University of Pittsburgh
Computing Services and Systems Development (CSSD)

Overview of Enterprise Network Firewalls

Enterprise Security Controls

Electronically stored academic, administrative, and research information is a critical University resource. All University units are required to use enterprise email, web services, and network firewalls. These Enterprise Security Controls help protect University data and significantly reduce security vulnerabilities. See http://technology.pitt.edu/security/compliance/enterprise-security.html for additional information about these requirements.

Additional Needs

As Enterprise Security Controls were being implemented, the following additional needs were identified by the University's research community:

- **Enhanced Research Collaboration** that enables individuals from other universities and institutions to transfer files, retrieve files, or execute programs.
- **"Power" VPN usage** that delivers secure remote access to University resources, meets the need for increased performance associated with large files, and provides support for 64-bit Linux operating systems. The University's existing Secure Remote Access service does not currently meet these needs.

Solutions

The following solutions are being implemented to support research collaboration with external institutions while also protecting the University's computing environment:

- A new **Research Firewall Zone** designed to meet the advanced collaboration requirements of the University's research community.
- A new **Research VPN** that provides better performance for high-capacity uses and supports 64-bit Linux operating systems.

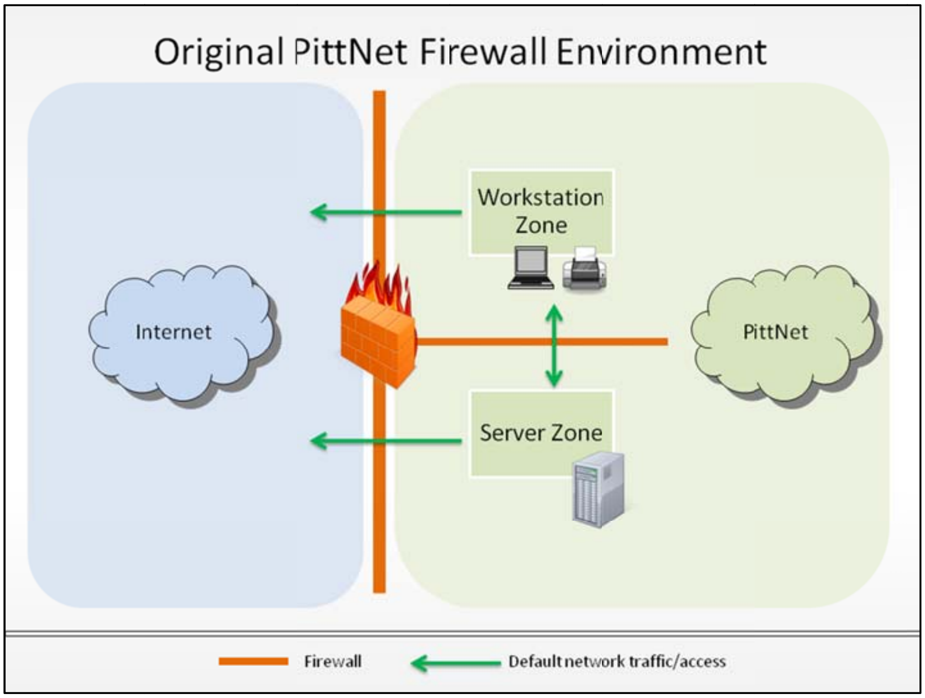
Types of Firewall Zones

With the addition of the Research Zone, there are four types of firewall zones that protect the University's computing network. Each has been created to address a specific set of needs and requirements while also providing the correct amount of security for each environment:

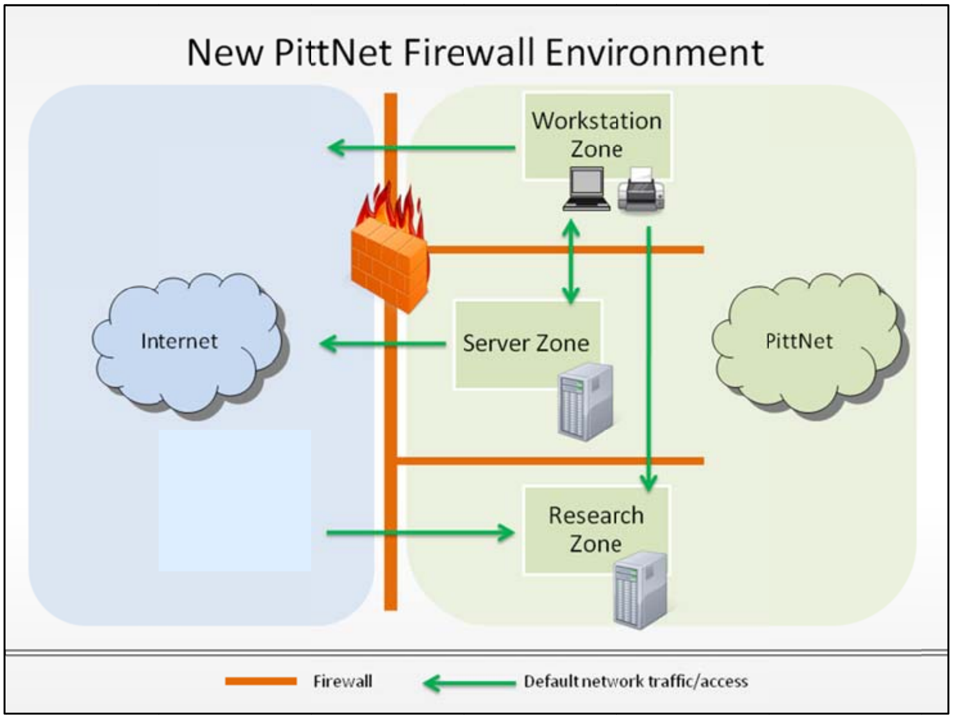
1. Workstation Zone
2. Server Zone
3. DMZ (Public Access Zone)
4. Research Zone *(NEW)*

Overview of Firewall Zone Environment

Before the implementation of the Research Zone, the University's firewall environment offered no unrestricted access to University network resources.


Original PittNet Firewall Environment
Workstation Zone
Internet
PittNet
Server Zone
Firewall
Default network traffic/access

Access to the Research Zone is permitted from anywhere on the Internet. It can be used to transfer data to a server or retrieve it. It can also be used to control a terminal from a remote location or execute programs. The Research Zone is described in more detail on page 3.



Descriptions of Firewall Zones

Workstation Zone

- **Purpose:** The purpose of the Workstation Zone is to protect the University's personal computers, workstations, and printers. For example, desktop and laptop computers with access to email and Internet resources are protected by this firewall zone.
- **Inbound Access:** No inbound access is permitted to the Workstation Zone, except when using the Secure Remote Access service or the new Research VPN (which requires CSSD approval).
- **Outbound Access:** There are no restrictions on outbound access.
- **Controls:** A 60-minute idle session timeout is the only special control in place for this zone.

Server Zone

- **Purpose:** The purpose of the Server Zone is to protect servers that store information that is used only by a department or a subset of a department. For example, file servers, application servers, and database servers are protected by this firewall zone.
- **Inbound Access:** With a few exceptions, no inbound access is permitted to the Server Zone. Inbound access is permitted from the proper Workstation Zone and DMZ Zone with CSSD-approved firewall exceptions. Inbound access is also permitted when using the Secure Remote Access service or the new Research VPN.
- **Outbound Access:** There are no restrictions on outbound access.
- **Controls:** A 60-minute idle session timeout is the only special control in place for this zone.

DMZ (Public Access Zone)

- **Purpose:** The purpose of the DMZ Zone is to protect servers that require inbound access from the Internet. No sensitive data can reside on these servers. Examples include departmental media servers (such as CIDDE's Mediasite) and Web servers that are used for departmental Web sites and housed on CSSD's Enterprise Web Infrastructure (EWI).
- **Inbound Access:** Inbound access to servers in the DMZ Zone is permitted from *any* device *anywhere* on the Internet via the http or https protocol. Additional inbound access, which requires CSSD approval, can be granted to allow for server administration or file transfers. This additional inbound access requires either 1) a special firewall exception from another secure Pitt zone, or 2) use of the Secure Remote Access service or Research VPN.
- **Outbound Access:** There are no restrictions on outbound access.
- **Controls:** A 60-minute idle session timeout is the only special control in place for this zone.

Research Zone

Purpose and Description

The purpose of the new Research Zone is to support the unique requirements for collaboration with external parties while protecting the University's computing environment. The Research Zone permits access from anywhere on the Internet. It protects machines in the zone by limiting functionality (for example, typical desktop computing functions like email and Web access are not permitted in the zone). Sensitive data cannot be stored on any machine in the Research Zone.

The Research Zone can be used to transfer data to a server or retrieve it. It can also be used to control a terminal from a remote location or execute programs.

Inbound Access

There are three general types of inbound access permitted to the Research Zone. All require CSSD approval.

1. *Data transfer OR retrieval*: Either a University Computing Account or a local account may be used. This type of access must be restricted to read OR write access (not both simultaneously). Access type is SSH (tcp/22) directly to a specific machine in the zone.

2. *Bidirectional data exchange, terminal control, and program execution*: A University Computing Account is required. Access type is SSH (tcp/22) directly to a specific machine in the zone.

3. *Other uses beyond port 22*: A primary University Computing Account is required. The Secure Remote Access service or Research VPN must be used with specific rules.

Note that there is no inbound access to the Research Zone from other secure Pitt firewall zones.

Outbound Access

In general there is no outbound access from the Research Zone. Exceptions are permitted to allow for access to central services (for example, DNS servers, time servers, log servers, backup servers, critical event handling, and Domain Controllers for authentication). If they are required, additional outbound access exceptions must be approved by CSSD.

Controls

In addition to the standard 60-minute idle session timeout control, several other controls are utilized in the Research Zone. These include:

- **Network Controls**, such as monthly vulnerability scans, real-time traffic monitoring, and MAC locking for all ports in the Research Zone
- **Machine controls**, which include:
  - Permitting local accounts to have only read OR write access, but NO execution access
  - Requiring a University Computing Account for executable or shell access
  - Using only the SSH V2 protocol
  - Requiring CSSD administrator access for scans
  - Disallowing remote administrator (root) logins (i.e., an account is required)
  - Implementing an annual CSSD review