Chapter 7

Configuring Dynamic IPSec Subscribers

This chapter describes how to securely terminate IPSec remote access subscribers. These subscribers can reside on different VPNs and the router can support many VPNs simultaneously. It contains the following sections:

Overview

You can use the E-series router to terminate users on multiple VPNs (that is, a private intranet where users can log in and access private servers). For the E-series router, VPNs appear as VRs or VRFs. Users that connect to the VPN terminate on the associated VR or VRF. The router contains a link between the VR or VRF and the private intranet containing the resources. This link can be a direct connection, or a tunnel (IPSec, IP-in-IP, GRE, or MPLS). Once establishing a connection, the router can pass traffic between the VPN and connected users.

The E-series router already supports termination of secure remote access subscribers using L2TP and IPSec. In this model, IPSec uses transport mode to "protect" PPP subscribers that use L2TP tunnels as described in RFC 3193. However, because they are handled by the PPP and L2TP application, IPSec has no direct information about the subscribers. By terminating dynamic IPSec subscribers, the IPSec protocol manages the subscribers completely.

Dynamic Connection Setup

Dynamic secure remote access subscribers initiate connections to the E-series router by establishing an IPSec phase 1 security association (SA; also known as an IKE SA or P1) with the router.

After establishing a security association, the subscriber is instantiated in the IPSec software. Following this instantiation, the router initiates the extended authentication (Xauth) protocol exchange to invoke the user to enter a username and password. The router uses existing authentication, authorization, and accounting (AAA) functionality to authenticate the user data.

After granting access, the router instantiates an IP interface for the new subscriber as well as an access route for the IP address assigned to the subscriber on the terminating virtual router. The subscriber also obtains IP interface data (IP address, subnetwork mask, primary and secondary DNS address, primary and secondary WINS address, and so on) during a configuration exchange.

Once instantiated, an access router created, and the client successfully set with interface data parameters, the router can terminate the Xauth exchange and enable the IPSec layer and phase 2 SAs (IPSec SAs or P2s) can begin. Following these exchanges, the full data path is ready and subscribers can exchange packets with the VR on which they terminate.

Dynamic Connection Teardown

The following events can trigger the teardown of a dynamic IPSec subscriber connection:

- All phase 1 and phase 2 SA deleted by a remote peer and no rekeying activity occurs for one minute
- Administrative logout
- IPSec card terminating the user becoming unavailable (for example, the card is reloading, disabled, or disconnected)
- Dead peer detection (DPD) reporting the phase 1 SA is unreachable
- Authentication, authorization, and accounting session or idle timeout values expire

Dynamic IPSec Subscriber Recognition

The E-series router expects to receive the Xauth vendor ID from the remote peer for dynamic interface instantiation. The expected Xauth vendor ID is 0x09002689DFD6B712.

NOTE: The E-series router does not initiate connections to new subscribers. Acceptable vendor IDs are global to the router and not user-configurable.

Phase 2 SAs intended for static tunnels and those intended for dynamic subscribers do not share the same phase 1 SA. This means that dynamic phase 1 SAs are only used to negotiate dynamic phase 2 SAs. Conversely, phase 1 SAs that are not recognized as dynamic are used only to negotiate phase 2 SA static tunnels.

Licensing Requirements

Each dynamic IPSec subscribers requires the use of two licenses:

- One B-RAS license
- One IPSec license

If either license is unavailable, the router denies access to the subscriber.

Inherited Subscriber Functionality

Dynamic IPSec subscribers inherit much of the built-in AAA subscriber management functionality. This functionality includes the following:

- AAAA subscriber management commands
- DNS (primary and secondary)
- WINS (primary and secondary)
- Session timeout
- Accounting features (interval, duplication, immediate update, broadcasting, Acct-stop)
- Duplicate address checking
- IP address pools
- Per virtual-router subscriber limit
- Policies
- Packet mirroring

For additional information on AAA functionality, see *JUNOSe Broadband Access Configuration Guide, Chapter 1, Configuring Remote Access*.

Using IPSec Tunnel Profiles

IPSec tunnel profiles serve the following purposes in the configuration of dynamic IPSec subscribers:

- Controlling which connecting user, based on the IKE identification, belongs to a given profile. Profile settings falling in this category include the following:
  - IKE identities from peers that can use this profile. These identities include IP addresses, domain names, and E-mail addresses. In addition, distinguished names that use X.509 certificates are permitted.
  - The router IKE identity.
- Terminating extraneous security and IP profile settings that exist after a subscriber is mapped to an IPSec tunnel. These settings include the following:
  - Maximum number of subscribers that this profile can terminate
  - AAA domain suffix intended for the username (helping to bridge users from a given IPSec tunnel profile to an AAA domain map)
  - Phase 2 SA selectors for use in phase 2 SA exchanges
  - IP profiles intended for users logging in using this profile (helping to bridge users from a given IPSec tunnel profile to an IP profile)
  - Reachable networks on the VPN (allowing for split tunneling when supported by the client software)
  - Security parameters intended to protect user traffic (including IPSec encapsulating protocol, encryption algorithms, authentication algorithms, lifetime parameters, perfect forward secrecy, and DH group for key derivation)
- Setting the IP address the router monitors for remote subscribers.

New subscribers are mapped only to IPSec tunnel profiles after the initial IKE SA is established. Like IPSec tunnels, IKE policy rules are required to control IKE SA acceptance and denial.

Relocating Tunnel Interfaces

Unlike static IPSec tunnels interfaces, dynamic IPSec subscribers do not relocate if the IPSec server card becomes unavailable. If the IPSec server card becomes unavailable, all dynamic subscribers that are logged in and located on that server card are logged out and must log back in to connect.

User Authentication

For IPSec subscribers, user authentication occurs in two phases. The first phase is an IPSec-level authentication (phase 1 or IKE authentication). Sometimes referred to as "machine" authentication, because the user PC is authenticated, the first authentication phase verifies private or preshared keys that reside on the PC. These keys are not easily moved from one PC to another and do not require user entry each time authentication is performed.

Depending on the IKE phase 1 exchange, restrictions on the authentication type or the access network setup might exist. To avoid any usage problems, keep the following in mind:

- If you are configuring a VPN where users perform preshared key IPSec authentication and use the IKE main mode exchange for phase 1, you must setup the access network such that the VPN has an exclusive local IP address.
- If you want to share a single server address on the access network for more than one VPN, you must either set the clients to use IKE aggressive mode or use a public and private key pair for authentication. This authentication type includes X.509v3 certificates).

After the IPSec-level authentication takes place, a user authentication occurs. Often considered a legacy form of authentication, the user authentication (like RADIUS) typically requires the user to enter information in the form of a username and password.

Platform Considerations

For information about modules that support dynamic IPSec subscribers on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See IPSec Service support in *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See IPSec Service support in *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support IPSec service.

References

For more information about dynamic IPSec subscribers, consult the following resources:

- The ISAKMP Configuration Method—draft-dukes-ike-mode-cfg-02.txt (March 2002 expiration)
- Extended Authentication within IKE (XAUTH)—draft-beaulieu-ike-xauth-02.txt (April 2002 expiration
- Extended Authentication within ISAKMP/Oakley (XAUTH)—draft-ietf-ipsec-isakmp-xauth-06.txt (May 2000 expiration)

NOTE: IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at http://www.ietf.org for the latest drafts.

For additional configuration information, see:

- *Chapter 6, Configuring IPSec*
- *Chapter 9, Configuring Digital Certificates*
- *Chapter 10, Configuring IP Tunnels*
- *JUNOSe Broadband Access Configuration Guide, Chapter 1, Configuring Remote Access*

Creating an IPSec Tunnel Profile

To create an IPSec tunnel profile, use the **ipsec tunnel profile** command. This command creates a tunnel profile of the name you specify and accesses the IPSec Tunnel Profile configuration mode (config-ipsec-tunnel-profile).

ipsec tunnel profile

- Use to create or configure a tunnel profile for IPSec and accesses the IPSec Tunnel Profile configuration mode (config-ipsec-tunnel-profile). To create a new profile, you must specify a profile name.
- Use the optional **virtual-router** keyword to specify the name of the virtual router on which you want to create the profile (if you do not specify a virtual router name, the profile is created on the context virtual router)
- Example

  host1(config)#**ipsec tunnel profile tunnel1**
  host1(config-ipsec-tunnel-profile)#

- Use the **no** version to delete the tunnel profile.

Configuring IPSec Tunnel Profiles

This sections explains how to configure the parameters that exist in the IPSec tunnel profile configuration mode.

Limiting Interface Instantiations on Each Profile

To define the maximum number of interfaces that the IPSec tunnel profile can instantiate, use the **max-interfaces** command. Once the profile reaches the maximum number of interfaces, the profile rejects any new interface instantiations and generates a warning-level log. The default value (using the **no** version of the command) specifies unlimited interface instantiation on a given profile.

max-interfaces

- Use to define the maximum number of interfaces that the IPSec tunnel profile can instantiate.
- Example

  host1(config-ipsec-tunnel-profile)#**max-interfaces 500**

- Use the **no** version to return the maximum value to unlimited, indicating no limit to the number of interfaces that can be instantiated on this profile.

Specifying IKE Settings

This section describes how to define the IKE local identity and IKE peer identity values.

Setting the IKE Local Identity

To set the IKE local identity (phase 1 identity) used for IKE security association negotiations, use the **ike local-identity** command.

NOTE: The authentication algorithm for an IKE SA is associated with its identity. You must ensure that the client and server are set accordingly to successfully establish IKE security associations.

ike local-identity

- Use to set the IKE local identity used for IKE security association (SA) negotiations.
- Example

  host1(config-ipsec-tunnel-profile)#**ike local-identity domain-name domain1**

- Use the **no** version to remove the specified IKE local identity.

Setting the IKE Peer Identity

To set the IKE peer identity values, use the **ike peer-identity** command. You can set the profile to accept logins from users that present one of the following:

- An asn1DN as an IKE identity type (an ASN.1-encoded distinguished name) and the user-provided IKE identity contains the substring configured for the profile.
- A userFQDN or FQDN as an IKE identity type and the domain name portion of the IKE identity matches the domain name setting for this profile. An empty string (default) means that IKE identity types of userFQDN and FQDN are not allowed for logins on this profile.

  The IKE identity type of userFQDN also carries a domain name. Users presenting this identity must also pass any restrictions set for the peer domain name for this profile before they are able to log in.
- An IP address as an IKE identity type and the IP address resides within the specified network. The default of 0.0.0.0/0 allows any peer IP address to this profile.
- A userFQDN as an IKE identity type and the username portion of the IKE identity matches the username setting for this profile. An empty string (default) means that an IKE identity type of userFQDN is not allowed for logins on this profile.

NOTE: You can also use the wildcard (*) for the username and domain name or as the first or last character in the username or domain name string.

ike peer-identity distinguished-name
ike peer-identity domain-name
ike peer-identity ip address
ike peer-identity username

- Use to set the IKE peer identity used for IKE security association (SA) negotiations.
- Example

  host1(config-ipsec-tunnel-profile)#**ike peer-identity domain-name domain2**

- Use the **no** version to remove the specified IKE peer identity.

Appending a Domain Suffix to a Username

The VPN to which a user is to be terminated is sometimes known from the IKE identities attached to the user. However, to assist in connecting users to the correct AAA domain for authentication, you can use the **domain-suffix** command to append a domain suffix to the username. Using the default, no domain suffix, passes usernames transparently to AAA.

domain-suffix

- Use to specify a domain suffix that you want to append to any usernames received on this profile.
- Example

  host1(config-ipsec-tunnel-profile)#**domain-suffix domain2**

- Use the **no** version to restore the default value, no domain suffix, and usernames are passed transparently to AAA.

Overriding IPSec Local and Peer Identities for SA Negotiations

You can use the **local ip identity** and **peer ip identity** commands to override the local and peer identities used for SA negotiations (respectively).

local ip identity

- Use to override the local identity (phase 2 identity) used for IPSec security association negotiations. For IPSec negotiations to succeed, the local and peer identities at one end of the tunnel must match the peer and local identities at the other end (respectively).
- Example

  host1(config-ipsec-tunnel-profile)#**local ip identity range 10.30.11.1 10.30.11.50**

- Use the **no** version to restore the default value, the internal IP address allocated for the subscriber.

peer ip identity

- Use to override the peer identity (phase 2 identity) used for IPSec security association negotiations. For IPSec negotiations to succeed, the local and peer identities at one end of the tunnel must match the peer and local identities at the other end (respectively).
- Example

  host1(config-ipsec-tunnel-profile)#**peer ip identity address 10.227.1.2**

- Use the **no** version to restore the default value, the internal IP address allocated for the subscriber.

Specifying an IP Profile for IP Interface Instantiations

The **ip profile** command specifies the IP profile that is passed from the IPSec layer to the IP layer upon request for upper layer instantiation.

ip profile

- Use to specify the IP profile that the IPSec layer passes on to the IP layer upon request for upper-layer instantiation.
- Example

  host1(config-ipsec-tunnel-profile)#**ip profile ipProfile1**

- Use the **no** version to remove the association with this profile.

Defining the Server IP Address

The **local ip address** command defines the specified local IP address as the server address. The router monitors UDP port 500 for incoming login requests (that is, IKE SA negotiations) from users.

NOTE: This address is typically made public to all users trying to connect to a VPN on this router.

This command enables you to optionally set a global preshared key for the specified server address. When using global preshared keys, keep the following in mind:

- Global preshared keys enable a group of users to share a single authentication key, simplifying the administrative job of setting up keys for multiple users.
- Specific keys for individual users have higher priority than global keys. If both individual and global keys are configured, the individual that also has a specific key must use that key or authentication fails.
- More than one profile can specify the same local endpoint and virtual router. Because the last value set overrides the other, we recommend that you avoid this type of configuration.

local ip address

- Use to specify the given local IP address as a server address.
- Example

  host1(config-ipsec-tunnel-profile)#**local ip address 192.2.52.12**

- Use the **no** version to stop the router from monitoring UDP port 500 for user requests and remove any preshared key associations with the local IP address.

Specifying Local Networks

The **local ip network** command enables you to specify local, reachable networks through the IPSec tunnel. This type of "split tunneling" enables a remote station to separate VPN traffic from Internet traffic. For example a client connecting to a corporate Intranet could use split-tunneling to send all traffic destined to 10.0.0.0/8 through the secure tunnel and reach the VPN. Other traffic (for example, Web browsing) would travel directly to the Internet through the local service provider without passing through the tunnel.

NOTE: Split tunneling functions only when supported by the client software. It is up to the client to modify its routing table with the network information for split tunneling to occur

local ip network

- Use to specify networks that are reachable through the IPSec tunnel. You can configure up to 16 networks for this method of "split-tunneling."
- Example

  host1(config-ipsec-tunnel-profile)#**local ip network 10.0.0.0 255.255.255.252**

- Use the **no** version to remove the specified network from the reachable list.

Defining IPSec Security Association Lifetime Parameters

The **lifetime** command defines the IPSec SA lifetime parameters the tunnel profile can use for IPSec SA negotiations. These parameters include the phase 2 lifetime as a range in seconds or traffic volume.

lifetime

- Use to specify the IPSec lifetime parameters used on IPSec SA lifetime negotiations.
- Example

  host1(config-ipsec-tunnel-profile)#**lifetime seconds 5000 25000**

- Use the **no** version to return the lifetime to its default value, 28800 seconds (8 hours) and no traffic volume limit.

Defining User Reauthentication Protocol Values

The **extended-authentication** command specifies the extended user authentication protocol for use during the extended user authentication protocol exchange.

The **re-authenticate** keyword enables the reauthentication option (a subsequent authentication procedure). When this option is enabled, rekeying of IKE SAs uses the initial authentication protocol to reauthenticate the user. When this option is disabled, authentication is only performed at the first IKE SA establishment. Subsequent IKE SAs rekey operations inherit the initial authentication and do not reauthenticate users.

NOTE: For maximum security, enable reauthentication.

The **skip-peer-config** keyword disables the router from configuring peer IP characteristics.

extended-authentication

- Use to specify the extended user authentication protocol for use during the extended user authentication protocol exchange. This command can also enable or disable the reauthentication option (a subsequent authentication procedure).
- The **re-authenticate** keyword enables the reauthentication option (a subsequent authentication procedure).
- The **skip-peer-config** keyword disables the router from configuring peer IP characteristics.
- Example

  host1(config-ipsec-tunnel-profile)#**extended-authentication chap**

- Use the **no** version to reset the extended authentication to the default protocol, pap.

Specifying IPSEC Security Association Transforms

The **transform** command specifies the IPSec transforms that IPSec SA negotiations can use for this profile. The router accepts the first transform proposed by a client that matches one of the transforms specified by this command. During an IPSec SA exchange with a client, the router proposes all transforms specified by this command and one is accepted by the client.

NOTE: You can specify up to six transform algorithms for this profile.

For additional information about transforms and transform sets, see *Chapter 6, Configuring IPSec*.

transform

- Use to specify the eligible transforms for this profile for IPSec security association negotiations.
- Example

  host1(config-ipsec-tunnel-profile)#**transform ah-hmac-md5**

- Use the **no** version to reset the transform to the default, esp-3des-sha1.

Specifying IPSec Security Association PFS and DH Group Parameters

The **pfs group** command specifies the IPSec SA perfect forward secrecy (PFS) option and Diffie-Hellman prime modulus group that IPSec SA negotiations can use for this profile.

NOTE: When the client initiates the IPSec negotiation, the router can accept Diffie-Hellman prime modulus groups that are higher than those configured.

For additional information about PFS, see *Chapter 6, Configuring IPSec*.

pfs group

- Use to configure perfect forward secrecy for connections created with this IPSec tunnel configuration profile by assigning a Diffie-Hellman prime modulus group.
- Example

  host1(config-ipsec-tunnel-profile)#**pfs group 5**

- Use the **no** version to remove PFS from the profile.

Defining the Tunnel MTU

The **tunnel mtu** command configures the maximum transmission unit size for the tunnel.

tunnel mtu

- Use to configure the maximum transmission unit size for the tunnel.
- Example

  host1(config-ipsec-tunnel-profile)#**tunnel mtu 3000**

- Use the **no** version to restores the default value, an MTU size of 1400 bytes.

Defining IKE Policy Rules for IPSec Tunnels

This section describes enhancements to some IKE policy rule commands to support dynamic IPSec subscribers.

Specifying a Virtual Router for an IKE Policy Rule

The **ip address virtual-router** command enables an IKE policy rule to limit its scope to a specific local IP address on a specific virtual router. When enabled, this limitation ensures that this policy rule is evaluated for IKE security association evaluations for only the specified IP address and virtual router.

When initiating and responding to an IKE SA exchange, the router evaluates the possible policy rules as follows:

- If an IP-address-specific IKE policy rule refers to the local IP address and virtual router for this exchange, the router evaluates this policy rule before any non-IP-address-specific IKE policy rules. If more than one IP-address-specific IKE policy rule exists, the router evaluates the policy rule with the lowest priority number first and then evaluates the policy rule with the next highest priority number and so on.
- If no IP-address-specific IKE policy rule refers to the local IP address and virtual router for this exchange, the router evaluates all non-IP-address-specific IKE policy rules in the normal IKE policy rule evaluation order.

You can define an IKE policy rule without specifying an IP address or virtual router (the default). When not specifically configured, the IKE policy rule remains valid for any local IP address on any virtual router residing on the router.

ip address virtual-router

- Use to limit the scope of the IKE policy rule to the specified local IP address on the specified virtual router. This limitation ensures that this policy rule is evaluated for IKE security association evaluations for only the specified IP address and virtual router.
- Example

  host1(config-ike-policy)#**ip address virtual-router VR1**

- Use the **no** version to remove the IP address and virtual router limitation.

Defining Aggressive Mode for an IKE Policy Rule

The **aggressive-mode** command enables aggressive mode negotiation for the tunnel. For additional information about aggressive mode and how it works, see *Main Mode and Aggressive Mode* on page 157.

aggressive-mode

- Use to enable aggressive mode negotiation for the tunnel.
- If you specify aggressive mode negotiation, the tunnel proposes aggressive mode to the peer in connections that the policy initiates.
- If the peer initiates a negotiation, the tunnel accepts the negotiation if the mode matches this policy.
- Use the **accepted** keyword to accept aggressive mode when proposed by peers
- Use the **requested** keyword to request aggressive mode when negotiating with peers
- Use the **required** keyword to only request and accept aggressive mode when negotiating with peers.
- Example

  host1(config-ike-policy)#**aggressive-mode accepted**

- Use the **no** version to set the negotiation mode to main mode.

Monitoring IPSec Tunnel Profiles

This section contains information about troubleshooting and monitoring dynamic IPSec subscribers.

System Event Logs

To troubleshoot and monitor dynamic IPSec subscribers, use the following system event log:

- ipsecIdDb—IPsec ID database
- ipsecXcfgSM—IPsec Xauth/ModeCfg state machine
- ipsecP1Throttler—Ongoing Phase 1 negotiations

For more information about using event logs, see the *JUNOSe System Event Logging Reference Guide*.

show Commands

To display user information for dynamic IPSec tunnel profiles or subscribers, use the following **show** commands.

show ipsec tunnel profile

- Use to display information about all existing IPSec tunnel profiles or a specified tunnel profile.
- Use the **detail** keyword to display detailed information about the tunnel profile.
- Example 1

```
host1#show ipsec tunnel profile
IPsec tunnel profile ipsec-spg is active with no subscriber
1 IPsec tunnel profile found
```

- Example 2

```
host1#show ipsec tunnel profile detail ipsec-spg
IPsec tunnel profile ipsec-spg is active with no subscriber
  Extended-authentication: pap, no re-authentication
  Peer IP characteristics configuration: enabled
  Virtual router: default
  Local IP address: 10.227.5.31
  Local IKE identity: 10.227.5.31
  Peer  IKE identity: IP network: not allowed
                      username: *
                      domain-name: spg.juniper.net
                      DN: not allowed
  Maximum subscribers: no limit
  Domain suffix: @spg
  IP profile: ip-spg
  Local IPsec identity: subnet 0.0.0.0 0.0.0.0, proto 0, port 0
  Peer IPsec identity: invalid identity
  Lifetime: between 1800 and 7200 seconds, and between 100000 and 500000 KB
  Reachable networks: none
  PFS not configured
  Transforms:, tunnel-esp-3des-sha1
  Subscribers rejected due to maximum subscribers limit: 0
  Completed sessions: 43, totaling 4873 seconds, statistics:
  ipsec stats:
    outbound:
      outboundUserPacketsReceived = 88
      outboundUserOctetsReceived  = 74544
      outboundAccPacketsReceived = 88
      outboundAccOctetsReceived = 79168
      outboundOtherTxErrors = 0
      outboundPolicyErrors = 0
    inbound:
      inboundUserPacketsReceived = 88
      inboundUserOctetsReceived  = 74880
      inboundAccPacketsReceived  = 88
      inboundAccOctetsReceived   = 79488
      inboundAuthenticationErrors= 0
      inboundReplayErrors = 0
      inboundPolicyErrors = 0
      inboundOtherRxErrors = 0
      inboundDecryptErrors = 0
      inboundPadErrors = 0
```

show subscribers

- Use to display the active subscribers on the router.
- Field descriptions
  - User Name—Name of the subscriber
  - Type—Type of subscriber: atm, ip, ipsec, ppp, tnl (tunnel), tst (test)
  - Addr | Endpt—IP or IPv6 address and source of the address: l2tp, local, dhcp, radius, user. For local, dhcp, radius, and user endpoints, the address is that of the user. When the endpoint is l2tp, the address is that of the LNS.
  - Virtual Router—Name of the virtual router context
  - Interface—Interface specifier over which the subscriber is connected
  - Login Time—Date, in YY/MM/DD format, and time the subscriber logged in
  - Circuit Id—User's circuit ID value specified by PPPoE
  - Remote Id—User's remote ID value specified by PPPoE
- Example

```
host1#show subscribers
                            Subscriber List
                            ----------------
                                                                  Virtual
      User Name           Type         Addr|Endpt                 Router
-----------------------   -----   --------------------   ------------
xcfgUser1@vpn1            ipsec   10.227.5.106/local     vpn1
      User Name                      Interface
-----------------------   --------------------------------
xcfgUser1@vpn1           FastEthernet 5/2.4
      User Name               Login Time           Circuit Id
-----------------------   -------------------   -------------------
xcfgUser1@vpn1            06/05/12 10:58:42     0.4.1.10.fe.25.3b.0
     User Name              Remote Id
-----------------------   ----------------
xcfgUser1@vpn1            (800) 555-1212
```