Smeal College of Business - Central Firewall Rules and Policies

1.0 Purpose

The purpose of this policy is to outline the College's use and management of centralized firewall services. This policy will set forth the College's guidelines for applying standard and custom firewall rules and the types of network roles to which those rules are applied within the Smeal College of Business. The Smeal College of Business recognizes that staff, faculty and students rely more than ever on computing systems to carry out their daily work. The College also recognizes that network based threats to computing resources, data and network security are growing at an increasing rate. The use of firewall systems is one method used to mitigate these threats while using the College's computing, data and network resources. College computing systems are for business purposes in serving the administrative, academic and research activities of the College, University, faculty, staff and students.

2.0 Scope

SCB-FWP-01 applies to guests, faculty, staff, students, contractors, consultants, temporaries, and other workers engaged in activities that require the use of the Smeal College of Business computing, data or network resources. This policy applies to all equipment that is connected to the Smeal College of Business network or provided to the user by the College for off-site use (home systems, loaner laptops, PDAs, cell phones, etc. and connected to the Smeal College network).

3.0 Policy

3.1 General Firewall Purpose

1. The Smeal College of Business has implemented and relies on centralized firewalls to protect the College's network, data and computing resources from potential "internet" based security threats from outside of the College.
2. Within the firewall system, the College's LANs (local area networks) are also segregated from each other in order to mitigate security threats coming from within the College, ie., an infected laptop brought in from outside of the College and connected to a Smeal network resource.

3.2 LAN Roles

The College's network is broken down into many smaller networks or LANs each having a specific purpose or "role." These individual LANs will each have a set of standard firewall rules and also in certain instances, a subset of custom rules. Custom rules must be requested in writing.

1. Faculty LAN – This is considered the standard administrative LAN for the College's faculty. Standard firewall rules apply and no exceptions are made for individual users.
2. Staff LAN – This is considered the standard administrative LAN for the College's staff. Standard firewall rules apply and no exceptions are made for individual users.
3. Grad LAN - This is considered the standard administrative LAN for the College's graduate students. Standard firewall rules apply and no exceptions are made for individual users.
4. Printers - This is considered the standard administrative LAN for the College's network printer resources. Standard firewall rules apply and no exceptions are made for individual users.
5. Faculty DMZ – This is considered the research or experimental network resource for faculty wanting to run their own server. Initially, standard firewall rules are applied and any custom firewall rules must be requested. Users take on a greater responsibility and risk when requesting to have a machine connected to this LAN.
6. Labs LAN – This is the LAN for all of the College's computer labs. Machines on this LAN resource must be managed by the RIIT Group. Custom rules may be requested ONLY by the lab manager.
7. Trading Room LAN – This is a special purpose LAN dedicated to the College's "Trading Room" laboratory resource and is not a part of the Labs LAN. Custom firewall rules may only be requested by the lab manager.
8. Mobility LAN – These LANs support the College's "wired" mobility service. This service allows users with a valid PSU ID and password to connect a university, college or personally owned device to the College's network. These LANs utilize the ITS "Portlogin" (https://clc.its.psu.edu/portlogin.aspx) service for individual user level authentication. Standard firewall rules apply to these LANS. In addition, custom rules may be applied ONLY by the network administrator in response to security or service issues on these LANs.
9. Server LAN – The server LANs support the college's research, teaching, public relations and backend administrative servers. Standard rules are applied and each server admin may request custom rules ONLY for the ip address(es)/servers that he or she is responsible for.
10. Video Conference LAN – This LAN supports the College's video conferencing service. Standard firewall rules apply. Custom rules may be requested ONLY by the video conference systems administrators.
11. Smeal VPN LAN – This LAN supports the College's VPN service. Standard rules apply. No custom rules or exceptions can be requested by individual users.

3.3 Standard Firewall Rules

By default, the College's "standard firewall rules" are applied to all interfaces on all firewalls. These standard rules follow this general template:

1. All outbound DNS requests are restricted to PSU DNS servers.
2. All remaining outbound network packets are allowed.

3. All incoming ICMP packets addressed to either the network or broadcast addresses are denied.
4. All incoming ICMP Ping, Traceroute and Echo packets are allowed.
5. All incoming Smeal or PSU VPN packets are allowed.
6. All incoming SOS subnet and individual addresses are allowed.
7. All incoming ITS or TNS system servers highlighted here: https://www.work.psu.edu/firewall_info/ or individually listed are allowed.
8. All incoming packets from "network management" machines are allowed.
9. All other incoming packets are denied.

3.4 Custom Firewall Rules

On LANs that were designed with custom rules in mind (such as the faculty dmz) users may make requests in writing for exceptions ONLY for the ip addresses which have been assigned to them. They may not make requests for exceptions for servers or ip addresses for which they have no administrative responsibility. All requests will be reviewed by the network administrator and discussed with the requestor before being implemented. Requestors are reminded that they are responsible for any adverse consequences resulting from issues arising from these custom rules. Users requesting exceptions are expected to be knowledgeable in the proper management of the server and services said machine is hosting.

4.0 Enforcement

The Smeal College of Business Research Instructional and Information Technology Group (RIIT Group) has been authorized by the Dean of the Smeal College of Business to enforce this policy.

Any employee found to be in violation of this may be subject to disciplinary action by their Administrative unit, the College, or the University.

4.1 Monitoring and Logging

In order to better control network based security threats, mitigate breaches, and provide network troubleshooting, the Smeal College of Business Research Instructional and Information Technology Group (RIIT Group) will monitor and log incoming network packets that that are denied by the firewall. The following is an example of a logged incoming firewall denial:

Apr 6 14:34:46 172.28.117.162 Apr 06 2011 14:55:07 172.28.117.162 : %FWSM-4-106023: Deny udp src outside:128.118.106.36/63050 dst fac_dmz:128.118.204.40/52311 by access-group "outside_inbound" [0xdb798377, 0x0]

These logs are rotated daily with the previous days logs compressed and moved to a daily archive folder.

All allowed data packets whether incoming or outgoing are only logged to a small rolling buffer on each firewall interface and are lost after a few minutes. These logs are used only for troubleshooting. The following is an example of an accepted packet:

Apr 13 2011 15:28:49 128.118.210.1 : %FWSM-6-302013: Built outbound TCP connection 144938937252507519 for RIIT_int:128.118.210.28/1664 (128.118.210.28/1664) to outside:dc2/135 (dc2/135)

4.2 Termination of Custom Rules Exceptions or Network Access

The Smeal College of Business reserves the right to remove, discontinue or rescind the allowance of custom firewall rules or may even terminate network access to individual users for any of the following breaches of conduct with regard to system, data and network resources:

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation, use or distribution of "pirated" or other software products that are not appropriately licensed for use by the Smeal College of Business.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the College Smeal College of Business or the end user does not have an active license is strictly prohibited.
3. It is illegal to export software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate College security officer should be consulted prior to export of any material that is in question.
4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using a Smeal College of Business computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any Smeal College of Business account. Or, offers of products, items, or services for personal profit from any Smeal College of Business account.
8. Making statements about warranty, either expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended

recipient or logging into a server or account that the employee is not expressly authorized to access. The only exception to this is when access is part of a security analysis performed by an authorized individual within the College or University. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information.

10. Port scanning or security scanning is expressly prohibited unless prior approval is obtained from the College Network Security team.
11. Executing any form of network monitoring which intercepts data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account apart from assigned duties performed by IT professionals.
13. Interfering with or unsanctioned denying of service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet apart from assigned duties performed by IT professionals.
15. Providing information about, or lists of, Smeal College of Business employees to parties outside the University.
16. Expanding the College's network through the use of private firewalls, routers or NAT devices without the consent of College IT department.
17. Obscuring PCs, servers or other devices attached to the Smeal College of Business network though the use of private firewalls, routers or NAT devices without the consent of the Smeal College of Business IT department (RIIT Group).

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone, pager, sms text messages or Instant Messaging services whether through content, language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for other email addresses, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" or "pyramid" schemes of any type.
6. Use of unsolicited email originating from within Smeal College of Business networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the Smeal College of Business or connected via Smeal College of Business networks.
7. Posting identical or similar non-business-related messages to large numbers of newsgroups (newsgroup spam) or forums.

5.0 Definitions

Term	**Definition**
Spam	Unauthorized and/or unsolicited electronic mass mailings.
Internet	A worldwide system of computer networks
Intranet	A private network that is contained within an enterprise.
Extranet	A private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses.

Firewall A system or device designed to prevent or allow certain network traffic to or from a subnet or subset of PCs on a subnet.

LAN (Local Area Network) A small computer network that may stand alone but that is usually connected to a gateway to allow machines on that network to "talk" to other machines on other networks. Consider a LAN to be the computer's idea of a neighborhood.

Rule A statement written in syntax understandable by the firewall that tells the firewall what specific network packets to allow or deny through to the internal LAN. Generally, a collection of rules tells the firewall what computers are allowed to "talk" to each other and what they can talk about together.