

DEPARTMENT OF THE ARMY
 HEADQUARTERS, UNITED STATES ARMY MATERIEL COMMAND
 5001 EISENHOWER AVE, ALEXANDRIA, VA 22333-0001

AMC MEMORANDUM
 NO. 380-12

15 August 2002

Information Assurance

U.S. Army Materiel Command (AMC) Policy on Firewalls and
 Firewall Configuration

	Paragraph	Page
Purpose	1	1
Scope	2	1
Responsibilities	3	1
Policy	4	1
Exceptions to Policy	5	4
Point of Contact	6	4
References	7	4

1. Purpose: To provide policy for the use, administration, and configuration of network-based, host-based, and desktop/personal firewalls.

2. Scope: This policy is effective immediately and applies to all unclassified networks within Headquarters AMC, its Major Subordinate Commands (MSCs), and Separate Reporting Activities.

3. Responsibilities:

a. The AMC Information Assurance Program Manager, MSC Information Assurance Managers (IAMs), and Information Assurance Security Officers (IASOs) will ensure the execution of this policy and guidance within their respective activities.

b. System Administrators (SA) and Network Managers (NM) will ensure the proper technical implementation of this policy on systems and networks for which they are responsible.

4. Policy:

In addition to the requirements outlined in Reference 7.b. below, all AMC organizations will comply with the following:

a. Architecture:

(1) All packets/data flowing out of and into a protected area (i.e., installation, enclave, or local area network) must pass through a firewall. The need for a firewall between trusted networks on a single installation/location will be addressed in the Installation/Unit Network Security Policy.

(2) No modem or other network device will be configured to bypass local network firewall configuration. This does not prohibit the use of Virtual Private Networks (VPNs).

(3) To maximize limited resources, firewall(s) will be implemented according to the following prioritized list:

(a) Where there is a connection to an external network.

(b) Where there are remote users accessing the network.

(c) Between enclaves where sensitive information is being processed.

(d) Between enclaves that have a direct Non-Classified Internet Protocol Router Network (NIPRNet) connection that bypasses the installation backbone.

b. Administration:

(1) On a daily basis or when log files become three-quarters full, the firewall administrator or designated alternate will move firewall logs to a separate system for review, analysis, and archiving. Secure Shell (SSH) or VPN connections will be used when transferring firewall logs from the firewall to the review/analysis/archive system. Alternatively, a firewall administrative workstation may be used to collect and analyze firewall logs. The firewall administrator will ensure the system clocks on the firewall and the firewall workstation are synchronized.

(2) The firewall administrator or designated alternate is responsible for backing up firewall logs. Firewall logs should be backed up on a network drive or

removable media (i.e., tape, CD-ROM) and kept for a period of not less than one (1) month.

(3) In accordance with Reference 7.a, firewall(s) and firewall logs will be regularly audited and monitored by the firewall administrator, IASO, or other properly trained SA to detect intrusions or computer security incidents. These logs will be used in conjunction with Intrusion Detection Systems (IDS) Logs for determining the nature of computer security incidents that require reporting via established procedures.

(4) All remote administration of the firewall will be encrypted (SSH v2 or later, VPN, HTTPS, etc). Under no circumstances will unencrypted sessions be used to administer the firewall on the public/untrusted/external interface. The firewall will be configured to use an alternate SSH port and will not use the default port (22) for remote administration. The firewall will be configured to only allow connections from authorized hosts (both internal and external) for remote administration purposes.

c. Configuration:

(1) All firewall(s) will have all TCP/IP ports closed (including those that provide connectivity for high bandwidth utilizing services such as audio/video streaming, peer-to-peer file sharing applications, and internet chat programs) except when specifically authorized in the Installation/Unit Network Security Policy and identified as mission essential.

(2) All incoming network management protocols including simple network management protocol (SNMP), network basic input output system (NetBIOS), and routing protocols (i.e., Routing Information Protocol (RIP), Open Shortest Path First (OSPF), etc.) will be denied except from authorized hosts.

d. Desktop/Personal Firewalls:

Desktop/personal firewalls are not mandatory, but may be used as part of a comprehensive "defense in depth" strategy. They may be used in situations where an additional layer of protection is needed for sensitive information. Desktop/personal firewalls may be either hardware or software based and should be centrally managed and/or controlled.

(1) Desktop/personal firewalls will be configured so they cannot be changed, disabled, managed, or uninstalled by the user and will be transparent to the user.

(2) Desktop/personal firewalls will be configured in a manner that does not prevent official security scans and network management or hide prohibited activity.

5. Exceptions to Policy:

Exceptions to this policy can only be approved by the local DAA. An appropriate Risk Management Review will be performed on the system or condition requiring an exemption. Copies of requests for exception, the Risk Management Review, and the approval/disapproval will be provided to HQ, AMC, ATTN: IAPM via e-mail: amcio-iapm@hqamc.army.mil.

6. Point of Contact:

The AMC Point of Contact for this memorandum is the Information Assurance Program Manager (AMCIO-A), Commercial: (703) 617-3462 or DSN: 767-3462, e-mail: amcio-a@hqamc.army.mil.

7. References:

a. Army Regulation 380-19, Information Systems Security, 27 February 1998.

b. HQDA Message 301200ZApr99, Department of the Army Firewall Policy

c. Army Information Assurance Message, Network Security Demilitarized Zone (DMZ), 2 November 1999

d. Army Materiel Command Supplement 1 to AR 380-19, Information Assurance, 1 December 2000

e. Office of the Assistant Secretary of Defense C4I, Memorandum dated 9 March 2002, Subject: Anti-Virus Enterprise Contract

f. Army Regulation 25-1, Army Information Management, 31 May 2002.

The proponent of this memorandum is the United States Army Materiel Command. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the Commander, HQ AMC, ATTN: AMCIO-A, 5001 Eisenhower Avenue, Alexandria, VA 22333-0001.

FOR THE COMMANDER:

OFFICIAL:

RICHARD A. HACK
Major General, USA
Chief of Staff

DENNIS A. DAVIS
Chief, Business Management
Division

DISTRIBUTION:

MSCs

ATTN: DOIMs, CIOs, AMC-IA-MSC, and AMC-IA-INST