

Network Security Assessment

Professional Services



Tools

Tools that may be used for the Security Vulnerability Assessment vary depending on devices being scanned. Depending on the environment and specific device types being assessed, these or others may be used during the assessment.

- Nessus
- NMAP
- WS Ping Pro Pack
- Angry IP Scanner
- GFI LAN Guard Security Scanner
- Sam Spade
- Cain and Abel
- Dumpsec
- Ethereal
- MBSA
- NBTscan
- Superscan
- TSgrind
- NetRecon
- Nikto
- LDAP Browser

- Out-of-Date IOS revision levels

Device	Platform	Current	Recommended
HS-ASA	ASA 5510	8.0(2)	8.2(1)
6509E-1	CAT 6509	CAT OS 8.5(9)	CAT OS 8.7(2a)
6509E-2	CAT 6509 MSFC	Advance Enterprise 12.2(18)SXF9	Advanced Enterprise 12.2(33)SX12
4506-West	CAT 4506	Enterprise Services 12.2(37)SG	Enterprise Services 12.2.53-SG
4506-East	CAT 4506	Enterprise Services 12.2(37)SG	Enterprise Services 12.2.53-SG
3024-3560	CAT 3560	IP Services 12.2(35)SE1	IP Services 12.2(50)SE3

- Improper or missing feature enablement affecting security & performance best practices

Findings	Recommendations \ Benefits	Priority
Lack of AAA access controls on Switches and Routers Affects Various	Sentinel recommends implementing AAA services on all Cisco switches and routers. TACACS should be used as the defacto authentication protocol. AAA services relieve the administration burden and complement an organization's password policy.	Medium

Excerpt from 6509E-1

AAA is configured but not applied to line interfaces.

```
aaa new-model
aaa authentication login default group tacacs+ local enable
line con 0
privilege level 15
```

Excerpt from 4506-West

AAA is partially configured but not applied to line interfaces.

```
aaa new-model
aaa authentication login default group tacacs+ local enable
```

Device Configuration Assessment

Sentinel reviews the configuration of key network equipment (routers, switches, firewalls, etc.) in order to identify any potential configuration issues. Sentinel's engineers will login and run commands to gather running configuration files on the production devices, highlighting lines and specific command statements containing configuration errors and/or security vulnerabilities and providing comments with specific command recommendations needed in order to correct configuration errors.

Information discovered that will be included in the final report can include:

- Misconfigured feature settings

Findings	Recommendations \ Benefits	Priority
VTP Domain is not secured Affects 6509E-1	Sentinel recommends securing the VTP domain by defining a name and password. An unsecured VTP domain allows the disclosure of all VLAN information. There is a risk of a serious DoS attack, in the case where VLAN database is maliciously manipulated.	High

Excerpt from 6509E-1

```
Version : running VTP2 (VTP3 capable)
Domain Name : SHS Password : not configured
Notifications: disabled Updater ID: 10.215.1.251
```

← Missing 'Mop password XXXX'

Pricing

Pricing for the security assessment services is based on number of devices being analyzed and can be further customized to meet individual customer needs.

Contact your Sentinel account representative to arrange a meeting and receive a pricing proposal.



Sentinel Technologies, Inc.
2550 Warrenville Road
Downers Grove, IL 60515
630-769-4300
www.sentinel.com