Securing Network Infrastructure Devices

Network infrastructure devices are the components of a network that transport communications needed for data, applications, services, and multi-media. These devices include routers, firewalls, switches, servers, load-balancers, intrusion detection systems, domain name systems, and storage area networks.

These devices are ideal targets for malicious cyber actors because most or all organizational and customer traffic must pass through them.

- An attacker with presence on an organization's gateway router can monitor, modify, and deny traffic to and from the organization.
- An attacker with presence on an organization's internal routing and switching infrastructure can monitor, modify, and deny traffic to and from key hosts inside the network and leverage trust relationships to conduct lateral movement to other hosts.

Organizations and individuals that use legacy, unencrypted protocols to manage hosts and services make successful credential harvesting easy for malicious cyber actors. Whoever controls the routing infrastructure of a network essentially controls the data flowing through the network.

What security threats are associated with network infrastructure devices?

Network infrastructure devices are often easy targets for attackers. Once installed, many network devices are not maintained at the same security level as general-purpose desktops and servers. The following factors can also contribute to the vulnerability of network devices:

- Few network devices—especially small office/home office and residential-class routers—run antivirus, integrity-maintenance, and other security tools that help protect general-purpose hosts.
- Manufacturers build and distribute these network devices with exploitable services, which are enabled for ease of installation, operation, and maintenance.
- Owners and operators of network devices often do not change vendor default settings, harden them for operations, or perform regular patching.
- Internet service providers may not replace equipment on a customer's property once the equipment is no longer supported by the manufacturer or vendor.
- Owners and operators often overlook network devices when they investigate, look for intruders, and restore general-purpose hosts after cyber intrusions.

How can you improve the security of network infrastructure devices?

The Cybersecurity and Infrastructure Security Agency (CISA) encourages users and network administrators to implement the following recommendations to better secure their network infrastructure:

- Segment and segregate networks and functions.
- Limit unnecessary lateral communications.
- Harden network devices.
- Secure access to infrastructure devices.
- Perform out-of-band (OoB) network management.

- Validate integrity of hardware and software.

Segment and Segregate Networks and Functions

Security architects must consider the overall infrastructure layout, including segmentation and segregation. Proper network segmentation is an effective security mechanism to prevent an intruder from propagating exploits or laterally moving around an internal network. On a poorly segmented network, intruders are able to extend their impact to control critical devices or gain access to sensitive data and intellectual property. Segregation separates network segments based on role and functionality. A securely segregated network can contain malicious occurrences, reducing the impact from intruders in the event that they have gained a foothold somewhere inside the network.

Physical Separation of Sensitive Information

Traditional network devices, such as routers, can separate Local Area Network (LAN) segments. Organizations can place routers between networks to create boundaries, increase the number of broadcast domains, and effectively filter users' broadcast traffic. Organizations can use these boundaries to contain security breaches by restricting traffic to separate segments and can even shut down segments of the network during an intrusion, restricting adversary access.

Recommendations

- Implement principles of least privilege and need-to-know when designing network segments.
- Separate sensitive information and security requirements into network segments.
- Apply security recommendations and secure configurations to all network segments and network layers.

Virtual Separation of Sensitive Information

As technologies change, new strategies are developed to improve information technology efficiencies and network security controls. Virtual separation is the logical isolation of networks on the same physical network. Virtual segmentation uses the same design principles as physical segmentation but requires no additional hardware. Existing technologies can be used to prevent an intruder from breaching other internal network segments.

Recommendations

- Use private Virtual Local Area Networks (VLANs) to isolate a user from the rest of the broadcast domains.
- Use virtual routing and forwarding (VRF) technology to segment network traffic over multiple routing tables simultaneously on a single router.
- Use Virtual Private Networks (VPNs) to securely extend a host/network by tunneling through public or private networks.

Limit Unnecessary Lateral Communications

Allowing unfiltered peer-to-peer communications, including workstation-to-workstation, creates serious vulnerabilities and can allow a network intruder's access to spread easily to multiple systems. Once an intruder establishes an effective beachhead within the network, unfiltered lateral communications allow the intruder to create backdoors throughout the network. Backdoors help the

intruder maintain persistence within the network and hinder defenders' efforts to contain and eradicate the intruder.

Recommendations

- Restrict communications using host-based firewall rules to deny the flow of packets from other hosts in the network. The firewall rules can be created to filter on a host device, user, program, or internet protocol (IP) address to limit access from services and systems.
- Implement a VLAN access control list (VACL), a filter that controls access to and from VLANs. VACL filters should be created to deny packets the ability to flow to other VLANs.
- Logically segregate the network using physical or virtual separation, allowing network administrators to isolate critical devices onto network segments.

Harden Network Devices

A fundamental way to enhance network infrastructure security is to safeguard networking devices with secure configurations. Government agencies, organizations, and vendors supply a wide range of guidance to administrators—including benchmarks and best practices—on how to harden network devices. Administrators should implement the following recommendations in conjunction with laws, regulations, site security policies, standards, and industry best practices.

Recommendations

- Disable unencrypted remote admin protocols used to manage network infrastructure (e.g., Telnet, File Transfer Protocol [FTP]).
- Disable unnecessary services (e.g., discovery protocols, source routing, Hypertext Transfer Protocol [HTTP], Simple Network Management Protocol [SNMP], Bootstrap Protocol).
- Use SNMPv3 (or subsequent version), but do not use SNMP community strings.
- Secure access to the console, auxiliary, and virtual terminal lines.
- Implement robust password policies, and use the strongest password encryption available.
- Protect routers and switches by controlling access lists for remote administration.
- Restrict physical access to routers and switches.
- Back up configurations and store them offline. Use the latest version of the network device operating system and keep it updated with all patches.
- Periodically test security configurations against security requirements.
- Protect configuration files with encryption or access controls when sending, storing, and backing up files.

Secure Access to Infrastructure Devices

Administrative privileges can be granted to allow users access to resources that are not widely available. Limiting administrative privileges for infrastructure devices is crucial to security because intruders can exploit administrative privileges that are improperly authorized, granted widely, or not closely audited. Adversaries can use compromised privileges to traverse a network, expand access, and take full control of the infrastructure backbone. Organizations can mitigate unauthorized infrastructure access by implementing secure access policies and procedures.

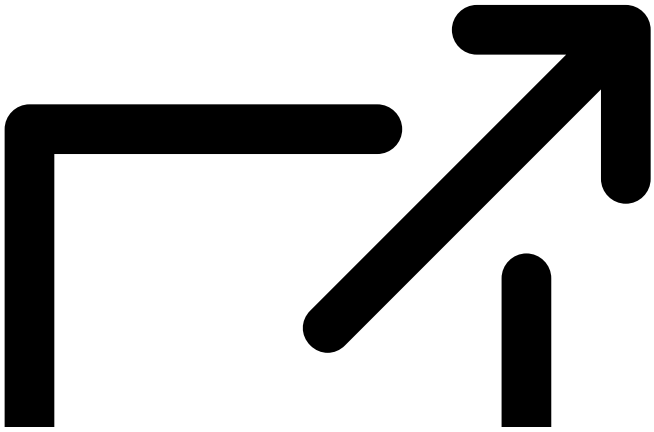
Recommendations

- **Implement multi-factor authentication (MFA).** Authentication is a process used to validate a user's identity. Attackers commonly exploit weak authentication processes. MFA uses at least two identity components to authenticate a user's identity. Identity components include

    - Something the user knows (e.g., password),
    - An object the user has possession of (e.g., token), and
    - A trait unique to the user (e.g., fingerprint).

- **Manage privileged access.** Use a server that provides authentication, authorization, and accounting (AAA) services to store access information for network device management. An AAA server will enable network administrators to assign different privilege levels to users based on the principle of least privilege. When a user tries to execute an unauthorized command, it will be rejected. If possible, implement a hard-token authentication server in addition to using the AAA server. Using MFA makes it more difficult for intruders to steal and reuse credentials to gain access to network devices.
- **Manage administrative credentials.** Take these actions if your system cannot meet the MFA best practice:

    - Change default passwords.
    - Ensure passwords are at least eight characters long, and allow passwords as long as 64 characters (or greater), in accordance with the National Institute of Standards and Technology's SP 800-63C Digital Identity Guidelines and Canada's User Authentication Guidance for Information Technology Systems ITSP.30.031 V3



.

    - Check passwords against deny lists of unacceptable values, such as commonly used, expected, or compromised passwords.
    - Ensure all stored passwords are salted and hashed.
    - Keep passwords stored for emergency access in a protected off-network location, such as a safe.

Perform Out-of-Band Management

OoB management uses alternate communications paths to remotely manage network infrastructure devices. These dedicated communications paths can vary in configuration to include anything from virtual tunneling to physical separation. Using OoB access to manage the network infrastructure will strengthen security by limiting access and separating user traffic from network management traffic. OoB management provides security monitoring and can perform corrective actions without allowing the adversary (even one who has already compromised a portion of the network) to observe these changes.

OoB management can be implemented physically, virtually, or through a hybrid of the two. Although building additional physical network infrastructure can be expensive to implement and maintain, it is the most secure option for network managers to adopt. Virtual implementation is less costly but still requires significant configuration changes and administration. In some situations, such as access to remote locations, virtual encrypted tunnels may be the only viable option.

Recommendations

- Segregate standard network traffic from management traffic.
- Ensure that management traffic on devices comes only from OoB.
- Apply encryption to all management channels.
- Encrypt all remote access to infrastructure devices such as terminal or dial-in servers.
- Manage all administrative functions from a dedicated, fully patched host over a secure channel, preferably on OoB.
- Harden network management devices by testing patches, turning off unnecessary services on routers and switches, and enforcing strong password policies. Monitor the network and review logs. Implement access controls that only permit required administrative or management services (e.g., SNMP, Network Time Protocol, Secure Shell, FTP, Trivial FTP, Remote Desktop Protocol [RDP], Server Message Block [SMB]).

Validate Integrity of Hardware and Software

Products purchased through unauthorized channels are often known as counterfeit, secondary, or gray market devices. Numerous media reports have described the introduction of gray market hardware and software into the marketplace. Illegitimate hardware and software present a serious risk to users' information and the overall integrity of the network environment. Gray market products can introduce risks to the network because they have not been thoroughly tested to meet quality standards. Purchasing products from the secondary market carries the risk of acquiring counterfeit, stolen, or second-hand devices because of supply chain breaches. Furthermore, breaches in the supply chain provide an opportunity for malicious software and hardware to be installed on the equipment. Compromised hardware or software can affect network performance and compromise the confidentiality, integrity, or availability of network assets. Finally, unauthorized or malicious software can be loaded onto a device after it is in operational use, so organizations should check the integrity of software on a regular basis.

Recommendations

- Maintain strict control of the supply chain and purchase only from authorized resellers.
- Require resellers to enforce integrity checks of the supply chain to validate hardware and software authenticity.
- Upon installation, inspect all devices for signs of tampering.
- Validate serial numbers from multiple sources.
- Download software, updates, patches, and upgrades from validated sources.
- Perform hash verification, and compare values against the vendor's database to detect unauthorized modification to the firmware.
- Monitor and log devices—verifying network configurations of devices—on a regular schedule.
- Train network owners, administrators, and procurement personnel to increase awareness of gray market devices.