



Converting Private Link to IPsec

This appendix is intended for the Private Link users who are migrating from the PIX Firewall Private Link feature to the IPsec feature. This section describes the main differences between the Private Link commands and the corresponding IPsec commands, and provides a procedure for how to convert a Private Link configuration into an IPsec configuration using IKE to establish security associations.

Private Link is no longer supported in the PIX Firewall starting with version 5.0. It is supported in version 4. The Private Link feature allows Virtual Private Networks (VPNs) to be established between PIX Firewalls that are connected to the same public network, such as the Internet. It enables incoming Private Link packets to bypass the Network Address Translation (NAT) and Adaptive Security Algorithm (ASA) features and terminate on the corresponding sending interface of the destination network. A sending interface is the interface from which the IPsec packet was sent from. For example, IPsec packets sent from a perimeter interface from one network would be terminated at the equivalent perimeter interface at the destination network.

The PIX Firewall currently can simulate the Private Link inside termination with the use of the **sysopt ipsec pl-compatible** command, but the termination on the inside interface is not a true termination. The use of the **sysopt ipsec pl-compatible** command allows IPsec packets to bypass the NAT and ASA features, and enables incoming IPsec packets to terminate on the inside interface only after initially terminating on the outside interface.

See the **sysopt** command in the *Cisco PIX Firewall Command Reference* for more information regarding the **sysopt ipsec pl-compatible** command.

This section contains the following topics:

- [Basic Difference between Private Link and IPsec](#)
- [Private Link Versus IPsec Commands](#)
- [Private Link to IPsec Conversion](#)

Basic Difference between Private Link and IPsec

IPsec is a more comprehensive feature set than Private Link and the main difference between Private Link and IPsec is that a Private Link tunnel begins on the receiving interface and ends on the sending interface, while an IPsec tunnel begins on the sending interface and terminates on the receiving interface.

Private Link Versus IPSec Commands

This section contains the following topics:

- [Link](#)
- [Linkpath](#)
- [Age](#)

[Table F-1](#) outlines the mapping of the core Private Link commands with the corresponding IPSec commands. A description of each command follows.

Table F-1 Mapping of Private Link Commands with IPSec Commands

Private Link Commands	IPSec Commands
None	sysopt ipsec pl-compatible
link (<i>inside</i>) <i>remote_peer_ip</i> <i>key_id</i> <i>key</i>	<ol style="list-style-type: none"> 1. isakmp policy <i>priority</i> authentication <i>pre-share</i> 2. isakmp key <i>keystring</i> address <i>peer-address</i> 3. crypto map <i>map-name</i> interface <i>interface-name</i>
link <i>remote_peer_ip</i> md5	<ol style="list-style-type: none"> 1. crypto ipsec transform-set <i>transform-set-name</i> <i>esp-des</i> <i>ah-md5-hmac</i> 2. crypto map <i>map-name</i> <i>seq-num</i> set transform-set <i>transform-set-name</i>
linkpath <i>remote_network_ip</i> <i>remote_netmask</i> <i>remote_peer_ip</i>	<ol style="list-style-type: none"> 1. access-list <i>access-list-name</i> permit <i>ip</i> <i>any</i> <i>remote_network_ip</i> <i>remote_netmask</i> 2. crypto map <i>map-name</i> <i>seq-num</i> match address <i>access-list-name</i> 3. crypto map <i>map-name</i> <i>seq-num</i> set peer <i>ip-address</i>
age <i>minutes</i>	crypto ipsec security-association lifetime <i>seconds</i> <i>seconds</i>

For more information about the IPSec-related commands listed in [Table F-1](#), refer to the following command pages in the *Cisco PIX Firewall Command Reference*:

- **access-list**
- **crypto ipsec**
- **crypto map**
- **isakmp**
- **sysopt**

Link

The **link** command creates an encrypted path between Private Link-equipped PIX Firewall units. This command also enables Private Link to associate the shared private keys between the local host and a remote peer. The **isakmp key** command in IPsec enables the local host to associate a shared key with a remote peer.



Note

Private Link uses up to seven shared keys between two hosts and rotates among the seven keys. ISAKMP uses only one shared key between any two hosts to authenticate and dynamically negotiate other keys to protect the communication as necessary.

The **link** command allows for the configuration of per packet authentication protection. In IPsec, the analogous protection is provided by the transform-set combination of ah-md5-hmac or esp-md5-hmac. You configure a transform set using the **crypto ipsec transform-set** command. See the **set transform-set** command in the *Cisco PIX Firewall Command Reference* for more information regarding this command.

Example F-1 defines two transform sets and specifies that they can both be used within a crypto map entry. This example applies only when IKE is used to establish security associations. With crypto maps used for manually established security associations, only one transform set can be included in a given crypto map entry.

Example F-1 Configuring Transform Sets

```
crypto ipsec transform-set my_t_set1 ah-md5-hmac
crypto ipsec transform-set my_t_set2 ah-md5-hmac esp-md5-hmac
crypto map mymap 10 ipsec-isakmp
match address 101
set transform-set my_t_set1 my_t_set2
set peer 10.0.0.1
set peer 10.0.0.2
```

In this example, when traffic matches access list 101, the security association can use either transform set **my_t_set1** (first priority) or **my_t_set2** (second priority) depending on the transform set that matches the transform set on the remote peer.

Linkpath

The **linkpath** command identifies the internal and external network interfaces on the remote peer running Private Link. The linkpath address selectors are used to select inbound traffic at the local, internal interface to encrypt and tunnel to the remote peer. In the reverse direction, the linkpath address selectors are used to decrypt outbound traffic, which originated from the remote peer, at the internal interface.

The PIX Firewall can have two or more network interfaces. For any pair of interfaces, one of the interfaces is the local, or internal interface, and one is the outside interface. The relative security level of the interface defines whether it is the local or outside interface; that is, the interface with the higher security level is the local interface, while the interface with the lower security level is the outside interface. For example, a perimeter interface with a security level of 70 is the local interface relative to another perimeter interface with a security level of 40.

The **linkpath** command identifies the internal and external network interfaces on the remote peer running Private Link. The **linkpath** command address selectors are used to select inbound traffic at the inside interface to encrypt and tunnel to the remote peer. In the reverse direction, the **linkpath** command address selectors are used to decrypt outbound traffic, which originated from the remote peer, at the inside interface.

In IPSec, the **access-list** command statement address selectors in the crypto map are used to select outbound traffic from the internal interface to encrypt and tunnel to the remote peer. In the reverse direction, the **access-list** command statement address selectors are used to decrypt inbound traffic, which originated from the remote peer, at the outside interface.

Use the following steps to convert from a linkpath tunnel into an IPSec tunnel. These steps are included within "[Private Link to IPSec Conversion](#)."

-
- Step 1** Define an **access-list** command statement that has the same address selectors as your **linkpath** command statement. ([Step 6](#) in "[Private Link to IPSec Conversion](#).")
 - Step 2** Associate the defined **access-list** command statement with a crypto map entry. ([Step 7](#) in "[Private Link to IPSec Conversion](#).")
 - Step 3** Associate the linkpath remote peer as the crypto map peer. ([Step 10](#) in "[Private Link to IPSec Conversion](#).")
-

Age

Private Link selects the next shared key in a "round-robin" method. The **age** command is used to define the number of minutes a current shared key is used before the rotation.

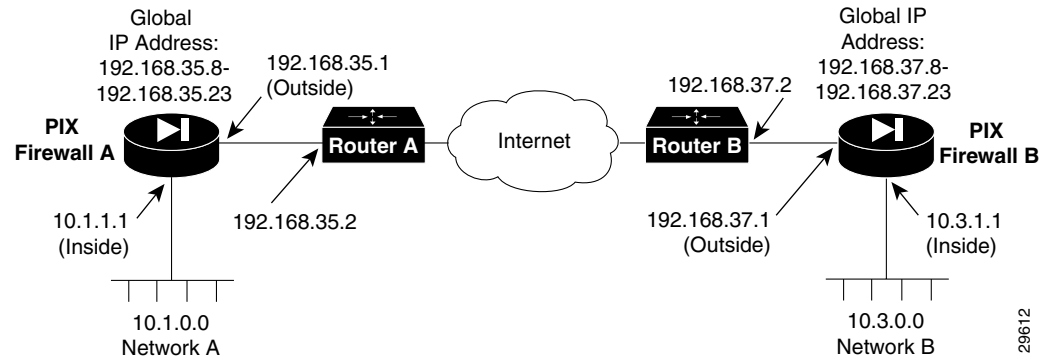
In IPSec, the **crypto ipsec security-association lifetime seconds** command is used to define the duration the current shared key and the security association are used before their set time expires.

Private Link to IPSec Conversion

This section provides the steps to convert your Private Link configuration into an IPSec configuration. An example of a Private Link configuration between two PIX Firewall units is provided for reference.

Figure F-1 shows the Private Link network diagram example to which to refer in this section.

Figure F-1 Example Private Link Network Diagram



The Private Link network diagram shown in Figure F-1 corresponds to the following configurations.

On PIX Firewall A, the Private Link configuration is as follows:

```
link 192.168.37.1 1 fadebacfadebac
link 192.168.37.1 2 bacfadefadebac
link 192.168.37.1 3 baabaaafadebac
link 192.168.37.1 4 beebeeefadebac
linkpath 10.3.0.0 255.255.255.0 192.168.37.1
```

On PIX Firewall B, the Private Link configuration is as follows:

```
link 192.168.35.1 1 fadebacfadebac
link 192.168.35.1 2 bacfadefadebac
link 192.168.35.1 3 baabaaafadebac
link 192.168.35.1 4 beebeeefadebac
linkpath 10.1.0.0 255.255.255.0 192.168.35.1
```

In this configuration, the **link** command specifies 192.168.35.1 as the external network interface IP address of PIX Firewall B, and 192.168.37.1 as the external network interface IP address of PIX Firewall A. The key IDs are 1 through 4. The four keys to be shared between the two PIX Firewall units are fadebacfadebac, bacfadefadebac, baabaaafadebac, and beebeeefadebac.

The **linkpath** command identifies the internal and external network interfaces belonging to the remote peer. So on the PIX Firewall A, PIX Firewall B's internal network interface IP address of 10.3.0.0 with a netmask of 255.255.255.0 and its external network interface IP address of 192.168.37.1 is set. On PIX Firewall B, PIX Firewall A's internal network interface IP address of 10.1.0.0 with a netmask of 255.255.255.0 and its external network interface IP address of 192.168.35.1 is set.

Follow these steps to convert your Private Link configuration to an IPsec configuration where IKE is used to establish security associations. Perform your configuration on each PIX Firewall:

Step 1 Allow incoming packets to terminate on the inside interface.

For example:

PIX Firewall A:

```
sysopt ipsec pl-compatible
```

PIX Firewall B:

```
sysopt ipsec pl-compatible
```

- Step 2** Specify that a pre-shared key will be used between PIX Firewall A and PIX Firewall B for authentication.

PIX Firewall A:

```
isakmp policy 10 authentication pre-share
```

PIX Firewall B:

```
isakmp policy 10 authentication pre-share
```

- Step 3** Specify a pre-shared key that PIX Firewall A and PIX Firewall B will share.

For example:

PIX Firewall A:

```
isakmp key fadebacfadebac address 192.168.37.1
```

PIX Firewall B:

```
isakmp key fadebacfadebac address 192.168.35.1
```

- Step 4** Define a crypto map entry that uses IKE to establish security associations.

For example:

PIX Firewall A:

```
crypto map Firewall-A 10 ipsec-isakmp
```

PIX Firewall B:

```
crypto map Firewall-B 10 ipsec-isakmp
```

- Step 5** Apply the crypto map set to the interface through which IPsec traffic will flow.

For example:

PIX Firewall A:

```
crypto map Firewall-A interface outside
```

PIX Firewall B:

```
crypto map Firewall-B interface outside
```

- Step 6** Create an access list to define the traffic to protect. Use the same address selectors used in your **linkpath** command statement.

For example:

PIX Firewall A:

```
access-list linkpath-aclA permit ip any 10.3.0.0 255.255.255.0
```

PIX Firewall B:

```
access-list linkpath-aclB permit ip any 10.1.0.0 255.255.255.0
```

- Step 7** Assign the access list to the crypto map entry you defined.

For example:

PIX Firewall A:

```
crypto map Firewall-A 10 match address linkpath-aclA
```

PIX Firewall B:

```
crypto map Firewall-B 10 match address linkpath-aclB
```

- Step 8** Configure the transform set that defines how the traffic will be protected. Use either esp-des ah-md5-hmac or esp-md5-hmac. Either one provides the analogous Private Link standard encryption and authentication protection.

For example:

PIX Firewall A:

```
crypto ipsec transform-set private-link-base esp-des ah-md5-hmac
```

PIX Firewall B:

```
crypto ipsec transform-set private-link-base esp-des ah-md5-hmac
```

- Step 9** Specify the transform set to be used with the crypto map entry.

For example:

PIX Firewall A:

```
crypto map Firewall-A 10 set transform-set private-link-base
```

PIX Firewall B:

```
crypto map Firewall-B 10 set transform-set private-link-base
```

- Step 10** Specify the remote peer to which the IPsec protected traffic can be forwarded. Specify the remote peer specified in your **linkpath** statement.

For example:

PIX Firewall A:

```
crypto map Firewall-A 10 set peer 192.168.37.1
```

PIX Firewall B:

```
crypto map Firewall-B 10 set peer 192.168.35.1
```

- Step 11** Apply the crypto map set to an interface through which IPsec traffic will flow.

- Step 12** For example:

PIX Firewall A:

```
crypto map Firewall-A interface outside
```

PIX Firewall B:

```
crypto map Firewall-B interface outside
```

