MODULE 3D: AUDITING NETWORKING DEVICES

OBJECTIVES

- Understand critical network controls
- Review specific controls for network gear, including routers, switches, firewalls, and wireless components

THE CHALLENGE OF NETWORKS

- Networking devices are not anything magical.
  - Routers and switches are just computers, with very specialized hardware and software.
- The TCP/IP stack was not built with secure by design principles.
- Networks are often very complex, and there are typically uniquely configured by the organization.

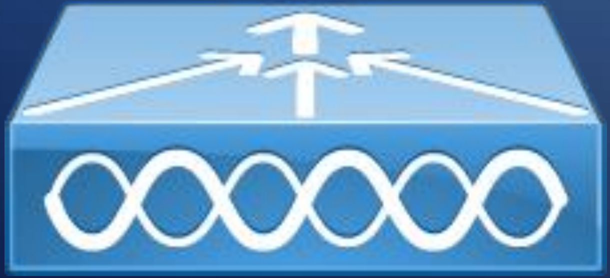
NETWORK AUDITING

Layer 3 Routers

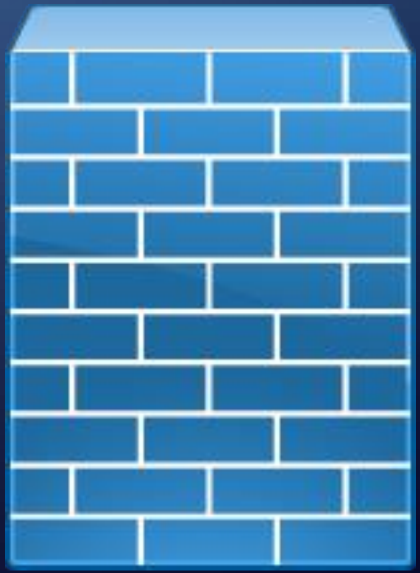
Layer 2 or 3 Switches

WiFi Access Point

Wireless LAN Controllers



Firewalls



GENERAL NETWORK EQUIPMENT AUDIT STEPS

- Begin the audit by asking the network engineers for a copy of the configuration file and the version of the device you intend to audit. For routers and switches, nearly all of the information you want is located in the configuration file, and having this prevents you from having to log onto the device repeatedly.
- Discuss change management practices with network administrators. Ensure that changes are planned, scheduled, documented (including the purpose of the change), and approved prior to implementation.

GENERAL NETWORK EQUIPMENT AUDIT STEPS

- Ensure that appropriate controls are in place for any vulnerabilities associated with the current software version. These controls might include software updates, configuration changes, or other compensating controls.
- Verify that all unnecessary services are disabled.
- If SNMP is being used – make sure it's SNMPv3!

GENERAL NETWORK EQUIPMENT AUDIT STEPS

- Review and evaluate procedures for creating user accounts and ensuring that accounts are created only when there is a legitimate business need. Also review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.
- Ensure that a standard naming convention is used for all devices.
- Verify that standard, documented processes exist for configuring network devices.
- Evaluate the use of network access control (NAC) technology to ensure the network is accessed in accordance with company policy.
- Review disaster recovery plans related to network devices.

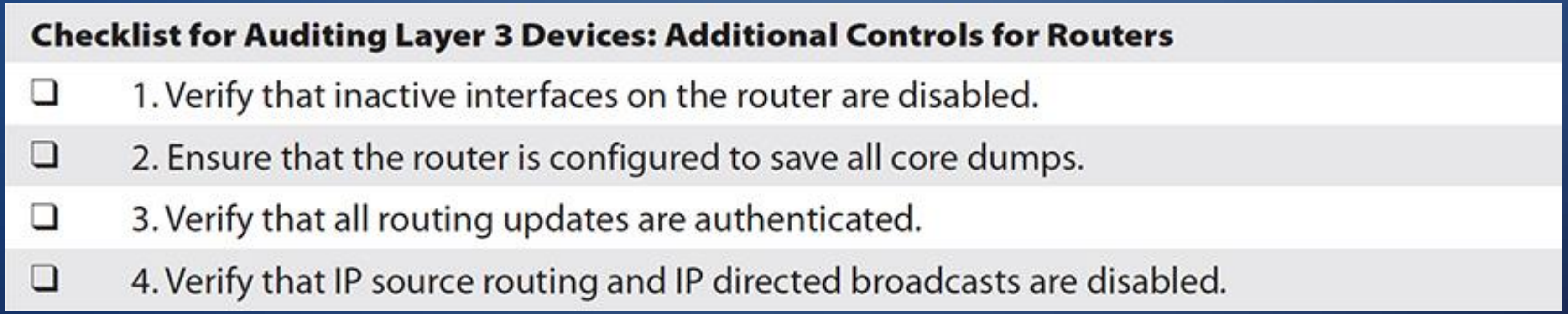
AUDITING SWITCHES

- Verify that administrators avoid using VLAN 1. Also called the native VLAN
- Evaluate the use of trunk autonegotiation.
- Verify that Spanning Tree Protocol attack mitigation is enabled (BPDU Guard, STP Root Guard).
  - Examine switch config files –
    - spanning-tree portfast
    - spanning-tree bpduguard enable
- Disable all unused ports and put them in an unused VLAN.

AUDITING SWITCHES

- **Evaluate use of the VLAN Trunking Protocol (VTP) in the environment.**
- Discuss use of the VTP with the network administrator to ensure that passwords are used if the VTP is necessary. VTP should be turned off if it’s not used. The VTP mode of a switch can be server, client, or transparent. Use transparent mode unless client or server is required.
- If VTP is necessary, domains should be set up for different areas of the network, and passwords should be enabled. Look for these lines in the configuration file:
  - vtp domain domain_name
  - vtp password password

AUDITING ROUTERS



Checklist for Auditing Layer 3 Devices: Additional Controls for Routers

□ 1. Verify that inactive interfaces on the router are disabled.

□ 2. Ensure that the router is configured to save all core dumps.

□ 3. Verify that all routing updates are authenticated.

□ 4. Verify that IP source routing and IP directed broadcasts are disabled.

AUDITING ROUTERS

- Discuss how the router handles core dumps with the network administrator. The core dumps should be located in a protected area that is accessible only to the network administrator, because disclosure of important information could occur.

  -
    ```
    ip ftp username username
    ip ftp password password
    exception protocol ftp
    exception region-size 65536
    exception dump ip address
    ```

AUDITING ROUTERS

- Verify that all routing updates are authenticated.
- Look in the config file:

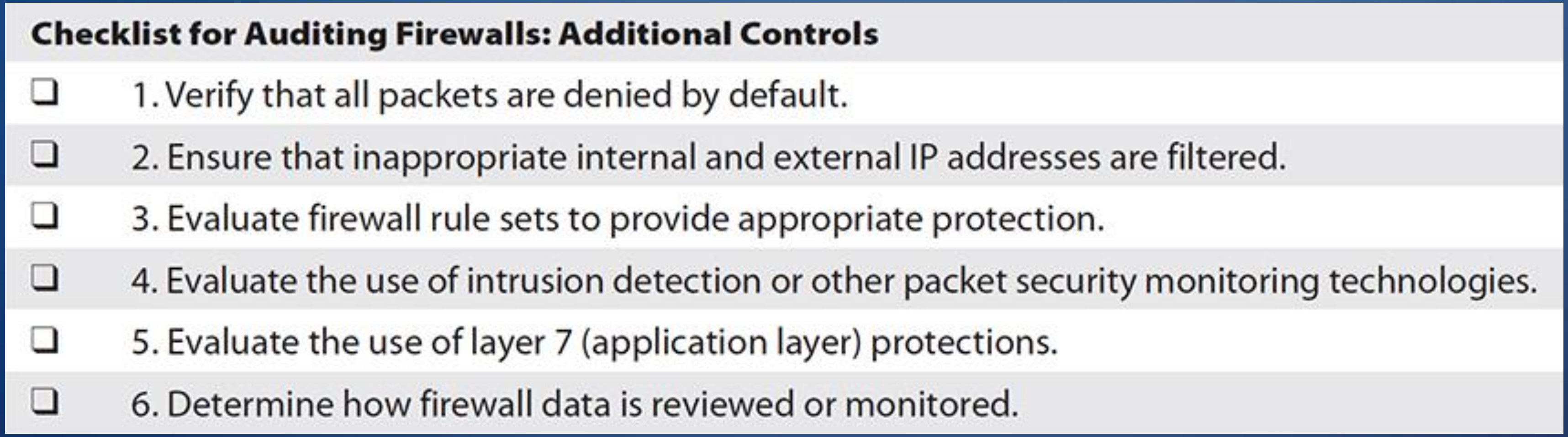
  -
    ```
    router ospf 1
    area 0 authentication message-digest
    interface ethernet 0
    ip ospf message-digest-key 1 md5 authentication_key
    ```
- Or for BGP:

  -
    ```
    router bgp 1
    neighbor ip_address password password
    ```

AUDITING ROUTERS

- Verify that IP source routing and IP directed broadcasts are disabled.
- Look for:
  - `no ip source-route`
  - `No ip directed-broadcast`

AUDITING FIREWALLS



Checklist for Auditing Firewalls: Additional Controls

☐ 1. Verify that all packets are denied by default.

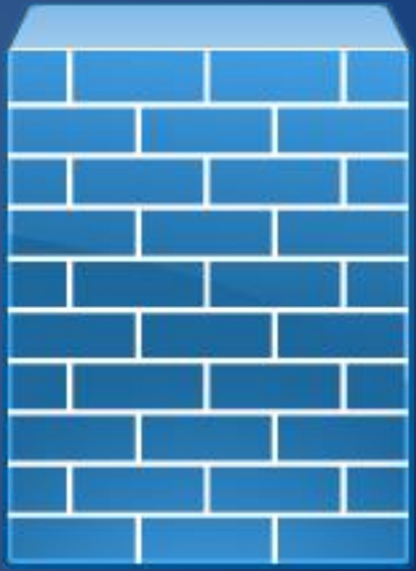
☐ 2. Ensure that inappropriate internal and external IP addresses are filtered.

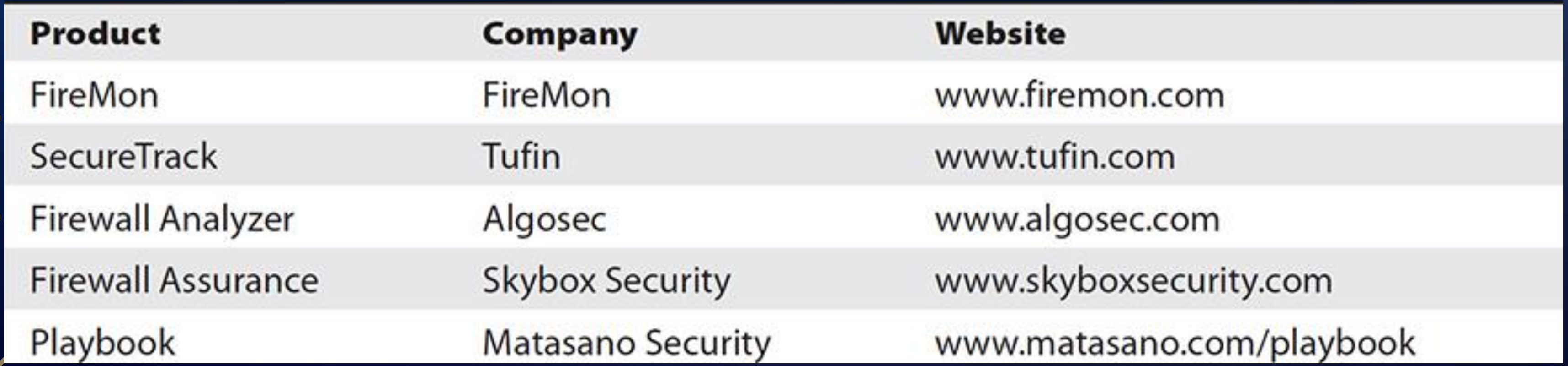
☐ 3. Evaluate firewall rule sets to provide appropriate protection.

☐ 4. Evaluate the use of intrusion detection or other packet security monitoring technologies.

☐ 5. Evaluate the use of layer 7 (application layer) protections.

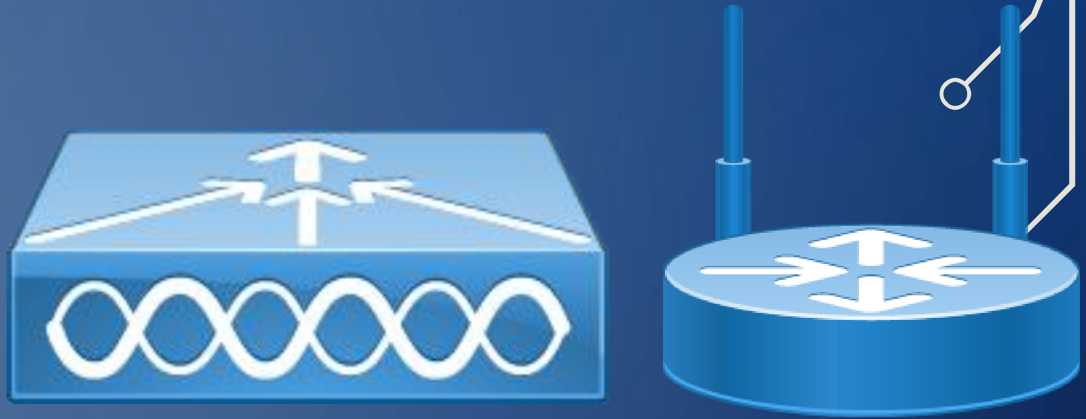
☐ 6. Determine how firewall data is reviewed or monitored.

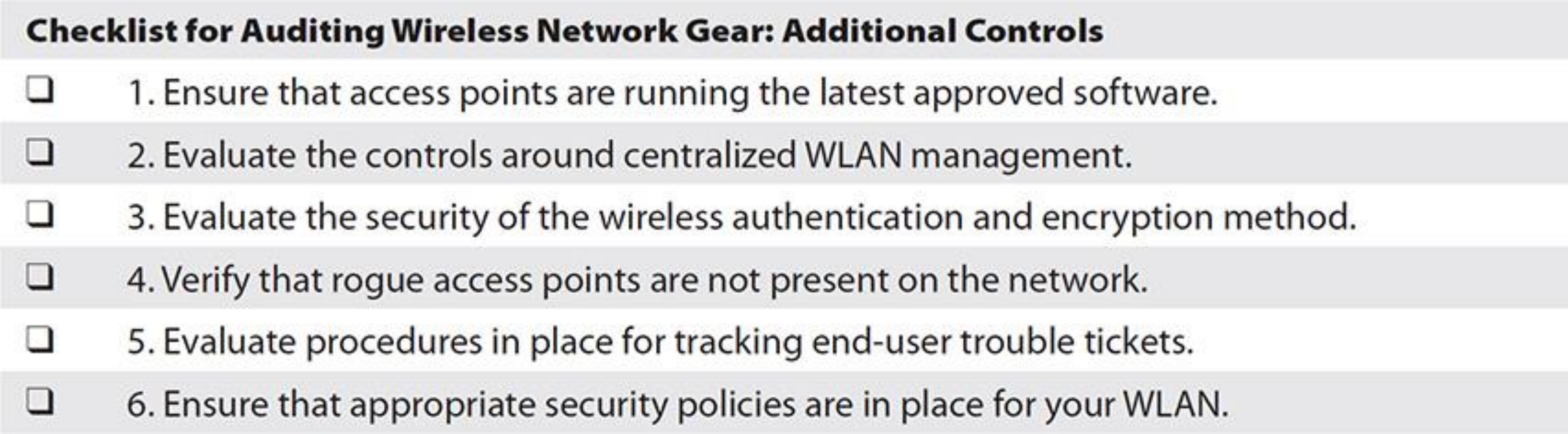




Product	**Company**	**Website**
FireMon	FireMon	www.firemon.com
SecureTrack	Tufin	www.tufin.com
Firewall Analyzer	Algosec	www.algosec.com
Firewall Assurance	Skybox Security	www.skyboxsecurity.com
Playbook	Matasano Security	www.matasano.com/playbook

AUDITING WIRELESS GEAR





Checklist for Auditing Wireless Network Gear: Additional Controls

□ 1. Ensure that access points are running the latest approved software.

□ 2. Evaluate the controls around centralized WLAN management.

□ 3. Evaluate the security of the wireless authentication and encryption method.

□ 4. Verify that rogue access points are not present on the network.

□ 5. Evaluate procedures in place for tracking end-user trouble tickets.

□ 6. Ensure that appropriate security policies are in place for your WLAN.