

SJSU Firewall Best Practice

UCAT Network Services

San Jose State University

Table of Contents

Scope

Campus Firewalls Environment

- Perimeter Firewall
- Server Farm Firewall
- Building/College Firewalls

Perimeter Firewall Traffic Restrictions

- Completely Blocked Services Inbound
- Inbound
- Outbound

Server Farm Firewall Traffic Restrictions

- Completely Blocked Services
- Public Servers
- Backend Servers
- Testing and Staging servers

Operational Procedure

- Firewall Request Work Flow

Scope

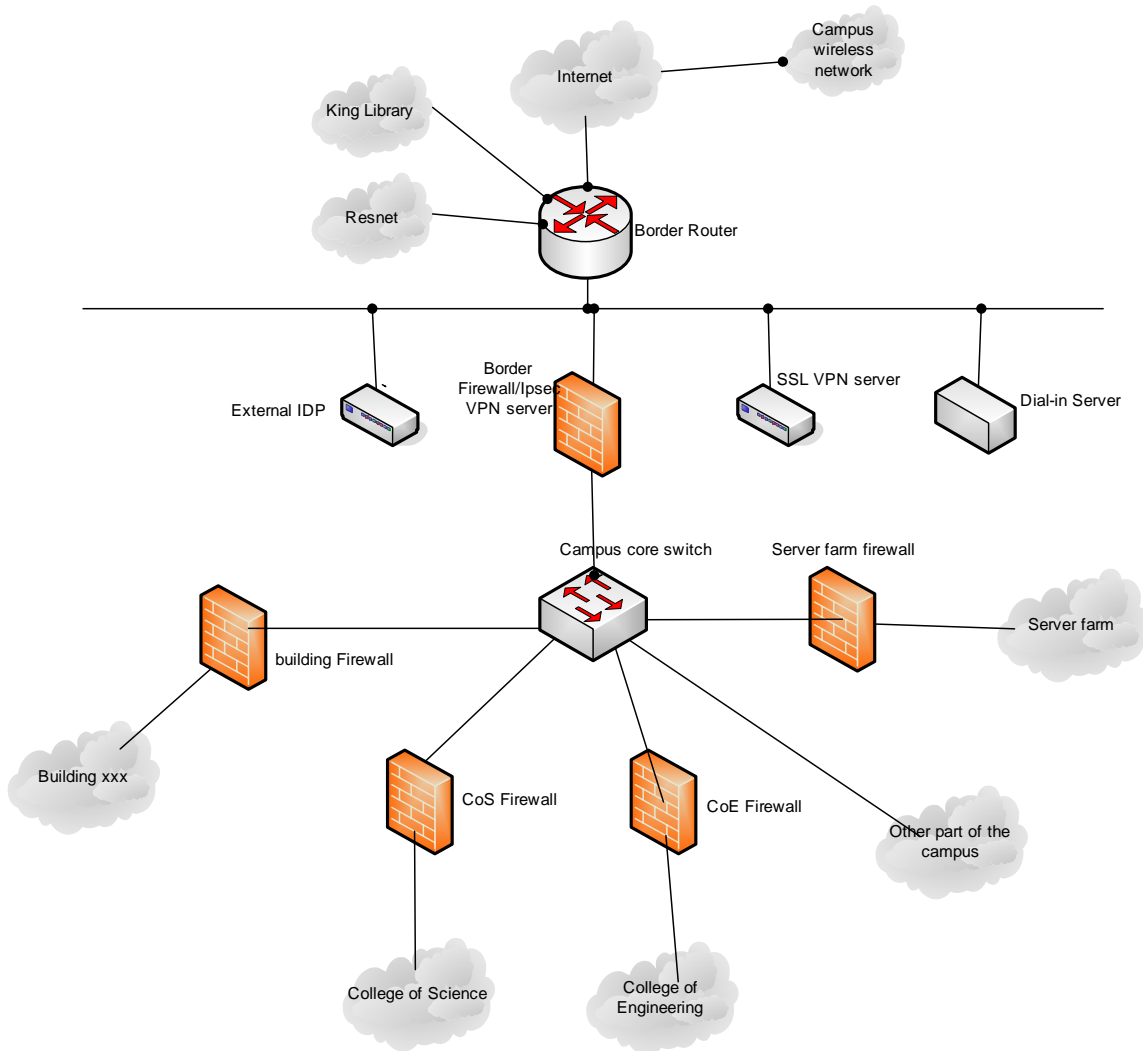
These practices are based on the Information Security Guidelines of San Jose State University. It is highly recommended that you review some of our other best practice documents. These documents can be found at <http://www.sjsu.edu/networking/policies/>.

Campus Firewalls Environment

All firewall and security policies should be audited and verified at least quarterly.

As a general rule, any protocol and traffic that is not necessary, i.e., not used or needed by the organization and/or denied by best practices, should be blocked via use of a border router and border firewall. This will result in reduced risk of attack and will create a network environment that has less traffic and is thus easier to manage and provide faster response.

SJSU Campus Firewall Environment



Perimeter Firewall

The perimeter firewall protects the campus as a whole from the Internet, campus wireless network, Resnet and King Library. The campus border firewall also has built-in IDP, which protects the campus network from attacks, viruses and worms.

Server Farm Firewall

The server farm firewall is used to protect the campus main servers including the mail servers, web servers, DNS server, DHCP server and database servers from the Internet and other parts of the campus network.

Building/College Firewall

Building or college firewalls protect the buildings and colleges between other parts of the campus. It also controls traffic between subnets within a building or college.

Perimeter Firewall Traffic Restrictions

Completely Blocked Services

Some services are prohibited both inbound and outbound on the campus perimeter firewall because they are dangerous services or viruses and worms are running on those ports.

The following services are not allowed through the firewall for both inbound and outbound traffic:

UCAT Firewall Best Practice Draft

Port(s) (Transport)	Server	Port(s) (Transport)	Server
1 (TCP & UDP)	tcpmux	1807 (TCP)	SpySender
7 (TCP & UDP)	echo	1981 (TCP)	Shockrave
9 (TCP & UDP)	discard	1999 (TCP)	BackDoor
11 (TCP & UDP)	systat	2001 (TCP)	Trojan Cow
13 (TCP & UDP)	daytime	2023 (TCP)	Ripper
15 (TCP & UDP)	netstat	2049 (TCP & UDP)	nfs
17 (TCP & UDP)	qotd	2115 (TCP)	Bugs
19 (TCP & UDP)	chargen	2140 (TCP)	Deep Throat
37 (TCP & UDP)	time	2222 (TCP)	Subseven21
43 (TCP & UDP)	whois	2301 (TCP & UDP)	compaqdiag
67 (TCP & UDP)	bootps	2565 (TCP)	Striker
68 (TCP & UDP)	bootpc	2583 (TCP)	WinCrash
69 (UDP)	tftp	2701 (TCP & UDP)	sms-rcinfo
93 (TCP)	supdup	2702 (TCP & UDP)	sms-remctrl
111 (TCP & UDP)	sunrpc	2703 (TCP & UDP)	sms-chat
135 (TCP & UDP)	loc-srv	2704 (TCP & UDP)	sms-xfer
137 (TCP & UDP)	Netbios-ns	2801 (TCP)	Phineas P.
138 (TCP & UDP)	Netbios-dgm	3268 (UDP)	msft-gc
139 (TCP & UDP)	Netbios-ssn	3269 (TCP)	msft-gc-ssl
177 (TCP & UDP)	xdmcp	4045 (UDP)	lockd
445 (TCP & UDP)	microsoft-ds	39168 (TCP)	Trinity V3
512 (TCP)	rexec	33270 (TCP)	Trinity V3
513 (TCP)	rlogin	6000 - 6063 (TCP)	X11 Window System
513 (UDP)	who	6665 - 6669 (TCP)	irc
514 (TCP)	rsh, rcp,rdist, rdump,rrestore	6711 - 6712 (TCP)	Subseven
515 (TCP)	lpr	6776 (TCP)	Subseven
517 (UDP)	talk	7000 (TCP)	Subseven21
518 (UDP)	ntalk	12345 - 12346 (TCP)	NetBus
540 (TCP)	uucp	16660 (TCP)	Stacheldraht
593 (TCP & UDP)	MS-RPC	27444 (UDP)	Trinoo
1024 (TCP)	NetSpy	27665 (TCP)	Trinoo
1045 (TCP)	Rasmin	31335 (UDP)	Trinoo
1090 (TCP)	Xtreme	31337 - 31338 (TCP&UDP)	Back Orifice
1170 (TCP)	Psyber S.S.	32700 - 32900 (TCP&UDP)	RPC services
1234 (TCP)	Ultors Trojan	65000 (TCP)	Stacheldraht
1243 (TCP)	Backdoor-G	161 - 162 (TCP/UDP)	SNMP
1245 (TCP)	VooDoo Doll	179 (TCP)	BGP
1349 (UDP)	Back Orifice DLL		
1492 (TCP)	FTP99CMP		
1600 (TCP)	Shivka-Burka		
1761 - 1764 (TCP&UDP)	sms-helpdesk		

The following types of network traffic are always blocked inbound and outbound:

- Inbound or outbound network traffic containing a source or destination address of 127.0.0.1 (localhost).
- Inbound or outbound network traffic containing a source or destination address of 0.0.0.0.
- Inbound or outbound traffic containing directed broadcast addresses.

Inbound

Inbound traffic includes traffic coming into campus wired network from Internet, King Library, Resnet and campus wireless network.

All inbound traffic, by default, is blocked unless otherwise requested by authorized departmental personnel. Thus, traffic from the following services and applications should be blocked inbound by firewall policy, with exceptions noted.

Appliciation	Port Numbers	Action
Login Services	telnet - 23/tcp	restrict w/ strong authentication
	SSH - 22/tcp	restrict to specific systems
	FTP - 21/tcp	restrict w/ strong authentication
Name Services	DNS - 53/udp	restrict to external DNS servers
Mail	SMTP - 25/tcp	block unless external mail relays
Web	HTTP - 80/tcp and SSL 443/tcp	block unless to public Web servers
Miscellaneous	finger - 79/tcp	always block
	NNTP - 119/tcp	always block
	NTP - 123/tcp	always block
	SNMP - 161/tcp/udp, 162/tcp/udp	always block
	BGP - 179/tcp	always block
	SOCKS – 1080/tcp	always block
ICMP	block incoming echo request (ping and windows traceroute) with very few exceptions.	

The following types of inbound network traffic are always blocked:

- Inbound traffic from a non-authenticated source system with a

destination address of the firewall system itself.

- Inbound traffic with a source address indicating that the packet originated within the SJSU network.
- Inbound traffic from a system using a source address that falls within the address ranges set aside in RFC 1918 as being reserved for private networks.
- Inbound traffic containing IP Source Routing information.

Outbound

Outbound traffic includes all traffic leaving campus wired network to the Internet, King Library, Resnet and campus wireless network.

All outbound SMTP traffic is blocked except for the three campus mail scrubbers, the mail relay server, and a few mail servers with special needs.

All other outbound traffic to the internet is allowed by default except for those listed above in the completely blocked services.

Server Farm Firewall Traffic Restrictions

Completely Blocked Services

This is the same as the perimeter firewall, except Netbios ports and Microsoft-ds port are allowed to the Windows AD servers from specific campus subnets.

Public Servers

These servers have ports opened to the public, either to the whole Internet, or to some parts of the campus. Outbound traffic from them will be limited. Campus DNS servers, email servers, and web servers are public servers.

Backend Servers

These servers don't have port opened to the public. They only have ports opened to some front end servers. Outbound traffic from them is limited. Most of them are database servers, or servers containing confidential information. Administrator access to the servers is limited to VPN, client authentication, or limited source IP address.

Testing and Staging servers

These servers don't have port opened to the public. The limitation is pretty much the same as backend servers. The only difference is that the firewall rules for these servers change constantly for testing purpose.

Operational Procedure

For any service that needs to be open to the public, UCAT will request a Nessus scan of the server. The server administrator will be required to fix all major and critical security problems before UCAT security team approving the request.

All firewall requests must come from the designated unit IT coordinator.

Please review the IT coordinator list here:

<http://helpdeskinternal.sjsu.edu/referrals.html>

To place a firewall request, open a GWI ticket. If GWI doesn't work, please email network@sjsu.edu for your request.

Please follow the diagram below before placing a firewall request.

Firewall Request Work Flow

Firewall Request Work Flow

