Application Notes for Site-to-Site VPN Tunnel using Juniper Networks SRX210 Services Gateway to support Avaya Aura® Communication Manager – Issue 1.0

Abstract

These Application Notes describe the steps for configuring a route-based Site-to-Site VPN Tunnel between two Juniper Networks SRX210 Services Gateways in an Avaya Telephony environment. 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.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe a solution for configuring a route-based Site-to-Site VPN tunnel using Juniper Networks SRX210 Services Gateways (herein referred to as SRX210) in an Avaya Telephony environment.

SRX210 Series Services Gateways are routing and network solutions for enterprise and service providers. During the compliance test, the following was performed with SRX210.

- Site-to-site VPN
- VPNremote phones (H.323)

2. General Test Approach and Test Results

All test cases were performed manually. The general approach was to place various types of calls (SIP to SIP, SIP to H.323 and H.323 to SIP) to and from stations through the VPN tunnel. For feature testing, the types of calls included inbound and outbound calls through the VPN tunnel, transferred calls, conferenced calls, and MWI and voicemail. During the compliance test, SRX210 was used for DHCP server. For serviceability testing, failures such as cable pulls, and resets were applied. All test cases passed.

During the compliance test for the VPNremote phone, the shuffling was turned off for the network region (Direct IP Audio was disabled). With shuffling on, one way audio was observed. By turning off shuffling, a call will utilize the media processor for the duration of the call.

2.1. Interoperability Compliance Testing

The interoperability compliance test included feature and serviceability testing. The feature testing evaluated the VPN tunnel between SRXs with inbound, outbound, transfer, conference, MWI, and voicemail. The serviceability testing introduced failure scenarios to see if SRX210 could resume operating after failure recovery.

2.2. Support

Technical support on SRX210 can be obtained through the following:

- **Phone:** (888) 314-5822
- **Web:** http://www.juniper.net/support/requesting-support.html

3. Reference Configuration

Figure 1 provides the test configuration used for the compliance testing.

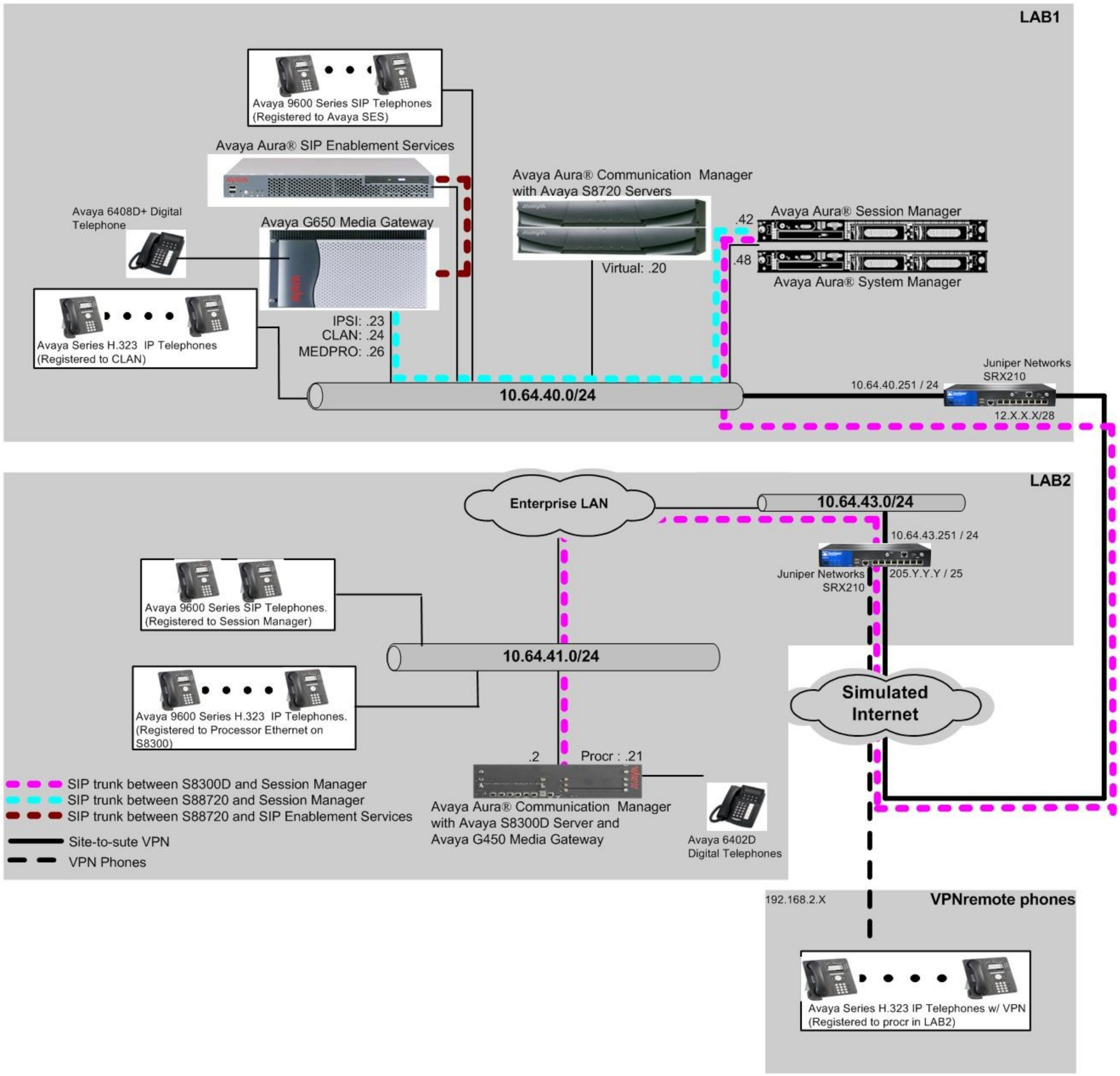
LAB1
Avaya 9600 Series SIP Telephones
(Registered to Avaya SES)
Avaya Aura® SIP Enablement Services
Avaya Aura® Communication Manager
with Avaya S8720 Servers
Avaya 6408D+ Digital
Telephone
Avaya G650 Media Gateway
.42
Avaya Aura® Session Manager
.48
Avaya Aura® System Manager
Virtual: .20
Avaya Series H.323 IP Telephones
(Registered to CLAN)
IPSI: .23
CLAN: .24
MEDPRO: .26
10.64.40.0/24
Juniper Networks
SRX210
10.64.40.251 / 24
12.X.X.X/28
LAB2
Enterprise LAN
10.64.43.0/24
10.64.43.251 / 24
Juniper Networks
SRX210
205.Y.Y.Y / 25
Avaya 9600 Series SIP Telephones.
(Registered to Session Manager)
10.64.41.0/24
Avaya 9600 Series H.323 IP Telephones.
(Registered to Processor Ethernet on S8300)
Simulated Internet
.2
Procr : .21
Avaya Aura® Communication Manager
with Avaya S8300D Server and
Avaya G450 Media Gateway
Avaya 6402D
Digital Telephones
SIP trunk between S8300D and Session Manager
SIP trunk between S88720 and Session Manager
SIP trunk between S88720 and SIP Enablement Services
Site-to-sute VPN
VPN Phones
192.168.2.X
VPNremote phones
Avaya Series H.323 IP Telephones w/ VPN
(Registered to procr in LAB2)

Figure 1: Juniper Networks SRX210s in an Avaya Telephony environment.

4. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300D Server with Avaya G450 Media Gateway	6.0.1(R016x.00.1.510.1) w/ patch 00.1.510.1-18860
Avaya Aura® System Manager	6.1 (R6-1-0-20-0)
Avaya Aura® Session Manager	6.1
Avaya S8700 Servers with Avaya G650 Media Gateway	Avaya Communication Manager 5.2.1 (R015x.02.1.016.4)
Avaya 9600 Series IP Telephones	
9620 (H.323) 9630 (H.323)	3.1 3.1
Avaya 9600 Series SIP Telephones	
9630 (SIP) 9640 (SIP) 9650 (SIP)	2.6.4 2.6.4 2.6.4
Avaya 6400 Series Digital Telephones	N/A
Avaya C363T-PWR Converged Stackable Switch	4.5.14
Extreme Networks Summit 48	4.1.21
Juniper Networks SRX210 Service Gateway	11.2R2.4

5. Configure Avaya Testing Environment

This section describes the configuration for the Avaya Telephony testing environment, shown in **Figure 1**. All calls between lab1 and lab2 go through the VPN tunnel. The main focus of the testing was verifying the VPN tunnel between SRX210s. Thus, configuration steps of Avaya testing environment will not be discussed in these Application Notes.

6. Configure Juniper Networks SRX210

This section describes the configuration for the SRX210 in **Figure 1**. It is assumed that basic configuration has been performed to allow for IP and WebUI connectivity into the SRX210. All steps in this section are performed using the command line interface (CLI) of the SRX210. The engineer from Juniper configured SRX 210s for setting up a VPN tunnel, using the IP address information that Avaya engineer provided.

The following configuration file describes the VPN settings on LAB2. This contains the HQ VPN Configuration as well as the configuration necessary to support VPNremote phone IPSec termination.

Full SRX Config (for HQ SRX-1)

Configure Network Interfaces

```
set interfaces ge-0/0/0 unit 0 family inet address 205.Y.Y.Y/25
set interfaces st0 unit 0 description VPN-Tunnel
set interfaces st0 unit 0 family inet
set interfaces vlan unit 0 family inet address 10.64.43.251/24
```

Configure static route

```
set routing-options static route 0.0.0.0/0 next-hop 205.Y.Y.1
set routing-options static route 10.64.41.0/24 next-hop 10.64.43.1
set routing-options static route 10.64.42.0/24 next-hop 10.64.43.1
set routing-options static route 10.64.40.0/24 next-hop st0.0
```

Configure VPN tunnel – Phase 1 Proposal

```
set security ike respond-bad-spi
set security ike proposal avaya-phones-p1 authentication-method pre-shared-keys
set security ike proposal avaya-phones-p1 dh-group group2
set security ike proposal avaya-phones-p1 authentication-algorithm md5
set security ike proposal avaya-phones-p1 encryption-algorithm 3des-cbc
set security ike proposal avaya-phones-p1 lifetime-seconds 28800
```

Configure VPN tunnel – Policy

```
set security ike policy avaya-phones mode aggressive
set security ike policy avaya-phones proposals avaya-phones-p1
set security ike policy avaya-phones pre-shared-key ascii-text 123456
set security ike policy SiteVPN mode main
set security ike policy SiteVPN proposals avaya-phones-p1
set security ike policy SiteVPN pre-shared-key ascii-text 123456
```

Configure VPNremote phone

```
set security ike gateway Avaya-Phone-IKE ike-policy avaya-phones
set security ike gateway Avaya-Phone-IKE dynamic user-at-hostname "vpnphone@avaya.com"
set security ike gateway Avaya-Phone-IKE dynamic connections-limit 10
set security ike gateway Avaya-Phone-IKE dynamic ike-user-type shared-ike-id
set security ike gateway Avaya-Phone-IKE dead-peer-detection interval 60
set security ike gateway Avaya-Phone-IKE dead-peer-detection threshold 2
set security ike gateway Avaya-Phone-IKE nat-keepalive 5
set security ike gateway Avaya-Phone-IKE external-interface ge-0/0/0.0
set security ike gateway Avaya-Phone-IKE xauth access-profile phone-users
set security ike gateway BranchVPN ike-policy SiteVPN
set security ike gateway BranchVPN address 12.X.X.X
set security ike gateway BranchVPN external-interface ge-0/0/0.0
```

Configure VPN tunnel – Phase 2

```
set security ipsec proposal Avaya-Phones-P2 protocol esp
set security ipsec proposal Avaya-Phones-P2 authentication-algorithm hmac-sha1-96
set security ipsec proposal Avaya-Phones-P2 encryption-algorithm aes-128-cbc
set security ipsec proposal Avaya-Phones-P2 lifetime-seconds 3600
set security ipsec policy Avaya-Phones-IPSec proposals Avaya-Phones-P2
set security ipsec vpn Avaya-Phones-VPN vpn-monitor
set security ipsec vpn Avaya-Phones-VPN ike gateway Avaya-Phone-IKE
set security ipsec vpn Avaya-Phones-VPN ike ipsec-policy Avaya-Phones-IPSec
set security ipsec vpn Branch-VPN bind-interface st0.0
set security ipsec vpn Branch-VPN vpn-monitor
set security ipsec vpn Branch-VPN ike gateway BranchVPN
set security ipsec vpn Branch-VPN ike proxy-identity local 10.64.0.0/16
set security ipsec vpn Branch-VPN ike proxy-identity remote 10.64.40.0/24
set security ipsec vpn Branch-VPN ike ipsec-policy Avaya-Phones-IPSec
set security ipsec vpn Branch-VPN establish-tunnels immediately
```

Lower the TCP-MSS values for IPSec Traffic

```
set security flow tcp-mss ipsec-vpn mss 1400
```

Security Zone and Policy Configuraiton

```
set security nat proxy-arp interface vlan.0 address 192.168.2.1/32 to 192.168.2.100/32
set security policies from-zone untrust to-zone trust policy Phone-VPN match source-address any
set security policies from-zone untrust to-zone trust policy Phone-VPN match destination-address 10.64.0.0/16
set security policies from-zone untrust to-zone trust policy Phone-VPN match application any
set security policies from-zone untrust to-zone trust policy Phone-VPN then permit tunnel ipsec-vpn Avaya-Phones-VPN
set security zones security-zone trust address-book address 10.64.0.0/16 10.64.0.0/16
set security zones security-zone trust interfaces vlan.0
set security zones security-zone trust interfaces st0.0 host-inbound-traffic system-services all
set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic system-services ike
```

VPNremote phone User configuration (Add additional users as desired)

```
set access profile phone-users client "vpnphone2@avaya.com" pap-password 123456
set access profile phone-users client "vpnphone2@avaya.com" firewall-user password 123456
set access profile phone-users client "vpnphone@avaya.com" pap-password 123456
set access profile phone-users client "vpnphone@avaya.com" firewall-user password 123456
set access profile phone-users address-assignment pool phone-pool
set access address-assignment pool phone-pool family inet network 192.168.2.0/24
set access address-assignment pool phone-pool family inet xauth-attributes primary-dns 4.2.2.2/32
set poe interface all
```

The following configuration file describes the VPN settings on the LAB1 side (the Remote Site VPN). It does not include the configuration for the VPNremote phones.

Full Config for Branch SRX Device (SRX-Branch) VPN Configuration only

```
set system host-name SRX210-Branch
```

Configure DHCP settings

```
set system services dhcp router 10.64.40.251
set system services dhcp option 242 string MCIPADD=10.64.41.21,HTTPSRVR=10.64.40.250,HTTPDIR=9600vpn,L2QVLAN=0
set system services dhcp pool 10.64.40.0/24 address-range low 10.64.40.2
set system services dhcp pool 10.64.40.0/24 address-range high 10.64.40.254
```

Configure Network Interfaces

```
set interfaces ge-0/0/0 unit 0 family inet address 12.X.X.X/28
set interfaces st0 unit 0 description "VPN Tunnel"
set interfaces st0 unit 0 family inet
set interfaces vlan unit 0 family inet address 10.64.40.251/24
```

Configure static route

```
set routing-options static route 0.0.0.0/0 next-hop 12.X.X.129
set routing-options static route 10.64.43.0/24 next-hop st0.0
set routing-options static route 10.64.41.0/24 next-hop st0.0
```

Configure VPN tunnel – Phase 1 Proposal

```
set security ike proposal SiteVPNP1 authentication-method pre-shared-keys
set security ike proposal SiteVPNP1 dh-group group2
set security ike proposal SiteVPNP1 authentication-algorithm md5
set security ike proposal SiteVPNP1 encryption-algorithm 3des-cbc
set security ike proposal SiteVPNP1 lifetime-seconds 28800
```

Configure VPN tunnel – Policy

```
set security ike policy SiteVPN mode main
set security ike policy SiteVPN proposals SiteVPNP1
set security ike policy SiteVPN pre-shared-key ascii-text 123456
set security ike gateway HQSite ike-policy SiteVPN
set security ike gateway HQSite address 205.Y.Y.Y
set security ike gateway HQSite external-interface ge-0/0/0.0
```

Configure VPN tunnel – Phase 2

```
set security ipsec proposal p2 protocol esp
set security ipsec proposal p2 authentication-algorithm hmac-sha1-96
set security ipsec proposal p2 encryption-algorithm aes-128-cbc
set security ipsec proposal p2 lifetime-seconds 3600
set security ipsec policy 2 proposals p2
set security ipsec vpn HQVPN bind-interface st0.0
set security ipsec vpn HQVPN ike gateway HQSite
set security ipsec vpn HQVPN ike proxy-identity local 10.64.40.0/24
set security ipsec vpn HQVPN ike proxy-identity remote 10.64.0.0/16
set security ipsec vpn HQVPN ike ipsec-policy 2
set security ipsec vpn HQVPN establish-tunnels immediately
```

Lower the TCP-MSS values for IPSec Traffic

```
set security flow tcp-mss ipsec-vpn mss 1400

set security zones security-zone untrust interfaces ge-0/0/0.0 host-inbound-traffic system-services ike
set poe interface all
```

The following file describes the 96xx type IP phones setting file used during the compliance test. A similar settings file will be needed to configure any 9600 Series phone running the VPN Firmware.:

Avaya 9600 settings file

```
SET NVVPNMODE 1
SET NVVPNCFGPROF 5
SET NVVPNAUTHTYPE 2
SET NVSGIP 205.Y.Y.Y
SET NVMCIPADD 10.64.41.21
SET NVVPNUSERTYPE 1
SET NVVPNUSER "vpnphone@avaya.com"
SET NVVPNPSWD "123456"
SET NVIKEID "vpnphone@avaya.com"
SET NVIKEPSK "123456"
SET NVVPNPSWDTYPE 1
SET NVVPNENCAPS 4
SET NVIKEIDTYPE 3
SET NVXAUTH 1
SET NVIKEXCHGMODE 1
SET NVIKECONFIGMODE 1
SET NVIKEDHGRP 0
SET NVIKEP1ENCALG 2
SET NVIKEP1AUTHALG 1
SET NVPFSDHGRP 0
SET NVIKEP2AUTHALG 0
SET NVIKEP2ENCALG 0
SET NVVPNCOPYTOS 1
SET QTEST 2
SET NVVPNCONCHECK 3
SET VPNPROC 2
SET NVIPSECSUBNET 10.64.0.0/16
SET ENHDIALSTAT 1
SET PHNCC 1
SET PHNDPLENGTH 4
SET PHNIC 011
SET PHNLD 1
SET PHNLDLENGTH 10
SET PHNOL 9
SET APPSTAT 1
SET OPSTAT 111
SET AGCHAND 1
SET AGCHEAD 1
SET AGCSPKR 1
SET PHY1STAT 1
SET PHY2STAT 1
SET BAKLIGHTOFF 30
SET SYSLANG English
SET SCREENSAVERON 30
SET RESTORESTAT 1
SET FTPUSERSTAT 1
SET AUDASYS 3
SET L2Q 0

GOTO END
# END
```

7. Verification Steps

7.1. Verification from SRX210

The following troubleshooting commands are available via the CLI interface of the Juniper Networks SRX 210 Service Gateway.

The following shows the status of IKE Phase I Negotiations. In this example both the remote site SRX210 as well as the VPNremote phones are active on the HQ Device.

```
root# run show security ike security-associations
Index     State   Initiator cookie       Responder cookie     Mode          Remote Address
8170169 UP      ee76cf905957c616   e767603b50769b05  Main            205.168.62.87
8170170 UP      041721ec381dc50e  208c1c3ac86a2b29   Aggressive    205.168.62.87
```

The following shows the IPSec Phase II Negotiation details on the HQ Device. In this example both the remote site SRX210 as well as the VPNremote phones have active IPSec Phase II SAs.

```
root# run show security ipsec security-associations
  Total active tunnels: 2
  ID    Algorithm       SPI      Life:sec/kb  Mon vsys Port  Gateway
  <131073 ESP:aes-128/sha1 ad3913ec 3530/ unlim U  root 500   205.168.62.87
  >131073 ESP:aes-128/sha1 8ef58c26 3530/ unlim U  root 500   205.168.62.87
  <133955585 ESP:aes-128/sha1 3bde4639 3531/ unlim U root 46174 205.168.62.87
  >133955585 ESP:aes-128/sha1 2e092118 3531/ unlim U root 46174 205.168.62.87

ESP Statistics:
  Encrypted bytes:        28470224
  Decrypted bytes:        17262371
  Encrypted packets:        130306
  Decrypted packets:        117594
AH Statistics:
  Input bytes:                 0
  Output bytes:                0
  Input packets:               0
  Output packets:              0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0
```

The following shows the active VPNremote phone users by IKE Identity and XAUTH Username as well as the assigned IP Address for each VPNremote phone.

```
root> show security ike active-peer
Remote Address      Port     Peer IKE-ID             XAUTH username          Assigned IP
205.168.62.87       500      205.168.62.87
205.168.62.87       40845    vpnphone@avaya.com      vpnphone@avaya.com      192.168.2.56
205.168.62.87       41923    vpnphone@avaya.com      vpnphone2@avaya.com     192.168.2.57
```

7.2. Verification from Avaya Aura® Communication Manager

After the VPN tunnel is up, check the status from Communication Manager, using the following command:

- "**status trunk xx**", where xx is the relevant trunk group number, and verify the trunk is up.
- "**list trace tac yy**", where yy is the relevant trunk access code, and verify the signaling and RTP can be crossed through the VPN tunnel.

8. Conclusion

These Application Notes describe the procedures required to configure Juniper Networks SRX210 Services Gateways in an Avaya Telephony environment. Juniper Networks SRX210 Services Gateways successfully passed compliance testing.

9. Additional References

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

[1] *Administering Avaya Aura™ Communication Manager*, Release 6.0, June 2010, Issue 6.0, Document Number 03-300509

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

[2] SRX Series Services Gateways for the Branch
http://www.juniper.net:80/elqNow/elqRedir.htm?ref=http://www.juniper.net/us/en/local/pdf/datasheets/1000281-en.pdf

[3] SRX210 Services Gateway Hardware documentation
http://www.juniper.net/techpubs/en_US/release-independent/junos/information-products/pathway-pages/hardware/srx210/index.html

[4] Powering Unified Communications with Branch SRX Series Services Gateways
http://www.juniper.net:80/elqNow/elqRedir.htm?ref=http://www.juniper.net/us/en/local/pdf/whitepapers/2000373-en.pdf

[5] Implementing Policy-Based IPsec VPN Using SRX Series Services Gateways
http://www.juniper.net:80/elqNow/elqRedir.htm?ref=http://www.juniper.net/us/en/local/pdf/app-notes/3500175-en.pdf

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 DevConnect Program at devconnect@avaya.com.