Seguridad y Ciber-guerra: Puntos críticos a considerar en una estrategia de Continuidad del negocio frente a Ataques dirigidos y otros posibles fallos de infraestructura o sistemas.

Yovani Piamba Londoño
Sales Engineer NOLA

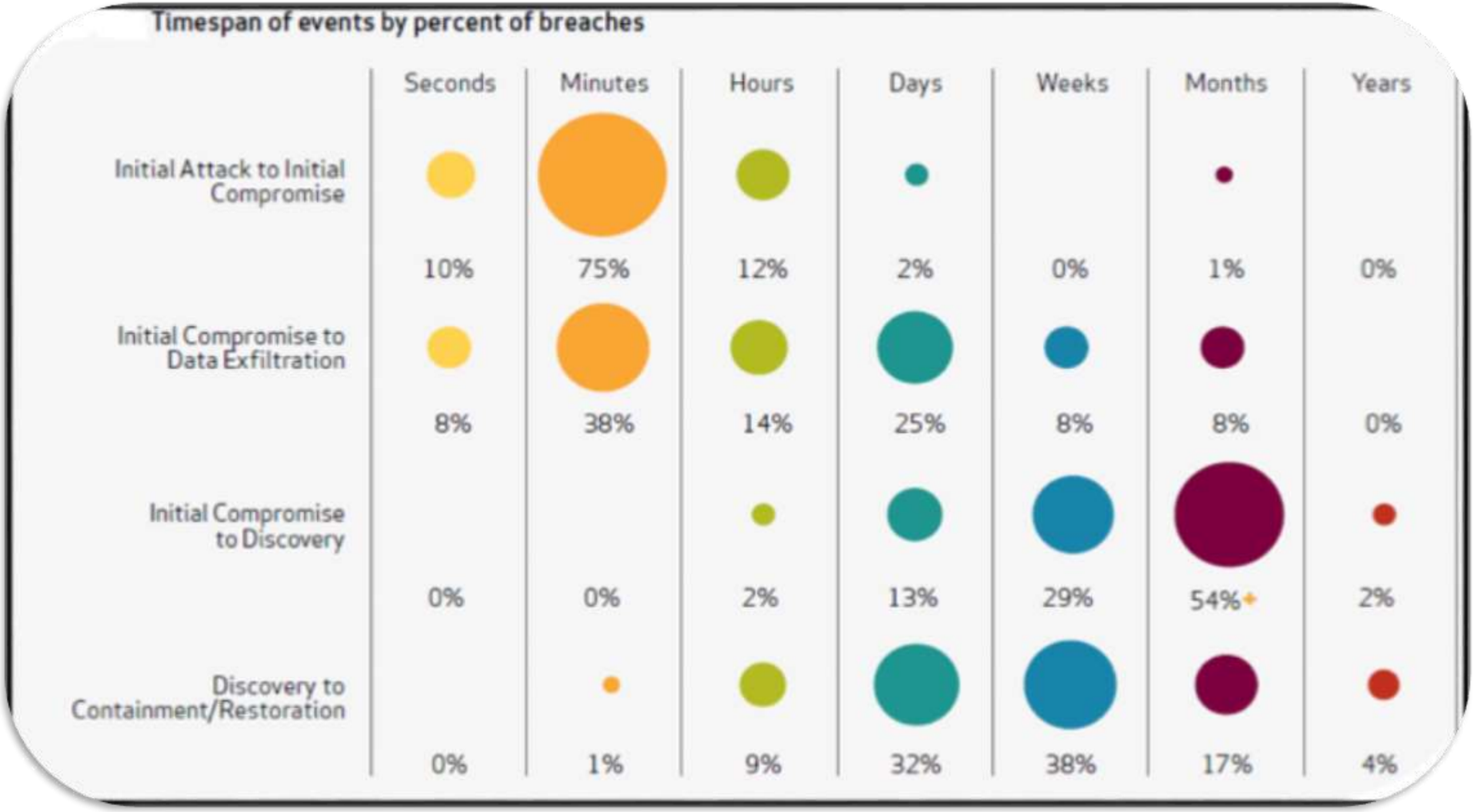
Evaluación de las Amenazas y su Respuesta

Seguridad en Oscuridad

Atacantes no son muy inteligentes (llave en la matera)
El código de nuestro producto es indescifrable
Algoritmos propios de encripción
Ocultamiento de puertos
Suficientes equipos de seguridad que contrarrestan todo

No subestime al adversario
Ejecute practicas de seguridad con un enfoque sólido.
Establezca un programa de seguridad basada en un marco de referencia.

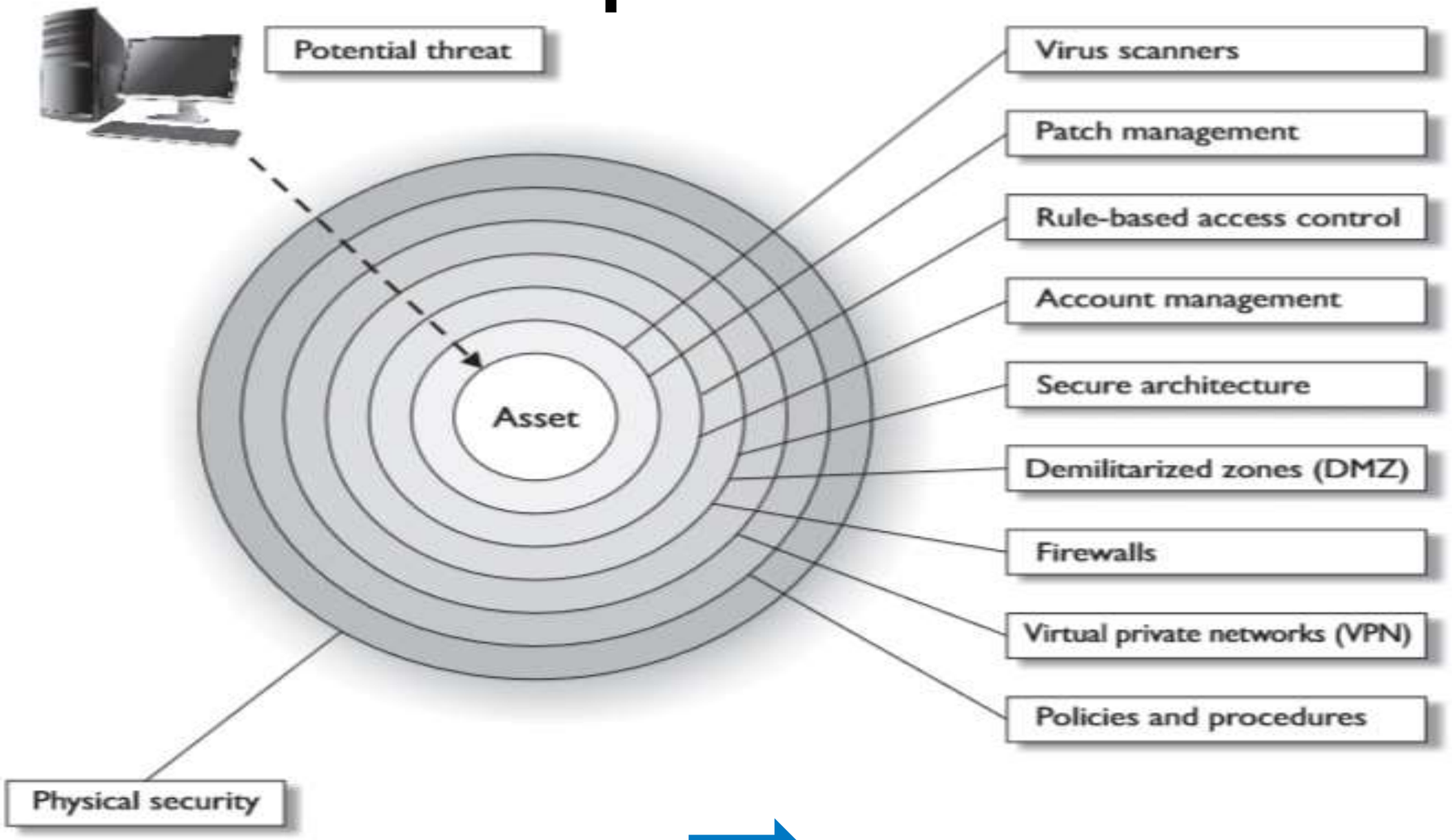
Evaluación de las Amenazas y su Respuesta



Verizon Report

Evaluación de las Amenazas y su Respuesta

Defensa en profundidad



SSL Insight

Detectar Amenazas ocultas en Trafico Cifrado

Riesgos En Encriptación SSL

Amenazas ocultas en Trafico Cifrado

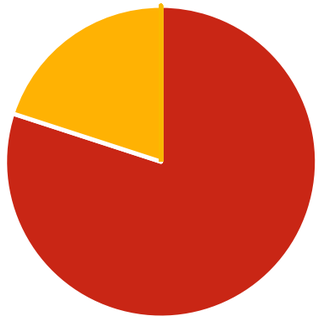
40% y creciendo !
del trafico Internet es cifrado

70%+
SSL Traffic

Para algunas organizaciones

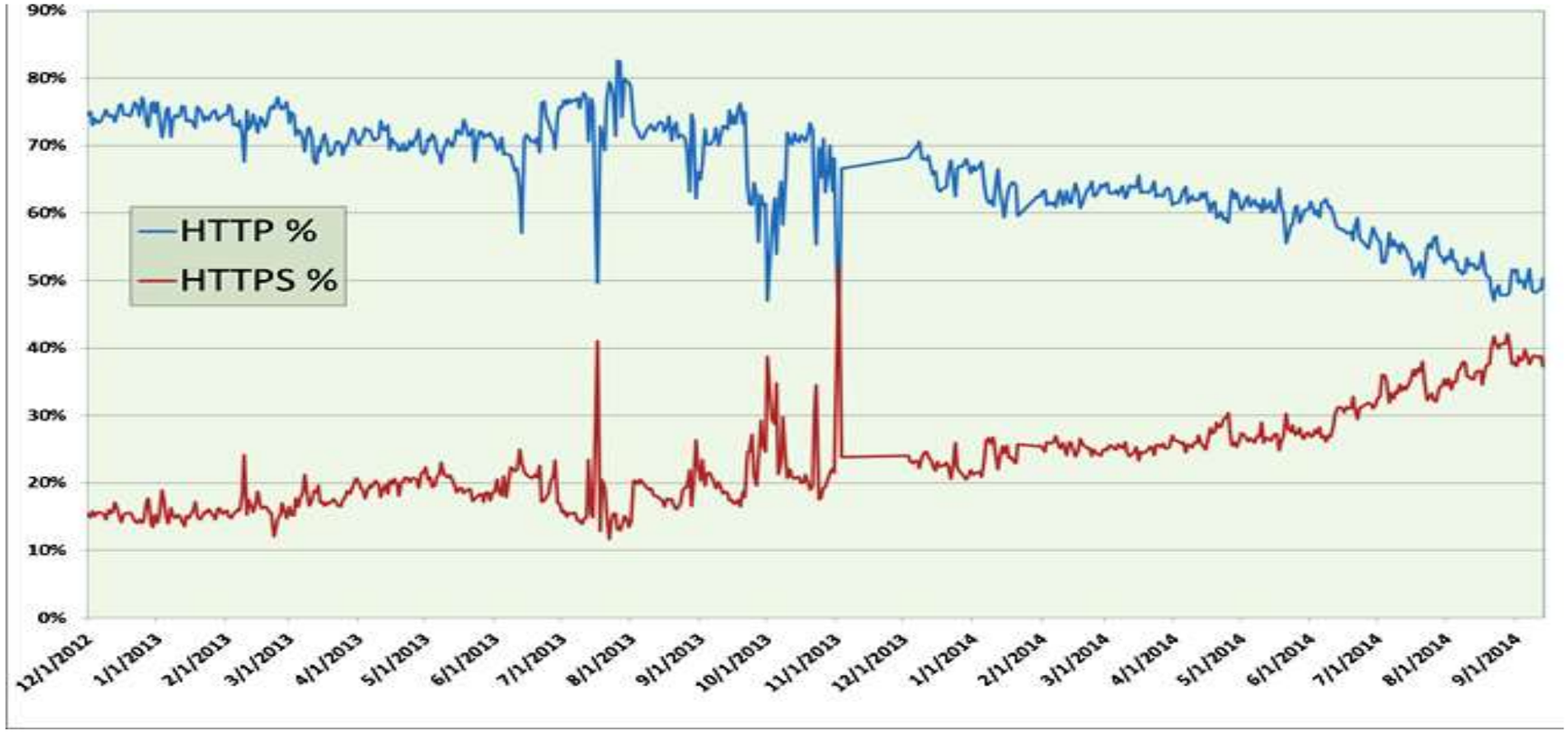
50%
de los ataques se realizaran mediante trafico cifrado para evitar controles de seguridad en 2017

80%+
de las organizaciones con soluciones de firewalls, IPS, o UTM no descifran el trafico SSL



Fuentes:
"SSL Performance Problems," NSS Labs, 2013
"Security Leaders Must Address Threats From Rising SSL Traffic," 2013

Crecimiento de tráfico SSL



- **SSL ~40% of Traffic**

- **Drivers:** Snowden, Google ranking SSL sites higher for SEO, foreign governments injecting surveillance software in web traffic

Limitaciones de los Firewall para desencriptar tráfico SSL

	Check Point 12600	Dell SonicWall E10800	Fortinet 3600C	Juniper SRX3600	Palo Alto Networks PA-5020	SourceFire 8250	SourceFire 8290	Stonesoft 3202
NSS Performance Rating	4,220	16,600	7,580	3,300	2,300	12,900	52,300	2,700
512b Cipher Performance Loss	550	2800	531	2150	795	2950	2950	1250
1024b Cipher Performance Loss	550	2550	493	2880	506	2900	2900	1100
2048b Cipher Performance Loss	550	1000	449	2130	484	2200	2200	650

Figure 4 – SSL Performance Impacts on Bandwidth

Informe NSS LABs

- Recent research on the NSS threat database found that while it is only a small percentage (~1%) of malware that is using SSL, this malware is highly sophisticated

- 16 million emails per day pass undetected through spam filters, 8 million of these are opened, and more than 800,000 users will click on the malicious links contained within these emails

- NSS research on the use of HTTPS reveals that within any given enterprise the current percentage of outbound network traffic that is SSL/TLS encrypted is about 25% – 35%

SSL insight - Modos de operación

- Inline SSL - Proxy Transparente. Envía tráfico desencriptado a dispositivos de seguridad inline.

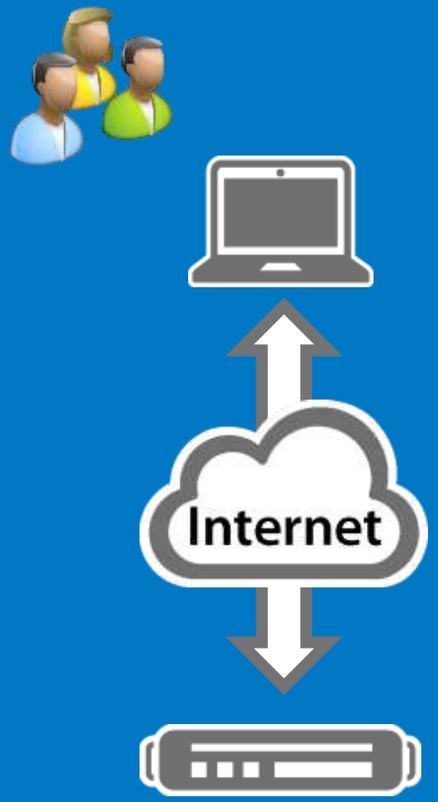
- Inline SSL – Proxy transparente Mirroring. Envía tráfico desencriptado a dispositivos de seguridad no-inline pasivos.

- Inline SSL – Proxy Explícito. Envía tráfico desencriptado a dispositivos de seguridad inline

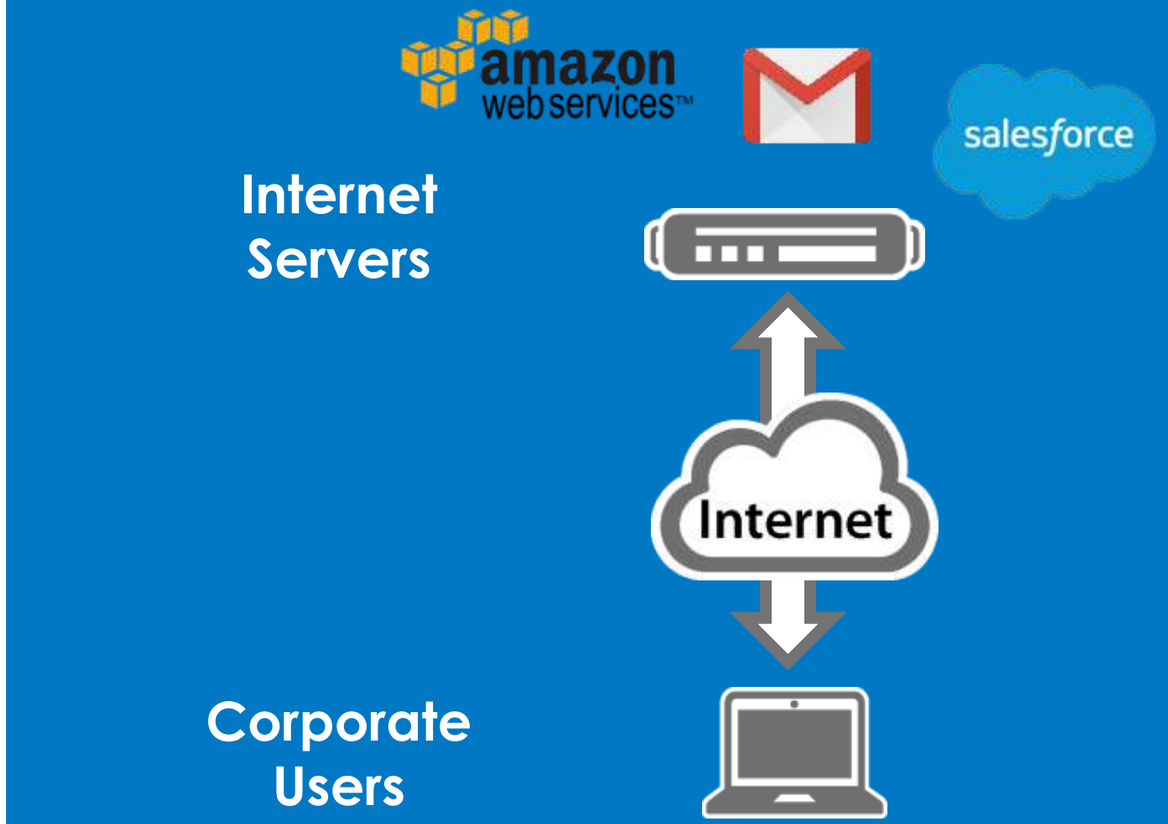
Inline SSL – Proxy Explicito Mirroring. Envía tráfico desencriptado a dispositivos de seguridad no-inline pasivos.

Securizando el trafico SSL Inbound y Outbound

SSL Inbound (Offload)



SSL Outbound (Insight)

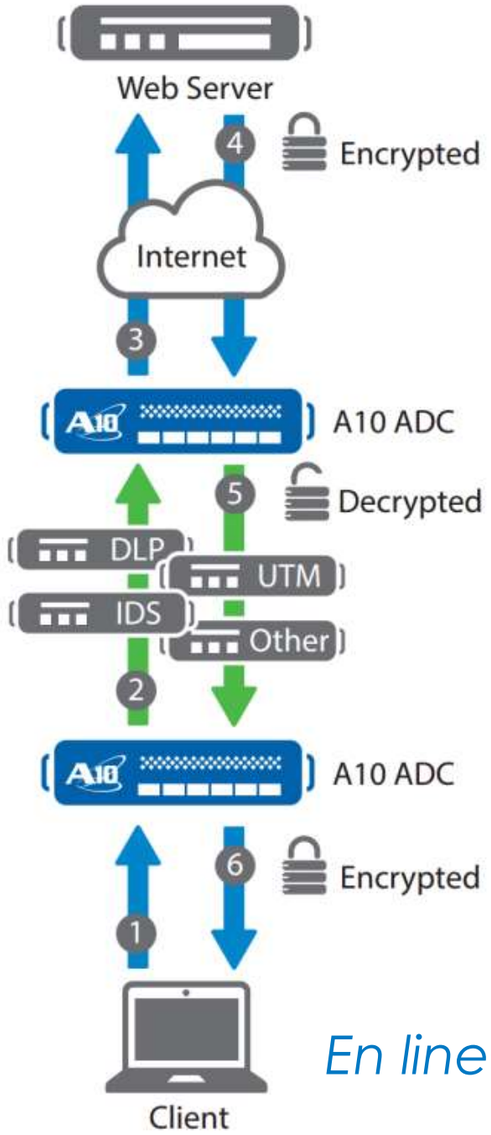


Securizando el trafico SSL Inbound y Outbound

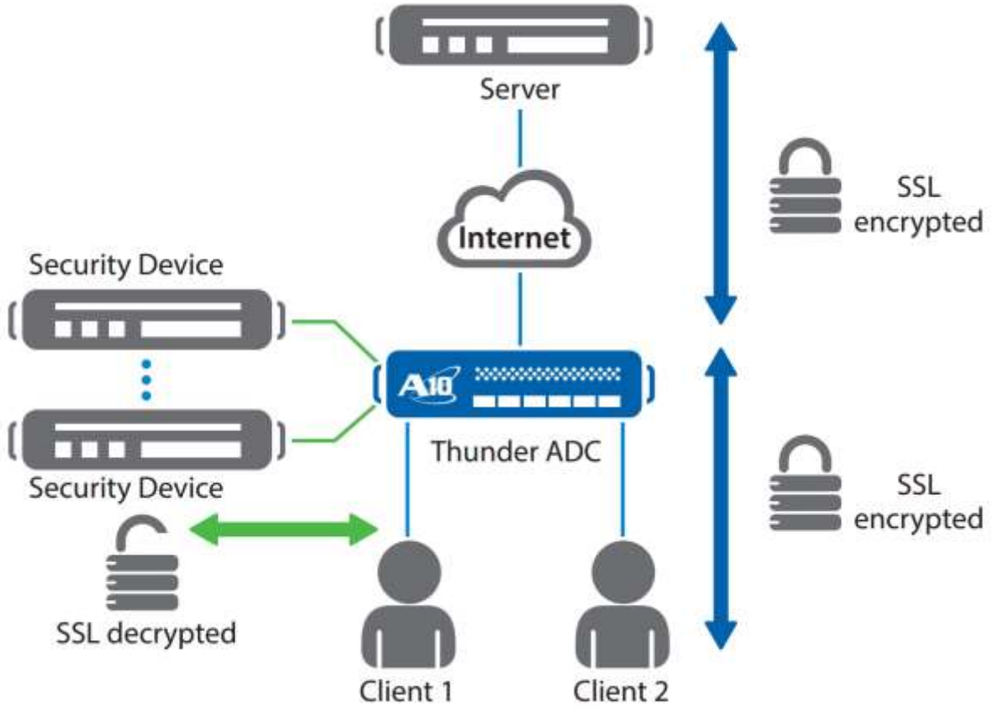
Beneficios:

- **Seguridad** – Detectar amenazas embebidas en trafico SSL Inbound y Outbound
- **Rendimiento** – Descarga el GW de Seguridad y los servidores de las tareas de procesamiento SSL
- **Disponibilidad** – Respuesta de los servidores más rápida y redundancia automática
- **Escalabilidad** – Permite la escalabilidad de servidores y de los gateways de Seguridad con capacidad integrada para balanceo de carga

Un solo punto para descifrar y analizar



En linea

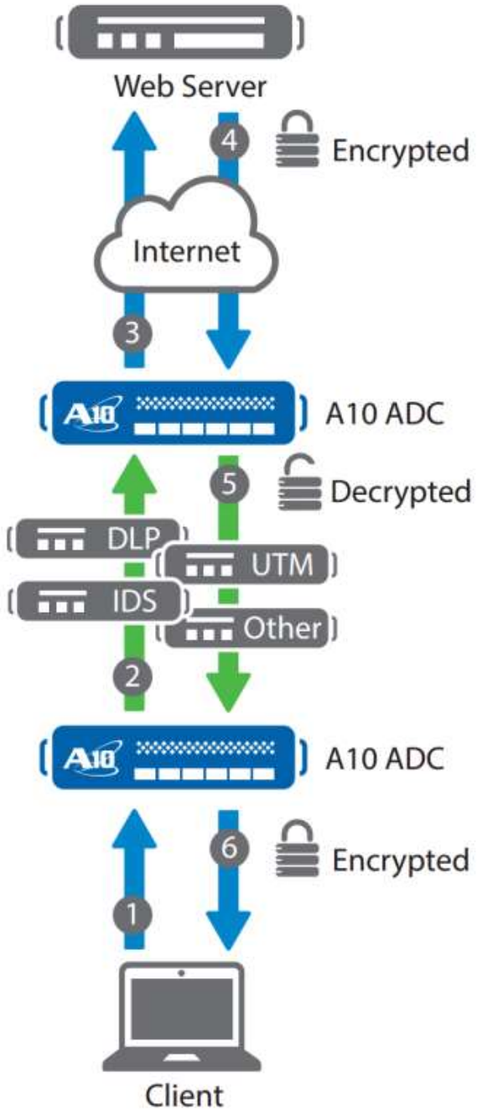


Fuera de linea

Thunder ADC puede trabajar con:

- Firewalls
- Intrusion Prevention Systems (IPS)
- Unified Threat Management (UTM) platforms
- Data Loss Prevention (DLP)
- Threat Prevention platforms
- Network forensics and web monitoring tools

SSL Insight – Flujo de tráfico



1. Tráfico encriptado del cliente es desencriptado por el ADC interno de cara al cliente
2. El Thunder ADC envía los datos desencriptados al equipo de seguridad el cual inspecciona los datos en texto claro
3. El appliance envía el tráfico al Thunder ADC externo el cual re-encripta los datos y lo envía al servidor
4. El servidor envía una respuesta encriptada al Thunder ADC externo.
5. El Thunder ADC desencripta la respuesta y lo reenvía al dispositivo de seguridad para inspección.
6. El dispositivo envía el tráfico hacia el ADC interno, re-encripta el tráfico y lo envía al cliente interno.

SSL Insight – Rendimiento y Resumen

	Small to Medium Enterprise		Medium to Large Enterprise		Service Provider
	Thunder 1030S	Thunder 3030S	Thunder 4430S	Thunder 5430S	Thunder 6430S
SSL Insight CPS (2048-bit)[7]	3,000	6,000	24,000	27,000	40,000
SSL Insight Throughput (2048-bit)[7]	1.5 Gbps	3 Gbps	10.6 Gbps	11.2 Gbps	23.8 Gbps
Application Throughput	10 Gbps	30 Gbps	38 Gbps	79 Gbps	150 Gbps

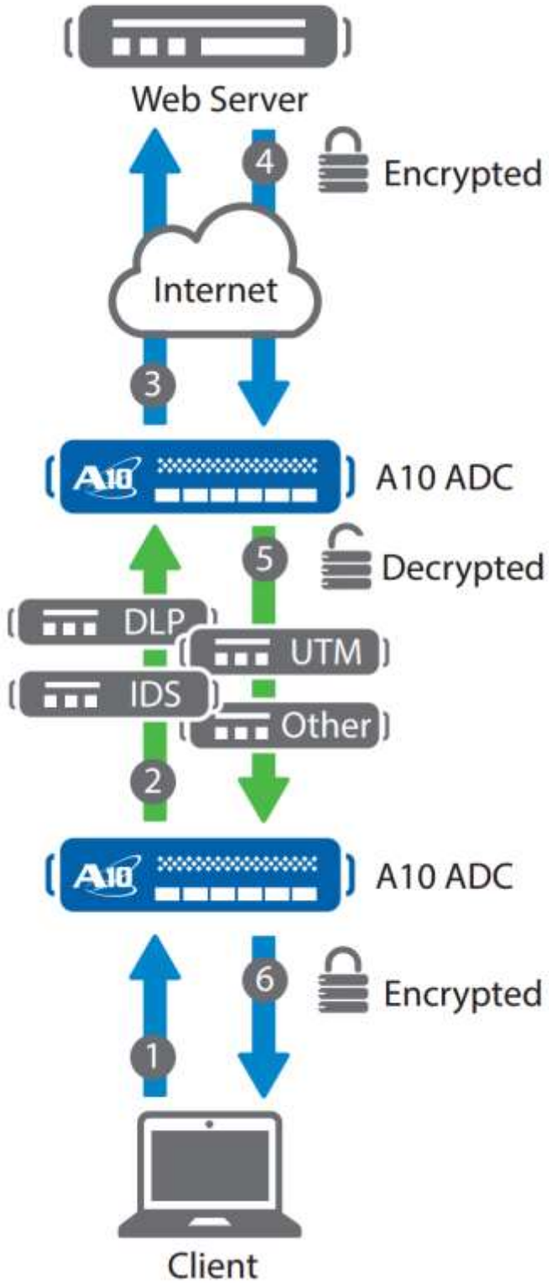
- **Escalabilidad**, con hasta 23.8 Gbps de rendimiento de inspección SSL en una configuración estándar
- **Load Balancing de dispositivos de seguridad** para maximizar el uptime y escalar la infraestructura
- **Funcionalidades avanzadas de SSL Insight** como suscripción de clasificación de URLs, gestión de certificados no confiables, …
- **Integración con Hardware Security Module (HSM)** para FIPS 140-2 nivel 3 cumpliendo con la gestión de llaves SSL
- **Traffic steering** para routing inteligente de trafico, optimiza el rendimiento y reduce el coste de los appliances de seguridad
- **Interoperabilidad validada** con FireEye, RSA, IBM y otras soluciones lideres de la industria asegura que nuestras soluciones funcionan juntas

SSL Insight

Con SSL Insight, las organizaciones pueden:

Disponer de un alto rendimiento con SSL gracias a hardware de aceleración SSL

- Escalar las soluciones de Seguridad con balanceo de carga
- Reducir la carga de la infraestructura de seguridad controlando el tipo de trafico que hay que descifrar
- Control granular de trafico con políticas aFlex
- Bypass selectivo de aplicaciones web sensibles*



** With ACOS 4.0.1*

Thunder ADC Mejora y garantiza la continuidad del Negocio:

Disponibilidad

- Escala WEB e Infraestructuras
- Reduce tiempos de inactividad
- Negocio siempre UP

Aceleración

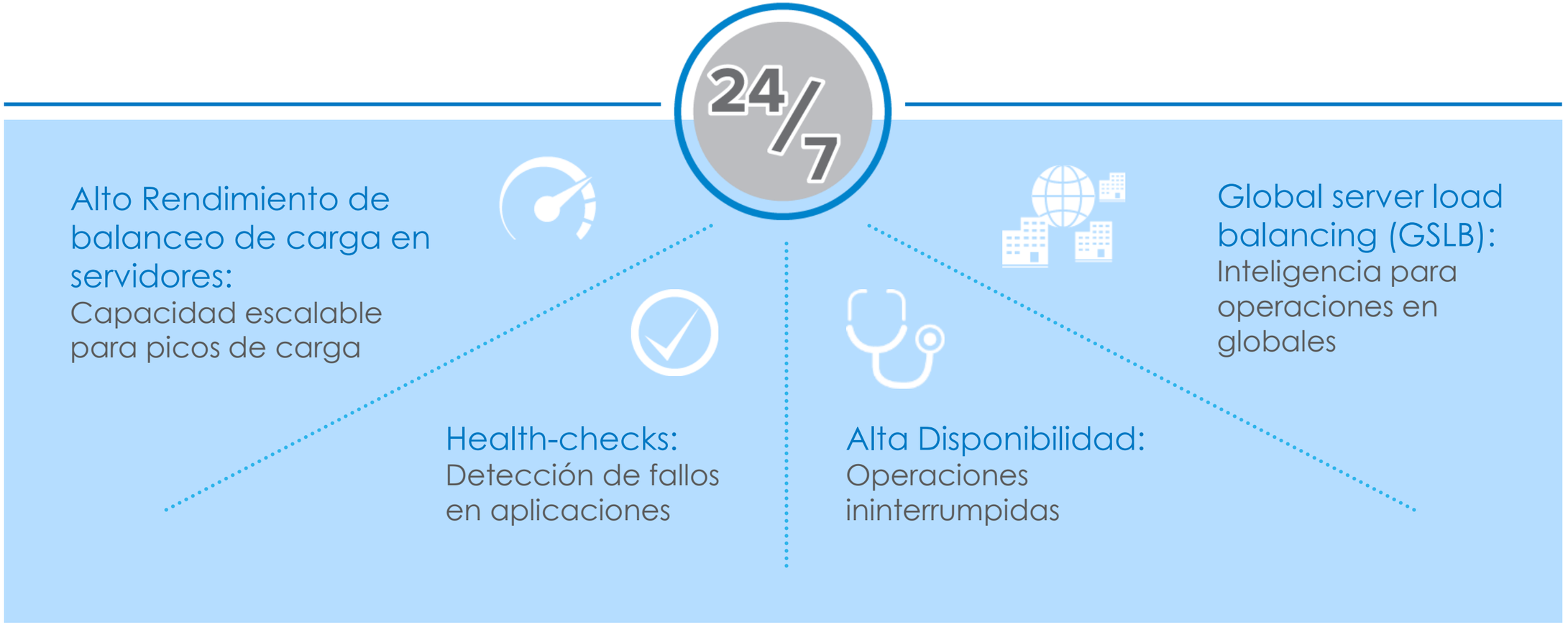
- Servicios Rápidos
- Ventajas Competitivas
- Reduce CAPEX y OPEX

Seguridad

- Protección contra Ataques avanzados
- Protección de la imagen de empresa
- Cumplimiento de estándares

Disponibilidad de Aplicaciones

Alta disponibilidad en aplicaciones y data centers



Aceleración de Aplicaciones

Aceleración de aplicaciones para una mejor experiencia de usuario y mejora de la utilización de la aceleración de las aplicaciones

TCP Optimización:
Mejora el rendimiento de las aplicaciones

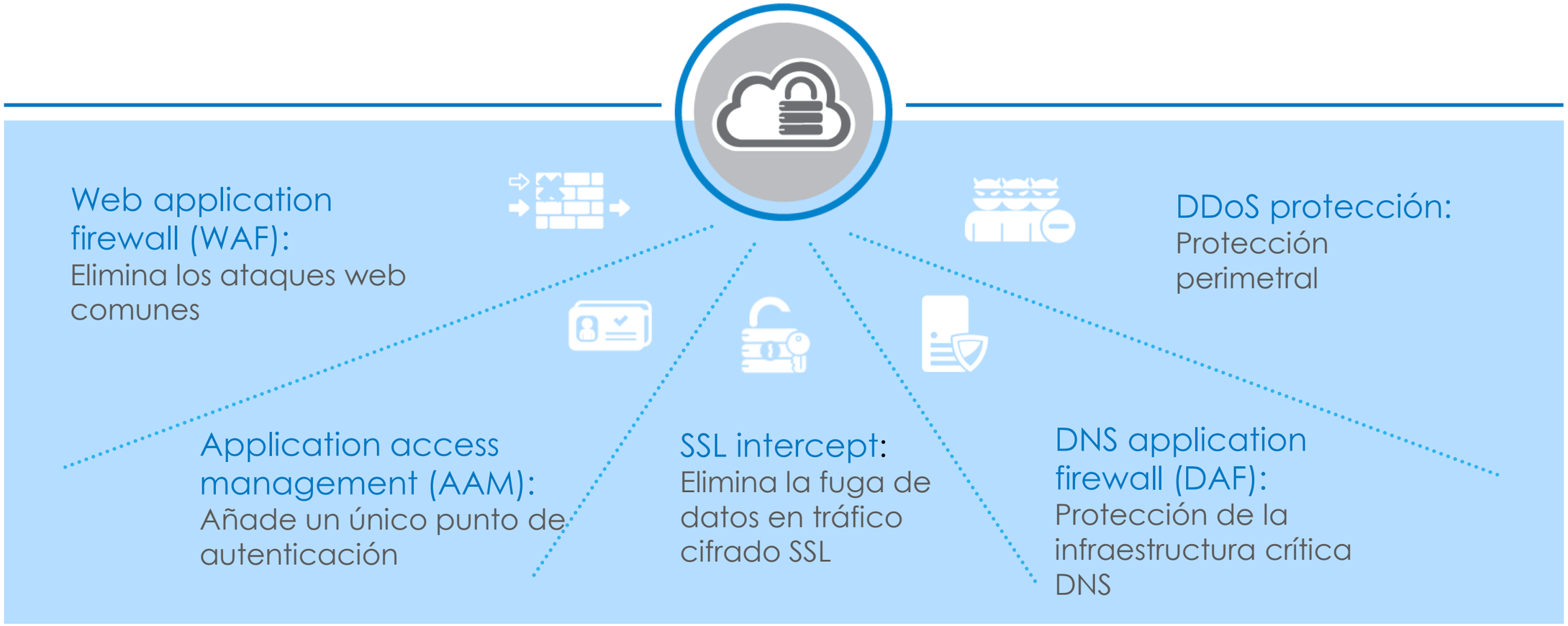
Compresión:
Optimiza el nivel del ancho de banda

SSL Aceleración:
Securiza las aplicaciones

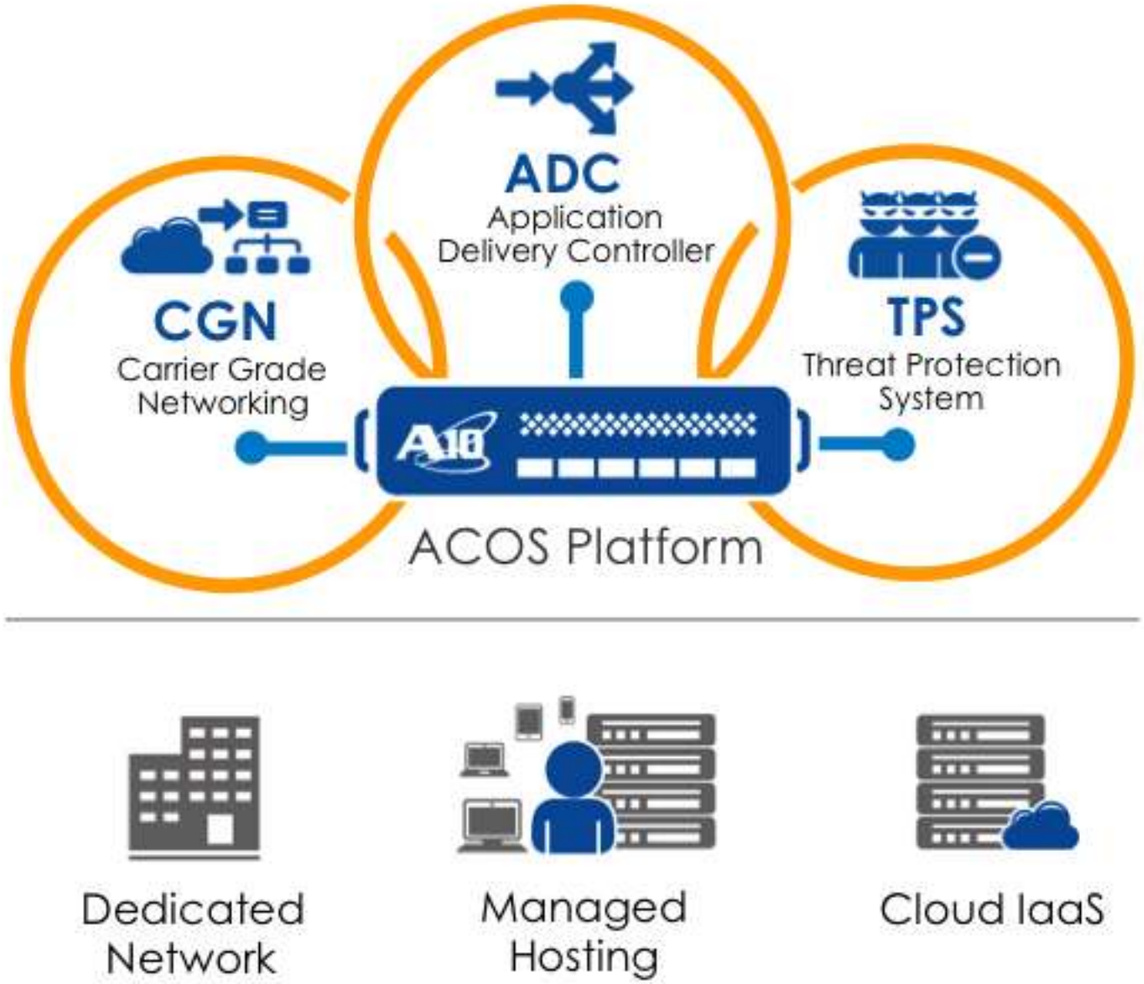
RAM Caching:
Mejora la carga de páginas

Seguridad de Aplicaciones

Complementa la seguridad existente, y protege contra las últimas amenazas



Portfolio de soluciones de A10



Lineas de Producto

- ADC – Application Acceleration & Security
- CGN – IPv4 Extension / IPv6 Migration
- TPS – Network Perimeter DDoS Security

Application Networking Platform

- Rendimiento
- Escalabilidad
- Crecimiento
- Flexibilidad

Modelos de despliegue

Más de 3400 Clientes en 65 Paises

Proveedores de Servicio

3 de los Top 4
U.S. WIRELESS CARRIERS

7 de los Top 10
U.S. CABLE PROVIDERS

Top 3
WIRELESS CARRIERS IN JAPAN

Empresas

Gigantes Web

Clientes en Colombia

PROCURADURIA GENERAL DE LA NACION

DANE

UTP Universidad Tecnológica de Pereira

Finandina

UNIDAD ADMINISTRATIVA PARA LA CONSOLIDACIÓN TERRITORIAL

REGISTRADURÍA NACIONAL DEL ESTADO CIVIL

MP marketing personal
El nuevo mundo para la mujer

Ventas y Servicios S.A.

ACR ALTA CONSEJERÍA PARA LA REINTEGRACIÓN
PRESIDENCIA DE LA REPÚBLICA

CNSC
Comisión Nacional del Servicio Civil

gasNatural fenosa

RBM Redeban Multicolor

MinSalud
Ministerio de Salud y Protección Social

Alcaldía de Envigado

50 años Banco Cooperativo CoopCentral

GENSA GESTION ENERGETICA S.A. E.S.P.

¡Gracias!