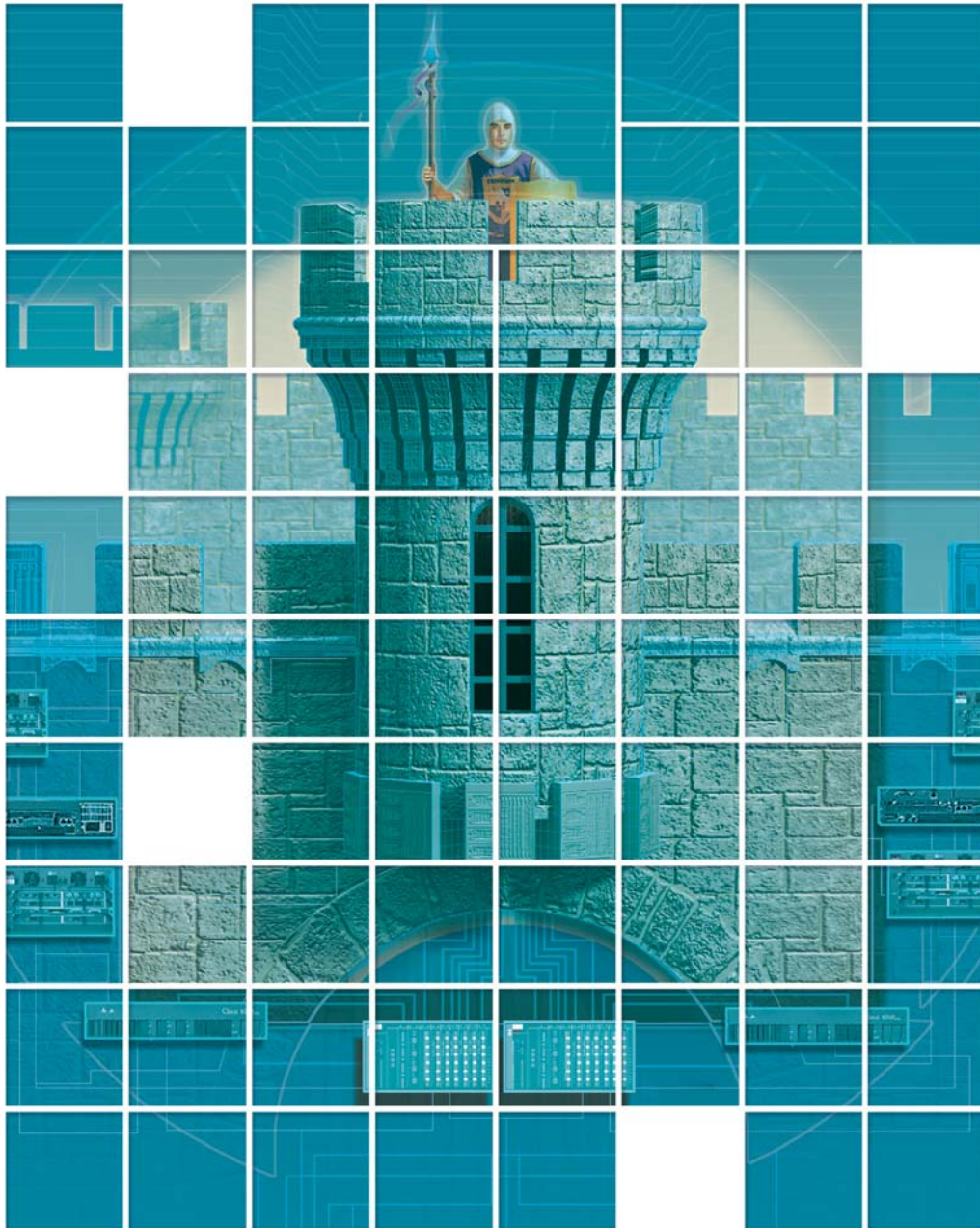




# SP Sentinel<sup>®</sup>

Network Audit, Security, and Policy-compliance for Service Providers





OPNET **SP Sentinel**<sup>®</sup>

Network Audit, Security, and Policy-compliance for Service Providers

Maintaining network integrity and security is imperative for ensuring quality service, meeting regulatory requirements, and managing operational risks. Service providers face numerous obstacles to achieving this, including technology migration, staffing and skills shortages, and pressure to accelerate new service deployment. Operational errors are frequently the consequence, as confirmed by industry studies that point to configuration issues as a major source of network downtime, degraded performance, and gaps in network security.

SP Sentinel is a software appliance for ensuring network integrity and security. SP Sentinel performs systematic configuration audits, analyzing an up-to-date model of the production network to diagnose device misconfigurations, policy violations, inefficiencies, and security gaps. Hundreds of standard checks incorporate industry best practices published by Cisco Systems, US government agencies, and others. Users are notified about critical issues, and comprehensive results are published to an integrated web-based Report Server.

**Reduce network outages:** SP Sentinel can detect configuration problems before they disrupt network operations. Extensive rule suites are applied including rules that analyze individual devices, groups of devices, topology, and routing information.

**Ensure network security:** Verify that network security policies have been implemented effectively. SP Sentinel simulates both authorized and unauthorized flows, revealing gaps in defenses, and pinpointing misconfigured nodes that block valid connectivity.

**Verify survivability:** Inspect complex back-up configurations across the network, diagnosing latent problems. SP Sentinel can simulate failures to test network resiliency and predict the impact on services, resources, and security.

**Demonstrate regulatory compliance:** Document compliance with regulatory requirements, such as Sarbanes-Oxley, Payment Card Industry Data Security Standard, HIPAA, the Federal Information Security Management Act (FISMA), and others.

**Enhance staff productivity:** Proactive identification of configuration errors can greatly reduce problems handled by the networking staff. Further, SP Sentinel eliminates the time-consuming task of manually checking device configurations.

**Low total cost of ownership:** SP Sentinel operates as an autonomous software appliance, minimizing staff time required to maintain network integrity and security.

# Automated Network Configuration Auditing

Detect issues that impact network availability, performance, and security.

**OPNET NetDoctor** Daily Network Integrity Audit (8/1/2007)

Project: Enterprise\_Network Scenario: Americas Report Generated: Thursday, August 2, 2007

**Executive Summary**

This report was created using OPNET NetDoctor, which provides network configuration analysis for routing, security, policy, and change management. This NetDoctor report shows the state of the network named "Enterprise\_Network".

The data used to generate this report came from 33 tested devices and 160 rules. The score for this report is 88.4 (out of 100). The tests resulted in 202 reported issues. A total of 23 rules reported at least one issue, and issues were found on 32 of the devices (representing 97% of the 33 devices in the network). The reported issues are comprised of 5 errors, 145 warnings, and 52 notes.

**Score: 88.4**

**202 Reported Issues**

- Errors: 5
- Notes: 52
- Warnings: 145

**33 Applicable Devices**

- With Errors: 5
- Passed: 1

Rules list includes: BGP: Redistribution References Undefined Route Map, OSPF: Mismatched Area ID, OSPF: Mismatched Hold Timers, IP Addressing: Overlapping Subnets, IP Multicast: Group List for Static RP References Undefined ACL, IP Routing: Inconsistent Metric Components, OSPF: ASBR Does Not Have Connection to Backbone Area, OSPF: Network Statement References Invalid Interface, OSPF (Advanced): Area Summary Includes Addresses Outside Area, OSPF (Advanced): Inconsistent.

Sentinel results are automatically published to an integrated web-based Report Server. The user can quickly drill down from top-level summary information to access underlying details regarding errors, affected devices, and the network configuration.

**OPNET Network Difference** Network Difference Report

Previous Network: Enterprise\_Network-August 1 Current Network: Enterprise\_Network-August 2 Report Generated: Thursday, August 2, 2007

**Executive Summary**

**Device Difference Summary**

- New: 1
- Modified: 17

**Device Boundary Summary**

Devices	Previous Network	Current Network
Cisco Systems Multi-layer Switch	3	3
Cisco Systems PIX Firewall	1	1
Cisco Systems Router	24	24
Cisco Systems Switch	3	3
Extreme Networks Multi-layer Switch	0	1
Foundry Networks Multi-layer Switch	0	1
Juniper Networks Router	2	2
Nokia Firewall	0	1
Nortel Networks Router	0	1
<b>Total</b>	<b>33</b>	<b>37</b>

**OPNET NetDoctor** SP Demo - Baseline with errors - Service Provider Integrity Check

Project: SP\_Demo Scenario: Baseline\_with\_errors

**Executive Summary**

(0) Allowed Rules

**Rules**

- BGP: Incorrect Neighbor Remote AS
- HSPF: Duplicate Virtual Address
- HSPF: Insufficient Number of Routers
- Organizational Policies: Cisco Router IOS Configuration Differs from Template File
- Route Maps and ACLs: Packet Filter References Undefined ACL
- MPLS: White: Asymmetric LSP L2VPN Transport Connection
- MPLS: White: Duplicate Route Distinguisher in BGP L2VPNs
- OSPF: Network Statement References Invalid Interface
- OSF: Interface References Undefined Profile
- BGP: BGP Neighbor not

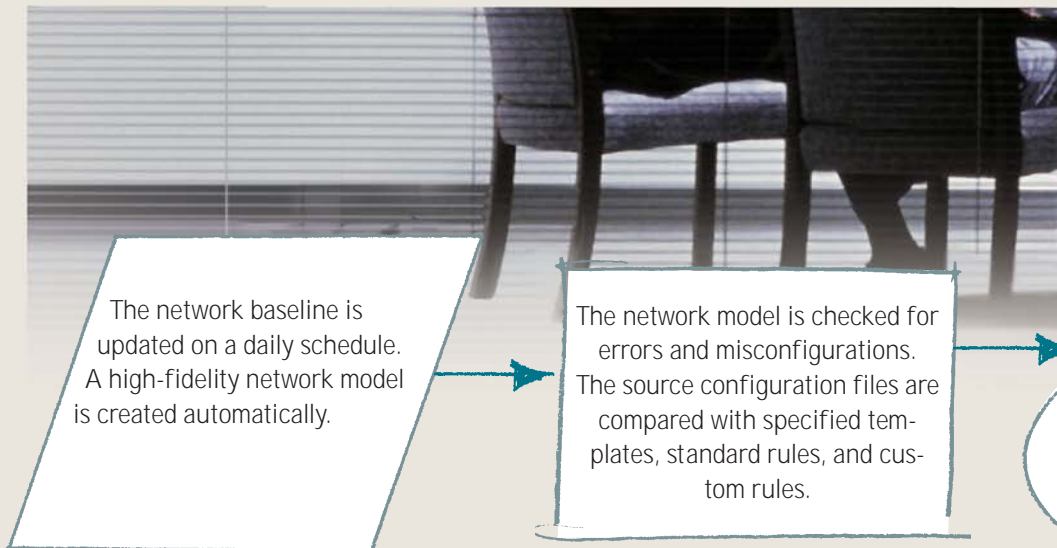
The screenshot displays a detailed network diagram of Europe with various nodes and connections, representing a service provider's network configuration.

The Network Difference Report pinpoints changes between successive network audits. SP Sentinel includes many standard reports. Additionally, User-Defined Reports can be customized in scope and format to meet unique requirements.

Sentinel analyzes an up-to-date model of the production network, leveraging OPNET's inherent understanding of topology and routing to detect issues that span groups of devices.

# SP Sentinel Workflow

SP Sentinel completely automates the workflow for daily or weekly configuration audits, proactively detecting issues that can compromise the network.



## Maintain network data to create virtual network model

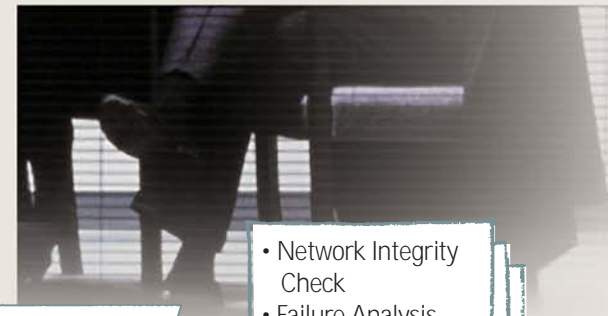
- Collect and merge data from network devices and third-party solutions
- Determine Layer 2/3 topology
- Obtain realtime awareness of configuration changes from network monitoring tools
- Select parts of the network for incremental analysis – Autonomous System, core and access, etc.
- Accurately overlay traffic onto the physical and logical topology

## Leverage extensive rule suites to diagnose configuration issues

- Detect protocol conflicts and misconfigurations
- Inspect device management and administration parameters
- Validate compliance with regulatory requirements
- Ensure that only authorized services are enabled

## Daily Configuration Checks

- Protocols: OSPF, IGRP, IS-IS, RIP, and BGP
- MPLS
- ATM
- HSRP and VRRP
- Firewalls, IPSec, AAA, Kerberos, NAT, RADIUS, TACACS+
- Route maps and ACLs
- SNMP configuration, system logging, router administration
- Duplicate IP addressing and overlapping IP subnets
- IPX, DLSw, and RSRB
- VPNs, VLANs, Tunnels



Failure is simulated to assess network resiliency. Security is checked with test traffic flows.

Critical errors? Page Network Engineering.

Publish results to Network Engineering intranet web site.

- Network Integrity Check
- Failure Analysis
- Sarbanes-Oxley, FISMA, PCI, and Other Compliance
- Security Audit
- Network Difference

### Audit network behavior

- Validate back-up configurations by modeling network failures
- Simulate unauthorized flows to pinpoint security gaps
- Identify nodes that block valid traffic
- Compare with previous network model, identifying differences

### Notify staff of critical network audit results

- Filter on error severity
- Automatically format for e-mail or pager
- Configure the volume and detail level of messages
- Notify staff when the audit is completed

### Automatically publish results to an integrated web server

- Access via a standard web browser
- Secure through username and password
- Automatically remove outdated material
- Include documents, charts, tables, and images
- Compare results with previous audits
- Create custom user-defined reports

## OPNET Customers *(partial list)*

Bulgaria Telecom  
Brasil Telecom S.A.  
BT  
Comcast Cable  
Cox Communications  
Deutsche Telekom  
eircom Ltd.  
France Telecom  
GenoTel GmbH  
Infonet  
Inmarsat  
Korea Telecom  
Nextel  
ntl  
NTT DoCoMo  
NTT Group  
O2  
Omnitel  
Polish Telecom  
Swisscom  
Telecom Italia  
Telekom Srbija  
Telefonica  
Telefonica Moviles  
Telenor  
Telstra  
TELUS  
THUS plc  
Verizon

## About OPNET Technologies

OPNET Technologies, Inc. is a leading provider of management software for networks and applications. OPNET's best-in-class solutions address: application performance troubleshooting, application deployment planning, systems capacity planning, network configuration auditing, network capacity and resiliency planning, and network technology R&D. OPNET solutions have been operationally proven in thousands of customer environments worldwide, including corporate enterprises, government and defense agencies, network service providers, and network equipment manufacturers. For more information about OPNET and its products, visit [www.opnet.com](http://www.opnet.com).

## Related OPNET Solutions:

### OPNET SP Guru® Network Planner

Embeds expert intelligence about how network devices and protocols operate, enabling service providers to automate complex tasks required for successful operations. SP Guru Network Planner enhances the productivity of operations and planning staff by providing a virtual environment for configuration change validation, planning, and engineering. With SP Guru Network Planner, service providers spend less to maintain competitive service levels.

### OPNET IT Sentinel®

Performs automated, systematic, network-wide configuration audits of an enterprise network, identifying errors and misconfigurations that can impact availability, performance, and security. IT Sentinel detects unexposed problems and proactively notifies networking staff of critical errors. Comprehensive results, with top-level summary and detailed audit information, are automatically published to an integrated web-based Report Server.



OPNET Technologies, Inc.  
7255 Woodmont Avenue  
Bethesda, Maryland 20814  
phone: (240) 497-3000  
email: [info@opnet.com](mailto:info@opnet.com)

NASDAQ: OPNT

[www.opnet.com](http://www.opnet.com)

## Awards

NetworkWorld  
200



NetworkWorld  
Best of the Tests



Network Computing  
Company to Watch



NetworkWorld  
Clear Choice Award



NetworkWorld+Interop and COMDEX  
Best of Show



SUPERCOMM  
Best E-Business Solution

