



Network Security Checklist - Firewall

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				

NET0190

V0003005 CAT III

LAN addresses are not protected from the public.

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that workstation clients' real IPv4 addresses are not revealed to the public by implementing NAT on the firewall or the router.

Vulnerability Discussion NAT works well with the implementation of RFC 1918 addressing scheme, it also has the privacy benefit of hiding real internal addresses. An attacker can learn more about a site's private network once it has discovered the real IP addresses of the hosts within.

Checks

NET NAT Requirement

Review the firewall or premise router configuration to determine if NAT has been implemented.

Default Finding Details NAT has not been implemented. Mark this as N/A for SIPRNet enclaves that have not implemented NAT.

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

Fixes

NET NAT Requirement

Implement Network Address Translation (NAT) on the firewall or premise router for NIPRNet Enclaves.

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 IAQ/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:

NET0366 V0014643 CAT II No proxy implementation

8500.2 IA Control: DCCS-2, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure proxies are implemented between the enclave and external network boundaries defined in the PPS CAL for listed examples in the following boundaries:

- Boundary 8 Outbound from Enclave to DoD Network
- Boundary 12 Outbound from Enclave to Enclave DMZ
- Boundary 13 Outbound from Enclave to External
- Boundary 16 Outbound from Enclave to Enclave

Vulnerability Discussion Creating a filter to allow a port or service through the firewall without a proxy, creates a direct connection between the host in the private network and a host on the outside; thereby, bypassing additional security measures that could be provided by the proxy server. This places the internal host at a greater risk of exploitation that could make the entire network vulnerable to an attack. A solution without a proxy server can not accept outbound traffic directly from internal systems, break the connection and filter or log the traffic, prior to passing it to the firewall for outbound delivery.

An example of a good implementation would be an HTTP proxy deployed behind the firewall; users would need to connect to this proxy en route to connecting to external web servers.

Checks

NET FW Application Proxies

- Review the firewall specification sheet. Verify the data entering or leaving the site is being proxied destined outside the enclave.

Due to technological advances there are devices such as SSL Gateways, E-mail Gateways, etc., that will proxy services to protect the enclave. Therefore, a layer 4 or stateful inspection firewall, in collaboration with application level proxy devices to service all connections identified in the PPS CAL boundaries 8, 12, 13 and 16 is an acceptable alternative.

Default Finding Details Proxies are not implemented between the enclave and external network boundaries defined in the PPS CAL for listed examples in the following boundaries:

- Boundary 8 Outbound from Enclave to DoD Network
- Boundary 12 Outbound from Enclave to Enclave DMZ
- Boundary 13 Outbound from Enclave to External
- Boundary 16 Outbound from Enclave to Enclave

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

Fixes

NET FW Application Proxies

Ensure the firewall has implemented proxies for all services that need to traverse the firewall. Utilize proxies provided by the firewall vendor.

Notes:

NET0368

V0004585 CAT II

Firewall policy is not IAW 8551.1 & Appendix C.

8500.2 IA Control: DCP-1, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAM will ensure that the firewall policy is in accordance with DoD Instruction 8551.1 and Appendix C.

Vulnerability Discussion Allowing only approved IP addresses through the perimeter router will control access to required ports and services. The perimeter will be protected IAW the guidance defined in Appendix C. In a permit any posture these must be explicitly blocked by ACLs.

Checks

NET FW 8551.1 & Appendix C

If the perimeter is in a Deny-by-Default posture, and what is allowed through the perimeter filtering is IAW DOD Instruction 8551.1 then the PPS would be covered under the Deny-by-Default rule, if permit rules are created for each approved port and protocol or all red ports were explicitly blocked. The permit rule with the port or protocol definition is required to prevent red PPS ports from traversing trusted subnets, otherwise a trusted subnet could use untrusted or red ports identified by the PPS, thus negating the blocking of ports identified in the PPS CAL.

Review the rules and filters applied to all interfaces of the firewall, both inbound and outbound directions to ensure that the firewall policy is IAW with DOD 8551.1 Ports, Protocols and Services and Appendix C.

Default Finding Details The firewall policy is not IAW DOD 8551.1 & Appendix C of the Network Infrastructure STIG.

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

Fixes

NET FW 8551.1 & Appendix C

Have the firewall administrators make the appropriate changes so that the policy is IAW DOD 8551.1 and Appendix C of the Network Infrastructure STIG.

Notes:

NET0375

V0003156 CAT II

Firewall is not configured to protect the network.

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure that the firewall is configured to protect the network against denial of service attacks such as Ping of Death, TCP SYN floods, etc.

Vulnerability Discussion A SYN-flood attack is a denial-of-service attack where the attacker send a huge amount of please-start-a-connection packets and then nothing else. This causes the device being attacked to be overloaded with the open sessions and eventually crash.

A ping sweep (also known as an ICMP sweep) is a basic network scanning technique used to determine which of a range of IP addresses map to live hosts (computers).

Checks

NET FW Protection Policies

Have the FW administrator show you the FW configuration files and rules to verify the compliance of this requirement.

CAVEAT: If the site has implemented SYN flood protection for the network using the premise router, it is not an additional requirement to implement this on the firewall.

Default Finding Details The firewall SYN-flood protection is not enabled, or the firewall does not support SYN-flood protection.

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

Fixes

NET FW Protection Policies

If the firewall support SYN-flood or ping sweep protection then enable these features. If the firewall does not support these features, enable the security features on the router to protect the network from these attacks.

Notes:

NET0377 **V0003054** **CAT II** **Firewall has unnecessary services enabled.**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The FA will ensure the firewall will not utilize any services or capabilities other than firewall software (e.g., DNS servers, e-mail client servers, ftp servers, web servers, etc.), and if these services are part of the standard firewall suite, they will be either uninstalled or disabled.

Vulnerability Discussion The additional services that the firewall has enabled increases the risk for an attack since the firewall will listen for these services. In addition, these services provide an unsecured method for an attacker to gain access to the router.

Checks

NET FW Unnecessary Services

Have the FA display the services running on the firewall appliance or underlying OS. CAVEAT: Anti-virus software running on the firewall's OS would be an exception to the above requirement. In fact, it is recommended that anti-virus software be implemented on any non-appliance firewall if supported. However, it is not a finding if anti-virus software has not been implemented.

Default Finding Details Firewall has unnecessary services enabled.

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

Fixes

NET FW Unnecessary Services

The Firewall Administrator will only utilize services related to the operation of the firewall and even if they are part of the firewall standard suite, they will be uninstalled or disabled.

Notes:

NET0378 **V0004592** **CAT II** **Firewall version is not a supported or current.**

8500.2 IA Control: ECSC-1, VIVM-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The FA will use a supported version of the firewall software with all security-related patches applied.

Vulnerability Discussion Unsupported versions will lack security enhancements as well as support provided by the vendors to address vulnerabilities.

Checks

NET FW Patch Mgt

Verify firewall release and maintenance level and research the vendors vulnerability list and upgrade database.

Default Finding Details The firewall is not utilizing the most current supported version of firewall software with all security related patches.

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

Fixes

NET FW Patch Mgt

The firewall administrator will install all version updates and security patches in a timely manner.

Notes:

NET0379 **V0004619** **CAT II** **Firewall is not operating on a STIG'd OS**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The FA will ensure that if the firewall product operates on an OS platform, the host must be STIG compliant prior to the installation of the firewall product.

Vulnerability Discussion If the host that a firewall engine is operating on is not secured, the firewall itself is exposed to greater risk.

Checks

NET FW STIG OS platform

Review documentation that the OS was STIG compliant prior to firewall installation and that the appropriate patches have been applied that address all IAVAs.

Default Finding Details Firewall is not operating on an OS platform that was STIG compliant.

The OS does not have all IAVA related patches applied.

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

Fixes

NET FW STIG OS Platform

The firewall administrator will install all patches that address IAVA.

Notes:

NET0380 **V0014644** **CAT II** **Firewall must block loopback address**

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure the firewall shall reject requests for access or services where the source address received by the firewall specifies a loopback address.

Vulnerability Discussion The loopback address is used by an Inter-Processor Control (IPC) mechanism that enables the client and server portion an application running on the same machine to communicate, and so it is trusted. It should never be used as the source IP address of an inbound or outbound transmission.

Checks

NET FW Loopback Addr

Ensure any attempt from the firewall or any network to pass any packets claiming to be from a loopback address is blocked.

Default Finding Details Firewall is not blocking loopback address.

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

Fixes

NET FW Loopback Addr

Establish filters to block any attempt from the firewall or any network to pass any packets claiming to be from a loopback address.

Notes:

NET0381 V0014645 CAT II Firewall must reject SMTP RCPT

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO will ensure the firewall shall reject traffic that contains source routing symbols (e.g., in the mailer RCPT commands).

Vulnerability Discussion Use of the relay function through arbitrary sites has been used as part of hostile efforts to hide the actual origins of mail.

Checks

NET FW SMTP RCPT

Have the FA identify how source routing symbols such as RCPT are blocked or disabled on the firewall.

Default Finding Details The firewall does not reject SMTP source routing symbols, such as RCPT commands..

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

Fixes

NET FW SMTP RCPT

Have the FA blocked or disabled source routing symbols such as RCPT on the firewall.

Notes:

NET0386 V0014646 CAT III FW must alarm at 75% log capacity

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The firewall will immediately alert the administrators by displaying a message at the local console, the remote administrative console, generate an audible alarm, and page or send an electronic message if the audit trail exceeds 75 % percentage or more of storage capacity.

Vulnerability Discussion By configuring the firewall to provide a message to the local console regardless of whether an administrator is logged in by sending alerts due to modification or exceeding capacity of audit logs ensures administrative staff is aware of critical alerts.

Checks

NET firewall full

Have the FA identify how the firewall is configured for this notification. The message should be displayed at the remote console if an administrator is already logged in, or when an administrator logs in. The firewall should be capable to generate the alarm and notification as described.

Default Finding Details Firewalls are not configured to alarm when the log reaches 75% full.

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

Fixes

NET firewall full

Have the FA configure the firewall to meet the requirement.

Notes:

NET0388

V0014647 CAT III

No FW log dump procedures

8500.2 IA Control: ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The FA will have a procedure in place to dump logs when they reach 75% capacity to a syslog server.

Vulnerability Having a procedure tested and verified will prevent the logs from filling when they reach 75% capacity.

Discussion

Checks

NET FW Log Dump

Have the FA identify how the firewall logs are managed during critical events.

Default Finding The firewall SA does not have a procedure in place to dump logs when they reach 75% capacity to a syslog server.

Details

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

Fixes

NET FW Log Dumps

Have the FA establish procedures for dumping the logs.

Notes:

NET0390

V0003176 CAT II

The firewall is not configured to alarm the admin

8500.2 IA Control: ECAT-2, ECSC-1

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IA/NSO will ensure the firewall is configured to alert the administrator of a potential attack or system failure.

Vulnerability The firewall is the first device that is under the sites control that has the possibility to alarm the local staff of an ongoing attack. The

Discussion firewall alarms are the first indication of an attack or system failure.

Checks

NET FW Alerts

The firewall shall immediately display an alarm message, identifying the potential security. Review the firewall configuration to determine what alerts have been defined and how the notifications are performed.

Default Finding The firewall is not configured to alarm the FA of a potential attack or system failure.

Details

The firewall does not support notification alarms.

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

Fixes

NET FW Alerts

Configure the firewall to alarm the FA of potential attacks or system failure.

Notes:

NET0391 **V0014648** **CAT II** **FW alert not written to console.**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the firewall provides critical alert message levels 0, 1, and 2 to the local console regardless of whether an administrator is logged in.

Vulnerability Discussion By immediately displaying an alarm message, identifying the potential security violation and making it accessible with the audit record contents associated with the auditable event(s) that generated the alarm provides the administration staff prompt alert messages 7 x 24 at a local console, regardless of if they are logged on.

Checks

NET FW alert written to consol

Review the firewall configuration to determine what alerts have been defined and how the notifications are performed.

Default Finding Details Firewall alerts are not written to the console, identifying the potential security violation and making it accessible with the audit record contents associated with the auditable event(s) that generated the alarm provides the administration staff prompt alert messages 7 x 24 at a local console, regardless of if they are logged on.

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

Fixes

NET FW alert written to consol

Configure the firewall to immediately write an alarm message to the local console.

Notes:

NET0392 **V0014649** **CAT II** **FW alert not written to remote console.**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure the message is displayed at the remote console if an administrator is already logged in, or when an administrator logs in if the alarm message has not been acknowledged

Vulnerability Discussion By immediately displaying an alarm message, identifying the potential security violation and making it accessible with the audit record contents associated with the auditable event(s) that generated the alarm provides the administration staff prompt alert messages at their work areas.

Checks

NET FW alert written to remote

Review the firewall configuration to determine what alerts have been defined and how the notifications are performed. The message must be displayed at the remote console if an administrator is already logged in, or when an administrator logs in if the alarm message has not been acknowledged. The firewall shall immediately display an alarm message, identifying the potential security violation and make accessible the audit record contents associated with the auditable event(s) that generated the alarm.

Default Finding Details Firewall alerts not written to remote consoles.

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

Fixes

NET FW alert written to remote

Configure the firewall to immediately write an alarm message to the remote consoles.

Notes:

NET0395

V0014653 CAT III

Audit record must display violation

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IA0/NSO will ensure the alarm message identifying the potential security violation makes accessible the audit record contents associated with the auditable event(s) until it has been acknowledged.

Vulnerability Discussion The relevant audit information must be available to administrators. The firewall shall immediately display an alarm message, identifying the potential security violation and make accessible the audit record contents associated with the auditable event(s) that generated the alarm.

Checks

NET FW violation msg

Review the firewall configuration to determine what alerts have been defined and how the notifications are performed. The relevant audit information must be available to administrators. The message will not be scrolled off the screen due to other activities taking place (e.g., the Audit Administrator is running an audit report).

Default Finding Details The alarm message identifying the potential security violation does not make accessible the audit record contents associated with the auditable event(s) until it has been acknowledged.

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

Fixes

NET FW violation msg

Configure the firewall to write violations to the console and make accessible the audit record contents.

Notes:

NET0396

V0014655 CAT III

Alarm must sound until acknowledged.

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IA0/NSO will ensure an audible alarm will sound until acknowledged by an administrator.

Vulnerability Discussion Critical alerts levels 0, 1 and 2 require immediate response. An audible alarm will sound until acknowledged by an administrator. The requirements are necessary to ensure an administrator will be aware of the alarm. The intent is to ensure that if an administrator is physically at the console or remote workstation the message will remain displayed until they have acknowledged it.

Checks

NET FW Alarms

Review the firewall configuration to determine what alerts have been defined and how the notifications are performed. Verify alerts levels 0, 1 and 2 generate the alarm.

Default Finding Details Critical alerts levels 0, 1 and 2 require immediate response. An audible alarm does not sound until acknowledged by an administrator.

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

Fixes

NET FW Alarms

Configure the firewall to send an audible alarm until acknowledged.

Notes:

NET0398 **V0014656** **CAT III** **FW acknowledge messages must be recorded**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure an acknowledgement message identifying a reference to the potential security violation is logged and it contains a notice that it has been acknowledged, the time of the acknowledgement and the user identifier that acknowledged the alarm, at the local console, and remote administrator sessions that received the alarm.

Vulnerability Discussion Acknowledging the message and audible alarm could be a single event, or different events. In addition, assurance is required that each administrator that received the alarm message also receives the acknowledgement message, which includes some form of reference to the alarm message, who acknowledged the message and when.

Checks

NET FW Msg Acknowledged

The firewall shall display an acknowledgement message identifying a reference to the potential security violation, a notice that it has been acknowledged, the time of the acknowledgement and the user identifier that acknowledged the alarm at the local console and remote administrator sessions that received the alarm. Have the administrator verify these capabilities.

Default Finding Firewall acknowledge messages are not recorded.
Details

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

Fixes

NET FW Msg Acknowledged

Configure the firewall to send acknowledge messages to administrators, referencing the alarm, who acknowledged the alarm, and timestamps.

Notes:

NET1300 **V0003178** **CAT III** **Firewall Admins will be logged.**

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

References: NETWORK INFRASTRUCTURE SECURITY TECHNICAL
IMPLEMENTATION GUIDE

Vulnerability The IAO/NSO will ensure administrator logons, changes to the administrator group, and account lockouts are logged.

Vulnerability Discussion The firewall and the associated logging functions allows for forensic investigations if properly configured and protected. The administrators account is the most sought after account so extra protection must be taken to protect this account and log its activity.

Checks

NET FW Admin Logged

Have the FA display the logging configuration. Review log data created by firewall and identify if these features are being logged, such as log on.

Default Finding The firewall does not log unsuccessful authentication attempts.
Details The firewall fails to log the administrator logons, changes to the administrator group, and account lockouts.

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

Fixes

NET FW Admin Logged

Have the FA make the necessary configuration changes and verify the corrections work by re-reviewing the firewall log.

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 IAO/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:

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: