Building Basic IPSec VPN Tunnels

The following sections show how to use CLI commands and ASDM to configure LAN-to-LAN and remote access tunnels, and use preshared keys or digital certificates to authenticate them:

Note ASDM comes with a complete online-help system. For field definitions on any panel, click **Help**.

For the complete syntax of the commands used in this chapter, see *Cisco Security Appliance Command Reference*.

Enrolling for Digital Certificates

This section describes how to enroll for a digital certificate using CLI commands and ASDM. Once enrolled, you can use the certificate to authenticate VPN LAN-to-LAN tunnels and remote access tunnels. If you intend to use only preshared keys to authenticate, you do not need to read this section.

Key Pairs

Each peer has a key pair containing both a public and a private key. These keys act as complements; any communication encrypted with one can be decrypted with the other.

Key pairs can be either RSA keys or DSA keys. Support for these two types of keys differs as follows:

- DSA keys cannot be used for SSH or SSL. To enable SSH or SSL access to a security appliance, use RSA keys.
- SCEP enrollment is only supported for the certification of RSA keys. If you use DSA keys, enrollment must be performed manually.
- For the purposes of generating keys, the maximum key modulus for RSA keys is 2048, and the maximum key modulus for DSA keys is 1024. The default size for either is 1024 bits.
- For signature operations, the supported maximum key sizes are 4096 bits for RSA keys and 1024 bits for DSA keys.

- You can generate a *general purpose* RSA key pair used for both signing and encryption, or *usage* RSA key pairs separated for each respective purpose, thus requiring two certificates for the corresponding identity. The default setting is general purpose. This topic does not apply to a DSA key pair because it is only for signing.

To configure a key pair for a certificate, you specify the labels to identify the key pair to be generated. The following sections show how to generate an RSA key pair with a default label using the CLI and a specified label using ASDM, and use the default settings for the other parameters.

Overview of Configuration Procedure

Enroll with a CA and get an identity certificate for authenticating tunnels as follows:

Note This example shows automatic (SCEP) enrollment.

1. Create a key pair for the identity certificate. The key pair can be either RSA or DSA. However, for automatic enrollment, you must use RSA keys. The instructions in the sections that follow show how to generate an RSA key pair.
2. Create a trustpoint. The name of the trustpoint in this example is newmsroot.
3. Configure an enrollment URL. The URL this example uses is http://10.20.30.40/certsrv/mscep/mscep.dll.
4. Authenticate the CA.
5. Enroll with the CA, which gets an identity certificate onto the ASA.

Using CLI Commands

You can enter the **show crypto key mypubkey DSA** or **show crypto key mypubkey RSA** command to display the current, operational key pairs.

The complete syntax of the CLI command to generate the key pair is as follows:

crypto key generate rsa [**usage-keys** | **general-keys**] [**label** *key-pair-label*] [**modulus** *size*]

For example, in global configuration mode, enter the following command to generate an RSA key pair with the default name <Default-RSA-Key>:

```
hostname(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
```

Using ASDM

Generate an RSA key pair using ASDM, as follows:

Step 1 Under the **Configuration > Properties > Certificate > Key Pair** panel, click **Add**.

Step 2 Configure the information in the **Add Key Pair** dialog box:

a. **Name—**Click to use the default name, or type a name for the key pair(s). This example uses the name key1.

b. **Size** list—For an RSA key pair, the **Size** list displays the options: 512, 768, 1024, or 2048. The default size is 1024. This example accepts the default setting.

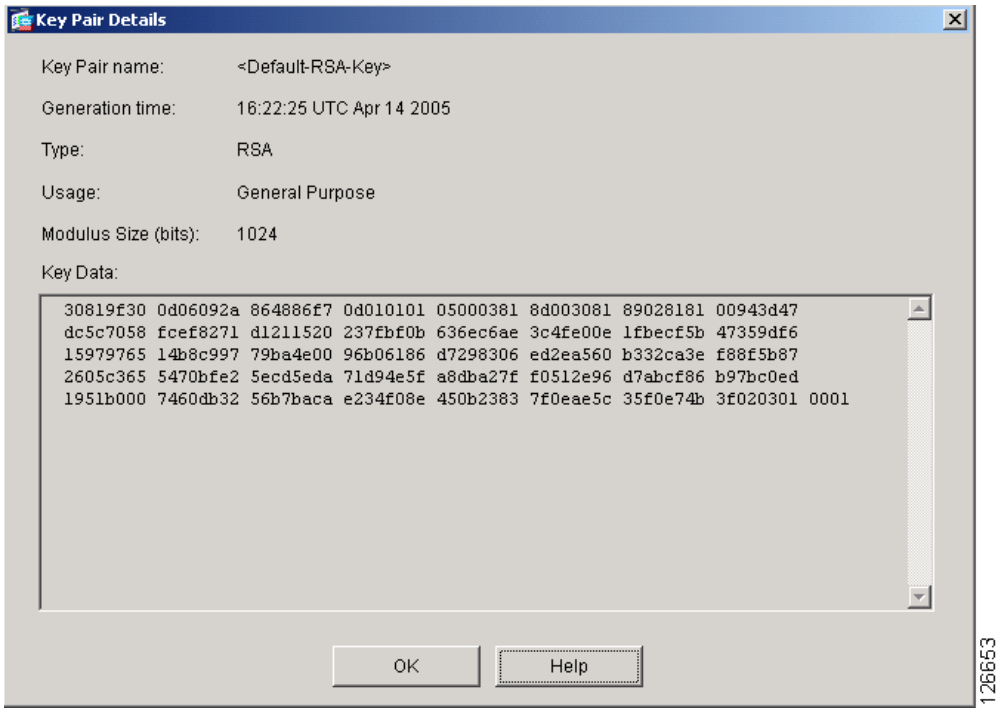
c. **Type** options—**Type** options are RSA and DSA. For this example, accept the default setting, RSA.

d. **Usage** options—(Applicable only if the Type is RSA.) The options are General Purpose (one pair for both signing and encryption) and Special (one pair for each respective function). For this example, accept the default setting (General Purpose).

Step 3 Click **Generate Now**.

Step 4 To view the key pair generated, click **Show Details**. ASDM displays information about the key pair. Figure 4-1 shows sample output.

Figure 4-1 Key-pair Details Display



Creating the Trustpoint

A trustpoint represents a CA/identity pair and contains the identity of the CA, CA-specific configuration parameters, and an association with one enrolled identity certificate. Refer to the section that names the interface you want to use to create a trustpoint.

Using CLI Commands

Use the **crypto ca trustpoint** CLI command to create a trustpoint. This command puts you in config-ca-trustpoint mode and lets you manage trustpoint information. Following this command, you need only two trustpoint commands: **enrollment url** and **subject-name**.

Follow these steps and use the syntax in the example commands:

Step 1 From global configuration mode, enter config-ca-trustpoint mode and create a new trustpoint. In this example, the name of the trustpoint is newmsroot.

```
hostname(config)# crypto ca trustpoint newmsroot
```

Step 2 To specify automatic enrollment (SCEP) to enroll with this trustpoint and configure the enrollment URL, use the **enrollment url** command. Then to specify the distinguished (X.500) name for the certificate, use the **subject-name** command. This is the person or system that uses the certificate. The DN field does support group matching. This example uses the common name (CN) and the organizational unit (OU).

```
hostname(config-ca-trustpoint)# enrollment url http://10.20.30.40/certsrv/mscep/mscep.dll
hostname(config-ca-trustpoint)# subject-name CN=Pat, OU=Techpubs
```

Step 3 (Optional) Display the trustpoint configuration, containing the default parameters and values.

```
hostname(config-ca-trustpoint)# show run all crypto ca trustpoint newmsroot
crypto ca trustpoint newmsroot
 crl nocheck
 enrollment retry period 1
 enrollment retry count 0
 enrollment url http://10.20.30.40/certsrv/mscep/mscep.dll
 fqdn hostname.ciscopix.com
 no email
 subject-name CN=Pat, OU=Techpubs
 serial-number
 no ip-address
 no password
 id-cert-issuer
 accept-subordinates
 support-user-cert-validation
 crl configure
  policy cdp
  cache-time 60
  enforcenextupdate
  protocol http
  protocol ldap
  protocol scep
```

Using ASDM

To create a trustpoint using ASDM, follow these steps:

Step 1 Under the **Configuration > Properties > Certificate > Trustpoint > Configuration** panel, click **Add**.

Step 2 Configure the basic information in the **Add Trustpoint Configuration** dialog box. For all other parameters, accept the default values.

a. **Trustpoint Name** box—Type the trustpoint name in the **Trustpoint Name** box. For this example, the name is newmsroot.

b. **Enrollment URL** box—In the **Enrollment Settings** panel, under the **Enrollment Mode** group box, click the **Use automatic enrollment** option. Then type the enrollment URL in the box. For this example, type **10.20.30.40/certsrv/mscep/mscep.dll**.

Step 3 Configure the subject name using the common name (CN) and the name of the organizational unit (OU):

a. In the **Enrollment Settings** panel, select the key pair you configured for this trustpoint in the **Key Pair** list. For this example, the key pair is key1.

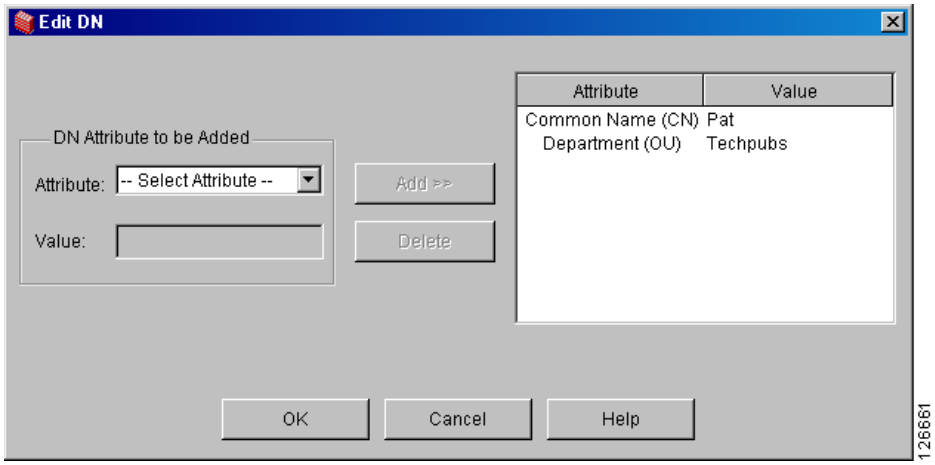
b. In the **Enrollment Settings** panel, click **Certificate Parameters**.

c. To add subject distinguished (X.500) name values, click **Edit** in the **Certificate Parameters** dialog box.

d. In the **Edit DN** box under **DN Attribute to be Added**, select an attribute in the **Attribute** list and type a value in the **Value** box. Then click **Add**. After entering the DN information, click **OK**.

For this example, first select **Common Name (CN)**, type **Pat** in the **Value** box, and click Add; then select **Department (OU)** and type **Techpubs** in the **Value** box. Figure 4-2 shows what you have entered in the **Edit DN** dialog box.

Figure 4-2 Subject Name Attributes and Values



Step 4 After reviewing the dialog box, click **OK**, then click **OK** in the remaining two dialog boxes.

Obtaining Certificates with SCEP

The following sections show how to configure certificates using SCEP. Repeat the instructions for each trustpoint you configure for automatic enrollment. As you complete the instructions for each trustpoint, the ASA receives a CA certificate for the trustpoint and one or two certificates for signing and encryption purposes. If you do not follow these procedures, the ASA prompts you to paste the base-64 formatted CA certificate into the text box.

If you use DSA keys, the certificate received is for signing only.

If you use general-purpose RSA keys, the certificate received is for signing and encryption. If you use separate RSA keys for signing and encryption, the security appliance receives separate certificates for each purpose.

Using CLI Commands

Use the **crypto ca authenticate** command in global configuration mode to obtain certificates. Optionally, you can supply a fingerprint consisting of alphanumeric characters for the ASA to use to authenticate the CA certificate. Issuing this command puts you in interactive mode. The ASA displays the fingerprint of the certificate and prompts you to accept this certificate. To accept the certificate, type **yes** (or **y**).

Note This example shows how to confirm a certificate with a "fingerprint." However, not all CAs require this confirmation.

```
hostname(config)# crypto ca authenticate newmsroot
INFO: Certificate has the following attributes:
Fingerprint:     3736ffc2 243ecf05 0c40f2fa 26820675

Do you accept this certificate? [yes/no]: y

Trustpoint 'newmsroot' is a subordinate CA and holds a non self signed cert.
Trustpoint CA certificate accepted.
```

Using ASDM

To use ASDM to obtain certificates, follow these steps:

Step 1 Go to the **Configuration >Properties > Certificate > Authentication** panel.

Step 2 In the **Trustpoint Name** list, select the name of the trustpoint. For this example, select **newmsroot**.

Step 3 Click **Authenticate**.

Step 4 Click **Apply**. When ASDM displays the **Authentication Successful** dialog, click **OK**.

Enrolling with the Certificate Authority

After you configure the trustpoint and authenticate with it, you can enroll for an identity certificate.

Using CLI Commands

You can use the **show running-config crypto ca certificates** *trustpoint_name* and **show running-config crypto ca trustpoint** *trustpoint_name* command to display the running configuration for a particular trustpoint.

When the trustpoint is configured for SCEP enrollment, as shown in the following example, the ASA displays a CLI prompt and displays status messages to the console.

To begin enrollment, use the **crypto ca enroll** command. The syntax is **crypto ca enroll** *trustpoint* [**noconfirm**]. Decide on a password before you start.

Note The interactive prompts vary depending on the configured state of the referenced trustpoint.

```
hostname(config)# crypto ca enroll newmsroot
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password: v$bx8*c

Re-enter password: v$bx8*c
% The subject name in the certificate will be: CN=Pat, OU=Techpubs
% The fully-qualified domain name in the certificate will be: hostname.ciscopix.com

% Include the router serial number in the subject name? [yes/no]: y
% The serial number in the certificate will be: P3000000098

Request certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
hostname(config)# The certificate has been granted by CA!
```

You now have both the CA and the identity certificate.

Using ASDM

To enroll for an identity certificate using ASDM, follow these steps:

Step 1 Go to the **Configuration > Properties > Certificate > Enrollment** panel.

Step 2 Select the trustpoint in the **Trustpoint Name** list. For this example, you would select **newmsroot**.

Step 3 Click **Enroll**.

Managing Certificates in ASDM

To manage certificates, go to the **Configuration > Properties > Certificate > Manage Certificates** panel.

You can use this panel to add a new certificate and delete a certificate. You can also display information about a certificate by clicking **Show Details**. The Certificate Details dialog displays three tables: General, Subject and Issuer.

The **General** panel displays the following information:

- Type—CA, RA, or Identity
- Serial number—Serial number of the certificate
- Status—Available or pending
  - Available means that the CA has accepted the enrollment request and has issued an identity certificate.
  - Pending means that the enrollment request is still in process and that the CA has not issued the identity certificate yet.
- Usage—General purpose or Signature
- CRL distribution point (CDP)—URL for obtaining the CRL for validating the certificate
- Dates/times within which the certificate is valid—Valid from, valid to

The **Subject** table displays the following information:

- Name—The name of the person or entity that owns the certificate
- Serial number—The serial number of the ASA
- Distinguished (X.500) name fields for the subject of the certificate—cn, ou, etc.
- Hostname of the certificate holder

The **Issuer** table displays the distinguished name fields for the entity that granted the certificate.

- Common name (cn)
- Organizational unit or department (ou)
- Organization (o)
- Locality (l)
- State (st)
- Country code (c)
- Email address of the issuer (ea)

Configuring a LAN-to-LAN Tunnel

The easiest way to configure an IPSec LAN-to-LAN tunnel between the ASA and a peer device is to use the VPN wizard. For information on using the wizard, see "Configuring a VPN Tunnel Using the VPN Wizard" which contains a list of the information to gather before running the wizard.

Use this section if you want to configure a tunnel without using the wizard, or make changes after the initial configuration. This section shows how to configure a LAN-to-LAN tunnel using the CLI as well as ASDM. Also, this section explains some of the VPN terminology used by the ASA that is different from that used by the VPN 3000 Concentrator.

Building a LAN-to-LAN VPN connection includes the following tasks:

- Configuring Interfaces
- Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface
- Creating a Transform Set
- Configuring an ACL
- Defining a Tunnel Group
- Creating a Crypto Map and Applying it to an Interface
- Permitting IPSec Traffic

Example Configuration

The commands shown below show how to configure a LAN-to-LAN connection. Later sections provide step-by-step instructions that explain how to configure this connection, and how to authenticate with preshared keys and certificates.

```
hostname(config)# interface g0/0
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# no shutdown
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 lifetime 43200
```

Note You only need to issue the following command once; it is not necessary for each tunnel.

```
hostname(config)# isakmp enable outside
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# access-list 121_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)# tunnel-group 10.10.4.108 type ipsec_l2l
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
hostname(config)# crypto map abcmap 1 match address xyz
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
```

Note You only need to issue the following two commands once unless you build a tunnel to a different interface.

```
hostname(config)# crypto map abcmap interface outside
hostname(config)# sysopt connection permit-vpn
hostname(config)# write mem
```

Configuring Interfaces

An ASA has at least four interfaces, two of which are referred to here as outside and inside. Typically, the outside interface is connected to the public Internet, while the inside interface is connected to a private network and is protected from public access.

Configure and enable two interfaces on the ASA, and assign a name, IP address and subnet mask. Optionally, configure its security level, speed, and duplex operation on the security appliance (not shown in this example).

Using CLI Commands

To configure interfaces in CLI, use the following steps and the command syntax in the examples as a guide.

Step 1 In global configuration mode, enter the **interface** command and the default name of the interface to be configured (for instance, g0/0). Doing so places your session in interface configuration mode. For example,

```
hostname(config)# interface g0/0
hostname(config-if)#
```

Step 2 Enter the **ip address** command and the IP address and subnet mask of the interface. In the following example, the IP address is 10.10.4.100 and the subnet mask is 255.255.0.0:

```
hostname(config-if)# ip address 10.10.4.100 255.255.0.0
hostname(config-if)#
```

Step 3 To name the interface, use the **nameif** command, maximum of 48 characters. You cannot change this name after you set it. In this example, the name of the g0/0 interface is outside.

```
hostname(config-if)# nameif outside
hostname(config-if)#
```

Step 4 To enable the interface, use the **no** version of the **shutdown** command. By default, interfaces are disabled.

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

Step 5 To save your changes, use the **write memory** command.

```
hostname(config-if)# write memory
hostname(config-if)#
```

Step 6 To configure a second interface, use the same procedure.

Using ASDM

To display the CLI commands that ASDM sends to the device, click the **Options** menu, click **Preferences**, and select **Preview commands before sending to the device**.

To configure these interfaces in the example using ASDM, follow these steps:

Step 1 Under the **Configuration > Interfaces** panel, click **Add**. ASDM opens the **Add Interface** dialog box.

Step 2 Click an interface in the **Hardware Port** list. For this example, select **g0/0**.

Step 3 Click **Enable Interface**.

Step 4 Type the name in the **Interface Name** box. For this example, the name is outside.

Step 5 Type the IP address in the **IP Address** box. For this example, the IP address is 10.10.4.100.

Step 6 Click a subnet mask in the **Subnet Mask** list. For this example, click **255.0.0.0**.

Step 7 Click the **Use Static IP** (for this example) and the click **OK**.

Step 8 To save the configuration, which you should do periodically, click **Save** on the tool bar and click **Yes**.

Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface

Internet Security Association and Key Management Protocol (ISAKMP), also called IKE, is the negotiation protocol that lets two hosts agree on how to build an IPSec Security Association. Each ISAKMP negotiation is divided into two sections called Phase1 and Phase2.

Phase 1 creates the first tunnel, which protects later ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data.

To set the terms of the ISAKMP negotiations, you create an ISAKMP policy, which includes the following:

- Authentication method to ensure the identity of the peers (either preshared key or certificate).
- Encryption method to protect the data and ensure privacy.
- Hashed message authentication codes (HMAC) method to ensure the integrity of the messages and the identity of the sender.
- Diffie-Hellman group to establish the strength of the algorithm that determines the encryption key. The ASA uses this algorithm to derive the encryption and hash keys.
- Expiration timer for the encryption key that determines when the ASA replaces it.

Table 4-1 provides information about the IKE policy keywords and their values.

Table 4-1 Phase 1 — IKE Policy Keywords for CLI Commands

Command	Keyword	Meaning	Description
isakmp policy authentication	rsa-sig dsa-sig pre-share	A digital certificate with keys generated by the RSA signatures algorithm A digital certificate with keys generated by the DSA signatures algorithm pre-shared keys	Specifies the authentication method the ASA uses to establish the identity of each IPSec peer.
isakmp policy encryption	des 3des aes aes-192 aes-256	56-bit DES-CBC 168-bit Triple DES	Specifies the symmetric encryption algorithm that protects data transmitted between two IPSec peers. The default is 56-bit DES-CBC, which is less secure and faster than the alternatives. The Advanced Encryption Standard supports key lengths of 128, 192, and 256 bits.
isakmp policy hash	sha md5	SHA-1 (HMAC variant) MD5 (HMAC variant)	Specifies the hash algorithm used to ensure data integrity. It ensures that a packet comes from whom you think it comes from and that it has not been modified in transit. The default is SHA-1. MD5 has a smaller digest and is considered to be slightly faster than SHA-1.
isakmp policy group	1 2 5 7	Group 1 (768-bit) Group 2 (1024-bit) Group 5 (1536-bit) Group 7 (Elliptical curve field size is 163 bits.)	Specifies the Diffie-Hellman group identifier, which the two IPSec peers use to derive a shared secret without transmitting it to each other. The default is Group 2 (1024-bit Diffie-Hellman).
isakmp policy lifetime	integer value	120 to 2147483647 seconds	Specifies the SA lifetime. The default is 86400 seconds or 24 hours. As a general rule, a shorter lifetime (up to a point) provides more secure IKE negotiations. However, with longer lifetimes, the ASA sets up future IPSec security associations more quickly.

Using CLI Commands

You can enter the **show run isakmp** command to display the current, operational isakmp configuration. The *priority* displayed after "policy" in the system response and in the commands that follow uniquely identifies the associated IKE policy and represents the priority assigned to the policy. It may be an integer from 1 to 65,534 with 1 being the highest priority and 65,534 the lowest.

To configure ISAKMP policies, in global configuration mode, use the **isakmp policy** command with its various arguments. The syntax for ISAKMP policy commands is:

isakmp policy *priority* **attribute_name** [**attribute_value** | *integer*]

Use the following steps and the command syntax in the examples as a guide.

Step 1 Set the authentication method. This example specifies RSA signatures as the authentication method. The default setting is **pre-share**. The priority is 1 in this step and the ones that follow.

```
hostname(config)# isakmp policy 1 authentication rsa-sig
hostname(config)#
```

Step 2 Set the encryption method. This example shows the default setting (**3des**).

```
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)#
```

Step 3 Set the HMAC method. This example shows the default setting (**sha**).

```
hostname(config)# isakmp policy 1 hash sha
hostname(config)#
```

Step 4 Set the Diffie-Hellman group. This example configures Group 2.

```
hostname(config)# isakmp policy 1 group 2
hostname(config)#
```

Step 5 Set the encryption key lifetime. This example configures 43,200 seconds (12 hours). The default setting is **86400**.

```
hostname(config)# isakmp policy 1 lifetime 43200
hostname(config)#
```

Step 6 Enable ISAKMP on the interface named outside. (This attribute does not have a default setting.)

```
hostname(config)# isakmp enable outside
hostname(config)#
```

Step 7 Use the **write mem** command to save your changes.

```
hostname(config)# write mem
hostname(config)#
```

Using ASDM

To configure ISAKMP policy in ASDM, follow these steps:

Step 1 Under the **Configuration > VPN > IKE > Policies** panel, click **Add**.

Step 2 Enter information from the example configuration:

a. Type **1** in the **Priority** box.

b. For a preshared key, click **pre-share** in the **Authentication** list. For certificate authentication, click **rsa-sig** instead.

c. Click **3des** in the **Encryption** list.

d. Click **sha** in the **Hash** list.

e. Click **2** in the **D-H group** list.

f. Type 43200 in the **Lifetime** box and click **Seconds** in the **Lifetime** list.

Step 3 Then to enable ISAKMP on the interface, in the **Configuration > Features > VPN > IKE > Global Parameters** panel, click the interface in the **Enable IKE** group box, and click **Enable**.

Creating a Transform Set

A transform set combines an encryption method and an authentication method. During the IPSec security association negotiation with ISAKMP, the peers agree to use a specific transform set to protect a specific data flow. The transform set must be the same for both peers.

You can create multiple transform sets, and then specify one or more of these transform sets in a crypto map entry. The ASA uses the transform set to protect the data flows for that crypto map entry access list.

The valid encryption methods are as follows:

- esp-des
- esp-3des
- esp-aes (128-bit encryption)
- esp-aes-192
- esp-aes-256
- esp-null

The valid authentication methods are as follows:

- esp-md5-hmac
- esp-sha-hmac

IPSec works in tunnel mode, which is the way in which IPSec is implemented between two ASAs that are connected over an untrusted network, such as the public Internet. This requires no configuration.

Using CLI Commands

You can enter the **show run crypto ipsec** command to display the current, operational transform set configuration.

To configure a transform set via the CLI, in global configuration mode, use the **crypto ipsec transform-set** command. The syntax is:

crypto ipsec transform-set *transform-set-name encryption-method authentication-method*

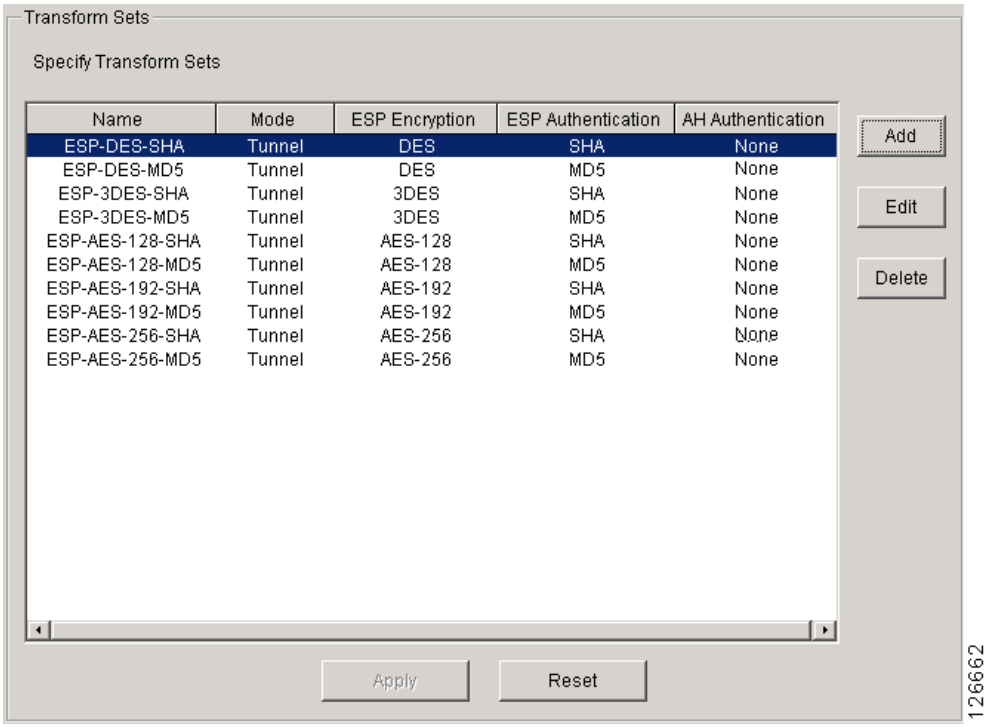
This example configures a transform set with the name FirstSet, esp-3des encryption, and esp-md5-hmac authentication.

```
hostname(config)# crypto ipsec transform-set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

Using ASDM

ASDM comes with all the standard transform sets already configured; most of the time there is no need to add one to the list. To view these transform sets, go to the **Configuration > VPN > IPSec > Transform Sets** panel.

Figure 4-3 Transform Sets Table



Configuring an ACL

The ASA uses access control lists (ACLs) to control network access. By default, the ASA denies all traffic. You need to configure an ACL that permits traffic.

The ACLs you configure for a LAN-to-LAN VPN control connections based on source and destination IP addresses. Configure ACLs that mirror each other on both sides of the connection.

Using CLI Commands

Step 1 To configure an ACL, use the **access-list extended** command. The following example creates an ACL named l2l_list that lets traffic from IP addresses in the 192.168.0.0 network travel to the 150.150.0.0 network. The syntax is **access-list** *listname* **extended permit ip** *source-ipaddress source-netmask destination-ipaddress destination-netmask.*

```
hostname(config)# access-list l2l_list extended permit ip 192.168.0.0 255.255.0.0
150.150.0.0 255.255.0.0
hostname(config)#
```

Step 2 Configure an ACL for the ASA on the other side of the connection that mirrors the ACL above. For this example, the prompt for the peer is hostname2, and the command enables traffic to pass travel from the 150.150.0.0 network to the 192.168.0.0.

```
hostname2(config)# access-list l2l_list extended permit ip 150.150.0.0 255.255.0.0
192.168.0.0 255.255.0.0
hostname2(config)#
```

Using ASDM

To configure an ACL using ASDM, follow these steps:

Step 1 Under the **Configuration > Security Policy > Access Rules** panel, click **Add**.

Step 2 For most of the fields, you can accept the defaults. You must enter the following information:

- IP address and mask for the source host/network (for example, this is 150.150.0.0/255.255.0.0)
- IP address and mask for the destination network (for example, this is 192.168.0.0/255.255.0.0)

Defining a Tunnel Group

A tunnel group is a set of records that contain tunnel connection policies. You configure a tunnel group to identify AAA servers, specify connection parameters, and define a default group policy. The ASA stores tunnel groups internally.

The two default tunnel groups in the ASA system are as follows:

- DefaultRAGroup, the default IPSec remote-access tunnel group.
- DefaultL2LGroup, the default IPSec LAN-to-LAN tunnel group.

You can modify these groups but you cannot delete them. You can also create one or more new tunnel groups to suit your environment. The ASA uses them to set default tunnel parameters for remote access and LAN-to-LAN tunnel groups when there is no specific tunnel group identified during tunnel negotiation.

To establish a basic LAN-to-LAN connection, you must set two attributes for a tunnel group:

- Set the connection type to IPSec LAN-to-LAN.
- Configure an authentication method; this example shows both a preshared key and certificate configuration.

Using CLI Commands

You can enter the **show run all tunnel** command to display the current, operational, tunnel group configuration.

Use the **tunnel-group** command to set the connection type to IPSec LAN-to-LAN, as follows:

Step 1 To set the connection type to IPSec LAN-to-LAN, use the **tunnel-group** command. The syntax is **tunnel-group** *name* **type** *type,* where *name* is the name you assign to the tunnel group, and *type* is the type of tunnel. The tunnel types as you enter them in the CLI are:

- ipsec_ra (IPSec remote access)
- ipsec_l2l (IPSec LAN to LAN)

In this example, the name of the tunnel group is the IP address of the LAN-to-LAN peer, 10.10.4.108.

```
hostname(config)# tunnel-group 10.10.4.108 type ipsec_l2l
hostname(config)#
```

Step 2 To set the authentication method, enter the ipsec-attributes mode and then use the **pre-shared-key** command to create the preshared key. You need to use the same preshared key on both ASAs for this LAN-to-LAN connection. For certificate authentication, use the **trust-point** command.

The preshared key is an alphanumeric string of 1-127 characters. In this example, the preshared key is xyzx. For certificate authentication, specify the trustpoint name, which in this example is newmsroot.

For preshared key authentication, the command is:

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
```

Or, for digital certificate authentication, the command is:

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# trust-point newmsroot
```

Using ASDM

To configure a tunnel group in ASDM using the information in this example:

Step 1 Under the **Configuration > VPN > General > Tunnel Group** panel, click **Add**. ASDM displays the **Add Tunnel Group** dialog box, which resembles the User Management section in the VPN 3000 Concentrator Manager.

Step 2 In the **Identity** panel, type a name for the tunnel group in the **Name** box and click the **IPSec for LAN to LAN** option. The name can be the hostname or the IP address of the LAN-to-LAN peer (10.10.4.108 in this example).

Step 3 In the **IPSec** panel, for preshared key authentication, type the preshared key in the **Pre-shared Key** box. For this example, type **xyzx**. For certificate authentication, select the trustpoint name (**newmsroot**) in the **Trustpoint Name** list.

Creating a Crypto Map and Applying it to an Interface

Crypto map entries pull together the various elements of IPSec security associations, including the following:

- Which traffic IPSec should protect, which you define in an access list.
- Where to send IPSec-protected traffic, by identifying the peer.
- What IPSec security applies to this traffic, which a transform set specifies.
- The local address for IPSec traffic, which you identify by applying the crypto map to an interface.

For IPSec to succeed, both peers must have crypto map entries with compatible configurations. The entries may be IPSec Remote Access (ipsec-ra) or LAN-to-LAN (ipsec-l2l). For two crypto map entries to be compatible, they must, at a minimum, meet the following criteria:

- The crypto map entries must contain compatible crypto access lists (for example, mirror image access lists). If the responding peer uses dynamic crypto maps, the entries in the ASA crypto access list must be *permitted* by the peer's crypto access list.
- The crypto map entries each must identify the other peer (unless the responding peer is using a dynamic crypto map).
- The crypto map entries on each peer must have at least one transform set in common.

If you create more than one crypto map entry for a given interface, use the sequence number (seq-num) of each entry to rank it: the lower the sequence number, the higher the priority. At the interface that has the crypto map set, the ASA evaluates traffic against the entries of higher priority maps first.

Create multiple crypto map entries for a given interface if either of the following conditions exist:

- Different peers handle different data flows.
- You want to apply different IPSec security to different types of traffic (to the same or separate peers), for example, if you want traffic between one set of subnets to be authenticated, and traffic between another set of subnets to be both authenticated and encrypted. In this case, define the different types of traffic in two separate access lists, and create a separate crypto map entry for each crypto access list.

Using CLI Commands

You can enter the **show run crypto map** command to display the current, operational crypto map configuration.

To create a crypto map and apply it to the outside interface in global configuration mode, use several of the **crypto map** commands. These commands use a variety of arguments, but the syntax for all of them begins **crypto map** *map-name-seq-num*. In the examples for this command, the map-name is abcmap, and the sequence number is 1. Enter these commands in global configuration mode.

Step 1 To assign an access list to a crypto map entry, use the **crypto map match address** command.

The syntax is **crypto map** *map-name seq-num* **match address** *aclname*. In this example the map name is abcmap, the sequence number is 1, and the access list name is xyz.

```
hostname(config)# crypto map abcmap 1 match address xyz
hostname(config)#
```

Step 2 To identify the peer(s) for the IPSec connection, use the **crypto map set peer** command.

The syntax is **crypto map** *map-name seq-num* **set peer** {*ip_address1* | *hostname1*}[... *ip_address10* | *hostname10*]. In this example the hostname is 10.10.4.108.

```
hostname(config)# crypto map abcmap 1 set peer 10.10.4.108
hostname(config)#
```

Step 3 To specify a transform set for a crypto map entry, use the **crypto map set transform-set** command.

The syntax is **crypto map** *map-name seq-num* **set transform-set** *transform-set-name*. In this example the transform set name is FirstSet.

```
hostname(config)# crypto map abcmap 1 set transform-set FirstSet
hostname(config)#
```

Using ASDM

To configure crypto map functionality in ASDM, using information from the example configuration:

Step 1 Under the **Configuration > VPN > IPSec > Tunnel Policy** panel, click **Add**.

Step 2 Select the interface and policy type:

a. Click **outside** in the **Interface** list.

b. Click **Static** in the **Policy Type** list.

Step 3 Type the priority (1) in the **Priority** box.

Step 4 Click a transform set from the **Transform Set to Be Added** list and click **Add**. For this example, click **ESP-3DES-MD5**.

Step 5 Select a connection type. For LAN to LAN, select **Bidirectional** in the **Connection Type** list.

Step 6 Enter the IP address of the peer device. If the connection type is bidirectional, you can enter only one peer device. Type the IP address (for this example, 192.168.1.1) in the **IP Address of Peer to be Added** box and click **Add**.

Applying Crypto Maps to Interfaces

When using the CLI interface, you must apply a crypto map set to each interface through which IPSec traffic travels. The ASA supports IPSec on all interfaces. Applying the crypto map set to an interface instructs the ASA to evaluate all interface traffic against the crypto map set and to use the specified policy during connection or security association negotiations. ASDM does this automatically.

Binding a crypto map to an interface also initializes the run-time data structures, such as the security association database and the security policy database. When you later modify a crypto map in any way, the ASA automatically applies the changes to the running configuration. It drops any existing connections and reestablishes them after applying the new crypto map.

To apply the configured crypto map to the outside interface, use the **crypto map interface** command.

The syntax is **crypto map** *map-name* **interface** *interface-name*

```
hostname(config)# crypto map abcmap interface outside
hostname(config)#
```

Permitting IPSec Traffic

The ASA accepts IPSec traffic only if you configure it to do so. The **sysopt** command permits IPSec traffic by letting tunneled traffic bypass interface ACLs to accept IPSec traffic. This means that decrypted traffic is not subject to interface ACLs.

Using CLI Commands

Using CLI commands, permit IPSec traffic and then save the configuration, as follows:

Step 1 Use the **sysopt** command in global configuration mode to have the ASA permit IPSec traffic.

```
hostname(config)# sysopt connection permit-vpn
hostname(config)#
```

Step 2 Save your changes.

```
hostname(config)# write mem
hostname(config)#
```

Using ASDM

In ASDM, enable IPSec traffic and then save the configuration, as follows:

Step 1 Go to the **Configuration > VPN > General > VPN System Options** panel.

Step 2 Click the **Enable IPSec authenticated inbound sessions to always be permitted through the ASA (that is, without a check of the access-list statements)** option.

Step 3 To save the running configuration to flash memory, click **Save** on the tool bar and then click **Yes** when ASDM asks you to confirm.

Configuring a Remote Access Tunnel

Building a remote access VPN tunnel includes the following tasks:

- Configuring Interfaces
- Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface
- Configuring an Address Pool
- Adding a User
- Creating a Transform Set
- Defining a Tunnel Group
- Creating a Dynamic Crypto Map
- Creating a Crypto Map Entry to Use the Dynamic Crypto Map (CLI Only)
- Permitting IPSec Traffic

Example Configuration Overview

This document uses the following configuration to explain how to configure a remote access connection. Later sections provide step-by-step instructions. The instructions show how to authenticate with preshared keys and certificates.

```
hostname(config)# interface g0/0
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)# nameif outside
hostname(config-if)# # no shutdown
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)# isakmp policy 1 hash sha
hostname(config)# isakmp policy 1 group 2
hostname(config)# isakmp policy 1 lifetime 43200
hostname(config)# isakmp enable outside
hostname(config)# ip local pool testpool 192.168.0.10-192.168.0.15
hostname(config)# username testuser password 12345678
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)# tunnel-group testgroup type ipsec_ra
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)# crypto map mymap interface outside
hostname(config)# sysopt connection permit-vpn
hostname(config)# write mem
```

Configuring Interfaces

A security appliance has at least two interfaces, referred to here as outside and inside. Typically, the outside interface is connected to the public Internet, while the inside interface is connected to a private network and is protected from public access.

To begin, configure and enable two interfaces on the ASA. Then assign a name, IP address and subnet mask. Optionally, configure its security level, speed and duplex operation on the security appliance.

Using CLI Commands

To configure interfaces, follow these steps and use the command syntax in the examples.

Note To display the configuration of all interfaces, enter the **show interface** command.

Step 1 To enter Interface configuration mode, in global configuration mode use the **interface** command with the default name of the interface to configure. In this example the interface is g0/0.

```
hostname(config)# interface g0/0
hostname(config-if)#
```

Step 2 To set the IP address and subnet mask for the interface, use the **ip address** command. In this example the IP address is 10.10.4.200 and the subnet mask is 255.255.0.0.

```
hostname(config-if)# ip address 10.10.4.200 255.255.0.0
hostname(config-if)#
```

Step 3 To name the interface, use the **nameif** command, maximum of 48 characters. You cannot change this name after you set it. In this example, the name of the g0/0 interface is outside.

```
hostname(config-if)# nameif outside
hostname(config-if)#
```

Note When you name the interface "outside," the ASA assigns the default settings g0/0 and Security Level 0. When you name the interface "inside," the ASA assigns the default settings g0/1 and Security Level 100.

Step 4 To enable the interface, use the **no** version of the **shutdown** command. By default, interfaces are disabled.

```
hostname(config-if)# no shutdown
hostname(config-if)#
```

Step 5 To save your changes, use the **write memory** command.

```
hostname(config-if)# write memory
```

Step 6 Using the same procedure, configure a second interface.

Using ASDM

To configure these interfaces in the example using ASDM, follow these steps:

Step 1 Under the **Configuration > Interfaces** panel, click **Add**. ASDM opens the **Add Interface** dialog box.

Step 2 Click an interface in the **Hardware Port** list. For this example, select **g0/0**.

Step 3 Click **Enable Interface**.

Step 4 Type the name in the **Interface Name** box. For this example, the name is outside.

Step 5 Type the IP address in the **IP Address** box. For this example, the IP address is 10.10.4.200.

Step 6 Click a subnet mask in the **Subnet Mask** list. For this example, the subnet mask is 255.0.0.0.

Step 7 Click the **Use Static IP** (for this example) and click **OK**.

Step 8 To save the configuration, which you should do periodically, click **Save** on the tool bar and click **Yes**.

Configuring ISAKMP Policy and Enabling ISAKMP on the Outside Interface

Internet Security Association and Key Management Protocol (ISAKMP) is the negotiation protocol that lets two hosts agree on how to build an IPSec Security Association. Each ISAKMP negotiation is divided into two sections called Phase1 and Phase2.

Phase 1 creates the first tunnel to protect later ISAKMP negotiation messages. Phase 2 creates the tunnel that protects data.

To set the terms of the ISAKMP negotiations, you create an ISAKMP policy. It includes the following:

- Authentication method to ensure the identity of the peers.

  This section shows both preshared key and certificate configurations.
- Encryption method to protect the data and ensure privacy.
- Hashed Message Authentication Codes (HMAC) method to ensure the identity of the sender and to ensure that the message has not been modified in transit.
- Diffie-Hellman group to set the size of the encryption key. The security appliance uses this algorithm to derive the encryption and hash keys.
- Encryption key expiration timer.

For more overview information, see Table 4-1 in the LAN-to-LAN section of this chapter.

Using CLI Commands

To configure ISAKMP policies, in global configuration mode, use the **isakmp policy** command with its various arguments. The syntax for ISAKMP policy commands is:

isakmp policy *priority* **attribute_name** [**attribute_value** | *integer*].

Use the following steps and the command syntax in the examples as a guide.

Step 1 Set the authentication method. The default setting is pre-share. The other options are **dsa-sig** and **rsa-sig** to use DSA or RSA signatures as the authentication method.

For example,

```
hostname(config)# isakmp policy 1 authentication pre-share
hostname(config)#
```

Step 2 Set the encryption method. This example configures 3DES.

```
hostname(config)# isakmp policy 1 encryption 3des
hostname(config)#
```

Step 3 Set the HMAC method. This example configures SHA.

```
hostname(config)# isakmp policy 1 hash sha
hostname(config)#
```

Step 4 Set the Diffie-Hellman group. This example configures Group 2.

```
hostname(config)# isakmp policy 1 group 2
hostname(config)#
```

Step 5 Set the encryption key lifetime. This example configures 43, 200 seconds (12 hours).

```
hostname(config)# isakmp policy 1 lifetime 43200
hostname(config)#
```

Step 6 Enable ISAKMP on the interface named outside.

```
hostname(config)# isakmp enable outside
hostname(config)#
```

Step 7 Use the **write mem** command to save your changes.

```
hostname(config)# write mem
hostname(config)#
```

Using ASDM

To configure ISAKMP policy in ASDM, follow these steps:

Step 1 Under the **Configuration > VPN > IKE > Policies** panel, click **Add**.

Step 2 Enter information from the example configuration:

a. Type **1** in the **Priority** box.

b. For preshared key, click **pre-share** in the **Authentication** list. For certificate authentication, click **rsa-sig** instead.

c. Click **3des** in the **Encryption** list.

d. Click **md5** in the **Hash** list.

e. Click **2** on the **D-H group** list.

f. Type 43200 in the **Lifetime** box and click **Seconds** on the **Lifetime** list.

Step 3 To enable ISAKMP on the interface, go to the **Configuration > Features > VPN > IKE > Global Parameters** panel, click the interface in the **Enable IKE** box, and click **Enable**.

Configuring an Address Pool

A security appliance requires a method for assigning IP addresses to users. A common method is using address pools. The alternatives are having a DHCP server assign addresses or having an AAA server assign them. This example uses an address pool.

Using CLI Commands

When configuring an address pool, you must supply the mask value if the IP addresses assigned to VPN clients belong to a non-standard network, and the data could be routed incorrectly if you use the default mask. A typical example is when the IP local pool contains 10.10.10.0/255.255.255.0 addresses, since this is a Class A network by default. This could cause some routing issues when the VPN client needs to access different subnets within the 10 network over different interfaces. For example, if a printer, address 10.10.100.1/255.255.255.0 is available via interface 2, but the 10.10.10.0 network is available over the VPN tunnel and therefore interface 1, the VPN client would be confused as to where to route data destined for the printer. Both the 10.10.10.0 and 10.10.100.0 subnets are in the 10.0.0.0 Class A network so the printer data may be sent over the VPN tunnel.

To configure an address pool, use the **ip local pool** command. The syntax is **ip local pool** *poolname first_address-last_address* [**mask** *mask*]. The following example command configures an IP address pool named firstpool. The starting address is 10.20.30.40 and the ending address is 10.20.30.50. The network mask is 255.255.255.0.

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
hostname(config)#
```

Use the **show running-config ip local pool** command to display the address pool configuration.

Using ASDM

To configure an address pool in ASDM, follow these steps:

Step 1 Under the **Configuration > VPN > IP Address Management > IP Pools** panel, click **Add**.

Step 2 Enter the name, starting IP address, and ending IP address. For this example:

a. Type testpool in the **Name** box.

b. Type **192.168.0.10** in the **Start IP** box.

c. Type **192.168.0.15** in the **End IP** box.

Step 3 In the **Subnet Mask** list, click one of the standard network masks, for this example, click **255.255.255.0**.

Adding a User

To identify remote access users to the ASA, configure usernames and passwords.

Using CLI Commands

To configure an entry in the internal database for each user, use the **username** command. The syntax is **username** *username* **password** *password*. In this example the username is testuser and the password is 12345678. For information on setting up external authentication, see "Authenticating with External Servers."

```
hostname(config)# username testuser password 12345678
hostname(config)#
```

Using ASDM

To configure usernames and passwords in ASDM, follow these steps:

Step 1 Under the **Configuration > Properties > Device Administration > User Accounts** panel, click **Add**.

Step 2 Enter the username and password, confirm password, and optionally a privilege level. For this example:

a. Under the **Identity** panel, type **testuser** in the **User Name** box.

b. Type **12345678** in the **Password** box.

c. Type the password again in the **Confirm Password** box.

Creating a Transform Set

A transform set combines an encryption method and an authentication method. During the IPSec security association negotiation with ISAKMP, the peers agree to use a specific transform set to protect a specific data flow. The transform set must be the same for both peers.

You can create multiple transform sets to support tunnel combinations comprising different attributes, and then specify one or more of these transform sets in a crypto map entry. The ASA uses the transform set to protect the data flows for that crypto map entry access list. For more overview information, including a table that lists valid encryption and authentication methods, see the LAN-to-LAN "Creating a Transform Set" section.

Using CLI Commands

To configure a transform set, in global configuration mode, use the **crypto ipsec transform-set** command. The syntax is:

crypto ipsec transform-set *transform-set-name encryption-method authentication-method*

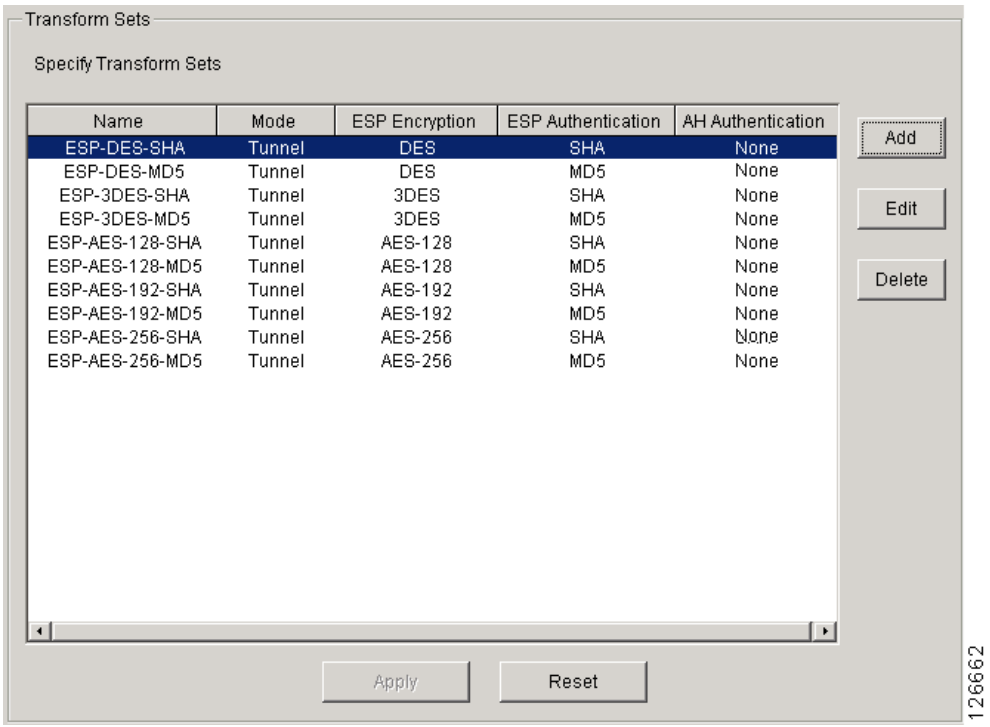
This example configures a transform set with the name FirstSet, esp-3des encryption, and esp-md5-hmac authentication.

```
hostname(config)# crypto ipsec transform set FirstSet esp-3des esp-md5-hmac
hostname(config)#
```

Using ASDM

ASDM comes with all the standard transform sets already configured; most of the time there is no need to add one to the list. To view these transform sets, go to the **Configuration > VPN > IPSec > Transform Sets** panel.

Figure 4-4 Transform Sets Table



Defining a Tunnel Group

A tunnel group is a set of records that contain tunnel connection policies. You configure a tunnel group to identify AAA servers, specify connection parameters, and define a default group policy. The ASA stores tunnel groups internally.

Two default tunnel groups in the ASA system are: DefaultRAGroup, the default IPSec remote-access tunnel group; and DefaultL2LGroup, the default IPSec LAN-to-LAN tunnel group. You can change them but not delete them. The ASA uses them to configure default tunnel parameters for remote access and LAN-to-LAN tunnel groups when there is no specific tunnel group identified during tunnel negotiation.

To establish a basic remote access connection, you must set three attributes for a tunnel group:

- Set the connection type to IPSec_RA (remote access).
- Configure the address assignment method. The following steps show an address pool.
- Configure an authentication method. The following steps show both a preshared key and a digital certificate.

Using CLI Commands

You can enter the **show run all tunnel** command to display the current, operational, tunnel group configuration.

Use the CLI to configure a trunk group, as follows:

Step 1 To set the connection type to IPSec remote access, use the **tunnel-group** command. The command syntax is **tunnel-group** *name* **type** *type,* where *name* is the name you assign to the tunnel group, and *type* is the type of tunnel. The tunnel types as you enter them in the CLI are:

- ipsec_ra (IPSec remote access)
- ipsec_l2l (IPSec LAN to LAN)

In this example, the name of the tunnel group is testgroup and the type is ipsec_ra.

```
hostname(config)# tunnel-group testgroup type ipsec_ra
hostname(config)#
```

Step 2 To configure an address pool for the tunnel group, enter the general-attributes mode and then use the **address-pool** command to create the address pool. In this example, the name of the group is testgroup and the name of the address pool is testpool.

```
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-general)# address-pool testpool
```

Step 3 To configure the authentication method, enter the ipsec-attributes mode and then use the **pre-shared-key** command to create the preshared key. You need to use the same preshared key on both devices for this remote-access connection. For certificate authentication, use the **trust-point** command.

The preshared key is an alphanumeric string of 1-127 characters. In this example, the preshared key is xyzx. For certificate authentication, you specify the trustpoint name, which in this example is newmsroot.

For preshared key authentication, the command is:

```
hostname(config)# tunnel-group testgroup ipsec-attributes
hostname(config-ipsec)# pre-shared-key xyzx
```

For digital certificate authentication, the command is:

```
hostname(config)# tunnel-group 10.10.4.108 ipsec-attributes
hostname(config-ipsec)# trust-point newmsroot
```

Using ASDM

Use the ASDM to configure a trunk group, as follows:

Step 1 Go to the **Configuration > VPN > General > Tunnel Group** panel and click **Add**.

Step 2 In the **Identity** panel, type the tunnel group name in the **Name** box; for this example the name is testgroup.

Step 3 In the **Type** group, click the **IPSec for Remote Access** option.

Step 4 In the **Client Address Assignment** panel, in the **Address Pool** group, select the address pool you added previously and click **Add**.

Step 5 In the **IPSec** panel, for preshared key, type the preshared key in the **Pre-shared Key** box. For this example, the preshared key is xyzx. Alternatively, for certificate authentication, select the name of the trustpoint in the **Trustpoint Name** list. For this example, the name is newmsroot.

Creating a Dynamic Crypto Map

The ASA uses dynamic crypto maps to define a policy template. These dynamic crypto maps let the ASA receive connections from peers without known IP addresses. Remote access clients are in this category.

Dynamic crypto map entries identify the transform set for the connection. You also enable reverse route injection (RRI), which lets the ASA learn routing information for connected clients. The ASA must also advertise it via RIP or OSPF. For clients that obtain their address from all methods (AAA, IP pools, and DHCP proxy), the ASA announces configured routes. For other address assignment methods, it uses a global enable/disable flag to determine the advertisement of client routes.

Using CLI Commands

You can enter the **show run all crypto dynamic-map** command to display the current, operational crypto dynamic map configuration.

To configure dynamic crypto map functionality in the CLI, using information from the example configuration, follow these steps:

Step 1 To specify a transform set for a dynamic crypto map entry, use following command syntax:

crypto dynamic -map *dynamic-map-name seq-num* **set transform-set** *transform-set-name*

In the following example, the name of the dynamic map is dyn1, the sequence number is 1, and the transform set name is FirstSet:

```
hostname(config)# crypto dynamic-map dyn1 1 set transform-set FirstSet
hostname(config)#
```

Step 2 To enable RRI for any connection based on this crypto map entry, use the **crypto dynamic-map set reverse route** command, as follows:

```
hostname(config)# crypto dynamic-map dyn1 1 set reverse-route
hostname(config)#
```

Step 3 Save your changes.

```
hostname(config)# write mem
hostname(config)#
```

Using ASDM

To configure dynamic crypto map functionality in ASDM, using information from the example configuration, follow these steps:

Step 1 Under the **Configuration > VPN > IPSec > Tunnel Policy** panel, click **Add**.

Step 2 Click an interface in the **Interface** box. For this example, click **outside**.

Step 3 Click **dynamic** in the **Policy Type** box.

ASDM names the dynamic map by combining the interface and policy type. In this example, the name of the crypto dynamic map becomes dyn1.

Step 4 Type the priority (**1**) in the **Priority** box.

Step 5 Click a transform set in the **Transform Set to Be Added** list and click **Add**. For this example, click **ESP-3DES-MD5**.

Step 6 Click **Advanced**.

Step 7 Click the **Enable Reverse Route Injection** option.

Step 8 Click **OK** to exit the **Tunnel Policy Advanced Settings** dialog box and then click **OK** again to exit the **Add Tunnel Policy** dialog box.

Step 9 Click **Apply**.

Figure 4-5 shows the CLI commands generated by the tunnel policy configuration. Notice that ASDM has generated crypto map commands that reference the crypto dynamic map dyn1.

Figure 4-5 Tunnel Policy

```
crypto dynamic-map outside_dyn_map 1 set transform-set ESP-3DES-MD5
crypto dynamic-map outside_dyn_map 1 set security-association lifetime seconds 28800 kilobyte
crypto dynamic-map outside_dyn_map 1 set nat-t-disable
crypto dynamic-map outside_dyn_map 1 set reverse-route
crypto map outside_map 65535 ipsec-isakmp dynamic outside_dyn_map
crypto map outside_map interface outside
```

Creating a Crypto Map Entry to Use the Dynamic Crypto Map (CLI Only)

If you are using the CLI, you must next create a crypto map entry that lets the ASA use the dynamic crypto map to set the parameters of IPSec security associations.

Note You do not have to create a crypto map to use the dynamic crypto map when you use ASDM. ASDM creates the crypto map automatically.

In the examples for this command, the name of the crypto map is mymap, the sequence number is 1, and the name of the dynamic crypto map is dyn1, the one created in the previous section Creating a Dynamic Crypto Map. Enter these commands in global configuration mode.

Step 1 To create a crypto map entry that uses a dynamic crypto map, use the **crypto map** command. The syntax is **crypto map** *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name.*

```
hostname(config)# crypto map mymap 1 ipsec-isakmp dynamic dyn1
hostname(config)#
```

Step 2 To apply the crypto map to the outside interface, use the **crypto map interface** command.

The syntax is **crypto map** *map-name* **interface** *interface-name*

```
hostname(config)# crypto map mymap interface outside
hostname(config)#
```

Permitting IPSec Traffic

The ASA permits IPSec traffic only if you configure it to do so. The **sysopt** command permits IPSec traffic by letting tunneled traffic bypass interface ACLs to accept IPSec traffic. This means that decrypted traffic is not subject to interface ACLs.

Using CLI Commands

Using CLI commands, permit IPSec traffic and then save the configuration, as follows:

Step 1 Use the **sysopt** command in global configuration mode to have the ASA permit IPSec connections.

```
hostname(config)# sysopt connection permit-vpn
hostname(config)#
```

Step 2 Save your changes.

```
hostname(config)# write mem
hostname(config)#
```

Using ASDM

In ASDM, permit IPSec traffic and then save the configuration, as follows:

Step 1 Click the **Configuration > VPN > General > VPN System Options** panel.

Step 2 Click the **Enable IPSec authenticated inbound sessions to always be permitted through the ASA (that is, without a check of the access-list statements)** option.

Step 3 To save the running configuration to flash memory, click **Save** on the tool bar and then click **Yes** when ASDM asks you to confirm.