UNIVERSITY OF SOUTH DAKOTA

Policy Number: 5.005
Originating Office: Information Technology Services
Responsible Executive: VP for Admin and Technology
Date Issued: 12/08/2010
Date Last Revised: 08/05/2015

Firewall & Router Review

Policy Contents

I. REASON FOR THIS POLICY 1
II. STATEMENT OF POLICY 1
III. DEFINITIONS 2
IV. PROCEDURES 3
V. RELATED DOCUMENTS, FORMS AND TOOLS 4

I. REASON FOR THIS POLICY

The University of South Dakota (USD) has established a formal policy and supporting procedures regarding Firewall and Router Review. This policy will be evaluated on an annual basis to ensure its adequacy and relevancy regarding the university's needs and goals.

The University is committed to operating a Science DMZ in support of research, as well as a University DMZ where publicly accessible academic and administrative applications are located. The Science DMZ is optimized for high-performance scientific applications and tailored for high-volume bulk data transfer, remote experiment control, and data visualization.

This policy also ensures USD's compliance with Payment Card Industry Data Security Standards (PCI DSS) requirements.

II. STATEMENT OF POLICY

This policy applies to all USD firewalls and routers in the USD network including those that transmit credit cardholder data. Both the University DMZ and Science DMZ are subject to this policy.

1. ITS will review firewall and router rule sets no less than every 6 months.
2. Servers must be approved by the IT Security Officer before they are added to the DMZ.
3. Network services provided by an authorized server must be approved by the IT Security Officer prior to modifying any rule set.

4. ITS will audit the DMZ at least once per month to confirm the servers are properly located within the University network.
5. ITS will monitor common vulnerabilities in the DMZ, and servers found to be vulnerable will be remediated in a timely manner.
6. Servers located in the DMZ must be secured using appropriate host-based security technologies.
7. Servers located in the DMZ will not run unnecessary network services.
8. Exceptions to this policy must be approved by the Vice President for Administration and Technology.

III. DEFINITIONS

Cardholder data: The combination of a credit cardholder's name, Primary Account Number (PAN), service code, and expiration date.

Cardholder data environment: All areas of computer system network that may possess cardholder data or sensitive authentication data for cardholder processing, storage, or transmission.

Computing equipment: Personal computing devices that utilize the wired or wireless network to transfer data; including, but not limited to, desktop computers, laptops, tablets, smart phones, and game consoles.

CVSS Score: The Common Vulnerability Scoring System is a standard for measuring the impact of a vulnerability. The scoring scale goes from 1 to 10, where 10 is the highest risk for vulnerability. A CVSS score 4 or above is a medium risk, and a CVSS score 7 or above is high risk.

DMZ: A location on the University network hosting public facing network services, such as web or email, and segmented from other network locations where cardholder data or other protected information is located. The Science DMZ is a special case which has been optimized for high-performance scientific applications.

Firewall: A security system whose primary function is to prevent unauthorized access to network services using a set of rules defined by an administrator. The system may be a dedicated appliance, or it may be a host-based software application.

Network Service: A software application which provides access to a resource via network requests from computing equipment; including, but not limited to, file and printer sharing, web servers, and domain name servers.

Router: A system capable of forwarding packets between 2 or more internet protocol (IP) networks. Routers may implement sets of rules, like firewalls, in order to limit access to or from specific IP networks.

Server: Any computer or device whose purpose is to provide a network service or storage to computing equipment; including, but not limited to, network-attached storage (NAS) devices, networked printers and multifunction copiers, and any computer running a network service.

IV. PROCEDURES

The firewall review procedure must include the following:

- Ensure that firewalls permit inbound communication only to authorized services within the University or Science DMZ
- Ensure that firewalls permit and/or restrict outbound communication as pertinent to external services including but not limited to Payment Card, State of SD, and Learning Management Systems
- Ensure that firewalls permit no unsolicited inbound communication to workstations

The router review procedure must include the following:

- Ensure that routers permit communication between authorized services and end-user workstations
- Ensure that routers permit DNS and NTP traffic to all workstations
- Ensure that routers restrict communications to specific devices as required

The DMZ approval procedure must include the following:

- A process to ensure that the server has no obvious medium risk vulnerabilities, defined by the CVSS score, on public facing services
- A process to ensure that the server has no obvious high-risk vulnerabilities, defined by the CVSS score, on internally facing services
- The DMZ audit procedure must include the following:
- Compare the inventory of servers and network services designated for the University and Science DMZs to the list of servers located in the DMZs at a point in time
- Update the DMZ inventory and/or remove servers from the DMZ as appropriate

The Vulnerability monitoring procedure must include the following:

- Perform scheduled vulnerability scans at least quarterly from both inside and outside of the campus firewall using a vulnerability scanner such as Nessus
- Review of scan results by a qualified individual in a timely manner
- Report on any vulnerabilities exceeding the maximum tolerable risk level to the owner of the server
- Create and implement a remediation plan for vulnerabilities in a timely manner

Host-based security technologies may include any of the following:

- At a minimum each server will run a host-based firewall such as iptables or Windows firewall
- Host-based IDS/IPS such as Snort
- File integrity monitoring such as OSSEC
- Log and event monitoring such as OSSIM
- All review procedures will include provisions to determine the status of servers and services to remove unneeded permissions and/or restrictions.

V. RELATED DOCUMENTS, FORMS AND TOOLS

Not Applicable