Ministerio de Modernización
Presidencia de la Nación

Código ETAP: SR-005-00

Servidores para Firewalls (Cortafuegos)

ETAP Versión 22

Realizado por:
Pablo Ferrante

Índice

1. Vista General de documento

Este documento permitirá agilizar la intervención técnica que realiza la Dirección de Estandarización Tecnológica (DET) en su función de participar en todos los proyectos de innovación tecnológica que abarca, entre otras, la adquisición, implementación, incorporación, e integración de las tecnologías de información en el ámbito del sector público.

En la sección 3, obran las especificaciones técnicas estándares.

El resto del documento y las notas agregadas dentro de recuadros en las especificaciones, contienen comentarios de ayuda, para que los organismos puedan completar fácilmente las especificaciones, seleccionando las características técnicas de los equipos y/o servicios en función de sus necesidades funcionales, por lo que, dichas notas de ayuda y comentarios, no deben ser transcriptas en la especificación final.

En las especificaciones técnicas hemos incluido características y elementos del recurso y/o servicio tecnológico que se detalla, que son ***de inclusión mandatoria*** por entender que los mismos resultan indispensables. Por lo cual, esperamos encontrarlos incluidos en el requerimiento técnico elevado para la intervención.

También hemos incluido características y elementos que son ***opcionales*** en la definición del recurso tecnológico y/o servicio que se detalla, los cuales deberán seleccionarse de acuerdo a sus necesidades funcionales. Para esto se usan “checkboxes” y “radio-buttons”, lo que facilita diferenciar entre grupos de opciones de selección libre, y grupos de opciones de selección mutuamente excluyente, respectivamente.

En ambos casos, describimos o definimos varias características y/o elementos, para que los organismos seleccionen las que más se ajusten a sus necesidades. En consecuencia, una vez que se seleccione la o las características y/o elementos deseados, las opciones no seleccionadas deberán eliminarse de la especificación.

El documento cuenta con 3 secciones:

Sección	Tema desarrollado en la sección
Vista General	La sección de *vista general de documento* detalla la forma de uso y las secciones que componen este documento.
Descripción del Estándar	Esta sección provee una breve Descripción del Estándar que se va a especificar.
Especificación Técnica	La sección de *Especificación Técnica* detalla las características generales y particulares del recurso tecnológico o servicio.

2. Descripción del Estándar

Servidores para Firewalls (Cortafuegos).

3. Especificación Técnica - SR-005-00 Servidores para Firewalls (Cortafuegos)

Esta sección provee el detalle técnico del recurso tecnológico definido en la descripción del estándar.

3.1 Características Generales

- Consideraciones Especiales para servidores definidas en CESP-001, CESP-002, CESP-005, y de corresponder CESP-006.
- Para la implementación de este tipo de servidor, se podrá optar por una de las 3 opciones siguientes: (1)

☐ Servidores de Red Genéricos – Arquitectura basada en X86 (SR-001).

☐ Servidores de Red Genéricos – Arquitectura RISC/EPIC (SR-002).

☐ Dispositivo del tipo “black-box” o “caja negra”, dedicado al filtrado de paquetes y servicios de red.

Nota : Se deberá tener en cuenta que no se puede dar una configuración específica ya que esto depende de varios parámetros que el organismo tendrá que considerar:

En los firewalls basados en servidores, la capacidad de disco necesaria es la que requiera el sistema operativo, el software del firewall propiamente dicho y los logs de operación. Por lo que la capacidad a solicitar deberá calcularse de acuerdo al tamaño de la imagen del S.O., del programa del firewall / aplicativos de soporte y del espacio de logging que se quiera mantener, el cual dependerá del tráfico de red y del nivel de detalle de la información que el organismo quiera obtener a los fines de analizar los posibles ataques o accesos indebidos.

La implementación mínima de un firewall requiere por lo menos dos placas de red, o bien de una placa multipuerto con al menos 2 puertos incorporados. Una placa conecta la red LAN interna del organismo con el firewall y la otra conecta el firewall a la Internet. En el caso de que el organismo decida aplicar políticas de máxima seguridad implementando subredes con diferentes niveles de seguridad, será necesario comprar más placas de red (o solicitar más puertos Ethernet para el caso black-box) según corresponda.

No es conveniente requerir interfaces más rápidas que los enlaces que se cursarán a través del equipo. Es innecesario requerir puertos Gigabit Ethernet si el firewall se utilizará solamente para enlaces de Internet, ya que estos difícilmente superen los

10Mb/s, y menos aún los 100Mb/s.

3.2 Detalle Técnico / Funcional

a) Opcionales Sólo Para Firewalls Del Tipo "Black-Box":

Deberá contar con interfaces de red con las siguientes características:

Capacidad de operación full duplex (IEEE 802.3x).

☐ Agente SNMP incluido. (3)

☐ Capacidad de administración vía RMON ó Wired For Management (WFM)(3)

☐ _____ (4) puertos Ethernet/FastEthernet 10/100BaseTX con las siguientes características:

Bite rate: 10/100 Mbps (autosensing).

Estándar: IEEE 802.3i 10BaseT, IEEE 802.3u 100BaseTX.

Conexión: UTP con conectores de salida RJ45.

☐ _____ (4) puertos Gigabit Ethernet con las siguientes características:

Bite rate: 10/100/1000 Mbps (autosensing).

Estándar: IEEE 802.3ab 1000BaseT

Conexión: UTP con conectores RJ45.

☐ 1 port Gigabit Ethernet 802.3z 1000BaseSX.

b) Software A Proveer Con El Firewall:

Si el software del firewall lo requiere, se deberán incluir en la cotización las licencias de conectividad que sean necesarias, a fin de brindar servicio a un máximo de _____ (3) usuarios concurrentes.

Deberá ser compatible con el sistema operativo instalado en el server/equipo

Deberá poseer los requerimientos mínimos que a continuación se detallan, consistentes en la capacidad de filtrar paquetes de red:

Por protocolo. (Por ejemplo IP, ICMP, etc.)

Por dirección IP fuente y/o destino.

Por puerto TCP/UDP fuente y/o destino (que identifica la aplicación).

Por interfaz de red (NIC) del firewall (admitiendo o no el ingreso/egreso de un paquete dependiendo de la interfaz de red involucrada).

Por estado de la conexión, es decir, si es nueva o si ya está establecida (Statefull Inspection).

Permitir el análisis del tráfico admitido y denegado, mediante la generación de registros detallados de auditoría.

c) Opcionales Para El Software:

☐ Administración bajo interface gráfica.(5)

☐ Administración centralizada para múltiples firewalls.(6)

☐ Soporte de Network Address Translation (NAT)

☐ Soporte de Virtual Private Networks (VPN) estándar basadas en IPSEC con autenticación utilizando mínimamente algunos de los métodos “PRE SHARED KEYS” o “PAR DE CLAVES pública/privada”.

☐ Administración remota a través de canal encriptado.

☐ Funcionalidad de Proxy en aplicaciones seleccionadas

Mínimamente debe permitir operar y tomar decisiones de filtrado basadas en el contenido de los servicios SMTP, FTP y HTTP.

Proveer autenticación de usuarios de una forma no basada en contraseñas estáticas y reutilizables, las que pueden ser fácilmente obtenidas utilizando “sniffers”.

☐ Soportar distintos esquemas de autenticación a saber.(2)

☐ Password de Sistema operativo

☐ S/key

- ☐ OTP (One Time Programming) Tokens
- ☐ RADIUS
- ☐ LDAP
- ☐ TACACS/TACACS+
- ☐ Certificados Digitales
- ☐ Admitir algoritmos estándares de encriptación como DES, TRIPLE DES y IPSec/IKE.

(1)Seleccionar aquellas opciones que se requieran adjuntar a la especificación.

(2)Se podrán seleccionar las opciones que sean necesarias, de acuerdo a las que estén siendo utilizadas o estén por utilizarse en el organismo.

(3)Se recomienda solicitar estos opcionales, sólo en el caso de que el organismo ya este utilizando este tipo de administración.

(4)Indicar la cantidad de puertos Ethernet/FastEthernet/Gigabit Ethernet necesarios según las subredes que se deseen implementar. Típicamente 2 a 4 puertos.

(5)La solicitud de administración con interfaz gráfica no es necesaria en la mayoría de los casos.

(6)En caso de que el organismo posea varios firewalls, puede ser más conveniente poseer un único punto de administración centralizado. No obstante, esto deberá decidirse de acuerdo a las políticas de seguridad del organismo, y a la necesidad de su uso.