Cisco Configuration Assurance Solution 2.0.2: Cisco Configuration Assurance Solution: Service Provider 2.0.2

Cisco® Configuration Assurance Solution (CAS) and Cisco Configuration Assurance Solution – Service Provider (CAS-SP) increase network security and availability, help ensure efficient application delivery, and document compliance with important regulatory and IT governance requirements. Cisco CAS and Cisco CAS-SP automatically perform regular, systematic audits of the production network, generating network-aware assessments of device misconfigurations, configuration policy violations, performance inefficiencies, and security gaps. Cisco CAS and Cisco CAS-SP provide network configuration and security baseline and post-change audit and analysis functions that are critical to a successful network configuration and change-management strategy.

Product Overview

Organizations need intelligent network visibility and security to avoid costly disruptions in their network and application services. Cisco Configuration Assurance Solution (CAS) and Cisco Configuration Assurance Solution – Service Provider (CAS-SP) are vital tools for improving network availability as well as application and service continuity. Cisco CAS and Cisco CAS-SP examine the production IP network for a broad range of configuration problems, including security best practices, addressing and routing, protocol configurations, route maps and access control lists (ACLs), Simple Network Management Protocol (SNMP), system logging, IP quality of service (QoS), custom policies, and more. Cisco CAS and Cisco CAS-SP process and interpret device configurations during audits the same way that production network devices do during operation. They embed expert knowledge of network devices, protocols, and routing behavior, enabling networkwide analysis of connectivity and resiliency, unlike other tools that are limited to simple syntax checks on a single device at a time. Actionable information derived from analysis supports automated or guided changes in the network to meet business objectives. With Cisco CAS and Cisco CAS-SP, network reliability can increase while operating costs decrease. Cisco CAS and Cisco CAS-SP help users to:

- Reduce network outages: Detect configuration problems before they disrupt network operations. An extensive rules library provides configurable rules to analyze individual devices, groups of devices, topology, and routing information.
- Ensure network security: Verify that network security policies are implemented effectively. An automated Port Scan analysis of the network model provides a nonintrusive vulnerability assessment.
- Verify network survivability: Inspect complex backup configurations across the network, diagnosing latent problems. Cisco CAS and Cisco CAS-SP can simulate network failures to test network resiliency and predict impacts on applications, resources, and security.
- Demonstrate regulatory compliance: Document compliance with regulatory requirements such as the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Federal Information Security Management Act (FISMA), and others.

Cisco CAS and Cisco CAS-SP support critical processes from popular IT governance frameworks including ITIL/BS15000 and ISO 17799.

High-Fidelity Network Data Model

Cisco CAS and Cisco CAS-SP include the Cisco Virtual Network Data Server (VNDS) that automatically maintains a detailed, near-real-time data model of the production network, including topology, configuration, and traffic. It collects and merges detailed network data from a broad range of sources, reconciling conflicts on the basis of user-configurable priorities. Information can be obtained online from network devices such as Cisco routers including the Cisco CRS-1 Carrier Routing System, Cisco Catalyst® switches, Cisco security devices, and third-party devices. Data can also be imported from CiscoWorks LAN Management Solution (LMS), CiscoWorks Network Compliance Manager, Cisco CNS NetFlow Collection Engine, and numerous third-party sources. Cisco VNDS can integrate with various platforms, including CiscoWorks LMS Resource Manager Essentials, CiscoWorks Network Compliance Manager, and Cisco Info Center, to obtain real-time awareness of configuration changes, helping ensure network data integrity.

Auditing the Network Configuration

Cisco CAS and Cisco CAS-SP completely automate the end-to-end workflow for network configuration audits. The operation of the core Audit and Analysis engine can be scheduled to run multiple regular audits that vary in terms of network scope, frequency, and target analyses. The results of successive network audits can be trended over time.

Cisco CAS and Cisco CAS-SP support a broad range of technologies and protocols. Both solutions are provided with hundreds of checks that reflect industry and security best practices published by Cisco, U.S. government agencies, and others. Checks encompass, among other things:

- IP addressing and routing
- Protocol configurations, including Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Interior Gateway Routing Protocol (IGRP), Enhanced IGRP (EIGRP), and Border Gateway Protocol (BGP)
- Route maps and ACLs
- Hot Standby Router Protocol (HSRP)
- SNMP, system logging, and router administration
- Firewall configurations and security protocols including authentication, authorization, and accounting (AAA), Kerberos Protocol, Network Address Translation (NAT), RADIUS, and TACACS+
- VPNs, tunnels, and VLANs
- QoS

Cisco CAS-SP adds additional rules for service provider environments, including:

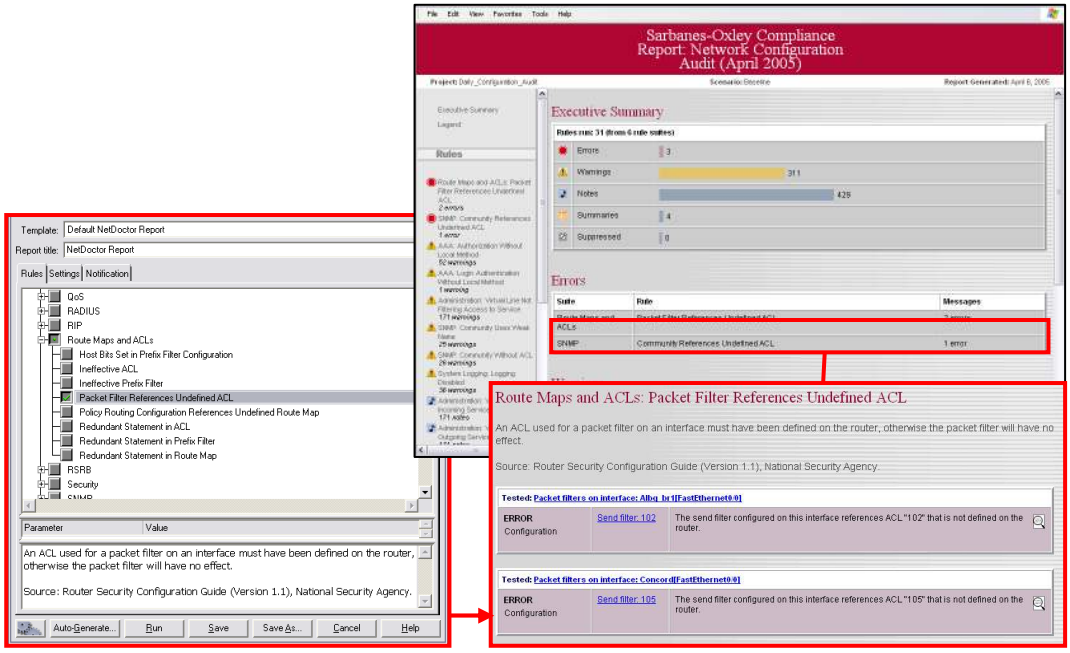
- MPLS Traffic Engineering
- IPv6
- Intermediate System-to-Intermediate System (IS-IS)

Rules are provided with source code, sample policy templates, and an integrated authoring environment to enable incorporation of your organization’s best practices.

Communicating Results

Cisco CAS and Cisco CAS-SP automatically publish results to an integrated Web-based Report Server, a central repository for reports encompassing documents, charts, tables, and images (Figure 1). These provide detailed results of the network audit, including informational reports summarizing network configuration characteristics such as deployed software releases and patch levels. Trending reports analyze the results of successive audits over time. Access can be restricted by username and password. Cisco CAS and Cisco CAS-SP can also be configured to notify users of critical errors through e-mail or pager.

Figure 1. Network Audit Reports Generated by the Cisco Report Server



Flow Analysis

The optional Cisco CAS – Flow Analysis Module (CAS-FAM) for Cisco CAS and Cisco CAS-SP provides support for simulation-based analyses as part of the configuration audit. These include survivability analysis, to verify that the network backup configuration will meet objectives in the event of a network failure. Cisco CAS-FAM also enables a nonintrusive test of network vulnerability through the Port Scan analysis.

Service Providers

Cisco CAS-SP is designed to address the demands of Service Provider network environments. Cisco CAS-SP provides all the functionality of Cisco CAS and supports Multiprotocol Label Switching (MPLS) analysis, in addition to IS-IS, IPv6, and Cisco IOS® Software XR-based device modeling and analysis. Cisco CAS-SP supports modeling and analysis of Cisco 12000 XR and Cisco CRS-1 devices.

Maximizing Network Security

Cisco CAS and Cisco CAS-SP support network security through configuration analysis and validation, with more than 150 rules for security-related issues. It includes rule suites for authentication, authorization, and accounting (AAA), kerberos, RADIUS, TACACS+, SNMP, system logging, device administration, and others. Out-of-the-box rules diagnose common ACL

errors, with additional customizable rules to enforce local policies. Configuration integrity can be checked under simulated failure conditions, to ensure that your back-up configuration meets operational objectives. An automated Port Scan analysis performs a non-intrusive vulnerability assessment. Unlike typical online vulnerability testing, a Port Scan analysis can be conducted under simulated failure conditions, to ensure that the backup network configuration is secure. Comprehensive audit reports provide detailed assessments of network change, localization of problems, and recommendations for resolution.

Cisco Proactive Automation of Change Execution

Cisco Proactive Automation of Change Execution (PACE) accelerates operational success by helping IT organizations securely automate and control network changes and configurations. This solution helps enterprises meet compliance requirements, accelerate growth, maintain business continuity, and increase user productivity without sacrificing network integrity and security.

Cisco CAS and Cisco CAS-SP play key roles in Cisco PACE, baselining the current and potential state of the network, assessing and testing for network security, and performing post-deployment, network-aware configuration audit and analysis. For more information on Cisco PACE visit http://www.cisco.com/go/pace.

System Requirements

Cisco CAS is available in multiple configurations to support networks of various sizes, starting at 50 nodes (which does not include Cisco VNDS) or 100 nodes (includes Cisco VNDS). Additional nodes can be added in varying increments up to 5100 nodes per single instance of Cisco CAS. Table 1 represents the system requirements for Cisco CAS, at up to 5100 nodes, and Cisco CAS-SP.

Cisco CAS and Cisco CAS-SP each comprises an Audit and Analysis engine; Cisco VNDS, which is generally implemented on a dual-processor platform with the prerequisite database environment; and a Web-based Report Server. The Audit and Analysis engine and Report Server can be implemented on the same (dual-processor) platform or on separate platforms as detailed in Table 1.

Table 1. System Requirements

	Audit and Analysis	Cisco VNDS	Report Server
Disk space	20 GB	160 GB (or larger depending on network size and data-retention practices)	60 GB (or larger depending on report-retention practices)
Hardware	3.0+ GHz Intel Pentium 4, M, D, or Xeon with 800 MHz front-side bus (FSB)	Dual 3.4+ GHz Intel Pentium D or Xeon with 1066 MHz FSB	1.5 GHz Intel Pentium 4 or Xeon
Memory	2 GB (minimum)	4 GB (minimum)	1 GB (minimum)
Software	Only English-language versions are supported: • Windows Server 2003 • Windows 2000 Server • Windows XP Professional • Windows 2000 Professional • Red Hat Enterprise Linux 3 (v2.4 Kernel) • Red Hat Enterprise Linux 4 (v2.6 Kernel)	Only English-language versions are supported: • Windows Server 2003 • Windows 2000 Server • Windows XP Professional • Windows 2000 Professional • Red Hat Enterprise Linux 3 (v2.4 Kernel) • Red Hat Enterprise Linux 4 (v2.6 Kernel)	Only English-language versions are supported: • Windows Server 2003 • Windows 2000 Server • Windows XP Professional • Windows 2000 Professional • Red Hat Enterprise Linux 3 (v2.4 Kernel) • Red Hat Enterprise Linux 4 (v2.6 Kernel)

Note: Cisco CAS is supported in Windows Server 2003 instances running in virtual machines hosted by VMware ESX Server versions 2.0 and 3.0

Ordering Information

Cisco Configuration Assurance Solution 2.0.2 and Cisco Configuration Assurance Solution – Service Provider 2.0.2 are available for purchase through regular Cisco sales and distribution channels worldwide. To place an order, contact your Cisco representative or visit http://www.cisco.com.

Cisco CAS and Cisco CAS-SP licensing options are described in the Cisco Assurance Solution 2.0/Cisco Assurance Solution – Service Provider 2.0 product bulletin, available at http://www.cisco.com/en/US/products/ps6364/prod_bulletins_list.html.

Service and Support

Cisco delivers a wide range of services programs through a unique combination of people, processes, tools, and partners, resulting in high levels of customer satisfaction. Cisco services help you to protect your network investment, optimize network operations, and prepare the network for new applications to extend network intelligence and the power of your business. For more information about Cisco services, contact your Cisco representative or visit http://www.cisco.com.

For More Information

For more information about Cisco Configuration Assurance Solution, contact your Cisco representative or visit http://www.cisco.com/go/cas.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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 C78-409400-00 06/07

