DESCRIPCIÓN Y ALCANCE DEL SERVICIO DE NSS S.A.
INTERNET PROTECT IPLAN

1. Introducción

El servicio INTERNET PROTECT de IPLAN provee una conexión a Internet permanente, simétrica, de alta confiabilidad, máxima seguridad y alta velocidad.

El servicio INTERNET PROTECT de IPLAN, es un servicio que tiene como objetivo proteger la infraestructura de Internet de los clientes contra Ataques Distribuidos de Denegación de Servicio, que intentan sobrecargar los recursos de red y servicios, afectando su disponibilidad.

¿Qué es un Ataque Distribuido de Denegación de Servicio? Un Ataque de Denegación de Servicio, también llamado ataque DoS (de las siglas en inglés Denial of Service), es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios que realizan transacciones y/o acceden en forma legítima. Normalmente provoca la pérdida de la conectividad de la red de acceso del cliente, por el consumo excesivo del ancho de banda de la red de la víctima o sobrecarga de los recursos del sistema de computación de la víctima.

Un ataque se genera mediante la saturación intencional de los puertos con flujo de información, haciendo que los recursos se sobrecarguen y no puedan seguir prestando servicios, por eso se le dice "denegación", pues hace que los servidores no tengan capacidad de responder a los usuarios que acceden en forma legítima. Esta técnica es usada por los llamados hackers para dejar fuera de servicio a servidores objetivo.

Una ampliación del ataque DoS es el llamado Ataque Distribuido de Denegación de Servicio, también llamado ataque DDoS (de las siglas en inglés Distributed Denial of Service), el cual se lleva a cabo generando un gran flujo de información desde varios puntos de conexión.

El servicio INTERNET PROTECT mitiga automáticamente una amplia gama de ataques DDoS, sin intervención humana, manteniendo una conectividad completa para evitar interrumpir la entrega de tráfico legítimo, deteniendo los ataques más rápidamente. Está optimizado para la utilización de aplicaciones en un entorno de oficina / corporativo / revendedor (ver detalle en el apartado siguiente).

Es sabido que Internet es un conjunto descentralizado de redes de comunicaciones interconectadas, que utilizan familias de protocolos para permitir que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Para asegurar los niveles de servicio dentro de la Internet, los distintos proveedores trabajan en mantener sus propias redes y las interconexiones de las mismas con otros proveedores. Al respecto, IPLAN posee una red de última generación acorde a las necesidades actuales de clientes y aplicaciones, de máxima calidad y escalabilidad.

2. Descripción general y alcances

La velocidad de acceso indica la capacidad máxima del vínculo de interconexión a Internet brindado por el servicio de IPLAN. Dicha velocidad es simétrica, lo que implica que se puede alcanzar la velocidad contratada tanto en sentido hacia como desde Internet, simultáneamente. Con este servicio se garantiza la posibilidad de alcanzar el 100% del total de ancho de banda contratado hasta el último extremo de la red de IPLAN.

Acorde a un servicio para empresas, con el servicio se incluye 1 (una) dirección IP pública y fija (la dirección IP no cambia al reiniciarse el equipamiento de acceso instalado en el cliente, como ocurre con los servicios provistos mediante DHCP –Dynamic Host Configuration Protocol-). Un número mayor de direcciones IP podrá ser contratado con posterioridad a la contratación del Servicio. Cabe aclarar que si la contratación del adicional de direcciones no se realiza en la etapa inicial de contratación del Servicio, esto implicará un cambio del rango de direcciones IP actual. Para acompañar la migración, IPLAN permitirá la convivencia del rango actual y el nuevo rango por un período de 15 días corridos, tras lo cual se dará de baja el rango original, salvo que la contratación de IP sea adicional a la contratación precedente, lo cual permitirá conservar ambos rango.

Típicamente, la utilización de Internet, para un entorno de oficina / corporativo / revendedor, se enmarca dentro de la categoría de: buscadores y navegación por páginas Web, navegación y lectura de páginas de noticias /

diarios online, envío y recepción de mails en modalidad usuario y/o servidor, utilización de redes sociales, utilización de plataformas de e-commerce en modalidad usuario y/o servidor, utilización de plataformas de e-learning en modalidad usuario y/o servidor (audio, video y documentos), utilización de plataformas de hosting de páginas Web en modalidad servidor, utilización de plataformas de streaming de audio y video en modalidad usuario y/o servidor (radios online, reproducción de video online), chat de texto y video en modalidad usuario y/o servidor, videoconferencia, cloud computing ó software as a service en modalidad usuario y/o servidor , VPNs –Virtual Private Networks- en donde las aplicaciones a utilizar sean muy sensibles al delay, Call Centers de VoIP –Voice over IP-, descarga y/o intercambio de archivos de misión crítica, utilización de Internet para revender a terceros, no siendo esta lista exhaustiva ni excluyente.

La concurrencia de usuarios en Internet está directamente relacionada con el consumo de ancho de banda total (una mayor concurrencia implica un mayor consumo de ancho de banda total). Consultar con su representante de Ventas para un adecuado dimensionamiento del servicio en función de la cantidad / concurrencia de usuarios y el perfil de consumo requerido.

A continuación se muestra una tabla con las características del servicio INTERNET PROTECT:

Característica		INTERNET PROTECT
Conectividad	Velocidad de acceso	de 100 a 300* Mbps
	Simetría	SI
	Garantía ancho de banda	Se da por escrito garantía sobre el total de ancho de banda dentro de la red Internet de IPLAN**
Direccionamiento IP	Privado / Público	Público
	Dinámico / Estático	Estático
	Cantidad***	1 (una)
	Cantidad adicional***	hasta 15 con cargo adicional
Perfil de usuario		Utilizan Internet como “core” para su trabajo y/o el funcionamiento de la empresa (es una herramienta de misión crítica en la operatoria de la empresa)
Aplicaciones****		Estándar + avanzadas + misión crítica
Acuerdo de Niveles de Servicio (SLA)*****		SI (especificación disponible a requerimiento del cliente)

* Velocidades superiores a 300 Mbps requerirán de una factibilidad técnica.

** Ver Límites del Servicio donde se hace referencia al control de Internet.

*** Las cantidades se determinan en subredes de 4, 8 y 16 direcciones IPs. Del número total de IPs se deben descontar 3 IPs, que son utilizadas internamente por IPLAN, para determinar el número de IPs disponibles para el cliente. Esta facilidad está sujeta a disponibilidad por parte de IPLAN.

**** El detalle orientativo de las aplicaciones se describen en este apartado

***** Es un contrato escrito entre IPLAN y el cliente, con el objeto de fijar un acuerdo de nivel para la calidad del servicio

El servicio de Internet se entrega mediante un equipo ONU (Unidad de Red Óptica) que cuenta con 1 (una) interface RJ-45 hembra y un cable de red UTP Ethernet de 1 (uno) metro de longitud, como punto de acceso a la red LAN del cliente y delimitación del servicio.

INTERNET PROTECT tiene como objetivo proteger la infraestructura de Internet de los clientes contra ataques que intentan sobrecargar los recursos de red y servicios, afectando su disponibilidad. El equipamiento del Cliente recibe tráfico de usuarios finales, tanto sea genuino como malicioso. INTERNET PROTECT realiza, a través de su

plataforma de detección, un monitoreo continuo de los patrones y perfiles de tráfico del cliente, lo cual permite una detección en forma temprana de un ataque DDoS.

Detecta rápidamente los ataques DDoS de todos los tamaños no solo bloqueando los ataques volumétricos grandes comúnmente asociados con DDoS, sino también detectando y bloqueando quirúrgicamente los ataques más comunes que usan los mismos vectores, muchos de los cuales son demasiado pequeños o de corta duración para ser mitigados por soluciones heredadas, garantizando la continuidad del servicio y la seguridad de los clientes. Es una solución que protege a los Clientes de Internet contra ataques de denegación de servicio DDOS de capa 3 y capa 7 automáticamente con tiempos de identificación y mitigación de ataques de menos de 5 minutos.

Mitiga automáticamente una amplia gama de ataques DDoS, sin intervención humana, manteniendo una conectividad completa para evitar interrumpir la entrega de tráfico legítimo, deteniendo los ataques más rápidamente.

El servicio Internet PROTECT incluye las siguientes especificaciones técnicas y configuraciones:

1. Detección y mitigación automáticas de ataques.
   1.a Anomalías de tráfico como: paquetes inválidos, paquetes malformados, suma de comprobación inválida, encabezado inválido y fragmentos inválidos.
   1.b Capacidad de implementación de protecciones granulares de ataques DDoS volumétricos a partir de 100 Mbps del Cliente.
2. Recepción de alertas automáticas enviadas por correo electrónico y disponibles en el portal web.
3. Mitigación de ataques DDoS volumétricos para el tráfico de Internet del Cliente.
4. Recepción del tráfico limpio del Cliente limitado al ancho de banda contratado.
5. Soporte para múltiples técnicas de mitigación: Inyección de agujeros negros, limpieza, filtrado y mitigación del tráfico.
6. Acceso al portal web para el Cliente.

A continuación se detallan los tipos de ataques y los anchos de banda mínimos para la detección de cada uno de ellos:

Lista de Ataques	Tipo	Identificado Como	Umbral de detección de "Paquetes por segundo"	Umbral de detección de "Ancho de banda (Mbps)"
ACK Attack of ACK-PUSH-FLOOD	Volumétrico	TCP ACK flood	15	40
DNS AMPLIFICADO	Volumétrico	UDP flood source port 53	30	80
DNS FLOOD	Volumétrico	UDP flood source port 53	10	50
Fraggle Attack	Volumétrico	UDP flood	450	1200
Fragmented ACK Flood	Volumétrico	TCP ACK flood / Fragment	15	40
ICMP Flood	Volumétrico	ICMP flood	10	10
ICMP Fragmentation Flood	Volumétrico	ICMP flood / Fragment	10	10
IP NULL	Volumétrico	IP Null - Malformed packet	10	10
Memcached Attack	Volumétrico	Memcached	20	100
Miral Botnet	Volumétrico	Mirai	10	10
Non-Spoofed UDP Flood	Volumétrico	UDP flood	450	1.2
NTP Amplified (Reflective)	Volumétrico	UDP flood source port 123	20	100
NTP Flood	Volumétrico	UDP flood source port 123	20	100
Other Amplified Attacks (Reflective)	Volumétrico	UDP flood	450	1.2
Ping Flood	Volumétrico	ICMP flood	10	10
RST/FIN Flood	Volumétrico	TCP RST/FIN flood	20	100
Same Source/Dest Flood	Volumétrico	ICMP flood	10	10

Smurf Attack	Volumétrico	ICMP flood	10	10
Specially Crafted Packet	Volumétrico	Malformed packet	20	60
SYN Flood	Volumétrico	TCP SYN flood	15	40
SYN-ACK Flood	Volumétrico	TCP SYN-ACK flood	25	60
TCP Null	Volumétrico	TCP Null flood	25	60
TOS Flood	Volumétrico	IP flood	20	60
UDP Fragmentation	Volumétrico	UDP flood	10	50
Volumetric Attack	Volumétrico	IP flood	800	2

En función a los umbrales de detección mencionados anteriormente, su contratación estará disponible para servicios de Internet cuyas velocidades sean mayores a los 100 Mbps.

El Cliente dispondrá de una web de monitoría a través de la cual dispondrá de una visión general del tráfico y, a su vez, los detalles del ataque. Cabe destacar que cuando se perciba un ataque y sea detectado, se informará al Cliente vía email, si así lo tuviese configurado. Por este motivo es muy importante que el Cliente configure el aviso por correo electrónico y mantenga actualizados los datos en todo momento.

Al poseer una subred exclusiva, las rutas del tráfico serán únicas, es decir, no es posible realizar un cambio de rutas por inconvenientes contra destinos particulares o generales.

Respecto de cualquier otro tipo de ataque recibido por el Cliente que no sea de los indicados en el cuadro precedente, se realizarán los mejores esfuerzos por detectarlo y mitigarlo, sin garantizar ni comprometer su identificación y / o filtrado.

En caso que el ataque provoque inconvenientes en algún equipo del Core de la red de IPLAN o de algún cliente de IPLAN y que el mismo no logre ser detectado y/o mitigado por la plataforma, como medida preventiva, se contactará al Cliente para informar de la situación y se bloqueará el tráfico entrante y saliente hacía la interface destino, es decir, se bloqueará el acceso a Internet sobre el enlace contratado por el Cliente. Una vez que el ataque cese, IPLAN restablecerá el servicio. Al contratar el Servicio el Cliente autoriza a IPLAN a efectuar el bloqueo en el supuesto mencionado precedentemente y expresamente renuncia a reclamar daño alguno por dicho bloqueo ya que el mismo es llevado a cabo para preservar la red IPLAN y el servicio que brinda a sus clientes.

2.1 Centro de atención al usuario

El Cliente dispone de acceso al Centro de Ayuda IPLAN, donde encontrará los manuales de uso de los servicios y una guía de preguntas técnicas y administrativas frecuentes para resolver las distintas necesidades que se presenten.

A su vez, dispone de la Zona de Clientes donde podrá descargar su factura, generar las solicitudes y reclamos técnicos o administrativos y gestionar los servicios contratados.

Para el acceso a dicho servicio el Cliente deberá disponer de su código de gestión personal (CGP), disponible en su factura. En caso de ser un Cliente nuevo, el mismo podrá gestionar dicho código a través de la Zona de Clientes en la Web de IPLAN.

Asistencia técnica y reclamos: a través del portal Web www.iplan.com.ar, o bien en forma telefónica al Centro de Atención al Cliente a los teléfonos: 5032-0000 y 0800-345-0000 las veinticuatro (24) horas del día, los trescientos sesenta y cinco (365) días del año.

El Cliente es responsable de mantener actualizada su información de contacto en el sistema que IPLAN pone a disposición de forma tal que eficientice cualquier necesidad de comunicación por parte de IPLAN.

2.2 Instalación y puesta en marcha del Servicio

El Plazo estimado de instalación / activación del Servicio indicado en el Contrato de Servicios, en el Anexo Comercial y/o en la Solicitud de Servicios, comenzará a contar a partir del momento en que el Cliente, entregue a IPLAN, el permiso y la información que resulte necesaria para permitir el acceso a los domicilios consignados, a efectos de instalar el equipamiento para la prestación de los Servicios y/o brinde la información y parámetros de configuración que los Servicios a implementar requieran.

En caso que la provisión del Servicio contratado requiera una instalación física en el domicilio del Cliente, la puesta en marcha del Servicio será realizada por el personal de IPLAN o terceros que actuarán en nombre de IPLAN, quienes dejarán el Servicio en condiciones de ser prestado y solicitarán al Cliente el conforme vía la firma del Formulario de Aceptación de Servicios (FAS). La firma de dicho formulario asume la conformidad del Cliente respecto de la instalación y de la capacidad de utilizar el Servicio en cuestión.

En caso que el Servicio sea una mejora a un servicio preexistente, que no requiera presencia física del personal de IPLAN en el domicilio del Cliente, IPLAN determinará el mejor medio para comunicar que se ha comenzado la prestación de dicho Servicio.

Se deja constancia que la entrada en vigencia de la prestación del Servicio se encuentra sujeta a factibilidad técnica e IPLAN no tendrá responsabilidad alguna en caso que el Servicio no pueda ser brindado por encontrarse el Cliente fuera del área de cobertura de IPLAN y/o por demoras y/o imposibilidad de completar las tareas de instalación del Servicio debido a: i) restricciones de acceso que pudieran producirse por falta de autorización por parte de la Administración del Edificio, para acceder u ocupar las áreas comunes dentro del mismo donde fuera necesario instalar equipamiento para la prestación del Servicio y/o ii) por falta de aprobación u otorgamiento de los permisos municipales que pudieran ser requeridos para realizar las tareas de instalación en la vía pública que fueran necesarias

3. Responsabilidades del Cliente

Para una correcta instalación del Servicio, el Cliente deberá tener en cuenta lo solicitado a continuación:

- Cableado de red desde el sitio donde se encuentra el CPE de Internet hasta cada uno de los puestos de trabajo. El cableado debe ser categoría 5e ó superior.

- El lugar deberá poseer suministro eléctrico al momento de la instalación. Deberán existir tomacorrientes para PCs, monitores y cualquier otro dispositivo electrónico. Adicionalmente, se requiere un tomacorriente disponible donde se instalará el enlace a Internet, para conectar el CPE provisto por IPLAN.

- Ports Ethernet libres para conectar en red las PCs y el equipamiento informático en cada puesto de trabajo, por medio de uno o más Switches que tengan las capacidades de Switch y no de Hub.

- Se recomienda la utilización de Switch / Router con capacidades de configuración de la velocidad de negociación en la interface de red Ethernet en forma manual. Se desaconseja la utilización de Switch /Router del tipo hogareño, en donde la velocidad sólo se establece automáticamente (por autosense).

- Deberán contar con un rack o un espacio adecuado acondicionado para centralizar todo el cableado y equipos de comunicaciones de forma prolija. Preferentemente, el sitio no deberá encontrarse en proceso de remodelación y/o etapa de obra.

- El técnico deberá tener acceso a la terraza del edificio, como a los montantes y/o subsuelo.

4. Propiedad y uso de los equipos

El Cliente reconoce que IPLAN es y continuará siendo durante todo el plazo de vigencia de la prestación de los Servicios titular del dominio de los equipamientos que utilice a los efectos de la prestación de los Servicios (“Equipamiento”). El Cliente como guardián y beneficiario de los Servicios que se prestan con el Equipamiento desde su instalación, tomará todas las medidas de hecho o de derecho, necesarias para evitar cualquier turbación

de hecho y/o de derecho sobre el Equipamiento, comunicando a IPLAN cualquier circunstancia que potencialmente pudiera ocasionar u ocasione tal turbación en cuanto llegara a su conocimiento. En atención a lo establecido, IPLAN facturará al Cliente todos aquellos cargos que se originen en el proceso de recuperación y ejercicio del legítimo derecho de dominio sobre el Equipamiento en caso de tal turbación. En caso de robo o hurto del Equipamiento, el Cliente deberá efectuar dentro de las veinticuatro (24) horas de sucedido el siniestro, la denuncia policial, notificar a IPLAN sobre lo sucedido por escrito y adjuntar copia de la denuncia policial. IPLAN tomará las medidas apropiadas para la recuperación del Equipamiento, con cargo al Cliente, quien deberá hacerse asimismo responsable por el costo del Equipamiento.

El Cliente mantendrá completamente visible la leyenda colocada sobre el Equipamiento, señalando al Cliente y a terceros que IPLAN es el propietario del mismo. El Cliente no podrá vender, ceder, rentar u ofrecer como garantía, o disponer en cualquier manera, el Equipamiento o sus partes.

Finalizada la prestación de los Servicios, por cualquier motivo, el Cliente devolverá a IPLAN el Equipamiento en perfecto estado de conservación, dentro del plazo de tres (3) días contados desde la finalización de la prestación de los Servicios, sin que el Cliente tenga derecho a retener el Equipamiento por razón alguna. En caso que el Cliente se niegue a devolver el Equipamiento, el Cliente autoriza a IPLAN a facturarlo, de acuerdo al valor vigente de mercado.

5. Límites del Servicio

El Cliente reconoce que IPLAN no puede ejercitar control sobre el contenido de la información que circula a través de la red Internet. Por lo tanto, IPLAN no es responsable del contenido de ningún mensaje y/o información tanto si el envío fue hecho o no por un cliente de IPLAN.

La seguridad informática en los equipos del Cliente contra intrusos, virus, hackers, etc., es exclusiva responsabilidad del propio Cliente. IPLAN recomienda el uso de programas Antimalware, Firewalls y cualquier software ó hardware vigente y actualizado que evite estos ataques.

El resguardo de la información en los equipos / sistemas del cliente queda bajo su exclusiva responsabilidad. IPLAN recomienda el uso de software ó hardware para resguardo y respaldo de la información almacenada en los equipos y sistemas del cliente.

Tanto el hardware como el software que el Cliente decida incorporar luego del Punto Terminal de Red de IPLAN deben estar debidamente homologados, cumplir con las normas técnicas emitidas por la Autoridad de Aplicación en la materia y deberán adecuarse a la tecnología utilizada por IPLAN, todo ello en cumplimiento de la normativa legal y regulatoria vigente en la materia.

El Cliente reconoce que IPLAN no tiene el control absoluto, extremo a extremo, en una conexión INTERNET siendo que la velocidad de transferencia trasciende la red de IPLAN y sus interconexiones directas. No obstante, IPLAN se compromete a mantener el extremo de la red bajo alcance, hasta la frontera con los diversos “Carriers” de interconexión local e internacional, con los más altos niveles de prestación de servicio, conforme la variante de producto.

IPLAN se reserva el derecho de realizar cambios y/o modificaciones del servicio de INTERNET si el consumo de ancho de banda supera límites de consumo netamente corporativo.

Cualquier servicio adicional al especificado en este documento requerido a IPLAN, será facturado como adicional al cargo de instalación y abono mensual convenido.

....

Firma del Cliente **Aclaración**

FECHA __/__/__