ASEP
Autoridad Nacional
de los Servicios Públicos

Manual de Procedimientos
Oficina de Informática

Procedimiento para Administrar el Firewall

Área	Proceso
Informática	Firewall

Revisado por			Aprobado por
Encargado del Área	Jefe de la Oficina de Informática	Jefe de la Oficina de Desarrollo Institucional	Director Ejecutivo

Código	Estado de Revisión	Fecha de Revisión
P-ASEP-OIT-04	1.0	Enero, 2014

COPIA NO CONTROLADA

CONTENIDO

HISTORIAL DE CAMBIOS

I. ASPECTOS GENERALES

A. OBJETIVO
B. ALCANCE
C. RESPONSABLES
D. NORMAS DE CONTROL INTERNO
E. GLOSARIO
F. DOCUMENTOS DE ORIGEN EXTERNO

II. ACTIVIDADES

III. ANEXOS

1. Bitácora del Firewall
2. Matriz base del Firewall

HISTORIAL DE CAMBIOS

Versión	Fecha del Cambio	Autor	Motivo del Cambio

I. ASPECTOS GENERALES

A. OBJETIVO

Establecer la metodología para definir y administrar las reglas de firewall que aseguren el bloqueo de las entradas y salidas del tráfico no deseado o generado por aplicaciones maliciosas o que permitan el acceso de intrusos a los recursos informáticos.

B. ALCANCE

Este procedimiento aplica a toda la red privada y demás recursos informáticos de la Autoridad Nacional de los Servicios Públicos.

C. RESPONSABLES

- Jefe de la Oficina de Informática
- Jefe de Seguridad de la Oficina de Informática
- Funcionarios de las áreas de Programación, Redes y Servidores de la Oficina de Informática

D. NORMAS DE CONTROL INTERNO

- El incumplimiento de las normas establecidas, se tomará como una falta bajo lo estipulado en el artículo 99 del Reglamento Interno vigente de la ASEP.
- Las reglas del firewall deben ser lo más específicas posibles y crearse de lo específico a lo general.
- Las reglas del firewall deben ser simples para evitar que se creen huecos que permitan el paso de tráfico no deseado a la red de la ASEP.
- Las reglas del firewall deben cubrir los servicios y las aplicaciones necesarias para realizar las funciones de la ASEP.
- Se crearán reglas generales en el firewall con la finalidad de proteger todos los recursos de la ASEP y reglas especiales para permitir la conectividad y proteger aquellas máquinas, aplicaciones y servicios especiales.

- Para la configuración de las reglas del firewall se debe utilizar, como punto inicial, la Matriz base (baseline) del Firewall (ver anexo No. 2) que incluye las diferentes aplicaciones y servicios que son requeridos para el funcionamiento normal de la Autoridad Nacional de los Servicios Públicos, el protocolo que utiliza al transmitir la información, los puertos que usan para enviar y recibir información y las reglas del firewall tanto internas (lo que sale desde la ASEP) como externas (lo que entra a los equipos de la ASEP) con respecto a las aplicaciones y servicios. Esta matriz tiene como base estándares de seguridad internos e internacionales y las necesidades de la entidad.

- Se bloqueará lo siguiente:

    - Todos los paquetes y conexiones del tráfico entrante, a menos que el tipo de tráfico y las conexiones sean explícitamente permitidas.

    - Los paquetes entrantes que contengan tráfico de ICMP (Internet Control Message Protocol).

    - El tráfico entrante y saliente que contenga la dirección de 0.0.0.0 como el destino o la fuente.

    - El tráfico entrante y saliente que contenga la dirección de 127.0.0.1 como destino o fuente.

    - El tráfico entrante y saliente con una dirección IP de una red privada como destino o fuente.

    - El tráfico entrante con una dirección de fuente que indique que el paquete se originó dentro de la red privada de la ASEP.

- Las direcciones de IP que tiene el firewall, la de entrada y la de salida dentro de la red de la sede, las regionales y sucursales de la Autoridad Nacional de los Servicios Públicos deben estar debidamente documentadas.

- La ubicación física y lógica del firewall en la red de la sede, las regionales y sucursales de la ASEP deben estar claramente señaladas en un diagrama.

- Todas las reglas del firewall deben estar documentadas y guardadas en estado físico y/o electrónico para asegurar su disponibilidad y utilización, en caso de emergencia.

- Previo a la actualización de la aplicación administrativa del firewall, se debe verificar que la actualización o el parche que se requiera instalar, no perjudique o comprometa la estabilidad del firewall.

- Las bitácoras del firewall deben ser revisadas diariamente de forma manual o con una aplicación que facilite esta revisión.

- Cada vez que haya un cambio mayor en la infraestructura de la red de la ASEP, las reglas del firewall deben ser revisadas para ajustarlas, a fin de que garantizar su seguridad.

- En caso de que el equipo se administre mediante una conexión remota, es necesario conectarse utilizando una conexión segura mediante SSHv2 o TLS/SSL (ver definiciones en el Glosario).
- La computadora que se utilice para acceder al firewall debe estar asegurada de la siguiente manera:

    - Quitar y/o cerrar aplicaciones y servicios innecesarios.

    - Quitar o deshabilitar del Sistema Operativo, todas las cuentas de usuario o de sistema innecesarias.

    - Aplicar todos los parches de seguridad del Sistema Operativo después de que éstos hayan sido probados en otra computadora y no presenten problemas.

- Efectuar una copia de respaldo del firewall antes de colocarlo en la red o ponerlo a funcionar.

- Las copias de respaldo deben ser completas y contener no solo los datos e información que hayan cambiado desde la última copia de respaldo realizada.

- Semanalmente, verificar el funcionamiento de las copias de respaldo y mantenerlas custodiadas en la caja fuerte de la unidad.

E. GLOSARIO

- **Firewall o cortafuego:** Sistema físico y/o lógico diseñado para prevenir el acceso no autorizado desde o hacia una red privada.

COPIA NO CONTROLADA

- **TLS / SSL - Transport Layer Security o Seguridad de la capa de transporte en el predecesor de Secure Sockets Layer:** Son protocolos que proveen un canal seguro de comunicación mediante la utilización de llaves cifradas, una pública y otra privada.

- **SSH – Secure Shell:** Protocolo de red que permite el intercambio de datos por medio de un canal seguro. Se usa para conectarse a una computadora de forma remota, ejecutar comandos y transferir datos.

F. DOCUMENTOS DE ORIGEN EXTERNO

No Aplica

II. ACTIVIDADES

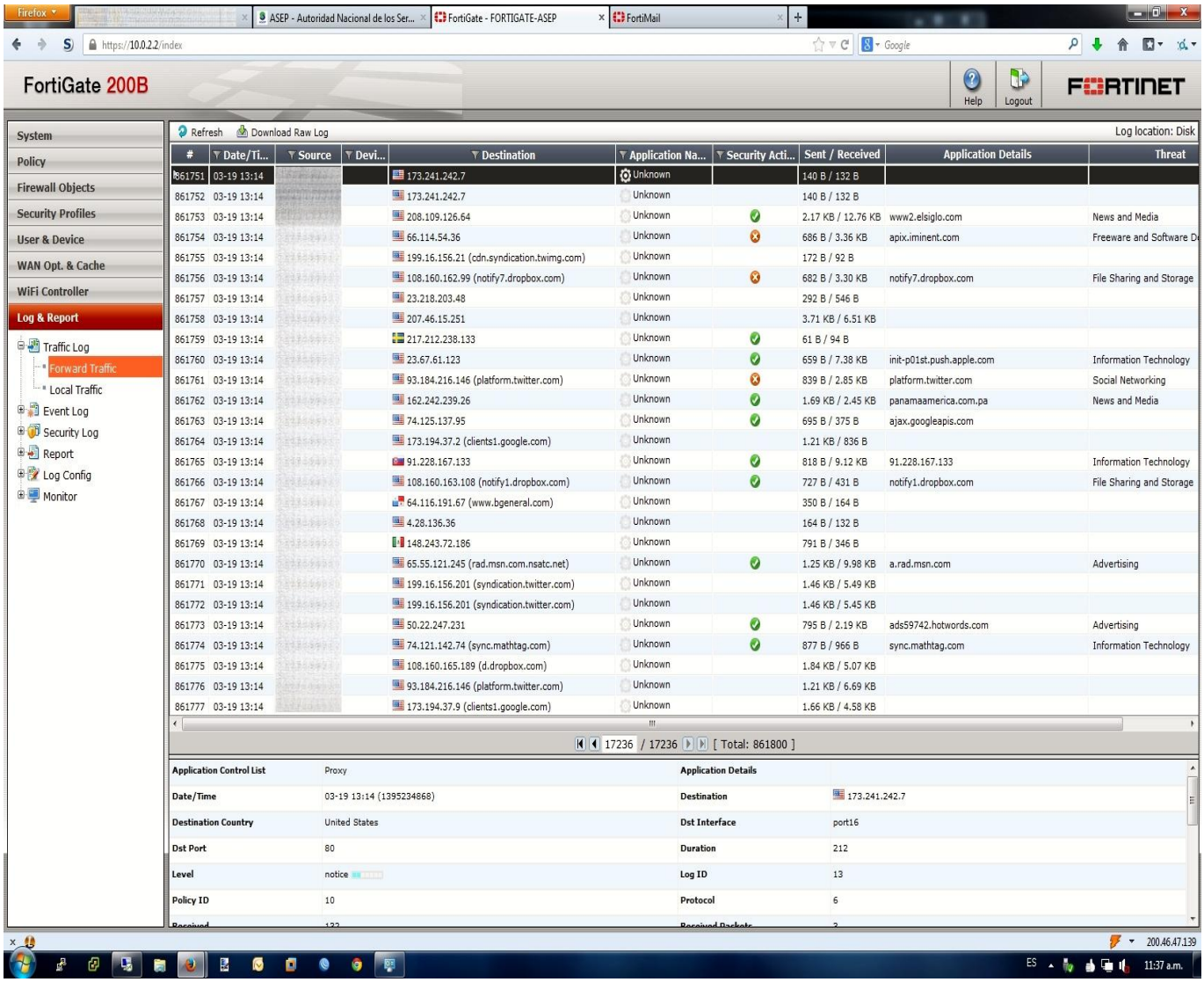
PASO	DESCRIPCIÓN	RESPONSABLE
	Administración del Firewall	
1	Diariamente revisa la Bitácora del Firewall (ver Anexo No. 1) para verificar, entre otras cosas, de qué máquina salió algún paquete, a qué página han entrado los usuarios, qué servicios o sistemas se mantienen.	Jefe de Seguridad de la OIT
2	Monitorea los paquetes que entran y que salen de los equipos de la ASEP.	
3	Si se necesita hacer algún cambio en alguna de las reglas establecidas en el firewall según la Matriz Base del Firewall (ver Anexo No. 2), por algún requerimiento solicitado por el programador, procede a efectuar dicho cambio, mediante el correo electrónico, asimpson@asep.gob.pa o witi_seg@asep.gob.pa autorizado por el Jefe de la OIT. Una vez que la solicitud haya sido atendida por el Jefe de Seguridad de la OIT, comunica al programador por medio de un correo electrónico que la nueva regla fue creada y que realice las pruebas necesarias.	
	Activación del Firewall para nuevas aplicaciones o nuevas Páginas WEB	
4	Desarrolla la aplicación o la nueva página WEB.	Programador
5	Coordina por correo con el Programador, qué requiere del firewall para que la aplicación funcione. La solicitud se realiza por medio de correo electrónico al correo asimpson@asep.gob.pa	Jefe de Seguridad de la OIT
6	Coordina por correo o reunión con el área de Redes la asignación y enrutamiento de la dirección IP y determina la necesidad de desarrollar nuevas reglas.	
7	Coordina por correo o reunión con el área de Servidores para determinar el equipo de servidores que se utilizará en esa nueva aplicación o página WEB.	
8	Una vez que la solicitud haya sido atendida por el Jefe de Seguridad de la OIT, comunica al programador por medio de un correo electrónico que la nueva regla fue creada y que realice las pruebas necesarias.	

COPIA NO CONTROLADA

ANEXOS

ANEXO No. 1

Bitácora del firewall



COPIA NO CONTROLADA

ANEXO No.2

Matriz Base del Firewall

Aplicación/Servicio	Protocolo	Puerto(s)	Regla Interna del Firewall	Regla Externa del Firewall
DNS	TCP/UDP	53	Permitir	Permitir
NetBIOS	TCP/UDP	137,138,139	Permitir	Tumbar
HTTP	TCP/UDP	80	Permitir	Permitir
HTTPS	TCP/UDP	443	Permitir	Permitir
Telnet	TCP	23	Tumbar	Tumbar
SMTP	TCP	25	Permitir	Permitir
IMAPS	TCP	993	Permitir	Permitir
SMTPS	TCP	465	Permitir	Permitir
POP3S	TCP	995	Permitir	Permitir
POP3	TCP	110	Permitir	Permitir
FTP	TCP	20,21	Permitir	Tumbar
ICMP/Basic	ICMP	-	Permitir	Tumbar
MS Global Catalog	TCP	3268	Permitir	Tumbar
UDP	UDP	161	Permitir	Tumbar
Remote Desktop	TCP/UDP	3389, 5900	Permitir	Tumbar
Reloj de Marcación	TCP	3001	Permitir	Solo a direcciones

COPIA NO CONTROLADA

				IP especificas
Claro-Lite (Telecom)	TCP/UDP	5060	Permitir	Permitir
SSHv2	TCP	22	Permitir	Permitir
MySQL	TCP/UDP	3306	Permitir	Tumbar
Microsoft SQL Server	TCP/UDP	1433,1434	Permitir	Permitir
Microsoft Directory Services	TCP/UDP	445	Permitir	Tumbar
DCE Endpoint Resolution (epmap)	TCP/UDP	135	Permitir	Tumbar
Line Printer Spooler	TCP/UDP	515	Permitir	Tumbar
Kerberos	TCP/UDP	88	Permitir	Tumbar
Network Time Protocol	TCP/UDP	123	Permitir	Solo al IP de CENAMEP 200.46.54.198
Simple Network Management Protocol (SNMP)	TCP/UDP	161	Permitir	Tumbar
LDAP	TCP/UDP	389	Permitir	Tumbar

COPIA NO CONTROLADA