



Feature Licenses and Specifications

This appendix describes the feature licenses and specifications. This appendix includes the following sections:

- [Supported Platforms, page A-1](#)
- [Platform Feature Licenses, page A-1](#)
- [Security Services Module Support, page A-7](#)
- [VPN Specifications, page A-7](#)

Supported Platforms

This software version supports the following platforms:

- ASA 5510
- ASA 5520
- ASA 5540
- ASA 5550
- PIX 515/515E
- PIX 525
- PIX 535

Platform Feature Licenses

[Table A-1](#) lists the feature support for the ASA 5500 series adaptive security appliances.

[Table A-2](#) lists the feature support for the PIX 500 series security appliances.



Note

Items that are in italics are separate, optional licenses that you can replace the base license. You can mix and match licenses, for example, the 10 security context license plus the Strong Encryption license; or the 500 WebVPN license plus the GTP/GPRS license; or all four licenses together.

Table A-1 ASA 5500 Series Adaptive Security Appliance License Features

Platforms and Features	Licenses											
ASA 5510	Base License						Security Plus					
Security Contexts	No support						No support					
VPN Sessions ¹	250 combined IPSec and WebVPN						250 combined IPSec and WebVPN					
Max. IPSec Sessions	250						250					
Max. WebVPN Sessions	2	Optional Licenses:					2	Optional Licenses:				
		10	25	50	100	250		10	25	50	100	250
VPN Load Balancing	No support						No support					
Failover	None						Active/Standby					
GTP/GPRS	No support						No support					
Max. VLANs	10						25					
Concurrent Firewall Connections ²	50 K						130 K					
Max. Physical Interfaces	3 at 10/100 plus the Management interface for management traffic only (to-the-security-appliance)						Unlimited					
Encryption	Base (DES)		Optional license: Strong (3DES/AES)				Base (DES)		Optional license: Strong (3DES/AES)			
Min. RAM	256 MB						256 MB					
ASA 5520	Base License											
Security Contexts	2	Optional Licenses:										
		5	10	20								
VPN Sessions ¹	750 combined IPSec and WebVPN											
Max. IPSec Sessions	750											
Max. WebVPN Sessions	2	Optional Licenses:										
		10	25	50	100	250	500	750				
VPN Load Balancing	Supported											
Failover	Active/Standby Active/Active											
GTP/GPRS	None		Optional license: Enabled									
Max. VLANs	100											
Concurrent Firewall Connections ²	280 K											
Max. Physical Interfaces	Unlimited											
Encryption	Base (DES)		Optional license: Strong (3DES/AES)									
Min. RAM	512 MB											

Table A-1 ASA 5500 Series Adaptive Security Appliance License Features (continued)

Platforms and Features	Licenses									
ASA 5540	Base License									
Security Contexts	2	Optional licenses:								
		5	10	20	50					
VPN Sessions ¹	5000 combined IPSec and WebVPN									
Max. IPSec Sessions	5000									
Max. WebVPN Sessions	2	Optional Licenses:								
		10	25	50	100	250	500	750	1000	2500
VPN Load Balancing	Supported									
Failover	Active/Standby Active/Active									
GTP/GPRS	None		Optional license: Enabled							
Max. VLANs	200									
Concurrent Firewall Connections ²	400 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)		Optional license: Strong (3DES/AES)							
Min. RAM	1024 MB									
ASA 5550	Base License									
Users, concurrent	Unlimited									
Security Contexts	2	Optional licenses:								
		5	10	20	50					
VPN Sessions ¹	5000 combined IPSec and WebVPN									
Max. IPSec Sessions	5000									
Max. WebVPN Sessions	2	Optional Licenses:								
		10	25	50	100	250	500	750	1000	2500
VPN Load Balancing	Supported									
Failover	Active/Standby Active/Active									
GTP/GPRS	None		Optional license: Enabled							
Max. VLANs	400									
Concurrent Firewall Connections ²	650 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)		Optional license: Strong (3DES/AES)							
Min. RAM	4 GB									

- Although the maximum IPSec and WebVPN sessions add up to more than the maximum VPN sessions, the combined sessions should not exceed the VPN session limit. If you exceed the maximum VPN sessions, you can overload the security appliance, so be sure to size your network appropriately.
- The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

Table A-2 PIX 500 Series Security Appliance License Features

Platforms and Features	Licenses											
PIX 515/515E	R (Restricted)			UR (Unrestricted)			FO (Failover) ¹			FO-AA (Failover Active/Active) ¹		
Security Contexts	No support			2	Optional license: 5		2	Optional license: 5		2	Optional license: 5	
IPSec Sessions	2000			2000			2000			2000		
WebVPN Sessions	No support			No support			No support			No support		
VPN Load Balancing	No support			No support			No support			No support		
Failover	No support			Active/Standby Active/Active			Active/Standby			Active/Standby Active/Active		
GTP/GPRS	None	Optional license: Enabled		None	Optional license: Enabled		None	Optional license: Enabled		None	Optional license: Enabled	
Max. VLANs	10			25			25			25		
Concurrent Firewall Connections ²	48 K			130 K			130 K			130 K		
Max. Physical Interfaces	3			6			6			6		
Encryption	None	Optional licenses:		None	Optional licenses:		None	Optional licenses:		None	Optional licenses:	
		Base (DES)	Strong (3DES/AES)		Base (DES)	Strong (3DES/AES)		Base (DES)	Strong (3DES/AES)		Base (DES)	Strong (3DES/AES)
Min. RAM	64 MB			128 MB			128 MB			128 MB		

Table A-2 PIX 500 Series Security Appliance License Features (continued)

Platforms and Features	Licenses																	
PIX 525	R (Restricted)			UR (Unrestricted)				FO (Failover) ¹				FO-AA (Failover Active/Active) ¹						
Security Contexts	No support			2	Optional licenses:				2	Optional licenses:				2	Optional licenses:			
					5	10	20	50		5	10	20	50		5	10	20	50
IPSec Sessions	2000			2000				2000				2000						
WebVPN Sessions	No support			No support				No support				No support						
VPN Load Balancing	No support			No support				No support				No support						
Failover	No support			Active/Standby Active/Active				Active/Standby				Active/Standby Active/Active						
GTP/GPRS	None	Optional license: Enabled		None	Optional license: Enabled				None	Optional license: Enabled				None	Optional license: Enabled			
Max. VLANs	25			100				100				100						
Concurrent Firewall Connections ²	140 K			280 K				280 K				280 K						
Max. Physical Interfaces	6			10				10				10						
Encryption	None	Optional licenses:		None	Optional licenses:				None	Optional licenses:				None	Optional licenses:			
		Base (DES)	Strong (3DES/AES)		Base (DES)	Strong (3DES/AES)	Base (DES)	Strong (3DES/AES)		Base (DES)	Strong (3DES/AES)							
Min. RAM	128 MB			256 MB				256 MB				256 MB						

Table A-2 PIX 500 Series Security Appliance License Features (continued)

Platforms and Features	Licenses																	
PIX 535	R (Restricted)			UR (Unrestricted)				FO (Failover) ¹				FO-AA (Failover Active/Active) ¹						
Security Contexts	No support			2	<i>Optional licenses:</i>				2	<i>Optional licenses:</i>				2	<i>Optional licenses:</i>			
					5	10	20	50		5	10	20	50		5	10	20	50
IPSec Sessions	2000			2000				2000				2000						
WebVPN Sessions	No support			No support				No support				No support						
VPN Load Balancing	No support			No support				No support				No support						
Failover	No support			Active/Standby Active/Active				Active/Standby				Active/Standby Active/Active						
GTP/GPRS	None	<i>Optional license: Enabled</i>		None	<i>Optional license: Enabled</i>			None	<i>Optional license: Enabled</i>			None	<i>Optional license: Enabled</i>					
Max. VLANs	50			150				150				150						
Concurrent Firewall Connections ²	250 K			500 K				500 K				500 K						
Max. Physical Interfaces	8			14				14				14						
Encryption	None	<i>Optional licenses:</i>		None	<i>Optional licenses:</i>			None	<i>Optional licenses:</i>			None	<i>Optional licenses:</i>					
		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>		<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>	<i>Base (DES)</i>		<i>Strong (3DES/AES)</i>	<i>Base (DES)</i>	<i>Strong (3DES/AES)</i>							
Min. RAM	512 MB			1024 MB				1024 MB				1024 MB						

1. This license can only be used in a failover pair with another unit with a UR license. Both units must be the same model.

2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with one host and one dynamic translation for every four connections.

Security Services Module Support

Table A-3 shows the SSMs supported by each platform:

Table A-3 SSM Support

Platform	SSM Models
ASA 5510	AIP SSM 10 CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5520	AIP SSM 10 AIP SSM 20 CSC SSM 10 CSC SSM 20 4GE SSM
ASA 5540	AIP SSM 10 AIP SSM 20 CSC SSM 10* CSC SSM 20* 4GE SSM
ASA 5550	No support (4GE SSM is built-in and not user-removable)
PIX 515/515E	No support
PIX 525	No support
PIX 535	No support

* CSC SSM licenses support up to 1000 users while the Cisco ASA 5540 Series appliance can support significantly more users. If you deploy CSC SSM with an ASA 5540 adaptive security appliance, be sure to configure the security appliance to send the CSC SSM only the traffic that should be scanned. For guidance with determining what traffic to scan, see the [“Limiting Connections Through the CSC SSM” section on page 19-11](#) for more information.

VPN Specifications

This section describes the VPN specifications for the security appliance. This section includes the following topics:

- [Cisco VPN Client Support, page A-8](#)
- [Cisco Secure Desktop Support, page A-8](#)
- [Site-to-Site VPN Compatibility, page A-8](#)
- [Cryptographic Standards, page A-9](#)

Cisco VPN Client Support

The security appliance supports a wide variety of software and hardware-based Cisco VPN clients, as shown in [Table A-4](#).

Table A-4 Cisco VPN Client Support

Client Type	Client Versions
SSL VPN clients	Cisco SSL VPN client, Version 1.1 or higher
Software IPSec VPN clients	Cisco VPN client for Windows, Version 3.6 or higher Cisco VPN client for Linux, Version 3.6 or higher Cisco VPN client for Solaris, Version 3.6 or higher Cisco VPN client for Mac OS X, Version 3.6 or higher
Hardware IPSec VPN clients (Cisco Easy VPN remote)	Cisco VPN 3002 hardware client, Version 3.0 or higher Cisco IOS Software Easy VPN remote, Release 12.2(8)YJ Cisco PIX 500 series security appliance, Version 6.2 or higher Cisco ASA 5500 series adaptive security appliance, Version 7.0 or higher

Cisco Secure Desktop Support

The security appliance supports CSD software Version 3.1.1.16.

Site-to-Site VPN Compatibility

In addition to providing interoperability for many third-party VPN products, the security appliance interoperates with the Cisco VPN products for site-to-site VPN connectivity shown in [Table A-5](#).

Table A-5 Site-to-Site VPN Compatibility

Platforms	Software Versions
Cisco ASA 5500 series adaptive security appliances	Version 7.0(1) or higher
Cisco IOS routers	Release 12.1(6)T or higher
Cisco PIX 500 series security appliances	Version 5.1(1) or higher
Cisco VPN 3000 series concentrators	Version 3.6(1) or higher

Cryptographic Standards

The security appliance supports numerous cryptographic standards and related third-party products and services, including those shown in [Table A-6](#).

Table A-6 **Cryptographic Standards**

Type	Description
Asymmetric (public key) encryption algorithms	RSA public/private key pairs, 512 bits to 4096 bits DSA public/private key pairs, 512 bits to 1024 bits
Symmetric encryption algorithms	AES—128, 192, and 256 bits DES—56 bits 3DES—168 bits RC4—40, 56, 64, and 128 bits
Perfect forward secrecy (Diffie-Hellman key negotiation)	Group 1— 768 bits Group 2—1024 bits Group 5— 1536 bits Group 7—163 bits (Elliptic Curve Diffie-Hellman)
Hash algorithms	MD5—128 bits SHA-1—160 bits
X.509 certificate authorities	Cisco IOS software Baltimore UniCERT Entrust Authority iPlanet/Netscape CMS Microsoft Certificate Services RSA Keon VeriSign OnSite
X.509 certificate enrollment methods	SCEP PKCS #7 and #10

