Feature Differences

This document helps current users of the VPN 3000 Series Concentrator migrate to the security appliance. The document highlights differences between the two devices and their software. For a full description of the security appliance features, please see the documents in the following list:

- *Cisco ASA 5500 Series Quick Start Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Product CD*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Cisco ASDM Online Help*
- *Cisco ASDM Release Notes*

The security appliance implements most of the features of the VPN 3000 Series Concentrator, but in some instances, the way you configure and use those features differs from what you have been accustomed to on the VPN 3000. This chapter lists some specific ways that the security appliance software differs from that of the VPN 3000 Series Concentrator. Appendix A, "Mapping Topics from VPN 3000 Series Concentrators to ASDM," lists the differences between the graphical user interfaces: VPN 3000 Concentrator Manager and the Adaptive Security Appliance Device Manager.

Mapping Features from the VPN 3000 Concentrators to ASA

Table 1-1 summarizes the mapping of the VPN 3000 Series Concentrator features to those available on ASA.

Table 1-1 Feature Map

Feature Name	VPN 3000	ASA
L2TP, L2TP over IPSec, and PPTP support	Supports L2TP, L2TP over IPSec, and PPTP features.	Does not include L2TP, L2TP over IPSec, or PPTP features.
Default encryption algorithm	3DES is the default for all crypto operations. No licensing is required for any crypto algorithm.	DES is the "base" encryption algorithm; 3DES and AES require "add-on" licenses.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
IKE negotiations	The IKE Phase 1 ID is either a group name (receive only), an IP address, or a certificate DN. The transmitted Phase 1 ID is based on whether the VPN 3000 Concentrator is doing preshared key or certificate negotiation.	ASA supports multiple transforms for IKE Phase 2 and can send multiple proposals for IKE Phase 1. The IKE Phase 1 ID has more options, and it is configurable.
Default Setting of Phase 2 Data Integrity	The default Phase 2 Data Integrity setting is MD5.	The default setting for the Phase 2 Data Integrity value is “off”, for compatibility with previous versions of PIX and IOS. When configuring the security appliance to interoperate with a VPN 3000 Concentrator, you might need to enable Phase 2 data integrity.To *ensure* that IPSec data is authenticated via one of the hashing algorithms (SHA1 or MD5), the network administrator must turn on Phase 2 Data Integrity. To enable Phase 2 Data Integrity, turn on SHA1 or MD5 in the transform sets associated with the crypto maps you are using by following the steps in the section NAME, following this table. These commands enable SHA/HMAC-160 as the hash algorithm.
Low memory actions	Memory red condition prevents new connections when low on memory.	Prevents new connections when the device is out of memory. No “memory red” condition exists.
“Nice Reboot” configuration	Supports the “Nice Reboot” feature, which prevents the VPN 3000 Concentrator from rebooting until some applications have appropriately cleaned up. In the case of IKE, the Concentrator does not reboot until all tunnels are down.	“Nice Reboot” feature works the same as in the VPN 3000, but it is configured differently. First, configure the reboot to wait for the subsystems to clean up before rebooting. Then configure IKE to be notified of the reboot and to allow the reboot when all tunnels are down.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
Hub-and-spoke configuration support	Supports a hub-and-spoke configuration.	Supports a hub-and-spoke configuration that lets encrypted traffic enter, be decrypted, and leave, in the clear, the same interface after firewall rules have been applied. Such "Client U-Turn" remote access connections can terminate on the outside interface of the security appliance, allowing Internet-destined traffic from remote-access user VPN tunnels to leave on the same interface as it arrived, after firewall rules have been applied.
Denial of Service (DoS) attack protection	To prevent a DoS attack, you can block Aggressive Mode. You can also disable DHCP relay.	To prevent a DoS attack, you can block Aggressive Mode.
CLI	Menu-driven selection. The primary interface with the product is the GUI.	PIX/IOS-like statement syntax.
Packet inspection	The VPN 3000 Concentrator does not inspect data going through it.	Because ASA is a firewall, it examines all data and does some level of intelligent inspection.
Configuring users	Users are configured under User Management.	Users are configured under Device Administration.
AIP SSM (Advanced Inspection and Prevention Security Services Module)	Not available	The AIP SSM features available depend on the ASA model.
Logging	Allows 13 severity levels of event logging.	Supports two logging mechanisms: • syslog, with levels 1through 7. This is equivalent to the VPN 3000 event logging function. • dbgtrace, a troubleshooting interface with limited reporting capabilities; for example, dbgtrace displays only to the console. dbgtrace has logging levels 1 through 11, plus 254 and 255. (See Appendix B, "Mapping Debug/Event Levels from VPN 3000 Series Concentrators to the ASA" for an explanation of these levels.)

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
Wildcard Masks	The VPN 3000 Concentrator uses wildcard masks, which are of the 0.0.0.255 variety as well as network masks, which are the inverse of wildcard masks in that they are of the 255.255.255.0 variety. VPN 3000 filters and downloadable ACLs are wildcard-based.	Wildcard masks do not work on the security appliance, which expects network masks in all cases. • When migrating from a VPN 3000 Concentrator to security appliance, network managers must configure security appliance crypto and interface ACLs with netmasks, not wildcards. • Existing VPN 3000 RADIUS DACL configurations must be modified to netmasks. • Mixed VPN 3000 and security appliance deployments, when downloading ACLs from RADIUS require some amount of segmentation, so that the VPN 3000 gets the DACLs with the wildcards, and the security appliance gets the DACLs with the netmasks.
Session timeout	Once some applications establish a TCP connection, they can stay up indefinitely without passing data. The VPN 3000 Concentrator tolerates this, but the security appliance does not.	ASA looks at TCP connections to make sure they active. If they are inactive for a configurable period of time, ASA tears down the TCP connection, which is comparable to terminating tunnels that have been unused for a long time. security appliance times out these sessions without indicating a reason. Thus, the application must reestablish the session to continue.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
PKI and X.509 Certificate Support	No concept of trustpoints.	Major philosophical shift, as well as many syntax changes: • New concept of trustpoints and the way certificates are associated with trustpoints. • Supports IOS-based PKI functions, with the addition of VPN 3000 PKI features.
	RSA keys can be up to 2K in length.	For encrypt/decrypt operations, the security appliance can process RSA keys up to 4K in length.
	Supports VPN client authentication using X.509 certificates.	X.509 certificates support includes support for n-tier certificate chaining (for environments with a multi-level certificate authority hierarchy) and manual enrollment (for environments with offline certificate authorities). This release also supports the new certificate authority introduced in Cisco IOS, a lightweight X.509 certificate authority designed to simplify roll-out of PKI-enabled site-to-site VPN environments.
WebVPN	Configurable, available on all models. Offers features available on the latest Release 4.7 VPN 3000 Concentrator sustaining release, including: • SSL VPN Client • Cisco Secure Desktop • Citrix • NTLM authentication • PDA support.	• Support for WebVPN is equivalent to that available on the VPN 3000 Series Concentrator Release 4.1.7. • WebVPN is not available on PIX hardware.
Licensing	No license required.	Depending on the hardware platform, you can add separate, optional licenses to the base license to gain access to additional features. You can mix and match licenses, as appropriate for the hardware platform. See Appendix A of the *Cisco Security Appliance Command Line Configuration Guide* for details.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
AAA	Uses the concepts of base group, groups, and users.	• ASA has two default tunnel groups, remote access and LAN-to-LAN, instead of the base group. There is only one default group policy. Default groups can no longer be used as a base group for certificate-based tunnels. • The functions of tunnel groups and group policies are split differently from the VPN 3000. Some attributes have moved to the tunnel group. These attributes cannot be configured on an external AAA server. The attributes that are not available in external groups are: – strip-realm – peer-id-validate – authorization-required – authorization-dn-attributes – authentication server type selection – authorization server type selection – radius-with-expiry
	Supports hybrid server groups (that is, servers in a group can be of different types).	Uses the concept of server groups. All servers in a server group must be of the same type.
	No fallback mechanism.	New fallback mechanism, including fallback to LOCAL if the named server is unavailable.
	No accounting for management traffic.	Richer administrative AAA features, including accounting for management traffic.
	RADIUS accounting data goes to a single server.	Supports simultaneous RADIUS accounting. You can specify whether accounting messages are sent to a single server (single mode) or sent to all servers in the group (simultaneous mode).
IPSec	Does not support tunneled ESP (ESP within an ESP tunnel).	Supports tunneled ESP.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
Object Groups	Not used. Instead, the VPN 3000 uses network lists to make configuration easier.	Uses object grouping to simplify access list creation and maintenance.
Group attribute: Group Lock	The Group Lock feature is either enabled or disabled. When enabled, the VPN 3000 checks whether the Group Name used in the VPN Client to establish the connection is the same as the Group Name the user was assigned to. If they are not the same, the connection is dropped. If they are the same, the connection is allowed.	In ASA, the group-lock attribute is part of a group policy, and the value the parameter takes is the actual name of a tunnel group. When group-lock exists in a group policy, the ASA checks during a connection to see whether the Group Name used in the VPN Client is the same as the tunnel-group name found in the group-lock attribute.
Load balancing	Supported for remote sessions initiated with the Cisco VPN Client (Release 3.0 and later), the Cisco VPN 3002 Hardware Client (Release 3.5 or later), or the Cisco PIX 501/506E when acting as an Easy VPN client. Load balancing works with both IPSec clients and WebVPN sessions.	Available only on ASA5520 and ASA5540 systems. Not available for PIX hardware or for ASA 5510 systems.
Modes	No conceptual equivalent	• Supports virtual contexts and transparent versus routed modes. • VPN works only in single routed mode, except that you can have one management session to an ASA in transparent mode.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
Quality of Service (QoS)	Configurable on all models.	Configurable only on ASA 5520 and ASA 5540 models. Not available for PIX hardware.
	Provides bandwidth policing to a maximum rate. Traffic that exceeds the maximum rate is dropped.	You can apply rate-limiting (policing) to all traffic, tunneled or non-tunneled, but you cannot apply rate limiting to priority-classed traffic. The ASA transmits traffic that exceeds the maximum rate, but throttles it to the maximum rate.
	• Guarantees a minimum bandwidth rate for tunneled traffic to assure that no one user can overwhelm the line rate at the interface and starve any other user. • Allows "stealing" of any unused bandwidth under reservation.	Bandwidth reservation is not supported. There is no minimum bandwidth guarantee.
	No low-latency queueing.	• Uses low-latency queueing (LLQ), so you can prioritize certain traffic types through the device. LLQ is *not* rate-limited. • All traffic other than LLQ traffic is considered "best effort." This traffic gets best-effort service after all LLQ traffic has been serviced, up to the depth of the best-effort queue. If the best-effort queue is full, any additional best-effort traffic is dropped.
	Applies only to tunneled traffic and is most commonly applied to the public interface.	You can configure QoS based on either tunnel-group information or ACLs.

Table 1-1 Feature Map (continued)

Feature Name	VPN 3000	ASA
Unlocking firewall function to allow VPN	Not applicable in VPN 3000.	No unlocking needed. After you enable ISAKMP on an interface, the security appliance can negotiate tunnels.
Filters/ACLs	Filters consist of rules that are applied to traffic in the order the rules are arranged on the filter. If a packet matches all the parameters specified in the rule, the system takes the action specified in the rule. If at least one rule parameter does not match, it applies the next rule; and so on. If no rule matches, the system takes the default action specified in the filter. • WebVPN uses filters to control access to specified URLs. • You can configure filters on a VPN Concentrator or on an external RADIUS server for use on the VPN 3000 Concentrator. Configuring a filter involves two steps: • Configuring the basic filter parameters (name, default action, etc. • Assigning rules to a filter. You apply filters to interfaces. These are the most important filters for security, because they govern all traffic through an interface. You also apply filters to groups and users and thus govern *tunneled* traffic through an interface.	• ACLs govern all traffic. • The Cisco ASA 5500 series security appliance supports outbound ACLs and time-based ACLs (building on existing inbound ACL support). Administrators can apply access controls as traffic enters an interface or exits an interface. Time-based access control lists provide administrators greater control over resource usage by defining when certain ACL entries are active. New commands let administrators define time ranges, and then apply these time-ranges to specific ACLs. • You can enable or disable specific ACL entries by appending an “active” or “inactive” keyword to those entries (rules without a keyword are active). This troubleshooting tool can facilitate fine-tuning ACLs.

Enabling Phase 2 Data Integrity for ASA

To *ensure* that IPSec data is authenticated via one of the hashing algorithms (SHA1 or MD5), the network administrator must turn on Phase 2 Data Integrity. To enable Phase 2 Data Integrity, turn on SHA1 or MD5 in the transform sets associated with the crypto maps you are using by following these steps. These commands enable SHA/HMAC-160 as the hash algorithm.

Note In the following descriptions, the terms IKE and ISAKMP are equivalent. VPN documentation tends to use IKE, and ASA tends to prefer ISAKMP (as does PIX). In ASA, all the commands use **isakmp**.

Step 1 Enable SHA/HMAC-160 for the transform-set you are using:

crypto ipsec transform-set *transform-set-name* **esp-3des esp-sha-hmac**

Step 2 Bind the transform set to the crypto map you are using:

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

The following example enables SHA1 for a transform set named ttt, and binds it to a crypto map named abc. The sequence number (seq-num) is 1.

```
hostname(config)# crypto ipsec transform-set ttt esp-3des esp-sha-hmac
hostname(config)# crypto map abc 1 set transform-set ttt
hostname(config)#
```