



Mitiga los ataques DDoS con SASE de proveedor único

A medida que las amenazas cibernéticas se hacen más complejas y frecuentes, las organizaciones se ven sometidas a una presión cada vez mayor para adoptar soluciones innovadoras para proteger sus redes. Los ataques distribuidos de denegación de servicio (DDoS) siguen siendo una de las formas más disruptivas de ciberataques, ya que causan tiempos de inactividad significativos, pérdidas financieras y daños a la reputación de las empresas.

El impacto de estos ataques es cada vez mayor: de acuerdo con el informe Gcore de 2024¹, los ataques DDoS aumentaron un 46 % en el primer semestre de 2024 en comparación con el mismo período de 2023, con la alarmante cifra de 445 000 ataques registrados solo en el segundo trimestre de 2024.

Para combatir estas amenazas en continua evolución, la solución HPE Aruba Networking SASE ofrece una potente defensa multicapa que integra una SD-WAN segura con protección contra DDoS adaptable. Esta protección avanzada se complementa con otras características de seguridad esenciales, como los sistemas de prevención y detección de intrusiones (IDS/IPS) y la segmentación basada en roles. Además, HPE Aruba Networking incorpora acceso a la red de confianza cero (ZTNA) en su solución SASE (extremo de servicio de acceso seguro), con lo que se reduce significativamente la superficie de ataque al garantizar que ningún servicio de red quede expuesto a usuarios no autorizados. Al aplicar estrictos controles de acceso, ZTNA no solo ayuda a minimizar el riesgo de ataques DDoS, sino que también proporciona una capa crítica de protección contra el acceso no autorizado, lo que mejora la postura de seguridad general de la organización.

Este enfoque integral ayuda a garantizar que las organizaciones estén equipadas para hacer frente al creciente panorama de amenazas con soluciones resilientes y adaptables, para protegerlas tanto de los ataques DDoS tradicionales como de los más sofisticados.

¿Qué es un ataque DDoS?

Antes de profundizar en cómo HPE Aruba Networking ayuda a mitigar los ataques DDoS, es importante entender qué es un ataque DDoS.

Un ataque DDoS es un intento malicioso de saturar una red, servicio o aplicación, inundándola con tráfico procedente de múltiples fuentes. El objetivo de un ataque de este tipo es interrumpir el funcionamiento normal del servicio en cuestión, de modo que no esté disponible para los usuarios legítimos. Los ataques DDoS se dividen en tres categorías: ataques basados en volumen, basados en protocolo y en la capa de aplicación.

¹ «[DDoS Attack Trends for Q1–Q2 2024: Insights from Gcore Radar Report](#)» («Tendencias de ataques DDoS para el primer y segundo trimestre de 2024: información sobre el informe Gcore Radar»), Gcore, 14 de agosto de 2024

Algunos ejemplos de ataques basados en volumen incluyen:

- **Inundación de ICMP:** los atacantes utilizan el protocolo de mensajes de control de internet (ICMP) para enviar un número masivo de solicitudes de ping, con lo que saturan el ancho de banda de la red.
- **Inundación de UDP:** los atacantes inundan el objetivo con paquetes del protocolo de datagramas de usuario (UDP), con el consiguiente consumo de recursos al obligar al servidor a procesar y responder a cada paquete.

Algunos ejemplos de ataques basados en protocolo incluyen:

- **Inundación de SYN:** los atacantes explotan el proceso de protocolo de enlace TCP enviando múltiples solicitudes de conexión que nunca llegan a completarse, con lo que consumen recursos del servidor.
- **Suplantación de IP:** los atacantes camuflan sus direcciones IP enviando tráfico que parece legítimo, lo que dificulta el bloqueo del tráfico malicioso.

Un ejemplo de ataque a la capa de aplicación es:

- **Inundación de HTTP:** una inundación de HTTP envía numerosas solicitudes HTTP GET o POST a un servidor web, lo que agota la capacidad de procesamiento y el ancho de banda del servidor.

Estos ataques pueden provocar importantes congestiones en la red, ralentizaciones de las aplicaciones o incluso la interrupción total del servicio, lo que puede afectar tanto a servicios web como a aplicaciones corporativas internas.

Desafíos en la defensa de ataques tradicionales DDoS

En el modelo tradicional, la protección contra DDoS era en gran medida reactiva y requería que los administradores establecieran manualmente umbrales de denegación de servicio (DoS) para detectar y mitigar el tráfico malicioso. Este enfoque presentaba varias limitaciones:

- **Configuración manual:** los administradores tenían que estimar los umbrales apropiados para detectar ataques DoS basándose en los patrones de tráfico de red. Este método solía presentar errores y a menudo conducía a subestimar o sobrestimar los umbrales.
- **Actualizaciones frecuentes:** los patrones de tráfico de la red cambian constantemente, por lo que es necesario ajustar los umbrales con frecuencia. Si no se actualizan los umbrales, podrían producirse ataques no detectados o el bloqueo de tráfico legítimo.
- **Respuesta inflexible:** los mecanismos de defensa contra DDoS tradicionales a menudo consideraban todos los picos de tráfico como potencialmente maliciosos. Este enfoque podía bloquear el tráfico legítimo durante los picos de tráfico, como los picos de inicio de sesión o las copias de seguridad periódicas, lo que causaba interrupciones de servicio.

Ante estos desafíos, existía una clara necesidad de una solución más dinámica y automatizada para gestionar las amenazas DDoS de manera eficaz.

DDoS adaptable: un nuevo enfoque para la defensa contra DDoS basado en el aprendizaje automático

EdgeConnect SD-WAN, que forma parte de HPE Aruba Networking SASE, ofrece una solución avanzada de protección contra DDoS adaptable, diseñada para hacer frente a las limitaciones de las defensas contra DDoS tradicionales, gracias a su cortafuegos integrado de última generación. A través del aprendizaje automático y del análisis de tráfico avanzado, la solución de protección contra DDoS adaptable proporciona una defensa continua y ayuda a garantizar que la red se adapte a los patrones de tráfico cambiantes en tiempo real.

Los administradores pueden gestionar la red durante un ataque DoS estableciendo umbrales mínimos y máximos. El umbral mínimo permite la detección temprana de posibles problemas, mientras que el umbral máximo ayuda a garantizar que el tráfico legítimo no se rechace demasiado pronto. Esto proporciona a los administradores un mayor control y ayuda a garantizar que el tráfico solo se bloquee cuando sea absolutamente necesario.

La solución de protección contra DDoS adaptable establece estos umbrales a través de dos características principales: la limitación automática de velocidad, que ajusta automáticamente el umbral mínimo con aprendizaje automático en función de las condiciones de la red, y Smart Burst, que optimiza el umbral máximo para gestionar los picos de tráfico (figura 1).

The screenshot shows the 'Firewall Protection Profile' configuration page. At the top, there is a toggle for 'Enable Protection Profile' which is turned on. Below it, the 'Profile Name' is set to 'smart_burst_preset'. Under 'Security Settings', several checkboxes are visible, including 'Enforce strict 3-way tcp', 'Discard non-syn tcp', 'Enforce DPI validation', 'Enforce IP spoof check', and 'Allow asymmetric routing'. The 'DoS Thresholds' section is set to 'Smart burst'. A table below lists various thresholds with columns for 'Edit', 'Classification...', 'Metric', 'IP protocol', 'Min label', 'Min value', 'Min action', 'Max label', 'Max value', and 'Max action'. Two blue boxes highlight the 'Min label' and 'Max label' columns, showing values like 'Baseline' and 'Excess burst'. A 'Show advanced settings' link is at the bottom right.

Edit	Classification...	Metric	IP protocol	Min label	Min value	Min action	Max label	Max value	Max action
	Source-level	Concurrent flo...	All	Baseline	Dynamic	Log	Committed burst	Dynamic	Drop excess
	Source-level	Flows per sec...	All	Baseline	Dynamic	Log	Custom	0.9%	Rapid aging
	Source-level	Embryonic flows	All	Baseline	Dynamic	Log	Custom	1.4%	Rapid aging
	Zone-level	Concurrent flo...	All	Baseline	Dynamic	Rapid aging	Excess burst	Dynamic	Drop excess

Figura 1. Definición de umbrales DDoS adaptables mínimos y máximos con limitación automática de velocidad basada en aprendizaje automático y Smart Burst

Limitación automática de velocidad

Esta función utiliza aprendizaje automático para calcular dinámicamente una línea de base para los patrones de tráfico de red normales. En función de las estadísticas y los patrones de la red, la limitación automática de velocidad ajusta continuamente el umbral DoS mínimo, que sirve como línea de base para detectar anomalías.

A medida que cambian las condiciones de la red (por ejemplo, se implementan nuevos servicios, aumenta el volumen de tráfico o cambian los picos de tráfico), la limitación automática de velocidad actualiza esta línea de base para reflejar la nueva normalidad. De este modo, se minimizan los falsos positivos y se detectan con antelación posibles amenazas DDoS.

La eliminación de la configuración manual de umbrales reduce la carga de los administradores y ayuda a garantizar que la red esté siempre protegida sin necesidad de realizar constantes reconfiguraciones.

Smart Burst

El objetivo de los ataques DDoS suele ser aprovechar los picos temporales de tráfico en la red. Sin embargo, no todos los picos de tráfico son maliciosos. Por ejemplo, actividades legítimas como el inicio de sesión de los usuarios o las copias de seguridad de datos pueden provocar aumentos significativos y temporales del tráfico.

Smart Burst está diseñado para gestionar estas ráfagas de tráfico **bueno**, al tiempo que ayuda a garantizar que el tráfico **malo** (es decir, malicioso) no consuma el ancho de banda de la red. Esta solución asigna de forma automática la capacidad de flujo no utilizada en las zonas del cortafuegos en función de las condiciones de tráfico actuales.

Smart Burst ofrece cuatro modos de funcionamiento:

Línea de base plus: añade un búfer al umbral de referencia para permitir picos de tráfico legítimos sin marcarlos prematuramente como ataques.

Ráfaga comprometida: asigna proporcionalmente capacidad de flujo adicional entre las zonas del cortafuegos, lo que ayuda a garantizar un uso óptimo del ancho de banda.

Ráfaga excesiva: comparte la capacidad de flujo no utilizada entre zonas, lo que proporciona una defensa adicional durante los picos repentinos de tráfico.

Personalizado: los administradores pueden definir sus propios umbrales y reglas de tráfico en determinados segmentos de la red.

Mediante la integración de aprendizaje automático y análisis de tráfico en sus mecanismos de defensa contra DDoS, la capacidad contra DDoS adaptable de HPE Aruba Networking proporciona protección automatizada, inteligente y dinámica que se ajusta al comportamiento de la red en tiempo real. Todo ello ayuda a garantizar un mejor control sobre la protección contra DDoS, sin la necesidad de una intervención manual constante.

Perfiles de protección mediante cortafuegos y control DDoS

Los perfiles de protección mediante cortafuegos (figura 2) de la red SD-WAN segura de HPE Aruba Networking permiten a los administradores informáticos aplicar protección contra DDoS. Pueden:

- **Aplicar un protocolo de enlace de tres vías estricto:** garantiza que todas las conexiones presenten información de estado, lo que permite gestionar de manera eficaz los ataques basados en protocolos, como los ataques de inundación de SYN.
- **Establecer umbrales mínimos y máximos:** los administradores pueden establecer umbrales basados en parámetros de tráfico, como la velocidad de flujo, los flujos concurrentes y los flujos embrionarios (es decir, conexiones TCP semiabiertas). El umbral mínimo ayuda a detectar los primeros signos de un ataque, mientras que el umbral máximo ayuda a garantizar que el tráfico legítimo no se rechace demasiado pronto.
- **Lista de bloqueo de atacantes conocidos:** el sistema puede mantener una lista de direcciones IP de atacantes conocidos y bloquear de forma automática el tráfico de estas fuentes durante un ataque.
- Al permitir que los administradores vinculen diferentes perfiles de protección mediante cortafuegos a las zonas del cortafuegos, la solución HPE Aruba Networking permite un control granular sobre los niveles de protección DDoS. Esta flexibilidad ayuda a garantizar que cada segmento de la red reciba el nivel de protección adecuado en función de su confidencialidad o función.

Firewall Protection Profile

Enable Protection Profile

Profile Name: WAN-SIDE

Security Settings

- Enforce strict 3-way tcp
- Discard non-syn tcp
- Allow asymmetric routing
- Enforce IP spoof check
- Enforce DPI app verification

DoS Thresholds: Strict Add custom threshold

Edit	Classification	Metric	IP protocol	Min valu...	Min action	Max valu...	Max action
	Source-level	Concurrent flows	All	1%	Log	2%	Drop excess
	Source-level	Flows per second	All	0.4%	Rapid aging	0.6%	Drop excess
	Source-level	Embryonic flows	All	0.6%	Rapid aging	0.9%	Drop excess
	Zone-level	Concurrent flows	All	15%	Rapid aging	30%	Drop excess

[Show advanced settings](#)

Allowlist: Management_Subnets

Blocklist: Eg: AddressGroup1

Figura 2. Perfil de protección mediante cortafuegos de SD-WAN EdgeConnect

Análisis DDoS: visibilidad y elaboración de informes

Para complementar su funcionalidad contra DDoS adaptable, la SD-WAN segura de HPE Aruba Networking incluye análisis integrales de DDoS. Estos informes proporcionan información valiosa sobre el rendimiento y la postura de seguridad de la red, lo que permite a los administradores realizar un seguimiento y responder a posibles amenazas en tiempo real (figura 3).

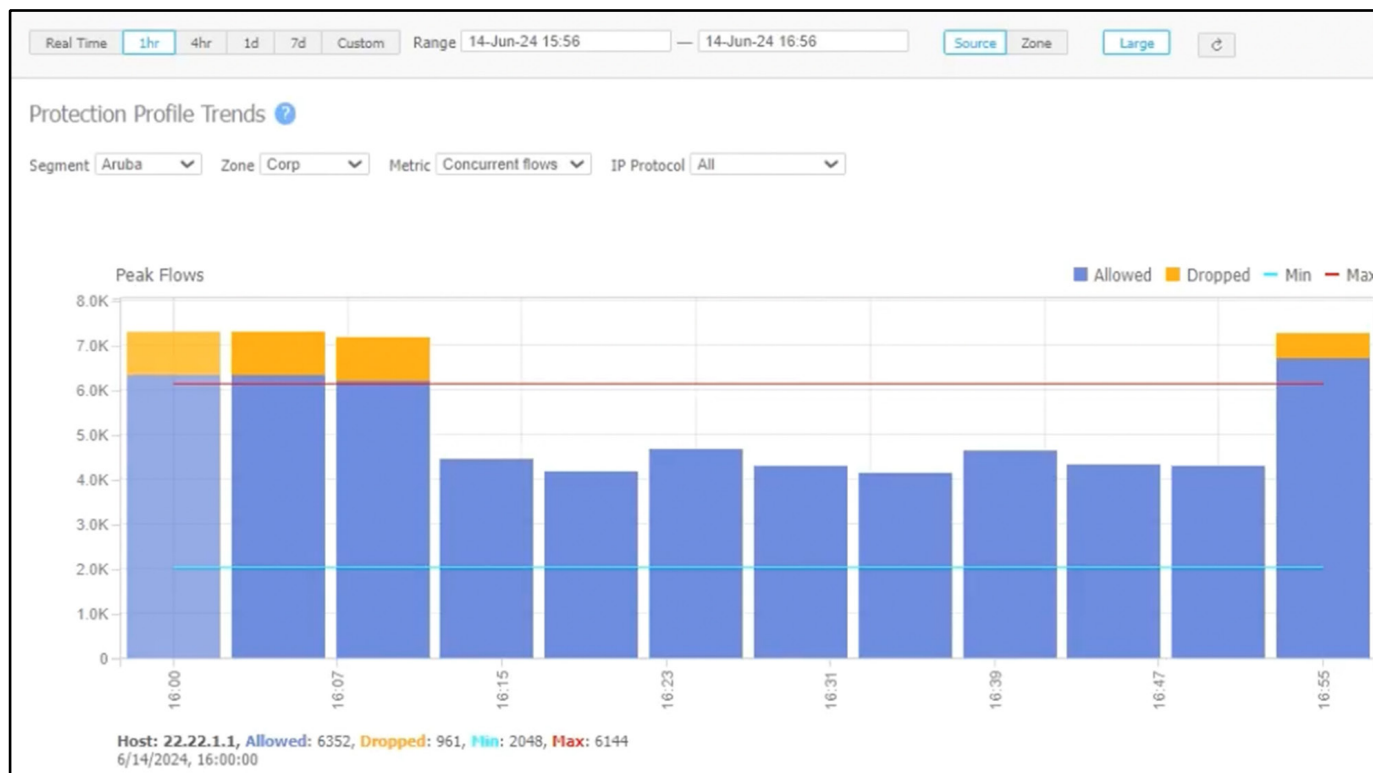


Figura 3. Número de flujos permitidos y rechazados en cada intervalo de cinco minutos por zona del cortafuegos en EdgeConnect SD-WAN

Los informes clave incluyen:

- **Violaciones de umbral:** alerta a los administradores cuando el tráfico supera los umbrales preestablecidos o configurados dinámicamente.
- **Rechazos de flujo:** proporciona detalles sobre los flujos rechazados, lo que ayuda a los administradores a identificar y hacer frente a posibles fuentes de ataque.
- **Hosts y paquetes denegados:** realiza un seguimiento de las direcciones IP y los paquetes bloqueados debido a comportamientos maliciosos ya conocidos.
- **Principales emisores:** identifica los dispositivos o usuarios que generan más tráfico, lo que ayuda a localizar posibles fuentes de tráfico anormal.
- **Notificaciones de alarma:** alerta automáticamente a los administradores cuando se superan los umbrales, lo que permite responder a tiempo a los ataques DoS.

Esta visibilidad granular de los patrones de tráfico y los incidentes de seguridad permite a los equipos de red tomar decisiones informadas, que mejoran la efectividad general de la estrategia de protección contra DDoS.

Complementar la defensa contra DDoS con ZTNA

Con la incorporación de ZTNA, como parte de HPE Aruba Networking SASE, las organizaciones pueden ofrecer una defensa multicapa contra los ataques DDoS. La capacidad de ZTNA para ocultar servicios de internet, segmentar el tráfico de aplicaciones y limitar el acceso solo a usuarios y dispositivos verificados, refuerza significativamente la estrategia general de protección contra DDoS (figura 4). Cuando se combina con la protección contra DDoS adaptable de EdgeConnect SD-WAN, las organizaciones obtienen una solución integral para proteger sus redes de los ataques DDoS.

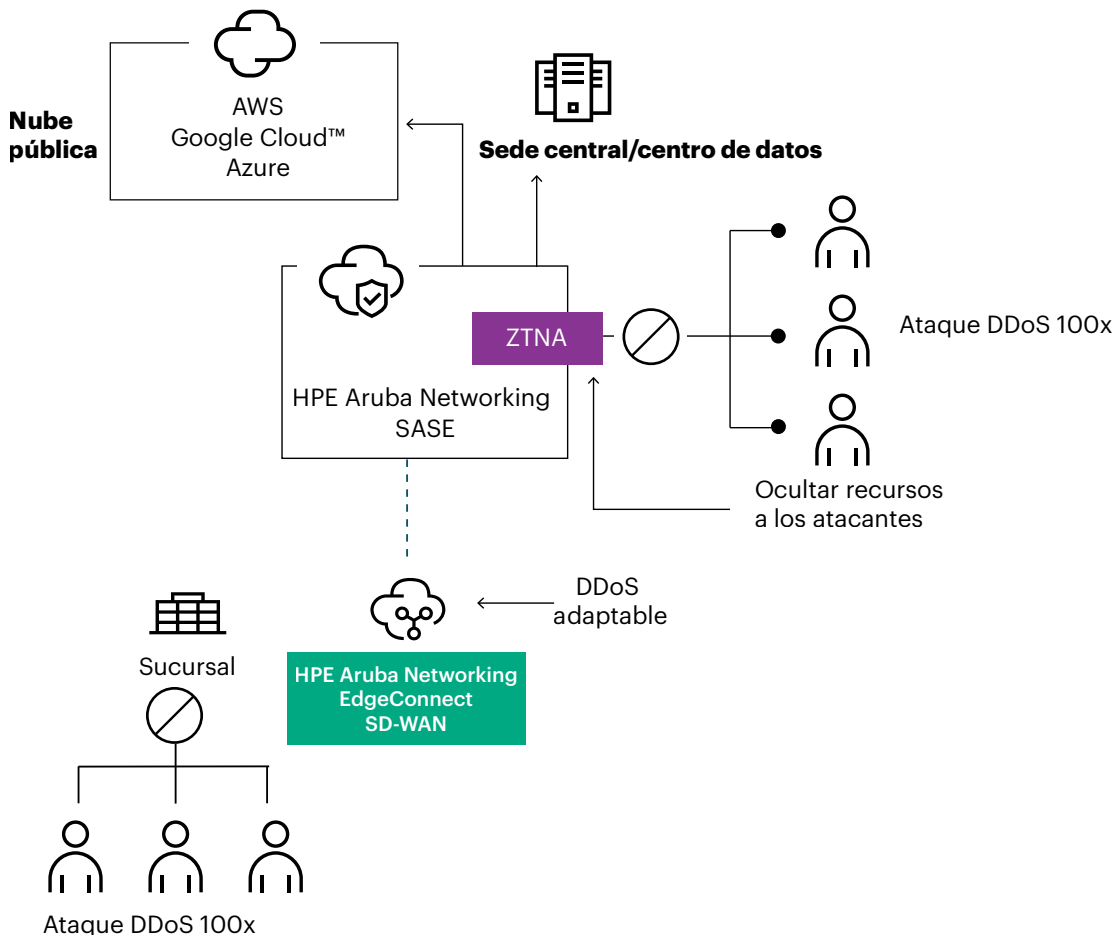


Figura 4. Protección DDoS de dos capas con la solución para DDoS adaptable de EdgeConnect SD-WAN combinada con HPE Aruba Networking ZTNA

HPE Aruba Networking ZTNA opera según el principio de «nunca confíes, verifica siempre». Al mantener los servicios internos ocultos de internet, ayuda a eliminar los puntos de entrada habituales de los ataques DDoS. Solo los dispositivos autenticados y autorizados pueden acceder a servicios específicos, lo que ayuda a garantizar que los atacantes externos no puedan dirigirse directamente a estos servicios para explotarlos mediante ataques DDoS.

Además, ZTNA no permite el movimiento lateral. Dado que ZTNA aplica estrictas políticas de control de acceso, los usuarios no pueden moverse lateralmente hacia otros recursos. Cada conexión se establece de manera exclusiva y conecta a los usuarios autorizados únicamente con los recursos autorizados. De esta manera se reduce la superficie global de ataque, lo que ayuda a garantizar que, aunque un dispositivo se vea comprometido, el impacto quede aislado y no se propague al resto de la red.

Además, a diferencia de las VPN, ZTNA no otorga acceso indiscriminado a los recursos internos. Por ello, ZTNA resulta una alternativa atractiva para las organizaciones que buscan reemplazar las VPN, ya que estas pueden constituir un punto de referencia para los ciberdelincuentes al exponer una amplia gama de recursos de red.

Al verificar continuamente la identidad del usuario y del dispositivo antes de otorgar el acceso, HPE Aruba Networking ZTNA ayuda a garantizar que solo el tráfico legítimo pueda fluir hacia la aplicación autorizada, mientras mantiene a los usuarios fuera de la red corporativa. Así se reducen las posibilidades de que el tráfico malicioso sature los recursos de la red, con lo que se mitigan aún más los riesgos de ataques DDoS. ZTNA reduce eficazmente el número de dispositivos y servicios que pueden ser objeto de ataques, lo que hace que los ataques a gran escala sean menos factibles.

Las políticas dinámicas basadas en el contexto de ZTNA permiten a los administradores de red y de seguridad especificar diferentes niveles de acceso según los roles de los usuarios, la postura del dispositivo y la ubicación. Este control granular protege aún más la red al ayudar a garantizar que solo el tráfico autenticado y de confianza pueda interactuar con los recursos críticos, lo que reduce el riesgo de que el tráfico malicioso se cuele y consuma ancho de banda durante los intentos de DDoS (figura 5).

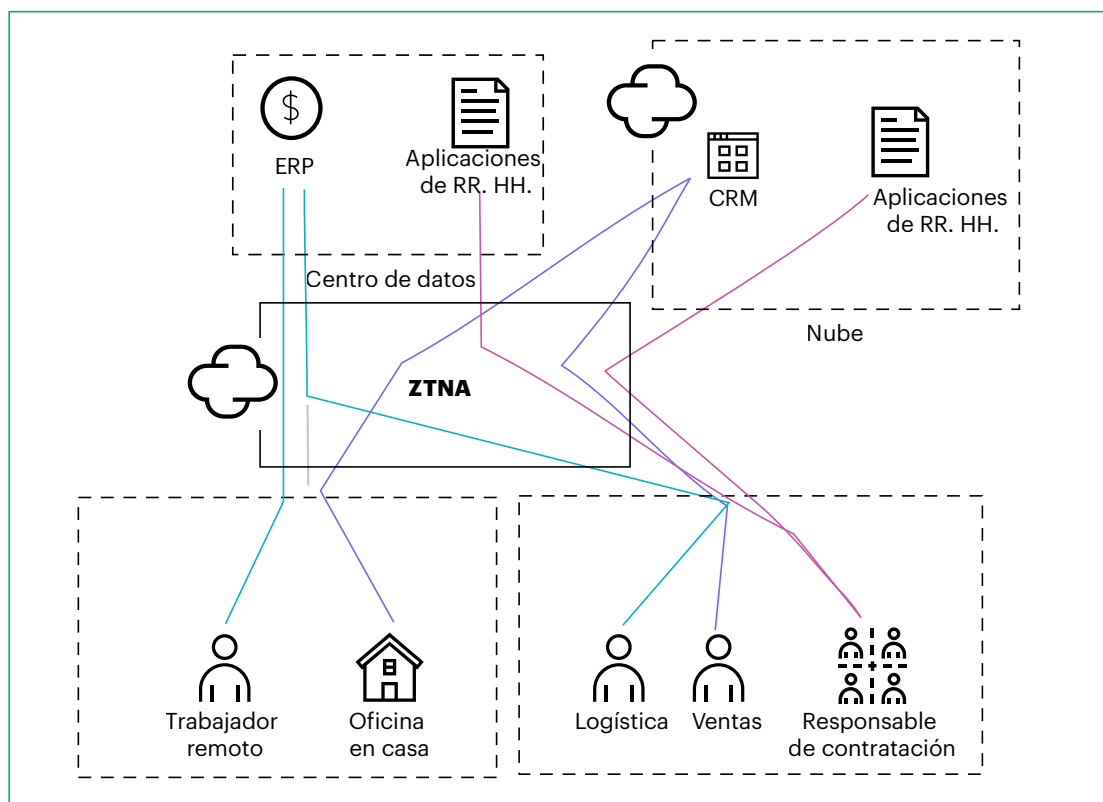


Figura 5. Aplicación de políticas estrictas de acceso con ZTNA

HPE Aruba Networking ZTNA admite usuarios locales y remotos con la capacidad de extremo local, que ayuda a garantizar que el tráfico local siga siendo local y a eliminar el enrutamiento en horquilla hacia la nube. Gracias al extremo local, ZTNA aplica las mismas políticas de control de acceso para los usuarios locales que para los usuarios remotos, lo que permite a las organizaciones mantener una política única y unificada para todos los usuarios. Este enfoque ayuda a minimizar la complejidad y reduce las posibles brechas de seguridad que a menudo surgen al gestionar políticas independientes para diferentes tipos de usuarios, y agiliza la seguridad a la vez que proporciona una protección homogénea.

Seguridad de red integral más allá de DDoS

Mientras que la solución contra DDoS adaptable proporciona protección dinámica y automatizada contra ataques DDoS, HPE Aruba Networking SASE ofrece un marco de seguridad holístico que incluye otras características críticas.

Por ejemplo, el cortafuegos de nueva generación integrado de EdgeConnect SD-WAN proporciona una segmentación de red global que abarca la LAN, la WAN e incluso la nube. Las políticas de seguridad se definen zona por zona, lo que limita la conectividad con otras zonas de conformidad con las políticas de seguridad predefinidas. EdgeConnect SD-WAN también se integra con HPE Aruba Networking ClearPass para proporcionar identidad de usuario y dispositivo y contexto basado en roles, a fin de lograr una segmentación detallada, lo que ayuda a garantizar que los usuarios y dispositivos, incluido IoT, solo lleguen a destinos acordes con su rol en la red.

EdgeConnect SD-WAN incluye un IDS/IPS basado en reglas diseñado para supervisar el tráfico de red e identificar patrones de ataque conocidos. Este sistema basado en firmas se puede configurar para funcionar en modo en línea para una mayor seguridad o en modo fuera de banda para priorizar el rendimiento. Cuando se combina con la protección contra DDoS, el IDS/IPS garantiza que la red permanezca segura frente a una amplia variedad de amenazas, no solo frente a ataques DDoS.

Además, la integración con Splunk ofrece un panel completo para visualizar eventos IDS/IPS, que permite a los administradores filtrar, clasificar y analizar los datos de eventos de seguridad con eficiencia (figura 6).

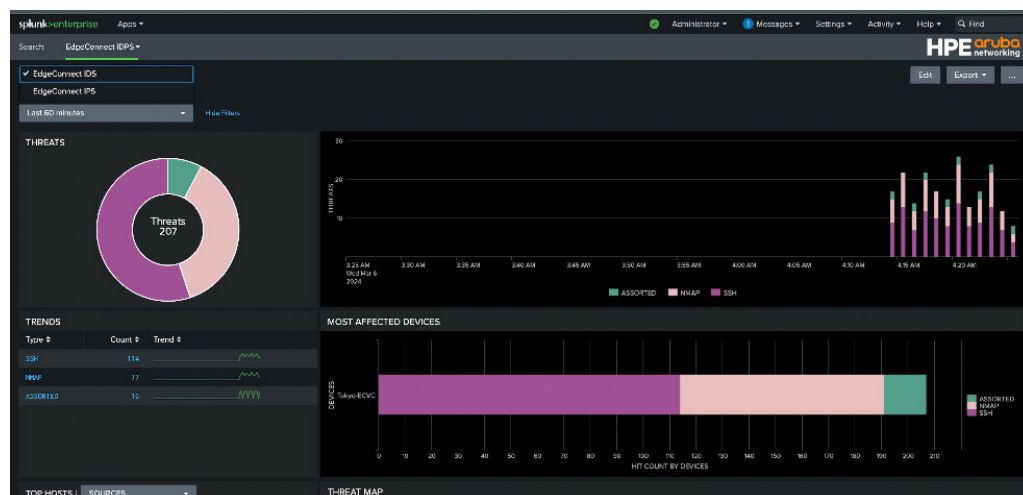


Figura 6. Vista de eventos IDS/IPS en Splunk procedentes de HPE Aruba Networking SD-WAN

Las organizaciones pueden reforzar su postura de seguridad añadiendo otras características de servicio de seguridad en el extremo (SSE), como la puerta de enlace web segura (SWG) y el agente de seguridad de acceso a la nube (CASB) de HPE Aruba Networking, para crear una solución SASE de proveedor único (figura 7).

SWG es una solución de seguridad que protege a los usuarios de las amenazas basadas en la web al supervisar y filtrar el tráfico de internet en tiempo real. Aplica políticas de seguridad para bloquear el acceso a sitios web maliciosos, impide la descarga de malware y filtra contenidos inapropiados o dañinos. Además, EdgeConnect SD-WAN se integra con nuestra SWG para proteger todos los dispositivos de red, incluidos los no gestionados (por ejemplo, invitados y dispositivos IoT), sin la necesidad de agentes individuales en cada dispositivo. Esta característica es particularmente útil para organizaciones con un gran número de dispositivos IoT, que pueden no ser compatibles con los agentes de seguridad tradicionales pero que, aún así, necesitan protección frente a las amenazas basadas en la web.

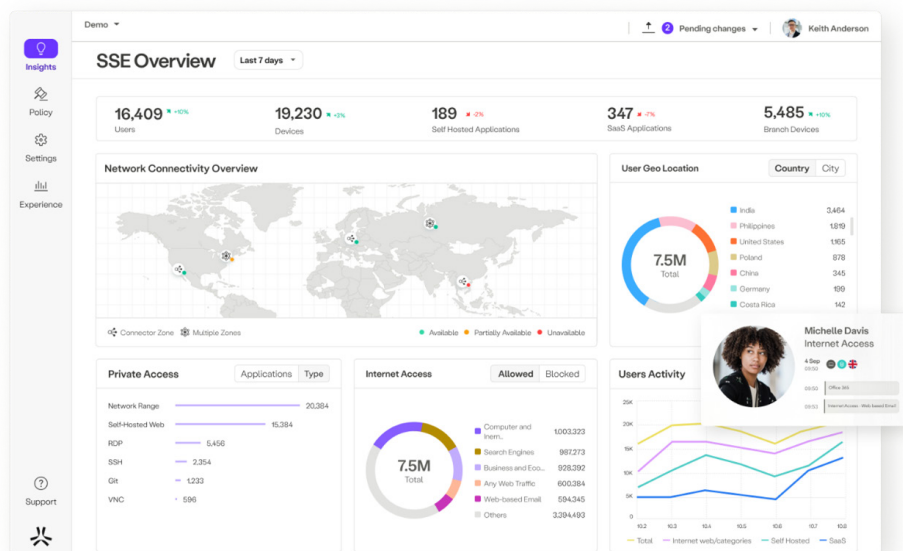


Figura 7. Vista del panel de HPE Aruba Networking SSE para supervisar el acceso a aplicaciones privadas, SaaS e internet

CASB actúa como un punto de control entre los usuarios de los servicios de nube y las aplicaciones SaaS, lo que ayuda a garantizar el uso seguro de los recursos basados en la nube. CASB proporciona visibilidad del uso de la nube en toda la organización, aplica políticas de seguridad y protege los datos confidenciales al supervisar el acceso y el comportamiento en las aplicaciones en la nube. CASB ayuda a prevenir filtraciones de datos mediante la aplicación de cifrado, prevención de pérdida de datos (DLP) y controles de acceso. Al ofrecer controles granulares sobre la forma en que los usuarios interactúan con los servicios de nube, CASB ayuda a proteger los datos confidenciales y a garantizar el cumplimiento de los requisitos normativos, al tiempo que permite una adopción segura de la nube.

Conclusión

HPE Aruba Networking EdgeConnect SD-WAN, mejorada con protección contra DDoS adaptable y HPE Aruba Networking ZTNA, ofrece una defensa fiable y multicapa contra ataques DDoS. La protección contra DDoS adaptable aprovecha el aprendizaje automático para ajustar dinámicamente los umbrales, lo que evita interrupciones y ayuda a garantizar que el tráfico legítimo fluya sin problemas. ZTNA reduce la superficie de ataque al aplicar controles de acceso estrictos y evitar la exposición no autorizada de los recursos de

red. Además, las organizaciones pueden reforzar aún más su postura de seguridad al integrar SWG y CASB para formar una arquitectura SASE completa. SWG brinda protección contra amenazas basadas en la web, mientras que CASB asegura el acceso a la nube, y juntos proporcionan una cobertura integral en todos los puntos de entrada y ayudan a garantizar un entorno de red resiliente y seguro contra DDoS y otras amenazas cibernéticas (figura 8).

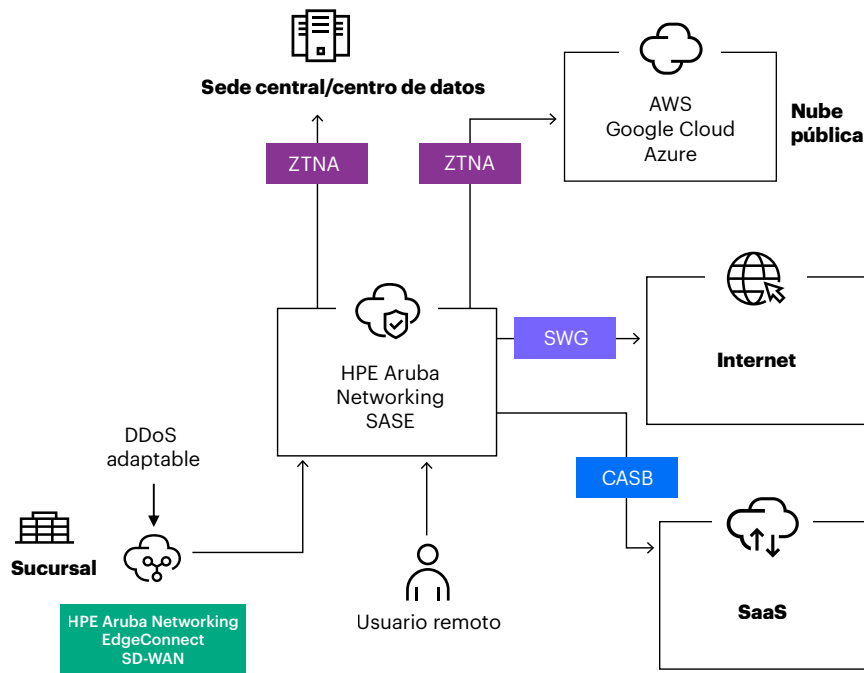


Figura 8. Protección mejorada contra DDoS y acceso seguro a aplicaciones privadas, SaaS e internet con HPE Aruba Networking SASE

Más información en

[HPE Aruba Networking SD-WAN](#)

[HPE Aruba Networking SSE](#)

[HPE Aruba Networking SASE](#)

Visita [HPE.com](https://www.hpe.com)

[Iniciar chat ahora](#)

© Copyright 2025 Hewlett Packard Enterprise Development LP. La información contenida en este documento está sujeta a cambios sin previo aviso. Las únicas garantías de los productos y servicios de Hewlett Packard Enterprise figuran en las declaraciones expresas de garantía incluidas en los mismos. Nada de lo que aquí se indica debe interpretarse como una garantía adicional. Hewlett Packard Enterprise no se hará responsable de los errores u omisiones técnicos o editoriales que pudiera contener el presente documento.

Google Cloud es una marca comercial de Google Inc. Azure es una marca comercial o marca comercial registrada de Microsoft Corporation en EE. UU. y en otros países. Todas las marcas de terceros son propiedad de sus respectivos titulares.

a50011705ESE, rev. 1

HEWLETT PACKARD ENTERPRISE

[hpe.com](https://www.hpe.com)

