



# Cisco ASA 5580 Series Release Notes Version 8.1(1)

---

**January 2009**

This document includes the following sections:

- [Introduction to the Cisco ASA 5580 Series Adaptive Security Appliance, page 1](#)
- [System Requirements, page 2](#)
- [New Features, page 5](#)
- [Important Notes, page 6](#)
- [Caveats, page 7](#)
- [End-User License Agreement, page 8](#)
- [Related Documentation, page 8](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 8](#)

## Introduction to the Cisco ASA 5580 Series Adaptive Security Appliance

Version 8.1 introduces the ASA 5580-20 and ASA 5580-40 adaptive security appliances. In addition to world-class performance, Version 8.1 also introduces new features and capabilities in the areas of scalable logging, system environmental monitoring, VPN Remote Access user limits, 10 Gigabit Ethernet interfaces, jumbo frame and more.

The ASA 5580-20 delivers 5 Gigabits per second of TCP traffic and UDP performance is even greater. Many features in the system are made multi-core capable to achieve this high throughput. In addition the system delivers greater than 60,000 TCP connections per second and supports up to 1 million connections.

The ASA 5580-40 delivers 10 Gigabits per second of TCP traffic and similar to ASA 5580-20 the UDP performance will be even greater. The ASA 5580-40 delivers greater than 120,000 TCP connections per second and up to 2 million connections in total.



---

**Americas Headquarters:**  
**Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA**

© 2008 Cisco Systems, Inc. All rights reserved.

The ASA 5580-20 and the ASA 5580-40 supports 50 security contexts and up to 100 VLAN interfaces (250 VLAN interfaces will be supported in a future release) and 1 Gigabit of IPSEC VPN 3DES performance. They support up to 24 Gigabit data ports or up to 12 Ten Gigabit data ports as well as two additional Gigabit ports for management. Optional redundant, hot-swappable power capabilities are available as well as hot-swappable cooling fans in case of a fan failure.

NetFlow version 9 will be used to export information about the progression of a flow from start to finish. The NetFlow implementation will export records indicating significant events in the life of a flow. This is different from traditional NetFlow which exports data about flows at regular intervals. The NetFlow module will also export records about the flows that are denied by Access Lists. You can configure an ASA5580 to send the following events using NetFlow:

- Flow Creation
- Flow Teardown
- Flow Denied - Only flows denied by ACL will be reported in the first release.

The system includes environmental monitoring which tracks the operational status of the Fans and power supplies. In addition, it tracks the temperatures of the CPUs and the ambient temperature of the system. ASDM provides you with a quick view into these items on the Device Dashboard and the new **show environment** command has been introduced to provide the information as well.

The ASA 5580 will also support up to 1000 SSL VPN peers, and up to 10,000 total VPN peers.

This release also introduces support for 10 Gigabit Ethernet interfaces and support for jumbo frames up to 9000.

In addition to the above, enhancements have been made to many existing commands to provide greater visibility to the operations of the high performance ASA 5580. You will find changes in the following commands: **show version**, **show activation-key**, **show interface**, **show tech**, **show asp**, and more.

For more information on all the new features, see [New Features, page 5](#).

Additionally, the adaptive security appliance software supports Cisco Adaptive Security Device Manager (ASDM). ASDM delivers world-class security management and monitoring through an intuitive, easy-to-use web-based management interface. Bundled with the adaptive security appliance, ASDM accelerates adaptive security appliance deployment with intelligent wizards, robust administration tools, and versatile monitoring services that complement the advanced integrated security and networking features offered by the market-leading suite of the adaptive security appliance. Its secure, web-based design enables anytime, anywhere access to adaptive security appliances. For more information on ASDM, see the [Cisco ASDM Release Notes Version 6.1](#).

## System Requirements

The sections that follow list the system requirements for operating an adaptive security appliance. This section includes the following topics:

- [Memory Requirements, page 3](#)
- [Determining the Software Version, page 4](#)
- [Installing or Upgrading Cisco Secure Desktop, page 5](#)

## Memory Requirements

Table 1 lists the DRAM memory requirements for the adaptive security appliance. The memory listed in this table is the default value that ships with each adaptive security appliance.

**Table 1** DRAM Memory Requirements

| ASA Model | Default DRAM Memory (GB) |
|-----------|--------------------------|
| 5580-20   | 8GB                      |
| 5580-40   | 12GB                     |



### Note

On both the ASA 5580-20 and the ASA 5580-40 adaptive security appliances only 4GB of memory is available for features. The rest are reserved or used by the OS. The **show memory** command will only display values relative to 4GB.

You can check the size of internal flash and the amount of free flash memory on the adaptive security appliance by doing the following:

- **ASDM**—Click **Tools > File Management**. The amounts of total and available flash memory appear on the bottom left in the pane.
- **CLI**—In Privileged EXEC mode, enter the **dir** command. The amounts of total and available flash memory appear at the bottom of the output.

For example:

```
hostname # dir
Directory of disk0:/

 2      drwx  4096      11:22:00 Dec 01 2006  cisco_config
 43     -rwx 14358528   08:46:02 Feb 19 2007  cdisk.bin
 44     -rwx  4634      14:32:48 Sep 17 2004  first-backup
 45     -rwx  4096      09:55:02 Sep 21 2004  fsck-2451
 46     -rwx  4096      09:55:02 Sep 21 2004  fsck-2505
 47     -rwx   774      10:48:04 Nov 21 2006  profile.tmpl
 48     -rwx 406963     12:45:34 Feb 06 2007  svc
 3      drwx  8192      03:35:24 Feb 02 2007  log
 49     drwx  4096      07:10:54 Aug 09 2006  1
 50     -rwx 21601      14:20:40 Dec 17 2004  tftp
 51     -rwx 17489      06:36:40 Dec 06 2006  custom.xml
136    -rwx 12456368    10:25:08 Feb 20 2007  asdmfile
 53     -rwx 20498      13:04:54 Feb 12 2007  tomm_english
 54     drwx  4096      14:18:56 Jan 14 2007  sdesktop
 56     -rwx 14358528   08:32:30 Feb 19 2007  asa800-215-k8.bin
 57     -rwx 10971      09:38:54 Apr 20 2006  cli.lua
 58     -rwx 6342320    08:44:54 Feb 19 2007  asdm-600110.bin
 59     -rwx   0        04:38:52 Feb 12 2007  LOCAL-CA-SERVER.udb
 60     -rwx  322       15:47:42 Nov 29 2006  tmpAsdmCustomization1848612400
 8      -rwx  65111     10:27:48 Feb 20 2007  tomm_backup.cfg
 61     -rwx 416354     11:50:58 Feb 07 2007  sslclient-win-1.1.3.173.pkg
 62     -rwx 23689      08:48:04 Jan 30 2007  asa1_backup.cfg
 63     -rwx 45106      07:19:18 Feb 12 2007  securedesktop_asa_3_2_0_54.pkg
 64     -rwx  224       01:22:44 Oct 02 2006  LOCAL-CA-SERVER.crl
 65     drwx  4096      12:37:24 Feb 20 2007  LOCAL-CA-SERVER
 66     -rwx  425       11:45:52 Dec 05 2006  anyconnect
 67     -rwx 1555       10:18:04 Sep 29 2006  LOCAL-CA-SERVER_00001.p12
 68     -rwx   0        12:33:54 Oct 01 2006  LOCAL-CA-SERVER.cdb
```

```

69      -rwx  3384309      07:21:46 Feb 12 2007  securedesktop_asa_3_2_0_57.pkg
70      -rwx   774         05:57:48 Nov 22 2006  cvcprofile.xml
71      -rwx   338         15:48:40 Nov 29 2006  tmpAsdmCustomization430406526
72      -rwx    32         09:35:40 Dec  8 2006  LOCAL-CA-SERVER.ser
73      -rwx  2205678      07:19:22 Jan  5 2007  vpn-win32-Release-2.0.0156-k9.pkg
74      -rwx  3380111      11:39:36 Feb 12 2007  securedesktop_asa_3_2_0_56.pkg

```

```
62881792 bytes total (3854336 bytes free)
```

```
hostname #
```

In a failover configuration, the two units must have the same hardware configuration, must be the same model, must have the same number and types of interfaces, and must have the same amount of RAM. For more information, see the [Configuring Failover](#) chapter in the *Cisco Security Appliance Command Line Configuration Guide*.


**Note**

If you use two units with different flash memory sizes, make sure that the unit with the smaller flash memory has enough space for the software images and configuration files.

## Determining the Software Version

Use the **show version** command to verify the software version of your adaptive security appliance. Alternatively, the software version appears on the Cisco ASDM home page.

## Downloading the Software

You can download the software from the following URL:

<http://www.cisco.com/cisco/software/navigator.html>

To download the software to flash memory, choose one of the following commands for the appropriate download server type:

- To copy from a TFTP server, enter the following command:

```
hostname# copy tftp://server[/path]/filename {flash:/ | disk0:/ |
disk1:/}[path/]filename
```

You can enter **flash:/** or **disk0:/** for the internal flash memory on the adaptive security appliance. The **disk1:/** keyword represents the external flash memory on the adaptive security appliance.

- To copy from an FTP server, enter the following command:

```
hostname# copy ftp://[user[:password]@]server[/path]/filename {flash:/ | disk0:/ |
disk1:/}[path/]filename
```

- To copy from an HTTP or HTTPS server, enter the following command:

```
hostname# copy http[s]://[user[:password]@]server[:port][/path]/filename {flash:/ |
disk0:/ | disk1:/}[path/]filename
```

- To use secure copy, first enable SSH, then enter the following command:

```
hostname# ssh scopy enable
```

Then from a Linux client, enter the following command:

```
scp -v -pw password filename username@asa_address
```

The **-v** specifies verbose. If **-pw** is not specified, you are prompted for a password.

## Installing or Upgrading Cisco Secure Desktop

Cisco Secure Desktop Release 3.2 requires ASA Version 8.1. You do not need to restart the adaptive security appliance after you install or upgrade Cisco Secure Desktop.



**Note** Archive and delete the Secure Desktop `desktop/data.xml` configuration file before upgrading to Cisco Secure Desktop 3.2. To create a clean configuration file, uninstall Cisco Secure Desktop before reinstalling it.

The expanded flexibility provided by a prelogin assessment sequence editor, and replacement of the Cisco Secure Desktop feature policies with a dynamic access policy (DAP) configured on the adaptive security appliance, are incompatible with Cisco Secure Desktop 3.1.1 configurations. Cisco Secure Desktop automatically inserts a new, default configuration file when it detects that one is not present.

For consistency with the previous release notes, these instructions provide the CLI commands needed to install Secure Desktop. You may, however, prefer to use ASDM. To do so, choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup** and click **Help**.

To install or upgrade the Cisco Secure Desktop software, perform the following steps:

- 
- Step 1** Download the latest Cisco Secure Desktop package file from the following web site and install it on the flash memory card of the adaptive security appliance:
- <http://tools.cisco.com/Support/BugToolKit/>
- Step 2** Enter the following commands to access webvpn configuration mode:
- ```
hostname# config terminal
hostname(config)# webvpn
hostname(config-webvpn)#
```
- Step 3** To validate the Cisco Secure Desktop distribution package and add it to the running configuration, enter the following command in webvpn configuration mode:
- ```
hostname(config-webvpn)# csd image disk0:/securedesktop_asa_3_2_0_build.pkg
hostname(config-webvpn)#
```
- Step 4** To enable Cisco Secure Desktop for management and remote user access, use the **csd enable** command in webvpn configuration mode. To disable Cisco Secure Desktop, use the **no** form of this command.
- ```
hostname(config-webvpn)# csd enable
hostname(config-webvpn)#
```
- 

## New Features

Released: March 1, 2008

Table 2 lists the new features for ASA Version 8.1(1). This ASA software version is only supported on the ASA 5580.

**Table 2**      **New Features for ASA Version 8.1(1)**

| Feature                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Introduction of the Cisco ASA 5580 | <p>The Cisco ASA 5580 comes in two models:</p> <ul style="list-style-type: none"> <li>• The ASA 5580-20 delivers 5 Gigabits per second of TCP traffic and UDP performance is even greater. Many features in the system have been made multi-core capable to achieve this high throughput. In addition the system delivers greater than 60,000 TCP connections per second and supports up to 1 million connections.</li> <li>• The ASA 5580-40 will deliver 10 Gigabits per second of TCP traffic and similar to ASA 5580-20 the UDP performance will be even greater. The ASA 5580-40 delivers greater than 120,000 TCP connections per second and up to 2 million connections in total.</li> </ul> |
| NetFlow                            | <p>The new NetFlow feature enhances the ASA logging capabilities by logging flow-based events through the NetFlow protocol. For detailed information about this feature and the new CLI commands, see the <i>Cisco ASA 5580 Adaptive Security Appliance Command Line Configuration Guide</i>.</p>                                                                                                                                                                                                                                                                                                                                                                                                   |
| Jumbo frame support                | <p>The Cisco ASA 5580 supports jumbo frames when you enter the <b>jumbo-frame reservation</b> command. A jumbo frame is an Ethernet packet larger than the standard maximum of 1518 bytes (including Layer 2 header and FCS), up to 9216 bytes. You can enable support for jumbo frames for all interfaces by increasing the amount of memory to process Ethernet frames. Assigning more memory for jumbo frames might limit the the maximum use of other features, such as access lists.</p>                                                                                                                                                                                                       |
| Timeout for SIP Provisional Media  | <p>You can now configure the timeout for SIP provisional media using the <b>timeout sip-provisional-media</b> command.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Details about the activation key   | <p>You can now view the permanent and temporary activation keys with their enabled features, including all previously installed temporary keys and their expiration dates using the <b>show activation key detail</b> command.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

## Important Notes

Please note the following:

- [Security Appliance Platform Support, page 7](#)
- [No .NET over Clientless, page 7](#)

## Security Appliance Platform Support

Version 8.1 is only supported on ASA 5580-20 and ASA 5580-40 adaptive security appliances.

## No .NET over Clientless

Clientless sessions do not support .NET framework applications (CSCsv29942).

## Caveats

The following sections describe the caveats for Version 8.1.

For your convenience in locating caveats in the Cisco Bug Toolkit, the caveat titles listed in this section are drawn directly from the Bug Toolkit database. These caveat titles are not intended to be read as complete sentences because the title field length is limited. In the caveat titles, some truncation of wording or punctuation may be necessary to provide the most complete and concise description. The only modifications made to these titles are as follows:

- Commands are in **boldface** type.
- Product names and acronyms may be standardized.
- Spelling errors and typos may be corrected.



**Note** If you are a registered cisco.com user, view Bug Toolkit on cisco.com at the following website:

<http://tools.cisco.com/Support/BugToolKit/>

To become a registered cisco.com user, go to the following website:

<http://tools.cisco.com/RPF/register/register.do>

## Open Caveats - Version 8.1

**Table 3**      *Open Caveats*

| DDTS Number | Software Version 8.1 |                                                                         |
|-------------|----------------------|-------------------------------------------------------------------------|
|             | Corrected            | Caveat                                                                  |
| CSCsm95566  | No                   | EIGRP: Does not send ALL redistributed static routes to peer devices    |
| CSCsm69576  | No                   | FT: "failover active" with 5000 IPsec RAS tunnels causes FO instability |
| CSCsl08271  | No                   | Standby Unit show incorrect memory usage in Admin context               |
| CSCsm12724  | No                   | page fault in PTHREAD-462 - eip wakeup+45 at finesse/thread.c:374       |
| CSCsm18209  | No                   | traceback: CHECKHEAPS HAS DETECTED A MEMORY CORRUPTION                  |
| CSCsm86597  | No                   | ASA console stops accepting input after "show crash webvpn detail"      |

Table 3 Open Caveats (continued)

| DDTS Number | Software Version 8.1 |                                                                       |
|-------------|----------------------|-----------------------------------------------------------------------|
|             | Corrected            | Caveat                                                                |
| CSCsm93700  | No                   | ACL logging prints 106100 always at informational level               |
| CSCsm86188  | No                   | FT: after multi-mode stress in routed, transp mode connectivity fails |
| CSCsm56371  | No                   | Shared management intf in active-active does not work                 |
| CSCsm80578  | No                   | FT: cannot establish 10,000 WebVPN sessions with full traffic         |

## End-User License Agreement

For information on the end-user license agreement, go to:

[https://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN\\_.html](https://www.cisco.com/en/US/docs/general/warranty/English/EU1KEN_.html)

## Related Documentation

For additional information on the adaptive security appliance, go to:

[http://www.cisco.com/en/US/products/ps6120/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html)

## Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2009 Cisco Systems, Inc.

All rights reserved.