

Alcance y descripción del servicio

FIREWALL VIRTUAL VS - **RINGO**



1. Introducción

Firewall Virtual VS IPLAN es la mejor opción para aquellas empresas que desean tener un nivel de seguridad adicional para su Servidor Virtual IPLAN, sin incurrir en altos costos vinculados a la adquisición, mantenimiento, renovación y crecimiento del equipamiento. Sobre una plataforma tecnológica de última generación provista por IPLAN, podrá tener su Servidor Virtual IPLAN securizado con la mejor relación precio / prestaciones del mercado.

2. Descripción General y Alcance

Firewall Virtual VS IPLAN entrega diferentes variantes en cuanto a las opciones de configuraciones del servicio:

- a. Dirección IP para Firewall – MANDATORIO
- b. Servidores en la LAN – MANDATORIO (con Opciones)
- c. Funcionalidades default para Firewall - MANDATORIO
- d. Funcionalidades adicionales – OPCIONAL

a. Dirección IP para Firewall (MANDATORIO)

La dirección IP es del tipo pública y estática en Internet. Actualmente, sólo se puede tener una única dirección IP pública con el servicio Firewall Virtual VS IPLAN. En caso de utilizar más de un Servidor Virtual IPLAN en la red LAN (Local Area Network) interna, se configurará el firewall para utilizar la modalidad de PAT (Port Address Translation), la cual permite a varias máquinas salir a Internet a través de una sola dirección IP pública.

b. Servidores en la LAN (MANDATORIO)

Determina la cantidad de Servidor Virtual IPLAN que se tienen en la red LAN (Local Area Network) interna. Actualmente, con Firewall Virtual VS IPLAN se pueden tener desde uno (1) a tres (3) Servidor Virtual IPLAN en la red LAN interna. En caso de requerir un número mayor de Servidor Virtual IPLAN en la red LAN interna, deberá consultarlo con su Ejecutivo de Cuentas.

c. Funcionalidades default para Firewall (MANDATORIO)

Los componentes básicos son:

Firewalling

- Firewall de perímetro (layer 3)
- SIP (Stateful Inspection Firewall) con reglas de control de conexiones entrante y saliente basadas en parámetros como dirección IP (fuente/destino), ports (fuente/destino), tipo de protocolo (TCP o UDP).

NAT / PAT (Network Address Translation / Port Address Translation)

- Traslación de direcciones IP hacia y desde el entorno del Servidor Virtual
- Enmascaramiento de direcciones IPs para lugares poco confiables

DHCP (Dynamic Host Configuration Protocol)

- Provisión de direcciones IP automáticas para el/los Servidor Virtual
- Parámetros definidos por el administrador (tales como conjunto de direcciones, tiempo de persistencia de direcciones, direcciones IP dedicadas)

Site to Site VPN (Virtual Private Network)

IPLAN

- IPSec VPN (Virtual Private Network) con soporte para autenticación por certificado así como shared key, basado en el protocolo IKE (Internet Key Exchange)

d. Funcionalidades adicionales (OPCIONAL)

Los componentes opcionales son:

Web load balancing

- Balanceo de carga entrante para todo el tráfico hacia los Servidores Virtuales incluyendo tráfico Web (http)
- Algoritmo round-robin
- Soporte para "sticky" sessions (todas los requerimientos relacionados serán enviados al Servidor Virtual que manejó el primer requerimiento de una consulta)

3. Restricciones comerciales y técnicas

- Sólo una (1) dirección IP pública y estática de Internet
- Hasta tres (3) Servidor Virtual IPLAN por cada Firewall Virtual VS IPLAN (cada Servidor Virtual IPLAN adicional tiene un cargo mensual adicional)
- La cantidad de cambios de configuración del Firewall Virtual VS IPLAN permitidos son 4 mensuales no acumulativos
- La funcionalidad Web load balancing tiene un cargo mensual adicional

4. Centro de Atención al Cliente

A través del Centro de Atención al Cliente de IPLAN, el cliente podrá ingresar reclamos o consultas en la modalidad 7x24.

5. Acuerdo de Nivel de Servicio

Los siguientes puntos muestran el alcance de los servicios.

- Se brindará soporte ante incidentes de Hardware y conectividad en modalidad 7 x 24 x 365.
- Disponibilidad estadística de la Plataforma: 99,9% anual.

Servicios adicionales: el Cliente contará con la opción de solicitar servicios adicionales a los anteriormente listados. IPLAN se compromete a evaluar la solicitud efectuada por el Cliente y a entregar una propuesta comercial que refleje los términos y condiciones aplicables a dicha contratación en caso de ser posible brindar los nuevos servicios solicitados por el Cliente.

6. Responsabilidades por parte del Cliente

El Cliente es responsable por la seguridad de su Servidor Virtual IPLAN, salvo expresa delegación de la administración de seguridad a IPLAN.

El Cliente es responsable por la integridad de su información. En ningún caso IPLAN será responsable por daño emergente, lucro cesante y/o cualquier otra pérdida que pudiera sufrir el Cliente como consecuencia directa o indirecta de la prestación de los servicios aquí detallados.



7. Limitaciones del Servicio

IPLAN no se hace responsable por la integridad, inconsistencia y/o pérdida de los datos que puedan ocasionar las fallas que involucren a los componentes del equipo adquiridos (hardware o software) ni errores humanos de terceros ajenos a IPLAN.

IPLAN no efectuará la gestión de la seguridad en el Firewall, entendiéndose por gestión de la seguridad a todas aquellas tareas derivadas de la propia operación y control de la seguridad; quedando dichas tareas bajo estricta responsabilidad del Cliente.

8. Acerca de IPLAN

En la actualidad IPLAN cuenta con la Certificación ISO 9001. El Datacenter RINGO se encuentra certificado bajo la norma de gestión de calidad a nivel mundial ISO9001, garantizando la adhesión a las más estrictas políticas de seguridad de la información.

De tal forma y continuando con su compromiso en relación a las mejoras continuas y el cumplimiento con los estándares de reconocimiento internacional, IPLAN mediante auditoría realizada, verificó el cumplimiento de los requisitos recogidos en la norma ISO 9001:2008.

.....
Firma del Cliente

.....
Aclaración

FECHA __/__/__