

Configuring Dynamic VPN v2.1 (last updated 1/2011)

Junos 10.4 and above

Configuring and deploying Dynamic VPNs (remote access VPNs) using SRX service gateways



Introduction

Remote access VPNs, sometimes called dialup VPNs, have been supported in ScreenOS and Junos devices for some time. However, traditional remote access VPNs require client software in order to establish the VPN and so installing and distributing the client software to all remote devices becomes a challenge.

The dynamic VPN feature available on SRX devices allows administrators to provide IPSec access to an SRX gateway while providing a simple way to distribute the client software through the use of a web portal.

Note: This Application Note applies to SRX Branch devices running Junos 10.4 or later. The configuration has improved and changed significantly from earlier versions of Junos. If your SRX Branch device is running Junos 10.3 or earlier, then refer to the other Application Note in <http://kb.juniper.net/InfoCenter/index?page=content&id=TN7>. For the list of improvements, refer to the Junos 10.4 Release Note.

Scope

The purpose of this application note is to provide dynamic VPN configuration examples and some common deployment scenarios.

Design Considerations

Branch SRX gateways can be deployed in standalone or redundant configurations. Through this application note we assume a standalone device is used to terminate the VPN, however the same concepts apply to clustered devices.

Hardware Requirements

- Branch Juniper Networks SRX Series Services Gateways (SRX1xx, SRX2xx and SRX6xx)

Software Requirements

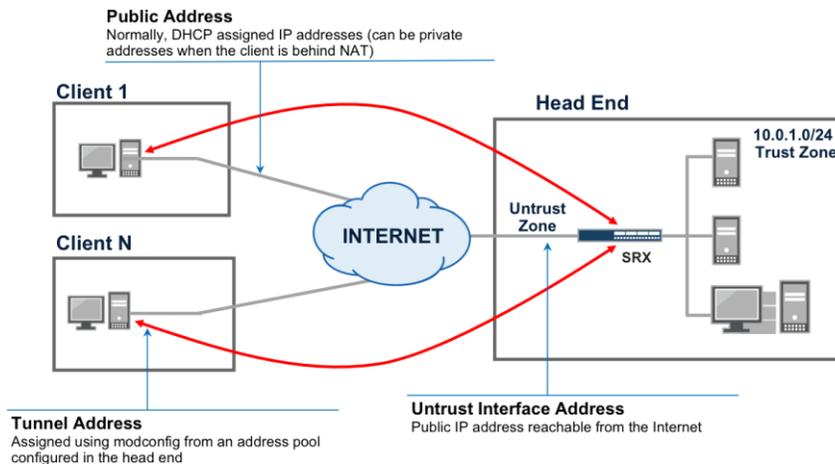
- JUNOS Software release 10.4r1 or later

Client Software Requirements

- Windows XP, Vista or Windows 7

Common Deployment Scenario

The most common deployment scenario is to provide VPN access to remote clients connected through a public network (Internet). A public IP address is assigned to one of the gateway's interface (normally the untrust interface). Remote clients can access the VPN Portal and, after being authenticated, they can download and install the VPN client.



Let's assume the untrust zone in the SRX at the headend is connected to the Internet, with a public static IP (It could also be connected through NAT, as long as the interface connected to the untrust zone is reachable). For this example, assume the untrust interface is configured with the 198.0.0.1 address.

The process for a client to access the VPN is as follows:

1. A client trying to access the VPN contacts the authentication portal, by establishing an http(s) connection to the interface configured to terminate the tunnels (in this example, doing an <https://198.0.0.1>)
2. The client will be redirected to the authentication portal, after which it will be prompted for his/her user credentials

JUNIPER
NETWORKS

USER AUTHENTICATION

User Login

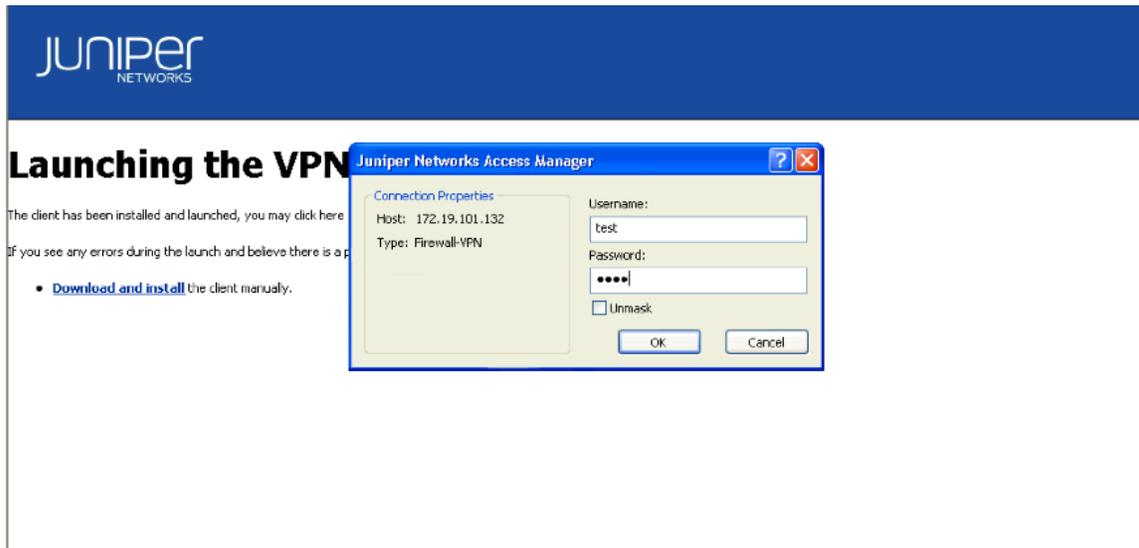
Username:

Password:

Copyright © 2010, Juniper Networks, Inc. [All Rights Reserved.](#) [Trademark Notice.](#) [Privacy.](#)

3. After successful authentication, the server will determine if the VPN software is installed in the client's machine. The server will also make sure the software version installed in the client's machine is the latest.
4. If the client has no VPN software installed, or it has an old version, a new software push will be initiated after which the software will be installed.

5. The VPN software is launched and a new authentication occurs. If this authentication process is successful the client downloads the latest configuration options from the server (this way the client always has the latest



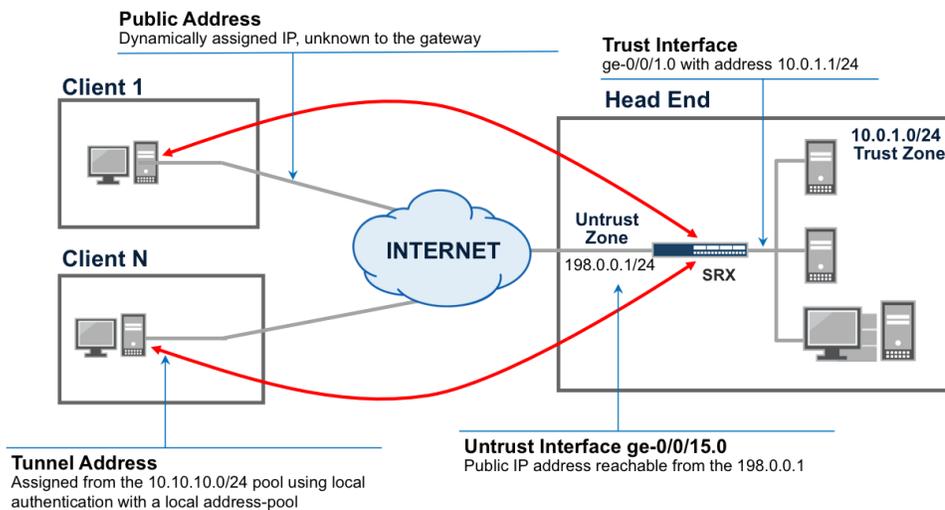
configuration at the time it attempts to build a tunnel)

6. A tunnel is established, a new authentication is performed, and an IP address is assigned to the VPN client (which could be allocated from a local address pool or an external radius server) after which traffic is allowed through the tunnel. This second authentication phase is done as part of the tunnel setup, using IPSec extended authentication (xauth).

After the VPN software has been installed, the users can access the VPN by either logging in to the portal or by launching the VPN software directly. In both cases the VPN client will authenticate with the SRX and download the latest available configuration for that user.

Configuration

For this scenario we will also assume that the client authentication and address assignments are done locally, without the use of an external radius server.



The configuration can be divided into three sections:

1. Configuring the VPN tunnel
2. Configuring the authentication and IP address assignment parameters
3. Associating VPNs users with dynamic-vpn configurations

Note: There is also an important note about the HTTPS daemon at the end of step 3.

The following sections explain the different configuration options for each of these steps.

1. Configuring the VPN tunnel

VPN tunnels are configured in the same way as traditional IPsec VPN tunnels; however, due to the specific requirements of this type of VPNs, not all IPsec VPN options are supported. In particular:

- Tunnels must be configured with extended authentication (XAUTH). Xauth is required in order to obtain username/password information during the IPsec negotiation and to be able to push an IP address (an optional DNS/WINS server addresses) to the client.
- Only policy-based VPNs are supported
- Traffic allowed from the VPN can be controlled by pushing some routes to the client, as part as the client's configuration. Because the VPN client only supports any/any proxy-ids, which are derived from the security policies used to map the traffic to one of the tunnels. The security policy that is used for remote access clients must permit all traffic.
- Only pre-shared keys are supported for phase I authentication. However, since these VPNs use xauth authentication, in most deployments it is possible to use the same pre-shared key for all the remote clients. Of course, each client/user will have different username/passwords assigned to use during the extended authentication phase.
- It is possible to configure a single VPN that is shared by all remote clients by using either shared or group IKE IDs. When a single VPN is shared, the total number of simultaneous connections to the gateway cannot be larger than the number of dynamic-vpn licenses installed. That is, when configuring a shared/group IKE ID gateway, it is possible to configure the max number of connections to be larger than the number of installed dynamic-vpn licenses. However, if at any given time a new connection attempt is made that would result in a number of concurrent connections greater than what is allowed by the license, the connection will be denied.

We are now in a position to configure an IPSec VPN to be used for a dynamic-vpn access. In order to simplify the configuration we will make use of pre-defined proposals for both phase I and phase II negotiations.

```
#Define the IKE gateway

#Use aggressive mode
set security ike policy ike-dyn-vpn-policy mode aggressive
set security ike policy ike-dyn-vpn-policy proposal-set standard

#Use pre-shared keys
set security ike policy ike-dyn-vpn-policy pre-shared-key ascii-text "$9$KHxWXNs2aikPdbkP5Q9CKM8"

set security ike gateway dyn-vpn-local-gw ike-policy ike-dyn-vpn-policy

#Using group-ike IDs
#Each client will have its own IKE-ID, which is derived from the username and group ID (dynvpn)
set security ike gateway dyn-vpn-local-gw dynamic hostname dynvpn
set security ike gateway dyn-vpn-local-gw dynamic ike-user-type group-ike-id

#The connection limit should not be larger than the number of installed licenses
set security ike gateway dyn-vpn-local-gw dynamic connections-limit 10

#Specify the interface to listen for connections
#This is important both for IKE and also for the authentication portal
set security ike gateway dyn-vpn-local-gw external-interface ge-0/0/15.0

#Xauth profile determines how to authenticate the user, assign addresses and access parameters
set security ike gateway dyn-vpn-local-gw xauth access-profile dyn-vpn-access-profile

#Define the IPSEC vpn
set security ipsec policy ipsec-dyn-vpn-policy proposal-set standard
set security ipsec vpn dyn-vpn ike gateway dyn-vpn-local-gw
set security ipsec vpn dyn-vpn ike ipsec-policy ipsec-dyn-vpn-policy
```

The security zone hosting the interfaces used to terminate the dynamic VPN need to allow IKE and HTTPS host-inbound traffic. (IKE and HTTPS are required at a minimum.)

```
set security zones security-zone untrust interfaces ge-0/0/15.0 host-inbound-traffic system-services ike
set security zones security-zone untrust interfaces ge-0/0/15.0 host-inbound-traffic system-services https
set security zones security-zone untrust interfaces ge-0/0/15.0 host-inbound-traffic system-services ping
set security zones security-zone untrust interfaces ge-0/0/15.0 host-inbound-traffic system-services ssh
```

NOTE: Keep in mind that the commands specified above may interfere with what is currently configured on your SRX device. Interface options take precedence over zone options. Therefore, adding configuration under the interface will override whatever is configured under the zone

Remote access tunnels are supported only using policy-based VPNs, we therefore need to configure a security policy allowing encrypted traffic from the clients which, in the deployment scenario described in this application note, comes from the untrust zone to the trust networks.

NOTE: Placement of this VPN security policy is **important**. It needs to be placed above more specific non-VPN policies so that traffic that is intended to be sent over the VPN is processed correctly.

```
set security policies from-zone untrust to-zone trust policy dyn-vpn-policy match source-address any
set security policies from-zone untrust to-zone trust policy dyn-vpn-policy match destination-address any
set security policies from-zone untrust to-zone trust policy dyn-vpn-policy match application any
#Note how the policy allows traffic only from the dyn-vpn IPSec vpn.
set security policies from-zone untrust to-zone trust policy dyn-vpn-policy then permit tunnel ipsec-vpn dyn-vpn
```

2. Configuring the authentication and IP address assignment parameters

The authentication parameters are configured under an access profile. Given the different places where authentication can occur, the profile is referenced under the ipsec vpn configuration (as can be seen in the previous section), the dynamic-vpn stanza and the firewall authentication.

```
#dyn-vpn-access-profile definition used for xauth, firewall-auth and dynamic-vpn

#This access profile has the following clients
set access profile dyn-vpn-access-profile client test firewall-user password "$9$uY4o0EyMWxdwgX7"
set access profile dyn-vpn-access-profile client user1 firewall-user password "$9$uY4o0EyMWxdwgX7"
set access profile dyn-vpn-access-profile client user2 firewall-user password "$9$uY4o0EyMWxdwgX7"

#This access profile uses local authentication and address assignment by pointing to a local address pool
set access profile dyn-vpn-access-profile address-assignment pool dyn-vpn-address-pool
set access address-assignment pool dyn-vpn-address-pool family inet network 10.10.10.0/24
set access address-assignment pool dyn-vpn-address-pool family inet range dvpn-range low 10.10.10.10
set access address-assignment pool dyn-vpn-address-pool family inet range dvpn-range high 10.10.10.20
set access address-assignment pool dyn-vpn-address-pool family inet xauth-attributes primary-dns 4.2.2.2/32

#Finally note how the access profile is used for web-auth (for the dynamic-vpn portal).
set access firewall-authentication web-authentication default-profile dyn-vpn-access-profile
```

Please note how the access profile is used for xauth and firewall authentication. To be precise, any authentication profile can be used for firewall auth, and it does not have to be the same used for dynamic-vpn access. However, if no access profile is configured for firewall-authentication, the authentication portal will not be enabled.

Lastly for this step, it is worth mentioning that the address pool could belong to a subnet directly connected to the SRX. As an example, consider the network diagram in figure I. If we were to choose an IP pool within the 10.0.1.0/24 subnet, say the 10.0.1.10 to 10.0.1.20, the SRX would have to respond to ARP requests to the addresses in the pool from machines in the Trust zone. This can be achieved by configuring proxy-arp as shown below, and it is only needed if the configured pool belongs to one of the subnets of the interfaces directly connected to the SRX. Of course, if these addresses do not belong to the addresses of a directly connected interfaces, other devices in the network will need a route pointing to this pool, in order to reach the client machines behind the tunnel.

```
#Assuming the ge-0/0/1.0 interface is connected to the trust network, and that the IP pool used for config mode
#is included in this interface's subnet
set security nat proxy-arp interface ge-0/0/1.0 address 10.0.1.10 to 10.0.1.20
```

3. Associating VPNs users with dynamic-vpn configurations

At this point we have the IPsec VPN configuration we want to use for the dynamic-vpn tunnels and we have created an access profile that is used for IPsec extended authentication (xauth). Every time a user attempts to establish a dynamic-VPN connection to an SRX, the latest available configuration is pushed to the client. In order to do this, there must be a way to associate IPsec VPN configurations with client names.

This last configuration example shows precisely how to do this, by declaring the authentication profile to be used with the dynamic-vpn portal, and the list of clients using a particular IPsec VPN configuration.

```
#Specify the authentication profile used for the dyn-vpn portal
#This profile should be the same as the one used for xauth
set security dynamic-vpn access-profile dyn-vpn-access-profile

#Specify a list of clients, with the ipsec vpn used
set security dynamic-vpn clients all ipsec-vpn dyn-vpn
set security dynamic-vpn clients all user test
set security dynamic-vpn clients all user user1
set security dynamic-vpn clients all user user2

#It is also possible to define the set of resources that will be accessible through the tunnel.
#Destinations matching any of the configured remote-protected-resources will be sent through the tunnel
set security dynamic-vpn clients all remote-protected-resources 10.0.0.0/8
#Destinations matching the exceptions will not be tunneled and will be sent out in cleat text
set security dynamic-vpn clients all remote-exceptions 0.0.0.0/0
```

As part of the dynamic-vpn profile, it is necessary to configure two prefix lists, the remote-protected-resources and the remote-exceptions. These lists allow administrators to configure which traffic will be sent through the IPsec tunnel and which traffic will be bypassed. Traffic to a destination matching any of the prefixes in the remote-protected resources will be sent through the tunnel, while traffic matching any of the prefixes in the remote exceptions will be sent in clear text.

IMPORTANT NOTE:

The dynamic-vpn portal requires the services of the https daemon, which can be enabled under the [system services web-management https] hierarchy. This configuration step is only required if this service is not already enabled. If this service is already enabled for J-web access, no further configuration is required. In order to enable this service only for dynamic-vpn access, without allowing for J-web access on any interface, simply configure the service without specifying any interface for J-web, as shown below:

```
# show system services web-management
https {
    system-generated-certificate;
}
```

Refer to the 'J-Web and Remote Access Portal Isolation' section for additional information.

At this point, the Dynamic VPN can connect to the SRX and access protected resources on the 10.0.0.0/8 network.

Using a Radius Server for User Authentication

If, instead of using local authentication, an external radius server is used to authenticate users and do the address assignment, the access profile must be changed to point to a radius server as shown below:

```
set access profile dyn-vpn-access-profile authentication-order radius
set access profile dyn-vpn-access-profile radius-server 172.19.101.101 secret "$9$D8H.5n/tIEyQFEylKx7jHq"
set access firewall-authentication web-authentication default-profile dyn-vpn-access-profile
```

The rest of the configuration remains unchanged, but now the radius server must pass on the IP address and other parameters assigned to the client during the IPSec negotiation. The following standard radius attributes are used for address assignment:

- Framed-IP-Address
- Framed-IP-Netmask

It is also possible to pass DNS and WINS servers to the client, using the following vendor specific attributes taken from a radius dictionary (the format is radius-specific, but it contains all the required information to define the same attributes in a radius server):

```
MACRO Juniper-VSA(t,s) 26 [vid=2636 type1=%t% len1=+2 data=%s%]

ATTRIBUTE Juniper-Primary-Dns          Juniper-VSA(31, ipaddr)  r
ATTRIBUTE Juniper-Primary-Wins         Juniper-VSA(32, ipaddr)  r
ATTRIBUTE Juniper-Secondary-Dns       Juniper-VSA(33, ipaddr)  r
ATTRIBUTE Juniper-Secondary-Wins      Juniper-VSA(34, ipaddr)  r
```

As an example, the “test” user configured before using local authentication can be configured in a free radius server by adding the following lines to the “/etc/raddb/users” file (assumes that the dictionary file includes the declaration for the Juniper-Primary-Dns attribute):

```
test  Auth-Type := Local, User-Password == "test"
      Service-Type = Login-User,
      Framed-IP-Address = 10.10.10.1,
      Framed-IP-Netmask = 255.255.255.0,
      Juniper-Primary-Dns = 4.2.2.2
```

Configuration Using the VPN Wizard

A configuration wizard has been added as part of the J-web management interface in Junos 10.4. This wizard is not meant to provide all the option available for the configuration of the remote access VPN (or Dynamic VPN) feature in the CLI, but rather to simplify the most common use-case. It is targeted for deployments that do not require radius authentication nor use multiple different VPN profiles (for example, by having different authentication/encryption parameters for different users).

The configuration using the wizard is much simpler than through the CLI, as it automates most of the provisioning. The first step is to launch the VPN wizard (found under the Wizards -> VPN Wizard menu) and select the Remote Access VPN type, as shown below:

The screenshot displays the Juniper VPN Wizard configuration interface. It is divided into two main sections.

Top Section: Select VPN Type

- Left Panel:** A list of steps: Select VPN Type (active), Remote, VPN, Remote Users, Traffic Profile, Review & Commit.
- Main Content:**
 - Select VPN Type:** A heading followed by instructions: "Select the type of VPN you wish to configure, and then click Start. You may also make changes to existing configurations." Below are two radio buttons: "Site-to-site VPN (Route based)" (unselected) and "Remote Access VPN" (selected).

Bottom Section: Remote Access VPN: Local Settings

- Left Panel:** A list of steps: Select VPN Type (checked), Local (active), VPN, Remote Users, Review & Commit.
- Main Content:**
 - Name:** A text input field labeled "VPN Name *" containing the value "wizard_dyn_vpn".
 - Protected Networks:** A section with a "Zone *" dropdown menu set to "trust". Below it is a "Network(s) *" list box containing "10.0.1.0/24". To the right of the list box are "Add" and "Remove" buttons. An example "Example: 1.2.3.0/24" is shown next to the "Add" button.
 - Public Network:** A section with an "Interface *" dropdown menu set to "ge-0/0/15.0" and an "Interface Zone *" dropdown menu set to "untrust".
- Bottom Right:** "Back" and "Next" buttons.

Additional Elements:

- About this page:** A scrollable text box on the left side of the bottom section. It explains that on this page, the user specifies the local private network and the public network through which the tunnel passes. It also notes that if a remote access VPN has been configured previously, this page can be used.
- Diagram:** A small diagram at the bottom left of the bottom section showing two blue boxes connected by a dashed line to a central cloud labeled "Internet".

The wizard provides a workflow-oriented way to configure the feature, and pre-provisions some of the values whenever possible like the VPN name, which is always "wizard_dyn_vpn". Following with our example, we want to provide access to the 10.0.1.0/24 subnet, connected to the Trust zone, while we expect the connections to be done through the ge-0/0/15.0 interface in the Untrust zone. When selecting the interface connected to the public network, the wizard will automatically show the zone the interface is bound to. If instead no zone has been assigned, a drop-down box allows users to choose a zone to bind the external interface to.

The next page allows users to modify the encryption and authentication parameters used for the VPN, along with some other VPN-related options. Because the configuration is automatically pushed to each client before they connect using a secure channel, sensible defaults are provided that will work in most situations, making this configuration step completely optional (note how this allow the wizard to pre-generate things like the pre-shared keys used for IKE, or the remote IKE identity as those values will be automatically relayed to the Remote Access VPN client).

The screenshot shows the 'Remote Access VPN: Remote User Settings' configuration page. The left sidebar indicates the progress: 'Select VPN Type' (checked), 'Local' (checked), 'VPN' (checked), and 'Remote Users' (selected). The main content area is divided into sections:

- Authentication:** A note states 'Same credentials used for Xauth and authentication for client download. At least one user must be created.' Below this is a table for user credentials:

User Name	Password
user1	*****
user2	****

 An 'Add More...' link is provided below the table.
- IP Settings:** Includes fields for 'IP Pool (for Config Mode)' (10.10.10.0/24), 'DNS Server' (IP), and 'WINS Server' (IP). A note states: 'Note: The pool settings are shared by multiple VPN's'.

At the bottom right, there are 'Back' and 'Next' buttons. A small diagram at the bottom left shows two computers connected to an 'Internet' cloud.

The next page allow us to configure the list of users allowed with their respective password, the address of the pool used to assign an IP to the users, and the addresses of the DNS and WINS server passed to them (the last two parameters are optional).

We are finally presented with a review page from which we can commit the configuration.

The screenshot shows the 'Review & Commit' page of the VPN Wizard. The left sidebar shows the progress: 'Select VPN Type' (checked), 'Local' (checked), 'VPN' (checked), 'Remote Users' (checked), and 'Review & Commit' (selected). The main content area is titled 'Review & Commit' and includes a summary of the configuration:

- VPN Name:** wizard_dyn_vpn
- Protected Networks:**
 - Zone: untrust
 - Networks: 10.0.1.0/24
- Public Network:**
 - Interface: ge-0/0/15.0
 - Interface zone: trust
- VPN settings:**
 - IKE security level: compatible
 - IKE preshared key: \$9\$7zV2aGDkqfzUDApu0IRLx7dYgDik5z3IH
 - Remote identity: Host name: srx240-2
 - Dead Peer Detection: (checkbox)
 - IPsec Security Level: compatible

At the bottom right, there are 'Back' and 'Commit' buttons. A small diagram at the bottom left shows two computers connected to an 'Internet' cloud.

J-Web and Remote Access Portal Isolation

The web management interface (J-web) and the portal used to authenticate dynamic-vpn users leverage the same http server infrastructure, configurable under the [system services web-management] hierarchy. All interfaces listed under the interface section will answer http or https requests (or both, based on the configuration).

It is possible to disable J-web access on the interfaces used for dynamic-vpn access. On releases previous to 10.4, in order to configure the dynamic-vpn feature, it was mandatory to add the ike listener interface to the list of management interfaces for https. In Junos 10.4 every interface used for dynamic-vpn access will automatically accept http and https connections to the dynamic-vpn portal. If an interface is used for dynamic-vpn access (that is, if an interface is configured under the ike listener interfaces in an IPSec VPN profile used for dynamic-vpn access) and that interface is not configured for web-management access, only access to the dynamic-vpn portal will be allowed, effectively disabling J-web access on that interface.

Since an interface can be configured for dynamic-vpn access by adding it to the ike listener interfaces, web-management access or both, access to the dynamic-vpn portal will depend on which interface a request comes from and how that interface is configured. The following table summarizes the different combinations:

Request	Dynamic-vpn access only	J-web access only	Both J-web and dynamic-vpn access enabled
HTTP(S) request to the / URL	User is redirected to the dynamic-vpn portal	User is redirected to the J-web login page	User is redirected to the dynamic-vpn portal
HTTP(S) request to the dynamic-vpn URL	Dynamic VPN portal is shown	Page Not Found is returned	User is redirected to the dynamic-vpn portal
HTTP(S) request to the management-url	Page Not Found is returned	User is redirected to the J-web login page	User is redirected to the J-web login page

The management-url configuration option can be used to specify the URL used to access the management interface (J-web) when a particular interface is used both for dynamic vpn and management. By default, a request arriving from an interface enabled both for dynamic-vpn and J-web will be redirected to the dynamic-vpn portal. When the management-url is configured, a request to http(s)://<interface-address>/<management-url> will, instead, present the management interface.

Monitoring

Dynamic-vpn clients use IPSec tunnels and, therefore, can be monitored using the same commands used to monitor site-to-site or dialup IPSec tunnels. In particular, the “show security ike security-associations” command displays all the list of SAs in the system and their status

```
#run show security ike security-associations
Index  Remote Address  State  Initiator cookie  Responder cookie  Mode
18     172.19.100.99  UP     37b45aa1469e488b  7d4454404002e2e6  Aggressive
```

The “show security ike active-peer” command can be used to display in a tabular form the list of all connected users, their remote IP addresses and the address assigned to them using xauth.

```
# run show security ike active-peer
Remote Address      Port  Peer IKE-ID      XAUTH username      Assigned IP
172.19.100.99      500   testdynvpn       test                  10.10.10.2
```

Similarly the “show security ipsec security-associations” command displays the status of the Phase II SAs.

```
# run show security ipsec security-associations
Total active tunnels: 1
ID      Gateway      Port Algorithm      SPI      Life:sec/kb  Mon vsys
<133955586 172.19.100.99 500 ESP:aes-128/sha1 9c23b7a9 2862/ 449996 - root
>133955586 172.19.100.99 500 ESP:aes-128/sha1 c72c8f88 2862/ 449996 - root
```

Additionally the “show security dynamic-vpn users” command can be used to display the number of concurrent connections for each connected user, and the negotiated parameters for that user

```
# run show security dynamic-vpn users
User: test , Number of connections: 1
Remote IP: 172.19.100.99
IPSEC VPN: dyn-vpn
IKE gateway: dyn-vpn-local-gw
IKE ID      : testdynvpn
IKE Lifetime: 28800
IPSEC Lifetime: 3600
Status: CONNECTED
```

Licensing

All devices ship with a two-user dynamic-vpn license. More licenses can be purchased, up to a certain maximum determined by each platform.

The “show system license” command can be used to display the number of licenses installed and currently used.

```
pato@SRX240-1> show system license
License usage:
```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
av_key_kaspersky_engine	0	1	0	2013-01-01 00:00:00 UTC
anti_spam_key_sbl	0	2	0	2013-01-01 00:00:00 UTC
wf_key_surfcontrol_cpa	0	1	0	2013-01-01 00:00:00 UTC
idp-sig	0	1	0	2013-01-01 00:00:00 UTC
dynamic-vpn	1	10	0	2011-07-25 00:00:00 UTC
ax411-wlan-ap	0	2	0	permanent

As previously mentioned, client connections will be rejected when the number of licenses used reaches the number of installed licenses. When users disconnect, the licenses are released so only the maximum number of simultaneous users is enforced (not the total number of configured clients).

Summary

The dynamic-vpn feature provides a simple way to grant IPSec VPN access for remote clients. With this feature, client software can be centrally distributed and configured, simplifying the deployment complexity and cost. Small enterprises can leverage this functionality to provide remote access without requiring any additional client software or costly VPN concentrators. Large-scale deployments will be better serviced deploying a full-featured SSLVPN solution, as the one provided by the Juniper SA product line.