Dealing with the problem…

- Securing Systems Management components requires a combination of network architecture and system configuration.

Two Core Designs

DMZ Network Architecture for System Management

- Example 1. Combination of Management and Production Traffic on the same untrusted segment.

- Definition of untrusted segment: Where untrusted users and/or processes can place packets on the segment.

- Advantages:
  - Simple to manage, do not have deal with multiple interfaces
  - Easier firewall rulesets and router ACLs to manage

DMZ Network Architecture for System Management

- Example 1. Combination of Management and Production Traffic on the same untrusted wire.
- Disadvantages:
  - Bandwidth utilization
  - Failure to segment different types of traffic introduces security risks
  - Must place loghosts, monitoring consoles, and control components on the internal network to keep isolation
  - Harder to monitor for policy violations
  - Untrusted segment behind firewall will advertise management services
  - For services that listen for input, must configure host-based inclusion rather than interface/network inclusion
  - Compromised host on segment could spoof management connection

DMZ Network Architecture for System Management

- Example 2: Separate Management LAN.
- Advantages:
  - Protects bandwidth on untrusted network segment
  - Introduces another hurdle for intruders to jump interfaces, which can be locked down more aggressively
  - Ability to monitor for violations in both segments improved
  - Can place loghosts, monitoring hosts, and control components in management LAN with less risk, reducing internal network exposure and reliance
  - Allows for more flexibility with private address space and less border firewall concerns

DMZ Network Architecture for System Management

- Example 2. Separate Management LAN.
- Disadvantages:
  - Need to make sure that forwarding is disabled; routing must be configured correctly on each host; additional configuration and equipment needed
  - Management LAN can still be used as a conduit to attack hosts if not properly secured and monitored
  - Adds complexity to segmented DMZs and potential bypass mechanism between segments

Advanced Design Issues

DMZ Network Architecture for System Management

- Example 3. Management Aggregation Points based on natural segregation of the segmented DMZ.
- Advantages:
  - Works well in segmented DMZs
  - Reduces management LAN bandwidth
  - All of the advantages of segmented DMZs
- Disadvantages:
  - More equipment and more routes
  - Need to maintain ACLs and rulesets between Management LANs
  - Additional points of failure
  - All of the disadvantages of segmented DMZs

DMZ Network Architecture for System Management

- Example 4. Pushing data versus pulling data.
- Pushing data from internal network to the DMZ/Admin LAN. Good – but how much do you trust your internal users?
- DMZ/Admin LAN pulling data from the internal network. Bad.
- Degrees of push:
  - File / Data one-way with or without validation
  - Interactive transfer with restricted privilege
  - Remote control administration with full interactivity
- Use the minimum amount of push whenever possible.
- When DMZ hosts need to push data for administrative purposes, aggregate in the same trust boundary. Then pull from a more trusted environment.
- Never have DMZ hosts pull or push from the Internet without appropriate risk analysis and mitigation.

The Need for Systems Management

- Backup
- Diagnostic information and availability monitoring
- Remote administration
- System logging

Backup Solutions

- Risks
  - Bandwidth utilization
  - Unauthorized restore / backup
  - Capture of backup traffic
  - Agent vulnerabilities – authentication
  - Procedures for restore offsite
  - Local backup devices unmanageable or difficult to scale
  - Backup clients not necessarily designed with security in mind

Backup Solutions

Securing Backup Solutions

- Protect the backup server at all costs
  - Place behind another firewall / filter
  - Backup server should initiate all backup / restore requests to eliminate inbound connections
  - Consider the physical security of the server and the media
  - Implement tight security controls on server.
- Encryption – examine the risks / benefits
  - Is the wire insecure? If so, client has burden of encrypting the data.
  - Store the data encrypted or not? How is key management performed? What happens if the key is lost?
  - Encrypt both on-site and off-site media?

Backup Solutions

Securing Backup Solutions

- Administrative LAN segment very beneficial for backup solutions
- Implementing a Storage Area Network may provide another means for backup that doesn't use the LAN
- One example of a hard-to-secure product:
  - Legato:
    - Server uses default ports 7937-9936/TCP&UDP
    - Client uses default ports 10001-30000/TCP&UDP
    - Runs its own portmapper
    - Ports can be restricted
    - Authentication client/server unclear
    - NAT not supported
    - Unable to determine which interface it listens on

Monitoring Solutions

SNMP

- Assume that anything sent over SNMP is readable by all.
- Community strings should be changed.
- If possible, limit the hosts that can query SNMP on the queried device itself.
- Examine the type of information that your device gives via SNMP – it may surprise you.
- Determine the criticality of the information when deciding whether or not to use SNMP.
- Never allow reconfiguration of devices via SNMP. Disable write privileges on any SNMP device.
- Traps should be used sparingly and there should be a dedicated receiver in the DMZ.
- NT SNMP giveaway.
- Oftentimes, it is the lesser of another evil.

Monitoring Solutions

ICMP

- Echo reply/request is fine on an internal interface.
- If possible, throttle your ICMP response queue.