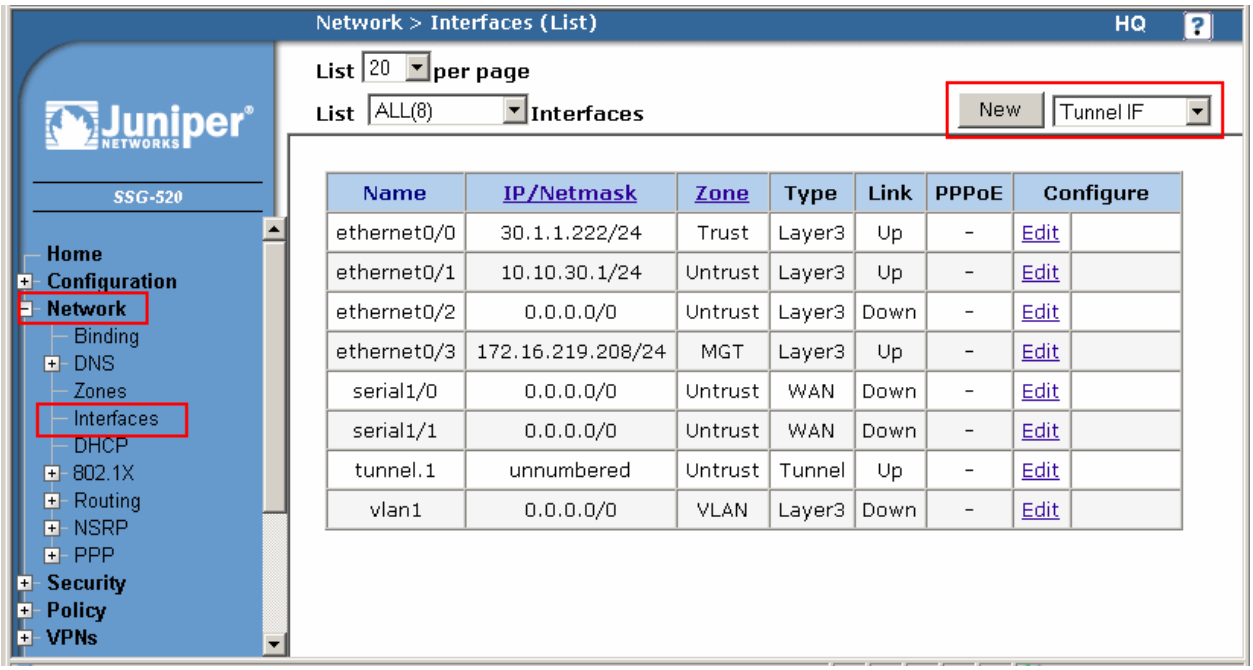
1. Access the WebUI of the SSG 520 by entering its IP address into the Web browser address field. Enter the appropriate **Admin Name:** and **Password:** to log in.



2. Define the interfaces by selecting **Network → Interfaces** from the left panel menu. The tunnel interface is created by selecting **Tunnel IF** from the drop down menu then

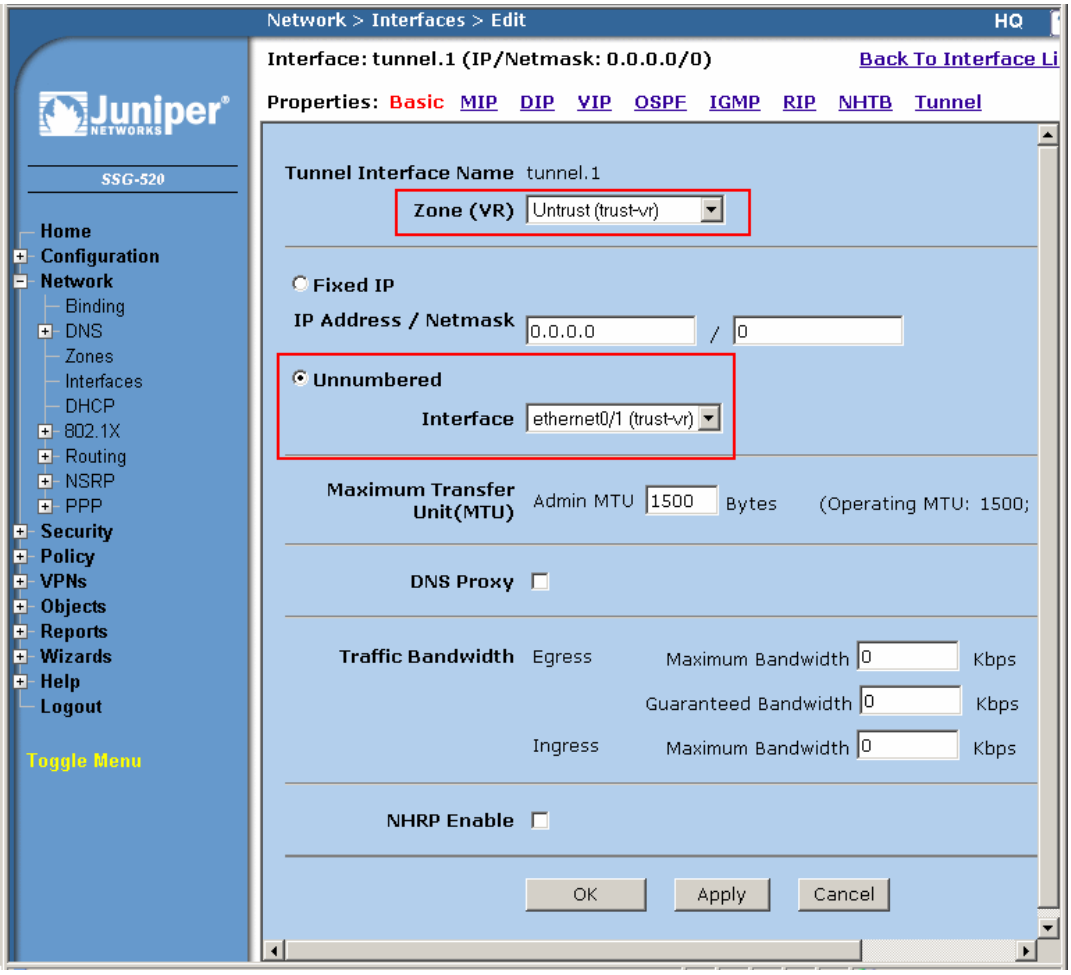
clicking **New**. The following screen capture shows the interfaces used in the sample networks. Below is a brief description for each interface used.

ethernet0/0 Connection to HQ LAN
ethernet0/1 Connection to the Simulated Internet
ethernet0/3 Connection to an out of band management network (optional)
tunnel.1 Virtual interface connecting to Branch-7 where VPN traffic goes through

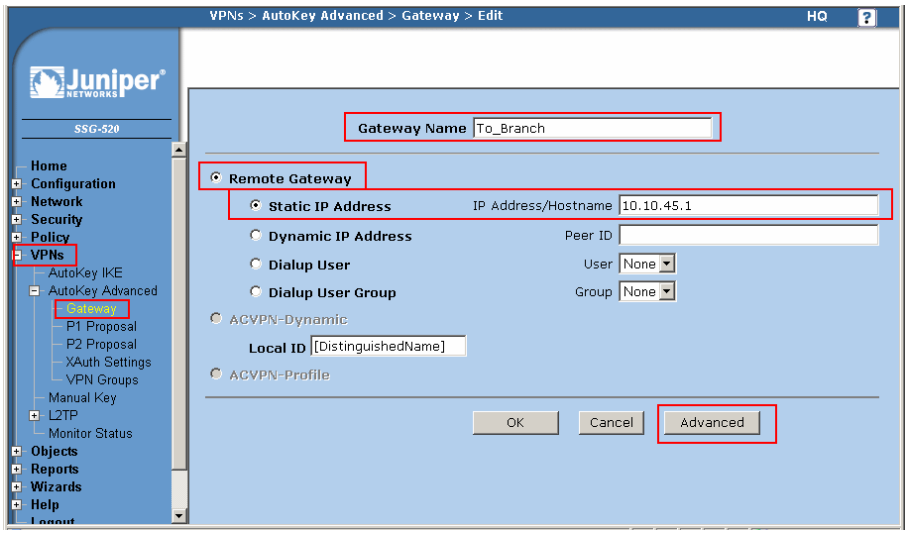


Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure	
ethernet0/0	30.1.1.222/24	Trust	Layer3	Up	-	Edit	
ethernet0/1	10.10.30.1/24	Untrust	Layer3	Up	-	Edit	
ethernet0/2	0.0.0.0/0	Untrust	Layer3	Down	-	Edit	
ethernet0/3	172.16.219.208/24	MGT	Layer3	Up	-	Edit	
serial1/0	0.0.0.0/0	Untrust	WAN	Down	-	Edit	
serial1/1	0.0.0.0/0	Untrust	WAN	Down	-	Edit	
tunnel.1	unnumbered	Untrust	Tunnel	Up	-	Edit	
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	Edit	

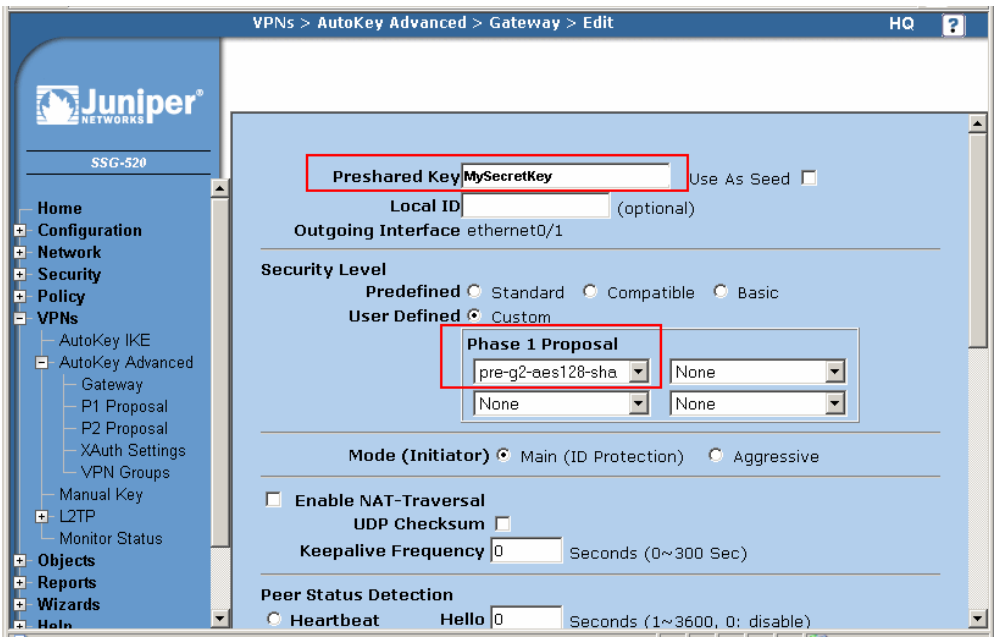
The following screen capture shows the detail for the **tunnel.1** interface.



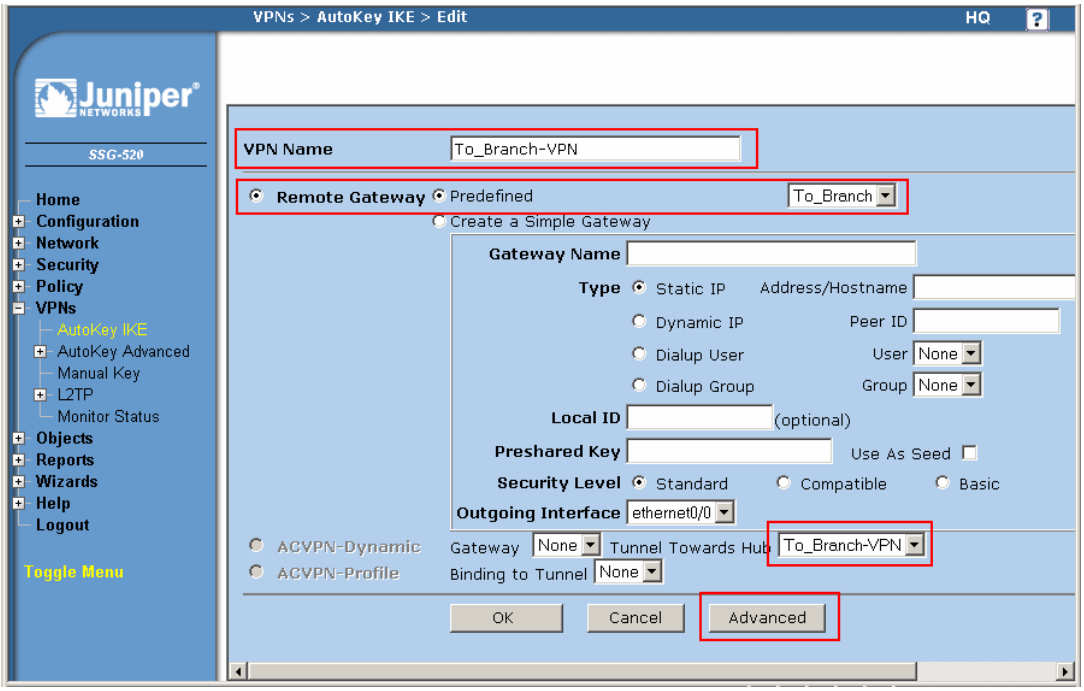
3. Begin VPN configuration by defining the remote gateway. Select **VPNs → Gateway** from the left panel menu. Since the remote gateway public IP address is known, the sample configuration uses this public IP address as the identifier and as a mean to connect to it. There are other means to identify a remote gateway when the remote gateway IP address is dynamic or not known. Please consult reference [7] for details. The following is a screen capture for the basic gateway configuration. Click on **Advanced** to continue the configuration.



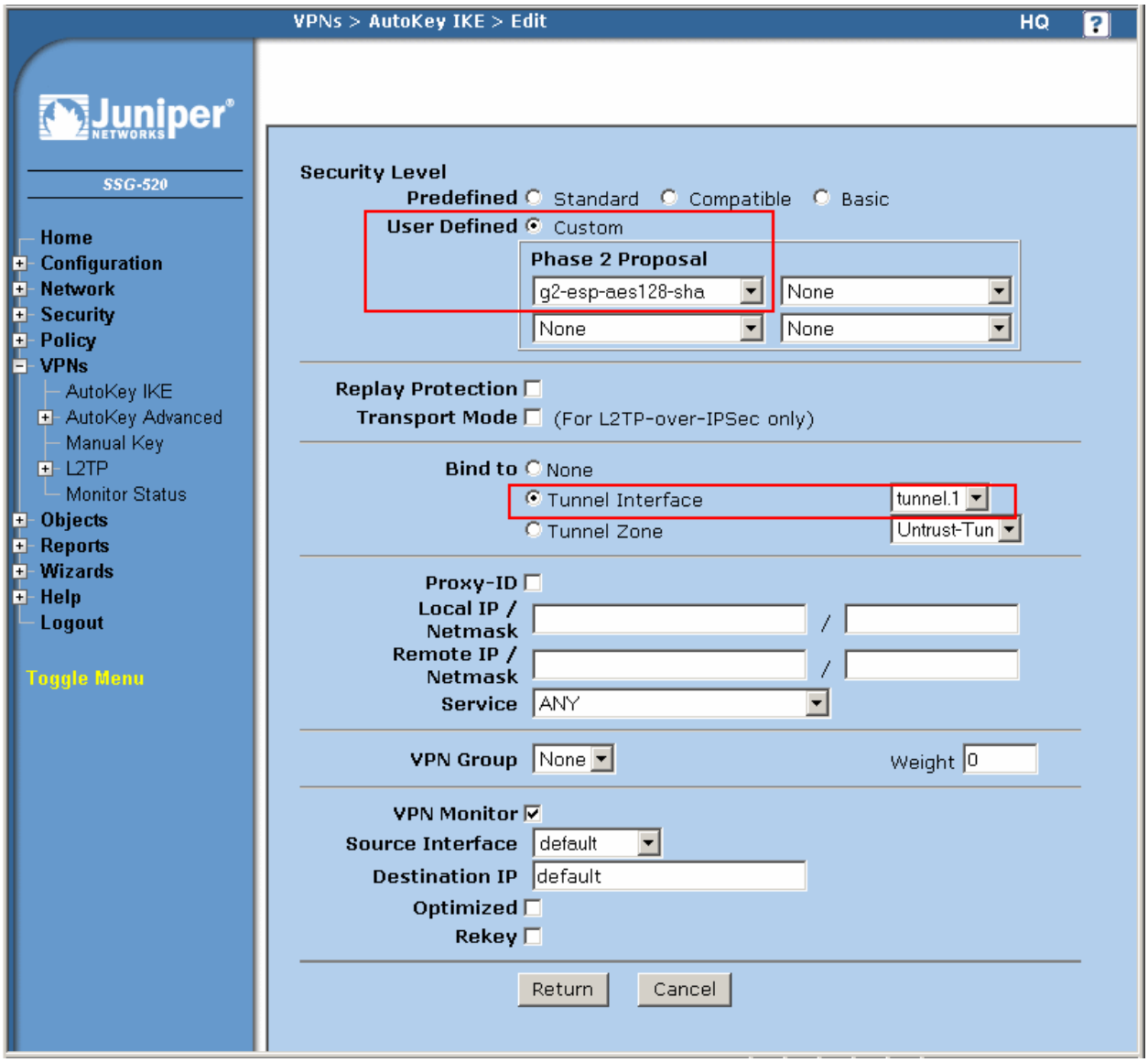
The following abbreviated screen captures shows the configuration used for the gateway after clicking on the **Advanced** button. The **Preshared Key** "MySecretKey" must be the same when entered in the SSG5. Make sure the same Phase 1 Proposal is selected when configuring the SSG5. Click OK (not shown) to complete.



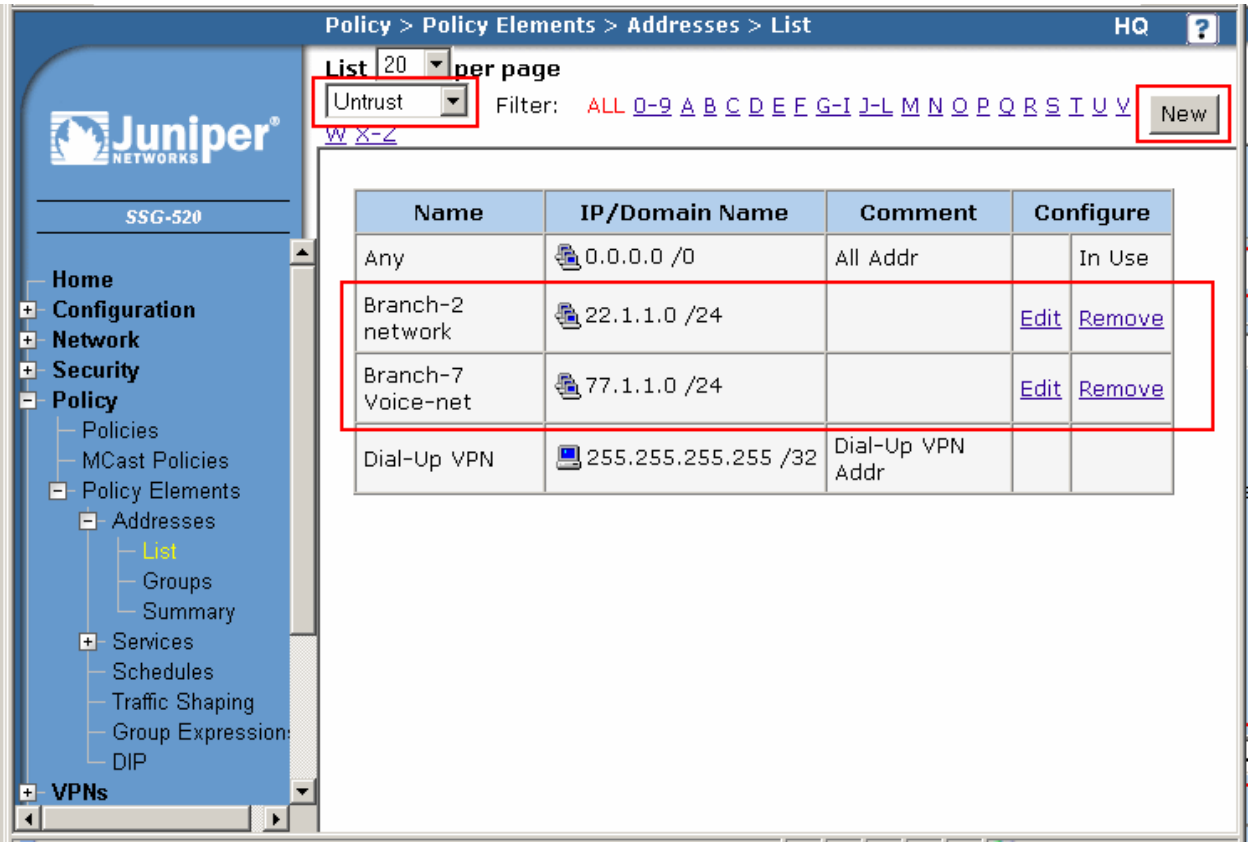
4. Configure the VPN tunnel by selecting **VPNs → AutoKey IKE** from the left panel menu. The following screen capture shows the configuration used for the sample network. Click the **Advanced** button to proceed to the next page.



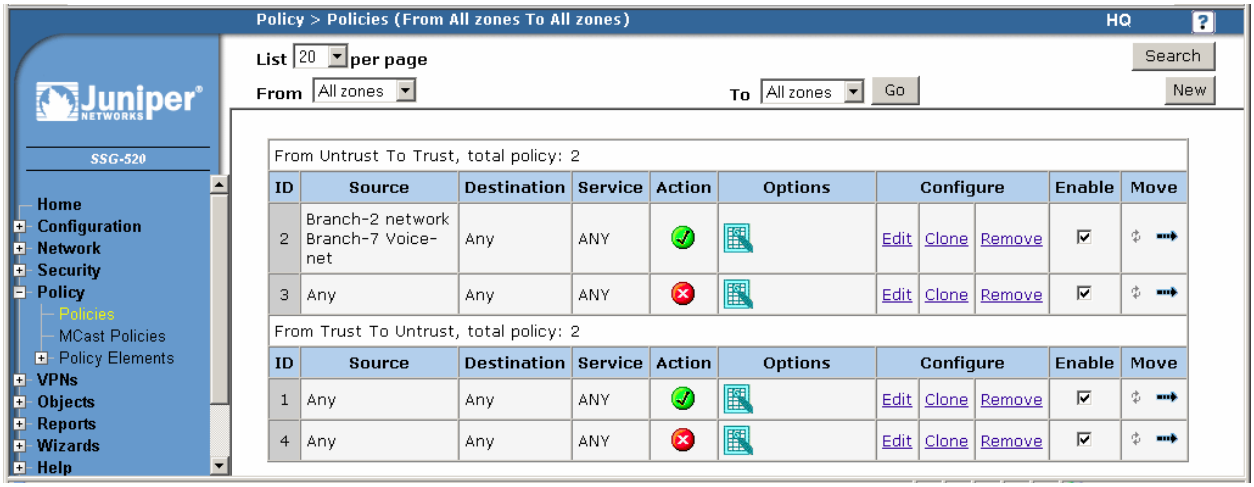
The following screen capture shows the Advanced setting. Ensure the same **Phase 2 Proposal** is selected in the SSG 5.



5. Configure the IP addresses for use by Policies by selecting **Policy → Policy Elements → Addresses → List** from the left panel menu then the **New** button. The following screen capture shows the IP network defined for the Untrust zone.



6. Create a policy by selecting **Policy → Policies** from the left panel menu and clicking **New** button after selecting the **From** and **To** zone in the drop down menu. The screen capture shows the policies defined in the sample network. Any traffic going from Trust to Untrust zone is allowed. The only traffic allowed from the Untrust zone to the Trust zone is from **Branch-2 network** and **Branch-7 voice-net** that were created in Step 5.



5. Configure Juniper Networks SSG 5

This section describes the configuration for the SSG 5 in **Figure 1**. It is assumed that basic configuration has been performed to allow for IP connectivity into the SSG 5. All steps in this section are performed using the Command Line Interface (CLI) of the SSG 5 as a alternative to the WebUI interface. The configuration for the SSG5 is similar to that of the SSG520.

```
#
#---Configure the interfaces
#
set interface ethernet0/0 zone Untrust
set interface ethernet0/0 ip 10.10.45.1/24
set interface ethernet0/0 route
set interface ethernet0/0 ip manageable
#
set interface ethernet0/1 zone Null
set interface ethernet0/1 ip manageable
set interface ethernet0/1 ip 77.1.1.254/24
#
set interface tunnel.1 zone Untrust
set interface tunnel.1 ip unnumbered interface ethernet0/0
#
#---Configure the VPN tunnel
#
set ike gateway "To_HQ" address 10.10.30.1 Main outgoing-interface
"ethernet0/0" preshare MySecretKey proposal "pre-g2-aes128-sha"
set vpn "To_HQ-VPN" gateway "To_HQ" no-replay tunnel idletime 0 proposal
"g2-esp-aes128-sha"
set vpn "To_HQ-VPN" id 1 bind interface tunnel.1
#
#---Configure the Policies
#
set address Trust Branch-7 net 77.1.1.0 255.255.255.0
set address Untrust Branch-2 22.1.1.0 255.255.255.0
set address Untrust HQ-net 30.1.1.0 255.255.255.0

set policy id 3 from Untrust to Trust  Branch-2 Any ANY permit log
set policy id 3
```

```
set src-address HQ-net
exit
set policy id 1 from Trust to Untrust  Any Any ANY permit log
exit
set policy id 4 from Untrust to Trust  Any Any ANY deny log
exit
set policy id 5 from Trust to Untrust  Any Any ANY deny log
exit
```

6. Conclusion

These Application Notes have described the administration steps required to configure a Route-Based Site-to-Site VPN tunnel between the HQ and the Branch-7 site.

7. Verification

1. Use "ping" from a PC to verify traffic can traverse through the VPN tunnel. PC from either the HQ or Branch-7 network should be able to ping another PC on the opposite side of the VPN tunnel.
2. Place call from a telephone to another telephone across the VPN tunnel.

8. Troubleshooting

The following troubleshooting commands are available via the CLI interface of the Juniper Networks Secure Services Gateway.

1. Use the **get sa active** command to get a list of all active Security Associations.

```
HQ-> get sa
total configured sa: 1
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000001<      10.10.45.1  500 esp:a128/sha1 cc166985  1923 unlim A/U    -1 0
00000001>      10.10.45.1  500 esp:a128/sha1 dbe3a951  1923 unlim A/U    -1 0
```

2. Use the **get ike cookie** command to display all the completed Phase 1 negotiations.

```
HQ-> get ike cookies

Active: 1, Dead: 0, Total 1

522f/0003, 10.10.45.1:500->10.10.30.1:500, PRESHR/grp2/AES128/SHA, xchg(5)
(To_Branch/grp-1/usr-1)
resent-tmr 1025 lifetime 28800 lt-recv 28800 nxt_rekey 15460 cert-expire 0
responder, err cnt 0, send dir 1, cond 0x0 nat-traversal map not available
ike heartbeat              : disabled
ike heartbeat last rcv time: 0
ike heartbeat last snd time: 0
XAUTH status: 0
DPD seq local 0, peer 0
```

3. Use the **debug ike basic** command to enable basic debugging of ike messages. Use the **clear dbuf** command to clear the debug buffer. Use the **get db stream** command to view the content of the debug buffer. Below is a sample output of a complete successful tunnel negotiation. To disable debugging, use the **undebug all** command.

```
HQ-> debug ike basic
HQ-> clear dbuf
HQ-> get db stream
## 2008-02-20 07:13:52 : IKE<10.10.45.1> ****** Recv packet if <ethernet0/1> of
vsys <Root> ******
## 2008-02-20 07:13:52 : IKE<10.10.45.1     > Recv : [SA] [VID] [VID] [VID]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [VID]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [VID]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [VID]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [SA]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct ISAKMP header.
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [SA] for ISAKMP
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct NetScreen [VID]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct custom [VID]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct custom [VID]
## 2008-02-20 07:13:52 : IKE<10.10.45.1     > Xmit : [SA] [VID] [VID] [VID]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> ****** Recv packet if <ethernet0/1> of
vsys <Root> ******
## 2008-02-20 07:13:52 : IKE<10.10.45.1     > Recv : [KE] [NONCE]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [KE]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [NONCE]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct ISAKMP header.
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [KE] for ISAKMP
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [NONCE]
## 2008-02-20 07:13:52 : IKE<10.10.45.1     > Xmit : [KE] [NONCE]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> ****** Recv packet if <ethernet0/1> of
vsys <Root> ******
## 2008-02-20 07:13:52 : IKE<10.10.45.1     > Recv*: [ID] [HASH]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [ID]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [HASH]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct ISAKMP header.
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [ID] for ISAKMP
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [HASH]
## 2008-02-20 07:13:52 : IKE<10.10.45.1     > Xmit*: [ID] [HASH]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> peer_identity_unregister_p1_sa.
## 2008-02-20 07:13:52 : IKE<10.10.45.1> peer_idt.c peer_identity_unregister_p1_sa
512: pidt deleted.
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Phase 1: Completed Main mode negotiation
with a <28800>-second lifetime.
## 2008-02-20 07:13:52 : IKE<10.10.45.1> ****** Recv packet if <ethernet0/1> of
vsys <Root> ******
## 2008-02-20 07:13:52 : IKE<10.10.45.1     > Recv*: [HASH] [SA] [NONCE] [KE] [ID]
[ID] [NOTIF]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [SA]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [KE]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [NONCE]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [ID]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [ID]:
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Process [NOTIF]:
## 2008-02-20 07:13:52 : IKE<0.0.0.0        > BN, top32 dmax64 zero<no>
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct ISAKMP header.
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [HASH]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [SA] for IPSEC
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [NONCE] for IPSec
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [KE] for PFS
```

```
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [ID] for Phase 2
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [ID] for Phase 2
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Construct [NOTIF] (NOTIFY_NS_NHTB_INFORM)
for IPSEC
## 2008-02-20 07:13:52 : IKE<10.10.45.1     > Xmit*: [HASH] [SA] [NONCE] [KE] [ID]
[ID] [NOTIF]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> ****** Recv packet if <ethernet0/1> of
vsys <Root> ******
## 2008-02-20 07:13:52 : IKE<10.10.45.1     > Recv*: [HASH]
## 2008-02-20 07:13:52 : IKE<10.10.45.1> Phase 2 msg-id <b0a50c7d>: Completed Quick
Mode negotiation with SPI <ce166985>, tunnel ID <1>, and lifetime <3600>
seconds/<0> KB.
## 2008-02-20 07:13:53 : IKE<0.0.0.0        > BN, top32 dmax64 zero<no>
```

4. Use the **clear ike** command to force a VPN tunnel to renegotiate. This command will clear Phase 1 and Phase 2 for the specified tunnel.

9. Additional References

Product documentation for Avaya products may be found at http://support.avaya.com

[1] *Avaya Distributed Office i120 Installation Quick Start*, May 2007 Issue 1, Document Number 03-602289
[2] *Sample Configuration for SIP Private Networking among Avaya Distributed Office sites and Avaya Communication Manager Release 5 with Co-Resident SES Home*, Issue 1, Application Notes
[3] *Sample Configuration for Juniper Networks Secure Services Gateway 5 to support Avaya 3631 Wireless Telephone registering with Avaya Distributed Office*, Issue 1.0

Product documentation for Juniper Networks products may be found at http://www.Juniper.net

[4] *Concepts & Examples ScreenOS Reference Guide, Volume 1: Overview*, Release 6.0.0 Rev. 02, Part Number 530-017768-01, Revision 02
[5] *Concepts & Examples ScreenOS Reference Guide, Volume 2: Fundamentals*, Release 6.0.0 Rev. 01, Part Number 530-017768-01, Revision 01
[6] *Concepts & Examples ScreenOS Reference Guide, Volume 3: Administration*, Release 6.0.0 Rev. 01, Part Number 530-017768-01, Revision 01
[7] *Concepts & Examples ScreenOS Reference Guide, Volume 5: Virtual Private Networks*, Release 6.0.0 Rev. 01, Part Number 530-017768-01, Revision 01

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