National Aeronautics and
Space Administration

NOT MEASUREMENT
SENSITIVE

NASA-STD-2813
August 19, 1997

# NASA FIREWALL STRATEGY, ARCHITECTURE, STANDARDS AND PRODUCTS

## NASA TECHNICAL STANDARD

# FOREWORD

This standard is approved for use by NASA Headquarters and all NASA Centers and is intended to provide a common framework for consistent practices across NASA programs.

The material covered in this standard is based on the consensus judgment of the NASA Chief Information Officer (CIO) Representatives Board and the NASA CIO Council. The purpose of this standard is to provide a framework for a consistent, Agency-wide approach toward the implementation of Firewalls within NASA. For the purposes of this paper, Firewalls may be considered a category of technologies that provide a network-level, first-line-of-defense mechanism that isolates specific Information Technology (IT) resources from other end-users, hosts and services. This document was developed by Marshall Space Flight Center in its role as the Expert Center for Network Security in conjunction with an Inter-Agency team of network and security specialists. It is intended for use by Agency IT service providers, NASA Program and Project Offices, and NASA business partners.

This Firewall Strategy, Architecture, Standards and Products document is based on two equally important considerations:

1. NASA is a publicly chartered scientific and research organization whose fundamental purpose is to create knowledge and to share that knowledge freely with the scientific community and the public-at-large.

2. NASA, within the context of mission, project and business processes, has the responsibility to protect IT resources in order to minimize and, where possible, eliminate, threat to life, limb or loss of capital and knowledge-based assets.

In recognition of these considerations, and the fact that NASA Centers and Projects have different mission goals and requirements, it is the intent of this document to allow significant Center discretion concerning the deployment and use of Firewalls. It also provides a framework which maximizes interoperability, facilitates efficient use of Agency IT resources (capital and labor) and articulates a concise, manageable approach toward the deployment of Firewall technologies.

Therefore, this document recommends that each NASA Center deploy IT resources within three information service “islands”, each of which provide varying levels of public and restricted access. Again, the approach assumes Center discretion, based on formal risk assessment, concerning the deployment of IT resources (end-users, networks, hosts and services) within these “islands”. The three Networks are:

1. Center Private Network - Contains those Center IT resources deemed necessary to be completely isolated from the global Internet.

2. Center Public Network - Contains those IT resources that must be accessible by the public-at-large, but at the same time, require protection in terms of data integrity and availability.

3. Center Open Network - Contains those IT resources that must be freely accessible, via the Internet, by the scientific community and the public-at-large, and require protection in terms of data integrity and availability, but without firewalls.

Within the context of the preceding Network definitions, this document also provides a specific Firewall technology “Features List” which defines those Firewall functional elements deemed by the Agency Firewall team to be either mandatory, preferred, or optional in terms of required functional capability. This Features List was used to evaluate several Firewall products and to produce a list of satisfactory products which met all mandatory Agency requirements. Based on these features and other discriminating factors, a preferred product recommendation is made.

Requests for information, corrections, or additions to this standard should be directed to the ISSO, Marshall Space Flight Center (MSFC), the Principal Center for Communications Architecture, Code AI52, Huntsville, Alabama 35640. Requests for additional copies of this standard should be sent to NASA Engineering Standards, EL01, MSFC, AL, 35812 (telephone 205-544-2448).

Ronald S. West
Chief Information Officer

CONTENTS

## FIGURES

FIGURE PAGE

## TABLES

TABLE PAGE

## APPENDICES

APPENDIX PAGE

# NASA FIREWALL STRATEGY, ARCHITECTURE, STANDARDS AND PRODUCTS

## 1. SCOPE

1.1 Scope. Marshall Space Flight Center (MSFC), chartered by Ames Research Center (ARC), the NASA Principal Center for IT, has the task to develop an Agency Firewall Architecture, Standards and Product (ASP) document. The MSFC approach has been to cultivate dialog with appropriate Agency entities and individuals, actively involve other Centers in order to share expertise and input, perform hands-on technology evaluation, and ultimately develop the Firewall ASP within the current Agency CIO, Principal Center and Network Consolidation activities.

1.2 Purpose. This document provides a framework for a consistent, Agency-wide approach toward the implementation of Firewalls within NASA. In recognition of the fact that NASA Centers, as well as Projects within a Center, have different mission goals and requirements, this Architecture is intended to allow significant Center discretion concerning the deployment and use of Firewall technologies to meet Center requirements. Risk assessment and the resultant security policies, processes and IT implementations are the responsibility of Centers and Projects. At the same time, it is the goal of this Architecture to ensure interoperability between NASA Centers, facilitate efficient use of Agency IT resources (capital and labor) and articulate a concise, actionable approach that positions the deployment of network security within the context of an over-all Agency IT security policy.

1.3 Applicability. It is important to note that developing a single detailed Firewall architecture or strategy to fulfill every Center's needs, without understanding their specific security requirements or network environment, is not practical or within the scope of this document. Keeping the absence of specific Center requirements in mind, the intent is the initial introduction of a document providing a framework or guidelines for consistent Agency-level Firewall implementations that foster compatibility and interoperability. Each Center will need to determine the level of protection required for their individual IT resources, establish their security policies, develop a Firewall implementation plan to assist in enforcing those policies, and understand that Firewalls are only one of several tools required to provide IT security. Cost, performance, support, available technology, and interoperability issues (in addition to security related issues) must be addressed while developing implementation plans. As NASA Firewall deployments become common and Firewall standards and technologies mature, the experiences and "lessons learned" should be used to update this document and share the evolving "Firewall expertise" across the Agency.

## 2. ACRONYMS

2.1 Acronyms used in this standard:

| | |
|---|---|
| • ARC | Ames Research Center |
| • ASP | Architecture, Standards and Product |
| • BSD | Berkeley Software Distribution |
| • CERT | Computer Emergency Response Team |
| • CIAC | Computer Incident Advisory Capability |
| • CIO | Computer Information Officer |
| • CSI | Computer Security Institute |
| • CPU | Central Processing Unit |
| • DB | Database |

| | |
|---|---|
| DMZ | Demilitarized Zone |
| DNS | Domain Name Server |
| FIPS | Federal Information Processing Standards |
| FTP | File-Transfer Protocol |
| FW | Firewall |
| GSFC | Goddard Space Flight Center |
| HTTP | Hyper Text Transport Protocol |
| HQ | NASA Headquarters |
| ICMP | Internet-Control Message Protocol |
| ID | Identification |
| IGMP | Internet Group Message Protocol |
| IP | Internet Protocol |
| IPX | Internetwork Packet Exchange |
| IRE | Information Resource Engineering |
| ISP | Information System Processor |
| ISS | Internet Security Systems |
| IT | Information Technology |
| ITSEC | Information Technology Security |
| LAN | Local Area Network |
| LDAP | Light Directory Access Protocol |
| MSFC | Marshall Space Flight Center |
| NASA | National Aeronautics and Space Administration |
| NASIRC | NASA Automated Systems Incident Response Capability |
| NCSA | National Computer Security Association |
| NFS | Network File System |
| NIS | Network Information Services |
| NISN | NASA Integrated Services Network |
| NTP | Network Time Protocol |
| NSA | National Security Agency |
| OMB | Office of Management and Budget |
| OS | Operating System |
| PC | Personal Computer |
| PCCA | Principal Center for Communications Architecture |
| RAS | Remote Access Client |
| RFC | Request For Comments |
| RIP | Routing Information Protocol |
| RMON | Remote Network Monitoring |
| RPC | Remote Procedure Call |
| SHTTP | Secure Hyper Text Transport Protocol |
| S-HUB | Switching Hub |
| SMTP | Simple Mail-Transfer Protocol |
| SNA | System Network Architecture |
| SNMP | Simple Network-Management Protocol |
| SOCKS | A networking proxy protocol |
| SSH | Secure Shell |
| SSL | Secure Socket Layer |
| TCP | Transmission-Control Protocol |
| TFTP | Trivial File-Transfer Protocol |
| UDP | User Datagram Protocol |
| VPN | Virtual Private Network |
| WAN | Wide Area Networks |
| XNS | Xerox Network System |

## 3. GENERAL REQUIREMENTS

When discussing NASA IT Security, there are two equally important considerations concerning access to, and provision of, NASA information. They are:

a. NASA is a scientific and research organization whose fundamental charter is to create knowledge and to share that knowledge freely with the scientific community and the public-at-large.

b. NASA, in the context of mission, projects and business processes, has the requirement and responsibility to protect IT resources in order to minimize, and/or eliminate, threat to life, limb or loss of capital and knowledge-based resources.

The draft *NASA Information Technology Security Architecture*, developed by ARC, states that NASA IT security implementations must:

- Protect NASA computer and communication systems from an increasingly hostile threat environment, including hacking and virus attempts.

- Provide access to a rich set of communications services to NASA end-users via the Internet and other Wide Area Networks (WAN).

- Provide appropriate access from external users to NASA systems, data, information and communication services.

- Provide appropriate security controls for NASA information and for NASA systems.

- Assure compliance with Federal Information Processing Standards (FIPS) and interoperability within NASA, with NASA business partners, and with the commercial, academic and research communities.

Therefore, NASA has the requirement that protective measures, based on risk assessment, be taken to maximize, and where possible ensure, the privacy, integrity and availability of IT resources and information. This document discusses those measures and the technologies that can be used to protect NASA assets at the network layer. Requirements and metrics associated with the protection of specific information system assets will be developed and documented as this Architecture evolves (e.g., Minimum recovery time for information on a public NASA service).

## 4. FIREWALL DEFINITION AND FUNCTIONALITY

According to the draft ARC *NASA Information Technology Security Architecture*, a Firewall is a hardware/software system(s) that enables network security through a combination of packet filtering routers, non-circumventable and non-spoofable logging and auditing mechanisms, and in some cases, application proxies executing on an isolated Local Area Network (LAN). For the purposes of this document, a Firewall is considered a category of technologies that acts as a logical point on a network through which all communications between a secure internal network, protected host or other IT resource and the outside “un-trusted” network, must pass. Further, this set of technologies may be configured to restrict and/or allow in-bound and out-bound access by specific devices, end-users, protocols and services while providing auditing, logging of access by these entities and alarm notification to administrators. The specific technologies include, but are not limited to, border routers, packet inspection mechanisms, proxy servers and Virtual Private Network (VPN) mechanisms. General definitions of these technologies are:

- Border Router - A border router is the connection point between an internal or Center network and external networks. These routers can be configured to specifically filter traffic based on network addresses and protocols and are typically a Center's first line of defense.

- Packet Inspection - Firewalls have the ability to analyze more "application specific" information inside each network packet. Thus "rules" can be defined which restrict access to those services which are explicitly defined.

- Proxy Server - When a Firewall acts as a Proxy Server for a specific service, it typically acts as a middle-man between network connections. An example is the case of an FTP session where a user must first connect to a Firewall for authentication. The Firewall then establishes a separate connection to a destination host, thus masking the internal network address.

- VPN - When two secure networks or hosts are connected by an un-trusted network, e.g., the Internet, and have the requirement to exchange information in a secure mode, a Virtual Private Network can be established using encryption, decryption, and authentication mechanisms. This enables a "secure tunnel" through public or potentially hostile networks. VPNs can be established between two Firewalls in order to encrypt data between whole networks or between individual clients and a Firewall. A common use of VPN technology is the utilization of public networks in order to provide a flexible and cost-effective alternative to private leased lines for Internet-working.

It is important to note that Firewalls are but one component of an overall set of security policies, processes and technologies. The ARC Security Architecture defines the generalized functional elements common to all Information Technology (IT) security components - including Firewalls. These functional elements include: identification and authentication, access control, auditing, data, data integrity and privacy, data flow control, tamperproof, always invoked and change detection. Firewalls are implemented at the network level to protect data from tampering and invasion of privacy, to provide access logging and auditing and to assist in ensuring network availability. Potential threats mitigated by Firewalls include:

- Masquerade. Hosts, services or end-users that attempt to masquerade as an authorized host or end-user violate system and network authenticity for all NASA end-users. An attack of this nature may be as simple as the use of a captured userid/password pair, or as complex as an IP spoof used to corrupt a Center Domain Name Service (DNS) server.

- Interception. Given the fact that networks are generally a broadcast media, data transmitted over them is subject to interception by one other than its intended recipient. Such an attack might be the act of capturing a userid/password pair, or the receipt of ongoing data transmissions without the knowledge and consent of both the transmitting and receiving parties.

- Modification. Once intercepted, data may be modified and retransmitted without the knowledge of the sender or the receiver. Using a captured userid/password pair, an intruder also has the potential to modify stored data or device configuration files without fear of detection. In the most extreme cases, data modification could result in service interruption.

- Interruption. The sole purpose of this attack is to deny legitimate end-user access to NASA systems and networks. This may be accomplished through a combination of the above threats, but also may be effected by exploiting known weaknesses in existing protocols and services. Examples of denial of service attacks follow:

  - Flooding network services: A network-based attack in which the perpetrator transmits large number of packets in an effort to overflow network buffers or saturate connections.
  - E-mail spamming: A network-based attack in which the perpetrator sends large quantities of mail messages to an end-user(s) of a given site, consuming bandwidth, disk space, and users' time.
  - Exhausting resources: A network- or system-based attack in which the perpetrator consumes resources such as disk, CPU, etc. by filling logs, running infinite loops, etc.
  - Software bugs: A network- or system-based attack in which bugs in system software are exploited to gain privileges, crash servers, etc.
  - Race conditions: A network- or system-based attack in which timing relationships between system components are exploited to gain privileges and/or crash servers.

In summary, a Firewall is a defense mechanism intended to discourage unwanted, and in some cases hostile, access at the network layer by enabling the isolation of a specific set of IT resources (network, host, end-user devices and services) from other end-users, hosts and services. It is a complementary technology to other network, desktop and applications-layer security mechanisms such as virtual private networks, public/private key systems, virus detection schemes and proprietary host and network operating system security structures.

## 5. AN AGENCY APPROACH TO FIREWALLS

Based on the requirements defined in Section 3.0, it is recommended that NASA create three information service “islands”, each of which provides varying levels of access. Further, it is recommended that Firewalls, combined with other security technologies and processes, be utilized and deployed to create these “islands”.

These information service “islands” are:

- A Center Private Network

- A Center Public Network

- A Center Open Network

As previously stated, this Architecture assumes Center discretion concerning the deployment of IT resources (end-users, networks, hosts and services) within these “islands”. Further, this document provides guidelines for protecting resources made available to the public; but does not dictate “who” at the Center determines where resources should be placed.

The Architecture is intended to provide flexibility of implementation and support future expansion of services while accommodating each Center's diverse needs. The key goal is to define a consistent, strategic, Agency-wide framework that facilitates interoperability, protects IT resources, and reduces management cost.

5.1 The Center Private Network. The Center Private Network would contain those Center IT resources deemed necessary, through risk assessment (including performance and cost issues), to be protected and isolated from the global Internet. The Center Private Network is to be protected by a combination of Firewall, VPN, proxy technologies as well as other network and host operation system security structures. Each Center will, in cooperation with Principal Center for Information Technology Security (ARC) and CIO entities, choose which IT resources are on the Private Network and develop an implementation scenario for its creation, operation, and management. Some Centers may choose to place the majority of their IT resources behind a Center Firewall, while other Centers may choose to leave most resources on the Open-side (much as it exists today).

It is not necessary that significant resources and energy be invested initially to create these Private Networks; they should be built incrementally and thoughtfully. IT resources (e.g., hosts, end-users, services, LANs, etc.) can be moved to, and in some cases, implemented within, the Private Network based on currently-defined, formal risk assessment processes.

The Center Private Network Firewall will provide the following minimum set of services:

a. Services provided for Internal Resources/Users

- Telnet through Firewall to external networks
- FTP through Firewall to external networks
- HTTP through Firewall to external networks
- SSL and/or SHTTP through the Firewall to external networks
- SMTP mail through Firewall to external networks
- DNS - external DNS information must be made available to internal clients
- Outbound TCP Proxy or Packet Inspection services as required
- SSH through Firewalls to external networks

b. Services provided for External Resources/Users

- SMTP mail must be deliverable to clients on internal networks
- DNS - some form of "presence" must be configurable
- VPN services to internal resources as required for previously authorized authenticated external users to previously authorized resources
- SSH must be able to access internal network devices for remote administration purposes"

5.2 The Center Public Network. The Center Public Network would contain highly-visible information resources that must be accessible by the public-at-large, but at the same time, requires very substantial protection to assure uncompromised information integrity and service availability. These include, but are not limited to, Public World Wide Web sites, Directory Servers (including Public Key Certificates) and Collaborative Environments (e.g., Lotus Notes Servers, CUSeeMe reflectors, shared file spaces, etc.). Inbound access to IT resources deployed on this network would be restricted to specific application services (e.g., HTTP, LDAP). There would be no end-users deployed in this information island. The only out-bound connections would be very controlled host-to-host, service-to-service information replication mechanisms. Generally, write access to systems in this network would be limited to authorized users originating sessions from either the private network or through external VPN connections. Further, administrator interaction with resources on the Center Public Network would require encrypted password, public/private key authentication and/or other security technologies such as “secure shell”.

The Center Public Network Firewall will provide the following minimum set of services:

a. Services provided for Internal Resources/Users

Sessions will not be permitted to originate from the public network to external networks. This prevents hackers from hopping to the private network should the public network be compromised. No user clients should be located in the public network. The intent of this network is to contain resources that require additional protection and serve the general public as well as internal users. Examples would be Web servers, FTP and Telnet hosts.

b. Services provided for External Resources/Users

- DNS - some form of "presence" must be configurable
- Telnet access to servers or hosts located on the public network
- FTP access to servers or hosts located on the public network
- HTTP access to servers located on the public network
- SSL and/or SHTTP access to servers located on the public network
- SSH for system administration and updating data securely on public network hosts

NOTE: These are general guidelines to help explain the environment and intent of the Public Network concept, but do not preclude other scenarios such as Web Servers with cgi scripts which accept data from a user.

5.3 The Center Open Network. The Center Open Network would contain IT resources which need to be freely accessible, via the Internet, by the scientific community and the public-at-large, and require protection in terms of data integrity and availability, but without firewalls. Security measures and risk management of hosts, services, LANs, and applications located on this Network will be the responsibility of the “data owners” or by a central organization at the Center’s discretion. The IT resources deployed on the Center Open Network will be protected by security measures deemed necessary by each Center IT Security Manager as well as any security measures provided by the Wide Area Network Service Provider. (It should be noted that access from the Center Open Network to resources on the Center Private Network should be restricted and, where necessary, will require a VPN or other form of authenticated and encrypted access.)

Figure 1 is a simplified view of the three proposed networks, their relationship to each other, to other Centers and the WAN.

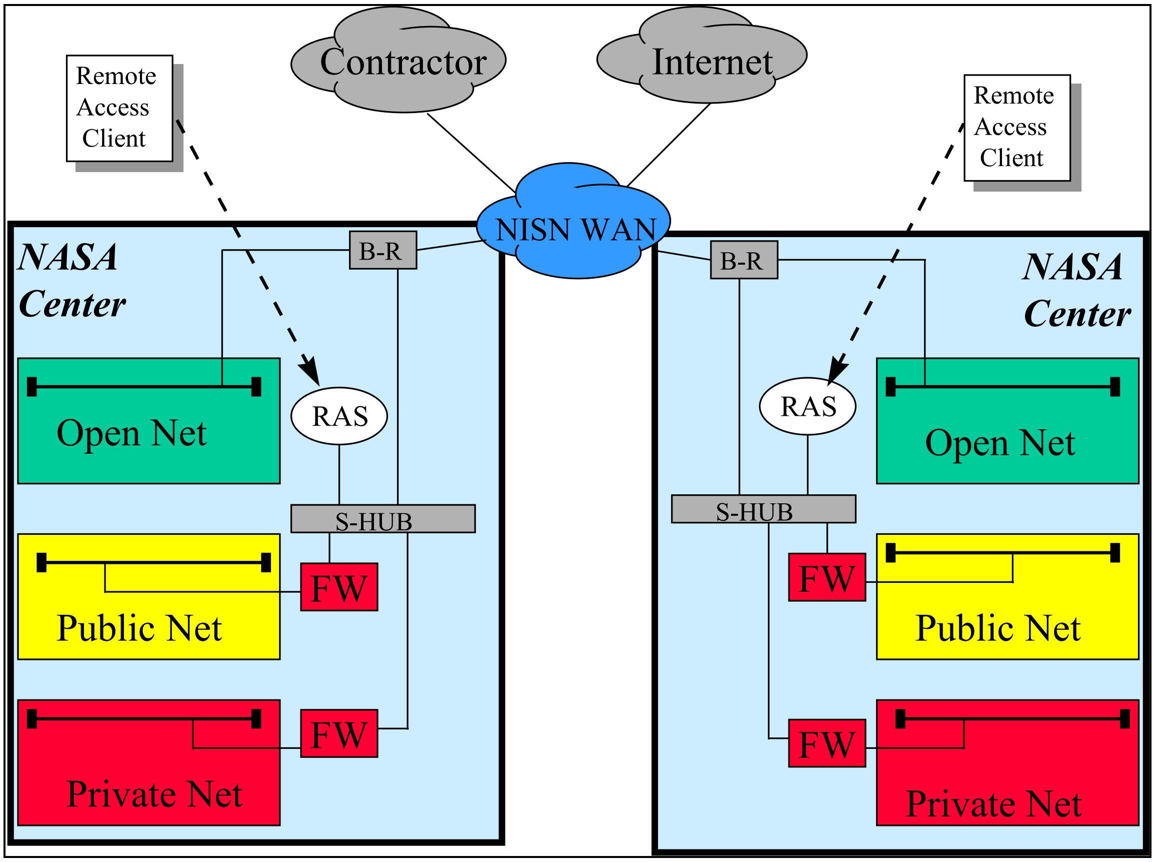

FIGURE 1. An Agency Approach To Firewalls

5.4 WAN Service Provider Responsibilities. In the preceding scenario, the NASA WAN Service Provider will implement network security capabilities necessary to perform basic denial of service actions (e.g., for known threats and intruders), logging (e.g., for incident tacking and investigations), and auditing (e.g., for network performance and traffic load) on the backbone infrastructure. In some instances, Centers may choose to implement 1) local ISP connections and 2) local Contractor connections connected at strategic network locations when it will best fit their own Internet traffic load, Center and Enterprise missions , and security considerations. For the purposes of this document, these connections will be considered independent WAN network providers and, as such, part of the external global Internet.

5.5 External Network Access of Private Network Resources. Access to IT resources within the Private Network (end-users, hosts and services) from the Center Public Network, the Center Open Network and the Internet will be achieved with authenticated, monitored and logged client-to-host security mechanisms such as virtual private networks, public/private key systems, encryption technologies, host and network operating system security structures.

5.6 External Network Access of Public Network Resources. Users in the Private Network, as well as external or Internet users, will have access to resources in the Public Network. However, access from administrators in the Private Network to update services within the Public Network will require controlled and secure access methods as stated in Section 5.2. Example: Web administrators updating Public Web pages, etc.

5.7 Dial-In/Remote Access. Dial-in traffic to systems inside the Public or Private Networks must pass through the Firewall for authorization, logging, and monitoring. Since a large portion of dial-in access is to public and administrative information and applications, the remote access servers will be connected outside the Center Private and Public Networks in a manner that provides access to all Center IT resources. Resources within the Private or Public Networks will then be accessed by VPN encryption and other security strategies.

5.8 Contractors and Business Partners. A determination must be made on a case-by-case basis regarding on-site and/or local contractors' systems and their placement within the three Center Networks. Each Center IT Security Manager must review and approve the security measures of non-NASA systems located on the any NASA network.

5.9 Project/Organization Firewalls. In some cases, Center and Agency-wide Projects and Organizations will deem it necessary, based on risk assessment and other mission requirements , to secure their IT resources behind an additional Firewall. Implementers of such firewalls should be cognizant of the Center's implementation of this Firewall Architecture for interoperability reasons. Each Center IT Security Manager should review Project/Organization level Firewall implementations. Figure 2 depicts this relationship.

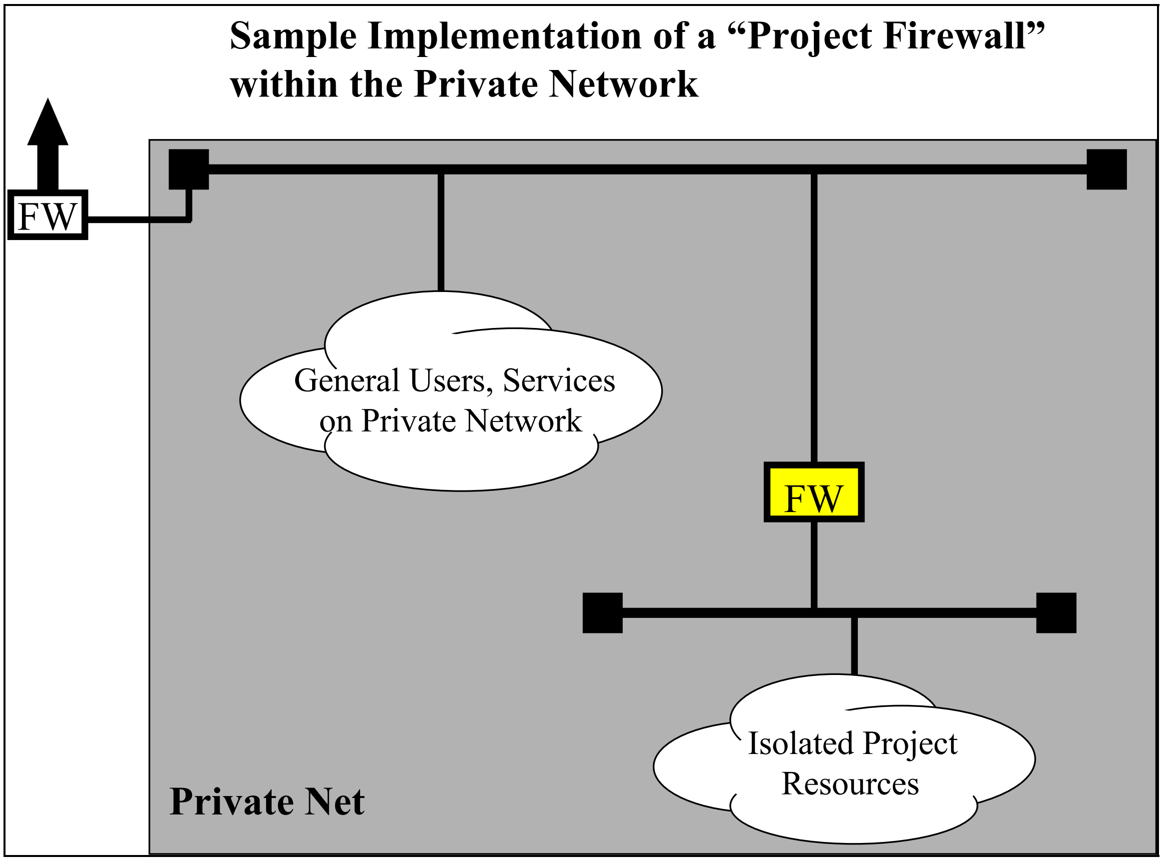
Sample Implementation of a "Project Firewall" within the Private Network
FW
General Users, Services on Private Network
FW
Isolated Project Resources
Private Net

FIGURE 2. Sample Implementation of a Project Firewall

## 6. INTEROPERABILITY CONSIDERATIONS

Firewalls are inherently a “disabling” technology. That is, they are intended to isolate and protect IT resources. At the same time, many of the resources deemed necessary to be protected via Firewalls are integral to Agency end-user, workgroup and Enterprise communication and collaboration. One of the reasons for the very existence of this Architecture is to provide an Agency framework within which Firewalls may be deployed without disrupting or preventing the implementation of fundamental Agency communication services. For the purposes of this document, interoperability means the degree to which end-users and IT services may successfully exchange information. When discussing Firewalls there are two levels of interoperability to consider: Firewall to Firewall interoperability and Service to Service (e.g., The capability for an E-mail client at one Center to access an E-mail server at another Center.)

### 6.1 Firewall to Firewall Interoperability.

a. Firewall to Firewall Communications - Client Services. Depending on Center requirements and specific implementation of Firewalls, they will either be “standalone” systems, requiring little or no compatibility between the Firewalls deployed (such as when a user sends SMTP mail or establishes a Telnet session from his internal network, out his Firewall to the Internet, and through another Firewall to a user on it’s internal network) or Firewalls working together to establish VPN links between Firewalls, or client VPN sessions established to a Firewall. In the first scenario, (standalone systems), interoperability isn’t much of a concern so long as both Firewalls are configured to allow the same services. When working together, it is important that the Firewalls be compatible. This can be achieved by 1) using the same Firewall product, or 2) performing extensive testing to ensure different vendor products have implemented compatible encryption and VPN technologies, in addition to having similar configurations for allowing services. This scenario will evolve as NASA more clearly defines the role of Firewalls in the IT infrastructure and as the Firewall technologies mature.

b. Firewall to Firewall Communications - Remote Management. Another example where Firewall interoperability is important is when multiple Firewalls will be deployed and need to be managed from a central location. Once again, this can be achieved either by using the same Firewall product supporting this feature, or by performing extensive testing to ensure different vendor products can be managed by a common central management interface.

### 6.2 Service to Service Interoperability.

a. Firewalls placed between a NASA Center and the General Public or Internet. Firewalls are designed to support authentication, auditing, and access for a limited set of services (Telnet, FTP, SMTP Mail, HTTP) between an internal trusted network (usually a corporate network) and an external untrusted network (usually the Internet). Those services are designed in the Firewall architecture and are ready for off-the-shelf deployment. Therefore, the Firewall installation between NASA Centers and the Internet should have minimum impacts.

Firewalls placed between different NASA Centers and Firewalls placed between NASA Centers and their off-site Contractors, Science Community, or Business Partners

Firewall interoperability between NASA Centers and between NASA contractors and business partners could have any extreme impact and must be adequately planned and tested. Network services utilized within this environment are typically considered as “trusted” within a corporation with “host-based” security measures usually considered adequate after a Firewall has restricted access from the Internet.

## 7. ASSUMPTIONS/CONCERNS

If risk assessments determine that networks at other NASA Centers, contractors, and business partners are to be treated the same as the  untrusted Internet, instead of establishing a secure network environment between Centers and deploying Firewalls for restricting Internet access or securing selective “project level networks within a Center”, then the following assumptions must be made before implementing this Architecture.

a. Assumptions:

- Current business applications and network services can be migrated to the appropriate network (Open, Public, or Private) based on security requirements, and once moved can be fully supported with the Firewall services outlined earlier for each network. (see Sections 5.1, 5.2, and 5.3)

- Current applications and protocols utilized by external NASA contractors connected to the NISN network can be fully supported with the Firewall services outlined earlier for each network. (see Sections 5.1, 5.2, and 5.3)

- Only Internet Protocol (IP) based protocols are required, and therefore allowed, on the WAN.

b. Concerns:

- Support for emerging Inter-Center applications and services that are not natively supported (requires specific access based on source and destination address and TCP or UDP port  through the Firewall) with current Firewall technologies (e.g., streaming media such as Video and Audio, Whiteboard, Shared Applications, Real-time/interactive Collaborative Tools).

- Agency use of legacy network protocols (e.g., Appletalk, SNA, DecNet, IPX, XNS). Some use of these protocols remains.  It may be necessary in some cases to circumvent the IP based Firewall structures, in which case, IT resources requiring these protocols must be deployed on a Center Open Network.

- External access to existing Agency IT resources (e.g., Contractor client/server applications).

- Potential availability of Inter-Center dedicated, high bandwidth, Guaranteed Level of Service mechanisms from WAN Service Providers (NISN).  Firewalls may deter access to these resources for some users and/or services.

- Relative Agency inexperience with utilizing and managing emerging, complex IT security technologies.

## 8. NASA FIREWALL FEATURES LIST

During 1996, an Inter-Center team of Firewall “experts” was formed to carry out hands-on Firewall technology evaluation, testing and integration. Over the course of several months, this team, with representatives from MSFC, ARC, Goddard Space Flight Center (GSFC) and NASA Headquarters, created the following “Features List”. It is intended that this Features List, used within the context of this Architecture, assist in the evaluation and rating of Firewall products under consideration for use within NASA. An initial product(s) recommendation is included in this document in Section 9.

TABLE 1. NASA Firewall Product Features List/Certification Matrix

**(Mandatory)**

| **Feature Description** | **Status** |
|---|---|
| Additional services can be defined by transport mechanism (TCP or UDP) and port number. | Mandatory |
| Support secure IP standards (RFC 1825-1829) as they become available. | Mandatory |
| Provide a "virtual private network" capability for secure point-to-point communications, secure remote user authentication, and secure remote administration. | Mandatory |
| Inbound packets to the firewall may be:<br>a. Logged. b. Decrypted. c. Allowed. d. Denied. | Mandatory |
| Outbound packets to the firewall may be:<br>a. Logged. b. Encrypted. c. Allowed. d. Denied | Mandatory |
| Provide the following security services in addition to those already provided by the network: a. User authentication (login/password). b. Service Access control (authorization). c. Data confidentiality (encryption). | Mandatory |
| Support at least two network interfaces: | Mandatory |
| Year 2000 compliant, as defined by the General Services Administration | Mandatory |
| Support the following protocols and services: IP ICMP TCP UDP FTP (including anonymous FTP) Telnet DNS Kerberos SNMP HTTP Secure HTTP SMTP NTP IGMP X-Window related packets | Mandatory |
| Able to detect and block packets using source routing. | Mandatory |
| Perform subnet filtering and support variable-length subnet masks. | Mandatory |
| Detect and block IP fragmentation attacks. These attacks are described in Request for Comment (RFC) 1858, Security Considerations for IP Fragment Filtering. | Mandatory |
| Firewall not automatically recycle log file when it is full or periodically | Mandatory |
| Sufficient product documentation | Mandatory |
| Utilize host authentication capabilities (if available) and provide support for other authentication mechanisms such as S/Key, SecureID. | Mandatory |
| Should detect, log, and block packets arriving from an external source that are not in response to an internal network request. | Mandatory |
| Should detect, log, and block packets arriving from an external source that do not respond to an internal network request within a specified time period. | Mandatory |
| Upgrades Available from Vendor | Mandatory |

TABLE I. NASA Firewall Product Features List/Certification Matrix
**(Mandatory) (Cont'd)**

| | |
|---|---|
| Detect and block IP spoofing attacks. These attacks are described in U.S. Department of Energy Computer Incident Advisory Capability (CIAC) Advisory F-08: IP Address Spoofing and Hijacked Session Attacks dated January 23, 1995. | Mandatory |
| Detect and block SYN-flood denial of service (DoS) attacks. These attacks are described in CERT Advisory CA- 96.21, TCP SYN Flooding and IP Spoofing Attacks dated September 19, 1996. | Mandatory |
| Support Network Address Translation | Mandatory |
| Configurable to maintain audit logs of all connections through the firewall. Log files can be maintained on directly connected or remote devices. Log files shall be configurable & renewable. | Mandatory |
| Capability to instruct the firewall to selectively record packets based on any combination of:<br>a. Protocol-carried end point.<br>b. Protocol-carried protocol parameters.<br>c. Datagram disposition (accept, deny, etc.).<br>d. Datagram parameters. | Mandatory |
| Each event logged by the firewall shall include (at a minimum):<br>a. Event time.<br>b. Nominal communication end-points and protocol parameters.<br>c. Message disposition. | Mandatory |
| Firewall stop all traffic when log file is full or provide adequate measures to ensure traffic is not allowed without being logged. | Mandatory |
| Throughput greater than or equal to 60% of line speed | Mandatory |

**(Preferred)**

| | |
|---|---|
| Capable of producing audit log summary reports. | Preferred |
| Capability of sending alarm messages via simple network management protocol (SNMP, RFC 1213) traps | Preferred |
| Firewall alarm messages must be configurable to include or exclude specific events or patterns of events ("signature patterns"). | Preferred |
| Graphically-oriented configuration interface. | Preferred |
| Upon installation of software updates and upgrades, accept the existing rules base and not require extensive reconfiguration. | Preferred |
| Report generation tools to assist in log interpretation and retrieval of data based on communication end-points (e.g. addresses), protocol parameters, and datagram disposition. | Preferred |
| The firewall administrator should be able to define new alarm signature patterns as additional situations are encountered or tools become available. | Preferred |
| Compatible with RMON (RFC 1271) | Preferred |
| 24 hour Technical Support | Preferred |
| Rules DB Caching to improve performance | Preferred |
| Have multiple rules set | Preferred |
| Filters & Rules easy to interpret | Preferred |
| System Administration doesn't require extensive UNIX knowledge | Preferred |
| Support comments on all configuration rules | Preferred |

TABLE I. NASA Firewall Product Features List/Certification Matrix
**(Preferred) (Cont'd)**

| | |
|---|---|
| Logging statistics easy to interpret | Preferred |
| Support at least three network interfaces: Outside, Inside, and DMZ | Preferred |
| Must have an optional client-server architecture, where several firewall client modules may be managed from a common firewall server. | Preferred |
| Java screening | Preferred |
| Active X screening | Preferred |
| Firewall certified by one of the following: NCSA, NSA, CSI, ITSEC, etc. | Preferred |

**(Optional)**

| | |
|---|---|
| Source Code available for inspection | Optional |
| Support multicasting (real audio / video) | Optional |
| E-mail attachments can be filtered. (allowed or blocked) | Optional |
| The firewall supports SOCKS | Optional |
| Should have an integrated capability to detect known computer viruses | Optional |
| Turn-key Solution (Hardware, Software, & Installation) | Optional |

## 9. PRODUCT RECOMMENDATIONS

Prior to and during the development of this Architecture, an independent, Inter-Center group of Firewall experts participated in Firewall technology discussions, evaluation and testing. A core Firewall evaluation test team was formed with representatives from MSFC, Ames Research Center, Goddard Space Flight Center, and NASA Headquarters. The resultant product recommendations are based on the consolidated inputs from each of these centers.

9.1 Test Environment. Each participating Center (ARC, GSFC, HQ, MSFC) utilized a lab environment containing an internal (trusted network) and an external (un-trusted network). In order to perform testing, the Firewall products were installed between the two networks. The external networks had connectivity to NASA's WAN and Internet in order to enable product testing between Centers. Figure 3 is a simplified drawing of the network environment used during this testing.

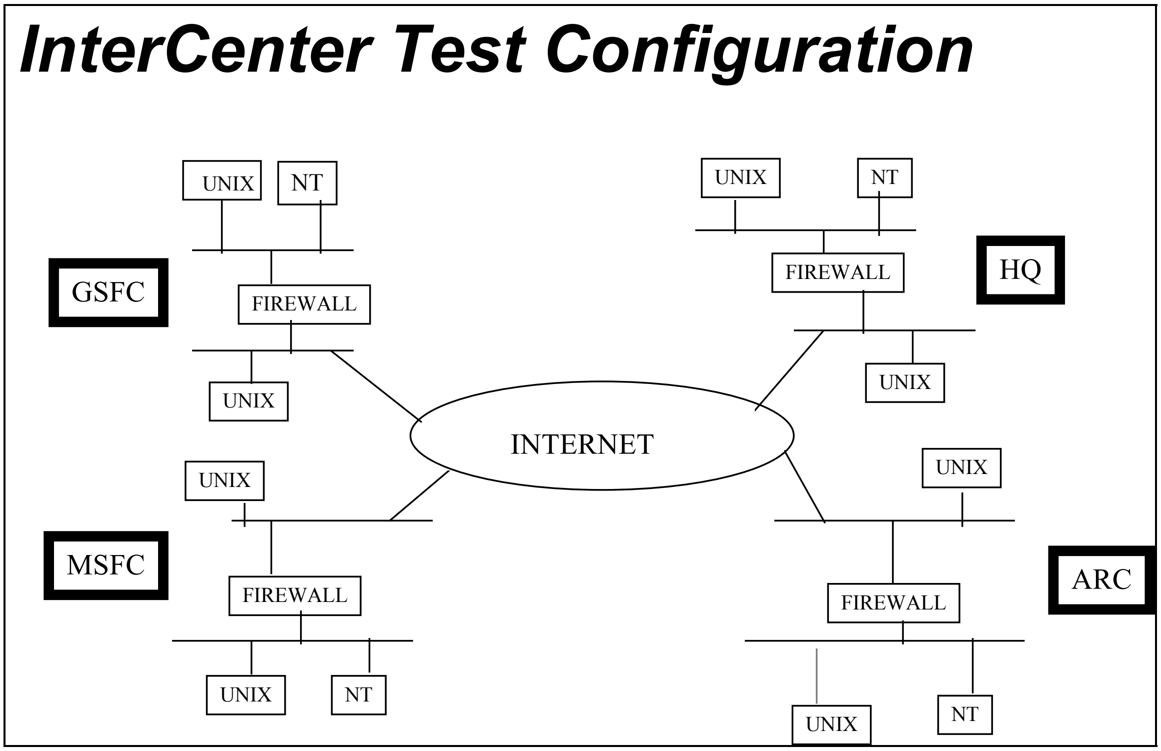

FIGURE 3. Firewall Test Environment

9.2 Testing Methodology. While each center was free to perform testing as required, the following summarizes the common test procedures used at each center.

After Firewalls were installed between the trusted and untrusted networks at each lab, Rules (databases) were then created on the Firewall and were configured to:

- Deny all external traffic to the internal network
- Permit outgoing Telnet and FTP from the internal network
- Permit incoming “authenticated” Telnet and FTP sessions from the external networks
- Establish virtual private networks (VPNs) between Centers

These simple rules allowed the Firewall administrators to run basic tests such as:

- Rules verification (attempting to access protected resources)
- File transfers and Telnet sessions through the Firewall to external resources
- File transfers and Telnet sessions through the Firewall to internal resources (user authentication features)
- File transfers and Telnet sessions through multiple Firewalls between trusted-hosts at different Centers (with and without encrypted VPN sessions)

During the installation, configuration, and testing process, Firewall administrators observed:

- Complexity of installation
- Complexity of the products graphical user interface when creating and modifying rules, VPNs, etc.
- Performance impacts
- Log file features, usability, behavior
- System alerts
- Compatibility/Interoperability issues

(Note: While some centers performed extensive performance testing, E-mail, HTTP, and additional services driven by individual Center requirements, the next phase of this work will require complete testing of all major network services that will be supported by the Firewall implementations. After the Firewall product, or products, has been selected, extensive test will be performed with E-mail, Web servers, File servers, remote access, and other services that will be required in a production environment.)

9.3 Product Recommendation. During the evaluation, Check Point's Firewall-1, Raptor, and Cyberguard were found to be satisfactory products meeting all mandatory Agency requirements. Other discriminating factors were used to determine a single product recommendation. These were obtained from observations accumulated during lab installations and testing.

As a result, there was unanimous agreement between the participating Centers that ***Check Point's Firewall-1*** was the overall product of choice. This recommendation was based largely on product flexibility that enables the product to support a variety of Agency-wide requirements. Again, this choice does not preclude a Center from implementing a different Firewall product that meets the needs of a specific network environment and the mandatory elements of the Features List. For example, Cyberguard's Firewall may be well suited for a project level Firewall where encryption and VPNs aren't required. Thorough consideration, however, should be taken to ensure interoperability with other Agency Firewalls (See Section 6.0). IPsec encryption standards are not complete, therefore VPN between different vendor Firewalls is currently not possible. Most Firewall vendors are participants in the standards committee or are planning to adhere to the standards as they mature. The following sections provide more specific detail on the product evaluations. No particular order of preference is implied.

a. Check Point. This product was extremely flexible in configuration setup and customization. It offers many standard services and possibilities to generate site specific services, therefore allowing a rapid response to a request from a customer. Check Point was the only Firewall evaluated that could be successfully configured to support multiple Meeting-Maker connections (a scheduling package in use at several centers). An unlimited site license for Check Point's VPN software is included with the Firewall. During testing, Check Point also had the smallest latency time. Latency was measured by determining the time it took packets to travel from one UNIX workstation to the other, the number of packets that were transmitted, and the throughput of the packets with the Firewall. Latency was measured from the inside LAN to the outside LAN and back. In other tests, the operator, using a 600 byte packet, increased the number of UDP packets in a transmission from 100 to 1,000,000 to learn what percentage of packets were lost in each size transmission through the Firewall. The smallest loss was with Check Point. Check Point's stateful inspection technology provides a high level of security and full application-layer awareness without requiring a separate Proxy for each service to be secured. This will result in improved performance and the ability to support new and custom applications much more quickly.

b. Raptor. Raptor was an excellent Firewall product and scored high on the features ratings. The primary reason Check Point was chosen over Raptor was due to the application gateway or proxy technology utilized by the product. Raptor does have the capability for an end-user to write site specific Proxies. This capability was tested during evaluation. The process of writing the proxy is fairly straight forward. (An end-user must access 2 screens to create the Proxy.). The Raptor VPN support was impressive; however, the software is sold separately on a per client basis. The results of the UDP test described in the preceding Check Point section showed a higher packet loss for Raptor. There was a 15-25% loss in the lower size transmissions, and even though Raptor was faster, and did a good job at the increased size transmissions, the operational environment requires predominately smaller transmissions.

c. Cyberguard. Cyberguard also proved to be an excellent Firewall product which ranked high on the Features List ratings. The ease of use of the graphical user interface during installation and configuration was outstanding. Cyberguard is very configurable and allows for rapid response. The proxies are easy to use and the rules easy to implement. This Firewall is comparable to Raptor and Check Point. The primary reason Cyberguard was not chosen was due to VPN issues. The Cyberguard software itself does not include VPN software, but support is available via a partnership with Information Resource Engineering, Inc. (IRE). There is currently no Macintosh or WIN95 client support for IRE's encrypted dial-in solutions. Cyberguard could still be considered a good choice for installations that do not require VPN capabilities. IRE solutions are impressive for certain network environments, but combining multiple products in order to provide VPN functionality for the Firewall imposed several limitations and restrictions on the Firewall's setup and limited it's flexibility. Used in combination, these restrictions and limitations would prove very cumbersome.

d. V-One. V-One was not chosen as a satisfactory product. Technically, V-One is a solid product on a BSDI platform. Operationally it was difficult to configure. An HTTP interface was provided for remote configuration only. Software products like Meeting Maker required a "hole" to be supported. VPN software was sold on a per client basis, and proved unstable. Key management was fully manual. Configuration difficulties by all NASA parties evaluating the product, in addition to the low features rating are responsible for its rejection.

# APPENDIX A

# FIREWALL HOST SECURITY

A1. Firewall Host Security. A host running a Firewall application is expected to take the extra precautions that the security world has deemed prudent for all hosts that reside on a network that is accessible either directly or indirectly via known interfaces or vulnerabilities. The precautions to be undertaken are supposed to protect the host against illegal access via unprotected accounts that should have been disabled, unneeded services left enabled, or unauthorized access via known vulnerabilities that have not been corrected. These hosts are also susceptible to eavesdropping, ip address spoofing, source routing, icmp redirects, sync flooding, and TCP connection spoofing unless protections are taken

Securing the Firewall host can be done by disabling or eliminating unneeded accounts, changing file permissions and eliminating unneeded root ownership, eliminating unneeded services, protecting enabled services, tightening the kernel, and providing good logging that is continually reviewed.

A center may bypass the concern about the host security by selecting a Firewall product that has been certified by one of the authorized certification centers such as NCSA, NSA, CSI, ITSEC, or their approved test partners. Buying a certified Firewall does not preclude the need to test the implementation for vulnerabilities by running Internet Security Scanner (ISS) and/or doing penetration testing.

A1.1 Accounts. Some accounts have been set up by the vendor as the owners of a particular device or “daemon”. They are still provided in the operating system with no passwords, which are exploited by attackers familiar with breaking out of a shell and gaining root access. These accounts need to be disabled. The passwords should indicate the accounts are locked and the shell should indicate “/bin/true” so that no remote access activity can occur using these user ids. For a Firewall, all unnecessary accounts need to be eliminated. There should be at most a security or system “admin” account, in addition to the root, and other daemon type accounts needed by the operating system. Normal users do not need access to the Firewall.

A1.2 Files and Programs. The vendor still provides many files and services set with no passwords, vulnerable permissions, or with unnecessary root ownership. This can open up the possibility of illegal access if a service vulnerability, such as buffer overflow, is exploited and a user is able to gain root access. There will always be buffer overflow and other vulnerabilities uncovered until the operating system software undergoes more rigorous quality assurance standards that have been impressed on NASA’s software developers in the past.

To make this task easier to accomplish, there are some freeware software programs such as Cops, Tripwire, and Tiger. These programs are accessible via the web and ftp sites. Cops scans the files for the unnecessary file permissions and ownerships. Tripwire scans the system files for any changes that may indicate file tampering. Tiger is another program like Cops but it scans other files. All three of these programs can be set up to run via a “cron” job daily or weekly. Their output can be sent to logs or a mail address.

A1.3 Services and Ports. Unnecessary and vulnerable services should be assessed for risks and precautions taken. Firewall products usually provide service proxies which add an additional protection layer with authorization and authentication as well as logging of the session. Some services that may utilize the proxies should still never be run on the Firewall itself. Services, such as a mail server, a web server, a web browser, and a FTP server, are all services that are subject to many vulnerabilities, and need careful configurations.

Rather than running sendmail on the Firewall, configure an internal mail server and an external mail server. All mail, destined for internal systems/users, would be delivered to the external mail server, and this mail server could then forward the mail t to the internal mail server. The internal mail server could send the external mail out without having to forward it to the external mail host. The SMTP service would only need to be enabled to forward mail from the external mail host to the internal mail host. Before the forwarding takes place, the external mail server could even be set up to scan any attached files for possible viruses or Trojan horses.

Utilizing a split DNS provides a way for the internal hosts to resolve external host names, and for the Firewall to resolve internal host names. An external DNS server would reside on the Firewall and would only advertise internal hosts that are allowed access from external users. This type of internal hosts would include hosts running ftp servers, web servers, and the internal mail relay software. The external DNS server would have to resolve internal host names without sending a query to the internal DNS server. An internal DNS server would reside on an internal host and all internal hosts would send their queries to the internal DNS host. If the internal DNS host could not resolve them internally, this server would send queries to the external DNS server on the Firewall, which would send the resolutions back to the internal DNS server for forwarding to the internal host

If implementing an anonymous FTP server, put its system files, programs and devices on a separate disk partition. A separate password file with only root and ftp as users is needed. The login shell for the ftp user should be set to /bin/true so that there are no attempts to login to the system using this user ID. It is not advisable to allow uploads (put) to the FTP server; however, if this is necessary then have the uploaded files written to a separate sub-directory and do not allow these files to be downloaded (get) by other users, overwritten, or even seen by others, until they have been scanned and moved to the proper directory where other files are available.

The services themselves need to be placed on a host either in front of or behind the Firewall, depending on the security policy for that site. In addition, services, such as NFS, NIS, RPC-based services, TFTP, RIP, finger, r-command type services, and Boot services, should be examined and assessed for need before enabling. Turn off the unneeded boot servers enabled at boot time (in the /etc/rc.* or equivalent files), turn off excess servers (in the /etc/inet/inetd.conf or equivalent file), check what processes are running (using the ps or equivalent command), what network sockets are running (using the netstat or equivalent command). If possible, comment all services at boot time except inetd, and syslogd. The only processes running without network traffic would be inetd, syslogd, cron, update, sh, and a few others related to the operating system.

Doing one’s own port scan of the Firewall host itself can uncover what unnecessary services are enabled. The ports for these services should also be disabled. It’s best to scan one’s self and disable unneeded services, before others do the scanning of the ports. All hosts, including the Firewall need to be able to detect any type of port scanning or login fishing expeditions. Some Firewalls will inform the operators when they are subject to a port scan. Port scans are done by attackers to determine what services are active so they can initiate the known vulnerabilities for that particular service.

There are some freeware products, such as Satan and ISS that will scan the hosts and the network for vulnerabilities, separate from the ones detected with the other host scanning software mentioned earlier. There are also a number of commercial products available that can perform these scans, checking for additional vulnerabilities. Commercial products, such as Pingware and ISS (an expanded version) have the added benefit of being maintained and usually provide updated versions throughout the software maintenance period.

A1.4 Tightening the Kernel. If the workstation was used before, third party software and unneeded software should be removed. Some Firewall products, such as Cyberguard, replace the kernel with one of their own, which controls changes to its secure operating system. Installing TCP Wrappers, a proxy-type freeware software program, will perform some access control and logging and provide the means to display the required Government warning banner.

Disabling packet filtering in the kernel allows the Firewall to control the packet flow, which is an important function of a Firewall that is trying to control access and authenticate the users allowed access.

There is freeware software known as ip_filt that can be used on the gateway as well as on any host, especially the bastion hosts. Ip_filt provides logging, packet sequencing and fragmentation checking, checks for established sessions, and can distinguish interfaces. Ip_filt supports Solaris, SunOS, NetBSD, FreeBSD, and BSD/OS, as well as network address translation.

If there are network management hooks or SNMP interfaces and they are not being used, then disable them. Ipforwarding should be disabled.

The use of one-time passwords is preferred, and definitely no remote logins to the Firewall by the administrator, unless the entire session is encrypted.

A1.5 Logging and Delogging. Good logging and delogging functions are usually provided with the Firewall host. Usually the Firewall itself will have one or more logs that can be accessed or scanned for one or more reduction type parameters (ex. Source ip address, time span, service type, rule failure, etc.) In addition, the operating system itself will have one or more logs (ex. syslog, messages, console log, sulog, daemon.log, etc.) concerning overall system activity that can be reviewed separately using scanning tools for delog reductions. Swatch is a freeware delog software, available via the web or ftp, which provides delog capability and log management for accessing the logs for possible vulnerabilities.

It is best to have logs for a network contained on one log host so that it can be managed with tighter security. This logging host could be a highly stripped-down workstation that would limit its services to accepting log data, and its logs could only be accessible via console login. The logs would not be deleted if the log file(s) were filled. The logging function would denote the need for some action by the operator when a log was a certain percentage full. If one is really concerned about the logs being altered or deleted, the logs could also be output to a high speed line printer or to a one-time only writeable CD-ROM, but this could lead to a higher cost for a risk that could be acceptable with a more secured logging host.

A1.6 Additional Steps. Test the host against the security policy in place to determine if there are any inaccurate configurations. It is also recommended the use of a commercial Internet security scanning program, such as Internet Security Scanner (ISS) for Firewalls. The advantage of using a commercial scanner is its ease of use and its multiple updates during a warranty period. The updates are based on newly reported vulnerabilities and maintenance changes in the software.

Protecting a host against unknown vulnerabilities is not always possible; however, there are steps that can be taken to ensure that one is able to take action once a new vulnerability is uncovered. The operating system of all hosts, not just the one running the Firewall needs to keep the security patches up-to-date to prevent a new known vulnerability from being exploited. Patches from the Firewall vendor should be installed when supplied. The logs need to be scanned daily and new or unusual occurrences reviewed. Subscribing to newsgroups on UNIX vulnerabilities is a good way to become aware of new vulnerabilities uncovered. NASIRC and CERT are organizations that report the vulnerabilities, provide workarounds, and indicate the ftp locations to obtain the fixes.

Since it may not always be possible to prevent an unauthorized user from accessing your host or network, it would be good at least to be aware of when it occurs and try to contain the damage, if any, or preserve any evidence of intrusion for later review. Some experts suggest utilizing an old PC whose function would be to report any host access. Having a “tempting morsel” on the network is one way of determining if someone is snooping around.

A sniffer could also be set up behind the Firewall to scan all network traffic and send an alert if it detects something either got through the Firewall or around it. The host running the sniffer would contain the inverted versions of the Firewall’s rules.