Cisco Nexus 1000V Release Notes, Release 4.2(1)SV2(2.3)

First Published: August 4, 2014

Last Updated: September 23, 2014

This document describes the features, limitations, and caveats for the Cisco Nexus 1000V Release 4.2(1)SV2(2.3) software.

Contents

This document includes the following sections:

Introduction

The Cisco Nexus 1000V provides a distributed, Layer 2 virtual switch that extends across many virtualized hosts. The Cisco Nexus 1000V manages a data center defined by the vCenter Server. Each server in the data center is represented as a line card in the Cisco Nexus 1000V and can be managed as if it were a line card in a physical Cisco switch.

Cisco Systems, Inc.
www.cisco.com

The Cisco Nexus 1000V consists of the following two components:

- Virtual Supervisor Module (VSM), which contains the Cisco CLI, configuration, and high-level features.
- Virtual Ethernet Module (VEM), which acts as a line card and runs in each virtualized server to handle packet forwarding and other localized functions.

Software Compatibility with VMware

The servers that run the Cisco Nexus 1000V VSM and VEM must be in the VMware Hardware Compatibility list. This release of the Cisco Nexus 1000V supports vSphere 5.5, 5.1, and 5.0 release trains. For additional compatibility information, see the *Cisco Nexus 1000V Compatibility Information*.

Note All virtual machine network adapter types that VMware vSphere supports are supported with the Cisco Nexus 1000V. Refer to the VMware documentation when choosing a network adapter. For more information, see the VMware Knowledge Base article #1001805.

Software Compatibility with Cisco Nexus 1000V

This release supports hitless upgrades from Release 4.2(1)SV1(4) and later. For more information, see the *Cisco Nexus 1000V Software Upgrade Guide*.

New and Changed Information

This section describes the new software features in Cisco Nexus 1000V Release 4.2(1)SV2(2.3).

Integration with Cisco Application Virtual Switch (Cisco AVS)

Starting this release, Cisco Nexus 1000V supports the Cisco Application Virtual Switch (Cisco AVS). Cisco AVS is a distributed virtual switch solution that extends across many virtualized hosts and is fully integrated within the VMware virtual infrastructure, including VMware vCenter for the virtualization administrator. It manages a data center defined by the vCenter Server. Cisco AVS is compatible with any upstream physical access layer switch that complies with the Ethernet standard, including Cisco Nexus switches.

The Cisco AVS is compatible with any server hardware listed in the VMware Hardware Compatibility List (HCL). This solution allows the network administrator to configure virtual switch and port groups in order to establish a consistent data center network policy.

Cisco AVS is integrated with the Cisco Application Centric Infrastructure (ACI) and is managed by Cisco Application Policy Infrastructure Controller (APIC). For detailed information about Cisco AVS, see the Cisco AVS documentation available at:

http://www.cisco.com/c/en/us/support/switches/application-virtual-switch/tsd-products-support-series-home.html

Limitations and Restrictions

This section describes the limitations and restrictions of the Cisco Nexus 1000V.

Configuration Limits

Table 1 shows the Cisco Nexus 1000V configuration limits:

Table 1 Configuration Limits for Cisco Nexus 1000V

Component	Supported Limits for a Single Cisco Nexus 1000V Deployment Spanning up to 2 Physical Data Centers	
Maximum modules	130	
Virtual Ethernet Module (VEM)	128	
Virtual Supervisor Module (VSM)	The VSMs can be placed in different physical data centers. Note that the previous restrictions requiring the active-standby VSMs in a single physical data center do not apply anymore.	
Hosts	128	
Active VLANs and VXLANs across all VEMs	2048 VLANs and 2048 VXLANs (with a combined maximum of 4096)	
MAC addresses per VEM	32000	
MAC addresses per VLAN per VEM	4096	
vEthernet interfaces per port profile	1024 (without **static auto expand** port binding) Same as DVS maximum (with **static auto expand** port binding)	
PVLAN	512	
Distributed Virtual Switches (DVS) per vCenter with VMware vCloud Director (vCD)	32	
DVS per vCenter without vCD	32	
vCenter Server connections	1 per VSM HA Pair[1]	
Maximum latency between VSMs and VEMs	100ms	
	Per DVS	**Per Host**
vEthernet interfaces	4096	300[2]
Port profiles	2048	—
System port profiles	32	32
Port channel	512	8
Physical trunks	512	—
Physical NICs	—	32
vEthernet trunks	256	8
ACL	128	16[3]
ACEs per ACL	128	128
ACL instances	4096	300

Table 1 Configuration Limits for Cisco Nexus 1000V (continued)

Component	Supported Limits for a Single Cisco Nexus 1000V Deployment Spanning up to 2 Physical Data Centers (continued)	
NetFlow policies	32	8
NetFlow instances	256	32
Switched Port Analyzer (SPAN)/Encapsulated Remote Switched Port Analyzer (ERSPAN) sessions	64	64
QoS policy maps	128	16
QoS class maps	1024	128
QoS instances	4096	300
Port security	2048	216
Multicast groups	512	512

1. Only one connection to vCenter Server is permitted at a time.
2. When you upgrade from an earlier version of the Cisco Nexus 1000V software to the current version of Cisco Nexus 1000V software, the maximum vEth ports are displays as 216. To get the current supported vEth limit, remove the host from the DVS and add the host again.
3. This number can be exceeded if VEM has available memory.

Single VMware Data Center Support

The Cisco Nexus 1000V can be connected to a single VMware vCenter Server data center object. Note that this virtual data center can span across multiple physical data centers.

Each VMware vCenter can support multiple Cisco Nexus 1000V VSMs per vCenter data center.

VMotion of VSM

VMotion of the VSM has the following limitations and restrictions:

- VMotion of a VSM is supported for both the active and standby VSM VMs. For high availability, we recommend that the active VSM and standby VSM reside on separate hosts.
- If you enable Distributed Resource Scheduler (DRS), you must use the VMware anti-affinity rules to ensure that the two virtual machines are never on the same host, and that a host failure cannot result in the loss of both the active and standby VSM.
- VMware VMotion does not complete when using an open virtual appliance (OVA) VSM deployment if the CD image is still mounted. To complete the VMotion, either click **Edit Settings** on the VM to disconnect the mounted CD image, or power off the VM. No functional impact results from this limitation.
- If you are adding one host in a DRS cluster that is using a vSwitch to a VSM, you must move the remaining hosts in the DRS cluster to the VSM. Otherwise, the DRS logic does not work, the VMs that are deployed on the VEM could be moved to a host in the cluster that does not have a VEM, and the VMs lose network connectivity.

For more information about VMotion of VSM, see the *Cisco Nexus 1000V Software Installation Guide*.

Access Lists

ACLs have the following limitations and restrictions:

Limitations:

- IPV6 ACL rules are not supported.
- VLAN-based ACLs (VACLs) are not supported.
- ACLs are not supported on port channels.

Restrictions:

- IP ACL rules do not support the following:
  - fragments option
  - addressgroup option
  - portgroup option
  - interface ranges
- Control VLAN traffic between the VSM and VEM does not go through ACL processing.

NetFlow

The NetFlow configuration has the following support, limitations, and restrictions:

- Layer 2 match fields are not supported.
- NetFlow Sampler is not supported.
- NetFlow Exporter format V9 is supported
- NetFlow Exporter format V5 is not supported.
- The multicast traffic type is not supported. Cache entries are created for multicast packets, but the packet/byte count does not reflect replicated packets.
- NetFlow is not supported on port channels.

The NetFlow cache table has the following limitation:

- Immediate and permanent cache types are not supported.

Note The cache size that is configured using the CLI defines the number of entries, not the size in bytes. The configured entries are allocated for each processor in the ESX host and the total memory allocated depends on the number of processors.

Port Security

Port security has the following support, limitations, and restrictions:

- Port security is enabled globally by default.
  The **feature/no feature port-security** command is not supported.
- In response to a security violation, you can shut down the port.

- The port security violation actions that are supported on a secure port are **Shutdown** and **Protect**. The **Restrict** violation action is not supported.
- Port security is not supported on the PVLAN promiscuous ports.

Port Profiles

Port profiles have the following restrictions or limitations:

- There is a limit of 255 characters in a **port-profile** command attribute.
- We recommend that you save the configuration across reboots, which shortens the VSM bringup time.
- We recommend that if you are altering or removing a port channel, you should migrate the interfaces that inherit the port channel port profile to a port profile with the desired configuration, rather than editing the original port channel port profile directly.
- If you attempt to remove a port profile that is in use, that is, one that has already been auto-assigned to an interface, the Cisco Nexus 1000V generates an error message and does not allow the removal.
- When you remove a port profile that is mapped to a VMware port group, the associated port group and settings within the vCenter Server are also removed.
- Policy names are not checked against the policy database when ACL/NetFlow policies are applied through the port profile. It is possible to apply a nonexistent policy.

SSH Support

Only SSH version 2 (SSHv2) is supported.

For more information, see the *Cisco Nexus 1000V Security Configuration Guide*.

Cisco NX-OS Commands Might Differ from Cisco IOS

Be aware that the Cisco NX-OS CLI commands and modes might differ from those commands and modes used in the Cisco IOS software.

For information about CLI commands, see the *Cisco Nexus 1000V Command Reference*.

Layer 2 Switching—No Spanning Tree Protocol

The Cisco Nexus 1000V forwarding logic is designed to prevent network loops so it does not need to use the Spanning Tree Protocol. Packets that are received from the network on any link connecting the host to the network are not forwarded back to the network by the Cisco Nexus 1000V.

For more information about Layer 2 switching, see the *Cisco Nexus 1000V Layer 2 Switching Configuration Guide*.

Cisco Discovery Protocol

The Cisco Discovery Protocol (CDP) is enabled globally by default.

CDP runs on all Cisco-manufactured equipment over the data link layer and does the following:

- Advertises information to all attached Cisco devices.
- Discovers and views information about those Cisco devices.
  - CDP can discover up to 256 neighbors per port if the port is connected to a hub with 256 connections.

If you disable CDP globally, CDP is also disabled for all interfaces.

For more information about CDP, see the *Cisco Nexus 1000V System Management Configuration Guide*.

DHCP Not Supported for the Management IP

DHCP is not supported for the management IP. The management IP must be configured statically.

LACP

The Link Aggregation Control Protocol (LACP) is an IEEE standard protocol that aggregates Ethernet links into an EtherChannel.

The Cisco Nexus 1000V has the following restrictions for enabling LACP on ports carrying the control and packet VLANs:

Note These restrictions do not apply to other data ports using LACP.

- If LACP offload is disabled, at least two ports must be configured as part of the LACP channel.

Note This restriction is not applicable if LACP offload is enabled. You can check the LACP offload status by using the **show lacp offload status** command.

- The upstream switch ports must be configured in spanning-tree port type edge trunk mode. For more information about this restriction, see Upstream Switch Ports, page 7.

Upstream Switch Ports

All upstream switch ports must be configured in spanning-tree port type edge trunk mode.

Without spanning-tree PortFast on upstream switch ports, it takes approximately 30 seconds to recover these ports on the upstream switch. Because these ports are carrying control and packet VLANs, the VSM loses connectivity to the VEM.

The following commands are available to use on Cisco upstream switch ports in interface configuration mode:

- **spanning-tree portfast**
- **spanning-tree portfast trunk**

- **spanning-tree portfast edge trunk**

DNS Resolution

The Cisco Nexus 1010 (1000V) cannot resolve a domain name or hostname to an IP address.

Interfaces

When the maximum transmission unit (MTU) is configured on an operationally up interface, the interface goes down and comes back up.

Layer 3 VSG

When a VEM communicates with the Cisco Virtual Security Gateway (VSG) in Layer 3 mode, an additional header with 94 bytes is added to the original packet. You must set the MTU to a minimum of 1594 bytes to accommodate this extra header for any network interface through which the traffic passes between the Cisco Nexus 1000V and the Cisco VSG. These interfaces can include the uplink port profile, the proxy ARP router, or a virtual switch.

Copy Running-Config Startup-Config Command

When you are using the **copy running-config startup-config** command, do not press the PrtScn key. If you do, the command aborts.

Dynamic Entries Are Not Deleted for Linux VM

On a Linux VM that has multiple adapters, a DHCP release packet is sent from an incorrect interface (because of OS functionality) and the DHCP release packet is dropped. As a result, the binding entry is not deleted. This issue is a Linux issue where the packets from all interfaces go out of one interface (which is the default interface). To avoid this issue, put the interfaces in different subnets and make sure that the default gateways for each interface is set.

Source Filter TX VLANs Are Missing After the VSM Restarts

When a SPAN (ERSPAN-source) session is created and the source interface is configured as a port channel and PVLAN Promiscuous access is programmed, the filter RX is not configured and the configured programmed filter TX is not persistent on a VSM reload.

To work around this issue, configure all the primary and secondary VLANs as filter VLANs while using the port channel with PVLAN Promiscuous access as the source interface.

Default SSH Inactive Session Timeout

The default SSH inactive session timeout is 30 minutes, but the timeout setting is disabled by default, so the connection remains active. The **exec-timeout** command can be used to explicitly configure the inactive session timeout limit.

Queueing Policy Cannot Be Changed in a Flexible Upgrade Setup

Queuing is valid starting from Cisco NX-OS Release 4.2(1)SV1(5.1). Any queueing configuration that exists on the VSM in an earlier release stops working. All port profiles that have a queueing configuration cannot be used. If a port is down, it should be moved to a profile without QoS queueing.

Clear QoS Statistics Fails on the VSM

When a policy-map, of type queuing, that has a class map of type “match-any” without any match criteria, is applied on an interface, a resource pool is not created for that specific class ID. As a result, the collection of statistics fails and no data is sent back to the VSM. To work around this issue, add a match criteria on the empty class map.

Span Source/Destination Removed from the Session Configuration After an Atomic Port-Profile Change

If a virtual Ethernet port is a SPAN/ERSPAN source or destination and its port profile changes atomically, the virtual Ethernet port is removed from the SPAN/ERSPAN configuration. If it was the only operational source/destination, the session might go down.

Open Caveats

The following sections describe open caveats in Cisco Nexus 1000V Release 4.2(1)SV2(2.3). The IDs are linked to the Cisco Bug Search tool.

VDP

Table 2 VDP

ID	Open Caveat Headline
CSCul54170	The VDP sends inconsistent IP address mappings for a VM’s NIC in some conditions.
CSCuj89678	Cisco Nexus 1000V VEM accepts system VLAN as a VDP allocated Dynamic VLAN.

VXLAN Gateway

Table 3 VXLAN Gateway

ID	Open Caveat Headline
CSCuj50237	The VXLAN gateway module flaps when the VTEP IP address is changed in the VSM.
CSCuh24446	LACP packets were not received on the VXLAN gateway VSB for traffic higher than 260 Kbps.
CSCuh26605	The throughput decreases with a unique source MAC address for each incoming flow.
CSCuh52879	Syslog messages from the VXLAN gateway do not go to the external syslog server.
CSCug89113	Retain relevant debug components are in the VXLAN gateway.
CSCuh61074	The VXLAN gateway does not inherit a modified port profile on reattach.
CSCui40317	Incorrect values are in the InOctets/OutOctets columns of the **show interface counters module** command.
CSCui40646	The InOctets counter for the VXLAN gateway vEth (vxlannic0) interface is not working.
CSCui27814	The port channel is down after you enter the **shut** or **no shut** command on the uplink port profile of a VXLAN gateway.
CSCug95878	The **show process CPU** command does not show the same result for vssnet.
CSCug73194	The configuration fails on a port profile inherited by VTEPs on the VEM and VXLAN gateway.
CSCug93645	The **attach module gateway** command hangs if the VSM is on Layer 3 through a control interface.
CSCug67857	The **show cdp neighbors** command on the VSM or VXLAN gateway does not show details of the upstream VXGW module.
CSCuh17978	The **show process** command does not display the reason for the crash.
CSCuh24446	In high-traffic scenarios, there is a possibility that IGMP-Query packets may be queued behind data packets. This issue can cause IGMP-Join(s) not to be sent for the corresponding VXLAN segments and cause traffic to fail for unknown-unicast/multicast/broadcast.
CSCuh41892	The VSM and gateway are out-of-sync after you reload the VSM after changing the port profile.
CSCuh52879	System log messages not going to the external system log server from the gateway.
CSCuh40181	Unable to deploy VXLAN gateway VSB using the **enable properties** command on the Cisco N1010.
CSCud87990	The output for certain fields are missing for the **vemcmd show card** command in the VXLAN gateway.
CSCuh53503	When you deploy a VXLAN gateway, the MAC address entered does not get validated for proper syntax.
CSCum70552	The VLAN pool-based network fails if the VSM reloads without copy r s.
CSCum71012	VXGW-VTEP transport VLAN in VXLAN-VLAN mapping disrupts traffic.
CSCum68686	VXLAN: TCO/TSO support for inner IPv6 traffic.

Platform, Infrastructure, Ports, Port Channel, and Port Profiles

Table 4 Platform, Infrastructure, Ports, Port Channel, and Port Profiles

ID	Open Caveat Headline
CSCui71195	Installing an earlier REST-API plug-in version results in HTML errors.
CSCui93564	Port channels do not come up in a non-LACP offload setup.

Table 4 Platform, Infrastructure, Ports, Port Channel, and Port Profiles (continued)

ID	Open Caveat Headline
CSCti98977	Not able to migrate VC/VSM and normal VM when adding a host to DVS.
CSCtj70071	SNMP V3 traps are not getting generated.
CSCtq92519	CDP does not work for certain NIC cards without VLAN 1 allowed.
CSCtr34519	Continuous SNMP polling causes high CPU usage.
CSCtz04587	Reloading the VSM takes 12 minutes for modules to come online and vEthernet interfaces to come up.
CSCtx06864	A native VLAN configured on the interface port channel is not programmed on the VEM.
CSCub23161	VCD does not display relevant error descriptions for error codes.
CSCub25986	NSM should fix the Cisco Nexus 1000V feature limitation issue.
CSCub69289	vEths mapped to the port profiles are not counted in the **show resource-availability monitor** command.
CSCuc63801	Traffic loss occurs after the VSM reloads if PSEC is restricted and the DSM bit is set.
CSCug25018	You cannot process a large number of IGMP queries from the upstream switch on the Cisco Nexus 1000V.
CSCuf89892	The VEM does not increase the number of maximum ports after an upgrade to the current version of the Cisco Nexus 1000V.
CSCue17860	snmpwalk does not return values of SyslogServer objects.
CSCue77534	Internal VLANs (3968 to 4047) are being trunked to configure on ports.
CSCug23565	Downloading the files from the VSM configuration with IPv6 throws an error.
CSCug36502	When the VSM is set up with an IPv6 address and accessed, the server drops or resets the connection randomly and causes multiple issues.
CSCug66317	When trying to install a license file, installation fails with an error message “file already exists” and the license file is not installed.
CSCuc75590	When plan mappings are configured on the port-channel interface directly, the mappings are incorrect on the VEM.
CSCug51163	A VEM upgrade from previous releases of the Cisco Nexus 1000V software to the current release of Cisco Nexus 1000V software fails.
CSCue50621	ifHCInOctets and ifInOctets wrap while taking a snapshot of virtual machines.
CSCuh20779	When you deploy a gateway as VSB, you are asked to enter the VSMs domain ID. For the gateway, you do not need the domain ID.
CSCub56123	The wrong message is displayed for VC user ID and password.
CSCuj19963	When ESX is upgraded to vSphere 5.5, Mellanox NICs get a policy mismatch.
CSCuj26459	When ESX is upgraded to vSphere 5.5, the host management connectivity is lost.
CSCuj19983	CDN NIC gets a previous port policy after a reboot.
CSCtk53802	Improper sync occurs with vCenter when port-profile names have special characters.
CSCts80394	A VEM upgrade fails when the scratch space is a network file system.

Quality of Service

Table 5 Quality of Service

ID	Open Caveat Headline
CSCuc71793	Ports go to the error-disabled state during ACL or QoS commit errors.
CSCtu36119	QoS marking limitation occurs in the VCD environment.

Features

Table 6 Features

ID	Open Caveat Headline
CSCtk65252	PSEC with multiple MAC addresses and PVLAN are not supported.
CSCtr06833	Split brain causes pending ACL/QoS transactions into an err-disabled state.
CSCub44964	A RADIUS AAA error occurs when the feature CTS is enabled and there is a switchover.
CSCuc80063	IGMP process fails to read the PVLAN association.
CSCue36581	The copy run start takes 8 to 10 minutes to complete the copy.
CSCug85914	The **show bridge-domain vteps** command shows the IP address even after removing the vEth.
CSCug72814	When ACL deny is applied on mgmt0 to block http and https, ACL counters are not incremented but HTTP and HTTS is blocked as expected.
CSCug74311	VTEP IP address is stuck in the VTEP list after a headless VEM reconnects to the VSM.
CSCuh11701	The **no acllog match-log-level** *level* command does not reset the ACL logging level to the default value.
CSCug07730	The vethPerHostUsed field is displaying the same value as the vethUsed field in the XML response for http://vsm_ip/api/vc/limits API. It should display the number of vEths on the host with the maximum used vEths.
CSCuh11779	An incorrect default value is shown for max-deny flows and max-permit flows.

Resolved Caveats

Table 7 lists caveats that were resolved in Cisco Nexus 1000V Release 4.2(1)SV2(2.3). The IDs are linked to the Cisco Bug Search tool.

Table 7 Resolved Caveats

ID	Resolved Caveat Headline
CSCub33444	Powering up a single VM configures all vApp networks.
CSCum99528	IP address configuration on interface control0 does not persist upon VSM reload.
CSCup03759	After reloading the VSM without copying the running config to the startup config, stale dynamic port profiles are not deleted.
CSCup52603	VLAN-related flows are not refreshed on the VXLAN gateway after a VMotion of the VXLAN VM, which causes VXLAN egress packets to reference a stale flow.

Table 7 Resolved Caveats (continued)

ID	Resolved Caveat Headline
CSCun52238	Packets with unknown d.mac are not flooded to interested VXLAN ports/vEths in VEM after decap.
CSCug61691	Denying IGMP traffic via an access control list does not deny IGMPv2 or IGMPv3.

MIB Support

The Cisco Management Information Base (MIB) list includes Cisco proprietary MIBs and many other Internet Engineering Task Force (IETF) standard MIBs. These standard MIBs are defined in Requests for Comments (RFCs). To find specific MIB information, you must examine the Cisco proprietary MIB structure and related IETF-standard MIBs supported by the Cisco Nexus 1000V Series switch.

The MIB Support List is available at the following FTP site:

ftp://ftp.cisco.com/pub/mibs/supportlists/nexus1000v/Nexus1000VMIBSupportList.html

Related Documentation

This section lists the documents used with the Cisco Nexus 1000V and available on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

General Information

Cisco Nexus 1000V Documentation Roadmap

Cisco Nexus 1000V Release Notes

Cisco Nexus 1000V Compatibility Information

Install and Upgrade

Cisco Nexus 1000V Installation and Upgrade Guide

Configuration Guides

Cisco Nexus 1000V High Availability and Redundancy Configuration Guide

Cisco Nexus 1000V Interface Configuration Guide

Cisco Nexus 1000V Layer 2 Switching Configuration Guide

Cisco Nexus 1000V License Configuration Guide

Cisco Nexus 1000V Network Segmentation Manager Configuration Guide

Cisco Nexus 1000V Port Profile Configuration Guide

Cisco Nexus 1000V Quality of Service Configuration Guide

Cisco Nexus 1000V REST API Plug-in Configuration Guide

Cisco Nexus 1000V Security Configuration Guide

Cisco Nexus 1000V System Management Configuration Guide

Cisco Nexus 1000V vCenter Plugin Configuration Guide

Cisco Nexus 1000V VXLAN Configuration Guide

Cisco Nexus 1000V VDP Configuration Guide

Cisco Nexus 1000V DFA Configuration Guide

Cisco Nexus 1000V vCenter Plugin Configuration Guide

Programming Guide

Cisco Nexus 1000V XML API User Guide

Reference Guides

Cisco Nexus 1000V Command Reference

Cisco Nexus 1000V Resource Availability Reference

Troubleshooting, Password Recovery, System Messages Guides

Cisco Nexus 1000V Troubleshooting Guide

Cisco Nexus 1000V Password Recovery Guide

Cisco NX-OS System Messages Reference

Virtual Services Appliance Documentation

The Cisco Nexus Virtual Services Appliance (VSA) documentation is available at http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Virtual Security Gateway Documentation

The Cisco Virtual Security Gateway documentation is available at http://www.cisco.com/en/US/products/ps13095/tsd_products_support_series_home.html

Virtual Network Management Center

The Cisco Virtual Network Management Center documentation is available at http://www.cisco.com/en/US/products/ps11213/tsd_products_support_series_home.html

Virtual Wide Area Application Services (vWAAS)

The Virtual Wide Area Application Services documentation is available at http://www.cisco.com/en/US/products/ps6870/tsd_products_support_series_home.html

ASA 1000V Cloud Firewall

The ASA 1000V Cloud Firewall documentation is available at http://www.cisco.com/en/US/products/ps12233/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see What's New in Cisco Product Documentation at: http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html.

Subscribe to What's New in Cisco Product Documentation, which lists all new and revised Cisco technical documentation, as an RSS feed and deliver content directly to your desktop using a reader application.