INTRODUCTION TO AUTOVPN

Implementing AutoVPN Network Design Using the SRX Series with iBGP as the Dynamic Routing Protocol

Table of Contents

List of Tables

List of Figures

Introduction

AutoVPN is a key feature that is configured and managed on the Juniper Networks® SRX Series Services Gateways. AutoVPN simplifies the planning, design, and provisioning process of VPNs by enabling network administrators to configure the hub just once, even when new spokes are deployed at a later time. Specifically, network administrators need to configure the routing, interfaces, Internet Key Exchange (IKE), and IPsec hub settings only once. No subsequent hub configuration changes are needed even when spoke devices are added or deleted. This capability reduces IT effort to save time and costs for configuring their VPN hub-and-spoke devices.

By reducing hub configuration for the VPN network to just one time for initial design, AutoVPN reduces the deployment and configuration complexity and risks associated with these changes. AutoVPN enables the automatic acceptance of permissible spokes with zero impact on existing connections. In aggregate, these capabilities reduce the risk of network downtime, ensuring business productivity and guaranteeing network service-level agreements (SLAs).

Scope

This document provides design guidance for deploying an AutoVPN solution that connects branch office locations to the data center as shown in Figure 1. It offers the connectivity practices and guidelines for network design using internal BGP (iBGP), X.509v3 certificates, and virtual routers in an AutoVPN hub-and-spoke deployment.

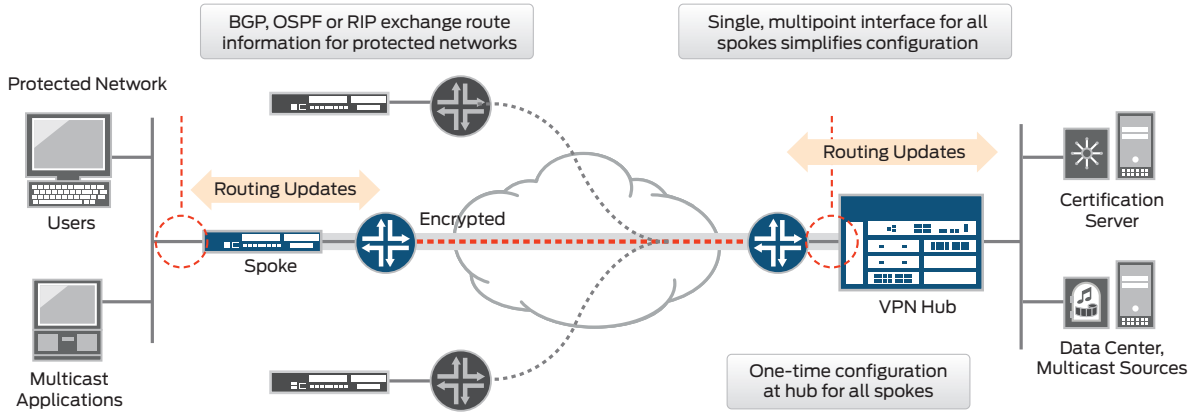

Figure 1: AutoVPN solution connecting data center and branch locations

Target Audience

- IT managers
- Systems engineers
- Network engineers
- Network administrators
- Security managers

Design Considerations

Platform Support

The AutoVPN feature set is supported on Juniper Networks SRX Series Services Gateways for the branch and high end, working in stand-alone and cluster mode. Following are lists of supported devices and the minimum software versions required. Note that Juniper Networks J Series Services routers do not support AutoVPN.

Hardware Requirements

Feature	SRX100 SRX110 SRX210 SRX220 SRX240	SRX550 SRX650	SRX1400 SRX3400 SRX3600 SRX5600 SRX5800	J Series
Hub	SRX240 only	Yes	Yes	No
Spokes	Yes	Yes	SRX1400 only	No

Software Requirements

- Juniper Networks Junos® operating system Release 12.1X45-D10 or later

AutoVPN Advantages

- Requires no hub reconfiguration effort for adding/deleting new spokes
- Minimizes network administration by reducing costs for configuration of VPN hub and spokes
- Simplifies design process with fewer components such as only routing and public key infrastructure (PKI)
- Centralizes VPN management to ensure consistent policy
- Minimizes impact to network and security uptime
- Seamlessly adds new spokes without changes to the network
- Eliminates risk due to configuration issues to the existing network when adding spokes

AutoVPN Limitations

- Manual next-hop tunnel binding (NHTB) is not supported for AutoVPN.
- Auto NHTB requires proprietary payload during IPsec negotiation; thus, interoperability with third-party vendor equipment is not supported. Interoperability with Juniper Networks M Series Multiservice Edge Routers, MX Series 3D Universal Edge Routers, and T Series Core Routers is not supported as well.
- VPN monitor "destination-ip" configuration cannot be supported in the hub with AutoVPN. When certificate-based authentication is used for AutoVPN with IKE main mode, there will be an additional configuration limitation (all gateway configurations having the same external interface must use the same IKE policy due to an IKEv1 protocol limitation).
- Interoperability with ScreenOS hub and spokes.
- In 12.1X45D10 release, the connection limit for high-end SRX Series gateways is not supported.
- Group IKE-ID with IKE-ID type as IP address is not supported.
- On high-end SRX Series devices, tunnel distribution for dial-up VPNs is based on round robin. This means that tunnels may not be evenly distributed.
- In 12.1X45D10 release, IKE-ID should not overlap with other dial-up gateways. If IKE-ID overlaps, IKE may be the wrong gateway for negotiation.
- AutoVPN support is only based on route-based dial-up VPN; there is no support for policy-based AutoVPN.
- In 12.1X45D10 release, initial contact for aggressive mode is not supported.
- In 12.1X45D10 release, PIM is supported with BGP and OSPF only, there is no RIP support.

AutoVPN vs. Other Solutions

Table 1: AutoVPN Compared to Other Solutions

	AutoVPN	Dynamic Multipoint VPN	Auto Connect VPN
OS support	Junos OS	IOS	ScreenOS
Dynamic hub-and-spoke deployment	Yes	Yes	Yes
Spoke-to-spoke deployment	No	Yes	Yes
Underlying technology	NHTB	Multipoint Generic Routing EncapsulationGRE and NHRP	NHRP
Redundancy	Yes	Yes	Yes

AutoVPN Interoperability

There is no AutoVPN interoperability with ScreenOS and with M Series, T Series, and MX Series devices.

AutoVPN Performance and Scaling

Table 2. Branch SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 Services Gateways

Platform	OSPF Max Routes	OSPF Neighbor	iBGP Max Routes	iBGP Max Neighbor	RIP Max Routes	RIP Max Neighbor
SRX100	512	100	8,000	100	2,000	128
SRX110	512	100	8,000	100	2,000	128
SRX210	512	100	16,000	100	2,000	128
SRX210E	2,000	100	16,000	100	2,000	128
SRX220	10,000	100	32,000	100	2,000	128
SRX240	10,000	100	64,000	512	2,000	128
SRX550	10,000	100	100,000	1,024	2,000	128
SRX650	10,000	500	100,000	1,024	2,000	128

Table 3. High-End SRX Series (SRX1K, SRX3K, SRX5K) Services Gateways

Platform	OSPF Max Routes	OSPF Neighbor	iBGP Max Routes	iBGP Max Neighbor	RIP Max Routes	RIP Max Neighbor
SRX1400	700,000	500	700,000	4,000	4,000	1,000
SRX3000 line	700,000	500	700,000	4,000	4,000	1,000
SRX5000 line	700,000	500	700,000	5,000	4,000	1,000

AutoVPN Debugging

Common Failures and Remedies

- Peer IP is not reachable: Make sure peer is reachable.
- Proposal mismatch: Make sure proposal is configured correctly.
- Network Time Protocol (NTP) is not set: NTP is mandatory; make sure that NTP is set and synchronized to server.
- Certificate validation fails: Make sure that certificate authority (CA)/local certificate is valid with “request security pki <ca-cert/local-cert> verify” command before initiating tunnel.
- Messages log for basic information. If the tunnel does not come up after checking that IP is reachable, CA has succeeded, and configuration is correct, then checking the messages log would be your first step. If there is no clue on the messages log, kmd and pkid trace option might need to be enabled

System Log Configuration for AutoVPN

- set system syslog file vpn_syslog daemon any
- set system syslog file vpn_syslog match “kmd|pkid”

Auto VPN Technology Overview

AutoVPN is supported on route-based IPsec VPNs. AutoVPN traffic must be IPv4. Dynamic routing protocols are supported to forward packets through the VPN tunnels.The supported authentication for AutoVPN hubs and spokes is X.509 public key infrastructure (PKI) certificates. The group IKE user type configured on the hub allows

strings to be specified to match the alternate subject field in spoke certificates. Partial matches for the subject fields in spoke certificates can also be specified.

AutoVPN is configured and managed on SRX Series devices using the CLI. Multiple AutoVPN hubs can be configured on a single SRX Series device. The maximum number of spokes supported by a configured hub is specific to the model of the SRX Series device.AutoVPN supports VPN monitoring and dead peer detection.

In AutoVPN deployments, the hub and spoke devices must have valid X.509 PKI certificates loaded. You can use the show security pki local-certificate detail command to display information about the certificates loaded in a device.

Group IKE ID Configuration on the Hub

The group IKE ID feature allows a number of spoke devices to share an IKE configuration on the hub. The certificate holder’s identification, in the subject or alternate subject fields in each spoke’s X.509 certificate, must contain a part that is common to all spokes; the common part of the certificate identification is specified for the IKE configuration on the hub.

For example, the IKE ID juniper.net can be configured on the hub to identify spokes with the hostnames host1.juniper.net, host2.juniper.net, and host3.juniper.net. The certificate on each spoke must contain a hostname identity in the alternate subject field withjuniper.net in the right-most part of the field; for example, host1.juniper.net. All spokes use this hostname identity in their IKE ID payload. During IKE negotiation, the

IKE ID from a spoke is used to match the common part of the peer IKE identity configuredon the hub. A valid certificate authenticates the spoke.

The common part of the certificate identification can be one of the following:

- A partial hostname in the right-most part of the alternate subject field of the certificate for example juniper.net.
- A partial e-mail address in the right-most part of the alternate subject field of the certificate, for example@juniper.net.

A container string, a set of wildcards, or both to match the subject fields of the certificate. The subject fields contain details of the digital certificate holder in Abstract Syntax Notation One (ASN.1) distinguished name (DN) format. Fields can include organization, organizational unit, country, locality, or common name.

To configure a group IKE ID to match subject fields in certificates, you can specify the following types of identity matches:

- **Container**—The hub authenticates the spoke's IKE ID if the subject fields of the spoke's certificate exactly match the values configured on the hub. Multiple entries can be specified for each subject field (for example, ou=eng,ou=sw). The order of values in the fields must match.
- **Wildcard**—The hub authenticates the spoke's IKE ID if the subject fields of the spoke's certificate match the values configured on the hub. The wildcard match supports only one value per field (for example, ou=eng or ou=sw but not ou=eng,ou=sw). The order of the fields is inconsequential.

Multicast Feature Detail

IP Multicast allows a single IP data stream to be replicated by the infrastructure (routers and switches) and sent from a single source to multiple receivers. IP Multicast is much more efficient than multiple individual unicast streams or a broadcast stream that would propagate everywhere.

To receive a particular IP Multicast data stream, end hosts must join a multicast group by sending an Internet Group Management Protocol (IGMP) message to their local multicast router. In a traditional IP Multicast design,

the local router consults another router in the network that is acting as a rendezvous point (RP) to map the receivers to active sources so that they can join their streams.

Multicast Applications

- File Distribution/Caching
- Voice/Video (IP TV, VoIP MOH)
- Push Media
- Announcements
- Monitoring
- Chat

Benefit of Multicast Applications through Tunnels

- Multicast Replication Requires Multicast IP Network
- Issue: Many IP Networks Not Multicast Aware
- IPSec Tunnels
- Makes Unicast Transit Network Behave like Multicast Transit
- Single Hop for Multicast Traffic

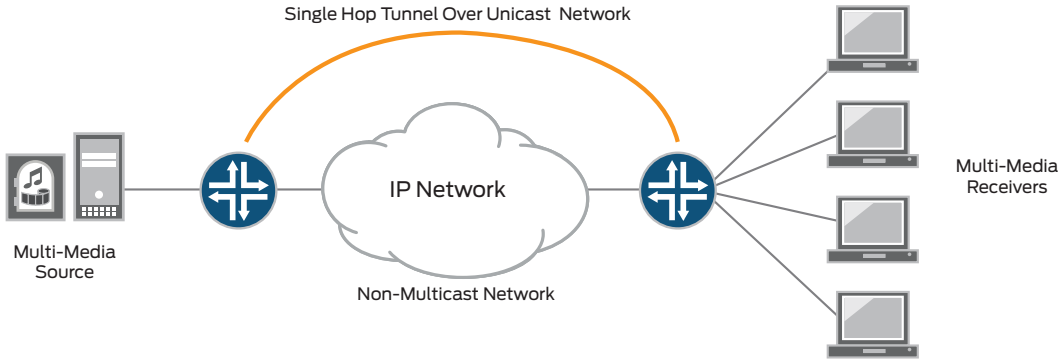

Figure 2: Auto VPN Multicast replication over Non-Multicast Network

In this App-note, which is based on sparse mode multi cast operation. Static RP is configure on HUB.. One of the key benefit of multicast over IPSEC tunnel is , it will makes unicast transit network behave like multicast transit.

Auto VPN replicate multicast stream using secure point to multipoint tunnel interfaces to host or location who express their interest in specific multicast groups through IGMP join request .as shown in figure “3” where only Marketing receive multicast stream.

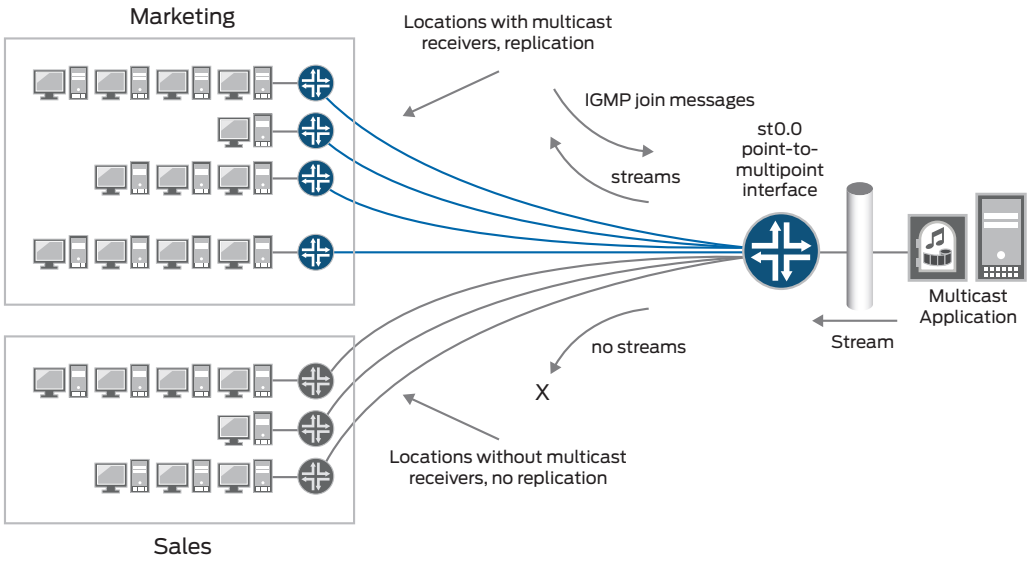

Figure 3: Auto VPN Multicast replication to only interested host

Multicast Protocols

- Internet Group Management Protocol (IGMP)
  - Layer 2: Hosts and Routers to Establish Multicast Group Membership
- Protocol Independent Multicast (PIM)
  - Layer 3: Between Routers to Direct Traffic to LAN Segments Where Multicast Group Receivers are Located
  - Sparse Mode: Rendezvous Point Used for Shared Tree per Group with Explicit Join
  - Requires Underlying IGP
    - RIP/OSPF/BGP

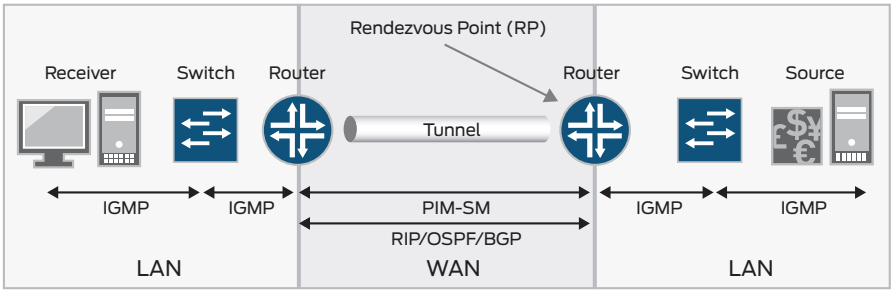

Figure 4: Auto VPN Multicast routing

Configure Auto VPN IP Multicast

This procedure includes steps for completing the IP Multicast configuration for Auto VPN.

Step 1: Configure PIM on L3 interfaces including tunnel interface in Auto VPN Hub.

Configure sparse-mode for IP Multicast on all layer3 interfaces, including tunnel interface.

```
set protocols pim interface ge-0/0/3
set protocols pim interface lo0.0
set protocols pim interface st0 mode sparse
set protocols pim interface st0 priority 100
set protocols pim interface st0 p2mp
set protocols pim graceful-restart restart-duration 60
```

Step 2: Configure PIM RP in Auto VPN Hub

```
set protocols pim rp local address 66.1.1.1
```

Step 3: Configure PIM on L3 interfaces including tunnel interface in Auto VPN Spoke1.

```
Configure sparse-mode for IP Multicast on all layer3 interfaces, including tunnel
interface
set protocols pim rp static address 66.1.1.1
set protocols pim interface fe-0/0/4.0
set protocols pim interface lo0.0
set protocols pim interface st0.1
```

Step 4: Configure IGMP on L3 interfaces receiving host request in Auto VPN Spoke1.

```
set protocols igmp interface fe-0/0/4.0
```

Step 5: Configure PIM on L3 interfaces including tunnel interface in Auto VPN Spoke2.

```
Configure sparse-mode for IP Multicast on all layer3 interfaces, including tunnel
interface
set protocols pim rp static address 66.1.1.1
set protocols pim interface fe-0/0/4.0
set protocols pim interface lo0.0
set protocols pim interface st0.1
```

Step 6: Configure IGMP on L3 interfaces receiving host request in Auto VPN Spoke2.

```
set protocols igmp interface fe-0/0/4.0
```

Additional Design Considerations

- The design in this application note uses a dual-hub approach; one hub is running in high availability (HA) and the other in stand-alone to demonstrate the possibilities of a more flexible design.
- The AutoVPN hubs use a common IKE gateway, a common VPN, and a common point-to-multipoint interface to service requests from all spokes.
- The AutoVPN hubs employ an ike-user-type of group-ike-id and wildcard matching policy for the peer's X.509v3 distinguished name (DN).
- The AutoVPN hubs do not employ additional virtual routers; all routing occurs within the inet.0 routing table.
- The AutoVPN hubs use iBGP to peer with spoke to exchange routing information. Each AutoVPN hub acts as a BGP route reflector, allowing prefixes learned from other spokes to be advertised without requiring a fully meshed design.

- The AutoVPN spoke uses two IKE gateways, two VPNs, and two point-to-multipoint interfaces to create tunnels to the hub devices (one for each).
- The AutoVPN spoke employs an ike-user-type of group-ike-id and container matching policy for the peer's X.509v3 DN.
- The AutoVPN spoke employs a virtual router when prefixes from both VPNs are used.
- The AutoVPN spoke uses iBGP to peer both hubs to exchange routing information.

Description and Deployment Scenario

BGP is a routing protocol used in Internet core routers. It works by maintaining a table of IP networks that designate network reachability. BGP does not use traditional interior gateway protocol (IGP) metrics, but makes routing decisions based on path, network policies, and/or preconfigured weights. In this document, BGP implementations propagate routing information with the aid of a route reflector.

The BGP routing topology shown in Figure 2 (stand-alone hub) and Figure 3 (HA hub) uses a route reflector to concentrate all BGP sessions. By using a route reflector, each VPN spoke only needs a single BGP session to each (as opposed to one BGP session to each of the spokes). This means that each spoke will have one BGP session to a route reflector independent of the IPsec tunnel topology.

The group IKE ID feature allows a number of spoke devices to share an IKE configuration on the hub. The certificate holder's identification, in the subject or alternate subject fields in each spoke's X.509 certificate, must contain a part that is common to all spokes, with the common part of the certificate identification specified for the IKE configuration on the hub.

The common part of the certificate identification can be one of the following:

- A partial hostname in the right most part of the alternate subject field of the certificate, for example, juniper.net.
- A partial e-mail address in the right most part of the alternate subject field of the certificate, for example, @juniper.net.
- A container string, a set of wildcards, or both to match the subject fields of the certificate. The subject fields contain details of the digital certificate holder in Abstract Syntax Notation One (ASN.1) DN format. Fields can include organization, organizational unit, country, locality, or common name.

To configure an IKE ID group to match subject fields in certificates, you can specify the following types of identity matches:

- **Container**: The hub authenticates the spoke's IKE ID if the subject fields of the spoke's certificate exactly match the values configured on the hub. Multiple entries can be specified for each subject field (for example, ou=eng,ou=sw). The order of values in the fields must match.
- **Wildcard**: The hub authenticates the spoke's IKE ID if the subject fields of the spoke's certificate match the values configured on the hub. The wildcard match supports only one value per field (for example, ou=eng or ou=sw but not ou=eng,ou=sw). The order of the fields is inconsequential.

AutoVPN iBGP Implementation with Stand-Alone Hub

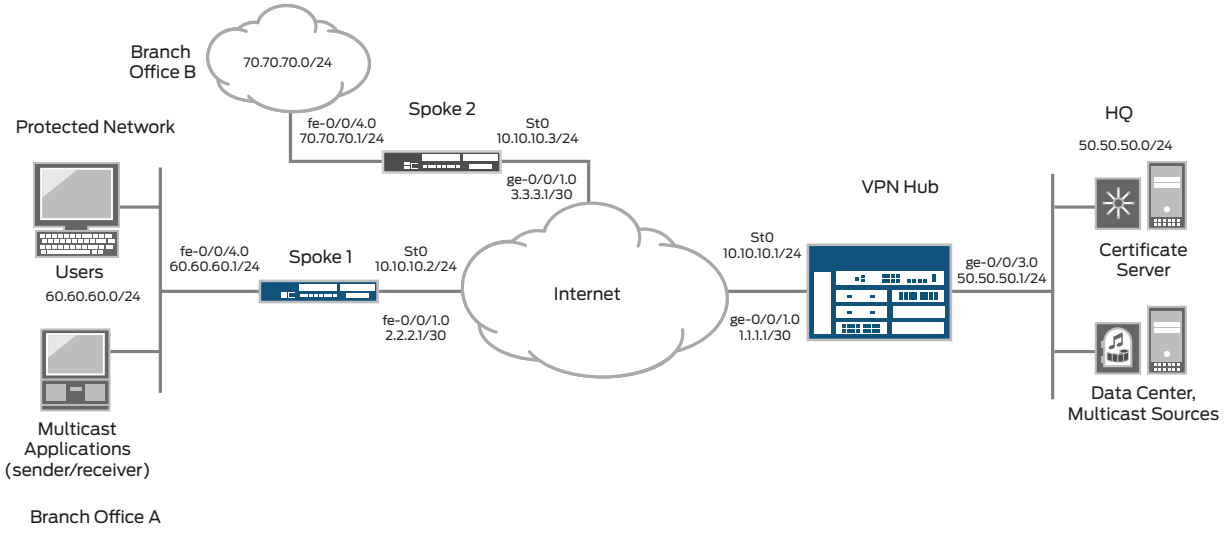

Figure 5: AutoVPN topology with stand-alone hub

- HQ LAN: 50.50.50.0/24; Branch A LAN: 60.60.60.0/24; Branch B LAN: 70.70.70.0/24
- HQ uses VPN hub, which is connected to the Internet with a single link ge-0/0/1.0 and IP address 1.1.1.1 connecting its LAN to branch "A" LAN and branch "B" LAN.
- The branch office "A" uses Spoke1, which is connected to the Internet with a single link fe-0/0/1.0 and IP address 2.2.2.1 connecting its LAN to HQ LAN and branch "B" LAN.
- The branch office "B" uses Spoke2, which is connected to the Internet with single link fe-0/0/4.0 and IP address 3.3.3.1 connecting its LAN to HQ LAN and branch "A" LAN.
- HQ has an IPsec tunnel configured to Spoke1 and Spoke2, and IBGP is configured over IPsec.
- Container is used to match the subject field in certificates (ou=sales,ou=customerA).

Stand-Alone Hub Configuration

```
set interfaces ge-0/0/1 unit 0 family inet address 1.1.1.1/30
set interfaces ge-0/0/3 unit 0 family inet address 50.50.50.1/24
set interfaces lo0 unit 0 family inet address 66.1.1.1/24
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.10.10.1/24
set policy-options policy-statement lan_nw from interface ge-0/0/3.0
set policy-options policy-statement lan_nw then accept
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.10.10.1
set protocols bgp group ibgp export lan_nw
set protocols bgp group ibgp cluster 1.2.3.4
set protocols bgp group ibgp peer-as 10
set protocols bgp group ibgp allow 10.10.10.0/24
set policy-options policy-statement adv_bgp_rt from protocol bgp
set policy-options policy-statement adv_bgp_rt then next-hop self
set policy-options policy-statement adv_bgp_rt then accept
set protocols bgp group ibgp export adv_bgp_rt
set routing-options static route 2.2.2.0/30 next-hop 1.1.1.2
set routing-options static route 3.3.3.0/30 next-hop 1.1.1.2
set routing-options autonomous-system 10
set protocols pim rp local address 66.1.1.1
set protocols pim interface ge-0/0/3
set protocols pim interface lo0.0
set protocols pim interface st0 mode sparse
set protocols pim interface st0 priority 100
set protocols pim interface st0 p2mp
set protocols pim graceful-restart restart-duration 60
set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy1 mode main
set security ike policy ike-policy1 proposals ike-proposal
set security ike policy ike-policy1 certificate local-certificate Local1
set security ike gateway hub-to-spoke-gw ike-policy ike-policy1
set security ike gateway hub-to-spoke-gw dynamic distinguished-name wildcard
OU=sales, O=customerA
set security ike gateway hub-to-spoke-gw dynamic ike-user-type group-ike-id
set security ike gateway hub-to-spoke-gw local-identity distinguished-name
set security ike gateway hub-to-spoke-gw external-interface ge-0/0/1.0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy1 proposals ipsec-proposal
set security ipsec vpn hub-to-spoke-vpn bind-interface st0.0
```

```
set security ipsec vpn hub-to-spoke-vpn ike gateway hub-to-spoke-gw
set security ipsec vpn hub-to-spoke-vpn ike ipsec-policy vpn-policy1
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces st0.0
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/3.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url
http://systest-pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable
```

Spoke1 Configuration

```
set interfaces fe-0/0/1 unit 0 family inet address 2.2.2.1/30
set interfaces fe-0/0/4 unit 0 family inet address 60.60.60.1/24
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.10.10.2/24
set policy-options policy-statement lan_nw from interface fe-0/0/4.0
set policy-options policy-statement lan_nw then accept
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.10.10.2
set protocols bgp group ibgp export lan_nw
set protocols bgp group ibgp neighbor 10.10.10.1
set routing-options static route 1.1.1.0/30 next-hop 2.2.2.2
set routing-options autonomous-system 10
set protocols igmp interface fe-0/0/4.0
set protocols pim rp static address 66.1.1.1
set protocols pim interface fe-0/0/4.0
set protocols pim interface lo0.0
set protocols pim interface st0.1

set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy1 mode main
set security ike policy ike-policy1 proposals ike-proposal
set security ike policy ike-policy1 certificate local-certificate Local1
set security ike gateway spoke-to-hub-gw ike-policy ike-policy1
set security ike gateway spoke-to-hub-gw address 1.1.1.1
set security ike gateway spoke-to-hub-gw local-identity distinguished-name
set security ike gateway spoke-to-hub-gw remote-identity distinguished-name
set security ike gateway spoke-to-hub-gw external-interface fe-0/0/1.0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy1 proposals ipsec-proposal
set security ipsec vpn spoke-to-hub bind-interface st0.0
set security ipsec vpn spoke-to-hub ike gateway spoke-to-hub-gw
set security ipsec vpn spoke-to-hub ike ipsec-policy vpn-policy1
set security ipsec vpn spoke-to-hub establish-tunnels immediately
```

```
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces fe-0/0/1.0
set security zones security-zone untrust interfaces st0.0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces fe-0/0/4.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url
http://systest-pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable
```

Spoke2 Configuration

```
set interfaces ge-0/0/1 unit 0 family inet address 3.3.3.1/30
set interfaces fe-0/0/4 unit 0 family inet address 70.70.70.1/24
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.10.10.3/24
set policy-options policy-statement lan_nw from interface fe-0/0/4.0
set policy-options policy-statement lan_nw then accept
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.10.10.3
set protocols bgp group ibgp export lan_nw
set protocols bgp group ibgp neighbor 10.10.10.1
set routing-options static route 1.1.1.0/30 next-hop 3.3.3.2
set routing-options autonomous-system 10
set protocols igmp interface fe-0/0/4.0
set protocols pim rp static address 66.1.1.1
set protocols pim interface fe-0/0/4.0
set protocols pim interface lo0.0
set protocols pim interface st0.1
set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy1 mode main
set security ike policy ike-policy1 proposals ike-proposal
set security ike policy ike-policy1 certificate local-certificate Local1
set security ike gateway spoke-to-hub-gw ike-policy ike-policy1
set security ike gateway spoke-to-hub-gw address 1.1.1.1
set security ike gateway spoke-to-hub-gw local-identity distinguished-name
set security ike gateway spoke-to-hub-gw remote-identity distinguished-name
set security ike gateway spoke-to-hub-gw external-interface ge-0/0/1.0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy1 proposals ipsec-proposal
set security ipsec vpn spoke-to-hub bind-interface st0.0
set security ipsec vpn spoke-to-hub ike gateway spoke-to-hub-gw
set security ipsec vpn spoke-to-hub ike ipsec-policy vpn-policy1
set security ipsec vpn spoke-to-hub establish-tunnels immediately
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces ge-0/0/1.0
set security zones security-zone untrust interfaces st0.0
```

```
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
set security zones security-zone trust interfaces fe-0/0/4.0
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url
http://systest-pc4/certsrv/mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable
```

AutoVPN iBGP Implementation with Stand-Alone HA Hub

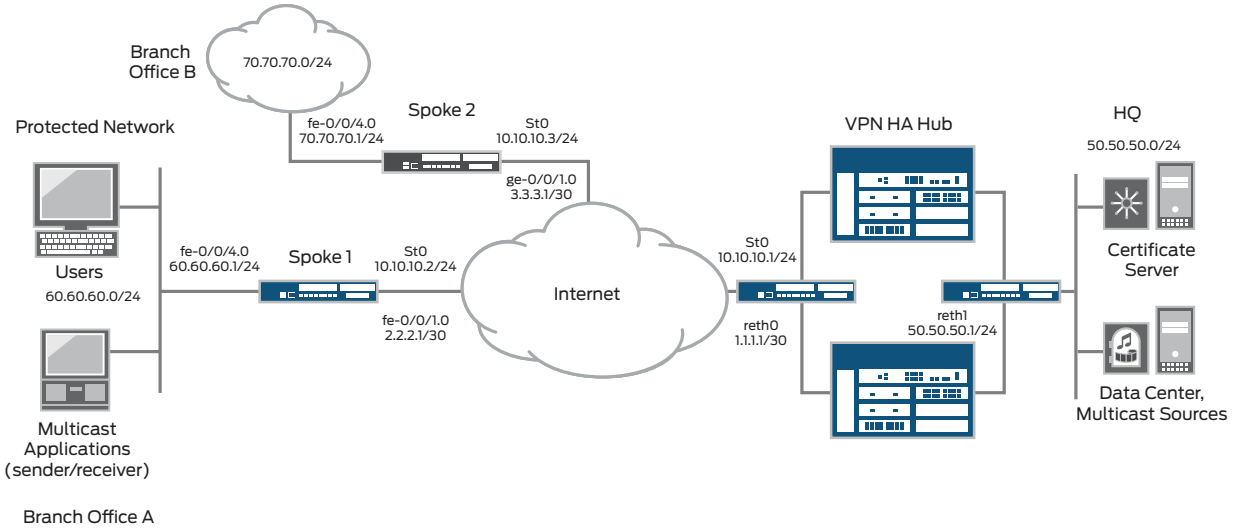

Figure 6: AutoVPN topology with HA hub

HA Hub Configuration

```
set interfaces fab0 fabric-options member-interfaces ge-11/3/0
set interfaces fab1 fabric-options member-interfaces ge-23/3/0
set groups node0
set groups node1
set groups node0 system host-name HA-Hub-Node0
set groups node0 interfaces fxp0 unit 0 family inet address 10.3.5.1/24
set groups node0 system backup-router 10.3.5.254 destination 0.0.0.0/0
set groups node1 system host-name HA-Hub-Node1
set groups node1 interfaces fxp0 unit 0 family inet address 10.3.5.2/24
set groups node1 system backup-router 10.3.5.254 destination 0.0.0.0/0
set apply-groups ${node}
set chassis cluster reth-count 2
set chassis cluster redundancy-group 0 node 0 priority 129
set chassis cluster redundancy-group 0 node 1 priority 128
set chassis cluster redundancy-group 1 node 0 priority 129
set chassis cluster redundancy-group 1 node 1 priority 128
set interfaces ge-0/0/1 gigether-options redundant-parent reth0
set interfaces ge-0/0/3 gigether-options redundant-parent reth1
set interfaces ge-12/0/0 gigether-options redundant-parent reth0
set interfaces ge-12/0/3 gigether-options redundant-parent reth1
set interfaces lo0 unit 0 family inet address 66.1.1.1/24
set interfaces lo0 redundant-pseudo-interface-options redundancy-group 1
set interfaces reth0 redundant-ether-options redundancy-group 1
set interfaces reth0 unit 0 family inet address 1.1.1.1/30
```

```
set interfaces reth1 redundant-ether-options redundancy-group 1
set interfaces reth1 unit 0 family inet address 50.50.50.0/24
set security zones security-zone untrust interfaces reth0.0
set security zones security-zone trust interfaces reth1.0
set interfaces st0 unit 0 multipoint
set interfaces st0 unit 0 family inet address 10.10.10.1/24
set policy-options policy-statement lan_nw from interface reth1.0
set policy-options policy-statement lan_nw then accept
set protocols bgp group ibgp type internal
set protocols bgp group ibgp local-address 10.10.10.1
set protocols bgp group ibgp export lan_nw
set protocols bgp group ibgp cluster 1.2.3.4
set protocols bgp group ibgp peer-as 10
set protocols bgp group ibgp allow 10.10.10.0/24
set policy-options policy-statement adv_bgp_rt from protocol bgp
set policy-options policy-statement adv_bgp_rt then next-hop self
set policy-options policy-statement adv_bgp_rt then accept
set protocols bgp group ibgp export adv_bgp_rt

set routing-options static route 2.2.2.0/30 next-hop 1.1.1.2
set routing-options static route 3.3.3.0/30 next-hop 1.1.1.2
set routing-options autonomous-system 10
set routing-options graceful-restart
set protocols pim rp local address 66.1.1.1
set protocols pim interface reth1
set protocols pim interface lo0.0
set protocols pim interface st0 mode sparse
set protocols pim interface st0 priority 100
set protocols pim interface st0 p2mp
set protocols pim graceful-restart restart-duration 60
set security ike proposal ike-proposal authentication-method rsa-signatures
set security ike proposal ike-proposal dh-group group2
set security ike proposal ike-proposal authentication-algorithm sha1
set security ike proposal ike-proposal encryption-algorithm aes-128-cbc
set security ike policy ike-policy1 mode main
set security ike policy ike-policy1 proposals ike-proposal
set security ike policy ike-policy1 certificate local-certificate Local1
set security ike gateway hub-to-spoke-gw ike-policy ike-policy1
set security ike gateway hub-to-spoke-gw dynamic distinguished-name wildcard
OU=sales, O=customerA
set security ike gateway hub-to-spoke-gw dynamic ike-user-type group-ike-id
set security ike gateway hub-to-spoke-gw local-identity distinguished-name
set security ike gateway hub-to-spoke-gw external-interface reth0
set security ipsec proposal ipsec-proposal protocol esp
set security ipsec proposal ipsec-proposal authentication-algorithm hmac-md5-96
set security ipsec proposal ipsec-proposal encryption-algorithm des-cbc
set security ipsec policy vpn-policy1 perfect-forward-secrecy keys group14
set security ipsec policy vpn-policy1 proposals ipsec-proposal
set security ipsec vpn hub-to-spoke-vpn bind-interface st0.0
set security ipsec vpn hub-to-spoke-vpn ike gateway hub-to-spoke-gw
set security ipsec vpn hub-to-spoke-vpn ike ipsec-policy vpn-policy1
set security zones security-zone untrust host-inbound-traffic system-services all
set security zones security-zone untrust host-inbound-traffic protocols all
set security zones security-zone untrust interfaces st0.0
set security zones security-zone untrust interfaces reth0
set security zones security-zone trust host-inbound-traffic system-services all
set security zones security-zone trust host-inbound-traffic protocols all
```

```
set security zones security-zone trust interfaces reth1
set security policies default-policy permit-all
set security pki ca-profile ca-profile1 ca-identity ca-profile1
set security pki ca-profile ca-profile1 enrollment url http://systest-pc4/certsrv/
mscep/mscep.dll
set security pki ca-profile ca-profile1 revocation-check disable
```

Spoke2 Configuration
Same as above

Spoke3 Configuration
Same as above

Summary

AutoVPN allows network administrators to configure a hub for current and future spokes. No configuration changes are required on the hub when spoke devices are added or deleted, thus allowing administrators flexibility in managing large-scale network deployments. AutoVPN offers easy, no touch deployment that ensures maximum network and security uptime for businesses of any size. The main advantages of using iBGP for a routing protocol are that it can accommodate multiple devices and can scale to a large number of remote offices (between 1,000 and 5,000 locations).

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net**.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: 31.0.207.125.700
Fax: 31.0.207.125.701

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

3500214-001-EN June 2013 Printed on recycled paper