Release Notes for the Cisco ASA 1000V, Version 8.7(x)

Updated: October 16, 2012
Released: August 20, 2012

This document contains release information for the Cisco ASA 1000V, Version 8.7(1.1) and includes the following sections:

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

Important Notes

Complete Solution Installation

- Neither the ASA 1000V nor VSG supports non-ASCII characters. To support localization, all components (that is, Cisco VNMC, Cisco VSG, and ASA 1000V) must meet this requirement.
- The ASA 1000V and Cisco VNMC require that the VMware vCenter installation, including keyboard and password or shared key settings, be set to American English.

ASA 1000V Installation

- You can use only one management mode (either VNMC or ASDM) on the ASA 1000V. They are mutually exclusive, and you need to decide on the mode before installation. If you want to switch management modes, you must reinstall the ASA 1000V.
- ASDM is used to monitor traffic on the ASA 1000V in both VNMC and ASDM modes.
- Routes through the management interface can only be configured using the CLI in VNMC mode.
- The VMs that are on the inside of the ASA 1000V need to be directly connected to a Nexus 1000V switch and in the same VLAN as the one you have configured on the inside of the ASA 1000V. Inside VMs must be layer 2 adjacent to the inside of the ASA 1000V. You cannot have a layer 3 hop, as with a physical router, on the inside of the ASA 1000V.

Limitations and Restrictions

The ASA 1000V does not support all features that are supported on ASA appliances. Table 1 lists the unsupported features on the ASA 1000V.

Note The commands that are associated with an unsupported feature are not available at the ASA 1000V CLI. Not all commands that are supported on ASA appliances are available on the ASA 1000V platform.

Table 1 Unsupported Features on the ASA 1000V

Feature	Description
AAA for network access	Not supported.
Active/Active failover and subsecond failover	Not supported.
Authentication using certificates	Not supported.
Shun	Not supported.
Botnet traffic filter	Not supported.
Dynamic DNS	Not supported.
Dynamic routing	Not supported.
GTP/GTPRS (Mobile Service Providers)	Not supported.
HTTP inspection maps for deep-packet inspection	Not supported.
Identity firewall	Not supported.
Inbound PAT	Not supported.
IPS and CSC modules	Not supported.

Table 1 Unsupported Features on the ASA 1000V (continued)

Feature	Description
IPv6	Not supported
Multiple contexts	Not supported.
NetFlow	Not supported.
PPPoE/VPDN	Not supported.
QoS	Not supported.
Redundant interfaces, EtherChannel interfaces, and subinterfaces	Not supported.
Threat detection	Not supported.
Transparent mode	Not supported.
Unified communications	Not supported. (Includes TLS Proxy, Phone Proxy, Proxy Limit, and IME.)
URL filtering	Not supported.
VPN remote access	Not supported. (Includes Remote Access, Clientless (SSL) Access, Multi-site (SSL) Access, Easy VPN on the ASA 5505, VPN Phones, AnyConnect Essentials, and AnyConnect Mobile.)
WCCP	Not supported.

System Requirements

This section describes the system requirements for using the ASA 1000V and includes the following topics:

Minimum Component Requirements for the ASA 1000V

Before you install the ASA 1000V, the following components must already be installed and configured:

- An x86 Intel server with a 64-bit processor, listed in the VMware Hardware Compatibility List, which runs VMware vSphere Hypervisor software 4.1 or 5.0 with a minimum of two processors of at least 1.5 GHz each, 8 GB of physical RAM, and 30 GB of disk space, with an Enterprise Plus license
- VMware vCenter 4.1 or 5.0 to manage the VMware vSphere Hypervisor, with an Enterprise Plus license
- Cisco Nexus 1000V Distributed Virtual Switch (DVS), version 4.2(1)SV1(5.2), created in VMware vCenter
- Cisco Nexus 1000V Virtual Ethernet Module (VEM) installed and running in the VMware vSphere Hypervisor host

- A VMware vSphere Hypervisor host added in the Cisco Nexus 1000V Distributed Virtual Switch (DVS)
- Four VLANs in the Cisco Nexus 1000V Virtual Supervisor Module (VSM): an inside VLAN for the ASA 1000V inside interface and an outside VLAN for the outside interface
- Internet Explorer 9.0 or Mozilla Firefox 10.0 with Adobe Flash Player 11.1
- Virtual Network Management Center (VNMC) Version 2.0
- (Optional) Virtual Security Gateway (VSG) Release 1.4

Memory Information

This section includes the following topics:

Memory Requirements and Allocation

VM resources are preset in the OVA file that is used to deploy the ASA 1000V. We recommend that you not change these settings.

The ASA 1000V allocates 1.5 GB of RAM per allocated CPU. One vCPU is allocated and a maximum of 5000 MHz is assigned to the ASA 1000V VM. Two virtual disks are created—one with 2 GB and one with 128 MB. If you have allocated less than this amount of memory, a warning message about insufficient memory appears on the console each time that you log in.

The following applies:

- If you allocate more than 100 percent of the allowable CPU limit (or of the allowable memory allocation), the ASA 1000V reboots after 24 hours.
- If you allocate more than 125 percent of the CPU limit, the ASA 1000V reboots after one hour.
- If you increase the vCPU limit, the ASA 1000V reboots immediately.
- If you decrease the amount of allocated memory, a warning message appears about insufficient memory and the ASA 1000V may not start.
- If you decrease both the amount of allocated memory and the CPU limit, performance will be degraded.
- Each ASA 1000V allocates 2.1 GB of hard disk space from the data store.

See the **show memory** and **show cpu** commands in the *Cisco ASA 5500 Series Command Reference* for more information.

Viewing Flash Memory

You can check the size of internal flash memory and the amount of free flash memory on the ASA 1000V by doing the following:

- ASDM—Choose **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.

DRAM, Flash Memory, and Failover

In a failover configuration, the two ASA 1000V instances must have the same amount of assigned DRAM.

ASA 1000V and ASDM Compatibility

Table 2 lists information about the ASA 1000V and ASDM compatibility.

Table 2 ASA 1000V and ASDM Compatibility

Application	Description
ASDM	ASA 1000V Version 8.7(1.1) requires ASDM Version 6.7(1). For information about ASDM requirements for other releases, see *Cisco ASA Compatibility* at: http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html

New Features

Note New, changed, and deprecated syslog messages are listed in the syslog messages guide.

Released: October 16, 2012

Table 3 lists the new features for ASA Version 8.7(1.1).

Note Version 8.7(1) was removed from Cisco.com due to build issues; please upgrade to Version 8.7(1.1) or later.

Table 3 New Features for ASA Version 8.7(1.1)

Feature	Description
Platform Features	
Support for the ASA 1000V	We introduced support for the ASA 1000V for the Nexus 1000V switch.
Cloning the ASA 1000V	You can add one or multiple instances of the ASA 1000V to your deployment using the method of cloning VMs.
Management Features	
ASDM mode	You can configure, manage, and monitor the ASA 1000V using the Adaptive Security Device Manager (ASDM), which is the single GUI-based device manager for the ASA.
VNMC mode	You can configure and manage the ASA 1000V using the Cisco Virtual Network Management Center (VNMC), which is a GUI-based multi-device manager for multiple tenants.

Table 3 New Features for ASA Version 8.7(1.1) (continued)

Feature	Description
XML APIs	You can configure and manage the ASA 1000V using XML APIs, which are application programmatic interfaces provided through the Cisco VNMC. This feature is only available in VNMC mode.
Firewall Features	
Cisco VNMC access and configuration	Cisco VNMC access and configuration are required to create security profiles. You can configure access to the Cisco VNMC through the Configuration > Device Setup > Interfaces pane in ASDM. Enter the login username and password, hostname, and shared secret to access the Cisco VNMC. Then you can configure security profiles and security profile interfaces. In VNMC mode, use the CLI to configure security profiles.
Security profiles and security profile interfaces	Security profiles are interfaces that correspond to an edge security profile that has been configured in the Cisco VNMC and assigned in the Cisco Nexus 1000V VSM. Policies for through-traffic are assigned to these interfaces and the outside interface. You can add security profiles through the Configuration > Device Setup > Interfaces pane. You create the security profile by adding its name and selecting the service interface. ASDM then generates the security profile through the Cisco VNMC, assigns the security profile ID, and automatically generates a unique interface name. The interface name is used in the security policy configuration. We introduced or modified the following commands: **interface security-profile**, **security-profile**, **mtu**, **vpath path-mtu, clear interface security-profile**, **clear configure interface security-profile**, **show interface security-profile**, **show running-config interface security-profile**, **show interface ip brief**, **show running-config mtu**, **show vsn ip binding**, **show vsn security-profile**.
Service interface	The service interface is the Ethernet interface associated with security profile interfaces. You can only configure one service interface, which must be the inside interface. We introduced the following command: **service-interface security-profile all**.
VNMC policy agent	The VNMC policy agent enables policy configuration through both the ASDM and VNMC modes. It includes a web server that receives XML-based requests from Cisco VNMC over HTTPS and converts it to the ASA 1000V configuration. We introduced the following commands: **vnmc policy-agent**, **login**, **shared-secret**, **registration host**, **vnmc org**, **show vnmc policy-agent, show running-config vnmc policy-agent, clear configure vnmc policy-agent.**

VMware Feature Support for the ASA 1000V

Table 4 lists the VMware feature support for the ASA 1000V.

Table 4 VMware Feature Support for the ASA 1000V

Feature	Description	Support (Yes/No)	Comment
Cold clone	The VM is powered off before cloning.	Yes	—
DRS	Used for dynamic resource scheduling and distributed power management.	Yes	—
Hot clone	The VM is running during cloning.	No	—
Snapshot	Freezes the VM for a few seconds. You may loose traffic. Failover may occur.	See comment.	Use with care.
VM migration	Used for VM migration.	Yes	—
vMotion	Used for live migration of VMs.	Yes	—
VMware FT	Used for HA for VMs.	No	Use ASA failover for ASA VM failures.
VMware HA	Used for ESX and server failures.	Yes	Use ASA failover for ASA VM failures.
VMware HA with VM heartbeats	Used for VM failures.	No	Use ASA failover for ASA VM failures.

Upgrading the ASA and ASDM Software

This section describes how to upgrade to the latest version and includes the following topics:

- Viewing Your Current Version, page 7
- Upgrading the ASA and ASDM Images, page 7

For ASDM procedures, see the ASDM release notes.

Viewing Your Current Version

Use the **show version** command to verify the software version of your ASA.

Upgrading the ASA and ASDM Images

This section describes how to install the ASDM and ASA images using TFTP. For FTP or HTTP, see the "Managing Software and Configurations" chapter in the *Cisco ASA 1000V CLI Configuration Guide for ASDM Mode*.

We recommend that you upgrade the ASDM image before the ASA image. You must upgrade the ASA by copying files through the ASA CLI. You must use the 6.7(1) version of the ASDM image; you cannot use another older version of the ASDM image with the ASA.

Note The VNMC does not support ASA image upgrade.

For information about upgrading software in a failover pair, see the "Performing Zero Downtime Upgrades for Failover Pairs" chapter in the *Cisco ASA 1000V CLI Configuration Guide for ASDM Mode*.

Detailed Steps

Step 1 If you have a Cisco.com login, you can obtain the ASA and ASDM images from the following website:

http://www.cisco.com/cisco/software/navigator.html?mdfid=279513386&i=rm

Step 2 Back up your configuration file. To print the configuration to the terminal, enter the following command:

```
hostname# show running-config
```

Copy the output from this command, and then paste the configuration into a text file.

For other backup methods, see the "Managing Software and Configurations" chapter in the *Cisco ASA 1000V CLI Configuration Guide for ASDM Mode*.

Step 3 Install the new images using TFTP. Enter the following command separately for the ASA image and the ASDM image:

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

For example:

```
hostname# copy tftp://10.1.1.1/asa870-4-k8.bin disk0:/asa871-k8.bin
...
hostname# copy tftp://10.1.1.1/asdm-67099.bin disk0:/asdm-671.bin
```

If the ASA does not have enough memory to hold two images, overwrite the old image with the new one by specifying the same destination filename as the existing image.

Step 4 Restart the ASA by entering the following command.

```
hostname(config)# reload
```

Step 5 You can choose the new boot image manually if it is not the default image. Change the ASA boot image to the new image name by entering the following commands:

```
hostname(config)# clear configure boot
hostname(config)# boot system {disk0:/ | disk1:/}[path/]new_filename
```

For example:

```
hostname(config)# clear configure boot
hostname(config)# boot system disk0:/asa871-k8.bin
hostname(config)# show boot
Boot variable = (hd1,0)/cdisk.smp
Current BOOT variable = disk0:/cdisk.smp
CONFIG_File variable =
Current CONFIG_FILE variable =
```

Step 6 Configure the ASDM image to the new image name by entering the following command:

```
hostname(config)# asdm image {disk0:/ | disk1:/}[path/]new_filename
```

Step 7 Save the configuration and reload by entering the following commands:

```
hostname(config)# write memory
hostname(config)# reload
```

Open Caveats

Table 5 lists open caveats in the ASA 1000V 8.7(1.1) release.

If you are a registered Cisco.com user, view more information about each caveat using the Bug Toolkit at the following website:

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

Table 5 Open Caveats in ASA 1000V Version 8.7(1.1)

Caveat	Description
CSCty75440	Traceback after vMotion ASA1000V in a failover setup.
CSCua59019	ACL with vZone is accepted wtihout error.
CSCua73963	Security profile interface configuration is allowed from console in VNMC mode.
CSCua79561	Edge profile configuration may fail under rare conditions.
CSCua86888	SPID to edge profile mapping mismatch between Cisco VNMC and ASA 1000V.
CSCua86898	**Setup** command adds route for Cisco VNMC IP in same subnet.
CSCua89185	Ping to inside fails when static dest NAT applied on outside.
CSCub02459	TCP connection not reset after timeout.
CSCub24747	Failed to process certificate error in failover setup.
CSCub27241	Incorrect behavior when applying erroneous policies in Cisco VNMC.
CSCub29529	Smart call home does not work for ASA 1000V.
CSCub35003	Policy map not created before being used in VNMC mode.
CSCub41235	Unsupported VPN configuration allowed in the CLI.
CSCub49338	FDD msg not clear when configuring ACL IPv4 protocol and port number.
CSCub52140	Editing DHCP relay server IP does not push the config to ASA 1000V.
CSCub54235	Unsupported SNMP command **fru-insert/fru-remove** in CLI.
CSCub56227	Unable to export capture with **/add-spid** to TFTP/FTP from CLI.
CSCub62281	Incorrect error message if ACL contains vZones with no protocol.
CSCub66617	IP binding not displayed after no org and reconfigure org on VSM

Licensing for the ASA 1000V

The ASA 1000V is licensed per each CPU socket that it is protecting. The Cisco Nexus 1000V switch provisions and enforces licenses for the ASA 1000V. Licenses are installed on the Virtual Supervisor Module (VSM) in the Cisco Nexus 1000V switch.

For more information, see the *Cisco Nexus 1000V License Configuration Guidelines* document at: http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_2/license/configuration/guide/n1000v_license.html

Release Notes for the Cisco Virtual Network Management Center, Version 2.0

For information about the Cisco VNMC 2.0 release that supports the ASA 1000V, see the *Release Notes for the Cisco Virtual Network Management Center, Version 2.0* at:

http://www.cisco.com/en/US/docs/unified_computing/vnmc/sw/2.0/release/notes/vnmc_rn.html

Release Notes for the Cisco Nexus 1000V, Version 4.2(1)SV1(5.2)

For information about the Cisco Nexus 1000V, Version 4.2(1)SV1(5.2) that supports the ASA 1000V, see the *Cisco Nexus 1000V Release Notes, Release 4.2(1)SV1(5.2)* at:

http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_1_5_2/release/notes/n1000v_rn.html

Related Documentation

For more information about the individual components that comprise the ASA 1000V, see the following documentation:

- Cisco Nexus 1000V
  http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html
- Cisco VNMC and Cisco VSG
  http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html
- VMware
  http://www.vmware.com/support/pubs/
- ASA 1000V
  http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html
- ASDM
  http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, 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

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.