Cisco Secure Network Server

Product Overview

Granting and denying network access has evolved beyond simple user name and password verifications. Today, additional attributes related to users and their devices are used as decision criteria in determining authorized network access. Additionally, network service provisioning can be based on data such as the type of device accessing the network, including whether it is a corporate or personal device.

The Cisco® Secure Network Server is a scalable solution that helps network administrators meet complex network access control demands by managing the many different operations that can place heavy loads on applications and servers, including:

- Authorization and authentication requests
- Queries to identity stores such as Active Directory and LDAP databases
- Device profiling and posture checking
- Enforcement actions to remove devices from the network
- Reporting

The Cisco® Secure Network Server is based on the Cisco UCS® C220 Rack Server and is configured specifically to support the Cisco Identity Services Engine (ISE), Network Admission Control (NAC), and Access Control System (ACS) security applications. The Secure Network Server supports these applications in two versions. The Cisco Secure Network Server 3415 is designed for small and medium-sized deployments. The Secure Network Server 3495 has several redundant components such as processors, hard disks, and power supplies, making it suitable for large deployments that require highly reliable system configurations.

When ordering a Secure Network Server, the customer has the flexibility to install the Cisco Identity Services Engine (ISE), Network Admission Control (NAC), or Access Control System (ACS) security applications.

Figure 1 shows the Cisco Secure Network Server.

Figure 1. Cisco Secure Network Server

Product Specifications

Table 1 lists specifications of the Cisco Secure Network Server.

Table 1. Product Specifications

Product Name	Secure Network Server 3415	Secure Network Server 3495
Supported Applications	Identity Services Engine Access Control System Network Admission Control	Identity Services Engine Network Admission Control
Processor	1 - Intel Xenon 2.4-GHz E5-2609	2 - Intel Xenon 2.4-GHz E5-2609
Memory	16 GB (4 x 4 GB)	32 GB (8 x 4 GB)
Hard Disk	1 - 2.5-in. 600-GB 6Gb SAS 10K RPM	2 - 2.5-in. 600-GB 6Gb SAS 10K RPM
Hardware RAID	No	Level 0 & 1 LSI 2008 SAS RAID Mezzanine Card
Network Interfaces	4 x 1 GB	4 x 1 GB
Power Supplies	1 x 650W	2 x 650W
Trusted Platform Module	Yes	Yes
SSL Acceleration Card	No	Yes

Security Applications

The Cisco Secure Network Server supports Cisco's powerful network access and control security applications:

Cisco Identity Services Engine

An integral component to Cisco's cybersecurity initiative, the Cisco Identity Services Engine (ISE) is a revolutionary product that extends the network access and admission control capabilities first offered in Cisco NAC and Cisco Secure ACS. Looking beyond user name and password, the Identity Services Engine delivers unprecedented abilities to acquire user and device identity and context information to forge flexible and powerful policies that govern authorized network access. ISE is an all-in-one enterprise policy control platform that can reliably provide secure access for wired, wireless and VPN networks. ISE can also help IT with secure BYOD on-boarding and allow IT to provide differentiated Guest Access. The Identity Services Engine provides enforcement actions that allow administrators to restrict devices from the network that are violating access and policies.

Table 2 lists ISE endpoint scalability metrics for the Secure Network Servers.

Table 2. Identity Services Engine Deployment Scalability

	Secure Network Server 3415	Secure Network Server 3495
Endpoints supported in an ISE deployment per server	5000	20,000

Cisco Network Admission Control

Cisco Network Admission Control (NAC) enables the network to enforce security policies on all devices seeking to access the network. Cisco NAC protects sensitive data and prevents unauthorized access by confirming a user's identity before network access is granted. Cisco NAC minimizes the risks associated with noncompliant devices. Regardless of system type, ownership, or access methods, noncompliant devices can be quarantined and brought into compliance. The optional Cisco NAC Guest Server supports the entire guest access lifecycle (provisioning, notification, management, and reporting).

Cisco Secure Access Control System

Cisco Secure ACS is the world's most trusted enterprise network access policy and identity system, used by more than 40,000 enterprises worldwide. With powerful performance and a design-for-versatility approach, Cisco Secure ACS provides a critical building block for almost any network identity and access policy strategy.

Cisco Secure ACS interacts with external identity databases and RADIUS servers, becoming a control point for managing network access policy.

Cisco Secure ACS provides better control, monitoring, and enforcement of access to corporate resources to meet ever-changing business and regulatory needs.

Ordering Information

Table 3 lists ordering information for the Cisco Secure Network Servers.

Table 3. Product Ordering Information

Server Part Numbers	Server Description	Comments
SNS-3415-K9	Secure Network Server for ISE, NAC, and ACS applications (small)	Customer must choose either ACS, ISE, or NAC
SNS-3495-K9	Secure Network Server for ISE, NAC and ACS applications (large)	Customer must choose either ACS, ISE or NAC

Table 4 lists the Secure Network Server component spares that can be used as Field Replaceable Units (FRUs).

Table 4. Spare Components for the Cisco Secure Network Server

Component Part Number	Component Description
A03-D600GA2=	600-GB 6Gb SAS 10K RPM SFF HDD/hot plug/drive sled mounted
UCSC-PSU-650W=	650W Power Supply
N20-BKVM=	KVM Cable
UCSC-RAIL1=	Rail Kit

Cisco UCS C220 M3 Server

The Cisco UCS C220 M3 Rack Server is designed for performance and density over a wide range of business workloads, from web serving to distributed databases.

The Cisco UCS C220 M3 Rack Server is a high-density general-purpose 2-socket server optimized to deliver high performance for a large range of workloads. Cisco UCS C-Series servers extend unified computing innovations to an industry-standard form factor to help reduce total cost of ownership (TCO) and increase business agility. Designed to operate both in standalone environments and as part of Cisco UCS, the Cisco UCS C-Series Rack Servers employ Cisco technology to help customers handle the most challenging workloads.

Trusted Platform Module (TPM)

The TPM is a chip (microcontroller) that can securely store artifacts used to authenticate the platform (server). These artifacts can include passwords, certificates, or encryption keys. The chip can also be used to store platform measurements that help ensure authentication and authorization, thereby keeping the platform trustworthy.

Connectors and LEDs

Table 5 lists Connectors and LEDs on the Cisco Secure Network Servers.

Table 5. Connectors and LEDs

Connector/LEDs	Description
Front-panel connector	One KVM console connector (supplies 2 USB, 1 VGA, and 1 serial connector)
Front-panel locator LED	Indicator to help direct administrators to specific servers in large data center environments
Additional rear connectors	Additional interfaces, including a VGA video port, 2 USB 2.0 ports, an RJ-45 serial port, 1 Gigabit Ethernet management port, and dual 1 Gigabit Ethernet ports

Form Factor

Physical dimensions (H x W x D) 1RU: 1.7 x 16.9 x 28.5 in. (4.32 x 43 x 72.4 cm)

Environmental

Table 6 lists environmental information for the Cisco Secure Network Servers.

Table 6. Regulatory Standards Compliance: Safety and EMC

Item	Specification
Temperature: Operating	32 to 104°F (0 to 40°C) (operating, sea level, no fan fail, no CPU throttling, turbo mode)
Temperature: Nonoperating	-40 to 158°F (-40 to 70°C)
Humidity: Operating	10 to 90% noncondensing
Humidity: Nonoperating	5 to 93% noncondensing
Altitude: Operating	0 to 10,000 ft (0 to 3000m); maximum ambient temperature decreases by 1°C per 300m
Altitude: Nonoperating	0 to 40,000 ft (12,000m)
Heat Dissipation	Approximately 2500 BTU/h

Regulatory Standards

Table 7 lists regulatory standards compliance information for the Cisco Secure Network Servers.

Table 7. Regulatory Standards Compliance: Safety and EMC

Specification	Description
Safety	• UL 60950-1 No. 21CFR1040 Second Edition • CAN/CSA-C22.2 No. 60950-1 Second Edition • IEC 60950-1 Second Edition • EN 60950-1 Second Edition • IEC 60950-1 Second Edition • AS/NZS 60950-1 • GB4943 2001
EMC: Emissions	• 47CFR Part 15 (CFR 47) Class A • AS/NZS CISPR22 Class A • CISPR2 2 Class A • EN55022 Class A • ICES003 Class A • VCCI Class A • EN61000-3-2 • EN61000-3-3 • KN22 Class A • CNS13438 Class A

Specification	Description
EMC: Immunity	• EN55024 • CISPR24 • EN300386 • KN24

For More Information

For more information, please visit the following resources:

- Cisco Identity Services Engine: http://www.cisco.com/go/ISE
- Cisco Access Control System: http://www.cisco.com/go/ACS
- Cisco Network Access Control: http://www.cisco.com/go/NAC
- Cisco UCS Servers: http://www.cisco.com/go/unifiedcomputing

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-726524-04 12/14