

Skybox Network Assurance Screenshots

The screenshot displays the 'Network Map - Default Map' interface. The main area shows a complex network topology with various nodes and connections. Nodes are represented by icons and labeled with IP addresses and device names, such as 'app1', 'db', 'prod FW', 'Partner1 FW', 'Partner1 VPN', 'Partner2', 'main FW', 'gatewayEastA', 'Non Router', 'gatewaySouth', 'Backbone', 'Operations Router', 'gatewayWest', 'recFW', 'gatewayWest', 'recL2FW', 'recL2S', 'recL2W', 'recServers', 'gatewayKbr', 'Finance FW', 'gatewayKbr', 'Finance Router', 'financeServ...', 'financeWind...', and 'financeChic...'. The right-hand side features a control panel with the following sections:

- Map:** Name: Default Map (dropdown), More... (button)
- View:** Zoom to Fit, Zoom to Area (button), Relayout (button)
- Display Filter:** Search & Filter by Distance, Node: (input field)
- Node Selection Effect:** Focus (button), Expand (button), Select (button)
- Distance: (slider set to 1), Show All (button)
- Highlight:** Neighbor Distance (dropdown set to 2), Node Type (dropdown set to None), Network Type (dropdown set to None), Location (dropdown set to None), Zone (dropdown set to None), Clear (button)

Collect all network device configurations, normalize, and create a virtual model of entire network.

Skybox Network Assurance Screenshots

The screenshot displays the Skybox View - Access Analyzer interface. The left sidebar contains the 'Access Query' section with fields for Source (Internet [cloud]), Destination (Any), and Services (Any). The main area shows 'Analysis Results' for 'Accessible Destinations' grouped by 'Network'. A tree view shows the following structure:

- Europe [768 IPs; 1 TCP port]
- US [256 IPs; 6 TCP/UDP ports]
- New York [256 IPs; 6 TCP/UDP ports]
- dmz [192.170.33.0 / 24] [256 IPs; 6 TCP/UDP ports]
- 192.170.33.0-192.170.33.255 [256 IPs; 6 TCP/UDP ports]
- 21 (TCP)
- 25 (TCP)
- 53 (TCP)
- 80 (TCP)
- 443 (TCP)
- 53 (UDP)

The 'Details' section shows the 'Access Route' from Internet (cloud) to dmz (192.170.33.0/24) (192.170.33.0-192.170.33.255). It indicates there is a single route:

- Internet (cloud)
 - source IP range(s) 0.0.0.0-9.255.255.255, 11.0.0.0-16.0.0.0, 16.0.0.2-172.15.255.255, ...
 - source service(s): 1-65535/TCP
 - destination IP range(s): 192.170.33.0-192.170.33.255
 - destination service(s): 21/TCP
- main FW (16.0.0.1)
 - Inbound access rule(s): 2 (ACCESS) - Allow
- prod FW (192.170.1.98)
 - Inbound access rule(s): 2 (ACCESS) - Allow
- dmz (192.170.33.0/24) (192.170.33.0-192.170.33.255)
 - destination IP range(s): 192.170.33.0-192.170.33.255
 - destination service(s): 21/TCP

Check connectivity across the entire network. View all accessible destinations by port or network.

Skybox Network Assurance Screenshots

The screenshot displays the Skybox View - Network Assurance interface. The main window shows the 'NIST 800-41 Policy (79%)' details. A pie chart indicates 79% compliance (green) and 21% non-compliance (red). A table summarizes the test results by severity level.

	Info	Low	Medium	High	Critical	Overall
Compliant Tests	0	0	286	181	73	540
Noncompliant Tests	0	0	121	22	4	147
Overall	0	0	407	203	77	687

Below the chart, a list of related policies and their compliance levels is shown:

- [NIST Internal Access](#) - 68% Compliance
- [NIST Partner Access](#) - 84% Compliance
- [NIST External Access](#) - 92% Compliance
- [NIST DMZ Access](#) - 96% Compliance

The interface also includes a sidebar with 'Access Policies' and 'Zones', and a bottom status bar showing 'No running tasks', 'User Name: skyboxview', and 'Server: LocalHost:8443'.

Test access policy rules against the network and (if applicable) relevant zones. View resulting network compliance level and all violations.

Skybox Network Assurance Screenshots

The screenshot displays the Skybox View - Network Assurance interface. The left sidebar shows a tree of policies, with 'Limited SMTP Access' selected under 'NIST-External to DMZ (71%)'. The main pane shows the 'Limited SMTP Access' policy details, including a table of access tests. One test, ID 6357, is highlighted in red, indicating a violation. The violation explanation states: 'Too many IP addresses are accessible in the destination; dmz [192.170.33.0 / 24]. The limit in the Access Check specifies that no more than 5 destination IP addresses should be accessible for the service smtp [25/TCP]. The following port exceeded the limit by being accessible on too many IP addresses: 25 (TCP) - reached on 256 IP addresses'.

Test ID	Source	Destination	Services	Has Exceptions	New
6357	Internet [cloud]	dmz [192.170.33.0 / 24]	smtp [25/TCP]		

Access Test: 1 Access Tests cloud] -> dmz [192.170.33.0 / 24]

Violation Explanation | Access Results | Exceptions | Tickets

Too many IP addresses are accessible in the destination; dmz [192.170.33.0 / 24]. The limit in the Access Check specifies that no more than 5 destination IP addresses should be accessible for the service smtp [25/TCP]. The following port exceeded the limit by being accessible on too many IP addresses:
25 (TCP) - reached on 256 IP addresses

Violation policy guideline helps user quickly understand the firewalls and rules that caused an exposure and how to fix it quickly.

Skybox Network Assurance Screenshots

The screenshot displays the Skybox View - Network Assurance interface. The left sidebar shows a tree view of Access Policies, including Public Access Policies (79%), NIST 800-41 Policy (79%), NIST External Access (92%), NIST Partner Access (84%), NIST DMZ Access (96%), NIST Internal Access (68%), NIST-Internal to External (67%), NIST-Internal to Partner (67%), NIST-Internal to DMZ (15%), Block ICMP Replying Message, Block Login Services (17%), Block Miscellaneous (17%), Block RPC and NFS (17%), Block Small Services (17%), Block Trojan and Worm Ports, Block X-Windows (17%), Limited Access - non-specific, Limited Access - Services(10), NIST-Internal to Internal (80%), PCI DSS V1.2 Policy, Private Access Policies, Access Policy Violations, and Zones.

The main window is titled "Block Login Services" and shows a table of violations. The table has columns for Test ID, Source, Destination, Services, Has Exceptions, and New. The violations listed are:

Test ID	Source	Destination	Services	Has Exceptions	New
5931	app0 [192.170.35.0 / 24]	dmz [192.170.33.0 / 24]	exec [512/TCP], pwdgen [12...		
5932	app1 [192.170.36.0 / 24]	dmz [192.170.33.0 / 24]	exec [512/TCP], pwdgen [12...		
5933	db [192.170.34.0 / 24]	dmz [192.170.33.0 / 24]	exec [512/TCP], pwdgen [12...		
5934	developmentServers [192.17...	dmz [192.170.33.0 / 24]	exec [512/TCP], pwdgen [12...		
5935	financeServers [192.170.27....	dmz [192.170.33.0 / 24]	exec [512/TCP], pwdgen [12...		

Below the table, the "Access Test: app0 [192.170.35.0 / 24] -> dmz [192.170.33.0 / 24]" details are shown. The "Access Results" tab is active, displaying a tree view of the network path. The path is: dmz [192.170.33.0 / 24] -> 192.170.33.0-192.170.33.255 -> 22-23 (TCP) -> 129 (TCP) -> 512-514 (TCP) -> 129 (UDP). A "Mark as Exception" button is visible over the path.

The status bar at the bottom indicates "No running tasks", "User Name: skyboxview", and "Server: LocalHost:8443".

Create network exceptions when connectivity paths are approved, but policy lists them as violations.