Introducing the ASA System

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

Brief Overview of Security Policy Features

The ASA system combines Cisco's most powerful firewall, VPN, and intrusion protection features in a best-of-breed security appliance.

- The ASA provides a majority of the software features supported in the VPN 3000 Concentrator, including WebVPN.
- The ASA hardware of the 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 have been updated to support functionality transported into the ASA from the VPN Concentrator and there are many new commands specifically designed for VPN features. For information on 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 device management software provides a multicontext management interface to the ASA system.

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

User Management Differences

Groups and users are core concepts in configuring the security of the VPN 3000 Concentrator. The attributes assigned to groups and users determine a user's access rights. In the VPN 3000, users are by default members of the *base group*. Otherwise, they are members of a customized group. The base group or customized group determines the attribute settings of each user. In the VPN 3000, the base group parameters are most likely to be common across all groups and users. As you configure a group, you can specify that it inherit parameters from the base group; a user can also inherit parameters from the group.

The ASA preserves the notion of groups and includes all of the group attributes provided by the VPN 3000 Concentrator. However, its implementation differs markedly. The ASA access rights to a user as follows:

1. Assigns access rights specified in the user profile.
2. Assigns the remaining rights from the group policy obtained from the first successfully received from the following sequence:
   a. Group policy named in the user profile.
   b. Otherwise, the group policy assigned to the tunnel group.
   c. Otherwise, the default group policy.

The user automatically inherits any attributes not explicitly set in the user profile.

The user attributes also support a null "none" value that you can set to ignore the associated setting in the group policy. Thus, the explicitly set user attribute settings and the remaining settings from the group policy determine the user's access rights to the VPN.

ASA Tunnel Groups, Group Policies, and Users

Note ASA 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

Tunnel groups contain a small number of attributes germane to creating the tunnel itself. These attributes include a pointer to a group policy that defines further connection terms. The ASA includes a default tunnel group for LAN-to-LAN connections named DefaultL2LGroup and one for remote access connections named DefaultRAGroup. You can modify the default tunnel groups and group policy, but you cannot delete them.

Tunnel groups are local to the ASA, and are not configurable on external servers.

Tunnel groups specify the attributes identified in the following sections.

Tunnel group name

Clients select a tunnel group by its name.

- IPSec clients using preshared keys to authenticate pass the group name to the ASA.
- IPSec clients using certificates to authenticate pass this name as part of the certificate distinguished name. The ASA extracts the name from the certificate.
- IPSec clients can code the tunnel group name into the username in the format *username@TunnelGroup*. If the client does not specify the tunnel group in the username, the ASA recalls the tunnel group name used in IKE negotiations.

Connection type

A tunnel group may be either of the following connection types:

- Remote access IPSec.
- LAN-to-LAN IPSec.

Authentication, authorization, and accounting servers

The ASA uses the AAA servers for the following purposes:

- To authenticate users.
- To obtain information about services users are authorized to access.
- To store accounting records.

A server group can consist of one or more servers.

A default group policy for the connection

This is the group policy whose attributes the ASA uses as defaults when authenticating or authorizing a tunnel user. The name of this group policy is DfltGrpPolicy, which you can edit but not delete.

A client address assignment method

This includes values for one or more of the following:

- DHCP servers or address pools that the security appliance assigns to clients.
- RADIUS authentication server group.
- Static IP addresses used by the clients.

IPSec connection parameters

IPSec parameters include the following:

- A client authentication method: preshared keys or certificates.
- ISAKMP keepalive settings.
- Values for defining authorization usernames.

Group Policies

A group policy is a set of user-oriented attributes for IPSec connections. The tunnel group refers to 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 rather than having to specify each attribute individually for each user.

By default, users inherit all user attributes from the assigned group policy. But the ASA also lets you modify individual attributes of group policies for individual users. There is one default group policy, which is named DfltGrpPolicy. You can modify this group policy, but you cannot delete it. You can also create one or more group policies specific to your environment.

In ASDM, use the **Configuration > Features > Device Administration > User Accounts** panel to assign a group policy to users or to modify a group policy for specific users. In the CLI, use the group-policy commands in global configuration mode.

Group policies include the following attributes:

Identity

Identifies the name of the group policy and its type.

- Name—must be unique.
- Type—Internal or External. Internal means that this group policy specifies authentication through a database. External means that this group policy specifies authentication through an external server such as RADIUS.

Tunneling protocols

Configures the tunneling protocols, such as IPSec or WebVPN that this group policy provides.

Filters

Specifies the filter to use for this group policy. Filters, referred to as *access control lists* in the ASA, are rules that determine whether to allow or reject tunneled data packets coming through the ASA, based on criteria such as source address, destination address, and protocol.

Connection settings

Specifies the following connection parameters:

- Access hours—Indicates the name of the selected access hours policy that this group policy uses.
- Simultaneous logins—Specifies the maximum number of simultaneous logins allowed for this group policy.
- Maximum connect time—Specifies the maximum user connection time in minutes.
- Idle timeout values—Specifies the amount of time that a user can be idle in minutes. If there is no communication activity on a user's connection in this period, the system terminates the connection. This value does not apply to WebVPN users.

Defining servers

Configures DNS, WINS, and optionally, the DHCP scope, as follows:

- DNS—Specifies the DNS servers to use. You can specify primary and secondary DNS servers.
- WINS—Specifies the WINS servers to use. You can specify primary and secondary WINS servers.
- DHCP Scope—Specifies the IP subnetwork the DHCP server uses to assign IP addresses to users of the group policy you are configuring.

IPSec settings

Configures the following parameters.

- ReAuth on Rekey—Enables/disables reauthentication when IKE re-key occurs. If reauthentication is enabled, the system prompts a user to enter an ID and password during Phase 1 IKE negotiation and also prompts for user authentication whenever a rekey occurs.
- IP Compression—Shrinks data by replacing repeating information with symbols that use less space.
- Perfect Forward Secrecy—Ensures that the key for a given IPSec SA was not derived from any other secret (such as some other key).
- Tunnel Group Lock—Enables locking of a specified tunnel group, which means that members of the tunnel group are restricted to remote access through this tunnel group only.
- Client Access Rules (access control lists)—configures up to 25 client access rules, which specify values for the priority of the rule, action allowed (permit or deny), and the VPN client type and version.

Client configuration

Configures the following parameters for remote-access VPN clients.

- Banner—Lets a network administer specify and edit text for the banner that the remote-access users see when connecting to the system.
- Default domain—Specifies the name of the default domain that the system passes to the IPSec client, for the client's TCP/IP stack to append to DNS queries that omit the domain field. This domain name applies only to tunneled packets.
- Split tunneling—Configures how to make tunneling decisions (see "Configuring Split Tunneling and Network Lists").
- Cisco client settings—Configures parameters specific to the Cisco VPN client, such as password storage on the client system, IPSec over UDP, UDP port parameter, and so on.

Client firewall

Configures client firewall options, including what type of firewall (if any) and the firewall policy for that firewall.

HW client settings

Configures the following EzVPN client settings for the group policy.

- Secure unit authentication—Enables/disables requirement for interactive client authentication. This requires the EzVPN client to authenticate with a username and password entered manually each time it initiates a tunnel.
- Individual user authentication—Enables/disables requirement for individual user authentication for users behind the EzVPN clients in the tunnel group using the group policy.
- User authentication idle timeout—Specifies the time to wait before terminating the connection when there is no communication activity on the connection.
- IP Phone Bypass—Lets Cisco IP phones bypass the interactive individual user authentication processes.
- LEAP Bypass—Enables/disables LEAP packets traveling from Cisco wireless devices. LEAP (Lightweight Extensible Authentication Protocol) Bypass lets LEAP packets from devices behind a EzVPN client travel across a VPN tunnel prior to individual user authentication.
- Allow Network Extension mode—Enables/disables restriction of network extension mode on the EzVPN client. Network extension mode is required for the EzVPN client to support IP phone connections.

WebVPN

Configures the following parameters for WebVPN connections.

- WebVPN functions, such as enabling URL entry, file server access, entry, browsing, and so on.
- Content filtering—Blocks or removes the parts of websites that do the following:
  - Use Java or Active X
  - Use scripts
  - Display images
  - Deliver cookies
- Homepage—Determines the home page.
- Port forwarding—Sets the port forwarding parameters.
- Server and url lists—Specifies whether to inherit the list of servers and URLs from the default group policy, to select an existing list, or create a new list.
- WebVPN ACL ID—Specifies the identifier of the WebVPN access control list to use.

User Accounts

This is where you assign a group policy to a user. You can also make exceptions for a user to one or more values in a group policy.

Attributes include:

- General
  - Username—Specifies the name of the user to whom the parameters in the user account apply.
  - Password—Specifies the unique password for this user.
  - Privilege Level—Specifies the privilege level assigned to the user account. The range is 0 (lowest) to 15 (highest). The authorization server uses Level 0 to permit VPN access, and the ASA uses Level 15 for the highest administrator access to the CLI commands. You can enter the **show running-config all privilege** CLI command to list all commands and their associated privilege levels.
- VPN Policies
  - Group Policy—Identifies which group policies are available to the user.
  - Tunneling Protocols—Specifies the tunneling protocols that this user can use: IPSec or WebVPN.
  - Filter parameters (ACLs)—Specifies the filter to use. Filters are rules that determine whether to allow or reject tunneled data packets coming through the security appliance based on criteria such as source address, destination address, and protocol.
  - Tunnel Group Lock parameters—Specifies the tunnel group lock that applies to a user. A tunnel group lock restricts users to specific tunnel groups.
  - Store Password on the client system—Controls whether to store the login password on the client system.
  - Connection Settings—Controls the following options: access hours, simultaneous logins, maximum connect time, and idle timeout.
  - Dedicated IP address—Specifies a static IP address and subnet mask.
- WebVPN Policies (see the "Group Policies" section)

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 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	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 supports either WebVPN or an ASDM administrative session on an interface, but not both simultaneously. To use ASDM and WebVPN at the same time, configure them on different interfaces.