

## Basic Firewall Rules June 2003

**Assumption:** A stateful firewall will be used to protect an entire VLAN and that firewall logs will be reviewed on a regular basis to identify security issues and configuration adjustments. It is further assumed that the campus unit's system administrator has scanned the VLAN to identify existing services that need to be considered during firewall configuration and require firewall rules in excess of the base rules stated below

**General Firewall Policy:** Deny all inbound traffic unless explicitly authorized and traffic from internal VLAN users is generally unrestricted. All deny rules are logged.

### **Suggested Base Rules - Comment**

*Deny all inbound traffic with network addresses matching internal VLAN addresses* – Inbound traffic should not originate from network addresses matching internal VLAN addresses.

*Normalize all inbound and outbound traffic (e.g., scrub in all)* – This rule will ensure inbound and outbound traffic is defragmented.

*Allow ICMP packets (ICMP TYPE 3, 8, 11) from any external address* – This rule permits acceptance of network maintenance traffic (Destination Unreachable, Echo and Time Exceeded) from any external address. The rule could be abused sending the VLAN excessive amounts of ICMP traffic. Under such circumstances, more restrictive controls should be considered. Further isolation could be achieved by limiting this traffic to only campus network addresses (note - add IP range). Alternatively, some firewall implementations allow for throttling of ICMP traffic, which is an effective way of allowing ICMP control communication but discouraging excessive use of ICMP. Throttling traffic levels may be preferable to defining specific firewall rules for ICMP functions.

*Allow RIP UDP traffic from router to VLAN hosts* – This rule should only be used if the department has hosts that require default route advertisements.

### **Suggested Optional Rules – Comment**

The following rules are offered as a guide and should only be considered if you offer the particular services on the protected VLAN. Management and support staff must evaluate the use of following firewall rules and determine whether the rule imposes a serious risk to the security of the protected resources behind the firewall.

The use of additional security measures must be used for resources shared through the firewall to ensure only authorized access and use. Additional security measures include account management, regular operating system and application maintenance, removal of unnecessary services/processes, access control measures and activation/inspection of event logs (Reference: SANS Step-by-Step Guides).

*Allow Web traffic (TCP 80/443) from any external address to internal web server –* Permit access to the specific IP address(es) of internal webservers via HTTP and HTTPS. Additional security measures must be considered for web servers as many security exploits use TCP port 80.

*Allow traffic (TCP 21) to internal FTP server –* If FTP services are provided to external users, this rule permits access to the FTP server. As a reminder, when using FTP services, user account and password information is transmitted in clear text. Use of passive FTP (PASV) will negotiate a random data port versus use of TCP port 20.

*Allow traffic (TCP 22) to internal SSH/SFTP server –* Use of encrypted SSH is preferred over insecure FTP/Telnet services. This rule permits use of SSH to access internal SSH hosts.

*Allow traffic (TCP 25) to internal SMTP server –* Permit external SMTP users and servers access to internal SMTP mail server. This rule presumes your campus unit is operating an SMTP server.

*Allow DNS (UDP 53) to internal DNS server –* If the unit runs internal DNS servers this rule is recommended. The rule is needed if a Windows Active Directory server is hosted on the internal network. You must permit TCP 53 for zone transfer capability, however this permission should not be applied by default.

*Allow traffic (UDP 67/68) for client access to DHCP server –* This rule permits DHCP clients to negotiate lease with DHCP server

*Allow traffic (TCP 110) to internal POP server –* Permit external POP users access to internal POP server. This rule presumes your campus unit is operating a POP server. It is strongly recommended that POP authentication traffic be conducted over a secure transport, such as TLS/SSL (TCP 995)

*Allow NTP traffic (TCP 123) to specific internal host address(es) –* This rule permits time synchronization and may be needed by selected internal hosts for time synchronization. This rule is required to support external client authentication to the internal Active Directory services.

*Allow traffic (TCP 143) to internal IMAP server –* This rule permits external IMAP clients to access internal IMAP server. It is strongly recommended that IMAP authentication traffic be conducted over a secure transport, such as TLS/SSL (TCP 993)

*Allow inbound traffic (TCP 515 from 169.237.104.59 and 169.237.104.65) for BANNER spooler/printing to specific internal printer address –* This rule will permit transcript printing.

*Allow inbound traffic (TCP 515 from 128.48.175.6) for PPS spooler/printing to specific internal network printer address –* This rule will permit printing Payroll/Personnel

reports. If you use Remote Printer Manager (PC) or Intersolv (Mac) for PPS printing to a non-network printer, the firewall rule must permit TCP515 traffic to the host with the direct connected printer.

*Allow access to internal MeetingMaker Server (TCP 2001, UDP 2000, UDP 417) – This rule permits inbound traffic to MeetingMaker servers residing on the protected network.*

*Allow access to MS SQL Server (TCP/UDP 1433 and 1434) to specific host address – This rule permits inbound traffic to communicate with a MS SQL Server residing on the protected VLAN.*

*Allow access to Microsoft Resources – Consult Microsoft's TechNet and Knowledge Base resources to verify firewall configuration requirements for Exchange, MS SQL Server, and shared MS network resources. Some firewall rules are determined by version. Shared resources must be properly secured or the VLAN hosts could be vulnerable to security compromises. See References section for additional information.*

*Allow traffic (TCP/UDP 135, 137, 138 139/445) for external access to specific shared resources – This rule permits external clients to access shared Microsoft resources behind the firewall.*

*Allow access (TCP 4899) to specific internal hosts using Famatech RADMIN remote administration application – This rule permits external administrators to communicate with hosts running the RADMIN utility.*

*Allow access (TCP 5641 and UDP 5642) from external clients running pcAnywhere to specific host addresses – This rule permits remote control of computing hosts behind the firewall using Symantec's PCAnywhere product.*

*Increase UDP timeout from default 2 minutes to 45 minutes – This rule is suggested to bypass DaFIS time restrictions.*

## **Suggested Microsoft References:**

MS Exchange:

- <http://support.microsoft.com/default.aspx?scid=kb;en-us;280132>
- <http://support.microsoft.com/default.aspx?scid=kb;en-us;q278339>
- <http://support.microsoft.com/default.aspx?scid=%2fservicedesks%2fwebcasts%2fwc070902%2fwcblurb070902.asp>

MS-SQL Server

- <http://msdn.microsoft.com/library/default.asp?url=/nhp/default.asp?contentid=28000409>

General MS Port Information

- <http://support.microsoft.com/default.aspx?scid=kb;en-us;150543>

## **Other Resources**

Internet Firewalls: Frequently Asked Questions, Matt Curtin and Marcus J. Ranum, December 2000, <http://www.ranum.com/pubs/fwfaq/>

Inside Network Perimeter Security: The Definitive Guide to Firewalls, Virtual Private Networks (VPNs), Routers, and Intrusion Detection Systems.

Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Fredrick, Ronald W. Ritchey, Que, 1st edition (June 28, 2002).

Building Internet Firewalls, 2nd Edition, Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, O'Reilly & Associates, Inc. June 2000

Firewall Mailing List, <http://www.isc.org/services/public/lists/firewalls.html>

Online Firewall Buyers Guide, ICSA Labs, TruSecure Corporation, [http://www.icsalabs.com/html/communities/firewalls/buyers\\_guide/index.shtml](http://www.icsalabs.com/html/communities/firewalls/buyers_guide/index.shtml)