Example: ES PIC IKE Dynamic SA Configuration

Figure 1: ES PIC IKE Dynamic SA Topology Diagram

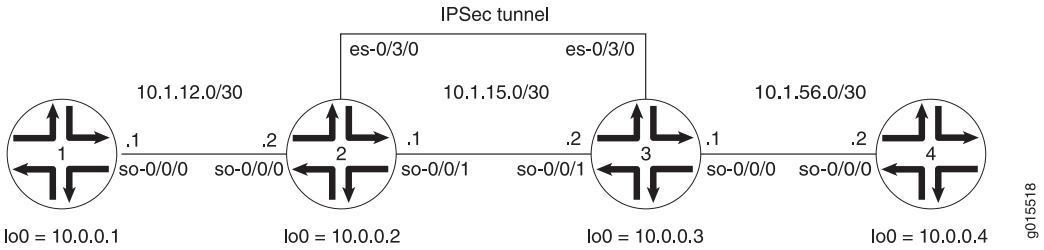

Figure 1 shows the same IPSec topology as seen in the ES PIC manual SA example. However, this time the configuration requires Routers 2 and 3 to establish an IPSec tunnel using an IKE dynamic SA, enhanced authentication, and stronger encryption. Routers 1 and 4 continue to provide basic connectivity 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, whereas 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, and 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 dynamic SA here.
            filter {
               input es-return; # Apply the filter that matches return IPSec traffic here.
            }
         }
      }
   }
   lo0 {
      unit 0 {
         family inet {
            address 10.0.0.2/32;
         }
      }
```

```
    }
}
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 {
        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 dynamic SA here.
            mode tunnel;
            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 10.1.15.2 { # Define your IKE policy specifications here.
            mode main;
            proposals es-ike-proposal; # Reference the IKE proposal here.
            pre-shared-key ascii-text "$9$TF6ABIcvWxp0WxNdg4QFn";
            ## The unencrypted preshared 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 {
```

```
                10.1.12.0/24;
            }
            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, whereas 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 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 dynamic SA here.
            mode tunnel;
            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 "$9$TF6ABIcvWxp0WxNdg4QFn";
            ## The unencrypted preshared 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;
      }
   }
}
```

Verifying 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 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: b5dbdfe2f9000000, 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: b5dbdfe2f9000000, 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
```

Published: 2010-04-15