



Network Security Checklist - Other Devices

Version 7, Release 1.1

20 November 2007

Developed by DISA for the DOD

UNCLASSIFIED

UNCLASSIFIED UNTILL FILLED IN

CIRCLE ONE

FOR OFFICIAL USE ONLY (mark each page)

CONFIDENTIAL and SECRET (mark each page and each finding)

Classification is based on classification of system reviewed:

Unclassified System = FOUO Checklist

Confidential System = CONFIDENTIAL Checklist

Secret System = SECRET Checklist

Top Secret System = SECRET Checklist

Site Name	
Address	
Phone	

Position	Name	Phone Number	Email	Area of Responsibility
IAM				
IAO				

NET0230 **V0003012** **CAT I** **Communications devices are not password protected.**

8500.2 IA Control: ECSC-1, IAIA-1, IAIA-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all communications devices are password protected.

Vulnerability Discussion The lack of a password protection for communications devices provides anyone access to the device, which opens a backdoor opportunity for intruders to attack and manipulate or compromise network resources. Vendors and programmers often leave methods of gaining access to a device that is outside the normal means of access. These backdoors or hidden userids are well known and are extremely dangerous if left active.

Checks

NET Password Protection

Interview the network administrator and attempt to logon to several devices.

Default Finding Details Communications devices are not password protected in accordance with DISA requirements.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET Password Protection

Ensure all communication devices are in compliance with password policy.

Notes:

NET0240 **V0003143** **CAT I** **Devices exist that have standard default passwords**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all default manufacturer passwords are changed.

Vulnerability Discussion Devices not protected with strong password schemes provide the opportunity for anyone to crack the password thus gaining access to the device and causing network, device, or information damage, or denial of service. Not changing the password in a timely manner increases the likelihood that someone will capture or crack the password and gain unauthorized access to the device.

Checks

NET Password Protection

Interview the network administrator and attempt to logon to several devices.

Default Finding Details

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET Password Protection

Ensure all communication devices are in compliance with password policy.

Notes:

NET0340 **V0003013** **CAT II** **Warning banner compliance to 8500.2 ECWM-1.**

8500.2 IA Control: ECWM-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure warning banners are deployed on all network devices allowing SSH, Telnet, File Transfer Protocol (FTP), or Hyper-Text Transfer Protocol (HTTP) access in accordance with DODI 8500.2 ECWM-1.

Vulnerability Discussion Failure to display the required login banner prior to logon attempts will limit the sites ability to prosecute unauthorized access and also presents the potential to give rise to criminal and civil liability for systems administrators and information systems managers. Not displaying the proper banner will also hamper the sites ability to monitor device usage.

Checks

NET Warning Banners

Have the network administrators sign onto each managed network device to ensure the DoD approved warning banners are displayed before the password prompt and after a correct login.

Default Finding Details DOD approved warning banners, adhering to Appendix C of the Network Infrastructure STIG, are not displayed on network managed devices.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET Warning Banner

Display the approved DOD login banner prior to a login attempt on all network devices allowing Telnet, File Transfer Protocol (ftp), or Hyper Text Transfer Protocol (http) access.

Notes:

NET1027 **V0003031** **CAT III** **Syslog SRV is not configured to collect levels 0-6**

8500.2 IA Control: ECAT-1, ECAT-2, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The syslog administrator will configure the syslog sever to collect syslog messages from levels 0 through 6.

Vulnerability Discussion Logging is a critical part of router security. Maintaining an audit trail of system activity logs (syslog) can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network. Syslog levels 0-6 are the levels required to collect the necessary information to help in the recovery process.

Checks

NET Syslog Srv Severity Codes

Review the syslog server configuration to ensure that it is collecting syslog messages levels 0 through 6 for the appropriate facilities (Cisco routers default to Local7).

Default Finding Details The syslog server is not configured to collect syslog message levels 0-6 and/or the router is not configured to send syslog message levels 0-6 to the syslog server.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET Syslog Srv Severity Codes

The router administrator will configure the router and syslog server to collect syslog messages levels 0 through 6.

Notes:

NET1028 **V0003033** **CAT III** **Restrict messages to the Syslog Server.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The syslog administrator will configure the syslog server to accept messages only from authorized devices (restricting access via source and destination IP address).

Vulnerability Discussion Restrict access to the Syslog server by approved IP addresses/users. If an unauthorized user gains access to the Syslog server and it is compromised, access to critical network information would be available. This information could be used to mount attacks against the network.

Checks

NET Syslog Srv Restrict Access

Base Procedure: Review the syslog server configuration to ensure that it is configured to accept messages from only authorized devices.

Default Finding Details The syslog server is not configured to restrict messages, via IP ACLs, from unauthorized devices.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET Syslog Srv Restrict Access

The router administrator will configure the router to restrict syslog server messages to only authorized devices (restricting access via source and destination IP address).

Notes:

NET1650 **V0003211** **CAT II** **Secure NMS traffic using IPSEC**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure IPsec is used to secure traffic between the network management workstation on DOD-managed LANs and all monitored devices sent via the Internet, NIPRNet, SIPRNet, or other external network.

Vulnerability Discussion To securely protect the network, Network Management Systems (NMS) and access to them must be controlled to guard against outside or unauthorized intrusion, which could result in system or network compromise. Allowing any device to send traps or information may create a false positive and having site personnel perform unneeded or potentially hazardous actions on the network in response to these false traps. These sessions must be controlled and secured by IPsec.

Checks

NET SNMP IPSEC

Interview the network administrator to ensure that IPSEC is being used to secure traffic sent between network management center workstations and all monitored devices.

Default Finding Details

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET SNMP IPSEC

The NSO will ensure IPsec is used to secure traffic sent between network management workstations and all monitored devices.

Notes:

NET1660

V0003196 CAT I

An insecure version of SNMP is being used.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IA/NSO will ensure that the SNMP Version 3 Security Model (both MD5 packet authentication and DES encryption of the PDU) is used across the entire network infrastructure.

Vulnerability Discussion SNMP Versions 1 and 2 are not considered secure. Without the strong authentication and privacy that is provided by the SNMP Version 3 User-based Security Model (USM), an attacker or other unauthorized user may gain access to detailed network management information and use that information to launch attacks against the network.

Checks

NET SNMP Version

Interview the network administrators and examine configurations of managed nodes (routers, switches, etc).

If the site is using Version 1 or Version 2 with all of the appropriate patches and has developed a migration plan to implement the Version 3 Security Model, this finding can be downgraded to a Category II.

To verify the appropriate patches on CISCO devices: Check IAVMs associated with SNMP. As of 11/01/2007 there were four (V0005835, V0005809, V0005942, V0012769).

To verify the appropriate patches on other vendors: Reference this website: <http://www.cert.org/advisories/CA-2002-03.html>

Default Finding Details SNMP V1 or V2 has been enabled on the network infrastructure.

SNMP V3 has been enabled on the network infrastructure without the V3 User-based Security Model authentication and privacy.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET SNMP Version

The NSO will ensure that the SNMP Version 3 Security Model (both MD5 packet authentication and DES encryption of the PDU) will be used across the entire network infrastructure.

Notes:

NET1665 **V0003210** **CAT I** **System community names or usernames use defaults**

8500.2 IA Control: ECSC-1, IAIA-1, IAIA-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAQ/NSO will ensure that all SNMP community strings are changed from the default values.

Vulnerability Discussion Community strings default to the name PUBLIC. This is known by those wishing to exert an attack against the devices in the network. This must be changed to something that is in compliance with DISA password guidelines. Not all individuals need write access to the device. Compromising the read password will have less of an impact if it cannot be used to change information. An erroneous message being sent to the NMS can cause network managers to act inappropriately in responding to an alarm or warning. It is important that the information being received is from valid managed devices.

Checks

NET SNMP Community Strings

Interview the network administrators and examine configurations of managed nodes (routers, switches, etc).

Default Finding Details

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET SNMP Community Strings

Most network management systems (NMSs) default to a community sign on name of public. This community name will be changed to something that is not easily guessed. It will be protected in the same way as any password is protected.

Notes:

NET1666 **V0005621** **CAT II** **Encryption required for SNMP community**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAQ/NSO will ensure that all SNMP community strings and usernames are protected via technology that secures using an encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion Compromising the network can cause erroneous messages being sent to the NMS that can cause network managers to act inappropriately in responding to an alarm or warning. It is important that the information being received is from valid managed devices.

Checks

NET SNMP encryption

Interview the network administrators and examine configurations of managed nodes (routers, switches, etc).

Default Finding Details Encryption required for SNMP community.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET SNMP encryption

Network management systems (NMSs) will be protected in the same way as any password is protected via FIPS 140-2 approved data encryption.

Notes:

NET1675

V0003043 CAT II

Exclusive use of privileged and non-privileged

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that if both privileged and non-privileged modes are used on all devices. Different community names will be used for read-only access and read-write access.

Vulnerability Discussion Numerous vulnerabilities exist with SNMP, therefore, without unique SNMP community names, the risk of compromise is dramatically increased. This is especially true with vendors default community names which are widely known by hackers and other networking experts. If a hacker gains access to these devices and can easily guess the name, this could result in denial of service, interception of sensitive information, or other destructive actions.

Checks

NET SNMP Least Privilege

Review the configuration of all managed nodes (SNMP agents) to ensure that different community names or usernames are used for read-only and read-write access.

Default Finding Details SNMP community names have not been changed from their default values and privilege levels are not set correctly.

The following community names have not been changed:

The following name appears on multiple devices:

The following privilege levels are set incorrectly:

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET SNMP Least Privilege

The NSO will ensure that SNMP community names are changed from the default public values to unique community names and developed IAW the Network Infrastructure STIG.

The NSO will ensure these names do not match any other network device passwords, keys or strings.

The NSO will ensure that unique community names are used for different access types, including read-only, read and write.

Notes:

NET1710

V0003046 CAT III

NMS security alarms not define by violation type.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that security alarms are set up within the managed network's framework. At a minimum, these will include the following:

- Integrity Violation: Indicates that network contents or objects have been illegally modified, deleted, or added.
- Operational Violation: Indicates that a desired object or service could not be used.
- Physical Violation: Indicates that a physical part of the network (such as a cable) has been damaged or modified without authorization.
- Security Mechanism Violation: Indicates that the network's security system has been compromised or breached.
- Time Domain Violation: Indicates that an event has happened outside its allowed or typical time slot.

Vulnerability Discussion Without the proper categories of security alarms being defined on the NMS, responding to critical outages or attacks on the network may not be coordinated correctly with the right personnel, hardware, software or vendor maintenance. Delays will inevitably occur which will cause network outages to last longer than necessary or expose the network to larger, more extensive attacks or outages.

Checks

NET SNMP Security Alarms

Request that the network engineer demonstrate the alert capabilities.

Default Finding Security alarms are not configured for the following network events:

Details
Integrity Violation
Operational Violation
Physical Violation
Security Mechanism Violation
Time Domain Violation

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET SNMP Security Alarms

The NSO will ensure that the NMS is configured, at a minimum, to alarm on the following security violations: integrity, operational, physical, security mechanism, and time domain violation.

Notes:

NET1720

V0003047 CAT III

NMS security alarms not defined by severity.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that alarms are categorized by severity using the following guidelines:

- Critical and major alarms are given when a condition that affects service has arisen. For a critical alarm, steps must be taken immediately in order to restore the service that has been lost completely.
- A major alarm indicates that steps must be taken as soon as possible because the affected service has degraded drastically and is in danger of being lost completely.
- A minor alarm indicates a problem that does not yet affect service, but may do so if the problem is not corrected.
- A warning alarm is used to signal a potential problem that may affect service.
- An indeterminate alarm is one that requires human intervention to decide its severity.

Vulnerability Discussion Without the proper categories of severity levels being defined on the NMS, outages or attacks may not be responded to by order of criticality. If a critical attack or outage is not responded to first, then there will be a delay in fixing the problem, which may cause network outages to last longer than necessary or expose the network to larger more extensive attacks or outages.

Checks

NET SNMP Alarm Categories

Request that the network engineer demonstrate the alert capabilities.

Default Finding Details NMS security alarm severity levels are not categorized according to major, minor, warning, and indeterminate.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET SNMP Alarm Categories

The NSO will ensure that the NMS security alarm severity levels are configured as critical, major, minor, warning and indeterminate.

Notes:

NET1750 V0003050 CAT III Logons and transactions are not being recorded.

8500.2 IA Control: ECAR-1, ECAR-2, ECAR-3, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IA/NSO will ensure a record is maintained of all logons and transactions processed by the management station.

NOTE: Include time logged in and out, devices that were accessed and modified, and other activities performed.

Vulnerability Discussion Logging is a critical part of network security. Maintaining an audit trail of system activity logs can help identify configuration errors, understand past intrusions, troubleshoot service disruptions, and react to probes and scans of the network. Audit logs are also necessary to provide a trail of evidence in case the network is compromised. Without an audit trail that provides a when, where, who and how set of information, repeat offenders could continue attacks against the network indefinitely. With this information, the network administrator can devise ways to block the attack and possibly identify and prosecute the attacker.

Checks

NET NMS Logs

Review the NMS configuration and logs

Default Finding Details NMS logons and transactions are not being recorded, to include: time logged in and out, devices that were accessed and modified, and other activities performed.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET NMS Logs

The NSO will ensure that the NMS records all logons and transactions on the management station. The log will include at a minimum: time logged in and out, devices that were accessed and modified, and other activities performed. The audit will be stored online for a minimum of 30 days and offline for at least one year.

Notes:

NET1760 V0003051 CAT I Logon access to the NMS is not restricted.

8500.2 IA Control: ECSC-1, IAIA-1, IAIA-2

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IA/NSO will ensure access to the NMS is restricted to authorized users with individual userids and passwords.

Vulnerability Discussion If unauthorized users gain access to the NMS they could change device configurations and SNMP variables that can cause disruptions and even denial of service conditions.

Checks

NET NMS Identity Management

Review the NMS configuration to verify compliancy.

Default Finding Details Access to the NMS is not restricted to authorized users with individual userids and passwords.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET NMS Identity Management

The NOC will ensure that access to the NMS is available only to authorized users with appropriate userids and passwords.

Notes:

NET1762 **V0004613** **CAT II** **In-band access to the NMS is not encrypted.**

8500.2 IA Control: ECNK-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that all in-band sessions to the NMS is secured using an encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion Without encrypted in-band management connections, unauthorized users may gain access to the NMS enabling them to change device configurations and SNMP variables that can cause disruptions and even denial of service conditions.

Checks

NET NMS In-band FIPS encrypted

Review the configuraton for the NMS to verify that only SSH can be used to access the NMS.

Default Finding Details In-band management access to a DOD system is not encrypted.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET NMS In-band FIPS encrypted

For in-band management, the router administrator will configure the network device to only allow SSH connections.

Notes:

NET1770 **V0003052** **CAT II** **Access to the NMS is not restricted by IP address.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure connections to the NMS are restricted by IP address to only the authorized devices being monitored..

Vulnerability Discussion Without restricting device connections by IP address to the NMS, unauthorized devices or users could send bogus messages that might flood the system with invalid information , degrade its operation, or make it unusable.

Checks

NET NMS Restricted LAN

Review the NMS configuration to verify compliancy.

Default Finding Details IP address restriction is not in place to limit connections to the NMS to only the authorized devices being monitored.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET NMS Restricted LAN

The NSO will ensure that the access to the NMS is restricted by IP address to only the authorized devices being monitored.

Notes:

NET1780

V0003184 CAT II

Least Privilege not IAW policies in NMS.

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure all accounts are assigned the lowest possible level of access/rights necessary to perform their jobs.

Vulnerability Discussion Without a formal personnel approval process, unauthorized users may gain access to critical DoD systems. It is imperative that only the required access to the required systems and information be provided to each individual.

The lack of a password protection for communications devices provides anyone access to the device, which opens a backdoor opportunity for intruders to attack and manipulate or compromise network resources. Vendors often assign default passwords to communication devices. These default passwords are well known to the hacker community and are extremely dangerous if left unchanged.

Checks

NET NMS Least Privilege

Review the user database to determine compliance.

Default Finding Accounts have been created without the lowest privilege level needed to perform their duties.

Details

Default vendor passwords have not been changed prior to deployment on the network.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET NMS Least Privilege

Have the NSO ensure that accounts are created with the lowest privilege necessary to perform their duties.

Notes:

NET1800

V0003008 CAT II

VPN is not configured as a tunnel type VPN.

8500.2 IA Control: EBVC-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure VPNs are established as tunnel type VPNs.

Vulnerability Discussion VPNs improperly deployed take away a firewalls ability to audit useful information, or to make decisions beyond the level of who is allowed to talk to whom. There are ways around this. The easiest way is for a hacker to make the firewall a trusted third member of the conversation.

Checks

NET VPN Tunnel Type

Have the SA display the configuration settings that enable this feature.

Review the network topology diagram, and review VPN concentrators. Determine if tunnel mode is being used by reviewing the configuration. Examples:

In CISCO

```
Router(config)# crypto ipsec transform-set transform-set-name transform1  
Router(cfg-crypto-tran)# mode tunnel
```

OR in Junos

```
edit security ipsec security-association sa-name] mode tunnel
```

Default Finding Details VPN is not configured as a tunnel type VPN.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET VPN Tunnel Type

Establish the VPN as a tunneled VPN.

Terminate the tunneled VPN outside of the firewall.

Ensure all host-to-host VPN are established between trusted known hosts.

Notes:

NET1837

V0003982 CAT II

The VPN connection is not using IPSec's ESP tunnel

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that remote access VPN concentrator uses IPSec ESP in tunnel mode. For legacy support, L2TP may be used if IPSec provides encryption (DAA approval required), or another technology that secures using an encryption such as AES, 3DES, SSH, or SSL.

Vulnerability Discussion The AH security protocol only provides data authentication and integrity for packets forwarded between systems. AH does this authentication by creating a hash value for the IP Header and Data. Once the packet arrives at the destination, the source and destination hash values must match. Otherwise the packet is dropped. The headers and data are not encrypted.

In transport mode, IPSec encrypts only the data component (payload) of the IP packet to be transported: application headers, TCP/UDP headers and data are encrypted, the original IP headers are readable exposing the client's source address.

In tunnel mode, IPSec encrypts both the payload and the headers.

Checks

NET VPN IPSEC ESP

Review the network topology diagram, and review VPN concentrators. Determine if tunnel mode is being used by reviewing the configuration. Example:

```
Router(config)# crypto ipsec transform-set transform-set-name transform1
```

```
Router(cfg-crypto-tran)# mode tunnel
```

OR in Junos

```
edit security ipsec security-association sa-name] mode tunnel
```

Default Finding Details The VPN connection is not using IPSec's ESP tunnel mode.

OPEN: **NOT A FINDING:** **NOT REVIEWED:** **NOT APPLICABLE:**

Fixes

NET VPN IPSEC ESP

Ensure that remote access via VPN will use IPSec ESP in tunnel mode.

Notes: