Hoja de datos

PROTECCIÓN CONTRA DDoS DE ARBOR CLOUD

Protección automatizada completa contra ataques DDoS modernos.

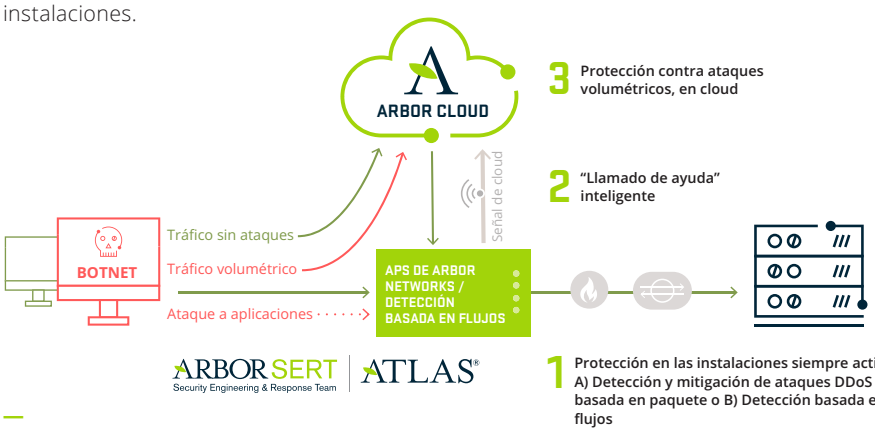
La tendencia de los ataques DDoS no es favorable para las empresas. Los ataques volumétricos crecen cada vez más. La creciente popularidad de los ataques de reflejo/amplificación agrega una nueva capa de complejidad. Los ataques DDoS modernos ahora emplean una combinación de vectores volumétricos, de agotamiento de estado TCP y de ataques a nivel de las aplicaciones. La protección contra DDoS de Arbor Cloud™ para empresas (Arbor Cloud) proporciona servicios de depuración de tráfico basados en cloud que están fuertemente integrados con la defensa de mitigación DDoS en las instalaciones. Este método de varias capas para la protección DDoS es una mejor práctica empresarial para la mitigación de las dinámicas amenazas DDoS de hoy en día.

Protección en capas contra el ataque DDoS moderno

Como parte de un método de capas para la protección contra DDoS, Arbor Cloud proporciona protección en cloud contra ataques DDoS avanzados y de alto volumen, sin interrumpir el acceso a sus aplicaciones y servicios. El servicio de depuración de tráfico a pedido de Arbor Cloud, con la asistencia de los expertos de seguridad DDoS de Arbor, defiende al cliente contra los ataques DDoS volumétricos que son demasiado grandes para ser mitigados en las instalaciones.

El componente en las instalaciones de Arbor Cloud, Arbor Networks® APS, proporciona una detección y mitigación de ataques DDoS en línea, basada en paquete y siempre activada. Arbor APS puede detectar y detener todos los tipos de ataques DDoS. Sin embargo, en caso de un ataque DDoS volumétrico grande que sobrecargue los circuitos en contacto con Internet y la protección local, a través de una función poderosa denominada "Cloud Signaling™", Arbor APS puede notificar y volver a enrutar automáticamente el tráfico de ataque hacia una ubicación de depuración de Arbor Cloud donde se mitiga el ataque. La combinación de Arbor APS en las instalaciones, Cloud Signaling y Arbor Cloud ofrece la protección más completa contra los ataques DDoS modernos.

Además, la opción de Detección basada en flujos de Arbor Cloud ofrece una alternativa a Arbor APS en las instalaciones. A través de la recolección y análisis de flujos, se detectan automáticamente los ataques DDoS y se envía una "Señal de cloud" a Arbor Cloud para la mitigación en cloud. Una implementación podría tener la combinación de Arbor APS y la Detección basada en flujos para una protección automatizada contra ataques DDoS en las instalaciones.



La combinación completamente integrada de 1) APS en las instalaciones para una protección en línea siempre activa contra ataques a nivel de las aplicaciones; 2) Cloud Signaling inteligente para que 3) Arbor Cloud detenga los ataques más grandes, todo equipado en forma continua con la inteligencia de amenazas globales de ATLAS/ASERT, ofrece la solución de protección contra DDoS más completa de la industria.

Características y beneficios principales

Protección global contra DDoS

Una única solución que ofrece protección contra DDoS independiente de la portadora, respaldada por inteligencia de seguridad de nivel mundial y productos de protección contra DDoS líderes en la industria.

Varios Tbps de protección en cloud

Filtra los ataques DDoS de gran volumen con vatios Tbps de capacidad de depuración de tráfico basado en cloud. Soporte para mitigación IPv4 e IPv6 en cloud.

Protección inteligente en capas

Integra Arbor APS en las instalaciones para una detección basada en paquete o Detección basada en flujos virtual con protección en cloud a través de la tecnología exclusiva de Cloud Signaling™.

Con Inteligencia de amenazas globales

Las soluciones de protección contra DDoS de Arbor Cloud y en las instalaciones están automáticamente equipadas con la inteligencia de amenazas globales más reciente de Arbor Security Engineering & Response Team (ASERT).

Servicio de APS administrados (mAPS)

Confíe en la experiencia líder en la industria de Arbor Networks para administrar y optimizar su protección contra DDoS en las instalaciones.

ARBOR® NETWORKS

The Security Division of NETSCOUT

Poderosa depuración de tráfico a pedido basada en cloud

Cuando ocurre un ataque, la velocidad y agilidad son críticas para la continuidad del negocio. En el caso de un ataque volumétrico, el APS en las instalaciones funciona como la primera línea de defensa que detecta el ataque. A medida que el ataque se aproxima a su capacidad de ancho de banda y APS se lo indica a Arbor Cloud para que tome el control, Arbor Cloud vuelve a enrutar el tráfico de entrada hacia uno de los cuatro centros de depuración global de Arbor para la mitigación basada en cloud. Los centros de depuración tienen varios Tbps de capacidad de mitigación DDoS en forma colectiva a su disposición. Cuando ocurre esto, el Centro de operaciones de seguridad disponible las 24 horas, los 7 días de la semana, de Arbor Cloud trabaja de cerca con sus equipos de seguridad/TI para bloquear rápidamente el tráfico DDoS malicioso, a la vez que devuelve todo su tráfico legítimo nuevamente a su data center.

Arbor Cloud proporciona una capacidad de depuración IPv4 e IPv6 global y puede manejar los ataques más grandes y complejos de la actualidad que amenazan la disponibilidad de los recursos y activos críticos.

Especificaciones de Arbor Cloud

Centro de operaciones de seguridad de Arbor Cloud

América del Norte (Sterling, VA)

Ubicaciones de centros de depuración basada en cloud

Depuración en cloud combinada > 1 Tbps

- Costa este (Ashburn, VA)
- Costa oeste (San José, CA)
- Europa central (Amsterdam, NL)
- Asia (Singapur)

Opciones de paquete

- Precio basado en el tráfico limpio
- Mitigación = ventana de uso de 72 horas
- Sin tarifa de configuración para el aprovisionamiento estándar
- Todos los precios son mensuales, a menos que se notifique lo contrario

Opciones de prestación de servicio

- Arbor Cloud Connect: Proporciona soporte de mitigación en cloud en espera en caso de un ataque
- Arbor Cloud Essentials: Proporciona soporte de mitigación en tiempo real hasta 12 veces por año
- Arbor Cloud Essentials+: Soporte de mitigación en cloud en tiempo real ilimitado

Paquete de servicios flexible

Opciones basadas en tráfico limpio

- 100 Mbps
- 500 Mbps
- 1 Gbps
- 2 Gbps
- 4 Gbps
- 8 Gbps
- 10 Gbps

Incluido

- 12 mitigaciones por año
- BGP: Protege 1/24 con 1 ubicación de retorno (GRE)
- DNS: 5 nombres de host protegidos
- Alertas y monitoreo de Cloud Signaling
- Informes de amenazas, análisis y advertencias de ataques de ASERT
- Servicios de soporte de nivel 1, 2 y 3 las 24 horas, los 7 días de la semana
- Acuerdo de nivel de servicios "Es hora de mitigar" de Arbor

Paquete de servicios de retención

Opciones basadas en tráfico limpio

- 100 Mbps
- 500 Mbps
- 1 Gbps

Incluido

- Tarifa de suscripción mensual baja
- Incluye 1 mitigación por año (mitigaciones adicionales por una tarifa)
- BGP: Protege 1/24 con 1 ubicación de retorno (GRE)
- DNS: 5 nombres de host protegidos
- Alertas y monitoreo de Cloud Signaling
- Informes de amenazas, análisis y advertencias de ataques de ASERT
- Servicios de soporte de nivel 1, 2 y 3 las 24 horas, los 7 días de la semana
- Acuerdo de nivel de servicios "Es hora de mitigar" de Arbor

Las opciones adicionales incluyen

Opciones de DNS

- Host adicional
- Certificado SSL (por certificado)
- Configuración/cambio de emergencia (una vez)

Opciones de BGP

- Extremo de túneles GRE adicional
- Adicional/24 horas de protección
- Conexión directa con uno o más centros de depuración de Arbor Cloud

Opciones en las instalaciones

Arbor APS

- Detección y mitigación en línea, basada en paquete y siempre activa
- Dispositivo 2U capaz de mitigar ataques de hasta 40 Gbps
- Dispositivo virtual capaz de detener ataques de menos de 1G; Hipervisores soportados: VMware, KVM; Orquestación VNF soportada: Cloud-Init, Openstack

Detección basada en flujos de Arbor Cloud

- Recopilación automatizada y virtual de flujos, análisis y detección de ataques DDoS
- Cloud Signaling automatizada para Arbor Cloud
- Hipervisores soportados: VMware, XEN, KVM

Arbor Security Engineering & Response Team (ASERT)

ASERT es un equipo de nivel mundial de investigadores de seguridad, con acceso a más de 140+ Tbps de tráfico de Internet global en tiempo real para analizar. ASERT utiliza una combinación sofisticada de recolección de datos de ataques, información de socios y herramientas de análisis para descubrir y analizar las amenazas de Internet emergentes así como crear defensas dirigidas para proteger al cliente contra los ataques más sofisticados y avanzados.

ASERT proporciona a los clientes inteligencia global a través de Informes de amenazas semanales que están disponibles en el portal de Arbor Cloud.

La siguiente información se puede ver desde el portal:

- Mapa de amenazas globales
- Informes de amenazas (Arbor Cloud), informes de inteligencia posteriores al incidente, en contexto y específico para el cliente
- Principales sources de amenazas
- Índice de amenazas
- Principales ataques de Internet

ARBOR NETWORKS
The Security Division of NETSCOUT

Estados Unidos
T: +1.781.362.4300
contact@arbor.net

Brasil
T: +55.11.4380.8035
brasil@arbor.net

México, Caribe & Central America
T: +52.55.4624.4842
mxcca@arbor.net

North of Latin America
T: +57.1.508.7099
nola@arbor.net

South of Latin America
T: +54.11.5218.4007
sola@arbor.net

www.arbornetworks.com

DS/ACE/SP/0717-LETTER