Introducing the ASA System

This chapter addresses some of the major differences between the VPN 3000 Concentrator and the Adaptive Security Appliance, specifically for VPN. It includes the following sections:

Brief Overview of Security Policy Features

The ASA combines Cisco's most powerful firewall, VPN, and intrusion protection features:

- The ASA provides a majority of the software features supported in the VPN 3000 Concentrator, including WebVPN. WebVPN requires ASA software running on an ASA device, not a PIX Firewall.
- The ASA hardware provides faster interfaces (10/100/1000), an additional interface (4), and is expandable, containing a slot for additional security services.
- The operating system uses IOS-like CLI commands, which adds power and flexibility, improves on the menu-based command-line interface of the VPN 3000 Concentrator, and adds the ability to use scripts to automate configuration and monitoring processes. The CLI commands support features moved into the ASA from the VPN Concentrator, and there are many new commands specifically designed for VPN features. For information about CLI commands, see the *Cisco Security Appliance Command Reference*.
- The ASA performance exceeds that of the VPN 3000 Concentrator.
- The ASA provides for scalability and investment protection: multiple services are available in the same device, expansion is possible in the future with additional interfaces or services.
- The Adaptive Security Device Manager software provides a multicontext management interface to the ASA system.

The following sections describe the key conceptual differences between the ASA and the VPN 3000 Concentrator.

User Management Differences

Groups and users are core concepts in managing the security of virtual private networks (VPNs) and in configuring the security appliance. They specify attributes that determine user access to and use of the VPN. A *group* is a collection of users treated as a single entity. *Users* get their attributes from *group policies*. *Tunnel groups* identify the group policy for a specific connection. If you do not assign a particular group policy to a user, the default group policy for the connection applies. There is no base group, as there is with the VPN 3000 Concentrator.

Tunnel groups and group policies simplify system management. To streamline the configuration task, the security appliance provides a default LAN-to-LAN tunnel group, a default remote access tunnel group, a default WebVPN tunnel group, and a default group policy (DfltGrpPolicy). The default tunnel groups and group policy provide settings that are likely to be common for many users. As you add users, you can specify that they "inherit" parameters from a group policy. Thus you can quickly configure VPN access for large numbers of users.

If you decide to grant identical rights to all VPN users, then you do not need to configure specific tunnel groups or group policies, but VPNs seldom work that way. For example, you might allow a finance group to access one part of a private network, a customer support group to access another part, and an MIS group to access other parts. In addition, you might allow specific users within MIS to access systems that other MIS users cannot access. Tunnel groups and group policies provide the flexibility to do so securely.

Note The security appliance also includes the concept of object groups, which are a superset of network lists. Object groups let you define VPN access to ports as well as networks. Object groups relate to ACLs rather than to group policies and tunnel groups.

ASA Tunnel Groups

A tunnel group consists of a set of records that determines tunnel connection policies. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers, if any, to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters. Tunnel groups include a small number of attributes that pertain to creating the tunnel itself. Tunnel groups include a pointer to a group policy that defines user-oriented attributes.

The security appliance provides the following default tunnel groups: DefaultL2LGroup for LAN-to-LAN connections, DefaultRAGroup for remote access connections, and DefaultWEBVPNGroup for WebVPN connections. You can modify these default tunnel groups, but you cannot delete them. You can also create one or more tunnel groups specific to your environment. Tunnel groups are local to the security appliance and are not configurable on external servers.

Tunnel groups specify the following attributes:

- General parameters
- IPSec connection parameters
- WebVPN connection parameters

General Tunnel-Group Connection Parameters

General parameters are common to both IPSec and WebVPN connections. The general parameters include the following:

- Tunnel group name—You specify a tunnel-group name when you add or edit a tunnel group. The following considerations apply:
  - For clients that use preshared keys to authenticate, the tunnel group name is the same as the group name that an IPSec client passes to the security appliance.
  - Clients that use certificates to authenticate pass this name as part of the certificate, and the security appliance extracts the name from the certificate.

  Tunnel group records contain tunnel connection policy information. These records identify the servers to which the tunnel user is authenticated, as well as the accounting servers, if any, to which connection information is sent. They also identify a default group policy for the connection, and they contain protocol-specific connection parameters.
- Connection type—Connection types include IPSec remote access, IPSec LAN-to-LAN, and WebVPN. A tunnel group can have only one connection type.
- Authentication, Authorization, and Accounting servers—These parameters identify the server groups or lists that the security appliance uses for the following purposes:
  - Authenticating users
  - Obtaining information about services users are authorized to access
  - Storing accounting records

  A server group can consist of one or more servers.
- Default group policy for the connection—A group policy is a set of user-oriented attributes. The default group policy is the group policy whose attributes the security appliance uses as defaults when authenticating or authorizing a tunnel user.
- Client address assignment method—This method includes values for one or more DHCP servers or address pools that the security appliance assigns to clients.
- Override account disabled—This parameter lets you override the “account-disabled” indicator received from a AAA server.
- Password management—This parameter lets you warn a user that the current password is due to expire in a specified number of days (the default is 14 days), then offer the user the opportunity to change the password.
- Strip group and strip realm—These parameters direct the way the security appliance processes the user names it receives. They apply only to user names received in the form user@realm. A realm is an administrative domain appended to a username with the @ delimiter (user@abc).

  When you specify strip-group processing, the security appliance selects the tunnel group for user connections by obtaining the group name from the username presented by the VPN client. The security appliance then sends only the user part of the username for authorization/authentication. Otherwise (if disabled), the security appliance sends the entire username, including the realm.

  Strip-realm processing removes the realm from the username when sending the username to the authentication or authorization server. If the command is enabled, the security appliance sends only the user part of the username authorization/authentication. Otherwise, the security appliance sends the entire username.
- Authorization required—This parameter lets you require authorization before user access or turn off that requirement.

- Authorization DN attributes—This parameter specifies which Distinguished Name attributes to use when performing authorization.

IPSec Tunnel-Group Connection Parameters

IPSec tunnel-group parameters include the following:

- A client authentication method: preshared keys, certificates, or both.
  - For IKE connections based on preshared keys, the alphanumeric key itself (up to 128 characters long), associated with the connection policy.
  - Peer-ID validation requirement—This parameter specifies whether to require validating the identity of the peer using the peer's certificate.
- ISAKMP (IKE) keepalive settings. This feature lets the security appliance monitor the continued presence of a remote peer and report its own presence to that peer. If the peer becomes unresponsive, the security appliance removes the connection. Enabling IKE keepalives prevents hung connections when the IKE peer loses connectivity.

  There are various forms of IKE keepalives. For this feature to work, both the security appliance and its remote peer must support a common form. This feature works with the following peers:
  - Cisco VPN client (Release 3.0 and above)
  - Cisco VPN 3000 Client (Release 2.x)
  - Cisco VPN 3002 Hardware Client
  - Cisco VPN 3000 Series Concentrators
  - Cisco IOS software
  - Cisco Secure PIX Firewall

  Non-Cisco VPN clients do not support IKE keepalives.

  If you are configuring a group of mixed peers, in which some of those peers support IKE keepalives and others do not, enable IKE keepalives for the entire group. The feature does not affect the peers that do not support it.

  If you disable IKE keepalives, connections with unresponsive peers remain active until they time out, so we recommend that you keep your idle timeout short.

Note To reduce connectivity costs, disable IKE keepalives if this group includes any clients connecting via ISDN lines. ISDN connections normally disconnect if idle, but the IKE keepalive mechanism prevents connections from idling and therefore from disconnecting.

If you do disable IKE keepalives, the client disconnects only when either its IKE or IPSec keys expire. Failed traffic does not disconnect the tunnel with the Peer Timeout Profile values as it does when IKE keepalives are enabled.

Note If you have a LAN-to-LAN configuration using IKE main mode, make sure that the two peers have the same IKE keepalive configuration. Both peers must have IKE keepalives enabled or both peers must have it disabled.

- If you configure authentication using digital certificates, you can specify whether to send the entire certificate chain (which sends the peer the identity certificate and all issuing certificates) or just the identity certificate.
- You can notify users who are using outdated versions of Windows client software that they need to update their client, and you can provide a mechanism for them to get the updated client version. For VPN 3002 hardware client users, you can trigger an automatic update. You can configure and change the client-update, either for all tunnel groups or for particular tunnel groups.
- If you configure authentication using digital certificates, you must specify the name of the trustpoint that identifies the certificate to send to the IKE peer.

WebVPN Tunnel-Group Connection Parameters

The following attributes are specific to WebVPN connections:

- The authentication method, either AAA or certificate.
- The name of the customization to apply. Customizations determine the appearance of the WebVPN portal page. You configure the customization parameters as part of configuring WebVPN.
- The DNS server-group name. The DNS server group specifies the DNS server name, domain name, name server, number of retries, and timeout values for a DNS server to use for a tunnel group.
- One or more group aliases; these are alternate names by which the server can refer to a tunnel group. At login, the user selects the group name from a dropdown menu.
- One or more group URLs. If you configure this parameter, users coming in on a specified URL need not select a group at login.
- A group policy that grants a WebVPN user access rights that are different from the default group policy.
- The name of the NetBIOS Name Service server (nbns-server) to use for CIFS name resolution.

Group Policies

A group policy is a set of user-oriented attribute/value pairs for IPSec connections that are stored either internally (locally) on the device or externally on a RADIUS server. The tunnel group uses a group policy that sets terms for user connections after the tunnel is established. Group policies let you apply whole sets of attributes to a user or a group of users, rather than having to specify each attribute individually for each user.

Enter the **group-policy** commands in global configuration mode to assign a group policy to users or to modify a group policy for specific users.

The security appliance includes a default group policy. In addition to the default group policy, which you can modify but not delete, you can create one or more group policies specific to your environment.

You can configure internal and external group policies. Internal groups are configured on the security appliance's internal database. External groups are configured on an external authentication server, such as RADIUS. Group policies include the following attributes:

- Identity
- Server definitions
- Client firewall settings
- Tunneling protocols

- IPSec settings
- Hardware client settings
- Filters
- Client configuration settings
- WebVPN functions
- Connection settings

Default Group Policy

The security appliance supplies a default group policy. You can modify this default group policy, but you cannot delete it. A default group policy, named DfltGrpPolicy, always exists on the security appliance, but this default group policy does not take effect unless you configure the security appliance to use it. When you configure other group policies, any attribute that you do not explicitly specify takes its value from the default group policy. To view the default group policy, enter the following command:

```
hostname(config)# show running-config all group-policy DfltGrpPolicy
hostname(config)#
```

Configuring Group Policies

A group policy can apply to any kind of tunnel. In each case, if you do not explicitly define a parameter, the group takes the value from the default group policy. A group policy can be either external or internal.To configure a group policy, you first specify the name and type of the group policy, then, for an internal group policy, you specify its attributes.

Configuring an External Group Policy

External group policies take their attribute values from the external server that you specify. For an external group policy, you must identify the AAA server group that the security appliance can query for attributes and specify the password to use when retrieving attributes from the external AAA server group. If you are using an external authentication server, keep in mind that user names and group names must be unique. When naming a group, do not pick a name that matches the name of any external user. Conversely, when assigning a name to an external user, do not choose the name of any existing group.

Note The security appliance supports user authorization on an external LDAP or RADIUS server. Before you configure the security appliance to use an external server, you must configure the server with the correct security appliance authorization attributes and, from a subset of these attributes, assign specific permissions to individual users.For an external group policy, RADIUS is the only supported AAA server type.

Configuring an Internal Group Policy

The attribute/value pairs for internal group policies are stored internally (locally) on the security appliance. To configure an internal group policy, specify a name and type for the group policy, then specify the attributes. You can initialize the attributes of an internal group policy to the values of a preexisting group policy by appending the keyword **from** and specifying the name of the existing policy. You can specify the following attributes for an internal group policy:

- Primary and secondary WINS and DNS servers

- VPN-specific attributes (access hours, number of simultaneous logins, VPN idle timeout and session timeout, the name of the ACL to use for VPN connections, VPN tunnel type (IPSec remote access or LAN-to-LAN, or WebVPN) for this group policy)
- Security settings (password storage, IP compression, whether to require that users reauthenticate on IKE rekey, whether to restrict remote users to access only through the tunnel group, and whether to enable perfect forward secrecy)
- Banner message
- IPSec over UDP (sometimes called IPSec through NAT)
- Split-tunneling policy and network list
- Domain attributes
- Attributes for VPN 3002 Hardware Clients (secure unit authentication, user authentication, user authentication idle timeout, IP phone bypass, LEAP bypass, and Network Extension Mode
- Backup server attributes
- Client firewall policies
- Client access rules

The group policy inherits from the default group any attributes you do not explicitly specify.

Configuring Group-Policy WebVPN Attributes

WebVPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. There is no need for either a software or hardware client. WebVPN provides easy access to a broad range of web resources and web-enabled applications from almost any computer that can reach HTTPS Internet sites. WebVPN uses SSL and its successor, TLS1, to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users. By default, WebVPN is disabled.

You can customize a WebVPN configuration for specific internal group policies.

Note The webvpn mode that you enter from global configuration mode lets you configure global settings for WebVPN. The webvpn mode described in this section, which you enter from group-policy configuration mode, lets you customize a WebVPN configuration for specific group policies.

In group-policy webvpn configuration mode, you can specify whether to inherit the settings for all the functions or customize the following parameters:

- WebVPN functions (auto-download, Citrix, file access, file browsing, file entry, filter, HTTP proxy, MAPI, port-forwarding, URL entry).
- ACLs and types of traffic to filter.
- Customizations that change the look-and-feel of the window that the user sees upon login.
- HTML-content-filter.
- Homepage.
- Filtering Java, ActiveX, images, scripts, and cookies for WebVPN sessions.
- Access Control List to use for WebVPN connections for this group.
- URL-list to appear on the WebVPN home page for this group.

- Port-forwarding and port-forward display name.
- Dead-peer detection attributes.
- Single signon server (sso server). Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without reentering a username and password more than once.
- Auto-signon, which automatically submits a WebVPN user's login credentials to internal servers.
- Deny message for a WebVPN user who logs on successfully, but who has no VPN privileges.
- SSL VPN Client (SVC) attributes. SVC is a VPN tunneling technology that gives remote users the benefits of an IPSec VPN client without the need for network administrators to install and configure IPSec VPN clients on remote computers.
- SVC keep-alive attribute, which adjusts the frequency of keepalive messages (specified by *seconds*), to ensure that an SVC connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle.
- SVC keep-installer, which enables the permanent installation of an SVC onto a remote computer.

Note WebVPN does not use ACLs defined in the **vpn-filter** command.

In many instances, you define the WebVPN attributes as part of configuring WebVPN, then you apply those definitions to specific groups when you configure the group-policy webvpn attributes. See the description of WebVPN in *Cisco Security Appliance Command Line Configuration Guide* and *Cisco Security Appliance Command Reference* for more information about configuring the WebVPN attributes.

Configuring User Attributes

By default, users inherit all user attributes from the assigned group policy. The security appliance also lets you assign individual attributes at the user level, overriding values in the group policy that applies to that user. For example, you can specify a group policy that gives all users access during business hours but then configure a specific user for 24-hour access.

Configuring Attributes for Specific Users

To configure attributes for specific users, you assign a password (or no password) and other values to a user using the **username** command, which enters username mode. Any attributes that you do not specify are inherited from the group policy.

The internal user authentication database consists of the users entered with the **username** command. To add a user to the security appliance database, enter the **username** command in global configuration mode. To remove a user, use the **no** version of this command with the username you want to remove. To remove all user names, use the **clear configure username** command without appending a username.

The username attributes that you can specify are as follows:

- Password and privilege level for this user
- Group policy from which to inherit the values of attributes that are not explicitly configured
- VPN access hours and number of simultaneous logins allowed
- VPN idle timeout and maximum connect time
- Name of a previously-configured, user-specific ACL to use as a filter for VPN connections

- IP address and netmask to assign to this user
- VPN tunnel types (IPSec remote access or WebVPN) that this user can use
- Whether to restrict remote users to access only through the specified, preexisting tunnel group
- Whether to let users store their login passwords on the client system

Configuring WebVPN for Specific Users

WebVPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. There is no need for either a software or hardware client. WebVPN provides easy access to a broad range of web resources and web-enabled applications from almost any computer that can reach HTTPS Internet sites. WebVPN uses SSL and its successor, TLS1, to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

To customize a WebVPN configuration for specific users, enter username webvpn configuration mode by using the **webvpn** command in username configuration mode. The **webvpn** commands for usernames define access to files, MAPI proxy, URLs and TCP applications over WebVPN. They also identify ACLs and types of traffic to filter. WebVPN is disabled by default. These **webvpn** commands apply only to the username from which you configure them.

In username webvpn configuration mode, you can specify whether to inherit the settings for all the functions or customize the following parameters:

- WebVPN functions (auto-download. Citrix, file access, file browsing, file entry, filter, HTTP proxy, MAPI, port-forwarding, URL entry).
- Customizations that change the look-and-feel of the window that the user sees upon login.
- HTML-content-filter.
- Homepage.
- Filtering Java, ActiveX, images, scripts, and cookies for WebVPN sessions.
- Access Control List to use for WebVPN connections for this group.
- URL-list to appear on the WebVPN home page for this group.
- Port-forwarding and port-forward display name.
- Dead-peer detection attributes.
- Single signon server (sso server). Single sign-on support, available only for WebVPN, lets users access different secure services on different servers without reentering a username and password more than once.
- Auto-signon (automatically submitting a WebVPN user's login credentials to internal servers).
- Deny message for a WebVPN user who logs on successfully, but who has no VPN privileges.
- SSL VPN Client (SVC) attributes. SVC is a VPN tunneling technology that gives remote users the benefits of an IPSec VPN client without the need for network administrators to install and configure IPSec VPN clients on remote computers.
- SVC keep-alive attribute, which adjusts the frequency of keepalive messages (specified by *seconds*), to ensure that an SVC connection through a proxy, firewall, or NAT device remains open, even if the device limits the time that the connection can be idle.
- SVC keep-installer, which enables the permanent installation of an SVC onto a remote computer.

Note WebVPN does not use ACLs defined in the **vpn-filter** command.

In many instances, you define the WebVPN attributes as part of configuring WebVPN, then you apply those definitions to specific users when you configure the username webvpn attributes. See the description of WebVPN for more information about configuring the WebVPN attributes. Enter username webvpn configuration mode by using the **webvpn** command in username configuration mode. WebVPN commands for usernames define access to files, MAPI proxy, URLs and TCP applications over WebVPN. They also identify ACLs and types of traffic to filter. WebVPN is disabled by default.

PKI Implementation on ASA

The implementation of PKI on the ASA differs from the VPN 3000 Concentrator implementation. The main concept of the PKI model on ASA is the trustpoint. Trustpoints have the following characteristics:

- Trustpoints have a one-to-one relationship with local identities.
- Trustpoints have a many-to-one relationship with CA identities.
- Trustpoints specify enrollment request content, defaults, and method of enrollment.
- Trustpoints specify CRL configuration parameters.

To configure trustpoints in the CLI, the ASA provides the **crypto ca trustpoint** command. This command contains a subset of IOS options and additional parameters for existing VPN 3000 features migrating to the ASA. For information on this command and its subcommands, see *Cisco Security Appliance Command Reference*. You can configure all the PKI features in ASDM (see "Enrolling for Digital Certificates" in this guide for more information).

Table 2-1 lists the other new PKI commands.

Table 2-1 New PKI Commands for the ASA

Command Sets	Action
crypto key	Generates key pairs: RSA or DSA.
crl configure	Under **crypto ca trustpoint**, this command enters **crl** configuration mode and lets you configure CRL parameters.
crl	Enables you to configure a large number of parameters carried over from the VPN 3000 Concentrator.
crypto ca authenticate	Obtains a CA certificate by downloading or pasting a certificate from a certification authority.
crypto ca enroll	Initiates enrollment with the CA.
crypto ca import (not a new command)	Installs a certificate received from a CA in response to a manual enrollment request.
crypto ca crl request	Requests a certificate revocation list based on the settings of the specified configuration.
crypto ca certificate map	Maintains a prioritized list of certificate-mapping rules. This command provides for certificate-group matching in the VPN 3000 Concentrator.
tunnel-group-map	Configures policy and rules by which certificate-based IKE sessions are mapped to tunnel groups.

ASDM and WebVPN Sessions per Interface

ASA version 7.1(1) and later supports both WebVPN and an ASDM administrative session on an interface simultaneously. The only restriction is that you must assign different ports for these functions. For example, if you want to run WebVPN using Port 443 for HTTPS traffic, assign a different port to the ASDM administrative session.

Using ASDM, you set the port in the Configuration > VPN > WebVPN > WebVPN Access window.