Defender las propiedades web de las amenazas modernas con Citrix NetScaler

CITRIX®

Defender las propiedades web de su organización nunca fue tan difícil. En el pasado, los equipos de seguridad de las TI tenían sólo un puñado de aplicaciones web empresariales que defender. Ahora deben proteger los backends web de muchas aplicaciones móviles, aplicaciones SaaS y otras soluciones cloud.

Al mismo tiempo, el número y la diversidad de las amenazas están creciendo. Por ejemplo, las defensas modernas deben tener en cuenta mucho más que la parte visible del paisaje de amenazas, los malware avanzados. Otras amenazas específicas que requieren diligencia incluyen ataques del nivel de aplicación web específica, ataques de denegación y denegación distribuida de servicio (DoS/DDoS) y problemas de uso inducido por la seguridad.

Este white paper analiza los retos de la defensa de propiedades web modernas de las amenazas actuales. En él se explica cómo el controlador de entrega de aplicaciones (ADC) Citrix®NetScaler® complementa la protección contra malware avanzado y otros productos de seguridad de alto perfil para proporcionar una solución ideal para defenderse contra las nuevas amenazas y proteger más objetivos. Las ventajas de utilizar NetScaler en esta función son:

- Menor riesgo de seguridad, bloqueando no solo el malware avanzado sino también los ataques DoS y los enfocados al nivel de la aplicación.
- Menor riesgo para el negocio con la automatización de la seguridad, la mejora de la capacidad de uso y un mejor rendimiento aumenta el uso por parte del cliente y las tasas de retención.
- Aumentar la agilidad de la empresa a partir de la capacidad de TI de aceptar plenamente soluciones móviles, web y cloud sin temor a comprometerse o a otros tipos de fallos relacionados con la infraestructura.

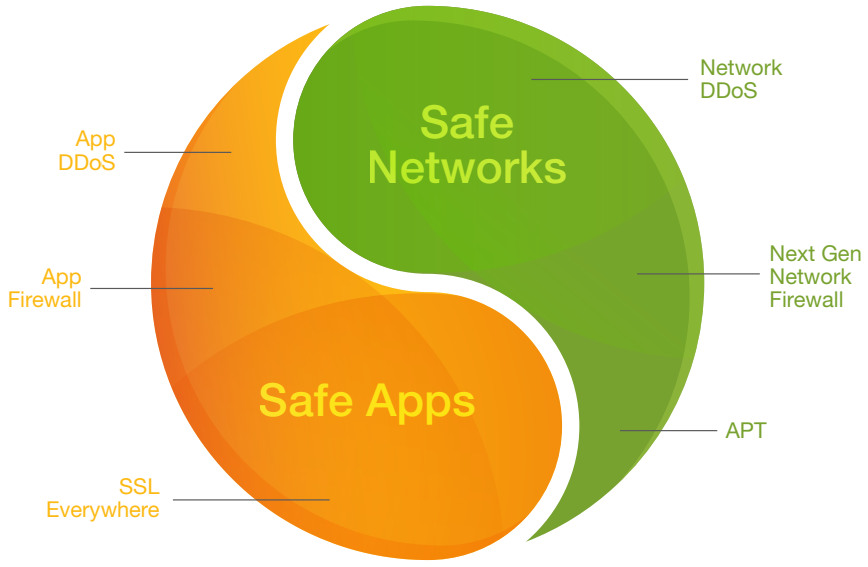

Imagen 1: Una solución completa para la defensa de la propiedad web

"¿Y qué pasa con las APT?"
Aunque los proveedores de protección contra malware avanzado a menudo los consideran iguales, las amenazas avanzadas persistentes (APT) y el malware avanzado no son lo mismo. En realidad, las ATP tienen más que ver con la amenaza actor -bien organizada, bien financiada y persistente- que con el mecanismo de amenaza específico utilizado. De hecho, las APT normalmente usan múltiples técnicas y métodos de ataque, incluyendo no sólo malware avanzado, también elementos de la capa de la aplicación y DoS, como por ejemplo, para acceder a los datos y luego crear una distracción mientras que los datos están siendo substraídos.

Modernas propiedades web: no solo sus aplicaciones web típicas

Al principio, las propiedades web involucraban poco más que un navegador web, normalmente Internet Explorer, para interactuar con una página web corporativa. Avanzando rápidamente hasta el presente, es un eufemismo decir que las soluciones web han evolucionado de forma incontrolada. Ahora, las propiedades web empresariales implican diversos componentes, que incluyen:

- Numerosos navegadores interactuando con numerosos componentes de la aplicación web y sitios web.
- Sitios y aplicaciones web alojadas en la nube y redes de distribución de contenido.
- SaaS y otra opciones de entrega cloud, tales como plataforma como servicio (PaaS) e infraestructura como servicio (IaaS), donde la empresa posee y controla cada vez menos la solución.
- Mashups, donde el contenido se extrae de forma dinámica de muchos sitios externos.
- Potentes API para permitir la integración de la cadena de suministro y mayor automatización.
- Soluciones móviles dónde microaplicaciones del lado del dispositivo se comunican con los sofisticados backend basados en web.

Como resultado de ello, defender las propiedades web ya no es simplemente proteger aplicaciones web empresariales. El ámbito de los recursos que necesitan protección se ha ampliado considerablemente, sobre todo para incluir soluciones móviles y cloud.

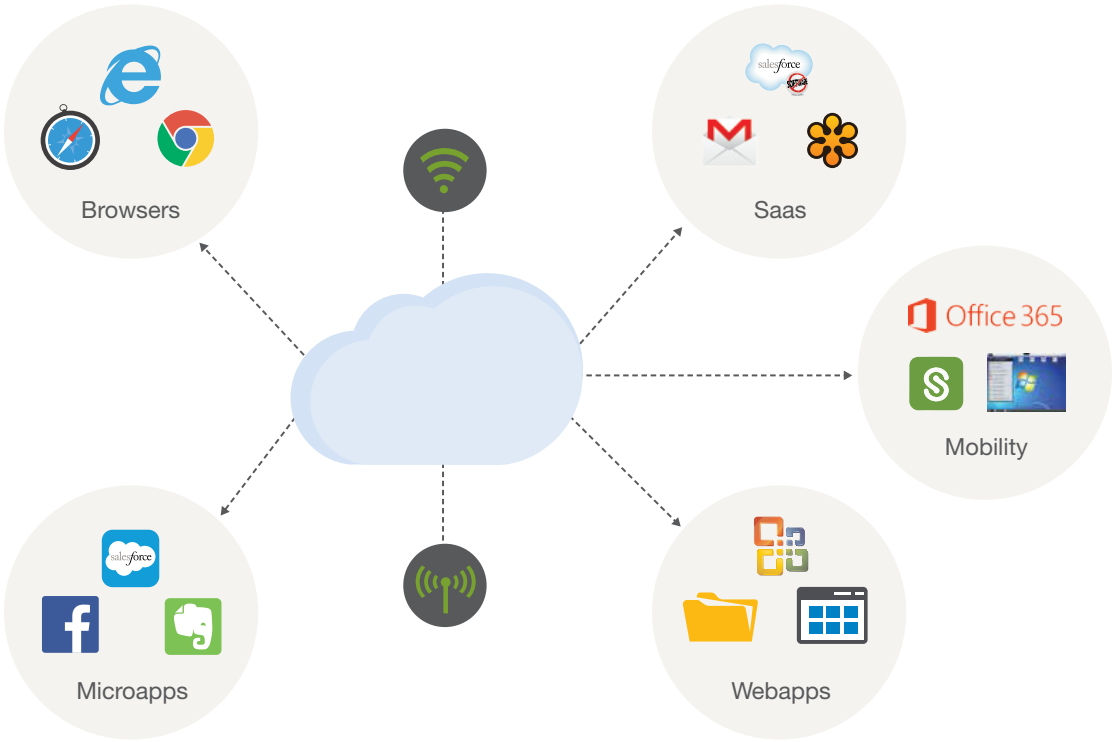

Imagen 2: El complejo mundo de las propiedades web

Amenazas modernas: El malware sofisticado es solo la punta del iceberg

El malware avanzado está atrayendo mucho la atención estos días y con razón. Comúnmente las defensas desplegadas basadas en firmas no son rival para la nueva generación de malware que está diseñado específicamente para evadirse de ellas, por ejemplo apuntando a las vulnerabilidades antes reveladas, aprovechando credenciales comprometidas o usando polimorfismo u otras técnicas para cambiar rápidamente las funcionalidades o la huella del código malicioso.

El resultado es una necesidad clara y presente para las organizaciones de hoy de invertir en soluciones de protección contra malware avanzado que no dependen de mecanismos basados en la firma y limitados a detectar solamente las amenazas identificadas previamente, también referidas como amenazas conocidas. Sin embargo, el malware avanzado es solamente una de las clases de amenazas que constituyen un riesgo significativo para las propiedades web de una organización. En particular, los ataques DoS, los ataques específicos de la web a la capa de la aplicación y los problemas de capacidad de uso, también requieren mitigar la amenaza.

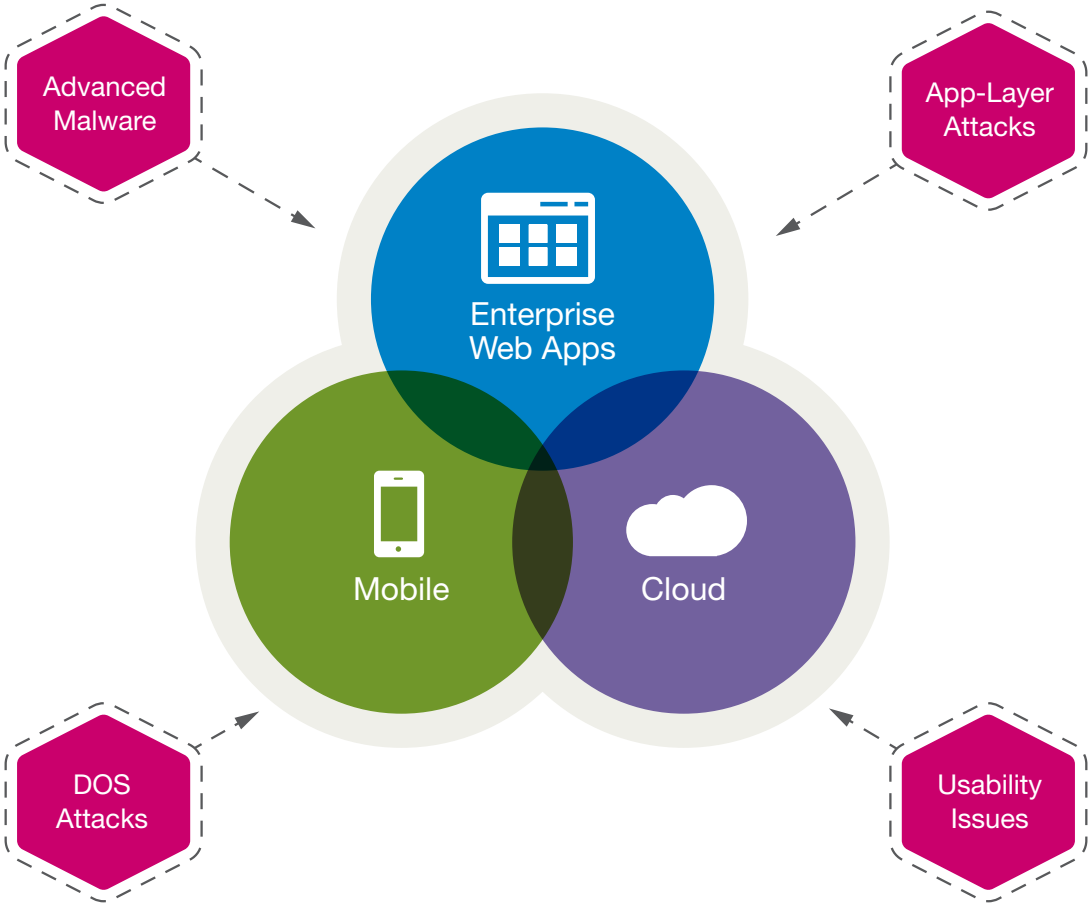

Imagen 3: Panorama actual de amenazas

Ataques DoS: en los últimos años que ha habido un marcado resurgimiento de ataques DoS, junto con cambios significativos en la naturaleza de la amenaza en sí misma. No solo las grandes propiedades de Internet están bajo amenaza. Gracias a la amplia disponibilidad de herramientas baratas y botnets (grupo de ordenadores controlados por un solo recurso) para la creación y ejecución de DoS respectivamente, ahora todas las empresas, sin importar su tamaño o sector,

están bajo riesgo. La detección de estos ataques también es mucho más difícil que en el pasado, ya que subrepticiamente, variantes de bajo ancho de banda de la capa de aplicación, centradas en agotar los recursos de backend, se han unido a los ataques ya familiares, de alto volumen que intentan inundar sus canales de Internet o tirar dispositivos de red de frontend como routers, firewalls o los ADC básicos.

Ataques web específicos al nivel de aplicación: La amenaza en este caso no es nueva, pero sigue siendo importante. Enfrentado con una plétora de defensas desplegadas comúnmente operando en la capa de red, los hackers lógicamente han optado por concentrar sus esfuerzos en las capas superiores de la capa informática para lograr resultados más favorables. El resultado es un porcentaje importante de ataques contra las debilidades descubiertas en componentes y tecnologías web ampliamente distribuidas como por ejemplo protocolo HTTP, Java o servidores web y aplicaciones populares, y las aplicaciones web personalizadas de una organización. Las amenazas comunes que entran en esta categoría incluyen falsas peticiones cross-site scripting y cross-site, inyección SQL y ataques de desbordamiento de memoria, solo por nombrar alguno.

Amenazas a la capacidad de uso: La degradación de la capacidad de uso a menudo se pasa por alto o subestima en base a que técnicamente es más un problema de rendimiento que una verdadera amenaza a la seguridad. Sin embargo a pesar de ello los problemas de capacidad de uso introducidos por soluciones de seguridad, siguen siendo una amenaza muy real, por lo menos en lo que al negocio se refiere. El pobre rendimiento resultante de las rutinas de inspección informáticas, sobrecargas SSL, complicados procesos de inicio de sesión y capacidades de acceso inconsistentes pueden llevar a los usuarios a buscar soluciones inseguras y a provocar la insatisfacción del cliente y, en última instancia, la deserción. Además, compensar estas condiciones puede exigir que las empresas compren más hardware o hardware de mayor capacidad de lo que estaba originalmente previsto. Por lo tanto, los equipos de seguridad de TI, necesitan ser conscientes de que las soluciones de seguridad en sí mismas pueden convertirse en una amenaza si no están diseñadas para evitar, o de otro modo compensar este tipo de problemas de capacidad de uso.

La conclusión es que defender las propiedades web modernas requiere tener en cuenta todas estas amenazas, no solo el malware avanzado. Los riesgos asumidos al no hacerlo así incluyen un mayor potencial de pérdida de datos o exposición, deserción del cliente, mayor coste total de propiedad (TCO) y el incumplimiento de las normativas vigentes.

Modernas defensas: El papel de NetScaler

NetScaler, el mejor ADC para la construcción de redes cloud empresariales, también la solución ideal para defender las modernas propiedades web. Ya un componente estratégico en miles de centros de datos empresariales y redes de proveedores cloud, NetScaler ofrece capacidades extensas de defensa web que se complementan perfectamente con las soluciones de protección de malware, como por ejemplo las de FireEye y Palo Alto Networks. Con NetScaler, las empresas obtienen todo lo que necesitan para asegurar la disponibilidad, seguridad, capacidad de uso y agilidad de sus propiedades web mientras que frustran con éxito ataques DoS y a la capa de aplicación previstos para interrumpir el negocio y extraer datos valiosos. Por otra parte, todas estas capacidades esenciales están disponibles como una solución integrada en una plataforma única y altamente escalable. Como resultado, las empresas ya no necesitan invertir e incurrir en la complejidad añadida de operar con múltiples productos de seguridad independientes.

Mantener las luces encendidas

Las propiedades web a las que no se puede acceder debido a las interrupciones de energía son prácticamente inútiles, y pueden incluso causar daño a la reputación de la empresa. Por lo tanto, las defensas de NetScaler de las propiedades web comienzan con un amplio conjunto de capacidades para la protección contra amenazas que pueden perturbar las operaciones y presentar servicios claves como no disponibles.

- **Alta disponibilidad (HA) para componentes críticos**: En caso de que un servidor web u otro componente clave de una propiedad web falle por cualquier motivo, los algoritmos de balanceo de carga dirigen dinámicamente el tráfico afectado hacia instancias alternativas configuradas como parte de un grupo dirigido por NetScaler. De esta manera, NetScaler proporciona una disponibilidad continua durante el mantenimiento programado y fallos imprevistos, así como las interrupciones de energía inducidas por algún ataque.
- **Supervisión del estado de salud para la gestión proactiva de los fallos**: La comprobación del estado de salud de NetScaler supervisa el estado de los componentes clave y compromete características fundamentales de balanceo de carga para evitar proactivamente puntos problemáticos. A diferencia de muchas soluciones de la competencia, que simplemente confirman la existencia de una conexión de red y que el servidor subyacente está online, NetScaler proporciona amplios controles de verificación de contenido para establecer que los servicios básicos del nivel del sistema y las rutinas individuales de software, también están en perfecto estado de funcionamiento.
- **GSLB para la recuperación ante desastres**: Un robusto conjunto de características del servidor global de balanceo de carga (GSLB) proporciona una recuperación ante desastres sin fisuras para las propiedades web modernas. Si un sitio completo se encuentra no disponible por cualquier razón, el tráfico afectado es dirigido automáticamente a un centro de datos alterno. También se puede garantizar una experiencia de usuario positiva mediante el aprovechamiento de políticas y una supervisión inteligente para dirigir las sesiones regularmente hasta el sitio óptimo basándose en prioridades seleccionadas por el administrador, como por ejemplo la proximidad, los niveles de utilización de recursos o el rendimiento general.
- **Protección multicapa contra ataques DoS**: con NetScaler las empresas obtienen una potente primera línea de defensa contra todo tipo de amenazas DoS. Proporciona cobertura no solo contra ataques volumétricos que tratan de consumir todo su ancho de banda de Internet, también para los más insidiosos que tratan de agotar los estados del dispositivo, hacer mal uso de la infraestructura o de la capa de servicios (por ejemplo, DNS, SSL y HTTP), o de alguna manera hacer mal uso de las características específicas de la aplicación de forma que degrada substancialmente el rendimiento (por ejemplo, emitiendo repetidamente peticiones que llevan a cálculos complejos, consultas al backend u operaciones de búsqueda).

Incremento de la dificultad de detección

	Ataques ejemplo	Características de mitigación de NetScaler
Aplicación	Inundación GET y POST maliciosos; slowloris, slow POST, y otras variantes de bajo ancho de banda	Validación del Protocolo de aplicación, protección contra picos, colas de prioridad, protección contra inundaciones HTTP, HTTP protección contra ataques de bajo ancho de banda
Conexión y sesión	Inundaciones de conexión, inundaciones SSL, inundaciones DNS (udp, query, nxdomain)	Arquitectura proxy completa, diseño de alto rendimiento, manejo inteligente de la memoria, amplias protecciones de DNS
Red	Inundación Syn, UDP, ICMP, PUSH y ACK; LAND, ataques smurf, teardrop	Defensas incorporadas, modelo de seguridad por denegación, validación de protocolos y tasa de limitación

Imagen 4: "Citrix NetScaler: una potente defensa contra los ataques de denegación de servicio"

Control para sobrecarga accidental: La sobrecarga importante en la utilización de una propiedad web puede tener el mismo impacto que un ataque DoS. NetScaler hace frente a esta situación con una protección contra las sobrecargas, una funcionalidad que controla correctamente oleadas de tráfico intermitente, basando el ritmo con el que se presentan las nuevas conexiones a los servidores de servicios de backend en la capacidad de gestión de los mismos. Significativamente, ninguna conexión válida cae con este mecanismo. NetScaler cachea y entrega conexiones en el orden en que fueron recibidas, pero solo cuando los servidores de backend están listos para gestionarlos.

Frustrar amenazas avanzadas

Superar las amenazas a la disponibilidad es solo un punto de partida, aunque este sea importante. Con NetScaler, las organizaciones también se benefician de una solución capaz no solo de frustrar directamente los ataques dirigidos a la capa de aplicación, también de trabajar junto a los principales productos de terceros para contrarrestar la última generación de malware sofisticado.

Protocolo de defensas de amplio espectro para protección de la capa de aplicación: implementar la normativa RFC y las mejores prácticas para el uso de HTTP es un método altamente eficaz utilizado por NetScaler para eliminar toda una clase de ataques basados en peticiones malformadas y comportamiento ilegal de protocolo HTTP. También se pueden añadir a la política de seguridad chequeos personalizados aprovechando el filtrado integrado de contenido, las acciones personalizadas de respuesta y funcionalidades de reescritura HTTP bidireccional. El resultado es una protección de amplio espectro contra el reconocimiento (por ejemplo, eliminando información de las respuestas del servidor que podrían ser utilizadas para perpetrar un ataque), malware basado en HTTP (por ejemplo, Nimda, Code Red) y otras amenazas de la capa de aplicación.

NetScaler AppFirewall para amenazas específicas de la capa de aplicación: los firewall de red tradicionales carecen de la visibilidad y control necesarios para proteger contra más del 70 por ciento de los ataques de Internet dirigidos a las vulnerabilidades de la capa de aplicación. En comparación, NetScaler AppFirewall™ es una solución de seguridad certificada ICSA que analiza todo el tráfico bidireccional, incluyendo las comunicaciones SSL cifradas, para contrarrestar las amenazas conocidas y desconocidas de la capa de aplicación sin necesidad de modificaciones a las propiedades web de una organización. Las capacidades clave incluyen:

- **Protección contra ataques**: Una combinación de modelos de seguridad positivos y negativos proporciona la protección más completa contra todas las formas de ataque. Para derrotar ataques nuevos y desconocidos, un motor de políticas de modelo positivo entiende las interacciones de aplicaciones de usuario permitidas y bloquea automáticamente todo el tráfico que queda fuera de este ámbito. Un motor de modelo negativo emplea simultáneamente firmas de ataque para protegerse de las amenazas a las aplicaciones e informar sobre ellas.
- **Protección contra el robo de datos**: Los controles Safe Object de datos protegen contra inesperadas filtraciones de información confidencial del negocio, tales como números de la tarjeta de crédito o la propiedad intelectual, ya sea debido a un ataque real, el uso indebido de un usuario autorizado o un fallo en el diseño de una aplicación web. Una combinación de las expresiones regulares definidas por el administrador y plug-ins personalizados indican a NetScaler App Firewall el formato de esta información, mientras que las reglas asociadas especifican las medidas a tomar, como por ejemplo enmascarar el campo protegido o bloquear todas las respuestas de la aplicación.
- **Protección para el cumplimiento normativo**: NetScaler AppFirewall permite a las empresas cumplir con la normativa Card Industry Data Security Standard (PCI-DSS), que fomenta explícitamente el uso de los firewall de aplicaciones web para aplicaciones orientadas al público que manejan información de tarjetas de crédito. NetScaler produce informes detallados para documentar todas las protecciones que se definen en la política de firewall que pertenecen a PCI-DSS y a otras normativas legales aplicables.

Imagen 5: NetScaler protege contra la filtración de datos sensibles, independientemente del tipo de amenaza responsable de haber causado la fuga. (fuente: NetScaler para la seguridad del centro de datos white paper)

Soluciones de partner Citrix Ready para detener el malware avanzado: Mientras que NetScaler no proporciona una detección directa de todas las formas de malware avanzado, su amplio conjunto de características de seguridad ofrece una medida considerable de la protección contra esta clase de amenazas crecientes. En particular, NetScaler puede disminuir el impacto del malware, por ejemplo, deteniendo cualquier mezcla de componentes utilizando técnicas de ataque web común, cualquiera de los componentes que causan o dependen de comportamiento anormal de la aplicación y los intentos por parte del malware de obtener datos sensibles del negocio. La red correspondiente y los datos del evento de la capa de aplicación generado por NetScaler pueden también utilizarse, normalmente en conjunción con otros eventos, para revelar inicialmente y ayudar posteriormente a detectar la presencia de malware. Además, las soluciones de los partners Citrix Ready diseñadas explícitamente para hacer frente al malware avanzado proporcionan protección específica contra las amenazas a las empresas de alto perfil.

Asegurar la capacidad de uso

La necesidad de evitar las interrupciones en las propiedades web modernas es un hecho. Menos evidentes, pero podría decirse que más impactantes debido a un aumento de la probabilidad, son los problemas de la capacidad de uso como por ejemplo un rendimiento pobre o procesos complicados o inconsistentes para proporcionar acceso a las propiedades web. A diferencia de la mayoría de las soluciones de seguridad, que tienden a exacerbar estos problemas, NetScaler trabaja activamente para superarlos a través de una combinación de diseño de decisiones inteligentes y numerosas características específicamente centradas en acelerar el rendimiento de la aplicación.

Garantía de alto rendimiento: Características de NetScaler que ayudan a las empresas a vencer los obstáculos de seguridad, red y rendimiento inducido de la aplicación son:

- Las optimizaciones TCP avanzadas tales como el almacenamiento en búfer avanzado, las técnicas de ampliación de ventanas y de control de la congestión, aumentan la capacidad del sistema, reducen el índice de pérdida de paquetes y mejoran los tiempos de respuesta utilizando más eficientemente el ancho de banda disponible y los recursos de los servidores.
- Almacenamiento en memoria caché de contenido tanto estático como dinámico (NetScaler AppCache™), combinada con agresivas rutinas de compresión de datos (NetScaler AppCompress) reduce la congestión de red y servidor mientras acelera significativamente los tiempos de respuesta de la aplicación.
- Mediante la incorporación de hardware de aceleración SSL dedicado y soporte para grandes claves de cifrado (2048 bits y mayores), NetScaler ofrece capacidades de cifrado esenciales que evitan la necesidad de realizar concesiones entre una seguridad más fuerte y una experiencia de usuario de alto rendimiento.

- Las colas de prioridad proporcionan un mecanismo QoS para priorizar las solicitudes entrantes basadas en la importancia relativa de las aplicaciones asociadas.
- Mediante la incorporación de un gateway SPDY, NetScaler permite utilizar este protocolo cada vez más popular que optimiza la forma en que las solicitudes y respuestas HTTP se envían por la red sin tener que modificar las aplicaciones del lado del servidor.
- NetScaler ActionAnalytics permite una supervisión totalmente automatizada y una respuesta a las condiciones de degradación del rendimiento, mientras NetScaler Insight Center™ proporciona a los administradores una visibilidad en profundidad para ayudarles a identificar y solucionar problemas emergentes antes de que se conviertan en problemas reales.

Acceso sin fisuras NetScaler ayuda a mitigar la amenaza de un uso pobre mejorando la experiencia del usuario en otras formas no relacionadas con el funcionamiento incluyendo soporte para:

- **Single sign on (SSO)**: Los usuarios necesitan acceder con sus credenciales solo una vez, ya que NetScaler les registra de forma transparente en todos los recursos dentro de un dominio dado.
- **Autenticación y autorización centralizada**: Se puede aprovechar el mismo grupo de servicios de control de acceso en todas las propiedades web de una organización y para todos los dispositivos del usuario. Esta capacidad no sólo simplifica la administración de los usuarios móviles y propiedad web, también garantiza una experiencia de usuario constante.

Facilitar el ahorro de costes y agilidad

Otra forma de que una solución de seguridad sea una amenaza, por lo menos desde la perspectiva de la gestión empresarial, es costando demasiado o en su defecto no alinearse con los objetivos clave del negocio. Sin embargo, Citrix, deliberadamente ha desarrollado y preparado NetScaler para que mitigue también estos desafíos.

Consolidación sin precedentes: NetScaler es la única solución de entrega de aplicaciones que combina el balanceo de carga, GSLB, conectividad VPN SSL y mucho más en una plataforma integrada, y altamente ampliable. Las soluciones de la competencia obligan a las organizaciones a adquirir, implementar e integrar múltiples productos y dispositivos para obtener un conjunto similar de capacidades para defender y entregar propiedades web. Con NetScaler SDX™, los departamentos de TI también obtienen la capacidad de consolidar su infraestructura ADC mediante la implementación de hasta 80 instancias aisladas de NetScaler en una única plataforma.

Alineación con la migración a cloud: El traspaso constante a redes cloud empresariales es facilitado por la disponibilidad de dispositivos virtuales listos para cloud NetScaler VPX™. Una versión completa de software del controlador de entrega de aplicaciones NetScaler App Delivery Controller™, esta solución ofrece la flexibilidad para implementar las capacidades de defensa y optimización de NetScaler on-demand, en cualquier lugar dentro de la empresa o en un centro de datos de terceros. NetScaler VPX permite a las organizaciones ejecutar correctamente sus aplicaciones web y servicios en el lugar que sea mejor para ellos.

Soporte a la movilidad del usuario: cuando se trata de apoyar las iniciativas de movilidad empresarial, NetScaler no para en la defensa y optimización de las propiedades web asociadas. También proporciona los mismos servicios para infraestructura de gestión relacionadas, en particular Citrix XenMobile®. Una solución integral para la gestión de dispositivos móviles, aplicaciones y datos, XenMobile ofrece a los usuarios la libertad de trabajar y vivir a su manera. Mientras que TI adquiere el control total y la capacidad de proteger todo el entorno móvil, los usuarios obtienen acceso con un solo clic a todos sus móviles, web y aplicaciones SaaS y Windows

desde una tienda unificada de aplicaciones corporativa. Combinar NetScaler con XenMobile proporciona:

- Alta disponibilidad para componentes clave de la infraestructura de movilidad empresarial.
- Capas adicionales de protección para dispositivos móviles, aplicaciones y datos.
- La capacidad de ampliar las operaciones móviles sin molestar a los empleados o sin la necesidad de realizar costosas actualizaciones.

Conclusión

Defender las propiedades web de su organización implica mucho más que proteger un puñado de aplicaciones web de empresa de la plaga de malware avanzado. Las defensas también deben montarse para los backend de la web que soportan las aplicaciones móviles nativas, soluciones SaaS y otros servicios cloud. Por otra parte, estas defensas deben proporcionar cobertura para otras clases de amenazas, igualmente problemáticas, incluyendo los ataques a la capa de aplicación, los ataques DoS y problemas de accesibilidad inducida.

Citrix NetScaler es un complemento ideal a las soluciones avanzadas de malware de hoy. NetScaler ADC:

- Reduce el riesgo de seguridad mitigando otras clases principales de amenazas a propiedades web, incluyendo DoS y ataques al nivel de aplicación.
- Reduce el riesgo del negocio mediante la mejora del uso de la propiedad web y del rendimiento al incrementar la retención y atracción del usuario.
- Disminuye el coste total de propiedad proporcionando amplias oportunidades para la consolidación de la infraestructura y optimización de la utilización de los recursos.
- Aumenta la agilidad del negocio y de las TI proporcionando a las organizaciones la seguridad y otras capacidades críticas que necesitan para perseguir iniciativas de movilidad de usuario, consumerización de las TI y redes cloud empresariales.

Si desea más información sobre cómo NetScaler puede ayudar a su organización a defender sus propiedades web críticas para el negocio, por favor visite www.citrix.es/netscaler.

Sede central corporativa
Fort Lauderdale, FL (EE.UU.)

Sede central de Silicon Valley
Santa Clara, CA (EE.UU.)

Sede central de EMEA
Schaffhausen (Suiza)

Centro de Desarrollo de la India
Bangalore (India)

Sede central de la División Online
Santa Bárbara, CA (EE.UU.)

Sede central del Pacífico
Hong Kong (China)

Sede central de América Latina
Coral Gables, FL (EE.UU.)

Centro de Desarrollo del Reino Unido
Chalfont (Reino Unido)

Acerca de Citrix

Citrix (NASDAQ: CTX) es un líder en espacios de trabajo móviles, que proporciona virtualización, gestión de la movilidad, networking y servicios cloud para habilitar nuevas formas para trabajar mejor. Las soluciones de Citrix impulsan la movilidad empresarial a través de espacios de trabajo seguros y personales que proporcionan a los usuarios un acceso instantáneo a las aplicaciones, puestos de trabajo, datos y comunicaciones en cualquier dispositivo, sobre cualquier red y cloud. Este año, Citrix celebra 25 años de innovación, logrando que las TI sean más sencillas y los trabajadores sean más productivos. Con unos ingresos anuales de 2900 millones de dólares en 2013, las soluciones de Citrix son utilizadas en más de 330 000 organizaciones y por más de 100 millones de personas en todo el mundo. Para más información, visite www.citrix.es.