FIREWALL RULE SUBMISSION v1.6
June 16, 2010

PROCEDURE: Firewall Rule Submission
Effective Date: July 13, 2009

STATEMENT: In order to properly maintain the rulebase in the firewall and to ensure rule sanity, a new set of guidelines for submitting rules is being put into place. Adherence to the rule submission guidelines will allow for rapid approval and deployment of new firewall rules.

APPLICABILITY: This procedure applies to all devices in all University data center(s) that require access through UISO-managed firewalls.

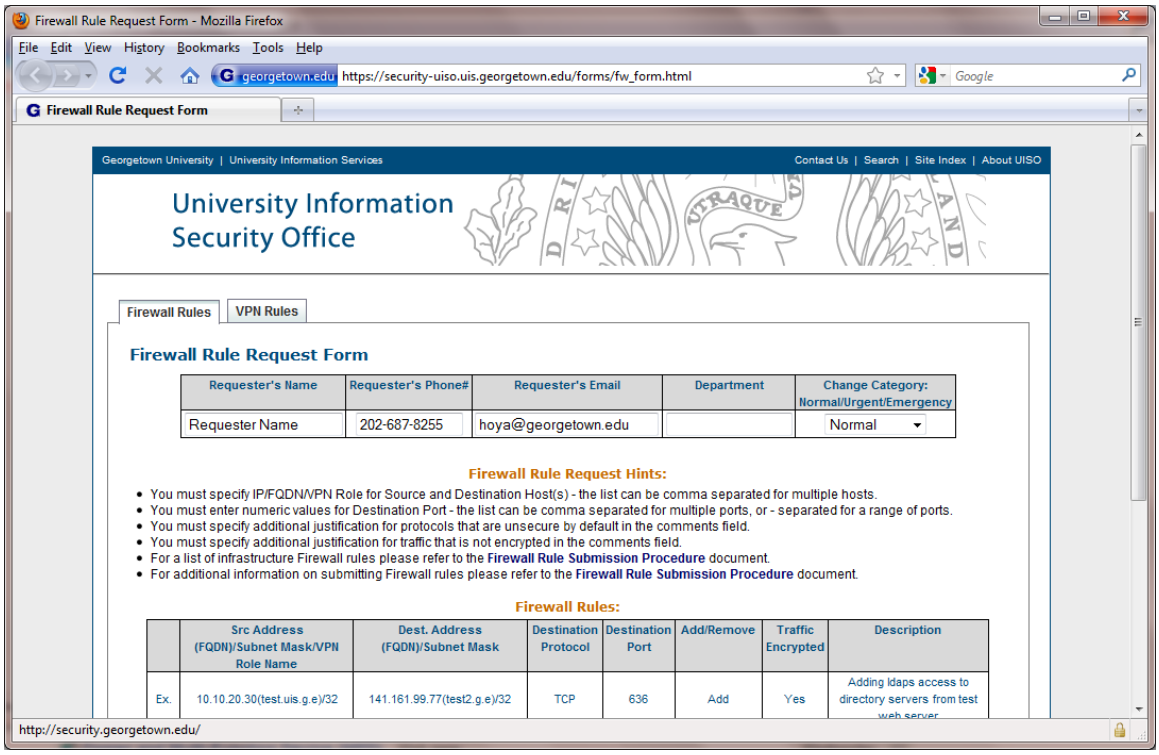
DEFINITIONS:

- Firewall – All firewall devices managed by the Security Office including
  - The UIS data center located on Georgetown main campus
  - The UIS data center located in Doha, Qatar
  - The independent departmental PIX firewalls
  - The UIS data center located in Loudon County, Va.
  - The UIS data center located in Laurel, MD
- System - Any device requiring access through a UIS-managed firewall.
- Change Summary: a summary of what the rule does.
- Requested by**:** The name of the person submitting the request.
- Person responsible for changes**:** The name of the person with oversight on the rule for future audits. Can be the same as Requested by.
- Source Address/FQDN/VPN Role Name: The IP address and fully qualified domain name of the data source. This field can also contain the VPN Role Name for VPN authorization.
- Destination Address/FQDN: The IP address and fully qualified domain name of the data.
- Protocol: The network protocol used for the communication (TCP/UDP/Both)
- Destination Port: The destination portused by the incoming traffic.
- Traffic encrypted? An indicator of whether or not the traffic is encrypted.
- Description: Additional details for the request, such as why traffic is not encrypted, why a range of IPs is needed instead of specific hosts, etc.
- VPN Role: Organizational name of a group of users that have the same VPN access parameters. Example: NCS-SM, EETS-CS
- VPN Rule: Specific firewall rule allowing a given VPN role to access specific servers on specific ports.

GUIDING PRINCPLES/PURPOSE: Effective firewall rules are those that are requested in the most specific format possible. The more specific a rule, the less likely something unexpected will slip through.

EXAMPLE:

To request a Firewall Rule please visit
(http://security-uiso.uis.georgetown.edu/forms/fw_request.html):



- Enter your NetID and password to authenticate in the Login box.
- Follow the instructions on the page to specify the Firewall rule request.
- Review the Firewall Rule(s) request for correctness.
- Submit the Firewall Rule(s) request.
- An e-mail will be sent to the Helpdesk to create a ticket.
- Confirmation e-mail will be sent to the person requesting the Firewall Rule(s).

HINTS AND TIPS:

To make your requests easier, please keep the following things in mind:

1. The following access and services are automatically included, meaning, there is no need to make separate requests for them:
    a. ICMP is automatically allowed
    b. DNS is automatically allowed
    c. SNMP monitoring by the Operations Center is automatically allowed
    d. Data center communications to and from SMS/Altiris is automatically allowed

   e. Data center communications to and from Astro/Netbackup are automatically allowed
   f. AD traffic to and from gt-dc3/4 and mei-dc3/4 are automatically allowed
   g. NTP traffic to the UIS time server is automatically allowed
   h. Scanning traffic from the UISO scanner VM is automatically allowed
   i. Kerberos traffic is automatically allowed
2. When submitting requests, please include both the system IP and the fully qualified domain name, even if that name is not in DNS yet.
3. Leave enough time for your change to be scripted, reviewed, and implemented. This means not bringing firewall rule requests in the middle of the afternoon because your contractor is coming the next day and you've known this for a week.
4. Access from your desk to hosts in protected networks (ie, any data center network) is provided via the Check Point VPN only. Do not make requests with your static desk IP as a source. We are no longer using static IPs to administer machines unless there is no technological away around it. If you do not have VPN access, please contact the UISO to see how to get it. All new VPN user requests require management approval.
5. Please do not include things like IPF configurations, configuration file snippets, or anything else in request. Please use the request as it appears. The request format was specifically designed to be easy to read, easy to follow, and easy to implement.
6. Hosts that are on the same subnet talk to each other without going through the firewall, there is no need to create a firewall rule for hosts on the same subnet.
7. Be aware that any change can be referred back to the requestor's management for additional approvals. This additional approval cycle can introduce delays in implementation that are outside the UISO's ability to control.
8. Hosts in the Private firewall zones (subnet 152 and 39) do not talk to anything other than other hosts in the data centers. They do not get access from the Internet, nor do they talk directly to the Internet. Do not request rules that violate this principle.
9. It is not necessary to request return traffic as part as a rule. Any traffic that is allowed by a rule is automatically allowed to come back. You should only submit rules that have new traffic being initiated. For example, if you submit a rule to allow SSH initiated from Host A to go to Host B, you don't need to request a rule allowing SSH from Host B to Host A **unless** SSH connections will also be initiated from Host B. SSH traffic returning to Host A will automatically be accepted.
10. Do not list sources or destinations as VLANs. VLAN tags do not necessarily match their subnet numbers. List IPs instead of VLAN tags.

REQUESTING VPN CHANGES AND ADDITIONS:

FIREWALL RULE SUBMISSION v1.6
June 16, 2010

The process for requesting new access to resources via the SafeConnect VPN is similar to requesting new rules but with a few differences.

In order to gain access to a particular server a user needs to be a member of the appropriate VPN Role and the VPN rule needs to include the server the user wants access to.

If a new VPN Role needs to be created, refer to the VPN Role Authorization Process documentation to properly format the request for creating a new role.

If the role already exists and a user needs to be added to that role use the web form located at:
https://www4.georgetown.edu/uis/keybridge/keyform/authenticated/form.cfm?FormID=2843

Once a VPN Role has been created and users have been associated with that role, use the web form (http://security-uiso.uis.georgetown.edu/forms/vpn_request.html) to request a Firewall Rule so the VPN Role can be authorized to access the system(s).

ADMINISTRATION AND IMPLEMENTATION:

The following conditions apply when requesting changes or additions to the firewall rules:

- All requests must be submitted via the web form. The web form will automatically submit a request to the Helpdesk to create a Peregrine Ticket.
- All requests are subject to appropriate management approval of the submitter.
- All systems mentioned in the request are subject to security scans, including non-Georgetown contractors or vendors. Poor results from a security scan can result in a denial of the request.
- All traffic passing through any UIS-managed firewall is subject to inspection and logging by the Information Security Office.
- New and existing firewall rules are subject to periodic review by the Information Security Office. Failure to participate in the review or provide the requested review information may result in the rule being disabled and access being interrupted.
- Firewall request approval turnaround time is 2 business days unless a legitimate emergency is declared and approved by management. Be aware that rules that are delivered after 1500 to the office with an expected implementation of the next day are not guaranteed to be completed on time.
- All UISO approved firewall requests are subject to standard UIS change control approval (typically 72 hours) unless a legitimate emergency is declared and approved by management.

The following restrictions apply when requesting changes or additions to the firewall rules:

- Firewall rules will have specific Source and Destination end points. Entire subnets will not be allowed through to servers behind the firewall. IP ranges will be permitted with specifically justified business needs.
- Firewall rules will have specific protocols allowed. Protocol ranges will not be allowed without a specifically justified business need (ex: client program will not use a single port but a randomly chosen one within a specific range). You must be able to thoroughly and accurately explain the use of all protocols that you are asking to allow through the firewall.
- Data transferred through the firewall will be encrypted. Unencrypted protocols will not be approved without a specific unavoidable business need.
- Systems behind the firewall do not have unrestricted access to the Internet. Specific access requirements are needed.

RESPONSIBILITY(IES):

- Requestor: The requestor is responsible for properly and completely filling out the firewall rule change request form and for researching the information necessary to do so as well as understanding the impact the requested changes will have.
- Person responsible for changes: The person responsible for changes is the individual that serves as the approval for any firewall rule changes being requested. They will have a record of what changes have been requested on behalf of their organization and will be able to participate in rule audits using that information.
- UISO: The University Information Security Office is responsible for reviewing the firewall rule requests, ensuring that the meet or exceed University security standards and to implement the approved rules within the predetermined window.

ENFORCEMENT: Firewall rules that do not meet University standards are not approved. As a result network access through the firewall is not allowed. Rules that do not pass periodic audits are disabled.

RESOURCE(S):

APPROVAL: David Smith

REVIEW CYCLE: This procedure will be reviewed yearly at the beginning of the fiscal cycle.