

6 June 2001

Information Management
U.S. Army Training and Doctrine Command (TRADOC)
Firewall Configuration

Summary. This regulation establishes policies, procedures, and responsibilities for implementing firewalls to increase the information systems security posture within TRADOC.

Applicability. This regulation is applicable to all TRADOC installations, activities and HQ TRADOC staff who operate a firewall(s) or have information systems with special requirements to operate through a firewall.

Forms. The “R” form at the back of this regulation is for local reproduction.

Suggested Improvements. The proponent of this regulation is the Deputy Chief of Staff for Information Management (DCSIM). Send comments and suggested improvements on DA Form 2028

(Recommended Changes to Publications and Blank Forms) through channels to Commander, TRADOC, 90 Ingalls Road, ATTN: ATIM-I, Fort Monroe, VA 23651-1065.

Distribution Restriction. Appendix C (separate cover) of this publication contains technical or operational information that is FOR OFFICIAL USE ONLY. Distribution is limited to U.S. Government agencies. Requests from outside agencies for the release of Appendix C under the Freedom of Information Act or the Foreign Military Sales Program must be made to the Commander TRADOC, ATTN: ATIM-I, Fort Monroe, VA 23651-1065.

Availability. This publication is available on the TRADOC Homepage at <http://www.tradoc.army.mil/>

Contents

	Paragraph	Page		Paragraph	Page
Chapter 1			Chapter 3		
Introduction			Policy and Procedures		
Purpose	1-1	2	General	3-1	3
References	1-2	2	Objectives	3-2	3
Explanation of abbreviations and terms ..	1-3	2	Protocols	3-3	3
Chapter 2			Configuration and security	3-4	4
Responsibilities			Internal controls	3-5	5
Deputy Chief of Staff for Information			Appendixes		
Management (DCSIM)	2-1	2	A. References		6
Installation commanders	2-1	2	B. Anti-Spoofing Techniques		6
Installation tenant organizations	2-3	2	C. Firewall Configuration - Ports and		
Designated Approval Authority	2-4	2	Protocols (FOUO)(Access Controlled to		
Installation Information			Authorized Personnel Only)		10
Assurance Managers	2-5	2	Glossary		
Information Assurance Security					10
Officers (IASO)	2-6	2			
Installation Firewall Configuration					
Control Board	2-7	3			
Firewall administrators	2-8	3			

Chapter 1 Introduction

1-1. Purpose. This regulation defines policies, procedures, and responsibilities for firewalls operated by TRADOC organizations. It specifically addresses operational objectives, TRADOC and installation-level firewall configuration policies, administration, and security of firewalls.

1-2. References. Appendix A contains a listing of required publications.

1-3. Explanation of abbreviations and terms. Abbreviations and terms used in this regulation are explained in the glossary.

Chapter 2 Responsibilities

2-1. Deputy Chief of Staff for Information Management (DCSIM). The DCSIM will:

a. Develop and maintain the TRADOC firewall configuration policy.

b. Establish and chair a TRADOC Firewall Configuration Control Board (CCB) to review and update the TRADOC firewall configuration policy.

c. Coordinate with external agencies regarding the operation of new systems and applications in accordance with (IAW) the TRADOC firewall configuration policy.

d. Ensure installations receive firewall generic accreditation/certification IAW DOD Instruction (DoDI) 5200.40 and AR 380-19.

2-2. Installation commanders will:

a. Appoint a Designated Approving Authority (DAA) for each local network, to include any firewall(s) protecting it.

b. Ensure appropriate installation firewall security policies are established.

c. Identify critical network assets and include in the installation information assurance policy.

d. Prepare budget and funding requests to support the firewall and other Command and Control Protect (C2P) requirements.

e. Establish an installation firewall CCB to:

(1) Review the installations firewall configuration policy biannually.

(2) Update installations firewall configuration policy.

(3) Propose changes to the TRADOC firewall configuration policy, as required.

f. Assign an installation representative to the TRADOC firewall CCB.

g. Ensure properly trained firewall administrators and assistants are appointed for all locally and tenant organization operated firewalls.

2-3. Installation tenant organizations will:

a. Submit TRADOC Form 25-74-1-R-E, Firewall Configuration Systems Summary, to the installation firewall CCB for each system that requires access through the firewalls.

b. Coordinate unique security requirements with the installation Information Assurance Manager (IAM) and the assigned network local DAA.

2-4. Designated Approval Authority will:

a. Ensure assigned firewalls are operationally accredited IAW DoDI 5200.40 and AR 380-19.

b. Review and approve the installation firewall security policy. The DAA appointed for an installations campus area network (CAN) backbone will ensure integration of the installations firewall policies.

c. Ensure firewall security policies are enforced.

2-5. Installation Information Assurance Managers will:

a. Ensure installation firewall policy accurately describes the intended firewall functionality and installation-operated firewalls are installed IAW that policy.

b. Ensure the certification and accreditation documents are developed and maintained for installation firewalls.

c. Serve as a member of the installation firewall CCB.

d. Ensure firewall security awareness training is incorporated into installation information system security training, to ensure system users do not compromise the firewall security features.

2-6. Information Assurance Security Officers (IASO). For firewalls operated by organizations within their assigned responsibilities, IASOs will:

a. Ensure the firewall is operated and maintained according to the vendors specifications and organizational requirements.

b. Ensure the firewall audit log is reviewed daily.

c. Report any security incidents involving the firewall to the IAM, as required by the organizational security regulations and AR 380-19.

d. Ensure the firewall security policy is properly implemented.

e. Continuously evaluate the firewall security environment; make recommendations for improvement to the IAM/DAA as appropriate.

2-7. Installation Firewall Configuration Control Board will:

a. Act as the technical advisory group to the DAA on the firewall configuration under the DAAs jurisdiction.

b. Make recommendations to the DAA on any exceptions to the installation firewall configuration policy.

2-8. Firewall administrators. For their assigned systems, firewall administrators will:

a. Ensure the operating system for the firewall is configured properly and the security features are properly set according to the security policy.

b. Understand and monitor the configuration of the firewall IAW Army, TRADOC and installation policies.

c. In coordination with the IASO, ensure adequate physical and administrative security is maintained over the firewall.

d. Make frequent backups of data and files on the firewall and ensure firewall software integrity is maintained.

e. Respond to any alarms or alerts from the firewall software IAW Army, TRADOC and installation policies.

f. Install current software upgrades, modifications and corrective patches to the firewall software IAW Army, TRADOC and installation policies. Periodically check with the firewall manufacturer on firewall security problems and apply patches in order to maintain firewall security.

g. Review the firewall audit logs on a daily basis.

h. Report any attacks or incidents on the firewall to the firewall IASO/IAM/Regional Computer Emergency Response Team-CONUS (RCERT-C).

i. Maintain minimum educational requirements as prescribed by the specific firewall selected and DA/TRADOC guidance.

j. Use approved Information Assurance Protect Tools to periodically review effectiveness of firewall security.

Chapter 3 Policy and Procedures

3-1. General. Firewalls will be used to protect data and information systems from unauthorized interference by any enclave, local area network, organization, installation or user that does not have a need to access the protected information. They create security checkpoints at the boundaries of private networks protecting access to/from a trusted network from a distrusted network. Firewalls minimize the risk posed to a network when used in conjunction with other network security devices and practices (e.g., Intrusion Detection Systems (IDS), complementing firewalls, Virtual Private Networks (VPNs)).

3-2. Objectives. TRADOC firewall policy is guided by two fundamental objectives:

- The firewall will ensure no traffic is admitted onto the protected network(s) unless it is expressly permitted.
- The firewall must be installed to ensure all traffic between the protected network(s) and the outside must pass through the firewall.

A weaker alternative to the first objective would be to permit any traffic that is not denied. This is not acceptable for TRADOC firewalls. The second objective is essential for security. Even one modem behind the firewall creates a potential backdoor to the protected network.

3-3. Protocols and Ports.

a. Protocols and Ports (P/P) are placed into three categories: Restricted, Prohibited, and Allowed.

(1) Restricted protocols and their corresponding ports are authorized for passing traffic through the firewall with some conditional restrictions such as outbound, inbound, IP restricted, etc.

(2) Prohibited protocols and their corresponding ports are denied the ability to pass through the firewall, primarily because of security issues.

(3) Allowed protocols and their corresponding ports are authorized for passing traffic through the firewall, if required. Allowed P/P that are not used by the installation will be blocked.

b. The TRADOC CCB is responsible for maintaining the list of prohibited P/P and restricted P/P for implementation across TRADOC.

c. Installation CCBs are responsible for determining the use of allowable and restricted P/P for their installation based on the TRADOC CCB guidance.

d. Waivers to the TRADOC Prohibited P/P must be submitted to the TRADOC Firewall CCB for approval through the TRADOC DCSIM, E-mail: atimi@monroe.army.mil, SUBJECT: Firewall CCB - Restricted Request, and include a completed TRADOC Form 25-74-1-R-E.

e. The DCSIM will maintain a current lists of restricted and prohibited and recommended allowable protocols at: <http://www-monroe.monroe.army.mil/isspmanager/intro.asp> (access controlled by local IAMs); and [https://workplace.us.army.mil/DiscussionArea:FIREWALLS](https://workplace.us.army.mil/DiscussionArea/FIREWALLS) (access controlled by TRADOC Information Assurance Program Manager (IAPM)).

3-4. Configuration and security.

a. General.

(1) To ensure network compatibility and interoperability, Directorate of Information Management (DOIM)/Chief Information Office (CIO) will coordinate with the Continental United States Theater Network Operations and Security Center (CONUS-TNOSC) and RCERT-C before installing any firewall. Access to the installations internal network for incident investigation or network restoration will be coordinated with CONUS-TNOSC and RCERT-C.

(2) Firewalls will be configured with as few services as possible. The installation DOIM/CIO will ensure that the firewall architecture supports the security objectives of TRADOC and the Army.

(3) An IDS will be used in conjunction with firewalls. The objective architecture includes an IDS placed behind a firewall on the protected network to focus the IDS on monitoring the services that are permitted to flow through the firewall. However, until the objective architecture is resourced, the CONUS-TNOSC monitored IDS located in the top-level architecture meets this requirement.

(4) To the maximum extent of their available capabilities, firewalls will:

(a) Pass encrypted information.

(b) Detect, prohibit, and report a hackers attempt to do port scanning.

(c) Detect, prohibit, and report use of the "SATAN" tool.

(d) Report or log all violations of this policy. The threshold for reporting or logging incidents or policy violations is event dependent. Report major violations immediately, a threshold of three events

within a reasonable time period may be set for random access events (e.g., attempted probes of a prohibited port from a specific source IP address to a wide range of IP addresses on the protected network).

(e) Provide proxy Wide Area Network (Internet) services to the extent the firewall is capable.

(f) Disable source routing.

(g) Incorporate anti-spoofing techniques (see app B).

(h) Notify locally identified personnel immediately of any firewall security alarm by the fastest means possible, so that an immediate response may be made to the firewall alarm.

(i) Have all default/factory passwords removed from the firewall.

b. Physical security.

(1) Firewall hardware will be located in a controlled environment (referred to as a "firewall enclosure" for the remainder of this regulation) with unescorted access restricted to essential personnel.

(2) Anyone entering a firewall enclosure without unescorted access privileges will sign a visitors log before entering and upon leaving the firewall enclosure.

(3) A firewall enclosure will be equipped with heat, air conditioning, and smoke alarms to ensure a proper operating environment for electronic equipment.

(4) Firewalls will be protected at all times against unauthorized hardware or software modifications.

c. Firewall administrative security.

(1) The firewall administrator and alternate will be trained in its administration, operation, and maintenance.

(2) The firewall administrators and their alternates must have completed background investigations as specified in AR 380-67 prior to assuming the duties of firewall administrator or alternate.

(3) Firewalls will be accredited IAW DoDI 5200.40 and AR 380-19 after installation. Re-accreditation will be IAW paragraph 3-6 of AR 380-19.

(4) Systems that are to be protected by firewalls will be explicitly identified to the installation firewall CCB.

d. Firewall configuration and management.

(1) Firewalls must be located and configured so they

(a) Can monitor and control all communications between the protected network and the systems on the outside of the firewall.

(b) Can withstand deliberate denial-of-service attacks such as “SYN” flooding and “ping of death” attacks.

(c) Cannot be bypassed or circumvented.

(d) Will not allow any outside traffic onto the protected network unless expressly permitted by the installation CCB.

(2) Management procedures.

(a) The TRADOC and installation CCBs must review requests for remote network management access through TRADOC-operated firewalls. The TRADOC CCB must review any plan for remote management through installation gateway firewalls. Final authority to allow remote management access into a campus area network (CAN) is the DAA appointed for the CAN. The installation CCB for that CAN will recommend a position to the DAA. TRADOC DCSIM will coordinate issues with external system developers and proponents.

(b) Establish procedures to allow CONUS-TNOSC and RCERT-C access to firewalls in support of network restoration and incident investigation, on an as-needed basis.

(c) Do not store any compilers, editors, communications software, user applications, or any other files on the firewall other than those directly related to the functioning of the firewall. A host-based IDS is permitted as an exception.

(d) Firewalls will be incorporated into the installations Information System Security Continuity of Operations Plan.

(e) Comply with Army procedures for the Information Assurance Vulnerability Alert (IAVA) process.

(f) Unauthorized access, events, incidents, or attacks will be reported IAW AR 380-19.

(3) Firewalls should:

(a) Require strong authentication before permitting a process to pass through to the protected network.

(b) Support VPNs.

(c) Utilize Network Address Translation so outbound network traffic appears to have originated

from the firewall. Justifiable systems that require static routable IP addresses are permitted with the approval of the installation CCB.

(d) After a failure, default to a configuration that denies all services, and requires the firewall administrator to re-enable services afterward.

(e) Have an uninterruptible power supply (UPS). The UPS should have sufficient capacity to facilitate proper shutdown of a firewall.

3-5. Internal controls.

a. Direct login to firewalls will be from the firewall keyboard and specified IP addresses inside the protected network only (i.e., firewall administrator and alternate); no indirect “in-band” logins will be permitted. Direct login privilege will be restricted to the firewall administrator, the IASO/IAM, and their alternates.

b. Firewall administrative personnel will develop local procedures to respond to various levels of security alerts and incidents. These procedures may include pager notification, automatic re-configuration, coordination with the CONUS-TNOSC/RCERT-C, etc.

c. Firewall integrity checks will be performed and documented on a routine basis. The local DOIM/CIO or an outside agency may perform the integrity check. At a minimum, firewall integrity checks will include:

(1) A port scan against the firewall from all segments connected to the firewall (quarterly).

(2) Review of all files that may have been modified, replaced, or deleted (weekly).

d. A firewalls system integrity and configuration management databases will be updated each time the firewalls configuration is modified. These files will be stored on read-only media or on off-line storage media.

e. Maintain backups of all relevant configuration data and files. At least one copy of the backup configuration data will be stored in a separate secure location.

f. The firewall audit trail and event logs shall be:

(1) Maintained in files accessible only by the firewall administrator, the IASO, or their alternates.

(2) Reviewed by the firewall administrator, the IASO, or their alternates on a daily basis.

(3) Maintained on file located separate from the firewall for a period determined by the local DAA and stated in the local firewall policy.

Appendix A References

Section I Required Publications

DoDI 5200.40
DoD Information Technology Security Certification
and Accreditation Process (DITSCAP)

AR 380-19
Information Systems Security

AR 380-67
The Department of the Army Personnel Security
Program

Section II Related Publication

Network Infrastructure Security Technical
Implementation Guide (STIG), V2r3, 22 Nov 99.
(Document can be found at: [https://iase.disa.mil/
techguid/stigs.html](https://iase.disa.mil/techguid/stigs.html) NOTE: Requires DoD Public
Key Infrastructure certificate to access.)

Section III Prescribed Form

TRADOC Form 25-74-1-R-E
Firewall Configuration Systems Summary (cited in
para 2-3a)

Appendix B Anti-Spoofing Techniques

B-1. General. See table B-1 for general anti-spoofing information.

**Table B-1
General**

DIRECTION	SOURCE ADDRESS	DEST. ADDRESS	PROTOCOL	SOURCE PORT	DEST. PORT	ACK SET	NOTES
In	Internal	Any	Any	Any	Any	Any	Deny
In	Any	255.255. 255.255	Any	Any	Any	Any	Deny
In	Any	0.0.0.0	Any	Any	Any	Any	Deny
In	Known trouble-Maker	Any	Any	Any	Any	Any	Deny/log
In	Any	Any	User Datagram Protocol (UDP)/Transmission Control Protocol (TCP)	Any	Problem Service	Any	Deny for unneeded services only (e.g., link, Trivial File Transfer Protocol)
Out	Not Internal	Any	UDP/TCP	Any	Any	Any	Deny

B-2. Outgoing File Transfer Protocol (FTP). Table B-2 contains guidelines for outgoing FTP, passive and normal.

Table B-2 - Passive and normal FTP

DIRECTION	SOURCE ADDRESS	DEST. ADDRESS	PROTOCOL	SOURCE PORT	DEST. PORT	ACK SET	NOTES
In	External	Internal	TCP	Any	2000	Any	Deny -- Open Windows attack on passive FTP
In	External	Internal	TCP	Any	6000-6xxx	Any	Deny --X11 attack on passive FTP
Out	Internal	External	TCP	>1023	21	Any	Outgoing Normal FTP request
In	External	Internal	TCP	21	>1023	Yes	Response to outgoing request
In	External	Internal	TCP	20	>1023	Any	Data channel creation for normal mode
Out	Internal	External	TCP	>1023	20	Yes	Data channel creation response, outgoing, normal mode
Out	Internal	External	TCP	>1023	>1023	Any	Data channel creation for outgoing FTP requests, passive mode
In	External	Internal	TCP	>1023	>1023	Yes	Data channel response for outgoing FTP request, passive mode

NOTE: Standard FTP uses ports above 1023 for its data connections; therefore, for standard FTP operation, ports above 1023 must all be open.

B-3. Outgoing TELNET. Procedures for outgoing TELNET are contained in table B-3.

Table B-3 - TELNET

DIRECTION	SOURCE ADDRESS	DEST. ADDRESS	PROTOCOL	SOURCE PORT	DEST. PORT	ACK SET	NOTES
Out	Internal	External	TCP	>1023	23	Any	Outgoing Telnet
In	External	Internal	TCP	23	>1023	Yes	Response to Telnet

B-4. Simple Mail Transfer Protocol (SMTP).

See table B-4 for incoming and outgoing mail (SMTP) anti-spoofing information.

Table B-4 - SMTP

DIRECTION	SOURCE ADDRESS	DEST. ADDRESS	PROTOCOL	SOURCE PORT	DEST. PORT	ACK SET	NOTES
Out	Internal	External	TCP	>1023	25	Any	Outgoing mail connection
In	External	Internal	TCP	25	>1023	Yes	Response to outgoing connection
In	External	Internal	TCP	>1023	25	Any	Incoming mail connection
Out	Internal	External	TCP	25	>1023	Yes	Response to incoming mail connection

NOTE: Access to TCP port 25 should be restricted to mail servers to the maximum extent possible.

B-5. Incoming and outgoing World Wide Web (WWW). Anti-spoofing techniques used with Hyper Text Transfer Protocol (HTTP) are found in table B-5.

Table B-5 - WWW (HTTP)

DIRECTION	SOURCE ADDRESS	DEST. ADDRESS	PROTOCOL	SOURCE PORT	DEST. PORT	ACK SET	NOTES
In	External	Internal	TCP	>1023	80	Any	Incoming web
Out	Internal	External	TCP	80	>1023	Yes	Response to incoming web
Out	Internal	External	TCP	>1023	80	Any	Outgoing web
In	External	Internal	TCP	80	>1023	Yes	Response to outgoing web

NOTE: Access to TCP port 80 should be restricted to WWW servers to the maximum extent possible.

B-6. Secure WWW. See table B-6 for incoming and outgoing secure WWW (Hyper Text Transfer Protocol Secure (HTTPS)) techniques.

Table B-6 - Secure WWW

DIRECTION	SOURCE ADDRESS	DEST. ADDRESS	PROTOCOL	SOURCE PORT	DEST. PORT	ACK SET	NOTES
In	External	Internal	TCP	>1023	443	Any	Incoming secure web
Out	Internal	External	TCP	443	>1023	Yes	Response to incoming web
Out	Internal	External	TCP	>1023	443	Any	Outgoing secure web request
In	External	Internal	TCP	443	>1023	Yes	Response to outgoing request

NOTE: Access to TCP port 443 should be restricted to secure WWW servers to the maximum extent possible.

B-7. Incoming and outgoing domain name service (UDP and TCP). Anti-spoofing techniques for UDP and TCP are in table B-7.

Table B-7 - UDP and TCP

DIRECTION	SOURCE ADDRESS	DEST. ADDRESS	PROTOCOL	SOURCE PORT	DEST. PORT	ACK SET	NOTES
In	External	Internal	UDP	>1023	53	N/A	Incoming UDP DNS query
Out	Internal	External	UDP	53	>1023	Yes	Response to incoming query
Out	Internal	External	UDP	>1023	53	N/A	Outgoing UDP DNS query
In	External	Internal	UDP	53	>1023	Yes	Response to outgoing request
In	External	Internal	TCP	>1023	53	N/A	Request for DNS zone transfer
Out	Internal	External	TCP	53	>1023	Yes	DNS zone transfer
Out	Internal	External	TCP	>1023	53	N/A	Request for DNS zone transfer
In	External	Internal	TCP	53	>1023	Yes	DNS zone transfer

NOTE: Access to TCP port 53 should be restricted to known secondary domain name servers to the maximum extent possible. This helps prevent intruders from gaining knowledge about the local network.

Appendix C Firewall Configuration - Ports and Protocols

The current lists of TRADOC restricted and prohibited Ports and Protocols are For Official Use Only (FOUO) (password required).

Authorized users can find the documents at:
<http://www-monroe.monroe.army.mil/isspmanager/intro.asp> (access controlled by local IAMs), and [https://workplace.us.army.mil/Discussion Area: FIREWALLS](https://workplace.us.army.mil/DiscussionArea:FIREWALLS) (access controlled by TRADOC Information Assurance Program Manager (IAPM)).

Glossary

Section I Abbreviations

C2P	Command and Control Protect
CAN	campus area network
CONUS- TNOSC	Continental United States Theater Network Operations and Security Center
CCB	Configuration Control Board
CIO	Chief Information Office
DAA	Designated Approving Authority
DCSIM	Deputy Chief of Staff for Information Management
DOIM	Director(ate) of Information Management
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
IAM	Information Assurance Manager
IAPM	Information Assurance Program Manager
IASO	Information Assurance Security Officer
IAW	in accordance with
IDS	intrusion detection system
IP	Internet protocol
P/P	protocols and ports
RCERT-C	Regional Computer Emergency Response Team-Continental United States
SMTP	Simple Mail Transfer Protocol

TCP	Transmission Control Protocol
UDP	User Datagram Protocol
UPS	uninterruptible power supply
VPN	virtual private network

Section II Terms

Ping of death - A flood of “pings” (simple server requests normally used to check net conditions) designed to disrupt the normal activity of a system.

Protected network - The internal network segment(s) that the firewall provides restricted access and protection in order to secure that network segment from other networks.

Service - A process or application that runs on a system and provides some benefit to a network user.

Spoofing - Attempting to gain illegal entry into a secure system by faking the sending address or fraudulently posing as an authorized user.

Strong authentication - A form of authentication whereby it is very difficult or impossible for a hostile user to successfully intercept and employ a transmitted authenticator (i.e., highly resistant to replay attack).

SYN flooding - A denial of service attack based on sending numerous session connection requests to a server and never completing the entire handshake.

Top-level architecture - The physical and logical segment of the network between the C2P security router (e.g., Cisco 7204/7206/7513 router) and the Army Defense Information Systems Network (DISN) Router Program (ADRP) router (e.g., Cisco 7513 router and/or Cisco 6509 Catalyst Switch).

FOR THE COMMANDER:

OFFICIAL: JOHN B. SYLVESTER
 Major General, GS
 Chief of Staff



THOM E. TUCKEY
 Colonel, GS
 Deputy Chief of Staff
 for Information Management

Firewall Configuration Systems Summary

(FOR USE OF THIS FORM, SEE TRADOC REG 25-74; PROPONENT IS DCSIM)

Complete one form per system; use blank sheets if necessary

I. Organization Name

Mailing Address:

Phone:

Commercial:

DSN:

Fax:

POC Name, Rank or Title:

POC E-mail:

II. System Description

System Name:

Functional Proponent (DA or Local):

Accredited:

Yes

No

Accreditation: Generic

Local

Accreditation Authority:

Hardware Platform:

Operating System (OS):

OS Version:

Briefly describe system application, functionality, and use:

III. Accreditation Documents (List items such as SOP, TFM, SFUG, etc.)

IV. Active Systems Security Mechanisms

Briefly describe the system security mechanisms that are currently active:

Firewall Configuration Systems Summary (cont)

(FOR USE OF THIS FORM, SEE TRADOC REG 25-74; PROPONENT IS DCSIM)

V. Active Auditing

Briefly describe the auditing features that are active on this system:

VI. Account Management

System access, initial security indoctrination:

VII. Password Procedures

Password assignment, composition, aging, revocation:

VIII. System Interfaces

1. List the connectivity interface(s) this system uses (FDDI, ethernet, etc.):

2. With what other systems does this system exchange data? (NIPRNET, dial-up, commercial interface, etc.)

3. How does this system connect to the main network infrastructure?