

Firewall Ports and Protocols Summary

This summary is intended to be a generic guideline for any host-based firewall implementation. The summary focuses on Windows network communication, but the individual options and roles should provide insight and guidance for the creation of appropriate rules for any platform.

Ports affected by a rule set are specified by port number and transport protocol, separated by a forward slash mark. Example: 21/tcp indicates port 21 using the TCP protocol (which happens to be FTP traffic).

If a rule set indicates that it provides a "Client" function, then the port that should be opened is OUTBOUND traffic to the specified port on some other computer. If a rule set indicates that it provides a "Server" function, then the port that should be opened is INBOUND traffic to the specified port on the computer to which you are applying the rule set. Note: Unless otherwise specified, rule sets by default provide a "Client" function.

Where a particular rule set duplicates another rule set's port and protocol combination, but specifically for a different server, the server in question is designated in capital letters, with a hanging indent, and with a generic name. Example:

```
Allow access to DNS (allow remote to port 53/tcp+udp)
    XYZ.com DNS Servers
```

BASE

A set of rules denying all access to and from the computer via the network and subsequent rules allowing back some basic Windows networking functions

Firewall

SUMMARY of Services

```
PING
DNS
NETBIOS
KERBEROS
```

```
Deny All by default
Allow ping locally
Allow access to DNS (allow remote to port 53/tcp+udp)
Allow local netbios traffic in and out (allow local to ports
135/udp,137/udp,138/udp,139/tcp,445/tcp)
Allow Kerberos New Ticket Request and [Windows OS only] Change Password
(allow 88/udp, 464/tcp)
```

ROLES

A cluster of existing options combined for convenience of implementation

- or -

any combination of existing options and application-specific functions that are required at minimum to ensure that an application can function through the firewall.

Banner

SUMMARY of Services

TNS_LISTENER
SSH
TEXAR Security
Banner Forms Servers Child Domain
LSA
LDAP
NTP

NOTE: NETBIOS functionality needed to access the Banner forms servers and to support ODBC connection to the Oracle Database servers is provided via the rules found in the base rule set

Allow TNS_LISTENER and SSH to Oracle server (Allow 1521/tcp, 22/tcp)
Allow TEXAR Security for load balance check (allow 333/tcp)
Allow LSA to Domain Controllers (allow 1026/tcp, 1028/udp, 1029/tcp)
Allow Active Directory (LDAP, LDAP/SSL) lookup to Domain Controllers (allow port 389/udp & 389/tcp, 636/tcp)
Allow Network Time Protocol to Domain Controllers (allow 123/udp, 123/tcp)

Banner Developer

SUMMARY of Services

All of the above found in the Banner role, plus:

CCC HARVEST
Banner Forms Servers Child Domain

All of the above found in the Banner role, plus:

Allow all to Oracle server for FTP (allow */tcp)
Allow all to Oracle server CCC HARVEST (allow */tcp)

Desktop

SUMMARY of Services

FTP (web downloads)
HTTP (web pages)
VT POP3 EMAIL
VT DIRECTORY LDAP

Allow FTP, PASV FTP to internet (allow 21/tcp, 20/tcp)
Allow connections to internet HTTP servers (allow remote to port 80/tcp,443/tcp)
Allow connections to POP3 mail servers (allow 25/tcp, 110/tcp ,995/tcp)
Allow LDAP and LDAP/SSL lookup to directory.vt.edu (allow 389/tcp, 389/udp, & 636/tcp)

Exchange

SUMMARY of Services

MS EXCHANGE to Va Tech Servers
TRUSTED DOMAIN CONTROLLERS

Allow connections to Exchange (allow 1712/tcp, 1097/tcp, 1701/tcp, 1066/tcp, 1670/tcp, all/udp to Exchange server)
Allow LSA to Domain Controllers (allow 1026/tcp, 1028/udp, 1029/tcp)
Allow Active Directory (LDAP, LDAP/SSL) lookup to Domain Controllers (allow port 389/udp & 389/tcp, 636/tcp)
Allow Network Time Protocol to Domain Controllers (allow 123/udp, 123/tcp)

Windows 2000 Domain

SUMMARY of Services

CHILD DOMAIN COMMUNICATION AND AUTHENTICATION

AD DDNS (Active Directory Dynamic DNS)
LSA (Local Security Authority)
LDAP (Lightweight Directory Access Protocol)
NTP (Network Time Protocol)
GLOBAL CATALOG

Note: You must include LSA, LDAP, & NTP entries for the IP addresses of the domain controllers for any other domain for which you wish to enumerate users. Use the DOMAINS option to add these other domain controllers.

Allow access to DNS (allow remote to port 53/tcp+udp)
Windows 2000 DDNS Servers
Allow LSA to Domain Controllers (allow 1026/tcp, 1028/udp, 1029/tcp)
Child Domain Controllers
Root Domain Controllers
Allow Active Directory (LDAP, LDAP/SSL) lookup to Domain Controllers (allow port 389/udp & 389/tcp, 636/tcp)

Child Domain Controllers
Root Domain Controllers
Allow Network Time Protocol to Domain Controllers (allow 123/udp,
123/tcp)
Child Domain Controllers
Root Domain Controllers
Allow access to Global Catalog Servers (allow 3268/tcp, 3269/tcp)
Normal = 3268, LDAP over SSL = 3269

OPTIONS

A specific set of rules that apply to allow one, unique function through the firewall.

Citrix

SUMMARY of Services

CITRIX CLIENT

NOTE: CITRIX initially connects on ICA (1494/tcp) and then negotiates a new connection to the server on a high port number (1023-65534) to separate out multiple client connections

Allow ICA to CITRIX server (allow all tcp)

Domains

SUMMARY of Services

Access to DCs of trusted Child Domains

LSA
LDAP
NTP

Allow LSA to Domain Controllers (allow 1026/tcp, 1028/udp, 1029/tcp)
Allow Active Directory (LDAP, LDAP/SSL) lookup to Domain Controllers (allow port 389/udp & 389/tcp, 636/tcp)
Allow Network Time Protocol to Domain Controllers (allow 123/udp, 123/tcp)

FTP Client

SUMMARY of Services

PASV FTP to internet
This only has marginal effectiveness - FTP is an old and firewall-unfriendly protocol.

Allow FTP, PASV FTP to internet (allow 21/tcp, 20/tcp)

FTP Server

SUMMARY of Services

PASV FTP SERVER

Allow FTP, PASV FTP to internet (allow 21/tcp, 20/tcp)

Instant Messaging

SUMMARY of Services

AOL INSTANT MESSAGING
ICQ INSTANT MESSAGING
MSN INSTANT MESSAGING

Allow access to AOL IM Servers (Allow 5190/tcp)
Allow access to ICQ IM Server (Allow 5190/tcp)
Allow access to MSN IM Servers (Allow 1863/tcp)

LDAP Client

SUMMARY of Services

LDAP CLIENT

Allow LDAP and LDAP/SSL lookup to directory.vt.edu (allow 389/tcp,
389/udp, & 636/tcp)

MeetingMaker

SUMMARY of Services

MEETING MAKER CLIENT

Allow Meeting Maker connection (allow 111/tcp)

Non-VT POP3

SUMMARY of Services

POP3 to non-VT mail servers

Allow connections to non-vt POP3 mail servers (allow 25/tcp, 110/tcp,
,995/tcp)

Print Client

SUMMARY of Services

TCP/IP PRINT CLIENT
LPR (Line Printing Resource)
STANDARD TCP/IP PRINTING

Allow LPR and Standard TCP/IP Printing (allow 515/tcp, 9100/tcp)

Print Server

SUMMARY of Services

TCP/IP PRINT SERVER
LPD (Line Printing Daemon)

Allow LPD Printing (allow 515/tcp, 9100/tcp)

Radmin

SUMMARY of Services

RADMIN Desktop remote Control Server
RADMIN Desktop remote Control Viewer

Allow RADMIN Desktop Control Server (allow 4899/tcp)
Allow RADMIN Desktop Control Viewer (allow 4899/tcp)

Retrospect

SUMMARY of Services

RETROSPECT CLIENT

Allow Retrospect to Retrospect server (allow 497/tcp, 497/udp)

Spamnet

SUMMARY of Services

SPAMNET

Allow connections to internet Cloudmark SPAMNET servers (allow 2703/tcp)

SSH Client

SUMMARY of Services

SSH

Allow SSH (allow 22/tcp)

Telnet Client

SUMMARY of Services

TELNET

Allow Telnet (allow 23/tcp)

Terminal Services Client

SUMMARY of Services

TERMINAL SERVICES CLIENT

Allow traffic to terminal Servers (allow port 3389/tcp)

Terminal Services Server

SUMMARY of Services

TERMINAL SERVICES SERVER

Allow traffic to terminal Servers (allow port 3389/tcp)

VT POP3

SUMMARY of Services

POP3 to VT mail servers

Allow connections to POP3 mail servers (allow 25/tcp, 110/tcp ,995/tcp)

Web Client

SUMMARY of Services

HTTP CLIENT

Allow HTTP client to Internet (allow 80/tcp, 443/tcp)

Web Server

SUMMARY of Services

HTTP SERVER

Allow HTTP Server (allow 80/tcp, 443/tcp)