Week 47: Switch security tips

searchsecurity.techtarget.com/tip/Week-47-Switch-security-tips

Whent When vulnerabilities are identified that affect your system and whenever patches and upgrades are applied....

Review and update your guidance policies at least annually.

Why
When your organization's networks are connected to the Internet without adequate security measures, you are vulnerable to attacks. If you've been reading the columns of firewalls and routers, this information should look pretty familiar. And, as before, these principles can be applied to all switches, regardless of the switch flavor you have.

Strategy
The NSA's System and Network Attack Center (SNAC) Cisco IOS Switch Security Configuration Guide discusses security and switch placement using three layers: access, distribution and core.

Its general security checklist recommends you:

- Cover switches in your network security policy, including operating system, passwords, management port, network services, port security, system availability, VLANs, Spanning Tree Protocol, access control lists, logging and debugging, and authentication, authorization and accounting.
- Control physical access to the switch.
- Install the latest stable version of the IOS on each switch.
- Create an "enable secret" password.
- Manage switches out-of-band. If that's not feasible, then dedicate a separate VLAN number for in-band management.
- Set timeouts for sessions and configure privilege levels.
- Configure a banner to state that unauthorized access is prohibited.
- Enable and securely configure necessary network services; disable unnecessary network services.
- Set a strong password for SSH and use it instead of telnet.
- Set a strong community string for SNMP, if it's in use.
- Implement port security to limit access based on MAC address. Disable auto-trunking on ports.
- Utilize the switch's port mirroring capability for IDS access.
- Disable unused switch ports and assign them a VLAN number not in use.
- Assign trunk ports a native VLAN number that is not used by any other port.
- Limit the VLANs that can be transported over a trunk.
- Utilize static VLAN configuration.
- Disable VTP, if possible. Otherwise, set the following for VTP: management domain, password and pruning. Then set VTP into transparent mode.
- Use access control lists where appropriate.

- Enable logging and send logs to a dedicated, secure log host.
- Configure logging to include accurate time information, using NTP and timestamps.
- Review logs for possible incidents and archive them in accordance with the security policy.
- Use AAA features for local and remote access to switch.
- Maintain the switch configuration file offline and limit access. It should contain descriptive comments for the different settings to provide perspective.

More information
The Cisco IOS Switch Security Configuration Guide is available at http://www.nsa.gov/snac/downloads_switches.cfm?MenuID=scg10.3.1 , but not to be confused with last week's similar-looking reference to the Router Security Technical Implementation Guides (STIG) at http://www.nsa.gov/snac/downloads_cisco.cfm?MenuID=scg10.3.1 . Included are sample configuration files for two Cisco switch models that combine most of the countermeasures covered in the STIG.

About the author
Shelley Bard, CISSP, CISM, is a senior security network engineer with Verizon Federal Network Systems (FNS). An information security professional for 17 years, Bard has briefed and written infosecurity assessments and technical reports for the White House and Department of Defense, special interest groups, industry and academia. Please e-mail any comments.

Opinions expressed in this column are those of Shelley Bard and don't necessarily reflect those of Verizon FNS.