



Feature Licenses and Specifications

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

- [Supported Platforms and Feature Licenses, page A-1](#)
- [Security Services Module Support, page A-9](#)
- [VPN Specifications, page A-10](#)

Supported Platforms and Feature Licenses

This software version supports the following platforms; see the associated tables for the feature support for each model:

- ASA 5505, [Table A-1](#)
- ASA 5510, [Table A-2](#)
- ASA 5520, [Table A-3](#)
- ASA 5540, [Table A-4](#)
- ASA 5550, [Table A-5](#)
- PIX 515/515E, [Table A-6](#)
- PIX 525, [Table A-7](#)
- PIX 535, [Table A-8](#)

**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 5505 Adaptive Security Appliance License Features

ASA 5505	Base License		Security Plus	
Users, concurrent ¹	10	<i>Optional Licenses:</i> 50 Unlimited	10	<i>Optional Licenses:</i> 50 Unlimited
Security Contexts	No support		No support	
VPN Sessions ²	10 combined IPSec and WebVPN		25 combined IPSec and WebVPN	
Max. IPSec Sessions	10		25	
Max. WebVPN Sessions	2	<i>Optional License: 10</i>	2	<i>Optional License: 10</i>
VPN Load Balancing	No support		No support	
Failover	None		Active/Standby (no Stateful Failover)	
GTP/GPRS	No support		No support	
Maximum VLANs/Zones	3 (2 regular zones and 1 restricted zone that can only communicate with 1 other zone)		20	
Maximum VLAN Trunks	No support		Unlimited	
Concurrent Firewall Conns ³	10 K		25 K	
Max. Physical Interfaces	Unlimited, assigned to VLANs/zones		Unlimited, assigned to VLANs/zones	
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>
Minimum RAM	128 MB		128 MB	

- In routed mode, hosts on the inside (Business and Home VLANs) count towards the limit when they communicate with the outside (Internet VLAN), including when the inside initiates a connection to the outside as well as when the outside initiates a connection to the inside. Note that even when the outside initiates a connection to the inside, outside hosts are *not* counted towards the limit; only the inside hosts count. Hosts that initiate traffic between Business and Home are also not counted towards the limit. The interface associated with the default route is considered to be the outside Internet interface. If there is no default route, hosts on all interfaces are counted toward the limit. In transparent mode, the interface with the lowest number of hosts is counted towards the host limit. See the **show local-host** command to view host limits.
- 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.

3. 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 ASA 5510 Adaptive Security Appliance License Features

ASA 5510	Base License					Security Plus						
Users, concurrent	Unlimited					Unlimited						
Security Contexts	No support					2	<i>Optional Licenses:</i>					
							5					
VPN Sessions ¹	250 combined IPSec and WebVPN					250 combined IPSec and WebVPN						
Max. IPSec Sessions	250					250						
Max. WebVPN Sessions	2	<i>Optional Licenses:</i>				2	<i>Optional Licenses:</i>					
		10	25	50	100	250		10	25	50	100	250
VPN Load Balancing	No support					No support						
Failover	None					Active/Standby or Active/Active						
GTP/GPRS	No support					No support						
Max. VLANs	50					100						
Concurrent Firewall Conns ²	50 K					130 K						
Max. Physical Interfaces	(For 7.2(1)) 3 at 10/100 plus the Management interface for management traffic only (For 7.2(2) and above) Unlimited					Unlimited (For 7.2(3) and above) Ethernet 0/0 and Ethernet 0/1 are used as Gigabit Ethernet interfaces.						
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>				Base (DES)	<i>Optional license: Strong (3DES/AES)</i>					
Min. RAM	256 MB					256 MB						

1. 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.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table A-3 ASA 5520 Adaptive Security Appliance License Features

ASA 5520	Base License							
Users, concurrent	Unlimited							Unlimited
Security Contexts	2	<i>Optional Licenses:</i>						
		5	10	20				
VPN Sessions ¹	750 combined IPSec and WebVPN							
Max. IPSec Sessions	750							
Max. WebVPN Sessions	2	<i>Optional Licenses:</i>						
		10	25	50	100	250	500	750
VPN Load Balancing	Supported							
Failover	Active/Standby or Active/Active							
GTP/GPRS	None	<i>Optional license: Enabled</i>						
Max. VLANs	150							
Concurrent Firewall Conns ²	280 K							
Max. Physical Interfaces	Unlimited							
Encryption	Base (DES)	<i>Optional license: Strong (3DES/AES)</i>						
Min. RAM	512 MB							

1. 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.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table A-4 ASA 5540 Adaptive Security Appliance License Features

ASA 5540	Base License									
Users, concurrent	Unlimited					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 or Active/Active									
GTP/GPRS	None	Optional license: Enabled								
Max. VLANs	200									
Concurrent Firewall Conns ²	400 K									
Max. Physical Interfaces	Unlimited									
Encryption	Base (DES)	Optional license: Strong (3DES/AES)								
Min. RAM	1 GB									

1. 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.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table A-5 ASA 5550 Adaptive Security Appliance License Features

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	5000	
VPN Load Balancing	Supported										
Failover	Active/Standby or Active/Active										
GTP/GPRS	None	Optional license: Enabled									
Max. VLANs	250										
Concurrent Firewall Conns ²	650 K										
Max. Physical Interfaces	Unlimited										
Encryption	Base (DES)	Optional license: Strong (3DES/AES)									
Min. RAM	4 GB										

1. 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.
2. The concurrent firewall connections are based on a traffic mix of 80% TCP and 20% UDP, with 1 host and 1 dynamic translation for every 4 connections.

Table A-6 PIX 515/515E Security Appliance License Features

PIX 515/515E	R (Restricted)		UR (Unrestricted)		FO (Failover) ¹		FO-AA (Failover Active/Active) ¹		
Users, concurrent	Unlimited		Unlimited		Unlimited		Unlimited		
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 Conns 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:	
		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		

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 1 host and 1 dynamic translation for every 4 connections.

Table A-7 PIX 525 Security Appliance License Features

PIX 525	R (Restricted)		UR (Unrestricted)				FO (Failover) ¹				FO-AA (Failover Active/Active) ¹			
Users, concurrent	Unlimited		Unlimited				Unlimited				Unlimited			
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 Conns 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			

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 1 host and 1 dynamic translation for every 4 connections.

Table A-8 PIX 535 Security Appliance License Features

PIX 535	R (Restricted)		UR (Unrestricted)				FO (Failover) ¹				FO-AA (Failover Active/Active) ¹				
Users, concurrent	Unlimited		Unlimited				Unlimited				Unlimited				
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 Conns 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>		<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 1 host and 1 dynamic translation for every 4 connections.

Security Services Module Support

Table A-9 shows the SSMs supported by each platform:

Table A-9 SSM Support

Platform	SSM Models
ASA 5505	No support
ASA 5510	AIP SSM 10 AIP SSM 20 CSC SSM 10 CSC SSM 20 4GE SSM

Table A-9 SSM Support (continued)

Platform	SSM Models
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 ¹ CSC SSM 20 ¹ 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

1. The 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 more information, see the [“Determining What Traffic to Scan” section on page 22-9](#) 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-11](#)
- [Cisco Secure Desktop Support, page A-11](#)
- [Site-to-Site VPN Compatibility, page A-11](#)
- [Cryptographic Standards, page A-12](#)

Cisco VPN Client Support

The security appliance supports a wide variety of software and hardware-based Cisco VPN clients, as shown in [Table A-10](#).

Table A-10 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-11](#).

Table A-11 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-12](#).

Table A-12 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