NSTISSAM COMPUSEC 1-98
DECEMBER 1998

THE ROLE OF FIREWALLS AND GUARDS IN ENCLAVE BOUNDARY PROTECTION

THIS DOCUMENT PROVIDES MINIMUM STANDARDS. FURTHER IMPLEMENTATION MAY BE REQUIRED BY YOUR DEPARTMENT OR AGENCY.

National Security Telecommunications And Information Systems Security Committee

NATIONAL MANAGER

FOREWORD

1. Ensuring system availability, data integrity and privacy, user authentication and transaction non-repudiation for communications and computer systems that comprise the National Information Infrastructure creates a host of Information Assurance (IA) challenges. One of the foremost of these challenges is the need to connect enterprise systems to external systems while protecting against the threat of external penetration with an adversarial goal of obtaining, manipulating or destroying critical information. The purpose of this Advisory Memorandum is to look at two available tools which are a part of the solution to this challenge.

2. Representatives of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) may obtain additional copies of this Instruction from the Secretariat at the address listed below.

KENNETH A. MINIHAN
Lieutenant General, USAF

NSTISSC Secretariat (V503)*National Security Agency*9800 Savage Road STE 6716*Ft Meade MD 50755-6716
(410) 859-6805*UFAX: (410) 859-6814

UNCLASSIFIED

NSTISS ADVISORY AND INFORMATION MEMORANDUM ON THE ROLE OF FIREWALLS AND GUARDS IN ENCLAVE BOUNDARY PROTECTION

SECTION I – GENERAL BACKGROUND

1. Enclave boundary protection is one element in an overall "defense-in-depth" strategy for providing Information Assurance (IA) for enterprise systems (i.e., information systems with functional responsibilities; e.g., command and control, administrative, logistics, etc.). Enclave boundary protection requires a combination of security configuration elements to include firewalls and guards, as well as authenticators, encryptors, and virus and intrusion detectors.

2. Firewalls and guards are enclave boundary protection devices located between a local area network, that the enterprise system has a requirement to protect, and a wide area network which is outside the control of the enterprise system. Their primary purpose is to control access to the local area network from the outside wide area network, and to control access from the local area network to the wide area network. In many instances, they are also used within local area networks to provide a level of access control between different sub-networks within the local area network.

SECTION II – TECHNICAL BACKGROUND

3. There are three general types of firewalls,

   a. Packet (or traffic) filtering,
   b. Application filtering, and a
   c. Hybrid of both.

4. *Packet (or traffic)* filtering devices typically filter (inspect) the source and destination address headers and/or service type (e.g.. FTP, Telnet) on individual data packets flowing across the device. Packet filtering devices are simple and fast. However, they make access control decisions based on a very limited amount of information.

5. *Application filtering,* also known as proxy servers, generally provide more security, but they are extremely complex and can be slower than packet filtering devices. Application filtering firewalls serve as proxies for outside users, intercepting packets and forwarding them to the appropriate application on the inside. Thus, outside users never have a direct connection to anything beyond the firewall. The fact that the firewall looks at the application information means that it can distinguish between different services such as Telnet, FTP, or SMTP traffic. Since application firewalls operate at the application layer of the OSI model they have more flexibility to perform detailed analysis on transiting packets.

6. *Hybrid firewalls* usually employ some combination of security characteristics of both packet filtering and application filtering products.

7. Additional details on these types of firewalls are documented in ANNEX A.

8. Guards are distinguished from firewalls in three major ways:

a. Guards have an application filtering capability that is much stronger than a typical application filtering firewall. Guards use a reclassifier application to control what data is passed from one enclave to another. The reclassifier application uses a collection of filters to review application data content.

b. Guard software is generally developed to meet higher assurance requirements.

c. Guards undergo a much more extensive test and evaluation (e.g. source code analysis, unconstrained penetration testing, and design documentation review) to provide a significantly higher level of confidence that they will operate correctly.

SECTION III – PROTECTION PROFILES AND SECURITY EVALUATIONS

9. The National Security Agency (NSA), in conjunction with other members of the IA community. Is presently specifying firewall and guard security functions and assurances (i.e., confidence measures that the functions are properly implemented) to aid vendors and users in the development, procurement, and deployment of these products. These specifications are contained in documents called Protection Profiles, written in accordance with the internationally adopted "International Common Criteria for Information Technology Security Evaluation."

10. A Guard Protection Profile, to be released in December 1998, addresses the role of guards in security configurations providing access control for networks with classified information, or information deemed to be critical to the performance of the missions assigned to the organizations owning and controlling those networks (i.e., mission critical information). Two Firewall Protection Profiles have already been developed: one for packet filtering firewalls; and one for application-level filtering firewalls. Depending on need, additional profiles may be developed. The firewall protection profiles already developed address the role of firewalls in security configurations providing access control for networks with sensitive but unclassified, non-mission critical information. Protection Profiles will be periodically reviewed and revised to keep pace with changing technologies, applications environments, and cyber attack methodologies.

11. Currently available Guard protection profiles maybe accessed via the INTERNET at http://csrc.nist.gov/cc/pp/pplist.htm#FIREWALL-REV.

SECTION IV - ACCREDITATIONS

12. NSA and the National Institute of Standards and Technology (NIST) have partnered in establishing the National Information Assurance Partnership (NIAP), a purpose of which is to identify and accredit commercial firms for conducting security evaluations of IA products, including firewalls and guards. Producers and vendors of IA products contract with NIAP accredited firms to conduct evaluations, validate vendor product functional and assurance claims, and determine whether the evaluated products meet the requisite protection profiles for the particular product in question (e.g.. firewalls or guards). In accordance with previously negotiated agreements, the results of these evaluations will be internationally recognized and accepted by all those nations participating in the Common Criteria program.

13. As an interim effort, until NIAP firms are accredited and fully operational, NSA has established the Trusted Technology Assessment Program (TTAP). Under this program, there are currently five participating TTAP firms which have been recognized and accredited as being capable of conducing evaluations of IA products. TTAP firms and their addresses are available at http://www.radium.ncsc.mil/tpep/ttap/.

SECTION V – GENERAL GUIDANCE

14. As a general rule, only guards should be specified for use in security configurations bridging and protecting local networks with classified Information from unclassified networks. These security configurations should he designed and implemented employing a system security engineering/risk management process. A Secret and Below Interoperability (SABI) program has been established within the Department of Defense (DoD) which identifies and implements a process for configuring and sustaining the proper security for bridging SECRET to Unclassified networks. This program may have broader applicability to similar requirements outside of the DOD community.

15. Similarly, only firewalls meeting published Protection Profiles should be specified for use in, security configurations protecting local networks containing administrative information (e.g.. payroll, medical, or logistics records), or sensitive but unclassified information, or for providing sub-network protection within classified network environments. These security configurations should be designed and implemented employing a well-designed system security engineering and risk management process.

16. Firewalls should not be used to protect connections between classified systems and unclassified systems. Firewalls with an application filtering capability provide more granular access control and a higher degree of security and, therefore, are preferred from a security perspective in many environments.

17. Prior to the initiation of the TTAP and NIAP programs, NSA conducted an analysis of the following firewalls to verify vendor claims of functionality and to check for commonly known vulnerabilities. They were not analyzed against a Protection Profile, nor against NSA security requirements and thus, should not be viewed as NSA approved or endorsed. These products include:

a. BDM Cybershield (Version 2.4)
b. V-One Smartwall (Version 3.3.1)
c. TIS Gauntlet (Version 3.0)
d. SCC Sidewinder (Version 2.1.2)
e. CheckPoint Firewall-1 (Release 3.0), and
f. Axent Eagle Raptor (NT Version 5.0.1, UNIX Version 4.0).

The results of the analysis have been shared with the vendors and the information is available from NSA.

NOTE:This Information is not intended for dissemination to the general public or to other contractors. Requestors and recipients are limited to departments or agencies of the U.S. Government.

CheckPoint has agreed to address discrepancies between their product and the published Protection Profiles, and have already contracted with one of the NIAP/TTAP firms for follow-on testing. Other vendors have also contracted for product testing with one of the TTAP firms with results expected during early 1999. In the future, all firewall vendors should be encouraged to have their products evaluated by one of the accredited TTAP or NIAP firms.

SECTION VI - SUMMARY

18. Guards and firewalls are not perfect security devices. All contain inherent vulnerabilities, some common to all and some unique to a particular product offering. Therefore, extreme care must be exercised in how they are implemented in specific security configurations with emphasis on how they are set up, as well as maintained. As noted above, guards and firewalls are but one element in a comprehensive Enclave Boundary Protection plan. The fact that a particular guard or firewall meets a published Protection Profile, does not necessarily guarantee that the product alone will provide an acceptable solution to a particular security need. In all cases, a system security engineering process should be employed to maximize IA goals and objectives.

19. NSA is available to provide system security engineering services, or to provide information on any of the other topics addressed in this Advisory Memorandum. Departments or Agencies should contact their NSA Customer Advocates, or simply call (410) 854-4384.

Encl:
ANNEX A

ANNEX A

Packet Filtering:

A packet filtering firewall is a router or computer software that has been configured to screen incoming and outgoing packets. A packet filtering firewall accepts or denies packets based on information contained in the packets' TCP and IP headers. For example, most packet filtering firewalls can accept or deny a packet based on the packets full association, which consists of the following: Source Address; Destination Address; Application or Protocol, and Destination Port Number.

In general, all routers routinely check the full association to determine where to send the packets they receive. However, a packet filtering firewall goes one stop further: before forwarding a packet, the firewall compares the full association against a table containing rules that dictate whether the firewall should deny or permit packets to pass.

Application-level Filtering:

An application-filtering firewall intercepts incoming and outgoing packets, runs proxies that copy and forward information across the firewall, and functions as a proxy server. The proxies that an application-level firewall runs are application specific and filter packets at the application layer of the OSI model.

Application specific proxies accept only packets generated by the services they are designed to copy, forward, and filter. For example, only an FTP proxy can copy, forward, and filter FTP traffic. In addition, if an application-level firewall is running FTP and Telnet proxies, only packets generated by those services could pass through the firewall. All other services would be blocked.

Application-level filtering allows the firewall to examine and filter individual packets rather than simply copying them and blindly forwarding them across the firewall. Application-specific proxies check each packet that passes through the firewall, verifying the contents of the packet up through the application layer.

Application-level firewalls also can be used to restrict specific actions from being performed. For example, the firewall could be configured to prevent users from performing the FTP "put" command which in effect allows users to write to the FTP server.

Hybrids:

A hybrid firewall combines aspects of a packet-filtering and an application-level filtering. Like packet-filtering, this firewall operates at the network layer of the OSI model, filtering all incoming packets based on source and destination IT' addresses and port numbers and determines whether the packets in a session are appropriate. It can also act like an application-level firewall in that it can review the contents of each packet up through the application layer.

DISTRIBUTION:

NSA AGC/I
NSA GC
NSA DDI REG
NSA C
NSA V
NSA X
NSA Y
NSA C21 NTIC
NSA V51
NSA V5212 (5)
NSA V513
NSA L1
NSA X3
NSA Liaison Ft. Huachuca
NSA NSTISSC Secretariat (50)
F1A
F1C
F1D
F1E
F1F
F1G
F1H
F1I
F1L
F1M
F2 (5)
F32
F321
F33
F34
F38
F4 (5)
F41
F45
F47
F6
F81
F83
F91
F92
F92 (Vital Records)

Department of Agriculture
HQ USAF/SYNI (2)
HQ AFC4A/SYS (3)
AF SA/ALC/LTMK (3)
Army SAIS-C4C
Army SAIS-PAC-1
USACCSLA (15)
CIA (2)
CINCUSACOM (2)
U.S. Army Forces Command (2)
Department of Commerce (3)
U.S. Customs Service
Drug Enforcement Administration
DEA (STTC) (2)
ODASD C3/ISS (2)
OUSD (Comptroller)
DoD INFOSEC Liaison Officer NATO
DoD NSA/CSS INFOSEC REP (Pentagon)
Defense Intelligence Agency (SY)
Defense Intelligence Agency (SYS-4)
Defense Intelligence Agency (DAC –214)
Defense Investigative Service
Defense Information Systems Agency
DISA/CISS
DLA
Defense Threat Reduction Agency
Defense Threat Reduction Agency (ISTS)
Department of Education
Department of Energy (8)
FBI (11)
FCC
Federal Reserve System
FEMA (2)
FEMA (Mt. Weather)
GSA (3)
HHS
HQ USSPACECOM (2)
HUD
INS
Department of the Interior
JCS (2)
Joint Staff ICP (5)
Department of Justice
Department of Labor
HQ,Marine Corps
NASA
CNO (N643)
NAVY (N6)
Naval Command, Control &
Ocean Surveillance Ctr. (20)
NAVY DCMS (2)
NAVY SPAWAR (2)
NCRDEF
NCS (2)
NIMA, ATETP
NIMA (NPI)
NIMA (ATI)
NIST
NRC (3)
NRO (3)

National Security Council
OMB (2)
OPM
SEC
Secret Service
Security Policy Board Staff
Department of State (DS/ISP/SSB) (3)
Department of State (A/IM/SO/TO/SI) (3)
Department of Transportation (OST/M-70) (2)
Department of Transportation (S-80)
CAA COGARD
COMDTCOGARD (G-TPS-4) (3)
COMDTCOGARD (G-OIN-3)
COMCOGARDONE
COMCOGARDTWO
COMCOGARDFIVE
COMCOGARDSEVEN
COMCOGARDEIGHT
COMCOGARDNINE
COMCOGARDTHIRTEEN
COMCOGARDFOURTEEN
FAA (ACO-400)
FAA (ACP-300)
Department of Treasury (Director of Security) (10)
Department of Treasury (Intelligence Support) (2)
Department of Treasury (3210 Annex)
Department of Treasury (3090 Annex)
USACOM/J6
USCENTCOM/CCJ6
USEUCOM/ECJ6
USSPACECOM/J4-6
USSOCOM/SOJ6
USTRANSCOM/TCJ6
USTRANSCOM/TCJ6
WHCA (Security & Safety)
WHCA (SSD-CMDSA) (2)
USIA
U.S. Senate INFOSEC
VA
HQ DA DALO-SMR (2)
HQ DA DAMI-CIS (2)
U.S. Army Material Command (AMCHI)
Department of the Air Force (SA/ALC/LTMK) (3)