



Skybox[®] Network Assurance

Network Compliance, Access Analysis

Skybox Network Assurance provides organizations the ability to evaluate large networks for access compliance, availability, and security risks. It allows the IT team to reduce the time spent finding and troubleshooting network issues by 80% or more. The solution collects network and security device configurations, creating a network topology map and network model. With this model, users can automatically determine access and connectivity routes paths and validate them against network policies to generate compliance reports and IT trouble tickets.

Discover and Map the Network

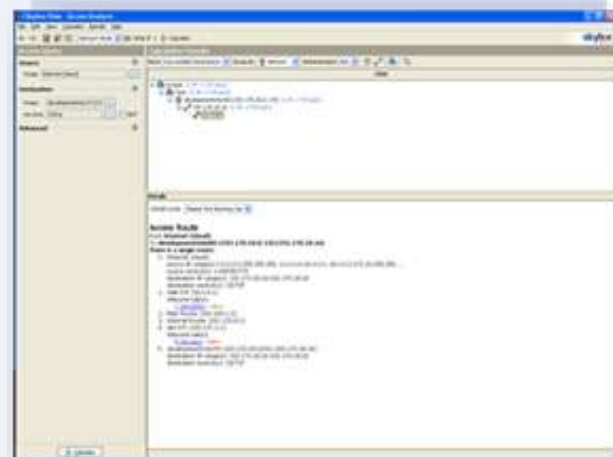
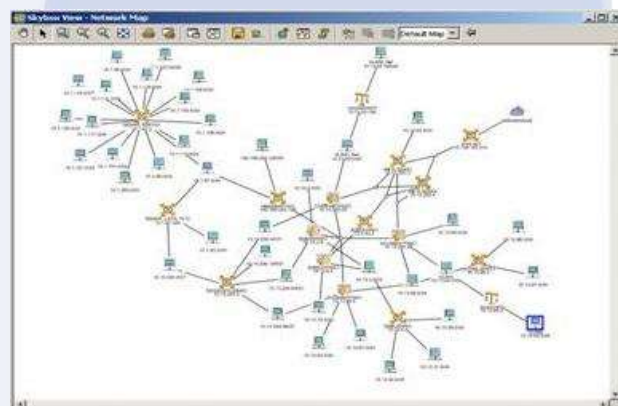
Network Assurance provides the visibility into the network structure and its access rights that most organizations lack. The solution collects and normalizes data from all devices in the network (scanners, routers, firewalls, etc.), and creates a central network device repository. This common database and map provide a comprehensive view of device behavior and interaction. Use this map to gain network visibility, troubleshoot network problems, and identify security holes.

Verify Access Compliance

Organizations can determine their access compliance status by validating configurations against out-of-the-box policies (based on PCI DSS and NIST guidelines) or by creating custom corporate policies. Analysis and reports on compliance metrics and violations can be generated on a daily or ad-hoc basis.

Troubleshoot Connectivity Issues

Network Assurance provides accurate information to troubleshoot access connectivity problems. Network Assurance analyzes root cause and path of network outages, finds blocking firewalls or missing routes, and identify security exposures. This allows the IT organization to quickly address availability and security issues.





Key Features

- Broad support for most network devices such as: Check Point, Cisco, ISS, Juniper, Nortel, Symantec
- Network and Firewall Configuration Management: AlterPoint, Check Point Provider-1, Cisco Works, HP NAS, Juniper NSM
- Holistic network access simulation
- Network access policy management
- Out-of-the-box best practice policy
- Customizable access policy (security and availability)
- Root cause analysis for access violations
- Compliance metrics and reporting

Supported Operating Systems

Windows 7, Windows Server 2008, Windows Server 2003 (32/64 bit)
Windows XP Professional SP2 or higher
Windows Vista
Red Hat Enterprise Linux v.4 (32/64 bit), v.5 (64 bit)
CentOS

Minimum Hardware Requirements*

Memory: 4GB RAM
CPU: 2.8 GHz
Storage: 20GB

Supported Devices—Network Devices

Check Point VPN-1, Firewall-1 and Provider-1
Fortinet Fortigate 2.x, 3.x, Fortinet VDOM
Nokia Appliances running Check Point FW-1/VPN-1
McAfee Secure Firewall (Sidewinder) G2, V.6
Cisco routers running Cisco IOS 11.x, 12.x
Cisco PIX, ASA, FWSM, Cisco Nexus
Juniper Netscreen, SSG, ISG running ScreenOS 4.x, 5.x, 6.x, and Network and Security Manager (NSM)
Symantec SGS

Supported Devices—Vulnerability Scanners

IBM Internet Scanner (V6 and V7)
IBM Proventia Network Enterprise Scanner
nCircle IP360, 6.x
McAfee Vulnerability Manager (formerly Foundstone Enterprise)
Nessus, V.2, V.3
NMAP Network Scanner, V.3, V.4
Qualys QualysGuard
eEye Retina V.4.x, V.5.x

Supported Devices—Threat Management Services

Symantec DeepSight
Verisign iDefense

Supported Devices—Management Systems

Cisco Works

* = Ask a Skybox Professional Service representative for additional information based on

skybox
security

Skybox Advantages

- Find root causes of outages and troubleshoot connectivity paths in seconds
- Evaluate network configuration and connectivity before changes
- Automatically analyze networks impact of security and availability requirements
- Visualize network topology and access routes

