Perform Out-of-Band Network Management

June 2016



Out-of-Band (OoB) network management is a concept that utilizes an alternate communication path to remotely manage network infrastructure devices. These alternate channels are designed and implemented to isolate management traffic from normal user traffic, so compromised user devices and communications cannot affect network operations or compromised network devices. These alternate channel implementations can range from virtual tunneling (sharing the same medium) to physically separate connections. OoB management creates a framework that enables administrators to improve security monitoring of the operational network by separating management traffic from operational traffic, and ensuring that management traffic only comes from the OoB.

Design Types for OoB

Design types for OoB management include physical, virtual, and a hybrid of the two. A single management design does not meet the security requirements and financial limitations for each installation. Fortunately, there are multiple approaches to implementing OoB management with a range of security protection and related costs. Asset owners need to perform a vulnerability and risk assessment for the network to determine which implementation will provide their system with the desired level of protection.

Physical Implementation

The preferred security design is to create a physically separate management infrastructure that allows for secure administration and monitoring services for network devices. These network channels can be implemented with classic dial-up modem, leased lines, or dedicated channels. In remote locations, the separate channel can provide a redundant network connection should there be physical damage to either network connection. Even with a separate channel, there is no guarantee the channel is physically secure end to end; therefore, strong encryption is still a requirement. Although providing a dedicated network infrastructure is the most secure option, it can be expensive to implement and maintain.

Virtual Implementation

Completing detailed vulnerabilities and risk assessments can allow the network owners to consider implementing a more cost-effective and economical virtual channel approach to network management. The virtual channel design is a less secure option but is attractive due to reduced cost and maintenance. The virtual channel allows the management traffic to share the same physical medium with operational traffic. However, the network designer must logically separate the two types of traffic. These virtual channels can be implemented using multiple Virtual Local Area Networks (VLANs) or Virtual Private Networks (VPNs). In all cases the management traffic must be encrypted. An additional benefit of properly separated traffic channels is simplified Intrusion Detection System (IDS) rule sets, resulting in improved warnings and alerts with reduced false alarms.

Hybrid Implementation

A hybrid option exists which can provide some of the benefits of both traditional approaches. In the hybrid design, the primary management implementation system is based on a virtual channel. However, a secondary management channel can be added with a secure dial-up connection. This secondary channel may provide the required redundancy channel for critical systems in remote locations. The dial-up connection requires special attention to ensure secure access including implementation of VPNs with IPSEC encryption and strong authentication. OoB management that uses a physical design increases the likelihood of maintaining management connectivity independent of the working state of in-band network components.

Recommendations

Implement Encryption

- Apply strong encryption to all OoB management channels, including remote connections. Encryption should always be used even when a physically separate OoB infrastructure is implemented.
- Encrypt network links (copper wire, fiber and wireless) that cannot be physically protected.
- Encrypt phone line connections with dial-back, caller ID, and inline TouchTone password capabilities.

Perform Out-of-Band Network Management

- 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.
- Restrict access to network devices only from the dedicated management hosts to prevent compromised lateral movement from devices.

Harden Network Management Devices

Secure OoB networks by decreasing the risk of adversaries moving laterally through un-patched systems, directing routing protocols and implanting malware.

- Test patches prior to implementing them on the network.
- Turn off unnecessary services on routers and switches.
- Implement multi-factor authentication to securely access the devices.
- Use strong passwords with a minimum length of 14 characters.

Monitor Network and Review Logs

- Establish and adhere to a site security policy for the OoB network that outlines roles and responsibilities of the administration functions, management of devices, and logging.
- Check logs for unauthorized logins, unauthorized reboots, and misconfigured settings.
- Continuously 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, especially an OoB network. Network management is an attractive target for an inside or outside adversary. Think like the adversary when developing OoB management systems to mitigate threats. All too often networks evolve over time and security is just an afterthought. For an OoB management framework to be successful, the network designer must start with a strong security policy.

- Establish policies/procedures for coordinating, approving, and executing changes to network infrastructure.
- 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.
- Take advantage of the security capabilities of the equipment attached to the OoB management network.
- 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 Access Control Lists to permit needed services (SNMP, NTP SSH, TFTP, FTP).
- Use Simple Network Management Protocol (SNMP) version 3 or newer with security features enabled, including encryption. Avoid any SNMP version prior to version 3 as these provide no acceptable security feature.

Contact Information

Industry Inquiries:

Business Affairs Office
410-854-6091
email: bao@nsa.gov

Client Requirements and General Information Assurance Inquiries:

IAD Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov

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.