



Política y Procedimiento del uso de Firewalls


Versión 1.1

Revisado por:

Georgios A. Kiragiannis-Collazo
Director Asociado en Infraestructura Tecnológica
DTAA
Fecha: 8/4/2008

Aprobado por:

Edwin J. Martínez, Ed.D.
Director Ejecutivo
DTAA
Fecha: 8/4/2008

	Política y Procedimiento del uso de Firewalls	Código: FW-DTAA-SOP-01
		Versión: 1.1
		Fecha de aprobación: 27/mayo/2008
		Página: 2 de 11

Control de Cambios

Fecha	Versión	Descripción	Autor
14/Enero/2008	1.0	Comenzando el desarrollo de las secciones	Roberto García
21/Febrero/2008	1.0	Revisión de Tabla de contenido, Secciones 3, 7.2, 9, 11, 12	Reinaldo Rivera
2/abril/2008	1.1	Se dividió el documento en Políticas y Procedimientos. Se añadieron secciones y sus respectivas explicaciones.	Georgios A. Kiragiannis
7/abril/2008	1.1	Modificaciones generales a las secciones ya establecidas. No se quitaron ni, añadieron secciones.	Dr. Edwin Martínez
27/mayo/2008	1.1	Correcciones gramaticales y de sintaxis en general.	Ismael García Ortega, Ayudante Especial del Decano de Cs. Sociales
27/mayo/2008	1.1	Añadir definiciones de algunos términos tecnológicos	Eileen M. Figueroa Ramos



	Política y Procedimiento del uso de Firewalls	Código: FW-DTAA-SOP-01
		Versión: 1.1
		Fecha de aprobación: 27/5/2008
		Página: 3 de 11

Tabla de Contenido

1.	Políticas del Uso de Firewalls	4
1.1	Propósito y Alcance:	4
1.2	Objetivos	4
1.3	Personal Impactado:	4
1.4	Políticas de conexiones de ingreso y salida	4
1.4.1	Políticas de conexiones de salida	4
1.4.2	Políticas de conexiones de ingreso	5
1.5	Excepciones a las Políticas de Conexiones	6
1.5.1	Requisición de Regla en Firewall	6
1.5.2	Responsabilidad de la Seguridad de la Red de UPR-RP	6
1.5.3	Responsabilidad del Administrador del Sistema	6
1.6	Aprobaciones	7
1.7	Renovaciones	7
2.	Procedimientos del uso de Firewalls	8
2.1	Propósito	8
2.2	Acrónimos:	8
2.3	Procedimiento para Administradores de Sistemas	8
2.3.1	Solicitar Regla al Firewall	8
2.3.2	Implementación de Regla en Firewall	8
2.3.3	Mantenimiento de Reglas en el Firewall	9
2.4	Procedimientos para Seguridad de Red	9
2.4.1	Registro de entradas y alertas	9
2.4.2	Registro de Servidores:	9
2.4.3	Revisión de Reglas	10
2.5	Procedimientos Administrativos	10
2.5.1	Proceso de Apelación	10
2.6	Puntos de Contactos	10
2.7	Acceso físico	10
3.	Definiciones de conceptos	11

	Política y Procedimiento del uso de Firewalls	Código: FW-DTAA-SOP-01
		Versión: 1.1
		Fecha de aprobación: 27/5/2008
		Página: 4 de 11

1. Políticas del Uso de Firewalls

1.1 Propósito y Alcance:

El equipo de *Firewall* (Cortafuego) de la Universidad de Puerto Rico Recinto de Río Piedras (UPR-RP) es un elemento importante de la seguridad de la red del Recinto. El equipo de *Firewall* restringe el acceso del Campus en formas específicas y permite analizar el tráfico en formas concretas. Combinado con otros controles de seguridad complementarios, el *Firewall* puede proteger los activos y la información del Recinto contra algunas amenazas que se relacionan con las conexiones a Internet. Este equipo mejora las habilidades del Recinto de detectar y responder a situaciones de seguridad que puedan ocurrir.

Esta política explica el role del *Firewall* en contribuir con la seguridad de la red de data de UPR-RP. Define tanto la responsabilidad del administrador de la red como de los usuarios finales de la red del Recinto y las consecuencias si estas responsabilidades no son cumplidas.

Esta política aplica a todos los componentes de la red de data de UPR-RP y a todos sus usuarios autorizados, tanto de forma remota como local.

1.2 Objetivos

La comunidad del Recinto disfruta el beneficio del acceso al Internet con restricciones mínimas. Nuestras actividades de enseñanza, aprendizaje, investigación y servicio pueden sufrir hasta cierto nivel si el acceso al Internet está muy restringido. Al mismo tiempo, la DTAA tiene una cantidad de activos e información que están a su cargo y cuidado. La DTAA tiene la responsabilidad ética y legal de proteger estos activos, y velar que la confidencialidad, integridad y disponibilidad pueden verse amenazadas si estos activos tuvieran muy pocas protecciones de los accesos al Internet.

Así que es por eso que hemos implantado el *Firewall* como método de control, con su objetivo principal de reducir el riesgo que tiene la red de UPR-RP al tener este acceso al Internet.


1.3 Personal Impactado:

- DTAA: Oficina para el Desarrollo y Mantenimiento de la Infraestructura
- Administradores de Sistemas de todas las dependencias de la UPR-RP

1.4 Políticas de conexiones de ingreso y salida

1.4.1 Políticas de conexiones de salida

Se entiende por conexiones de salida todo tráfico donde la petición inicial se origine en el Recinto. Tráfico interno al exterior – esta regla por defecto será que todo lo que internamente se solicita a un recurso externo se permitirá el acceso con la excepción de todo tráfico que la Seguridad de Red determine que sea peligroso o innecesario que tenga salida. En caso de querer filtrar algo en la red interna entonces se harán reglas TCP/UDP/ICMP para cumplir con el propósito que se quiere lograr. De requerir bloquear algún otro puerto cualquier usuario seguirá el procedimiento establecido en la sección 2.3.1.

	Política y Procedimiento del uso de Firewalls	Código: FW-DTAA-SOP-01
		Versión: 1.1
		Fecha de aprobación: 27/5/2008
		Página: 5 de 11

Actualmente las reglas que existen para bloquear tráfico de salida son:

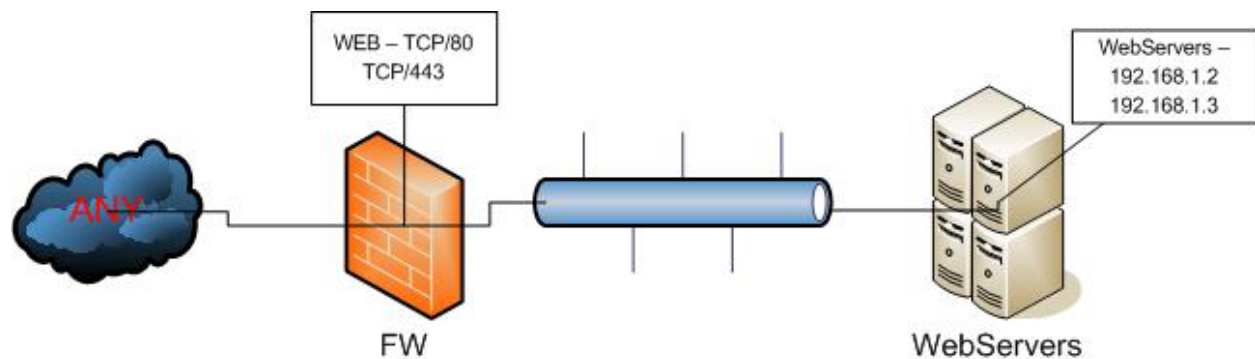
- Puertos: 25 SMTP
- Puertos: 135,139,445 Microsoft
- Puertos: 1433,1434 SQL
- Puertos: 5900 VNC
- Puertos: 2967, 2968 Norton Server
- Puertos: 69 TFTP
- Puertos: 6667 Virus IRC

1.4.2 Políticas de conexiones de ingreso

Se entiende por conexiones de ingreso todo tráfico donde la petición inicial se origine desde el exterior de la red del Recinto. Para las conexiones de ingreso se harán grupos de servicio y grupos de protocolos. También se añadirán las máquinas que accederán estos servicios. Se creará una regla de filtrado que incluya estos grupos como destino y servicio. El propósito de esta regla es facilitar el trabajo de los servidores para brindar un servicio con mayor eficacia. Una vez creada la regla se añade el IP del *host* al grupo de *WebServers* para que el tráfico de información comience sin necesidad de alterar las reglas.


- No se permitirá la conexión irrestricta desde el exterior de la red del Recinto.
- Todo equipo (servidores, instrumentos científicos, computadoras) que requieran acceso desde el exterior de la red del Recinto tiene que estar registrado. Ver sección 2.3.1.

Por ejemplo se creara un grupo llamado *WebServers*, el cual albergará todos los servidores con http activo, un grupo llamado *Web*, que tendrá todos los puertos tcp/udp necesarios para este propósito como TCP: 80/TCP: 443.



```
access-list Outside2SF extended permit tcp any object-group
WebServers object-group Web
```

Figure 1: Diagrama de ejemplo de regla

	Política y Procedimiento del uso de Firewalls	Código: FW-DTAA-SOP-01
		Versión: 1.1
		Fecha de aprobación: 27/5/2008
		Página: 6 de 11

1.5 Excepciones a las Políticas de Conexiones

1.5.1 Requisición de Regla en Firewall

- El administrador del sistema interesado en tener acceso desde el exterior tiene que cumplimentar una solicitud para el registro del equipo.

1.5.2 Responsabilidad de la Seguridad de la Red de UPR-RP

El término Seguridad de la Red se refiere sólo a la responsabilidad colectiva que tiene la unidad organizacional responsable de administrar el equipo y las políticas del *Firewall* del Recinto. Puntos de contacto específicos son determinados en el procedimiento que acompaña esta política.


- La Seguridad de la Red notificará a los administradores de sistemas de cambios en los requerimientos de los servidores atacados. (Ejemplos: Nuevas reglas de seguridad necesarias al descubrir vulnerabilidades)
- La Seguridad de la Red podrá realizar pruebas de vulnerabilidades a servidores antes de ser implementados o aprobados para su acceso al Internet.
- Si la regla en el *Firewall* ha sido aprobada, la Seguridad de la red implementará esta regla, luego que el sistema ha pasado su auditoría inicial y pruebas de conformidad.
- La Seguridad de la Red realizará periódicamente, auditorías de vulnerabilidades a cada servidor. Estas pruebas no serán planificadas ni anunciadas.
- La Seguridad de la red le notificará a los Administradores de Sistemas cuando las reglas aprobadas están para ser renovadas y procesará la reprobación de las reglas sometidas.
- Tener y Guardar una lista actualizada de rangos de direcciones de IP internas y externas utilizadas por la UPR-RP.
- Tener y guardar una lista actualizada de los computadores por nombre asignados en las reglas del FW.
- Tener y guardar una lista actualizada de Firewalls y usuarios, y una lista de sus roles en cada sistema.

1.5.3 Responsabilidad del Administrador del Sistema

El administrador del sistema es responsable de cumplir con los siguientes requisitos. El requisito inicial tiene que ser cumplido antes de que la Seguridad de la Red pueda implementar los cambios aprobados. Los requisitos de cualquier regla tienen que ser cumplidos de forma vitalicia. Si en algún momento, cualquier requerimiento de una regla ya aprobada no es cumplido, la Seguridad de la Red tiene la autoridad de tomar los pasos necesarios para proteger la red de UPR-RP.

1.5.3.1 Requisitos Iniciales

- Auditoría inicial – El grupo de Seguridad de Red realizará un avalúo (assesment) de vulnerabilidades al servidor. El Administrador del Sistema cooperará con el personal designado para completar cualquier acción necesaria especificada por el representante.
- Registro de entradas de seguridad – Copias de un grupo de registro de eventos será transmitido en tiempo real a un sitio central dónde se le especificará al Administrador del Sistema. El

	Política y Procedimiento del uso de Firewalls	Código: FW-DTAA-SOP-01
		Versión: 1.1
		Fecha de aprobación: 27/5/2008
		Página: 7 de 11

Administrador del Sistema demostrará que la configuración de registro de entradas ha sido configurado exitosamente.

1.5.3.2 Requisitos Continuos

- Notificación de Cambio – El Administrador del Sistema notificará a la sección de Seguridad de Red cualquier cambio emitido en la requisición de regla de *Firewall*.
- Notificación de Incidentes – El Administrador del Sistema notificará cualquier situación o incidente de seguridad que envuelva el sistema.
- Auditorías – El grupo de Seguridad de la Red podrá realizar auditorías a los sistemas para verificar que el sistema este funcionado correctamente y que no representa riesgo para la red.
- Respuesta Rápida a Vulnerabilidades – El administrador del sistema es responsable de responder con celeridad cualquier situación que pueda poner en riesgo al sistema y a la red.
- Será responsabilidad del administrador del sistema mantener actualizado el mismo con la instalación de actualizaciones y parches.

1.6 Aprobaciones


La Seguridad de la Red tiene la autoridad de revisar, y aprobar o desaprobar, toda requisición de nueva regla al *Firewall*.

Si la requisición de la regla es aprobada, el Administrador del Sistema tiene que cumplir con todos los Requisitos Iniciales descritos en la sección anterior antes que la Seguridad de la Red implemente la regla.

Si la requisición es denegada por la Seguridad de la Red, el Administrador del Sistema tiene el derecho de apelar dicha decisión como se describe en el procedimiento que acompaña esta política.

1.7 Renovaciones

Toda regla del *Firewall* tiene que ser renovada anualmente. De no recibirse la solicitud de renovación se entenderá no es necesario el acceso desde fuera del recinto para ese sistema.

	Política y Procedimiento del uso de Firewalls	Código: FW-DTAA-SOP-01
		Versión: 1.1
		Fecha de aprobación: 27/5/2008
		Página: 8 de 11

2. Procedimientos del uso de Firewalls

2.1 Propósito

La Sección [Políticas del uso de Firewalls](#), define las políticas que gobiernan la administración del equipo *Firewall*, y ciertos aspectos de la administración de servidores que se enmarcan dentro de este alcance. La sección de Procedimientos explica los procedimientos específicos que los Administradores de Sistemas tienen que esperar a seguir de acuerdo con las políticas mencionadas en la sección descrita.

El equipo de *Firewalls* es uno de los mecanismos de seguridad que se utiliza en el campo de la tecnología de información. Este es un componente necesario que complementa los mecanismos de seguridad de los sistemas a nivel de capa de comunicaciones L3-L7. El siguiente documento es un procedimiento de mejores prácticas desarrollado para la Universidad de Puerto Rico en el Recinto de Río Piedras para tener una referencia y asegurar que sus equipos de *Firewalls* estén configurados de forma óptima y efectiva.

2.2 Acrónimos:

- DTAA División de Tecnología Académica y Administrativa
- ODMI Oficina para el Desarrollo y Mantenimiento de la Infraestructura de la DTAA
- FW *Firewall*
- OS Oficial de Seguridad
- IT Tecnología de Información
- TCP *Transport Control Protocol*
- IP Protocolo de Internet

2.3 Procedimiento para Administradores de Sistemas

2.3.1 Solicitar Regla al Firewall

El Administrador de Sistemas de un servidor o servicio que está localizado en, o estará relocalizado en, los perímetros de la red de UPR-RP puede solicitar cambios a las reglas del *Firewall* para permitir la entrada de conexiones del Internet a servicios específicos o una agrupación de servicios de ese servidor.


2.3.1.1 Solicitar: Hacer el registro correspondiente del sistema en la forma FW-DTAA-01, localizada en <http://www.uprrp.edu/dtaa/>.

2.3.1.2 De la solicitud no ser aprobada por la Seguridad de Red entonces prosiga con la sección 2.5.

2.3.2 Implementación de Regla en Firewall

2.3.2.1 Cooperar con la sección de Seguridad de Red en el itinerario de la auditoría de vulnerabilidades del servidor. Completar cualquier acción remediaria específica que el auditor recomiende.

2.3.2.2 Configurar un acceso remoto al servidor para demostrar conformidad de las especificaciones requeridas por la política.

	Política y Procedimiento del uso de Firewalls	Código: FW-DTAA-SOP-01
		Versión: 1.1
		Fecha de aprobación: 27/5/2008
		Página: 9 de 11

2.3.3 *Mantenimiento de Reglas en el Firewall*

2.3.3.1 Notificar a la sección de Seguridad de Red de algún cambio en la información documentada en la requisición de regla para el *Firewall*.

2.3.3.2 Notificar de cualquier incidente anormal o de seguridad haciendo una llamada al Service Desk del Recinto de Río Piedras.

2.3.3.3 Realizar cambios recomendados por las auditorías periódicas que la sección de Seguridad de Red recomiende.

2.4 **Procedimientos para Seguridad de Red**

El personal gerencial de la División de Tecnologías Académicas y Administrativas y la Oficina para el Desarrollo y Mantenimiento de la Infraestructura (ODMI) son los responsables de velar por las vulnerabilidades, accesos no autorizados y mitigar riesgos dentro de la red del Recinto de Río Piedras. La Sección de Seguridad de Red y la sección de Telecomunicaciones están a cargo de realizar cambios correctivos inmediatos, identificados como puntos débiles en la red. Recursos adicionales se involucrarán con la solución dependiendo de la complejidad y debilidad de la descripción.

2.4.1 *Registro de entradas y alertas*


El registro de entradas y alertas se hará mediante un servidor de bitácoras. Este servidor debe guardar las bitácoras de al menos treinta (30) días de operación del aparato de red. Se revisarán periódicamente las entradas en bitácora para predecir patrones en comportamiento de aparatos internos y externos. Esto nos ayudará a identificar posibles ataques e infecciones virales contra los sistemas.

2.4.2 *Registro de Servidores:*

Se mantendrá un listado actualizado de todo equipo al que se le cree regla en el *Firewall*. Refiérase a la sección de Solicitar Regla al Firewall. La información que se incluirá en dicho listado será:

- Nombre del Equipo
- Sistema Operativo
- Ubicación
- Propósito
- Departamento
- Nombre del Administrador
- Teléfono del administrador
- Correo electrónico del Administrador
- Nombre del Supervisor y/o Director y/o Decano
- Servicio que brindará
- Usuarios del Sistema (local, Intranet, Internet)

Todo registro de servidor deberá ser autorizado por el Director del Departamento Solicitante y el Administrador de Red del Recinto. Solamente los servidores debidamente registrados serán autorizados a transmitir y recibir comunicación de la red del Recinto.

	Política y Procedimiento del uso de Firewalls	Código: FW-DTAA-SOP-01
		Versión: 1.1
		Fecha de aprobación: 27/5/2008
		Página: 10 de 11

2.4.3 Revisión de Reglas

Las reglas serán revisadas periódicamente para mantener el equipo de *Firewall* actualizado. Esto evitará que reglas que están en desuso sean detectadas. Habrá dos tipos de revisión, la revisión total y la revisión por muestras. Este procedimiento será realizado dos veces al año y se documentará enviando un informe de la revisión al Supervisor de la Seguridad de la Red.

2.4.3.1 La Revisión Total: Será la revisión de todas las reglas dentro del equipo de seguridad.

2.4.3.2 La Revisión por Muestra: Será la revisión de un número de reglas escogidas al azar para ver el porcentaje de actualización del *Firewall*.

Los cambios en configuración del firewall que sean a las reglas serán adaptadas por el personal a cargo de la red en conjunto con el oficial de seguridad, para garantizar un uso efectivo de las reglas. Cambios en cuanto a desempeño y conexión a nivel de red serán hechos por el personal a cargo de red. Las reglas deben ser discutidas por el oficial de seguridad, gerente de sistemas y el personal a cargo de la red para buscar la aprobación a las mismas. Se utilizará el formulario Revisión de Reglas para documentar lo detectado.

2.5 Procedimientos Administrativos

2.5.1 Proceso de Apelación

Si el Administrador de Sistemas hace una requisición de regla en el *Firewall* que es denegada por el grupo de Seguridad de red, la decisión puede ser apelada por los siguientes canales:


- Director Asociado en Infraestructura Tecnológica
- Director Ejecutivo de la DTAA
- Rector(a) de UPR-RP

2.6 Puntos de Contactos

- DTAA-Service Desk, teléfono: (787) 764-0000 x.7800
- Sección de Telecomunicaciones: (787) 764-0000 x.5900
- Oficina del Director Asociado en Infraestructura Tecnológica de la Oficina para el Desarrollo y Mantenimiento de la Infraestructura: (787) 764-2502
- Oficina del Director Ejecutivo de la DTAA: (787) 764-2258

2.7 Acceso físico

El acceso físico a los firewalls estará restringido al personal de ODMI que tienen acceso al salón de telecomunicaciones. Este acceso lo proveerá el oficial de seguridad en la máquina de seguridad de acceso físico, el mismo será programado en la tarjeta del empleado con los accesos requeridos a su puesto.

	Política y Procedimiento del uso de Firewalls	Código: FW-DTAA-SOP-01
		Versión: 1.1
		Fecha de aprobación: 27/5/2008
		Página: 11 de 11

3. Definiciones de conceptos

LAN (Local Area Network) – es la interconexión de computadoras y estaciones de trabajo en oficinas, fábricas, entre otras para compartir recursos e intercambiar datos y aplicaciones.

WAN (Wide Area Network) – es un tipo de red que da servicio a un país o un continente. Cualquier red en la cual no estén en un mismo edificio todos sus miembros. Este tipo de red es construída por y para organizaciones, empresas o para uso privado como lo son los proveedores de Internet.

Internet – es un método de interconexión descentralizada de redes de computadoras implementando en un conjunto de protocolos denominados TCP/IP y garantiza que redes físicas funcionen como una red lógica única, de alcance mundial.

Firewall (cortafuego) – es un elemento utilizado en una red de computadoras para controlar las comunicaciones, permitiéndolas o prohibiéndolas según las políticas de red ya establecidas. Su modo de funcionar es definido por las características de comportamiento y requerimientos de operabilidad. Su ubicación es en el punto de conexión de la red interna con la Internet, de este modo se protege la red interna de intentos de acceso no autorizado desde Internet aprovechando las vulnerabilidades de los sistemas.

Host (equipo anfitrión) – cualquier computadora que funcione como la fuente de toda información o servicios.

Paquete - información que se transmite con un entero.

Filtro – descarta paquetes del LAN que no sean confiables.