National Security Agency | Cybersecurity Information

Performing Out-of-Band Network Management

Out-of-Band (OoB) network management is a concept that uses an alternate communication path to manage network infrastructure devices. These alternate paths are designed to isolate management traffic from operational traffic. This isolation prevents compromised user devices or malicious network traffic from impacting network operations or compromising network infrastructure. Implementing these alternate paths can vary in configuration from virtual tunneling (sharing the physical network connections with the operational network) to a physically segmented network infrastructure. OoB management creates a framework that enables administrators to improve the security of their networks by segmenting management traffic from operational traffic, and ensuring that management traffic only comes from the OoB communication path.

Out-of-Band Architecture Design

A single OoB management design may not fall within the security requirements or financial constraints for each installation. Fortunately, there are multiple approaches to implementing OoB management with a range of security protections and related costs. To begin the process of determining which implementation will provide the desired level of protection, network owners need to perform a vulnerability and risk assessment. The information gathered from these assessments will aid in deciding to implement a virtually or physically segmented OoB network architecture. Regardless of architecture design, NSA recommends all management traffic utilize only encrypted protocols, such as Secure Shell (SSH), Hypertext Transfer Protocol Secure (HTTPS), Simple Network Management Protocol v3 (SNMPv3), Secure Copy (SCP), and Secure File Transfer Protocol (SFTP), with strong encryption algorithms and key sizes. NSA also recommends never managing any device over an untrusted network, which includes the operational network, without a strong Virtual Private Network (VPN). Never should a network device's management interface be directly accessible from the Internet.

Physical Segmentation

The most secure OoB management design is to create a physically segmented management infrastructure that allows for secure administration and monitoring of network devices. Each operational network device will have a dedicated interface connecting to the physically segmented management network. These dedicated interfaces must be isolated from the operational network and have strict Access Control Lists (ACLs) implemented to prevent a possible misconfiguration from allowing unauthorized access to management services. Administrator workstations should only be connected to the management network and all other network access should be restricted. For critical devices, such as perimeter firewalls or routers, the use of console management switches can be used to create a protocol break and eliminate the possibility of a compromised device from accessing other devices on the management network. A dedicated physical network infrastructure is the most secure option; however, it can be expensive to implement and maintain as it requires additional network devices, cabling, and servers.

Virtual Segmentation

Completing detailed vulnerability and risk assessments allows the network owners to consider implementing a more cost-effective and economical virtual segmentation approach to network management. The virtual segmentation design is a less secure option, but it is attractive due to reduced cost and maintenance. Virtual segmentation allows the management traffic to share the same physical links with operational traffic. However, the network designer must logically segment the two types of traffic. This virtual segmentation can be implemented using multiple Virtual Local Area Networks (VLANs), Virtual Routing and Forwarding (VRFs), VPNs, or other zero trust and micro-segmentation technologies. The major vulnerability in these configurations is potential data leakage where devices on the operational network may capture sensitive management traffic or management traffic is accidentally sent over the operational network. To mitigate most of these vulnerabilities, NSA recommends the management traffic utilize strong encryption.

An often overlooked security design flaw with virtually segmented networks is authentication, logging, and other management services that are not properly isolated. When deploying a virtually segmented OoB network, these services should not be shared with the operational network. If these services are shared between the management and the operational network, they create a hop point between the two. Adversaries will use this access to expand to other network devices through the legitimate management network. Also, a shared authentication server could allow an adversary to pivot from the operational network to the management network by compromising the authentication server itself with a simple “Pass-the-Hash” type of credential reuse.

Recommendations

Implement Encryption

- Utilize only encrypted protocols on all OoB management traffic.
- Utilize VPNs when connecting to management networks over an operational network.
- Ensure encrypted protocols are configured to use strong cryptographic algorithms and key sizes.

Harden Network Management Devices

- Restrict all management access on network devices to only allow the management network.
- Execute all management operations from dedicated, fully patched hosts accessible only by authorized network administrators. At least two such management hosts should be available to provide redundancy.
- Allow only dedicated management hosts to access network devices to prevent compromised lateral movement from user devices.
- Secure OoB networks by continually applying patches.
- Test patches prior to implementing them on the network.
- Turn off unnecessary services on routers and switches.
- Implement multi-factor authentication to access the devices securely.
- Use only serial connections or console management switches for critical devices.

Monitor Network and Review Logs

- Establish and adhere to a Site Security Policy (SSP) for the OoB network guidelines that articulate the design for management devices, the roles and responsibilities of administrators, and the process for logging.
- Check logs for unauthorized logins, unauthorized reboots, and misconfigured settings.
- Monitor and verify network configurations on a regular basis.

Establish Configuration Management Procedures

- Configuration management is critical to the health, maintenance, and security of any network. NSA recommends establishing a configuration review and check-in process. This process will create a history of network changes and allow an administrator to quickly identify malicious changes.
- Include the identification by job title of all individuals who must approve changes to the OoB management network as well as those who execute the changes.
- Define access control configurations in the security policy.
- Use “Principle of Least Privilege” when defining access controls.
- Enable strong authentication mechanisms and require network administrators to use strong passwords with a minimum length of 14 characters.
- Use secure communication protocols on the OoB management network and disable all protocols that are not required.
- Maintain ACLs to permit needed services (HTTPS, SNMPv3, SSH, SCP, and SFTP) and deny all others.
- Use Simple Network Management Protocol (SNMP) version 3 or newer with encryption enabled. Avoid using SNMPv1 and SNMPv2. They are legacy protocols and do not provide an adequate level of security.

Disclaimer

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Purpose

This document was developed in furtherance of NSA's cybersecurity missions, including its responsibilities to identify and disseminate threats to National Security Systems, Department of Defense, and Defense Industrial Base information systems, and to develop and issue cybersecurity specifications and mitigations. This information may be shared broadly to reach all appropriate stakeholders.

Contact Information

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410-854-4200, Cybersecurity_Requests@nsa.gov
Media inquiries / Press Desk: Media Relations, 443-634-0721, MediaRelations@nsa.gov