DEPERTMENT OF VETERANS AFFAIRS
Washington, DC 20420

VA HANDBOOK 6500.11
Transmittal Sheet
August 22, 2017

VA FIREWALL CONFIGURATION

1. REASON FOR ISSUE: This document establishes a baseline for secure external connection via ports that are allowed between the Department of Veterans Affairs (VA) internal network and other (non-VA) networks, including the Internet. In addition, this document defines the approved use for each port, as well as the baseline firewall capabilities to which traffic on each port will be subjected. Port restrictions are a component of larger, all-encompassing firewall configuration and this Handbook needs to be applied consistent with other VA Office of Information and Technology (OI&T) policy. VA firewall configurations must comply with the provisions of Federal Information Security Moderization Act (FISMA) and other related information security requirements promulgated by the National Institute of Standards and Technology (NIST) and the Office of Management and Budget (OMB) as referenced in Appendix C.

2. SUMMARY OF CONTENTS/MAJOR CHANGES: This Handbook identifies the security policies designed to establish secure interconnections of the VA internal network to any other external networks, and provides the current external facing firewall configuration settings which minimize the security risks to Veteran's data while maintaining the ability of the VA to fulfill its mission and provide service to the Veteran community.

3. RESPONSIBLE OFFICE: The Office of the Assistant Secretary for Information and Technology (005), Information Security (005R), Cyber Security Policy and Compliance (005R2) is responsible for the security content.

4. RELATED DIRECTIVE: VA Directive 6500, Managing Information Security Risk: VA Information Security Program and VA Directive 6004, Configuration, Change, and Release Management Programs.

5. RESCISSIONS: None

CERTIFIED BY:

/s/
Dat P. Tran
Acting Assistant Secretary for
Office of Enterprise Integration

BY DIRECTION OF THE SECRETARY OF VETERANS AFFAIRS:

/s/
ROB C. THOMAS, II
Acting Assistant Secretary for
Information & Technology and Chief
Information Officer

Distribution: Electronic Only

This page is intentionally blank for the purpose of printing front and back copies.

VA FIREWALL CONFIGURATION

CONTENTS

PARAGRAPH PAGE

APPENDICES PAGE

This page is intentionally blank for the purpose of printing front and back copies.

VA FIREWALL CONFIGURATION

1. PURPOSE

a. This Handbook establishes a baseline for secure external connection via ports that are allowed between the VA internal network and other (non-VA) networks, including the Internet. In addition, this Handbook defines the approved use for each port, as well as the baseline firewall capabilities to which traffic on each port will be subjected. Port restrictions should be a component of a larger, all-encompassing firewall configuration.

b. VA firewall configurations must comply with the provisions of FISMA and other related information security requirements promulgated by NIST and OMB.

2. SCOPE

a. This Handbook identifies the security policies designed to establish secure interconnections of the VA intranet to any other external networks, and provides the current external facing firewall configuration settings which minimize the security risks to Veteran's data while maintaining the ability of the VA to fulfill its mission and provide service to the Veteran community. The handbook also documents the roles and responsibilities of VA organizations.

b. This Handbook is intended for VA firewall systems administrators, vendors hosting VA systems, the Office of Acquisition Operations, the Technology Acquisitions Center, VA information technology customers, VA senior leadership, and external network administrators responsible for implementing security policy standards for the security of VA information systems.

3. BACKGROUND/OVERVIEW

a. The security of VA information and information systems is vital to the success of VA’s mission. External networks constitute a major source of threats to the security of VA intranet.

b. To improve the effectiveness and security of firewalls, NIST 800-41 Special Publication (SP) Rev. 1, *Guidelines on Firewalls and Firewall Policy,* recommends that agencies create a firewall policy that specifies how firewalls manage inbound and outbound network traffic.

c. VA OI&T is responsible for developing, approving and implementing, and system security baseline configurations for all VA platforms and systems. OI&T also leverages existing standards and best practices, where available, and tailors specifications for the VA environment. All standard, non-standard, custom-developed, and single instance platforms and applications are required to have an established baseline configuration from which to measure compliance and to assist Office of Cyber Security (OCS) with determining the overall security compliance of the system.

d. VA firewall baselines must adhere to standards set by Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB), and Defense Information Systems Agency Security Technical Implementation Guides (DISA STIG) where these standards apply. In cases where standards, guidance, or best practices do not exist to assist with developing a secure baseline configuration, Information Technology Operations and Services (ITOPS) will collaborate with Office of Information Security (OIS) to develop, test, and implement an agreed-upon baseline.

4. POLICY AND PROCEDURES

a. Information Flow and Boundary Protection

(1) As stated in VA Handbook 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program,* information flow enforcement regulates where information is allowed to travel within or between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. VA will use information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path.

(2) Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that use rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or provide message-filtering capability based on content (e.g., using key word searches or document characteristics relating to privacy and security).

(3) OI&T will use boundary protection mechanisms to separate information system components supporting missions and/or business functions. Mechanisms include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks).

b. Configuration

(1) In accordance with VA Directive 6004, *Configuration, Change and Release Management Programs*, and in support of public law and other Federal guidance, each VA system owner must document, implement, and maintain configuration, change, and release management plans and processes.

(2) ITOPS establishes and documents configuration setting parameters that can be changed in hardware, software, or firmware components of the information system that affect the security posture and/or functionality of the system. Information Technology (IT) products for which security-related configuration settings can be defined include, mainframe computers, servers (e.g., database, email, authentication, web, proxy, file, domain name), workstations, input/output devices (e.g., scanners, copiers, and printers), network components (e.g., firewalls, routers, gateways, voice and data switches, wireless access points, network appliances, sensors), operating systems, middleware, and applications. Security-related parameters include the registry settings account, file, and directory settings

(i.e., permissions); and settings for services, ports, protocols, services, and remote connections.

(3) Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to the configuration settings for IT products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities.

(4) Prior to a firewall being configured to support a specific application, system, or service, all required documentation must be submitted to and approved by the Enterprise Security Change Control Board (ESCCB).

c. **Authorized Ports, Protocols, and Services**

(1) A validated VA business process needing an external port requires OI&T policy adherence for authorization of ports, protocols and services. Appendix D, *Outbound Initiated Authorized Ports, Protocols, and Services,* and Appendix E, *Inbound-initiated Authorized Ports, Protocols, and Services*, provide identification of services and ports that are allowed as constrained by their respective configuration directions. An outbound-initiated connection is a flow (source/destination Internet Protocol [IP] and port) where the first packets establishing the flow are sent from a VA host to the outside world. An inbound-initiated connection is a flow where the first packets establishing the flow are sent from a host outside of the VA to a host within the VA. If the port is being used for the Internet Assigned Numbers Authority (IANA) registration purpose, no ESCCB approval is required.

Note 1: *Refer to Appendix F, Terminology Key, for Appendix D and Appendix E firewall services applied terminology.*

(2) If the service and port is not being used for the IANA-registered purpose, and/or if the respective configuration directions cannot be followed, ESCCB approval must be requested.

Note 2: *IANA information may be retrieved from http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml*

(3) Source, destination, and applied firewall services are from the perspective of the edge VA Firewall and are not intended to indicate configuration on any particular firewall device.

(4) Outbound-initiated Authorized Ports, Protocols, and Services include the following:

(a) World Wide Web Hypertext Transfer Protocol (HTTP), Transport Protocol Transmission Control Protocol (TCP), Port 80

1. Used in communications between Web browsers and Web servers.

2. Outbound HTTP session requests to external servers must be proxied at the external gateway. A content filter must be employed to prevent the accessing of objectionable sites.

3. HTTP sessions exchanging sensitive information must be encrypted (e.g., Transport Layer Security [TLS]) if transferred over public networks (e.g., the Internet). If encrypted packets are passed through the gateway, appropriate protections must be implemented at the internal encryption/decryption point to accomplish all bypassed gateway security functions.

4. Similar security measures must be implemented on alternative HTTP ports (e.g., 8080) and vendor specific HTTP implementations assigned to different ports, if used.

(b) HTTP Protocol over TLS, Transport Protocol TCP, Port 443

1. HTTPS is used in secure (encrypted) communications between Web browsers and Web servers.

2. If encrypted packets are passed through the gateway, appropriate protections must be implemented at the internal encryption/decryption point to accomplish all bypassed gateway security functions.

(5) Inbound-initiated Authorized Ports, Protocols, and Services include the following:

(a) Simple Mail Transfer Protocol (SMTP), Transport Protocol TCP, Port 25

1. Transfers mail messages between systems. SMTP can be exploited to facilitate mail bombing, mail spamming, and denial of service attacks.

2. All SMTP-based mail must be proxied at the external gateway.

3. Internal SMTP traffic to and from the gate way must be limited to specifically identified internal mail servers.

4. All external requests to route mail to other external addresses must be blocked.

5. All (unencrypted) inbound and outbound mail will be scanned for malicious code at the gateway (Note: Secure/Multipurpose Internet Mail Extensions [S/MIME] encryption of email will inhibit malicious code scanning of email in transit).

(b) Domain Name Server (DNS), Transport Protocol TCP, Port 53

1. DNS matches IP addresses to hostnames (and vice versa).

2. Clients make requests of the DNS servers when they want to communicate with systems for which they have only the fully qualified host name.

3. DNS poisoning could result in denial of service or redirection of network traffic to an unintended (unauthorized) destination.

4. For security, a “split” DNS configuration must be implemented that consists of internal DNS servers and externally facing DNS servers.

5. The internal servers resolve queries from host machines on internal networks and forwards queries for external name resolution to the externally facing DNS servers.

6. The externally facing DNS servers must be security hardened. They resolve queries from the internal DNS server and present a restricted DNS database to external systems.

7. Inbound and outbound DNS queries must be restricted to specially identified externally facing DNS servers.

(c) DNS, Transport Protocol User Datagram Protocol (UDP), Port 53

1. DNS matches IP addresses to hostnames (and vice versa).

2. Clients make requests of the DNS servers when they want to communicate with systems for which they have only the fully qualified host name.

3. DNS poisoning could result in denial of service or redirection of network traffic to an unintended (unauthorized) destination.

4. For security, a “split” DNS configuration must be implemented that consists of internal DNS servers and externally facing DNS servers.

5. The internal servers resolve queries from host machines on internal networks and forwards queries for external name resolution to the externally facing DNS servers.

6. The externally facing DNS servers must be security hardened. They resolve queries from the internal DNS server and present a restricted DNS database to external systems.

7. Inbound and outbound DNS queries must be restricted to these specially identified externally facing DNS servers.

(d) World Wide Web HTTP (HTTP), Transport Protocol TCP, Port 80

1. Used in communications between Web browsers and Web servers.

2. VA information intended to be publicly available must be placed on a security hardened web server within a Demilitarized Zone (DMZ) isolated from the VA internal network.

3. Inbound HTTP session requests must be restricted to specifically identified internal web servers and must be “reverse proxied” at the boundary between the VA intranet and the Internet.

4. HTTP sessions exchanging sensitive information must be encrypted (e.g., TLS) if transferred over public networks (e.g., the Internet). If encrypted packets are passed through the gateway, appropriate protections must be implemented at the internal encryption/decryption point to accomplish all bypassed gateway security functions.

5. Similar security measures must be implemented on alternative HTTP ports (e.g., 8080) and vendor specific HTTP implementations assigned to different ports, if used.

(e) HTTP Protocol over TLS, Transport Protocol TCP, Port 443

1. HTTPS is used in secure (encrypted) communications between Web browsers and Web servers.

2. If encrypted packets are passed through the gateway, appropriate protections must be implemented at the internal encryption/decryption point to accomplish all bypassed gateway security functions.

d. Protocol and Port Cross Reference

Protocols, approaches, and reference sources are as follows:

(1) In Appendix G, *Ports, Protocols, and Services Requiring ESCCB Approval*, a list of protocols and ports is provided that can be allowed if given authorization by the ESCCB.

(2) After ESCCB authorization is granted, the constraints in Appendix G should be used to configure the rule. If the protocols and ports are to be used for a purpose other than listed in this appendix, the intended use must be justified in writing and will factor into the ESCCB decision.

(3) Appendix G represents protocols and ports commonly used within VA. Other protocols and ports may be authorized by ESCCB on a case-by-case basis.

(4) Source, destination, and applied firewall services in Appendix G are from the perspective of the Trusted Internet Connection (TIC) and are not intended to indicate configuration on any particular firewall device.

5. RESPONSIBILITIES

The responsibilities listed below are specific responsibilities related to VA firewall configuration management. For overall information security program responsibilities for these positions, see VA Directive and Handbook 6500.

a. **Assistant Secretary for Information and Technology**, as VA's Chief of Information Officer (CIO), is responsible for:

(1) Assuming the responsibility, as the Authorizing Official (AO), to ensure information systems operate at an acceptable level of risk;

(2) Designating a Chief Information Security Officer (CISO);

(3) Developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements;

(4) Overseeing OI&T personnel with significant responsibilities for information security, and ensuring that personnel are adequately trained;

(5) Assisting senior VA officials concerning their security responsibilities;

(6) Coordinate information technology policy and operations with other senior officials; and,

(7) Report annually to the Secretary of VA on the overall effectiveness of VA's information security program, including progress of any remediation.

b. **Deputy Assistant Secretary for Information Security**, (DAS OIS), created under the IT single authority by the VA CIO, is responsible for:

(1) Establishing, coordinating, maintaining, and monitoring Department-wide information security policies, procedures, control techniques, training, and inspection requirements as elements of the Department information security program;

(2) Providing oversight and guidance for VA compliance with applicable privacy and confidentiality laws, regulations, and policies, including the Privacy Act, 5 United States Code (U.S.C.) § 552a, and 38 U.S.C. §§ 5701, Confidential Nature of Claims, Health Insurance Portability and Accountability Act (HIPAA), 38 U.S.C. § 5705, Confidentiality of Medical Quality-Assurance Records, and 38 U.S.C. § 7332, Confidentiality of Certain Medical Records;

(3) Providing guidance and procedures for protecting information as required by 38 U.S.C. §§ 5721-5728 , Veterans' Benefits, Information Security; and

(4) Actively monitoring all VA network intrusion detection sensors, firewall alerts, network operations, security logs for abnormal activity, attempted intrusions/ compromises, and other manners of security alerts that may be generated; follow up as appropriate to minimize the impact of security incidents on VA information systems.

c. **Director, Office of Cyber Security Policy and Compliance** is responsible for:

(1) Developing and coordinating the implementation and maintenance of VA information security policies and procedures consistent with Federal laws and VA policies; and

(2) Reviewing VA information security policies and procedures related to information security across VA organizations to provide assistance and guidance as well as to ensure compliance.

d. **The Enterprise Program Management Office (EPMO**) is the system owner for all mission IT systems and is responsible for the duties of the system owner for these systems.

e. **Deputy Chief Information Officer for Service Delivery and Engineering and Information System Owners** (ISOs) are responsible for the overall procurement, development, integration, modification, daily operations, maintenance, and disposal of VA information and information systems, including:

(1) Acting as the ISO for General Support Systems (GSS) and is responsible for working with all VA organizations to ensure the security of the system;

(2) Providing appropriate access to VA systems (including types of privileges or access), in coordination with VA managers and ISOs;

(3) Ensuring compliance with Federal security regulations and VA security policies;

(4) Ensuring the system is deployed, maintained, and operated in accordance with the agreed-upon security controls;

(5) Developing and maintaining an IT system Configuration, Change, and Release Management Plan;

(6) Ensuring system users and support personnel receive required security training;

(7) Assisting the local system administrators in the identification, implementation, and assessment of security controls; and

(8) Ensuring compliance with the Enterprise and Security Architecture throughout the system life cycle.

f. **Information System Owners** are responsible for:

(1) Determining system design based on security and business requirements and must include system/security design, interfaces, design documents, and lower-level system development documentation;

(2) Reviewing the information system to identify unnecessary and/or non-secure functions, ports, protocols, and services, and disables functions, ports, protocols, and services within the information system deemed to be unnecessary and/or non-secure; and FISMA Controls (CM-7) (SI-4) (SI-4 (4)) (SI-8)

(3) Designing and developing an acceptable security control baseline for each information system, system component, or information system service appropriate to the impact level of the system. Control (SA-4)

g. **Enterprise Security Configuration Control Board (ESCCB)** consists of representation from Enterprise Operations & Field Development, Office of Enterprise Development, Information Protection and Risk Management, IT Resource Management, lines of business representatives, Change Managers, and Enterprise Strategy, Policy, Plans, & Programs. ESCCB is responsible for:

(1) Reviewing all changes proposed to external connections that involve VA network resources within 10 business days to ensure changes are viable from technical, security and privacy standpoints;

(2) Validating all proposed external connection changes do not adversely impact the operation or security of the existing system or subsystem;

(3) Certifying that any external connection complies with Federal and VA policies and procedures;

(4) Maintaining an accurate inventory of all external connection Request for Comments (RFCs) and their status;

(5) Coordinating with all key stakeholders to provide written guidance and procedures via VA User Guides and Standard Operating Procedures (SOPs);

(6) Escalating RFCs to higher boards for review and approval per the board's escalation criteria and VA Directive 6004, Configuration, Change and Release Management Programs; and

(7) Providing security configuration services to VA clients.

h. **Network and Security Operations Center (NSOC)** is responsible for:

(1) Evaluating external connection RFCs for impact (security or otherwise) at the gateways and Internet Protocol (IP) address/port security settings;

(2) Providing recommendations, based on the VA NSOC team's evaluation of the RFCs, to the ESCCB voting membership through the appropriate venue;

(3) Participating as a voting member of the ESCCB;

(4) Implementing the external connection changes once approved by ESCCB;

(5) Monitoring all external connections for compliance with existing federal laws and VA policies; and

(6) Ensuring all external connections are in compliance with the TIC 2.0. All external connections to the internet must be through a TIC gateway.

Appendix A. TERMS AND DEFINITIONS

1. **Anti-spam (AS):** The firewall reduces the occurrence of illegitimate email through context-sensitive spam detection.

2. **Anti-spyware (AW):** The firewall performs layer 7 inspection and blocks known spyware signatures.

3. **Anti-virus (AV) Software:** A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents. SOURCE: NIST SP 800-83. The firewall performs layer 7 inspection and blocks known virus signatures.

4. **Application Identification (AI):** The firewall determines the layer 7 application in use, can apply policy based on this identification, and can log based on this identification.

5. **Application-Proxy Gateway:** A firewall capability that combines lower-layer access control with upper layer-functionality, and includes a proxy agent that acts as an intermediary between two hosts that wish to communicate with each other. SOURCE: NIST SP 800-41

6. **Demilitarized Zone (DMZ):** An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. SOURCE: NIST SP 800-41

7. **Data Filtering (DF):** The firewall blocks data streams containing pre-defined character strings that are administratively prohibited (for example, social security numbers).

8. **File Blocking (FB):** The firewall blocks the transfer of files that are administratively prohibited.

9. **Firewall:** A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures. SOURCE: NIST SP 800-41, CNSSI-4009

10. **General Support Systems (GSS):** interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people. SOURCE: OMB Circular A-130, Appendix III,

11. **Geographic IP (GI):** The firewall permits or denies traffic based on location of traffic origin or destination. Location is determined based on IP-to-locale database.

12. **Inbound-Initiated:** Traffic initiated from outside of the VA and directed to the VA.

13. **Information System Owner:** Official responsible for the overall procurement, development, integration, modification, daily operations, maintenance, and implementation of security over VA information and information systems.

14. **IP Blacklist (IB):** The firewall blocks all communication to and from IP addresses on the IP blacklist. The blacklist is maintained by VA Enterprise Network Defense (END).

15. **Mission IT System:** Any IT system in the organization which is essential to business operation or supports the organization's core processes or functions

16. **Outbound-Initiated:** Traffic initiated from inside the VA and directed outside of the VA.

17. **Packet Filter:** A routing device that provides access control functionality for host addresses and communication sessions. SOURCE: NIST SP 800-41

18. **Proxy Server:** A proxy server is a computer that offers a computer network service to allow clients to make indirect network connections to other network services. A client connects to the proxy server, then requests a connection, file, or other resource available on a different server. SOURCE: CNSSI-4009

19. **Reputation Filtering (RF):** The firewall validates blocks email from senders with poor track records for sending spam.

20. **Restricted:** Only a finite list of IP addresses is allowed.

21. **Sender Policy Framework (SP):** The firewall protects against email spoofing by verifying that incoming mail was delivered by a host authorized by the administrators of the sender.

22. **Stateful Inspection (SI):** Packet filtering that also tracks the state of connections and blocks packets that deviate from the expected state. SOURCE: NIST SP 800-41. The firewall tracks the connection from start to finish and ensures all packets are valid.

23. **System Owner:** Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. SOURCE: CNSSI 4009

24. **Transmission Control Protocol (TCP):** TCP is the protocol that major Internet applications such as the World Wide Web, email, remote administration and file transfer rely on. Applications that do not require reliable data stream service may use the User Datagram Protocol (UDP), which provides a connectionless datagram service that emphasizes reduced latency over reliability. SOURCE: DARPA RFC 793

25. **Trusted Internet Connection (TIC):** A secure connection between and agency system and an external system routed through an approved TIC gateway. SOURCE: OMB Memorandum M-08-05

26. **Unrestricted:** Any IP address is allowed. In the context of outbound-initiated traffic, it is understood that an unrestricted source address falls within the 10.0.0.0/8 address range.

27. **URL Filtering (UR):** The firewall allows or denies HTTP or HTTPS connections to a website based on an administrative policy of allowed and denied URL categories.

28. **User Datagram Protocol (UDP):** UDP is defined to make available a datagram mode of packet-switched computer communication in the environment of an interconnected set of computer networks. This protocol assumes that the Internet Protocol (IP) is used as the underlying protocol. SOURCE: DARPA RFC 760

29. **VA System Owner:** This official must document, implement, and maintain configuration, change, and release management plans and processes.

30. **Vulnerability (VU):** The firewall scans traffic and blocks attempts to exploit system flaws or gain unauthorized access to systems.

31. **Web Application Firewall (WA):** The firewall fronts connections to VA-operated web servers and protects against web-specific attacks such as cross-site scripting, SQL-injection, and cookie poisoning.

This page is intentionally blank for the purpose of printing front and back copies.

Appendix B. ACRONYMS AND ABBREVIATIONS

Acronym/ Abbreviation	Definition
ACL	Access Control List
AH	Authentication Header
ANSI	American National Standards Institute
AO	Authorizing Official
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CM	Configuration Management
DAS	Deputy Assistant Secretary
DICOM	Digital Imaging and Communications in Medicine
DISA STIG	Defense Information Systems Agency Security Technical Implementation Guides
DMZ	Demilitarized Zone
DNS	Domain Name Service
Email	Electronic Mail
EPMO	Enterprise Program Management Office
ESCCB	Enterprise Security Change Control Board
ESP	Encapsulating Security Payload
FDCC	Federal Desktop Core Configuration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GRE	Generic Routing Encapsulation
GSS	General Support Systems
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
HTTP	Hyper Text Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICA	Independent Computing Architecture
ICMP	Internet Control Message Protocol
ID	Identification
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPSEC	Internet Protocol Security
ISAKMP	Internet Security Association and Key Management Protocol
ISO	Information Security Officer

Acronym/ Abbreviation	Definition
IT	Information Technology
ITOPS	Information Technology Operations and Services
L2F	Layer 2 Firewall
LDAP	Lightweight Directory Access Protocol
NAS	Network Attached Storage
NIST	National Institute of Standards and Technology
NNTP	Network News Transfer Protocol
NSOC	Network Security Operations Center
OCS	Office of Cyber Security
OIS	Office of Information Security
OI&T	Office of Information and Technology
OMB	Office of Management and Budget
OSPF	Open Shortest Path First
PPTP	Point-to-Point Tunneling Protocol
POP	Post Office Protocol
PVT	Patch and Vulnerability Team
RFC	Request for Comments
RSS	Rich Site Summary
S/MIME	Secure/Multipurpose Internet Mail Extensions
SA	Security Associations
SDLC	System Development Life Cycle
SMTP	Simple Mail Transfer Protocol
SNPP	Simple Network Paging Protocol
SOP	Standard Operating Procedure
SP	Special Publication
SQL	Structured Query Language
SSH	Secure Shell
SSP	System Security Plan
TCP	Transmission Control Protocol
TIC	Trusted Internet Connection
TLS	Transport Layer Security
TLSP	Transport Layer Security Protocol
TTL	Time-to-Live
UDP	User Datagram Protocol
U.S.C.	United States Code
USGCB	United States Government Configuration Baseline
VA	Department of Veterans Affairs

Acronym/ Abbreviation	Definition
VA-NSOC	Veterans Affairs Network Security Operations Center
VPN	Virtual Private Network
WMP	Windows Media Player
WMS	Windows Media Server

Appendix C. REFERENCES

1. National Institute of Standards and Technology (NIST) Special Publications (SP)

a. NIST SP 800-41 Rev. 1, *Guidelines on Firewalls and Firewall Policy*

b. NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*

c. NIST SP 800-53, *Security and Privacy controls for Federal Information systems and Organizations*

2. VA Directives and Handbooks

a. VA Directive 6500, *Risk Management Framework for VA Information Systems – Tier 3: VA Information Security Program*

b. VA Handbook 6513, *Secure External Connections*

3. Other References

a. 44 U.S.C. § 3541-3549, Federal Information Security Management Act of 2002

b. Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information *Systems*

c. Office of Management and Budget (OMB) Circular A-130, *Appendix III, Security of Federal Automated Information Resources*

This page is intentionally blank for the purpose of printing front and back copies.

Appendix D. AUTHORIZED OUTBOUND PORTS, PROTOCOLS & SERVICES

Transport Protocol	Port	IANA-registered Service Name	IANA Description	VA Use	Source	Destination	Firewall Services Applied
TCP	80	http	World Wide Web HTTP	HTTP	unrestricted	unrestricted	GI, SI, AV, AW, VU, FB, DF, UR, AI, IB
TCP	443	https	http protocol over TLS	HTTPS	unrestricted	unrestricted	GI, SI, UR, AI, IB

This page is intentionally blank for the purpose of printing front and back copies.

Appendix E. AUTHORIZED INBOUND PORTS, PROTOCOLS & SERVICES

Transport Protocol	Port	IANA-registered Service Name	IANA Description	VA Use	Source	Destination	Firewall Services Applied
TCP	25	smtp	Simple Mail Transfer	Mail Transfer	unrestricted	restricted	GI, SI, AV, AW, VU, FB, DF, AI, IB, SP, RF
TCP	53	domain	Domain Name Server	DNS - TCP	unrestricted	restricted	GI, SI, AV, AW, VU, FB, DF, AI, IB
UDP	53	domain	Domain Name Server	DNS - UDP	unrestricted	restricted	GI, SI, AV, AW, VU, FB, DF, AI, IB
TCP	80	http	World Wide Web HTTP	HTTP	unrestricted	restricted	GI, SI, AV, AW, VU, FB, DF, WA, AI, IB
TCP	443	https	http protocol over TLS	HTTPS	unrestricted	restricted	GI, SI, WA, AI, IB

This page is intentionally blank for the purpose of printing front and back copies.

Appendix F. PORTS, PROTOCOLS, & SERVICES REQUIRING ESCCB APPROVAL

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	22	ssh	The Secure Shell (SSH) Protocol	GI, SI, AI, IB

Discussion: SSH is a method of performing client authentication and safeguarding multiple service sessions between two systems. SSH can be combined with other services (such as File Transfer Protocol [FTP] and telnet) to provide authentication and confidentiality to otherwise insecure processes. In bound sessions must be restricted to specifically identify internal network devices. If encrypted packets are passed through the gateway, appropriate protections must be implemented at the internal encryption/decryption point to accomplish all bypassed gate way security functions.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
UDP	53	dns	Domain Name Server	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: DNS matches IP addresses to hostnames (and vice versa). Clients make requests of the DNS servers when they want to communicate with systems for which they have only the fully qualified host name. DNS poisoning could result in denial of service or redirection of network traffic to an unintended (unauthorized) destination. For security, a “split” DNS configuration must be implemented that consists of internal DNS servers and externally facing DNS servers. The internal servers resolve queries from host machines on internal networks and forwards queries for external name resolution to the externally facing DNS servers. The externally facing DNS servers must be security hardened. They resolve queries from the internal DNS server and present a restricted DNS database to external systems. Inbound and outbound DNS queries must be restricted to these specially identified externally facing DNS servers.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	53	dns	Domain Name Server	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: See UDP port 53 discussion

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	66	sql-net	Oracle SQL*NET	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: Structured Query Language (SQL) is an American National Standards Institute (ANSI) standard language for accessing databases (e.g., Oracle, Microsoft SQL Server). Multiple ports/protocols are used for SQL. Firewalls may be configured to allow use of these ports/protocols only if there is a validated business case for use; otherwise, these ports must be closed by default - Outbound and inbound SQL sessions must be restricted to specifically identified internal and external database servers.- Transfer of sensitive information over public networks must be encrypted. - Non-standard ports are sometimes used for SQL Listening. Restricted use of such additional ports is allowed (without waiver) on a validated, case-by-case and individual port-by-port, basis.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP/UDP	104	acr-nema	ACR-NEMA Digital Imag. & Comm. 300	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: The Digital Imaging and Communications in Medicine (DICOM) Upper Layer Protocol for TCP/IP is used for DICOM based medical imaging communication. Communications on Port 104 must be restricted to specific IP source and destination addresses. - As appropriate, an additional standalone DICOM firewall or proxy server should be installed locally to adequately protect particularly critical systems and sensitive data. An alternative option, if supported by the system, would be to use DICOM-ISCL (Port 2761) or DICOM-TLS (Port 2762)

Note: Port 104 is the de facto standard port for DICOM; the default DICOM port used by some systems may be different. If so, it must be verified that the alternative port is not one that is known to be used for malicious purposes (e.g., Trojan Horse communications).

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	110	pop3	Post Office Protocol (POP) - Version 3	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: POP is used to connect to a system and retrieve mail using a user-name and password. The User-name and password is transmitted in clear text (unencrypted) and is vulnerable to being captured by a sniffer (network analyzer). This information can then be exploited to gain unauthorized access to sensitive information or to use the mail service as an unauthorized mail relay. [Unencrypted] Email received from an external POP server must be scanned for viruses at the external gateway [Note: S/MIME encryption of email will inhibit malicious code scanning of email in transit]. Externally originating POP connections must be limited to those arriving at the gateway via a strongly authenticated Virtual Private Network (VPN) tunnel and restricted to specifically identify internal mail servers.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	119	nntp	Network News Transfer Protocol (NNTP)	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: NNTP is used in the delivery of "news" from "news groups". Outbound NNTP session requests must be highly restricted for validated business requirements to specifically identified external (non-VA) News servers. News traffic must be scanned for malicious code at the external gateway.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	143	imap	Internet Message Access Protocol (IMAP)	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: IMAP4 is the next evolutionary step to POP3. IMAP4’s improvements are functional (vice security) in nature. Thus, as with POP3, Email received from an external IMAP4 server must be scanned for viruses at the gateway. Externally originating IMAP4 connections must be limited to those arriving at the gateway via a strongly authenticated VPN tunnel and restricted to specifically identify internal mail servers.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	179	BGP	Border Gateway Protocol	SI, AI, IB

Discussion: The Border Gateway Protocol (BGP) is an inter Autonomous System routing protocol. There are known vulnerabilities with BGP that can be exploited by attackers to redirect packet routing for denial of service or intercept purposes. BGP traffic must be restricted at the external gateway to specifically identified routing devices. These connections must also use additional device authentication (e.g., MD5) and data integrity methods to preclude spoofing and poisoning of routing information.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	389	ldap	Lightweight Directory Access Protocol (LDAP)	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: LDAP is a subset of the X.500 directory access protocol. LDAP is used to access a standardized hierarchical database storing information about network objects. Inbound TCP/IP LDAP requests must be restricted to specifically identify internal LDAP servers. Out bound LDAP requests are allowed unrestricted.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	444	snpp	Simple Network Paging Protocol (SNPP)	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: SNPP provides a simple way to make a link between the Internet and a TAP compliant paging terminal. Messages are sent from a computer to the paging or cellular carrier via the Internet using SNPP or the simple network paging protocol. The carrier then passes the message to the paging terminal. The paging terminal then broadcasts the message via radio waves to the paging device, mobile phone, billboards, LCDs or other designated wireless device.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
UDP	500	isakmp	isakmp	GI, SI, AI, IB

Discussion: Internet Security Association and Key Management Protocol (ISAKMP) defines procedures and packet formats to establish, negotiate, modify and delete Security Associations (SA). ISAKMP is used to support the negotiation of SAs for security protocols at all layers of the network stack (e.g., Internet Protocol Security [IPSEC], TLS, TLSP [Transport Layer Security Protocol], Open Shortest Path First [OSPF], etc.). Inbound ISAKMP traffic must be restricted to authorized servers or network encryption devices. - Outbound ISAKMP traffic must be restricted by Source and/or Destination IP addresses, as applicable.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	554	rtsp	Real Time Streaming Protocol	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: Streaming media services are used to simultaneously transfer and play audio and video files. Different streaming media software vendors (e.g., Real Networks and Microsoft) implement this service in different ways on different ports. Due to the potential for impacting the limited bandwidth available for official business, the use of streaming media must be restricted to validated business cases. These ports must not be left open (i.e., "Unrestricted") by default.- Streaming Media requests are initiated on an assigned control port (Real Media [TCP Only]: 554 & 7070 / Windows Media [TCP & UDP]: 1755). The normal Streaming Media process requires support for dynamic reallocation of sessions to random UDP "high-ports" (Real Media: 6970-7170/Windows Media: 1024-5000). Thus, the gateway firewall must be configured to allow the Streaming Media server to dynamically establish a UDP high port connection back to the initiating client only if that client first initiated the session to that particular server using the associated control port. By default, this service and these ports must be blocked if the firewall cannot track session state and port reallocation exactly as described - Outbound streaming media session requests must filtered to prevent the accessing of objectionable sites.

Note: In response to standard firewall restrictions that initially precluded widespread access to publicly available, Internet based, streaming media, streaming media software vendors have designed their software to be easily reconfigurable to utilize alternative ports (e.g., HTTP port 80), effectively bypassing any firewall based filtering. Accordingly, content filtering services must be installed and configured at the external gateway to block access to unauthorized content.

- VA streaming media intended to be publicly available must be placed on a security hardened streaming media server within a DMZ isolated from the VA intranet.
- Inbound streaming media session requests must be restricted to specifically identified internal streaming

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
TCP	563	nntps	nntp protocol over TLS (was snntp)	GI, SI, AI, IB

Discussion: Network News transfer protocol is used to read content from news servers, which are defined as "sets of software used to handle Usenet articles." While Usenet is still in use today, its relevance in mainstream internet usage has declined. Rich Site Summary (RSS) feeds have become a more common method of acquiring news.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
TCP	636	ldaps	ldap protocol over TLS	GI, SI, AI, IB

Discussion: LDAP is an open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an IP network. A common usage of LDAP is to provide Single-Sign-On where one password for a user is shared between many services, such as applying a company login code to web pages (so that staff log in only once to company computers, and then are automatically logged into the company intranet).

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
TCP	8080	http-alt	HTTP Alternate	GI, SI, AV, AW, VU, FB, DF, UR, AI, IB

Discussion: See discussion for TCP port 80.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
TCP	993	imaps	imap4 protocol over TLS	GI, SI, AI, IB

Discussion: In computing, the IMAP is an Internet standard protocol used by e-mail clients to retrieve e-mail messages from a mail server over a TCP/IP connection. IMAP was designed with the goal of permitting complete management of an email box by multiple email clients; consequently, clients generally leave messages on the server until the user explicitly deletes them. An IMAP server typically listens on port number 143. IMAP over TLS (IMAPS) is assigned the port number 993. Virtually all modern e-mail clients and servers support IMAP. IMAP is one of the most prevalent standard protocols for email retrieval, with many webmail service providers such as Gmail, Outlook.com and Yahoo! Mail supporting it. This protocol has been widely observed in relation to personal webmail use at VA.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
TCP	995	pop3s	pop3 protocol over TLS	GI, SI, AI, IB

Discussion: The POP is an application layer Internet standard protocol used by local email clients to retrieve email from a remote server over a TCP/IP connection. POP supports simple download and delete requirements for access to remote mailboxes (also known as maildrop). Other protocols, notably Internet Message Access Protocol (IMAP) provide more complete and complex remote access to typical mailbox operations. A POP3 server listens on port 110. Encrypted communication for POP3 is either requested after the protocol initiation, using the STLS command (STARTTLS – method to upgrade from plain text to an encrypted connection), if supported or by POP3S, which connects to the server using TLS on TCP port 995 (POP3S).

POP3 servers hold incoming email messages until you check your email, at which point they will be transferred to your computer. In addition to IMAP, POP3 is one of the most common account types for personal email (Gmail, Yahoo, et cetera).

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
UDP	1024-5000	NA	NA	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: 1024-5000 and 5004 is a UDP port range used by Windows Media Server (WMS) for unicast streams. The client running Windows Media Player (WMP) initiates a TCP connection to the WMS over port 1755. Next, the WMP client picks a random UDP port between 1024 and 5000 and establishes a UDP connection on port 1755 to handle UDP re-sends. At this point, the WMS launches a UDP port scan against the client so it can find the client's listening port and start sending the media stream.

If the WMS cannot find a listening UDP port on the WMP client within the 1024-5000 range, the server tries to send the stream over TCP as an HTTP stream. The Group Policy editor allows administrators to specify which protocol WMS uses when streaming, as well as which UDP ports it uses if UDP is allowed.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	1433	ms-sql-s	Microsoft-SQL-Server	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: See Discussion for Port 66

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	1434	ms-sql-m	Microsoft-SQL-Monitor	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: See Discussion for Port 66

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
UDP	1494	ica	ica	GI, SI, AV, AW, VU, FB, DF, AI, IB
Discussion: Citrix Independent Computing Architecture (ICA) technology provides the foundation for deploying applications and information onto any device. On the server, Citrix ICA separates application logic from the user interface. On the client, users see and work with the application's interface, but 100 percent of the application executes on the server. Accordingly, with ICA, applications consume as little as one-tenth of their normal network bandwidth. - Permitting Citrix absolutely requires a firewall capable of tracking session state to dynamically allocated high ports (above 1024) as follows. - For internal (VA) Citrix servers, inbound Citrix sessions must be restricted to specifically designated internal Citrix servers. Upon initiation, the session will be dynamically reassigned by the internal server to a random high port. Thus, the firewall must be configured to allow the internal server to establish a high port connection back to an external client only if the external client first initiated the session.- Likewise, for external (non-VA) Citrix servers, out bound Citrix sessions must be restricted to specifically designated external Citrix servers. Upon initiation, the session will be dynamically reassigned by the external server to a random high port. Thus, the firewall must be configured to allow the external server to establish a high port connection back an internal client only if the internal client first initiated the session. - By default, this service and these ports must be blocked if the firewall cannot track session state and port reallocation exactly as described. Individual specification of each Citrix server (both external and internal) by IP address is mandatory. If the Citrix session involves processing or display of sensitive information, transport encryption (e.g., TSL, IPSEC) is also required.				
Transport Protocol	**Port**	**IANA-registered Service Name**	**IANA Description**	**Firewall Services To Be Applied**
TCP	1521	NA	NA	GI, SI, AV, AW, VU, FB, DF, AI, IB
Discussion: See Discussion for Port 66.				
Transport Protocol	**Port**	**IANA-registered Service Name**	**IANA Description**	**Firewall Services To Be Applied**
TCP	1525	orasrv	oracle	GI, SI, AV, AW, VU, FB, DF, AI, IB
Discussion: See Discussion for Port 66.				
Transport Protocol	**Port**	**IANA-registered Service Name**	**IANA Description**	**Firewall Services To Be Applied**

TCP	1527	tlisrv	oracle	GI, SI, AV, AW, VU, FB, DF, AI, IB
Discussion: See Discussion for Port 66.				
Transport Protocol	**Port**	**IANA-registered Service Name**	**IANA Description**	**Firewall Services To Be Applied**
TCP	1529	coauthor	oracle	GI, SI, AV, AW, VU, FB, DF, AI, IB
Discussion: See Discussion for Port 66.				
Transport Protocol	**Port**	**IANA-registered Service Name**	**IANA Description**	**Firewall Services To Be Applied**
UDP	1604	icabrowser	icabrowser	GI, SI, AV, AW, VU, FB, DF, AI, IB
Discussion: See Discussion for Port 1494.				

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
TCP	1627	t128-gateway	T.128 Gateway	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: The T.128 protocol supports multipoint computer application sharing by allowing a view onto a computer application executing on one device to be advertised within a session on other devices. Under specified conditions, each device can take control of the shared computer application by sending remote keyboard and pointing device information. This style of application sharing does not require and does not make provision for the synchronization of multiple instances of the same computer application running at multiple locations. Instead, it enables remote viewing and control of a single application instance in order to provide the illusion that the application is running locally.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	1701	l2f	l2f	GI, SI, AI, IB

Discussion: Layer 2 Tunneling Protocol (L2TP) was designed by combining parts of Point-to-Point Tunneling Protocol (PPTP) and Cisco's Layer Two Firewall (L2F). Most commonly used with IPSec, L2TP focuses on creating a tunnel between two authenticated points using IPSec for encryption. Inbound sessions must be restricted to specifically identify internal network devices. If encrypted packets are passed through the gateway, appropriate protections must be implemented at the internal encryption/decryption point to accomplish all bypassed gateway security functions.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	1720	h323hostcall	H.323 Call Control Signaling	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: H.323 is used for voice-over IP call set-up. TCP Port 1720 is most commonly used for H.323 call set-up.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
UDP	1723	pptp	pptp	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: PPTP is an encryption technique developed by Microsoft. Generic Routing Encapsulation (GRE) (Network Protocol #47) is used in conjunction with PPTP to create the VPNs. Microsoft's initial implementation of PPTP used authentication based on the Point-to-Point Protocol (PPP) and encryption based on a Microsoft algorithm. Both the authentication mechanism and encryption algorithm of the initial implementation of PPTP by Microsoft have been broken and should be treated as insecure. Microsoft has subsequently released software patches and updates that fix these vulnerabilities.- Both server and client end patches must be installed to eliminate the vulnerabilities. Patch installations must be verified on all participants (clients and servers) prior to use. Otherwise, an alternative authentication and encryption method (such as the IPSec based L2TP protocol implemented by Microsoft in Windows 2000) must be used in lieu of PPTP. - PPTP (Port 1723) session requests must be restricted to specifically identified internal or external servers. Likewise, GRE sessions may then be statefully allowed from the specific server back to the specific client that first initiated the PPTP session. - If encrypted packets are passed through the gateway, appropriate protections must be implemented at the internal encryption/decryption point to accomplish all bypassed gateway security functions.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	1731	msiccp	MSICCP	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: The Audio Call Control Protocol is used to establish and maintain datastream sessions for multimedia collaborative applications.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP/UDP	1755	ms-streaming	ms-streaming	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: See discussion for Port 554.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	2761	dicom-iscl	DICOM ISCL	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: See discussion for Port 104.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	2762	dicom-tls	DICOM TLS	GI, SI, AI, IB

Discussion: See discussion for Port 104.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
TCP	3101	NA	NA	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: Port 3101 is used to connect a BlackBerry Enterprise Server to the General Packet Radio Service (GPRS) wireless network. Communications on port 3101 must be strictly limited to internally initiated TCP/IP sessions between specifically identified internal BlackBerry Enterprise Server(s) and the specifically identified external GPRS wireless network server(s).

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	5631	pcanywheredata	pcANYWHEREdata	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: pcANYWHERE is a software based remote access and management software. Use of the pcANYWHERE is allowed for validated business purposes. - pcANYWHERE connectivity must be restricted at the external gateway to allow connectivity between specifically identified internal and external workstations and servers. - Inbound pcANYWHERE session requests must be restricted to those arriving at the gateway via a strongly authenticated VPN tunnel and restricted to specifically identified internal workstations or servers.- pcANYWHERE software installed on VA workstations and servers must be configured in accordance with the Baseline Security Configuration Guide for pcANYWHERE Software developed by OCS.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
TCP	8080	http-alt	HTTP Alternate	GI, SI, AV, AW, VU, FB, DF, UR, AI, IB

Discussion: See discussion for TCP port 443.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
TCP	8443	NA	NA	GI, SI, WA, AI, IB

Discussion: See discussion for TCP port 443.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
TCP/UDP	10000	ndmp	Network Data Management Protocol	GI, SI, AI, IB

Discussion: Network Data Management Protocol is a protocol intended to transport data between Network Attached Storage (NAS) devices and backup devices. This removes the need for transporting the data through the backup server itself, thereby enhancing the performance of and removing load from the backup server.

Common backup technologies that support this protocol include EMC NetWorker, Symantec NetBackup, Backup Exec, CommVault, IBM Tivoli, Hitachi, Dell NetVault, and HP Data Protector.

Port 10000 has been known to be associated with Trojan activity (TCP Door, XHX).

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
UDP	33434-33534	traceroute	traceroute use	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: Traceroute is a computer network diagnostic tool for displaying the route and measuring transit delays of packets across an Internet Protocol network. Traceroute is multi-platform. Whereas Windows traceroute uses ICMP packets, *nix traceroute uses UDP packets. For *nix traceroute, only the outbound packets are sent to UDP ports starting with 33434. The returning packets are Internet Control Message Protocol (ICMP) and the UDP port number on the outbound packet usually increments upwards from UDP 33434 to match the Time-to-Live (TTL) set in the IP Header. This is why some firewalls block UNIX/Linux/BSD traceroute but let Windows traceroute through.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services Applied
UDP	33494	traceroute	traceroute use	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: 33494 is an unassigned UDP port. The traceroute application used by Unix, Linux and some Cisco routers takes advantage of this vacancy by sending an incrementing UDP probe to each port within the 33434 - 33494 range. Applications typically don't listen on port 33494 since it's unassigned; therefore, the probed destination usually returns an unreachable port response and successfully contributes to the initial hop count query.

Using UDP in this manner is an archaic approach to tracerouting. ICMP is the most common method. Assuming that we don't have any monitoring systems that rely upon the traceroute application, creating an Access Control List (ACL) to deny UDP any communication over port 33434 should block the outbound Time Exceeded message from reaching the source.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
TCP	50080	NA	NA	GI, SI, AV, AW, VU, FB, DF, AI, IB

Discussion: PILOTS uses port 50080 for HTTP based database requests to the PILOTS server hosted for the VA by the Dartmouth College Information Services. - Outbound HTTP session requests on port 50080 must be restricted by destination solely to the Dartmouth server. Responses from that server are then allowed back to the client that initiated the session. If possible, the HTTP session should also be proxied and filtered similar to other port 80 based HTTP sessions.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
AH	NA	NA	NA	GI, SI, AI, IB

Discussion: Encapsultating Security Payload (ESP) and Authentication Header (AH) are Network Protocols (akin to TCP & UDP) used by IPSec for encryption and authentication. Since traffic encrypted at the network layer, passing through an enclave boundary, cannot be inspected and/or filtered to the same degree as unencrypted traffic, inbound ESP & AH traffic must be restricted to authorized servers or network encryption devices and outbound ESP & AH traffic must be restricted by Source and/or Destination IP addresses, as applicable. Additionally, provision MUST be made for equivalent inspection, filtering (using the guidelines contained herein) and intrusion detection of the decrypted traffic at the internal point of decryption. In the situation where either the originating or destination system is not located on a VA network or where the traffic passes across a shared public network (e.g., Internet), a strong, two-way, identification and authentication process (e.g., asymmetric key/PKI, Secure ID, etc.) MUST also be utilized during establishment of the IPSec connection.

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
ESP	NA	NA	NA	GI, SI, AI, IB
Discussion: See Discussion for AH (Network Protocol #51)				

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
IPSec	NA	NA	NA	GI, SI, AI, IB
Discussion: See Discussion for AH (Network Protocol #51)				

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
GRE	NA	NA	NA	GI, SI, AV, AW, VU, FB, DF, AI, IB
Discussion: GRE is a network tunneling protocol.				

Transport Protocol	Port	IANA-registered Service Name	IANA Description	Firewall Services To Be Applied
ICMP	NA	NA	NA	GI, SI, AI, IB
Discussion: ICMP is part of the Internet Protocol Suite and is generally used by network administrators to identify routing issues and to perform other network diagnostics. In Windows, Ping.exe is an ICMP utility that can be used to determine whether a specific host is online and available for further contact, whereas traceroute can determine the fastest path to a device on the network. A common action performed by attackers on the network is a "ping sweep" in which a large number of IP addresses are pinged in succession to determine available IP ranges for lateral movement. At a minimum, the firewall should be configured to prevent ICMP requests from external sources.				