

Chapter 14

IPSec

IP Security (IPSec) provides a secure way to authenticate senders and encrypt IP traffic between network devices, such as routing platforms and hosts. IPSec offers network administrators and their users the benefits of data confidentiality, data integrity, sender authentication, and anti-replay services. IPSec is increasingly becoming a critical component in today's contemporary IP networks.

This feature guide covers these topics:

Overview on page 578

System Requirements on page 583

Terms and Acronyms on page 583

Configuring IPSec on page 585

Example: ES PIC Manual SA Configuration on page 600

Checking Your Work on page 606

Example: Adaptive Services PIC Manual SA Configuration on page 611

Checking Your Work on page 618

Example: ES PIC IKE Dynamic SA Configuration on page 621

Checking Your Work on page 628

Example: Adaptive Services PIC IKE Dynamic SA Configuration on page 633

Checking Your Work on page 640

Example: IKE Dynamic SA Between an Adaptive Services PIC and an ES PIC Configuration on page 644

Checking Your Work on page 651

For More Information on page 657

Revision History on page 657

Overview

IPSec is a framework for ensuring secure private communication over IP networks and is based on standards developed by the International Engineering Task Force (IETF). IPSec provides security services at the network layer of the Open Systems Interconnection (OSI) model by enabling a system to select required security protocols, determine the algorithms to use for the security services, and implement any cryptographic keys required to provide the requested services. You can use IPSec to protect one or more paths between a pair of hosts, between a pair of security gateways (such as routing platforms), or between a security gateway and a host.

The terminology and components of IPSec can be intimidating to first-time users. However, if you learn a few key concepts, you can quickly master and deploy IPSec in your network. The main concepts you need to understand are as follows:

IPSec-Enabled PICs on page 578

Authentication Algorithms on page 579

Encryption Algorithms on page 579

IPSec Protocols on page 580

Security Associations on page 582

IPSec Modes on page 582

IPSec-Enabled PICs

The first choice you need to make when implementing IPSec on a JUNOS-based routing platform is the type of Physical Interface Card (PIC) you wish to use. There are two types of PIC available for M-series and T-series platforms:

The ES PIC is a first-generation PIC that provides encryption services and software support for IPSec.

The Adaptive Services PIC is a next-generation PIC that provides IPSec services and other services, such as Network Address Translation (NAT) and stateful firewall.

The J-series Services Routers also perform IPSec services in a manner similar to the Adaptive Services PIC. However, the J-series routers do this using the JUNOS software without a corresponding PIC. For more information about implementing IPSec on a J-series Services Router, see the *J-series Services Router User Guide*.

Authentication Algorithms

Authentication is the process of verifying the identity of the sender. Authentication algorithms use a shared key to verify the authenticity of the IPsec devices. The JUNOS software uses the following authentication algorithms:

Message Digest 5 (MD5) uses a one-way hash function to convert a message of arbitrary length to a fixed-length message digest of 128 bits. Because of the conversion process, it is mathematically infeasible to calculate the original message by computing it backwards from the resulting message digest. Likewise, a change to a single character in the message will cause it to generate a very different message digest number.

To verify that the message has not been tampered with, the JUNOS software compares the calculated message digest against a message digest that is decrypted with a shared key. The JUNOS software uses the MD5 hashed message authentication code (HMAC) variant that provides an additional level of hashing. MD5 can be used with authentication header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE).

Secure Hash Algorithm 1 (SHA-1) uses a stronger algorithm than MD5. SHA-1 takes a message of less than 264 bits in length and produces a 160-bit message digest. The large message digest ensures that the data has not been changed and that it originates from the correct source. The JUNOS software uses the SHA-1 HMAC variant that provides an additional level of hashing. SHA-1 can be used with AH, ESP, and IKE.

Encryption Algorithms

Encryption encodes data into a secure format so that it cannot be deciphered by unauthorized users. Like authentication algorithms, a shared key is used with encryption algorithms to verify the authenticity of the IPsec devices. The JUNOS software uses the following encryption algorithms:

Data Encryption Standard-cipher block chaining (DES-CBC) is a symmetric secret-key block algorithm. DES uses a key size of 64 bits, where 8 bits are used for error detection and the remaining 56 bits provide encryption. DES performs a series of simple logical operations on the shared key, including permutations and substitutions. CBC takes the first block of 64 bits of output from DES, combines this block with the second block, feeds this back into the DES algorithm, and repeats this process for all subsequent blocks.

Triple DES-CBC (3DES-CBC) is an encryption algorithm that is similar to DES-CBC, but provides a much stronger encryption result because it uses three keys for 168-bit (3 x 56-bit) encryption. 3DES works by using the first key to encrypt the blocks, the second key to decrypt the blocks, and the third key to reencrypt the blocks.

IPSec Protocols

IPSec protocols determine the type of authentication and encryption applied to packets that are secured by the routing platform. The JUNOS software supports the following IPSec protocols:

AH—Defined in RFC 2402, AH provides connectionless integrity and data origin authentication for IP packets. It also provides protection against replays. AH authenticates as much of the IP header as possible, as well as the upper level protocol data. However, some IP header fields may change in transit. Because the value of these fields may not be predictable by the sender, they cannot be protected by AH. In an IP header, AH can be identified as IP protocol 51. An example of the IPSec protection offered by AH is shown in Figure 47.



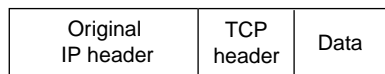
NOTE: AH is not supported on the T-series and M320 routing platforms.

Figure 47: AH Protocol

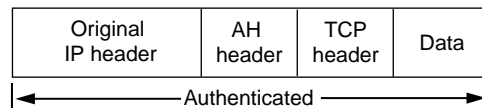
Header format

Byte 0	Byte 1	Byte 2	Byte 3
Next header	Payload length	Reserved	
Security Parameters Index (SPI)			
Sequence number			
Authentication data (variable)			

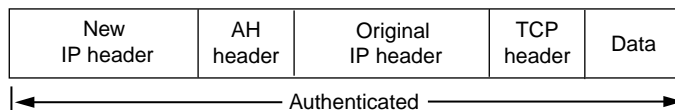
Original IPv4 packet before AH is applied



IPv4 packet after AH transport mode is applied



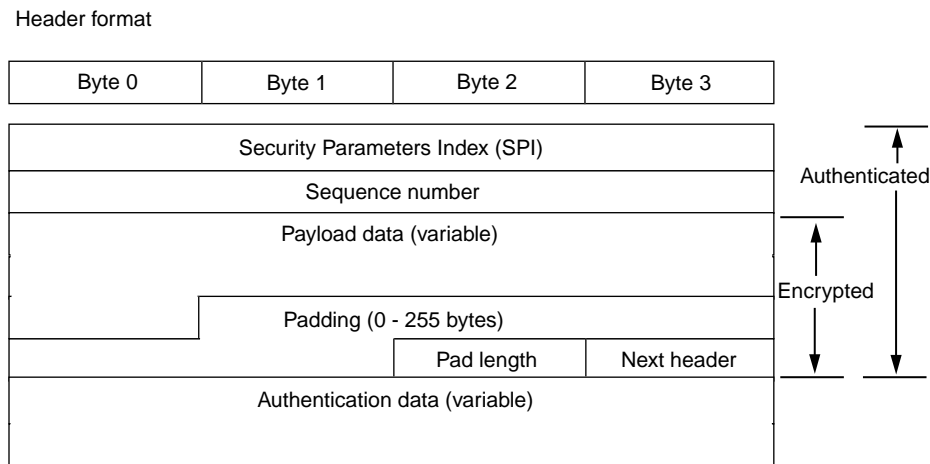
IPv4 packet after AH tunnel mode is applied



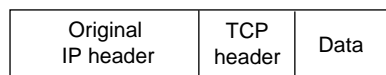
g015522

ESP—Defined in RFC 2406, ESP can provide encryption and limited traffic flow confidentiality, or connectionless integrity, data origin authentication, and an anti-replay service. In an IP header, ESP can be identified as IP protocol 50. An example of the IPsec protection offered by ESP is shown in Figure 48.

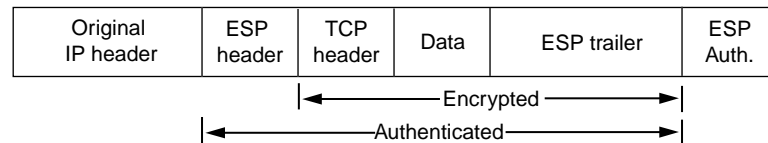
Figure 48: ESP Protocol



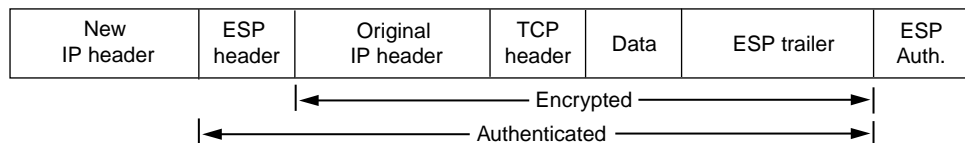
Original IPv4 packet before ESP is applied



IPv4 packet after ESP transport mode is applied



IPv4 packet after ESP tunnel mode is applied



g015521

Bundle—When you compare AH with ESP, there are some benefits and shortcomings in both protocols. ESP provides a decent level of authentication and encryption, but does so only for part of the IP packet. Conversely, although AH does not provide encryption, it does provide authentication for the entire IP packet. Because of this, the JUNOS software offers a third form of IPsec protocol called a protocol bundle. The bundle option offers a hybrid combination of AH authentication with ESP encryption.

Security Associations

Another IPsec consideration is the type of security association (SA) that you wish to implement. An SA is a set of IPsec specifications that are negotiated between devices that are establishing an IPsec relationship. These specifications include preferences for the type of authentication, encryption, and IPsec protocol that should be used when establishing the IPsec connection. An SA can be either unidirectional or bidirectional, depending on the choices made by the network administrator. An SA is uniquely identified by a Security Parameter Index (SPI), an IP destination address, and a security protocol (AH or ESP) identifier.

You can configure IPsec with a preset, preshared manual SA or use IKE to establish a dynamic SA. Manual SAs require you to specify all the IPsec requirements up front. Conversely, IKE dynamic SAs typically contain configuration defaults for the highest levels of authentication and encryption.

IPsec Modes

The last major consideration is the type of IPsec mode you wish to implement in your network. The JUNOS software supports the following IPsec modes:

Tunnel mode is supported for both AH and ESP in the JUNOS software and is the usual choice for a routing platform. In tunnel mode, the SA and associated protocols are applied to tunneled IP packets. For a tunnel mode SA, an outer IP header specifies the IPsec processing destination, and an inner IP header specifies the ultimate destination for the packet. The security protocol header appears after the outer IP header, and before the inner IP header. In addition, there are slight differences for tunnel mode when you implement it with AH and ESP:

For AH, portions of the outer IP header are protected, as well as the entire tunneled IP packet.

For ESP, only the tunneled packet is protected, not the outer header.

When one side of a security association is a security gateway (such as a routing platform), the SA must use tunnel mode. However, when traffic (for example, SNMP commands or BGP sessions) is destined for a routing platform, the system acts as a host. Transport mode is allowed in this case because the system does not act as a security gateway and does not send or receive transit traffic.

Transport mode provides a security association between two hosts. In transport mode, the protocols provide protection primarily for upper layer protocols. In IP version 4 (IPv4), a transport mode security protocol header appears immediately after the IP header and any options, and before any higher layer protocols (for example, TCP or UDP). There are slight differences for transport mode when you implement it with AH and ESP:

For AH, selected portions of the IP header are protected, as well as selected portions of the extension headers and selected options within the IPv4 header.

For ESP, only the higher layer protocols are protected, not the IP header or any extension headers preceding the ESP header.

System Requirements

To implement IPSec, your system must meet these minimum requirements:

JUNOS Release 7.1 or later for IPSec on the ES PIC for T-series and M320 routing platforms

JUNOS Release 7.0 or later for IPSec on a J-series Services Router

JUNOS Release 6.4 or later for IPSec on the Adaptive Services PIC for T-series and M320 routing platforms

JUNOS Release 6.2 or later for IPSec on the Adaptive Services PIC for M-series routers

JUNOS Release 5.7 or later for multicast over IPSec tunnels on M-series routers

JUNOS Release 5.2 or later for IPSec on the ES PIC for M-series routers

Two Juniper Networks J-series, M-series, or T-series routing platforms

Two ES PICs or Adaptive Services PICs for M-series and T-series routing platforms

Terms and Acronyms

Triple Data Encryption Standard (3DES)—An enhanced DES algorithm that provides 168-bit encryption by processing data three times with three different keys.

Adaptive Services PIC—A next-generation Physical Interface Card (PIC) that provides IPSec services and other services, such as Network Address Translation (NAT) and stateful firewall, on M-series and T-series platforms.

authentication header (AH)—A component of the IPSec protocol used to verify that the contents of a packet have not changed (data integrity), and to validate the identity of the sender (data source authentication). For more information about AH, see RFC 2402.

cipher block chaining (CBC)—A cryptographic method that encrypts blocks of ciphertext by using the encryption result of one block to encrypt the next block. Upon decryption, the validity of each block of ciphertext depends on the validity of all the preceding ciphertext blocks. For more information on how to use CBC with DES and ESP to provide confidentiality, see RFC 2405.

Data Encryption Standard (DES)—An encryption algorithm that encrypts and decrypts packet data by processing the data with a single shared key. DES operates in increments of 64-bit blocks and provides 56-bit encryption.

ES PIC—A PIC that provides first-generation encryption services and software support for IPSec on M-series and T-series platforms.

Encapsulating Security Payload (ESP)—A component of the IPSec protocol used to encrypt data in an IP packet, provide data integrity, and ensure data source authentication. For more information about ESP, see RFC 2406.

Hashed Message Authentication Code (HMAC)—A mechanism for message authentication using cryptographic hash functions. HMAC can be used with any iterative cryptographic hash function, such as MD5 or SHA-1, in combination with a secret shared key. For more information on HMAC, see RFC 2104.

Internet Key Exchange (IKE)—Establishes shared security parameters for any hosts or routers using IPSec. IKE establishes the SAs for IPSec. For more information about IKE, see RFC 2407.

Message Digest 5 (MD5)—An authentication algorithm that takes a data message of arbitrary length and produces a 128-bit message digest. For more information, see RFC 1321.

Perfect Forward Secrecy (PFS)—Provides additional security by means of a Diffie-Hellman shared secret value. With PFS, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.

Routing Engine—A PCI-based architectural portion of a JUNOS-based routing platform that handles the routing protocol process, the interface process, some of the chassis components, system management, and user access.

Secure Hash Algorithm 1 (SHA-1)—An authentication algorithm that takes a data message of less than 264 bits in length and produces a 160-bit message digest. For more information on SHA-1, see RFC 3174.

security association (SA)—Specifications that must be agreed upon between two network devices before IKE or IPSec are allowed to function. SAs primarily specify protocol, authentication, and encryption options.

Security Association Database (SADB)—A database where all SAs are stored, monitored, and processed by IPSec.

Security Policy Database (SPD)—A database that works with the SADB to ensure maximum packet security. For inbound packets, IPSec checks the SPD to verify if the incoming packet matches the security configured for a particular policy. For outbound packets, IPSec checks the SPD to see if the packet needs to be secured.

Security Parameter Index (SPI)—An identifier that is used to uniquely identify an SA at a network host or routing platform.

Configuring IPSec

To implement IPSec, you must configure the following:

Considering General IPSec Issues on page 585

Configuring Security Associations on page 588

Using a Filter to Select Traffic to Be Secured on page 593

Applying the Filter or Service Set to the Interface Receiving Traffic to Be Secured on page 595

Option: Using Filter-Based Forwarding to Select Traffic to Be Secured on page 596

Option: Using IPSec with a Layer 3 VPN on page 597

Option: Securing BGP Sessions with Transport Mode on page 599

To apply your knowledge, visit these sections:

Example: ES PIC Manual SA Configuration on page 600

Checking Your Work on page 606

Example: Adaptive Services PIC Manual SA Configuration on page 611

Checking Your Work on page 618

Example: ES PIC IKE Dynamic SA Configuration on page 621

Checking Your Work on page 628

Example: Adaptive Services PIC IKE Dynamic SA Configuration on page 633

Checking Your Work on page 640

Example: IKE Dynamic SA Between an Adaptive Services PIC and an ES PIC Configuration on page 644

Checking Your Work on page 651

Considering General IPSec Issues

Before you configure IPSec, it is helpful to understand some general guidelines.

Configuration syntax differences between the Adaptive Services PIC and the ES PIC—There are slight differences in the configuration statements and operational mode commands that are used with the PICs that support IPSec. As a result, the syntax for the Adaptive Services PIC cannot be used interchangeably with the syntax for the ES PIC. However, the syntax for one PIC can be converted to its equivalent syntax on the other PIC for interoperability. The differences are highlighted in Table 35 on page 586.

Table 35: Comparison of IPSec Configuration Statements and Operational Mode Commands for the Adaptive Services PIC and ES PIC

Adaptive Services PIC Statements and Commands	ES PIC Statements and Commands
Configuration Mode Statements	
[edit service-set <i>name</i>]	—
[edit services ipsec-vpn ike] policy {...} proposal {...}	[edit security ike] policy {...} proposal {...}
[edit services ipsec-vpn ipsec] policy {...} proposal {...}	[edit security ipsec] policy {...} proposal {...}
[edit services ipsec-vpn rule <i>rule-name</i>] remote-gateway <i>address</i>	[edit interface <i>es-fpc/pic/port</i>] tunnel destination <i>address</i>
[edit services ipsec-vpn rule <i>rule-name</i> term <i>term-name</i>] from <i>match-conditions</i> {...} then dynamic {...} from <i>match-conditions</i> {...} then manual {...}	[edit security ipsec] security-association <i>name</i> dynamic{...} security-association <i>name</i> manual{...}
[edit services ipsec-vpn rule-set]	—
[edit services service-set ipsec-vpn] local-gateway <i>address</i>	[edit interface <i>es-fpc/pic/port</i>] tunnel source <i>address</i>
Operational Mode Commands	
show services ipsec-vpn ike security-associations	show ike security-associations
show services ipsec-vpn ipsec security-associations	show ipsec security-associations



NOTE: Keep in mind the following limitations of IPSec services on the Adaptive Services PIC:

The Adaptive Services PIC does not transport packets containing IP options across IPSec tunnels. If you try to send packets containing IP options across an IPSec tunnel, the packets are dropped. Also, if you issue a ping command with the record-route option across an IPSec tunnel, the ping fails.

Destination class usage is not supported with IPSec services on the Adaptive Services PIC.

Configuring keys for authentication and encryption—When preshared keys are required for authentication or encryption, you must use the guidelines shown in Table 36 to implement the correct key size.

Table 36: Authentication and Encryption Key Lengths

	Number of Hexadecimal Characters	Number of ASCII Characters
Authentication		
HMAC-MD5-96	32	16
HMAC-SHA1-96	40	20
Encryption		
DES-CBC	16	8
3DES-CBC	48	24

Rejection of weak and semi-weak keys—The DES and 3DES encryption algorithms will reject weak and semi-weak keys. As a result, do not create keys that contain the patterns listed in Table 37.

Table 37: Weak and Semi-Weak Keys

Weak Keys			
0101	0101	0101	0101
1F1F	1F1F	1F1F	1F1F
E0E0	E0E0	E0E0	E0E0
FEFE	FEFE	FEFE	FEFE
Semi-Weak Keys			
01FE	01FE	01FE	01FE
1FE0	1FE0	0EF1	0EF1
01E0	01E0	01F1	01F1
1FFE	1FFE	0EFE	0EFE
011F	011F	010E	010E
E0FE	E0FE	F1FE	F1FE
FE01	FE01	FE01	FE01
E01F	E01F	F10E	F10E
E001	E001	F101	F101
FEF1	FEF1	FE0E	FE0E
1F01	1F01	0E01	0E01
FEEO	FEEO	FEF1	FEF1

Configuring Security Associations

The first IPSec configuration step is to select a type of security association for your IPSec connection. You must statically configure all specifications for manual SAs, but you can rely on some defaults when you configure an IKE dynamic SA. To configure a security association, see the following sections.

Configuring Manual SAs on page 588

Configuring IKE Dynamic SAs on page 590

Configuring Manual SAs

On the ES PIC, you configure a manual security association at the [edit security ipsec security-association *name*] hierarchy level. Include your choices for authentication, encryption, direction, mode, protocol, and SPI. Be sure that these choices are configured exactly the same way on the remote IPSec gateway.

```
[edit security]
ipsec {
  security-association sa-name {
    description description;
    manual {
      direction (inbound | outbound | bidirectional) {
        authentication {
          algorithm (hmac-md5-96 | hmac-sha1-96);
          key (ascii-text key | hexadecimal key);
        }
        auxiliary-spi auxiliary-spi;
        encryption {
          algorithm (des-cbc | 3des-cbc);
          key (ascii-text key | hexadecimal key);
        }
        protocol (ah | esp | bundle);
        spi spi-value;
      }
    }
  }
  mode (tunnel | transport);
}
```

On the Adaptive Services PIC, you configure a manual security association at the [edit services ipsec-vpn rule *rule-name*] hierarchy level. Include your choices for authentication, encryption, direction, protocol, and SPI. Be sure that these choices are configured exactly the same way on the remote IPSec gateway.

```
[edit services ipsec-vpn]
rule rule-name {
  match-direction (input | output);
  term term-name {
    from {
      destination-address address;
      source-address address;
    }
    then {
      backup-remote-gateway address;
      clear-dont-fragment-bit;
      manual {
        direction (inbound | outbound | bidirectional) {
          authentication {
            algorithm (hmac-md5-96 | hmac-sha1-96);
            key (ascii-text key | hexadecimal key);
          }
          auxiliary-spi spi-value;
          encryption {
            algorithm (des-cbc | 3des-cbc);
            key (ascii-text key | hexadecimal key);
          }
          protocol (ah | bundle | esp);
          spi spi-value;
        }
      }
      no-anti-replay;
      remote-gateway address;
      syslog;
    }
  }
}
rule-set rule-set-name {
  [ rule rule-names ];
}
```

Configuring IKE Dynamic SAs

On the ES PIC, you configure an IKE dynamic SA at the [edit security ike] and [edit security ipsec] hierarchy levels. Include your choices for IKE policies and proposals, which include options for authentication algorithms, authentication methods, Diffie-Hellman groups, encryption, IKE modes, and preshared keys. The IKE policy must use the IP address of the remote end of the IPSec tunnel as the policy name. Also, include your choices for IPSec policies and proposals, which include options for authentication, encryption, protocols, Perfect Forward Secrecy (PFS), and IPSec modes. Be sure that these choices are configured exactly the same way on the remote IPSec gateway.

```
[edit security]
ike {
  proposal ike-proposal-name {
    authentication-algorithm (md5 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group2);
    encryption-algorithm (3des-cbc | des-cbc);
    lifetime-seconds seconds;
  }
  policy ike-peer-address {
    description description;
    encoding (binary | pem);
    identity identity-name;
    local-certificate certificate-filename;
    local-key-pair private-public-key-file;
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposals [ proposal-names ];
  }
}
ipsec {
  proposal ipsec-proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    description description;
    encryption-algorithm (3des-cbc | des-cbc);
    lifetime-seconds seconds;
    protocol (ah | esp | bundle);
  }
  policy ipsec-policy-name {
    description description;
    perfect-forward-secrecy {
      keys (group1 | group2);
    }
    proposals [ proposal-names ];
  }
  security-association sa-name {
    description description;
    dynamic {
      ipsec-policy policy-name;
      replay-window-size (32 | 64);
    }
    mode (tunnel | transport);
  }
}
```

On the Adaptive Services PIC, you configure an IKE dynamic security association at the [edit services ipsec-vpn ike], [edit services ipsec-vpn ipsec], and [edit services ipsec-vpn rule *rule-name*] hierarchy levels. Include your choices for IKE policies and proposals, which include options for authentication algorithms, authentication methods, Diffie-Hellman groups, encryption, IKE modes, and preshared keys. Also, include your choices for IPSec policies and proposals, which include options for authentication, encryption, protocols, PFS, and IPSec modes. Be sure that these choices are configured exactly the same way on the remote IPSec gateway.

If you choose not to explicitly configure IKE and IPSec policies and proposals on the Adaptive Services PIC, your configuration can default to some preset values. These default values are shown in Table 38.

Table 38: IKE and IPSec Proposal and Policy Default Values for the Adaptive Services PIC

IKE Policy Statement	Default Value
mode	main
proposals	default
IKE Proposal Statement	Default Value
authentication-algorithm	sha1
authentication-method	pre-shared-keys
dh-group	group2
encryption-algorithm	3des-cbc
lifetime-seconds	3600 (seconds)
IPSec Policy Statement	Default Value
perfect-forward-secrecy keys	group2
proposals	default
IPSec Proposal Statement	Default Value
authentication-algorithm	hmac-sha1-96
encryption-algorithm	3des-cbc
lifetime-seconds	28800 (seconds)
protocol	esp



NOTE: If you use the default IKE and IPSec policy and proposal values preset within the Adaptive Services PIC, you must explicitly configure an IKE policy and include a preshared key. This is because the pre-shared-keys authentication method is one of the preset values in the default IKE proposal.

If you decide to configure values manually, the following information shows the complete statement hierarchy and options for dynamic IKE SAs on the Adaptive Services PIC:

```
[edit services ipsec-vpn]
ike {
  proposal proposal-name {
    authentication-algorithm (md5 | sha1);
    authentication-method (dsa-signatures | pre-shared-keys | rsa-signatures);
    description description;
    dh-group (group1 | group2);
    encryption-algorithm (3des-cbc | des-cbc);
    lifetime-seconds seconds;
  }
  policy policy-name {
    description description;
    local-id {
      ipv4_addr [ values ];
      key_id [ values ];
    }
    mode (aggressive | main);
    pre-shared-key (ascii-text key | hexadecimal key);
    proposals [ proposal-names ];
    remote-id {
      ipv4_addr [ values ];
      key_id [ values ];
    }
  }
}
ipsec {
  proposal proposal-name {
    authentication-algorithm (hmac-md5-96 | hmac-sha1-96);
    description description;
    encryption-algorithm (3des-cbc | des-cbc);
    lifetime-seconds seconds;
    protocol (ah | esp | bundle);
  }
  policy policy-name {
    description description;
    perfect-forward-secrecy {
      keys (group1 | group2);
    }
    proposals [ proposal-names ];
  }
}
```

```

rule rule-name {
  match-direction (input | output);
  term term-name {
    from {
      destination-address address;
      source-address address;
    }
    then {
      backup-remote-gateway address;
      clear-dont-fragment-bit;
      dynamic {
        ike-policy policy-name;
        ipsec-policy policy-name;
      }
      no-anti-replay;
      remote-gateway address;
      syslog;
    }
  }
}
rule-set rule-set-name {
  [ rule rule-names ];
}

```

Using a Filter to Select Traffic to Be Secured

For the ES PIC, you need to configure a firewall filter to direct traffic into the IPSec tunnel. To apply a security association to traffic that matches a firewall filter, include the `ipsec-sa sa-name` statement at the [edit firewall filter *filter-name* term *term-name* then] hierarchy level.

```

[edit firewall filter filter-name]
term term-name {
  from {
    source-address {
      ip-address;
    }
    destination-address {
      ip-address;
    }
  }
  then {
    count counter-name;
    ipsec-sa sa-name;
  }
}
term other {
  then accept;
}

```

For the Adaptive Services PIC, you do not need to configure a separate firewall filter. A filter is already built into the IPsec VPN rule statement at the [edit services ipsec-vpn] hierarchy level. To apply a security association to traffic that matches the IPsec VPN rule, include the dynamic or manual statement at the [edit services rule *rule-name* term *term-name* then] hierarchy level. To specify whether the rule should match input or output traffic, include the match-direction statement at the [edit services rule *rule-name*] hierarchy level.

After defining the rules for your IPsec VPNs, you must apply the rules to a service set. To do this, include the ipsec-vpn-rules *rule-name* statement at the [edit services service-set *service-set-name*] hierarchy level. Include a local IPsec gateway with the local-gateway *local-ip-address* statement at the [edit services service-set *service-set-name*] hierarchy level.

Also, you must select either a single interface or a pair of interfaces that participate in IPsec. To select a single interface, include the interface-service *interface-name* statement at the [edit services service-set *service-set-name*] hierarchy level. To select a pair of interfaces and a next hop, include the next-hop-service statement at the [edit services service-set *service-set-name*] hierarchy level and specify an inside interface and an outside interface. Only next-hop service sets support IPsec within Layer 3 VPNs.

```
[edit services]
service-set service-set-name {
  interface-service {
    service-interface interface-name;
  }
  next-hop-service {
    inside-service-interface interface-name;
    outside-service-interface interface-name;
  }
  ipsec-vpn-options {
    local-gateway local-ip-address;
  }
  ipsec-vpn-rules rule-name;
}
ipsec-vpn {
  rule rule-name {
    term term-name {
      from {
        source-address {
          ip-address;
        }
        destination-address {
          ip-address;
        }
      }
      then {
        remote-gateway remote-ip-address;
        (dynamic | manual);
      }
    }
    match-direction output;
  }
}
```

Applying the Filter or Service Set to the Interface Receiving Traffic to Be Secured

For the ES PIC, apply your firewall filter on the input interface receiving the traffic that you wish to send to the IPSec tunnel. To do this, include the filter statement at the [edit interfaces *interface-name* unit *unit-number* family inet] hierarchy level.

```
[edit interfaces interface-name unit unit-number family inet]
filter {
    input filter-name;
}
```

For the Adaptive Services PIC, apply your IPSec-based interface service set to the input interface receiving the traffic that you wish to send to the IPSec tunnel. To do this, include the service-set *service-set-name* statement at the [edit interfaces *interface-name* unit *unit-number* family inet service (input | output)] hierarchy level.

```
[edit interfaces interface-name unit unit-number family inet]
service {
    input {
        service-set service-set-name;
    }
    output {
        service-set service-set-name;
    }
}
```

To configure a next-hop-based service set on the Adaptive Services PIC, include the service-domain statement at the [edit interfaces *interface-name* unit *unit-number*] hierarchy level and specify one logical interface on the Adaptive Services PIC as an inside interface and a second logical interface on the Adaptive Services PIC as an outside interface.

```
[edit interfaces sp-fpc/pic/port]
unit 0 {
    family inet {
        address ip-address;
    }
}
unit 1 {
    family inet;
    service-domain inside;
}
unit 2 {
    family inet;
    service-domain outside;
}
```

Option: Using Filter-Based Forwarding to Select Traffic to Be Secured

Instead of using a firewall filter, you can also forward traffic into an IPSec security association by using a filter-based forwarding instance. First, configure the filter-based forwarding instance. Then, configure a routing table group to advertise the routes from the filter-based forwarding instance. Next, create a firewall filter for the ES PIC and reference the filter-based forwarding instance. Lastly, apply the filter and IPSec security association to the ES PIC.

```
[edit]
routing-instances {
  forwarding {
    instance-type forwarding;
    routing-options {
      static {
        route 10.10.10.0/24 next-hop 192.168.0.5;
      }
    }
  }
}
routing-options {
  rib-groups {
    group-name {
      import-rib [ inet.0 forwarding.inet.0 ];
    }
  }
}
firewall {
  family inet {
    filter filter-name {
      term term-name {
        then routing-instance instance-name;
      }
    }
  }
}

[edit]
interfaces {
  es-0/0/0 {
    unit 0 {
      tunnel {
        source source-ip-address;
        destination destination-ip-address;
      }
      family inet {
        ipsec-sa sa-name;
        filter {
          input filter-name;
        }
        address ip-address;
      }
    }
  }
}
```

Option: Using IPSec with a Layer 3 VPN

The following configuration for an Adaptive Services PIC on a provider edge (PE) router demonstrates the required use of next-hop service sets with an IKE dynamic SA in a VPN routing and forwarding (VRF) routing instance:

```
[edit]
interfaces {
  so-0/0/0 {
    description "Interface connected to the customer edge (CE) router";
    unit 0 {
      family inet {
        address 10.6.6.6/32;
      }
    }
  }
  so-2/2/0 {
    description "Source IPSec tunnel interface to the network core";
    unit 0 {
      family inet {
        address 10.10.1.1/30;
      }
    }
  }
  sp-3/1/0 {
    description "Adaptive Services PIC interface";
    unit 0 {
      family inet {
        address 10.7.7.7/32;
      }
    }
    unit 1 {
      family inet;
      service-domain inside;
    }
    unit 2 {
      family inet;
      service-domain outside;
    }
  }
}
policy-options {
  policy-statement vpn-export-policy {
    then {
      community add community-name;
      accept;
    }
  }
  policy-statement vpn-import-policy {
    term term-name {
      from community community-name;
      then accept;
    }
  }
  community community-name members target:100:20;
}
}
```

```

routing-instances {
  vrf {
    instance-type vrf;
    interface sp-3/1/0.1; # Inside sp interface.
    interface so-0/0/0.0; # Interface that connects to the CE router.
    route-distinguisher route-distinguisher;
    vrf-import vpn-import-policy;
    vrf-export vpn-export-policy;
    routing-options {
      static {
        route ip-address/prefix next-hop so-0/0/0.0; # Routes for the CE router.
        route ip-address/prefix next-hop sp-3/1/0.1; # Routes for IPSec.
      }
    }
  }
}
services {
  service-set service-set-name {
    next-hop-service {
      inside-service-interface sp-3/1/0.1;
      outside-service-interface sp-3/1/0.2;
    }
    ipsec-vpn-options {
      local-gateway 10.10.1.1;
    }
    ipsec-vpn-rules rule-name;
  }
  ipsec-vpn {
    rule rule-name {
      term term-name {
        from {
          source-address {
            source-ip-address;
          }
        }
        then {
          remote-gateway 10.10.1.2;
          dynamic {
            ike-policy ike-policy-name;
          }
        }
      }
    }
    match-direction direction;
  }
  ike {
    policy ike-policy-name {
      pre-shared-key ascii-text preshared-key;
    }
  }
}
}

```

For more information on VRF routing instances, see the *JUNOS VPNs Configuration Guide*. For more information on next-hop service sets, see the *JUNOS Services Interfaces Configuration Guide*.

Option: Securing BGP Sessions with Transport Mode

For the ES PIC, you can use IPSec to secure BGP sessions between Routing Engines in M-series and T-series platforms. To configure, create a transport mode security association and apply the SA to the BGP configuration by including the `ipsec-sa` statement at the `[edit protocols bgp group group-name]` hierarchy level.

```
[edit]
protocols {
  bgp {
    group group-name {
      local-address ip-address;
      export export-policy;
      peer-as as-number;
      ipsec-sa sa-name;
      neighbor peer-ip-address;
    }
  }
}
```

Example: ES PIC Manual SA Configuration

Figure 49: ES PIC Manual SA Topology Diagram

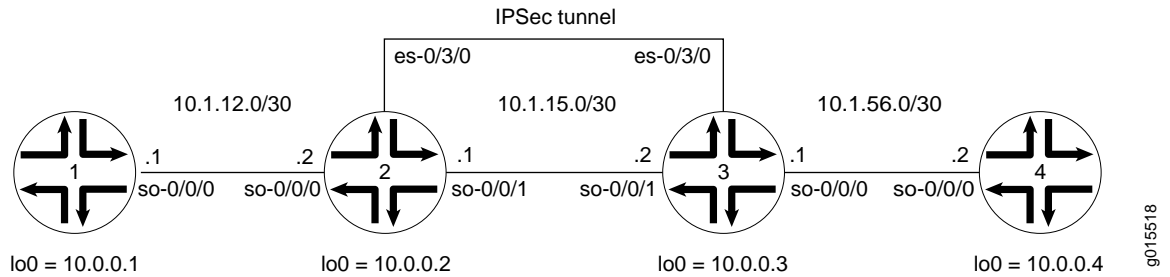


Figure 49 shows an IPSec topology containing a group of four routers. Routers 2 and 3 establish an IPSec tunnel using an ES PIC and manual SA settings. Routers 1 and 4 provide basic connectivity and are used to verify that the IPSec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

```

Router 1 [edit]
interfaces {
  so-0/0/0 {
    description "To R2 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.1/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.1;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}

```

g015518

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional manual SA called `sa-manual` at the [edit security ipsec security-association] hierarchy level. Use AH for the protocol, 400 for the SPI, HMAC-MD5-96 for authentication, and a 32-bit hexadecimal authentication key for the MD5 authentication key. (For more information about key length, see Table 36 on page 587.) Because you are using AH, there is no need to configure encryption.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The `es-traffic` filter matches inbound traffic from Router 1 destined for Router 4, while the `es-return` filter matches the return path from Router 4 to Router 1. Apply the `es-traffic` filter to the `so-0/0/0` interface, then apply both the `es-return` filter and the `sa-manual` SA to the `es-0/3/0` interface.

```
Router 2 [edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        filter {
          input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
        }
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.1/30;
      }
    }
  }
  es-0/3/0 {
    unit 0 {
      tunnel { # Specify the IPSec tunnel endpoints here.
        source 10.1.15.1;
        destination 10.1.15.2;
      }
      family inet {
        ipsec-sa sa-manual; # Apply the manual SA here.
        filter {
          input es-return; # Apply the filter that matches return IPSec traffic here.
        }
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.2/32;
      }
    }
  }
}
```

```

routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
security {
  ipsec {
    security-association sa-manual { # Define the manual SA specifications here.
      mode tunnel;
      manual {
        direction bidirectional {
          protocol ah;
          spi 400;
          authentication {
            algorithm hmac-md5-96;
            key hexadecimal "$9$r0/eK8x7VY2ahSvL7-2gfTQF9Apu1EhrmfF/CtI
RIKMW7-VwYg4ZhSeW8XbwoJGjHmP5QF69wY4Zjif5369ApBSyKv8XRE";
          }
        }
      }
    }
  }
}

```

The 32-bit unencrypted hexadecimal key is **abcdef01abcdef01abcdef01abcdef01**.

```

firewall {
  filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
    term to-es {
      from {
        source-address {
          10.1.12.0/24;
        }
        destination-address {
          10.1.56.0/24;
        }
      }
      then {
        count ipsec-tunnel;
        ipsec-sa sa-manual;
      }
    }
    term other {
      then accept;
    }
  }
  filter es-return { # Define a filter that matches return IPSec traffic here.
    term return {
      from {
        source-address {
          10.1.56.0/24;
        }
        destination-address {
          10.1.12.0/24;
        }
      }
      then accept;
    }
  }
}

```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional manual SA called `sa-manual` at the [edit security ipsec security-association] hierarchy level. Use the exact same specifications that you used for the SA on Router 2: AH for the protocol, 400 for the SPI, HMAC-MD5-96 for authentication, and a 32-bit hexadecimal authentication key of `abcdef01abcdef01abcdef01abcdef01` for the MD5 authentication key. (For more information about authentication key length, see Table 36 on page 587.) Because you are using AH, there is no need to configure an encryption algorithm.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The `es-traffic` filter matches inbound traffic from Router 4 destined for Router 1, while the `es-return` filter matches the return path from Router 1 to Router 4. Apply the `es-traffic` filter to the `so-0/0/0` interface, then apply both the `es-return` filter and the `sa-manual` SA to the `es-0/3/0` interface.

```

Router 3 [edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
      family inet {
        filter {
          input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
        }
        address 10.1.56.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R2 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.2/30;
      }
    }
  }
  es-0/3/0 {
    unit 0 {
      tunnel { # Specify the IPSec tunnel endpoints here.
      source 10.1.15.2;
      destination 10.1.15.1;
    }
    family inet {
      ipsec-sa sa-manual; # Apply the manual SA here.
      filter {
        input es-return; # Apply the filter that matches return IPSec traffic here.
      }
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.3/32;
    }
  }
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
}

```


On Router 4, provide basic OSPF connectivity to Router 3.

```

Router 4 [edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}

```

Checking Your Work

To verify proper operation of a manual IPsec SA on the ES PIC, use the following commands:

```
ping
```

```
show ipsec security-associations (detail)
```

```
traceroute
```

The following sections show the output of these commands used with the configuration example:

Router 1 on page 607

Router 2 on page 608

Router 3 on page 609

Router 4 on page 610

Router 1

On Router 1, issue a ping command to the so-0/0/0 interface of Router 4 to send traffic across the IPSec tunnel.

```
user@R1> ping 10.1.56.2
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=253 time=0.939 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=253 time=0.886 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=253 time=0.826 ms
^C
--- 10.1.56.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.826/0.884/0.939/0.046 ms
```

You can also issue the traceroute command to verify that traffic to 10.1.56.2 travels over the IPSec tunnel between Router 2 and Router 3. Notice that the second hop does not reference 10.1.15.2—the physical interface on Router 3. Instead, the loopback address of 10.0.0.3 on Router 3 appears as the second hop. This indicates that the IPSec tunnel is operating correctly.

```
user@R1> traceroute 10.1.56.2
traceroute to 10.1.56.2 (10.1.56.2), 30 hops max, 40 byte packets
 1 10.1.12.1 (10.1.12.1) 0.655 ms 0.549 ms 0.508 ms
 2 10.0.0.3 (10.0.0.3) 0.833 ms 0.786 ms 0.757 ms
 3 10.1.56.2 (10.1.56.2) 0.808 ms 0.741 ms 0.716 ms
```

Router 2

Another way to verify that matched traffic is being diverted to the bidirectional IPSec tunnel is to view the firewall filter counter. After you issue the ping command from Router 1 (three packets), the es-traffic firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                Bytes    Packets
ipsec-tunnel        252      3
```

After you issue the ping command from both Router 1 (three packets) and Router 4 (two packets), the es-traffic firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                Bytes    Packets
ipsec-tunnel        420      5
```

To verify that the IPSec security association is active, issue the show ipsec security-associations detail command. Notice that the SA contains the settings you specified, such as AH for the protocol and HMAC-MD5-96 for the authentication algorithm.

```
user@R2> show ipsec security-associations detail
Security association: sa-manual, Interface family: Up

Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)

Direction: inbound, SPI: 400, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Anti-replay service: Disabled

Direction: outbound, SPI: 400, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Anti-replay service: Disabled
```

Router 3

View the firewall filter counter to continue verifying that matched traffic is being diverted to the bidirectional IPSec tunnel. After you issue the ping command from Router 1 (three packets), the es-traffic firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                Bytes    Packets
ipsec-tunnel        252      3
```

After you issue the ping command from both Router 1 (three packets) and Router 4 (two packets), the es-traffic firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                Bytes    Packets
ipsec-tunnel        420      5
```

To verify that the IPSec security association is active, issue the `show ipsec security-associations detail` command. Notice that the SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ipsec security-associations detail
Security association: sa-manual, Interface family: Up

Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)

Direction: inbound, SPI: 400, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Anti-replay service: Disabled

Direction: outbound, SPI: 400, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: AH, Authentication: hmac-md5-96, Encryption: None
Anti-replay service: Disabled
```

Router 4

On Router 4, issue a ping command to the so-0/0/0 interface of Router 1 to send traffic across the IPsec tunnel.

```
user@R4> ping 10.1.12.2
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=253 time=0.937 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=253 time=0.872 ms
^C
--- 10.1.12.2 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.872/0.905/0.937/0.032 ms
```

You can also issue the traceroute command to verify that traffic to 10.1.12.2 travels over the IPsec tunnel between Router 3 and Router 2. Notice that the second hop does not reference 10.1.15.1—the physical interface on Router 2. Instead, the loopback address of 10.0.0.2 on Router 2 appears as the second hop. This indicates that the IPsec tunnel is operating correctly.

```
user@R4> traceroute 10.1.12.2
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1 10.1.56.1 (10.1.56.1) 0.670 ms 0.589 ms 0.548 ms
 2 10.0.0.2 (10.0.0.2) 0.815 ms 0.791 ms 0.763 ms
 3 10.1.12.2 (10.1.12.2) 0.798 ms 0.741 ms 0.714 ms
```

Example: Adaptive Services PIC Manual SA Configuration

Figure 50: Adaptive Services PIC Manual SA Topology Diagram

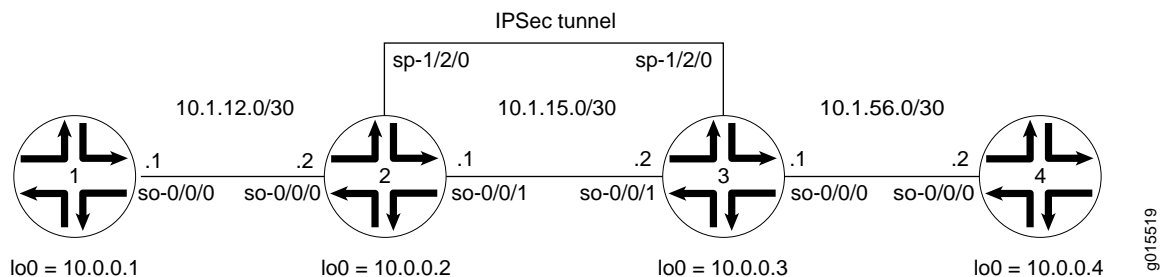


Figure 50 shows a similar IPsec topology to the one used in the ES PIC manual SA example. The difference is that Routers 2 and 3 establish an IPsec tunnel using an Adaptive Services PIC and use slightly modified manual SA settings. Routers 1 and 4 again provide basic connectivity and are used to verify that the IPsec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

```

Router 1 [edit]
interfaces {
  so-0/0/0 {
    description "To R2 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.1/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.1;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}

```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional manual SA in a rule called `rule-manual-SA-BiEspshades` at the `[edit ipsec-vpn rule]` hierarchy level. Reference this rule in a service set called `service-set-manual-BiEspshades` at the `[edit services service-set]` hierarchy level.

Configure all specifications for your manual SA. Use ESP for the protocol, 261 for the SPI, HMAC-SHA1-96 for authentication, DES-CBC for encryption, a 20-bit ASCII authentication key for the SHA-1 authentication key, and an 8-bit ASCII encryption key for the DES-CBC authentication key. (For more information about key lengths, see Table 36 on page 587.)

To direct traffic into the Adaptive Services PIC and the IPsec tunnel, include match conditions in the `rule-manual-SA-BiEspshades` IPsec VPN rule to match inbound traffic from Router 1 that is destined for Router 4. Because the rule is already referenced by the service set, apply the service set to the `so-0/0/1` interface. To count the amount of traffic that enters the IPsec tunnel, configure a firewall filter called `ipsec-tunnel` and apply it to the `sp-1/2/0` interface.

```

Router 2 [edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
      family inet {
        service { # Apply the service set here.
          input {
            service-set service-set-manual-BiEspshades;
          }
          output {
            service-set service-set-manual-BiEspshades;
          }
        }
        address 10.1.15.1/30;
      }
    }
  }
  sp-1/2/0 {
    services-options {
      syslog {
        host local {
          services info;
        }
      }
    }
  }
}

```

```

    unit 0 {
        family inet {
            filter {
                input ipsec-tunnel; # Apply the firewall filter with the counter here.
            }
        }
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.0.0.2/32;
        }
    }
}
}
routing-options {
    router-id 10.0.0.2;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface so-0/0/1.0;
            interface lo0.0;
        }
    }
}
}
firewall {
    filter ipsec-tunnel { # Configure a firewall filter to count IPSec traffic here.
        term 1 {
            then {
                count ipsec-tunnel;
                accept;
            }
        }
    }
}
}

```

```

services {
  service-set service-set-manual-BiEspshades { # Define your service set here.
    interface-service {
      service-interface sp-1/2/0; # Specify an interface to process IPSec.
    }
    ipsec-vpn-options {
      local-gateway 10.1.15.1; # Specify the local IP address of the IPSec tunnel.
    }
    ipsec-vpn-rules rule-manual-SA-BiEspshades; # Reference the IPSec rule here.
  }
  ipsec-vpn {
    rule rule-manual-SA-BiEspshades { # Define your IPSec VPN rule here.
      term term-manual-SA-BiEspshades {
        from {
          source-address {
            10.0.0.0/8;
          }
        }
        then {
          remote-gateway 10.1.15.2; # The remote IP address of the IPSec tunnel.
          manual { # Define the manual SA specifications here.
            direction bidirectional {
              protocol esp;
              spi 261;
              authentication {
                algorithm hmac-sha1-96;
                key ascii-text "$9$v.s8xd24Zk.5bs.5QFAtM8XNVYJGifT3goT369
                OBxNdw2ajHmFnCZUnCtuEh";
              }
            }
            encryption {
              algorithm des-cbc;
              key ascii-text "$9$3LJW/A0EclXdBlxdfsJZn/CpOR";
            }
          }
          ## The unencrypted key is juniperjuniperjunipe (20 characters for HMAC-SHA-1-96).
        }
      }
    }
  }
  match-direction output;
}

```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional manual SA in a rule called `rule-manual-SA-BiEspshades` at the `[edit ipsec-vpn rule]` hierarchy level. Reference this rule in a service set called `service-set-manual-BiEspshades` at the `[edit services service-set]` hierarchy level.

Configure the same specifications for your manual SA that you specified on Router 2. Use ESP for the protocol, 261 for the SPI, HMAC-SHA1-96 for authentication, DES-CBC for encryption, a 20-bit ASCII authentication key for the SHA-1 authentication key, and an 8-bit ASCII encryption key for the DES-CBC authentication key. (For more information about key lengths, see Table 36 on page 587.)

To direct traffic into the Adaptive Services PIC and the IPSec tunnel, include match conditions in the `rule-manual-SA-BiEspshades` IPSec VPN rule to match inbound traffic from Router 4 that is destined for Router 1. Because the rule is already referenced by the service set, apply the service set to the `so-0/0/1` interface. To count the amount of traffic that enters the IPSec tunnel, configure a firewall filter called `ipsec-tunnel` and apply it to the `sp-1/2/0` interface.

```

Router 3 [edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R2 so-0/0/1";
    unit 0 {
      family inet {
        service { # Apply the service set here.
          input {
            service-set service-set-manual-BiEspshades;
          }
          output {
            service-set service-set-manual-BiEspshades;
          }
        }
        address 10.1.15.2/30;
      }
    }
  }
  sp-1/2/0 {
    services-options {
      syslog {
        host local {
          services info;
        }
      }
    }
  }
}

```

```

    unit 0 {
      family inet {
        filter {
          input ipsec-tunnel; # Apply the firewall filter with the counter here.
        }
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.3/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
}
firewall {
  filter ipsec-tunnel { # Configure a firewall filter to count IPSec traffic here.
    term 1 {
      then {
        count ipsec-tunnel;
        accept;
      }
    }
  }
}

```


On Router 4, provide basic OSPF connectivity to Router 3.

```

Router 4 [edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}

```

Checking Your Work

To verify proper operation of a manual IPsec SA on the Adaptive Services PIC, use the following commands:

```

ping
show services ipsec-vpn ipsec security-associations (detail)

```

The following sections show the output of these commands used with the configuration example:

Router 1 on page 619

Router 2 on page 619

Router 3 on page 620

Router 1

On Router 1, issue a ping command to the lo0 interface on Router 4 to send traffic across the IPsec tunnel.

```
user@R1> ping 10.0.0.4
PING 10.0.0.4 (10.0.0.4): 56 data bytes
64 bytes from 10.0.0.4: icmp_seq=0 ttl=254 time=1.375 ms
64 bytes from 10.0.0.4: icmp_seq=1 ttl=254 time=18.375 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=254 time=1.120 ms
^C
--- 10.0.0.4 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.120/6.957/18.375/8.075 ms
```

Router 2

One way to verify that matched traffic is being diverted to the bidirectional IPsec tunnel is to view the firewall filter counter. After you issue the ping command from Router 1 (three packets), the ipsec-tunnel firewall filter counter looks like this:

```
user@R2> show firewall filter ipsec-tunnel
Filter: ipsec-tunnel
Counters:
Name                Bytes    Packets
ipsec-tunnel        252      3
```

To verify that the IPsec security association is active, issue the `show services ipsec-vpn ipsec security-associations detail` command. Notice that the SA contains the settings you specified, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

```
user@R2> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-manual-BiEspshades

Rule: rule-manual-SA-BiEspshades, Term: term-manual-SA-BiEspshades,
Tunnel index: 1
Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
Local identity: ipv4_subnet(any:0,[0..7]=10.0.0.0/8)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)

Direction: inbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled

Direction: outbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled
```

Router 3

View the firewall filter counter to continue verifying that matched traffic is being diverted to the bidirectional IPSec tunnel. After you issue the ping command from Router 1 (three packets), the ipsec-tunnel firewall filter counter looks like this:

```
user@R3> show firewall filter ipsec-tunnel
Filter: ipsec-tunnel
Counters:
Name                Bytes    Packets
ipsec-tunnel        252      3
```

To verify that the IPSec security association is active, issue the `show services ipsec-vpn ipsec security-associations detail` command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-manual-BiEspshades

Rule: rule-manual-SA-BiEspshades, Term: term-manual-SA-BiEspshades,
Tunnel index: 1
Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=10.0.0.0/8)
Remote identity: ipv4_subnet(any:0,[0..7]=0.0.0.0/0)

Direction: inbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled

Direction: outbound, SPI: 261, AUX-SPI: 0
Mode: tunnel, Type: manual, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: des-cbc
Anti-replay service: Disabled
```

Example: ES PIC IKE Dynamic SA Configuration

Figure 51: ES PIC IKE Dynamic SA Topology Diagram

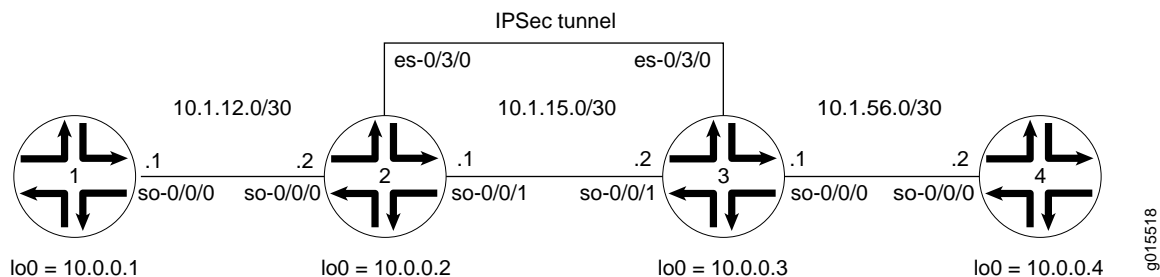


Figure 51 shows the same IPsec topology as seen in the ES PIC manual SA example. However, this time the configuration requires Routers 2 and 3 to establish an IPsec tunnel using an IKE dynamic SA, enhanced authentication, and stronger encryption. Routers 1 and 4 continue to provide basic connectivity and are used to verify that the IPsec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

```

Router 1 [edit]
interfaces {
  so-0/0/0 {
    description "To R2 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.1/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.1;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}

```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional IKE dynamic SA called sa-dynamic at the [edit security ipsec security-association] hierarchy level. For your IKE policy and proposal, use preshared keys for the authentication method, SHA-1 for the authentication algorithm, 3DES-CBC for encryption, group 2 for the Diffie-Hellman group, main mode, 3600 seconds for the lifetime, and a preshared key of juniper for the initial IKE negotiation. For your IPSec policy and proposal, use ESP for the protocol, HMAC-SHA1-96 for authentication, 3DES-CBC for encryption, 28800 seconds for the lifetime, and group 2 for the PFS group.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The es-traffic filter matches inbound traffic from Router 1 destined for Router 4, while the es-return filter matches the return path from Router 4 to Router 1. Apply the es-traffic filter to the so-0/0/0 interface, then apply both the es-return filter and the sa-dynamic SA to the es-0/3/0 interface.

```

Router 2 [edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        filter {
          input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
        }
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.1/30;
      }
    }
  }
  es-0/3/0 {
    unit 0 {
      tunnel { # Specify the IPSec tunnel endpoints here.
        source 10.1.15.1;
        destination 10.1.15.2;
      }
      family inet {
        ipsec-sa sa-dynamic; # Apply the IKE dynamic SA here.
        filter {
          input es-return; # Apply the filter that matches return IPSec traffic here.
        }
      }
    }
  }
}

```



```
firewall {  
  filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.  
    term to-es {  
      from {  
        source-address {  
          10.1.12.0/24;  
        }  
        destination-address {  
          10.1.56.0/24;  
        }  
      }  
      then {  
        count ipsec-tunnel;  
        ipsec-sa sa-dynamic;  
      }  
    }  
    term other {  
      then accept;  
    }  
  }  
  filter es-return { # Define a filter that matches return IPSec traffic here.  
    term return {  
      from {  
        source-address {  
          10.1.56.0/24;  
        }  
        destination-address {  
          10.1.12.0/24;  
        }  
      }  
      then accept;  
    }  
  }  
}
```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional IKE dynamic SA called sa-dynamic at the [edit security ipsec security-association] hierarchy level. Use the same policies and proposals that you used on Router 2.

For your IKE policy and proposal, use preshared keys for the authentication method, SHA-1 for the authentication algorithm, 3DES-CBC for encryption, group 2 for the Diffie-Hellman group, main mode, 3600 seconds for the lifetime, and a preshared key of juniper for the initial IKE negotiation. For your IPSec policy and proposal, use ESP for the protocol, HMAC-SHA1-96 for authentication, 3DES-CBC for encryption, 28800 seconds for the lifetime, and group 2 for the PFS group.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The es-traffic filter matches inbound traffic from Router 4 destined for Router 1, while the es-return filter matches the return path from Router 1 to Router 4. Apply the es-traffic filter to the so-0/0/0 interface, then apply both the es-return filter and the sa-dynamic SA to the es-0/3/0 interface.

```

Router 3 [edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
      family inet {
        filter {
          input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
        }
        address 10.1.56.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R2 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.2/30;
      }
    }
  }
  es-0/3/0 {
    unit 0 {
      tunnel { # Specify the IPSec tunnel endpoints here.
        source 10.1.15.2;
        destination 10.1.15.1;
      }
      family inet {
        ipsec-sa sa-dynamic; # Apply the IKE dynamic SA here.
        filter {
          input es-return; # Apply the filter that matches return IPSec traffic here.
        }
      }
    }
  }
}

```

```

lo0 {
  unit 0 {
    family inet {
      address 10.0.0.3/32;
    }
  }
}
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
security {
  ipsec {
    proposal es-ipsec-proposal { # Define your IPSec proposal specifications here.
      protocol esp;
      authentication-algorithm hmac-sha1-96;
      encryption-algorithm 3des-cbc;
      lifetime-seconds 28800;
    }
    policy es-ipsec-policy { # Define your IPSec policy specifications here.
      perfect-forward-secrecy {
        keys group2;
      }
      proposals es-ipsec-proposal; # Reference the IPSec proposal here.
    }
    security-association sa-dynamic { # Define your IKE dynamic SA here.
      dynamic {
        ipsec-policy es-ipsec-policy; # Reference the IPSec policy here.
      }
    }
  }
}
ike {
  proposal es-ike-proposal { # Define your IKE proposal specifications here.
    authentication-method pre-shared-keys;
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 3600;
  }
  policy 10.1.15.1 { # Define your IKE policy specifications here.
    mode main;
    proposals es-ike-proposal; # Reference the IKE proposal here.
    pre-shared-key ascii-text "$9$TF6ABlcvWxp0WxNdg4QFn";
  }
}
## The unencrypted pre-shared key for this example is juniper.
}
}
}

```

```

firewall {
  filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
    term to-es {
      from {
        source-address {
          10.1.56.0/24;
        }
        destination-address {
          10.1.12.0/24;
        }
      }
      then {
        count ipsec-tunnel;
        ipsec-sa sa-dynamic;
      }
    }
    term other {
      then accept;
    }
  }
  filter es-return { # Define a filter that matches return IPSec traffic here.
    term return {
      from {
        source-address {
          10.1.12.0/24;
        }
        destination-address {
          10.1.56.0/24;
        }
      }
      then accept;
    }
  }
}

```

On Router 4, provide basic OSPF connectivity to Router 3.

```

Router 4 [edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}

```

Checking Your Work

To verify proper operation of an IKE-based dynamic SA on the ES PIC, use the following commands:

```

ping
show ike security-associations (detail)
show ipsec security-associations (detail)
traceroute

```

The following sections show the output of these commands used with the configuration example:

Router 1 on page 629

Router 2 on page 629

Router 3 on page 631

Router 4 on page 632

Router 1

On Router 1, issue a ping command to the so-0/0/0 interface of Router 4 to send traffic across the IPSec tunnel.

```
user@R1> ping 10.1.56.2
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=253 time=0.917 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=253 time=0.881 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=253 time=0.897 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=253 time=0.871 ms
64 bytes from 10.1.56.2: icmp_seq=4 ttl=253 time=0.890 ms
64 bytes from 10.1.56.2: icmp_seq=5 ttl=253 time=0.858 ms
64 bytes from 10.1.56.2: icmp_seq=6 ttl=253 time=0.904 ms
^C
--- 10.1.56.2 ping statistics ---
7 packets transmitted, 7 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.858/0.888/0.917/0.019 ms
```

You can also issue the `traceroute` command to verify that traffic to 10.1.56.2 travels over the IPSec tunnel between Router 2 and Router 3. Notice that the second hop does not reference 10.1.15.2—the physical interface on Router 3. Instead, the loopback address of 10.0.0.3 on Router 3 appears as the second hop. This indicates that the IPSec tunnel is operating correctly.

```
user@R1> traceroute 10.1.56.2
traceroute to 10.1.56.2 (10.1.56.2), 30 hops max, 40 byte packets
 1 10.1.12.1 (10.1.12.1) 0.655 ms 0.549 ms 0.508 ms
 2 10.0.0.3 (10.0.0.3) 0.833 ms 0.786 ms 0.757 ms
 3 10.1.56.2 (10.1.56.2) 0.808 ms 0.741 ms 0.716 ms
```

Router 2

Another way to verify that matched traffic is being diverted to the bidirectional IPSec tunnel is to view the firewall filter counter. After you issue the ping command from Router 1 (seven packets), the `es-traffic` firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                Bytes      Packets
-----                -
ipsec-tunnel         588         7
```

After you issue the ping command from both Router 1 (seven packets) and Router 4 (five packets), the `es-traffic` firewall filter counter looks like this:

```
user@R2> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                Bytes      Packets
-----                -
ipsec-tunnel        1008        12
```

To verify that the IKE SA negotiation between Routers 2 and 3 is successful, issue the `show ike security-associations detail` command. Notice that the SA contains the settings you specified, such as SHA-1 for the authentication algorithm and 3DES-CBC for the encryption algorithm.

```
user@R2> show ike security-associations detail
IKE peer 10.1.15.2
Role: Initiator, State: Matured
Initiator cookie: b5dbdfef9000000, Responder cookie: a24c868410000041
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 10.1.15.1:500, Remote: 10.1.15.2:500
Lifetime: Expires in 401 seconds
Algorithms:
Authentication : sha1
Encryption     : 3des-cbc
Pseudo random function: hmac-sha1
Traffic statistics:
Input bytes :      1736
Output bytes :     2652
Input packets:      9
Output packets:    15
Flags: Caller notification sent
IPSec security associations: 3 created, 0 deleted
Phase 2 negotiations in progress: 0
```

To verify that the IPSec security association is active, issue the `show ipsec security-associations detail` command. Notice that the SA contains the settings you specified, such as ESP for the protocol, HMAC-SHA1-96 for the authentication algorithm, and 3DES-CBC for the encryption algorithm.

```
user@R2> show ipsec security-associations detail
Security association: sa-dynamic, Interface family: Up

Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
Local identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)

Direction: inbound, SPI: 2133029543, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26212 seconds
Hard lifetime: Expires in 26347 seconds
Anti-replay service: Disabled

Direction: outbound, SPI: 1759450863, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26212 seconds
Hard lifetime: Expires in 26347 seconds
Anti-replay service: Disabled
```

Router 3

View the firewall filter counter to continue verifying that matched traffic is being diverted to the bidirectional IPSec tunnel. After you issue the ping command from Router 1 (seven packets), the es-traffic firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                Bytes    Packets
ipsec-tunnel        588      7
```

After you issue the ping command from both Router 1 (seven packets) and Router 4 (five packets), the es-traffic firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name                Bytes    Packets
ipsec-tunnel        1008     12
```

To verify the success of the IKE security association, issue the show ike security-associations detail command. Notice that the SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ike security-associations detail
IKE peer 10.1.15.1
Role: Responder, State: Matured
Initiator cookie: b5dbdf2f9000000, Responder cookie: a24c868410000041
Exchange type: Main, Authentication method: Pre-shared-keys
Local: 10.1.15.2:500, Remote: 10.1.15.1:500
Lifetime: Expires in 564 seconds
Algorithms:
Authentication      : sha1
Encryption          : 3des-cbc
Pseudo random function: hmac-sha1
Traffic statistics:
Input bytes :      2652
Output bytes :     1856
Input packets:      15
Output packets:     10
Flags: Caller notification sent
IPSec security associations: 3 created, 4 deleted
Phase 2 negotiations in progress: 0
```

To verify that the IPSec security association is active, issue the `show ipsec security-associations detail` command. Notice that the SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ipsec security-associations detail
Security association: sa-dynamic, Interface family: Up

Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)

Direction: inbound, SPI: 1759450863, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26427 seconds
Hard lifetime: Expires in 26517 seconds
Anti-replay service: Disabled

Direction: outbound, SPI: 2133029543, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26427 seconds
Hard lifetime: Expires in 26517 seconds
Anti-replay service: Disabled
```

Router 4

On Router 4, issue a ping command to the `so-0/0/0` interface of Router 1 to send traffic across the IPSec tunnel.

```
user@R4> ping 10.1.12.2
user@R4> ping 10.1.12.2
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=253 time=13.528 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=253 time=0.873 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=253 time=32.145 ms
64 bytes from 10.1.12.2: icmp_seq=3 ttl=253 time=0.921 ms
64 bytes from 10.1.12.2: icmp_seq=4 ttl=253 time=0.899 ms
^C
--- 10.1.12.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.873/9.673/32.145/12.255 ms
```

You can also issue the `traceroute` command to verify that traffic to 10.1.12.2 travels over the IPSec tunnel between Router 3 and Router 2. Notice that the second hop does not reference 10.1.15.1—the physical interface on Router 2. Instead, the loopback address of 10.0.0.2 on Router 2 appears as the second hop. This indicates that the IPSec tunnel is operating correctly.

```
user@R4> traceroute 10.1.12.2
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1 10.1.56.1 (10.1.56.1) 0.681 ms 0.624 ms 0.547 ms
 2 10.0.0.2 (10.0.0.2) 0.800 ms 0.770 ms 0.737 ms
 3 10.1.12.2 (10.1.12.2) 0.793 ms 0.742 ms 0.716 ms
```

Example: Adaptive Services PIC IKE Dynamic SA Configuration

Figure 52: Adaptive Services PIC IKE Dynamic SA Topology Diagram

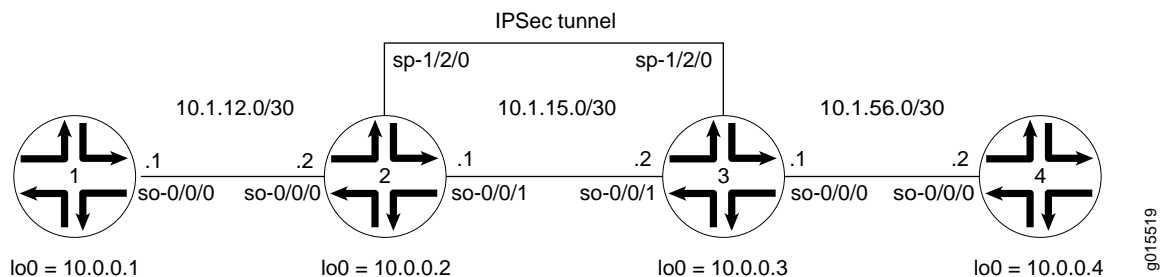


Figure 52 shows the same IPsec topology as seen in the Adaptive Services PIC manual SA example. However, this configuration requires Routers 2 and 3 to establish an IPsec tunnel using an IKE dynamic SA, enhanced authentication, and stronger encryption. Routers 1 and 4 continue to provide basic connectivity and are used to verify that the IPsec tunnel is operational.



NOTE: When you do not specify an IKE proposal, an IPsec proposal, and an IPsec policy on an Adaptive Services PIC, the JUNOS software defaults to the highest level of encryption and authentication. As a result, the default authentication protocol is ESP, the default authentication mode is HMAC-SHA1-96, and the default encryption mode is 3DES-CBC. For more information about default IKE and IPsec policies and proposals on the Adaptive Services PIC, see Table 38 on page 591.

On Router 1, provide basic OSPF connectivity to Router 2.

```
Router 1 [edit]
interfaces {
  so-0/0/0 {
    description "To R2 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.1/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.1;
}
```

```

protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}

```

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional IKE dynamic SA in a rule called `rule-ike` at the [edit ipsec-vpn rule] hierarchy level. Reference this rule in a service set called `service-set-dynamic-BiEspsha3des` at the [edit services service-set] hierarchy level.

Using default values in the Adaptive Services PIC, you do not need to specify an IPSec proposal, IPSec policy, or IKE proposal. However, you do need to configure a preshared key in an IKE policy with the `pre-shared-key` statement at the [edit services ipsec-vpn ike policy *policy-name*] hierarchy level. (For more information about default IKE and IPSec policies and proposals on the Adaptive Services PIC, see Table 38 on page 591.)

To direct traffic into the Adaptive Services PIC and the IPSec tunnel, include match conditions in the `rule-ike` IPSec VPN rule to match inbound traffic from Router 1 that is destined for Router 4. Because the rule is already referenced by the service set, apply the service set to the `so-0/0/1` interface. To count the amount of traffic that enters the IPSec tunnel, configure a firewall filter called `ipsec-tunnel` and apply it to the `sp-1/2/0` interface.

```

Router 2 [edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
      family inet {
        service { # Apply the service set here.
          input {
            service-set service-set-dynamic-BiEspsha3des;
          }
          output {
            service-set service-set-dynamic-BiEspsha3des;
          }
        }
        address 10.1.15.1/30;
      }
    }
  }
}

```

```

sp-1/2/0 {
  services-options {
    syslog {
      host local {
        services info;
      }
    }
  }
  unit 0 {
    family inet {
      filter {
        input ipsec-tunnel; # Apply the firewall filter with the counter here.
      }
    }
  }
}
lo0 {
  unit 0 {
    family inet {
      address 10.0.0.2/32;
    }
  }
}
}
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
}
firewall {
  filter ipsec-tunnel { # Configure a firewall filter to count IPSec traffic here.
    term 1 {
      then {
        count ipsec-tunnel;
        accept;
      }
    }
  }
}
}

```

```

services {
  service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
    interface-service {
      service-interface sp-1/2/0; # Specify an interface to process IPSec.
    }
    ipsec-vpn-options {
      local-gateway 10.1.15.1; # Specify the local IP address of the IPSec tunnel.
    }
    ipsec-vpn-rules rule-ike; # Reference your IPSec VPN rule here.
  }
  ipsec-vpn {
    rule rule-ike { # Define your IPSec VPN rule here.
      term term-ike {
        from {
          source-address {
            10.1.12.0/24;
          }
          destination-address {
            10.1.56.0/24;
          }
        }
        then {
          remote-gateway 10.1.15.2; # The remote IP address of the IPSec tunnel.
          dynamic { # This creates an IKE dynamic SA.
            ike-policy ike-policy-preshared; # Reference your IKE policy here.
          }
        }
      }
      match-direction output; # Specify in which direction the rule should match.
    }
    ike {
      policy ike-policy-preshared { # Define your IKE policy specifications here.
        pre-shared-key ascii-text "$9$KtKWX-YgJHqfVwqfTzCAvWL";
      }
    }
  }
}
## The unencrypted pre-shared key for this example is juniper.
}
} # Using default values, you do not need to specify an IPSec proposal,
} # IPSec policy, or IKE proposal.
}

```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional IKE dynamic SA in a rule called rule-ike at the [edit ipsec-vpn rule] hierarchy level. Reference this rule in a service set called service-set-dynamic-BiEspsha3des at the [edit services service-set] hierarchy level.

Again, use the same default policies and proposals that you used on Router 2. However, remember to configure a preshared key in an IKE policy with the pre-shared-key statement at the [edit services ipsec-vpn ike policy *policy-name*] hierarchy level. The key must match the one you specified on Router 2. (For more information about default IKE and IPSec policies and proposals on the Adaptive Services PIC, see Table 38 on page 591.)

To direct traffic into the Adaptive Services PIC and the IPSec tunnel, include match conditions in the rule-ike IPSec VPN rule to match inbound traffic from Router 4 that is destined for Router 1. Because the rule is already referenced by the service set, apply the service set to the so-0/0/1 interface. To count the amount of traffic that enters the IPSec tunnel, configure a firewall filter called ipsec-tunnel and apply it to the sp-1/2/0 interface.

```

Router 3 [edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R2 so-0/0/1";
    unit 0 {
      family inet {
        service { # Apply the service set here.
          input {
            service-set service-set-dynamic-BiEspsha3des;
          }
          output {
            service-set service-set-dynamic-BiEspsha3des;
          }
        }
        address 10.1.15.2/30;
      }
    }
  }
  sp-1/2/0 {
    services-options {
      syslog {
        host local {
          services info;
        }
      }
    }
  }
}

```

```

    unit 0 {
      family inet {
        filter {
          input ipsec-tunnel; # Apply the firewall filter with the counter here.
        }
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.3/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.3;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
}
firewall {
  filter ipsec-tunnel { # Configure a firewall filter to count IPSec traffic here.
    term 1 {
      then {
        count ipsec-tunnel;
        accept;
      }
    }
  }
}

```

```

services {
  service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
    interface-service {
      service-interface sp-1/2/0; # Specify an interface to process IPSec.
    }
    ipsec-vpn-options {
      local-gateway 10.1.15.2; # Specify the local IP address of the IPSec tunnel.
    }
    ipsec-vpn-rules rule-ike; # Reference your IPSec VPN rule here.
  }
  ipsec-vpn {
    rule rule-ike { # Define your IPSec VPN rule here.
      term term-ike {
        from {
          source-address {
            10.1.56.0/24;
          }
          destination-address {
            10.1.12.0/24;
          }
        }
        then {
          remote-gateway 10.1.15.1; # The remote IP address of the IPSec tunnel.
          dynamic { # This creates an IKE dynamic SA.
            ike-policy ike-policy-preshared; # Reference your IKE policy here.
          }
        }
      }
      match-direction output; # Specify in which direction the rule should match.
    }
    ike {
      policy ike-policy-preshared { # Define your IKE policy specifications here.
        pre-shared-key ascii-text "$9$KtKWX-YgJHqfVwqfTzCAvWL";
      }
    }
  }
}

```

The unencrypted pre-shared key for this example is **juniper**.

On Router 4, provide basic OSPF connectivity to Router 3.

```

Router 4 [edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}

```

Checking Your Work

To verify proper operation of an IKE-based dynamic SA on the Adaptive Services PIC, use the following commands:

```

ping
show services ipsec-vpn ike security-associations (detail)
show services ipsec-vpn ipsec security-associations (detail)
traceroute

```

The following sections show the output of these commands used with the configuration example:

Router 1 on page 641

Router 2 on page 641

Router 3 on page 642

Router 4 on page 643

Router 1

On Router 1, issue a ping command to the so-0/0/0 interface on Router 4 to send traffic across the IPSec tunnel.

```
user@R1> ping 10.1.56.2
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=254 time=1.351 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=254 time=1.187 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=254 time=1.172 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=254 time=1.154 ms
64 bytes from 10.1.56.2: icmp_seq=4 ttl=254 time=1.156 ms
^C
--- 10.1.56.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.154/1.204/1.351/0.074 ms
```

Notice that if you try to ping the loopback address of R4, the operation fails because the address is not part of the match condition in the IPSec VPN IKE rule on Router 2.

```
user@R1> ping 10.0.0.4
PING 10.0.0.4 (10.0.0.4): 56 data bytes
^C
--- 10.0.0.4 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

Router 2

One way to verify that matched traffic is being diverted to the bidirectional IPSec tunnel is to view the firewall filter counter. Before any traffic flows, the ipsec-tunnel firewall filter counter looks like this:

```
user@R2> show firewall filter ipsec-tunnel
Filter: ipsec-tunnel
Counters:
Name          Bytes    Packets
ipsec-tunnel      0         0
```

After you issue the ping command from Router 1 (five packets) to 10.1.56.2, the ipsec-tunnel firewall filter counter looks like this:

```
user@R2> show firewall filter ipsec-tunnel
Filter: ipsec-tunnel
Counters:
Name          Bytes    Packets
ipsec-tunnel  420         5
```

After you issue the ping command from both Router 1 to 10.1.56.2 (five packets) and from Router 4 to 10.1.12.2 (six packets), the ipsec-tunnel firewall filter counter looks like this:

```
user@R2> show firewall filter ipsec-tunnel
Filter: ipsec-tunnel
Counters:
Name          Bytes    Packets
ipsec-tunnel  924        11
```

To verify that the IKE SA negotiation is successful, issue the `show services ipsec-vpn ike security-associations` command.

```
user@R2> show services ipsec-vpn ike security-associations
Remote Address State      Initiator cookie Responder cookie Exchange type
10.1.15.2    Matured      03075bd3a0000003 4bff26a5c7000003 Main
```

To verify that the IPsec security association is active, issue the `show services ipsec-vpn ipsec security-associations detail` command. Notice that the SA contains the default settings inherent in the Adaptive Services PIC, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

```
user@R2> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-dynamic-BiEspsha3des
```

```
Rule: rule-ike, Term: term-ike, Tunnel index: 1
Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
Local identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
```

```
Direction: inbound, SPI: 2666326758, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26863 seconds
Hard lifetime: Expires in 26998 seconds
Anti-replay service: Enabled, Replay window size: 64
```

```
Direction: outbound, SPI: 684772754, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26863 seconds
Hard lifetime: Expires in 26998 seconds
Anti-replay service: Enabled, Replay window size: 64
```

Router 3

View the firewall filter counter to continue verifying that matched traffic is being diverted to the bidirectional IPsec tunnel. After you issue the ping command from Router 1 (five packets) and Router 6 (six packets), the ipsec-tunnel firewall filter counter looks like this:

```
user@R3> show firewall filter ipsec-tunnel
Filter: ipsec-tunnel
Counters:
Name              Bytes      Packets
ipsec-tunnel      924        11
```

To verify that the IKE SA negotiation is successful, issue the `show services ipsec-vpn ike security-associations` command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ike security-associations
Remote Address State      Initiator cookie Responder cookie Exchange type
10.1.15.1    Matured      03075bd3a0000003 4bff26a5c7000003 Main
```

To verify that the IPsec SA is active, issue the `show services ipsec-vpn ipsec security-associations detail` command. To be successful, the SA on Router 3 must contain the same settings you specified on Router 2.

```
user@R3> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-dynamic-BiEspsha3des
```

```
Rule: rule-ike, Term: term-ike, Tunnel index: 1
Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
```

```
Direction: inbound, SPI: 684772754, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26598 seconds
Hard lifetime: Expires in 26688 seconds
Anti-replay service: Enabled, Replay window size: 64
```

```
Direction: outbound, SPI: 2666326758, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 26598 seconds
Hard lifetime: Expires in 26688 seconds
Anti-replay service: Enabled, Replay window size: 64
```

Router 4

On Router 4, issue a ping command to the `so-0/0/0` interface on Router 1 to send traffic across the IPsec tunnel.

```
user@R4> ping 10.1.12.2
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=254 time=1.350 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=254 time=1.161 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=254 time=1.124 ms
64 bytes from 10.1.12.2: icmp_seq=3 ttl=254 time=1.142 ms
64 bytes from 10.1.12.2: icmp_seq=4 ttl=254 time=1.139 ms
64 bytes from 10.1.12.2: icmp_seq=5 ttl=254 time=1.116 ms
^C
--- 10.1.12.2 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.116/1.172/1.350/0.081 ms
```

Example: IKE Dynamic SA Between an Adaptive Services PIC and an ES PIC Configuration

Figure 53: Adaptive Services PIC to ES PIC IKE Dynamic SA Topology Diagram

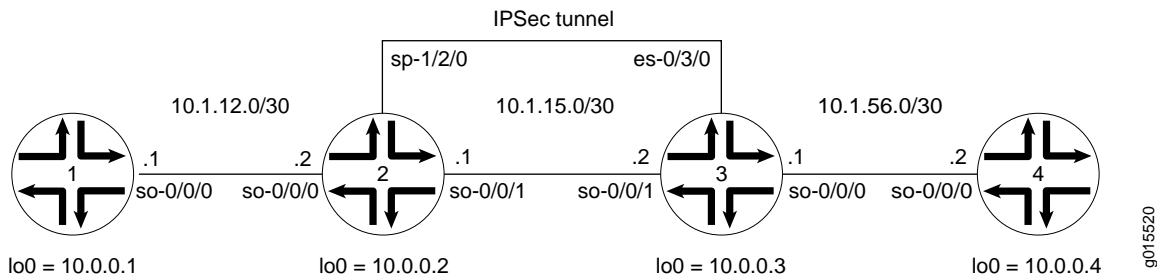


Figure 53 shows a hybrid configuration that allows you to create an IPSec tunnel between the Adaptive Services PIC and the ES PIC. Router 2 contains an Adaptive Services PIC at sp-1/2/0 and Router 3 has an ES PIC at es-0/3/0. To establish an IPSec tunnel using an IKE dynamic SA, the key is to learn the default IKE SA and IPSec SA settings built into the Adaptive Services PIC and configure them explicitly on the ES PIC. Routers 1 and 4 again provide basic connectivity and are used to verify that the IPSec tunnel is operational.

On Router 1, provide basic OSPF connectivity to Router 2.

```

Router 1 [edit]
  interfaces {
    so-0/0/0 {
      description "To R2 so-0/0/0";
      unit 0 {
        family inet {
          address 10.1.12.2/30;
        }
      }
    }
    lo0 {
      unit 0 {
        family inet {
          address 10.0.0.1/32;
        }
      }
    }
  }
  routing-options {
    router-id 10.0.0.1;
  }
  protocols {
    ospf {
      area 0.0.0.0 {
        interface so-0/0/0.0;
        interface lo0.0;
      }
    }
  }
}

```

9015620

On Router 2, enable OSPF as the underlying routing protocol to connect to Routers 1 and 3. Configure a bidirectional IKE dynamic SA in a rule called rule-ike at the [edit ipsec-vpn rule] hierarchy level. Reference this rule in a service set called service-set-dynamic-BiEspsha3des at the [edit services service-set] hierarchy level.

Using default values in the Adaptive Services PIC, you do not need to specify an IPSec proposal, IPSec policy, or IKE proposal. However, you do need to configure a preshared key in an IKE policy with the pre-shared-key statement at the [edit services ipsec-vpn ike policy *policy-name*] hierarchy level. (For more information about default IKE and IPSec policies and proposals on the Adaptive Services PIC, see Table 38 on page 591.)

To direct traffic into the Adaptive Services PIC and the IPSec tunnel, include match conditions in the rule-ike IPSec VPN rule to match inbound traffic from Router 1 that is destined for Router 4. Because the rule is already referenced by the service set, apply the service set to the so-0/0/1 interface. To count the amount of traffic that enters the IPSec tunnel, configure a firewall filter called ipsec-tunnel and apply it to the sp-1/2/0 interface.

```

Router 2 [edit]
interfaces {
  so-0/0/0 {
    description "To R1 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.12.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R3 so-0/0/1";
    unit 0 {
      family inet {
        service { # Apply the service set here.
          input {
            service-set service-set-dynamic-BiEspsha3des;
          }
          output {
            service-set service-set-dynamic-BiEspsha3des;
          }
        }
        address 10.1.15.1/30;
      }
    }
  }
  sp-1/2/0 {
    services-options {
      syslog {
        host local {
          services info;
        }
      }
    }
  }
}

```

```

    unit 0 {
      family inet {
        filter {
          input ipsec-tunnel; # Apply the firewall filter with the counter here.
        }
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.2/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.2;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface so-0/0/1.0;
      interface lo0.0;
    }
  }
}
firewall {
  filter ipsec-tunnel { # Configure a firewall filter to count IPSec traffic here.
    term 1 {
      then {
        count ipsec-tunnel;
        accept;
      }
    }
  }
}

```

```

services {
  service-set service-set-dynamic-BiEspsha3des { # Define your service set here.
    interface-service {
      service-interface sp-1/2/0; # Specify an interface to process IPSec.
    }
    ipsec-vpn-options {
      local-gateway 10.1.15.1; # Specify the local IP address of the IPSec tunnel.
    }
    ipsec-vpn-rules rule-ike; # Reference your IPSec VPN rule here.
  }
  ipsec-vpn {
    rule rule-ike { # Define your IPSec VPN rule here.
      term term-ike {
        from {
          source-address {
            10.1.12.0/24;
          }
          destination-address {
            10.1.56.0/24;
          }
        }
        then {
          remote-gateway 10.1.15.2; # The remote IP address of the IPSec tunnel.
          dynamic { # This creates an IKE dynamic SA.
            ike-policy ike-policy-preshared; # Reference your IKE proposal here.
          }
        }
      }
      match-direction output; # Specify in which direction the rule should match.
    }
    ike {
      policy ike-policy-preshared { # Define your IKE policy specifications here.
        pre-shared-key ascii-text "$9$KtKWX-YgJHqfVwqfTzCAvWL";
      }
    }
  }
}
## The unencrypted pre-shared key for this example is juniper.
}
} # Using default values, you do not need to specify an IPSec proposal,
} # IPSec policy, or IKE proposal.
}

```

On Router 3, enable OSPF as the underlying routing protocol to connect to Routers 2 and 4. Configure a bidirectional IKE dynamic SA called sa-dynamic at the [edit security ipsec security-association] hierarchy level. To allow the ES PIC to communicate with the IKE dynamic SA established on Router 2, you must explicitly configure the same policies and proposals on the ES PIC that are available by default on the Adaptive Services PIC. (For more information about default IKE and IPSec policies and proposals on the Adaptive Services PIC, see Table 38 on page 591.)

For your IKE policy and proposal, use preshared keys for the authentication method, SHA-1 for the authentication algorithm, 3DES-CBC for encryption, group 2 for the Diffie-Hellman group, main mode, 3600 seconds for the lifetime, and a preshared key of juniper for the initial IKE negotiation. For your IPSec policy and proposal, use ESP for the protocol, HMAC-SHA1-96 for authentication, 3DES-CBC for encryption, 28800 seconds for the lifetime, and group 2 for the PFS group.

To direct traffic into the ES PIC and the IPSec tunnel, create two firewall filters. The es-traffic filter matches inbound traffic from Router 4 destined for Router 1, while the es-return filter matches the return path from Router 1 to Router 4. Apply the es-traffic filter to the so-0/0/0 interface, then apply both the es-return filter and the sa-dynamic SA to the es-0/3/0 interface.

```

Router 3 [edit]
interfaces {
  so-0/0/0 {
    description "To R4 so-0/0/0";
    unit 0 {
      family inet {
        filter {
          input es-traffic; # Apply a filter that sends traffic to the IPSec tunnel here.
        }
        address 10.1.56.1/30;
      }
    }
  }
  so-0/0/1 {
    description "To R2 so-0/0/1";
    unit 0 {
      family inet {
        address 10.1.15.2/30;
      }
    }
  }
  es-0/3/0 {
    unit 0 {
      tunnel { # Specify the IPSec tunnel endpoints here.
        source 10.1.15.2;
        destination 10.1.15.1;
      }
      family inet {
        ipsec-sa sa-dynamic; # Apply the IKE dynamic SA here.
        filter {
          input es-return; # Apply the filter that matches return IPSec traffic here.
        }
      }
    }
  }
}

```

```

    }
    lo0 {
        unit 0 {
            family inet {
                address 10.0.0.3/32;
            }
        }
    }
}
routing-options {
    router-id 10.0.0.3;
}
protocols {
    ospf {
        area 0.0.0.0 {
            interface so-0/0/0.0;
            interface so-0/0/1.0;
            interface lo0.0;
        }
    }
}
security {
    ipsec {
        proposal es-ipsec-proposal { # Define your IPSec proposal specifications here.
            protocol esp;
            authentication-algorithm hmac-sha1-96;
            encryption-algorithm 3des-cbc;
            lifetime-seconds 28800;
        }
        policy es-ipsec-policy { # Define your IPSec policy specifications here.
            perfect-forward-secrecy {
                keys group2;
            }
            proposals es-ipsec-proposal; # Reference the IPSec proposal here.
        }
        security-association sa-dynamic { # Define your IKE dynamic SA here.
            dynamic {
                ipsec-policy es-ipsec-policy; # Reference the IPSec policy here.
            }
        }
    }
}
ike {
    proposal es-ike-proposal { # Define your IKE proposal specifications here.
        authentication-method pre-shared-keys;
        dh-group group2;
        authentication-algorithm sha1;
        encryption-algorithm 3des-cbc;
        lifetime-seconds 3600;
    }
    policy 10.1.15.1 { # Define your IKE policy specifications here.
        mode main;
        proposals es-ike-proposal; # Reference the IKE proposal here.
        pre-shared-key ascii-text "$9$TF6ABlcvWxp0WxNdg4QFn";
    }
}
## The unencrypted pre-shared key for this example is juniper.
}
}

```

```

}
firewall {
  filter es-traffic { # Define a filter that sends traffic to the IPSec tunnel here.
    term to-es {
      from {
        source-address {
          10.1.56.0/24;
        }
        destination-address {
          10.1.12.0/24;
        }
      }
      then {
        count ipsec-tunnel;
        ipsec-sa sa-dynamic;
      }
    }
    term other {
      then accept;
    }
  }
  filter es-return { # Define a filter that matches return IPSec traffic here.
    term return {
      from {
        source-address {
          10.1.12.0/24;
        }
        destination-address {
          10.1.56.0/24;
        }
      }
      then accept;
    }
  }
}

```

On Router 4, provide basic OSPF connectivity to Router 3.

```

Router 4 [edit]
interfaces {
  so-0/0/0 {
    description "To R3 so-0/0/0";
    unit 0 {
      family inet {
        address 10.1.56.2/30;
      }
    }
  }
  lo0 {
    unit 0 {
      family inet {
        address 10.0.0.4/32;
      }
    }
  }
}
routing-options {
  router-id 10.0.0.4;
}
protocols {
  ospf {
    area 0.0.0.0 {
      interface so-0/0/0.0;
      interface lo0.0;
    }
  }
}

```

Checking Your Work

To verify proper operation of an IKE-based dynamic SA on the Adaptive Services PIC, use the following commands:

```

ping
show services ipsec-vpn ike security-associations (detail)
show services ipsec-vpn ipsec security-associations (detail)
traceroute

```

To verify proper operation of an IKE-based dynamic SA on the ES PIC, use the following commands:

```

ping
show ike security-associations (detail)
show ipsec security-associations (detail)
traceroute

```

The following sections show the output of these commands used with the configuration example:

Router 1 on page 652

Router 2 on page 653

Router 3 on page 654

Router 4 on page 656

Router 1

On Router 1, issue a ping command to the so-0/0/0 interface of Router 4 to send traffic across the IPSec tunnel.

```
user@R1> ping 10.1.56.2
PING 10.1.56.2 (10.1.56.2): 56 data bytes
64 bytes from 10.1.56.2: icmp_seq=0 ttl=253 time=1.172 ms
64 bytes from 10.1.56.2: icmp_seq=1 ttl=253 time=1.020 ms
64 bytes from 10.1.56.2: icmp_seq=2 ttl=253 time=0.998 ms
64 bytes from 10.1.56.2: icmp_seq=3 ttl=253 time=1.037 ms
^C
--- 10.1.56.2 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max/stddev = 0.998/1.057/1.172/0.068 ms
```

You can also issue the traceroute command to verify that traffic to 10.1.56.2 travels over the IPSec tunnel between Router 2 and Router 3. Notice that the traced path does not reference 10.1.15.2—the physical interface on Router 3. Instead, traffic arriving at Router 2 is immediately filtered into the IPSec tunnel and the path is listed as unknown with the *** notation. This indicates that the IPSec tunnel is operating correctly.

```
user@R1> traceroute 10.1.56.2
traceroute to 10.1.56.2 (10.1.56.2), 30 hops max, 40 byte packets
 1 ***
 2 10.1.56.2 (10.1.56.2) 1.045 ms 0.915 ms 0.850 ms
```

Router 2

One way to verify that matched traffic is being diverted to the bidirectional IPSec tunnel is to view the firewall filter counter. Before any traffic flows, the ipsec-tunnel firewall filter counter looks like this:

```
user@R2> show firewall filter ipsec-tunnel
Filter: ipsec-tunnel
Counters:
Name                Bytes    Packets
ipsec-tunnel        0         0
```

After you issue the ping command from Router 1 (four packets) to 10.1.56.2, the ipsec-tunnel firewall filter counter looks like this:

```
user@R2> show firewall filter ipsec-tunnel
Filter: ipsec-tunnel
Counters:
Name                Bytes    Packets
ipsec-tunnel        336       4
```

After you issue the ping command from both Router 1 to 10.1.56.2 (four packets) and from Router 4 to 10.1.12.2 (six packets), the ipsec-tunnel firewall filter counter looks like this:

```
user@R2> show firewall filter ipsec-tunnel
Filter: es-traffic
Counters:
Name                Bytes    Packets
ipsec-tunnel        840      10
```

To verify that the IKE SA negotiation is successful, issue the show services ipsec-vpn ike security-associations detail command. Notice that the SA contains the default IKE settings inherent in the Adaptive Services PIC, such as SHA-1 for the authentication algorithm and 3DES-CBC for the encryption algorithm.

```
user@R2> show services ipsec-vpn ike security-associations detail
IKE peer 10.1.15.2
  Role: Responder, State: Matured
  Initiator cookie: c8e1e4c0da000040, Responder cookie: 4fbaa5184e000044
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.1.15.1:500, Remote: 10.1.15.2:500
  Lifetime: Expires in 3535 seconds
  Algorithms:
    Authentication    : sha1
    Encryption        : 3des-cbc
    Pseudo random function: hmac-sha1
  Traffic statistics:
    Input bytes :      840
    Output bytes :     756
    Input packets:      5
    Output packets:     4
  Flags: Caller notification sent
  IPSec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 0
```

To verify that the IPsec security association is active, issue the `show services ipsec-vpn ipsec security-associations detail` command. Notice that the SA contains the default settings inherent in the Adaptive Services PIC, such as ESP for the protocol and HMAC-SHA1-96 for the authentication algorithm.

```
user@R2> show services ipsec-vpn ipsec security-associations detail
Service set: service-set-dynamic-BiEspsha3des
```

```
Rule: rule-ike, Term: term-ike, Tunnel index: 1
Local gateway: 10.1.15.1, Remote gateway: 10.1.15.2
Local identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
```

```
Direction: inbound, SPI: 407204513, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 24546 seconds
Hard lifetime: Expires in 24636 seconds
Anti-replay service: Disabled
```

```
Direction: outbound, SPI: 2957235894, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 24546 seconds
Hard lifetime: Expires in 24636 seconds
Anti-replay service: Disabled
```

Router 3

View the firewall filter counter to continue verifying that matched traffic is being diverted to the bidirectional IPsec tunnel. After you issue the ping command from Router 1 (four packets), the es-traffic firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name           Bytes      Packets
ipsec-tunnel   336        4
```

After you issue the ping command from both Router 1 (four packets) and Router 4 (six packets), the es-traffic firewall filter counter looks like this:

```
user@R3> show firewall filter es-traffic
Filter: es-traffic
Counters:
Name           Bytes      Packets
ipsec-tunnel   840       10
```

To verify the success of the IKE security association on the ES PIC, issue the show ike security-associations detail command. Notice that the IKE SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ike security-associations detail
IKE peer 10.1.15.1
  Role: Initiator, State: Matured
  Initiator cookie: c8e1e4c0da000040, Responder cookie: 4fbaa5184e000044
  Exchange type: Main, Authentication method: Pre-shared-keys
  Local: 10.1.15.2:500, Remote: 10.1.15.1:500
  Lifetime: Expires in 3441 seconds
  Algorithms:
    Authentication      : sha1
    Encryption          : 3des-cbc
    Pseudo random function: hmac-sha1
  Traffic statistics:
    Input bytes :      756
    Output bytes :      840
    Input packets:      4
    Output packets:     5
  Flags: Caller notification sent
  IPsec security associations: 1 created, 0 deleted
  Phase 2 negotiations in progress: 0
```

To verify that the IPsec security association is active, issue the show ipsec security-associations detail command. Notice that the IPsec SA on Router 3 contains the same settings you specified on Router 2.

```
user@R3> show ipsec security-associations detail
Security association: sa-dynamic, Interface family: Up

Local gateway: 10.1.15.2, Remote gateway: 10.1.15.1
Local identity: ipv4_subnet(any:0,[0..7]=10.1.56.0/24)
Remote identity: ipv4_subnet(any:0,[0..7]=10.1.12.0/24)

Direction: inbound, SPI: 2957235894, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 28555 seconds
Hard lifetime: Expires in 28690 seconds
Anti-replay service: Disabled

Direction: outbound, SPI: 407204513, AUX-SPI: 0
Mode: tunnel, Type: dynamic, State: Installed
Protocol: ESP, Authentication: hmac-sha1-96, Encryption: 3des-cbc
Soft lifetime: Expires in 28555 seconds
Hard lifetime: Expires in 28690 seconds
Anti-replay service: Disabled
```

Router 4

On Router 4, issue a ping command to the so-0/0/0 interface on Router 1 to send traffic across the IPSec tunnel.

```
user@R4> ping 10.1.12.2
PING 10.1.12.2 (10.1.12.2): 56 data bytes
64 bytes from 10.1.12.2: icmp_seq=0 ttl=254 time=1.350 ms
64 bytes from 10.1.12.2: icmp_seq=1 ttl=254 time=1.161 ms
64 bytes from 10.1.12.2: icmp_seq=2 ttl=254 time=1.124 ms
64 bytes from 10.1.12.2: icmp_seq=3 ttl=254 time=1.142 ms
64 bytes from 10.1.12.2: icmp_seq=4 ttl=254 time=1.139 ms
64 bytes from 10.1.12.2: icmp_seq=5 ttl=254 time=1.116 ms
^C
--- 10.1.12.2 ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max/stddev = 1.116/1.172/1.350/0.081 ms
```

Again, the traceroute command verifies that traffic to 10.1.12.2 travels over the IPSec tunnel between Router 3 and Router 2. Notice that the second hop does not reference 10.1.15.1—the physical interface on Router 2. Instead, the second hop is listed as unknown with the *** notation. This indicates that the IPSec tunnel is operating correctly.

```
user@R4> traceroute 10.1.12.2
traceroute to 10.1.12.2 (10.1.12.2), 30 hops max, 40 byte packets
 1 10.1.56.1 (10.1.56.1) 3.561 ms 0.613 ms 0.558 ms
 2 * * *
 3 10.1.12.2 (10.1.12.2) 1.073 ms 0.862 ms 0.818 ms
```

For More Information

For additional information about IPSec, see the following:

JUNOS System Basics Configuration Guide

JUNOS Services Interfaces Configuration Guide

R. Rivest, *The MD5 Message-Digest Algorithm* , RFC 1321, April 1992

H. Krawczyk, M. Bellare, and R. Canetti, *HMAC: Keyed-Hashing for Message Authentication* , RFC 2104, February 1997

R. Atkinson and S. Kent, *Security Architecture for the Internet Protocol*, RFC 2401, November 1998

R. Atkinson and S. Kent, *IP Authentication Header* , RFC 2402, November 1998

C. Madson and N. Doraswamy, *The ESP DES-CBC Cipher Algorithm With Explicit IV*, RFC 2405, November 1998

R. Atkinson and S. Kent, *IP Encapsulating Security Payload (ESP)* , RFC 2406, November 1998

D. Maughan, et. al., *Internet Security Association and Key Management Protocol (ISAKMP)*, RFC 2408, November 1998

D. Carrel and D. Harkins, *The Internet Key Exchange (IKE)* , RFC 2409, November 1998

D. Eastlake and P. Jones, *US Secure Hash Algorithm 1 (SHA1)* , RFC 3174, September 2001

U.S. Department of Commerce/National Institute of Standards and Technology, *Data Encryption Standard*, Federal Information Processing Standards (FIPS) Publication 46-3, October 1999,
<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>
 (includes information about DES and 3DES)

Revision History

2 February 2005—Document converted to Feature Guide format, thoroughly revised, and enhanced with updated examples, JUNOS Release 7.1R1. Richard Hendricks.

07 March 2002—Initial Quick Start Guide written. Tony Sinopoli.

