HPE aruba networking

Solution overview

Mitigate DDoS attacks with single-vendor SASE

HPE

As cyber threats grow in complexity and frequency, organizations are under increasing pressure to adopt innovative solutions to safeguard their networks. Distributed denial of service (DDoS) attacks continue to be one of the most disruptive forms of cyberattacks, causing significant downtime, financial losses, and reputational damage.

The impact of these attacks is escalating — according to the Gcore 2024 Report[1], DDoS attacks surged by 46% in the first half of 2024 compared to the same period in 2023, with an alarming 445,000 attacks recorded in Q2 2024 alone.

To combat these evolving threats, the HPE Aruba Networking SASE solution offers a powerful, multilayered defense that integrates secure SD-WAN with Adaptive DDoS protection. This advanced protection is complemented by other essential security features such as intrusion detection and prevention systems (IDS/IPS) and role-based segmentation. Additionally, HPE Aruba Networking incorporates zero trust network access (ZTNA) into its secure access service edge (SASE) solution, which significantly reduces the attack surface by ensuring no network services are exposed to unauthorized users. By enforcing strict access controls, ZTNA not only helps minimize the risk from DDoS attacks but also provides a critical layer of protection against unauthorized access, enhancing the overall security posture of the organization.

This comprehensive approach helps ensure organizations are equipped to face the growing threat landscape with resilient, adaptable solutions that protect their organizations from both traditional and sophisticated DDoS attacks.

What is a DDoS attack?

Before delving into how HPE Aruba Networking helps mitigate DDoS attacks, it is important to understand what a DDoS attack is.

A DDoS attack is a malicious attempt to overwhelm a network, service, or application by flooding it with traffic from multiple sources. The goal of such an attack is to disrupt the normal functioning of the targeted service, rendering it unavailable to legitimate users. DDoS attacks fall into three categories: volume-based, protocol-based, and application-layer attacks.

[1] "DDoS Attack Trends for Q1–Q2 2024: Insights from Gcore Radar Report," Gcore, August 14, 2024

Examples of volume-based attacks include:

— **ICMP flood:** Attackers use the Internet Control Message Protocol (ICMP) to send massive numbers of ping requests, overwhelming the network's bandwidth.

— **UDP flood:** Attackers flood the target with User Datagram Protocol (UDP) packets, consuming resources by forcing the server to process and respond to each packet.

Examples of protocol-based attacks include:

— **SYN flood:** Attackers exploit the TCP handshake process by sending multiple connection requests but never completing them, thus consuming server resources.

— **IP spoofing:** Attackers disguise their IP addresses by sending traffic that appears to be legitimate, making it difficult to block malicious traffic.

An example of application-layer attacks is:

— **HTTP flood:** An HTTP flood sends numerous HTTP GET or POST requests to a web server, exhausting server processing capacity and bandwidth.

These attacks can cause significant network congestion, application slowdowns, or even complete outages, affecting everything from web services to internal corporate applications.

Challenges in traditional DDoS defense

In the traditional model, DDoS protection was largely reactive, requiring administrators to manually set denial of service (DoS) thresholds to detect and mitigate malicious traffic. This approach had several limitations:

— **Manual configuration:** Administrators had to estimate the appropriate thresholds for detecting DoS attacks based on network traffic patterns. This method was error-prone and often led to either underestimating or overestimating thresholds.

— **Frequent updates:** Network traffic patterns constantly change, requiring frequent threshold adjustments. Failure to update thresholds could result in undetected attacks or legitimate traffic being blocked.

— **Inflexible response:** Traditional DDoS defense mechanisms often treated all traffic surges as potentially malicious. This approach could block legitimate traffic during peak times, such as log-in spikes or regular backups, causing service disruptions.

Given these challenges, there was a clear need for a more dynamic, automated solution to handle DDoS threats effectively.

Adaptive DDoS: A new approach to DDoS defense based on machine learning (ML)

HPE Aruba Networking EdgeConnect SD-WAN, part of HPE Aruba Networking SASE, offers a cutting-edge Adaptive DDoS protection solution designed to address the limitations of traditional DDoS defenses, thanks to its built-in next-generation firewall. By leveraging ML and advanced traffic analysis, Adaptive DDoS provides continuous protection and helps ensure that the network adapts to changing traffic patterns in real time.

Administrators can manage the network during a DoS attack by setting both minimum and maximum thresholds. The minimum threshold allows for early detection of potential issues while the maximum threshold helps ensure legitimate traffic isn't dropped too soon. This provides administrators with greater control, helping ensure that traffic is only blocked when absolutely necessary.

Adaptive DDoS sets these thresholds through two key features: Auto rate limiting, which automatically adjusts the minimum threshold with machine learning (ML) based on network conditions, and Smart Burst, which optimizes the maximum threshold to handle traffic spikes (Figure 1).

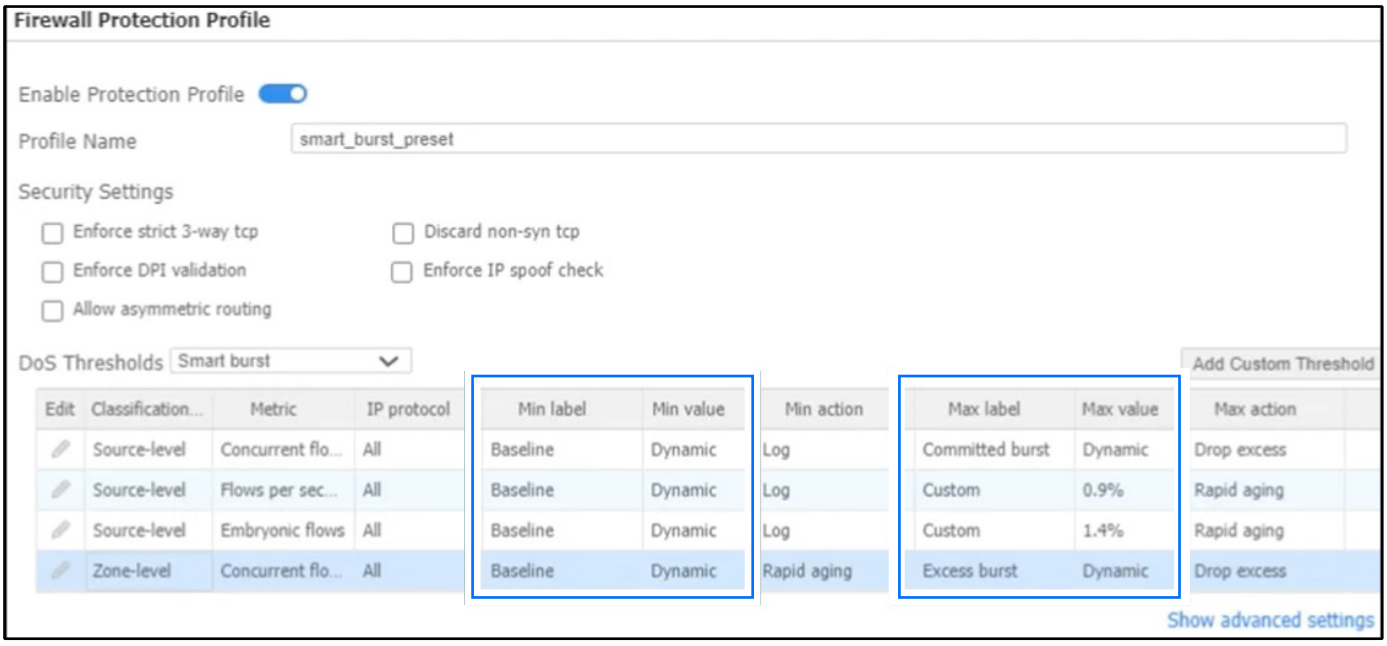

Figure 1. Minimum and maximum Adaptive DDoS threshold definition leveraging ML-based auto rate limiting and Smart Burst

Auto rate limiting

This feature uses ML to dynamically calculate a baseline for normal network traffic patterns. Based on network statistics and patterns, auto rate limiting continuously adjusts the minimum DoS threshold, which serves as the baseline for detecting anomalies.

As network conditions change (for example, new services are deployed, traffic volume grows, or peak times shift), auto rate limiting updates this baseline to reflect the new normal. This helps minimize false positives while providing early detection of potential DDoS threats.

The elimination of manual threshold configuration reduces the burden on administrators and helps ensure that the network is always protected without constant reconfiguration.

Smart Burst

DDoS attacks often aim to exploit temporary surges in network traffic. However, not all traffic spikes are malicious. For instance, legitimate activities such as user logins or data backups may cause significant, temporary increases in traffic.

Smart Burst is designed to handle these **good** traffic bursts while helping ensure that **bad** traffic (that is, malicious) does not consume the network's bandwidth. It automatically allocates unused flow capacity across firewall zones based on current traffic conditions.

Smart Burst offers four operational modes:

Baseline plus: Adds a buffer to the baseline threshold, allowing for legitimate traffic spikes without prematurely flagging them as attacks

Committed burst: Proportionally allocates extra flow capacity across firewall zones, helping ensure optimal bandwidth usage

Excess burst: Shares unused flow capacity across zones, providing additional defense during sudden traffic surges

Custom: Administrators can define their own thresholds and traffic rules for specific network segments

By integrating ML and traffic analysis into its DDoS defense mechanisms, HPE Aruba Networking Adaptive DDoS capability provides automated, intelligent, and dynamic protection that adjusts to network behavior in real time. This helps ensure better control over DDoS protection without the need for constant manual intervention.

Firewall Protection Profiles and DDoS control

The Firewall Protection Profiles (Figure 2) within HPE Aruba Networking secure SD-WAN allows IT administrators to enforce DDoS protection. They can:

— **Enforce strict three-way handshake** — This ensures that all connections are stateful, effectively managing protocol-based attacks, such as SYN flood attacks.

— **Set minimum and maximum thresholds** — Administrators can set thresholds based on traffic parameters, including flow rate, concurrent flows, and embryonic flows (that is, half-open TCP connections). The minimum threshold helps detect early signs of an attack while the maximum threshold helps ensure that legitimate traffic isn't dropped too early.

— **Known attacker block list** — The system can maintain a list of known attacker IP addresses, automatically blocking traffic from these sources during an attack.

— By allowing administrators to bind different Firewall Protection Profiles to firewall zones, HPE Aruba Networking solution enables granular control over DDoS protection levels. This flexibility helps ensure that each segment of the network receives the appropriate level of protection based on its sensitivity or function.

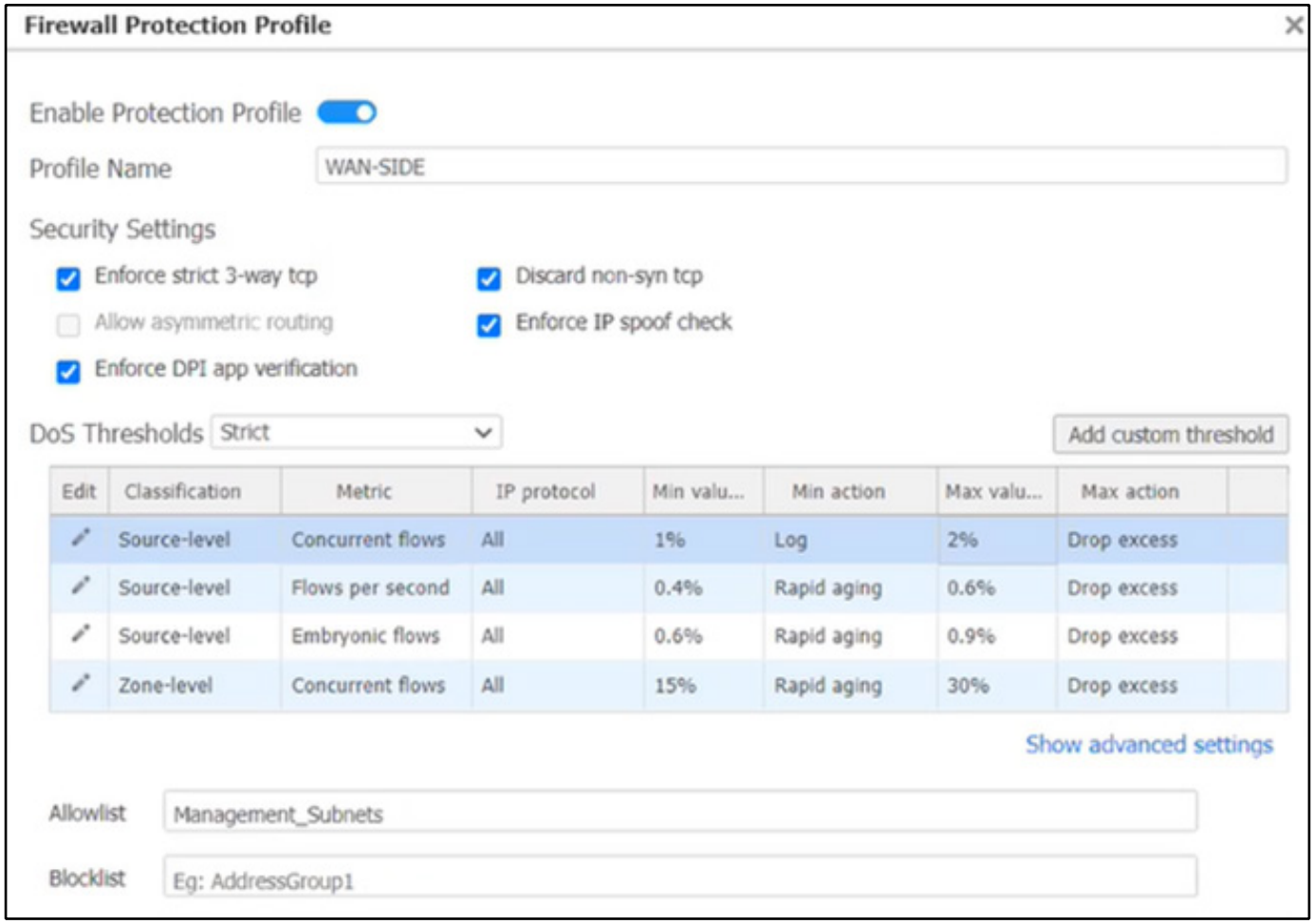

Figure 2. HPE Aruba Networking EdgeConnect SD-WAN Firewall Protection Profile

DDoS analytics: Visibility and reporting

To complement its Adaptive DDoS functionality, HPE Aruba Networking secure SD-WAN includes comprehensive DDoS analytics. These reports provide valuable insights into the network's performance and security posture, allowing administrators to track and respond to potential threats in real time (Figure 3).

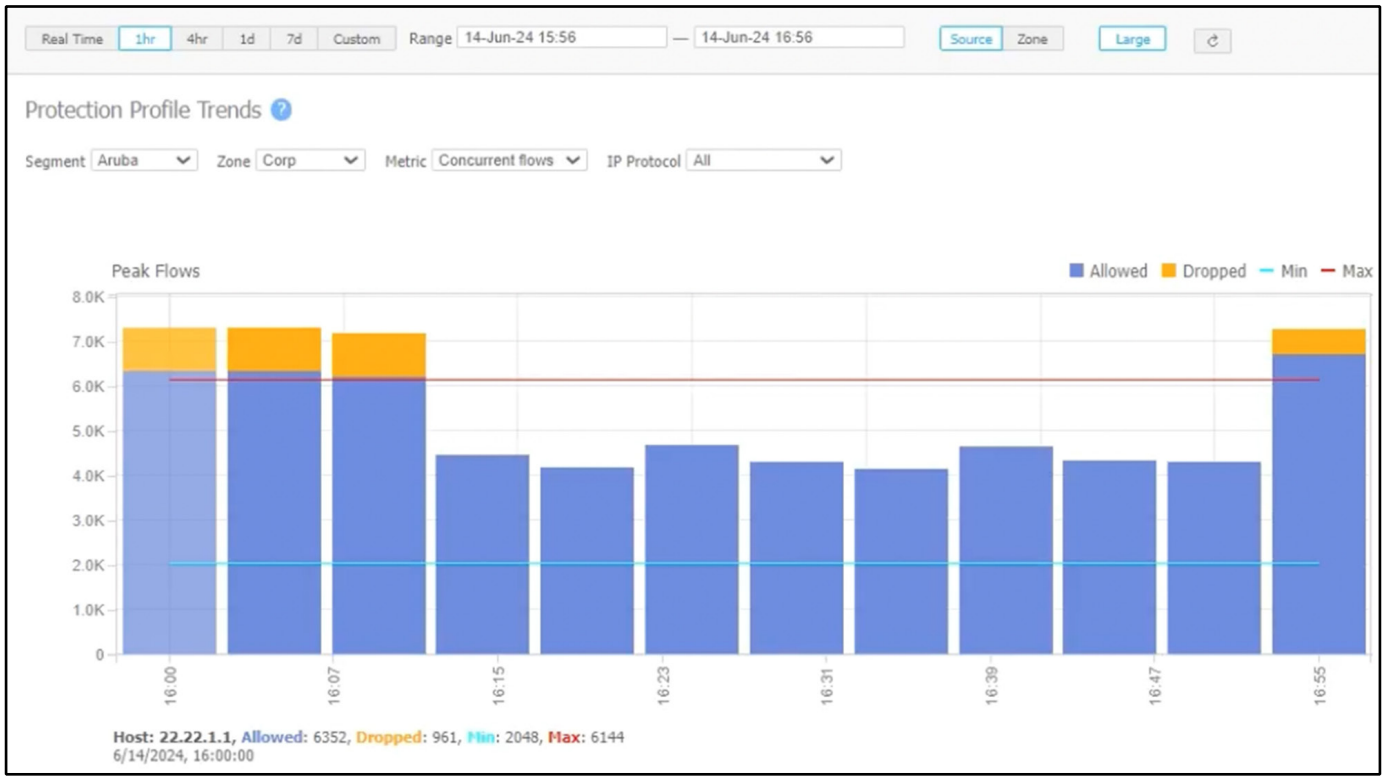

Figure 3. Number of flows allowed and dropped for each five-minute time interval per firewall zone in HPE Aruba Networking EdgeConnect SD-WAN

Key reports include:

- **Threshold violations:** Alerts administrators when traffic exceeds preset or dynamically configured thresholds
- **Flow drops:** Provides details on dropped flows, helping administrators identify and address potential attack sources
- **Denied hosts and packets:** Tracks IP addresses and packets that were blocked due to known malicious behavior
- **Top talkers:** Identifies the devices or users generating the most traffic, helping pinpoint potential sources of abnormal traffic
- **Alarm notifications:** Automatically alerts administrators when thresholds are exceeded, enabling timely response to DoS attacks

This granular visibility into traffic patterns and security incidents allows network teams to make informed decisions, enhancing the overall effectiveness of the DDoS protection strategy.

Complement DDoS defense with ZTNA

By adding ZTNA, part of HPE Aruba Networking SASE, organizations can deliver a multilayered defense against DDoS attacks. ZTNA's ability to hide services from the internet, segment application traffic, and limit access to only verified users and devices significantly strengthens the overall DDoS protection strategy (Figure 4). When combined with Adaptive DDoS protection from HPE Aruba Networking EdgeConnect SD-WAN, organizations get a comprehensive solution to safeguard their networks from DDoS attacks.

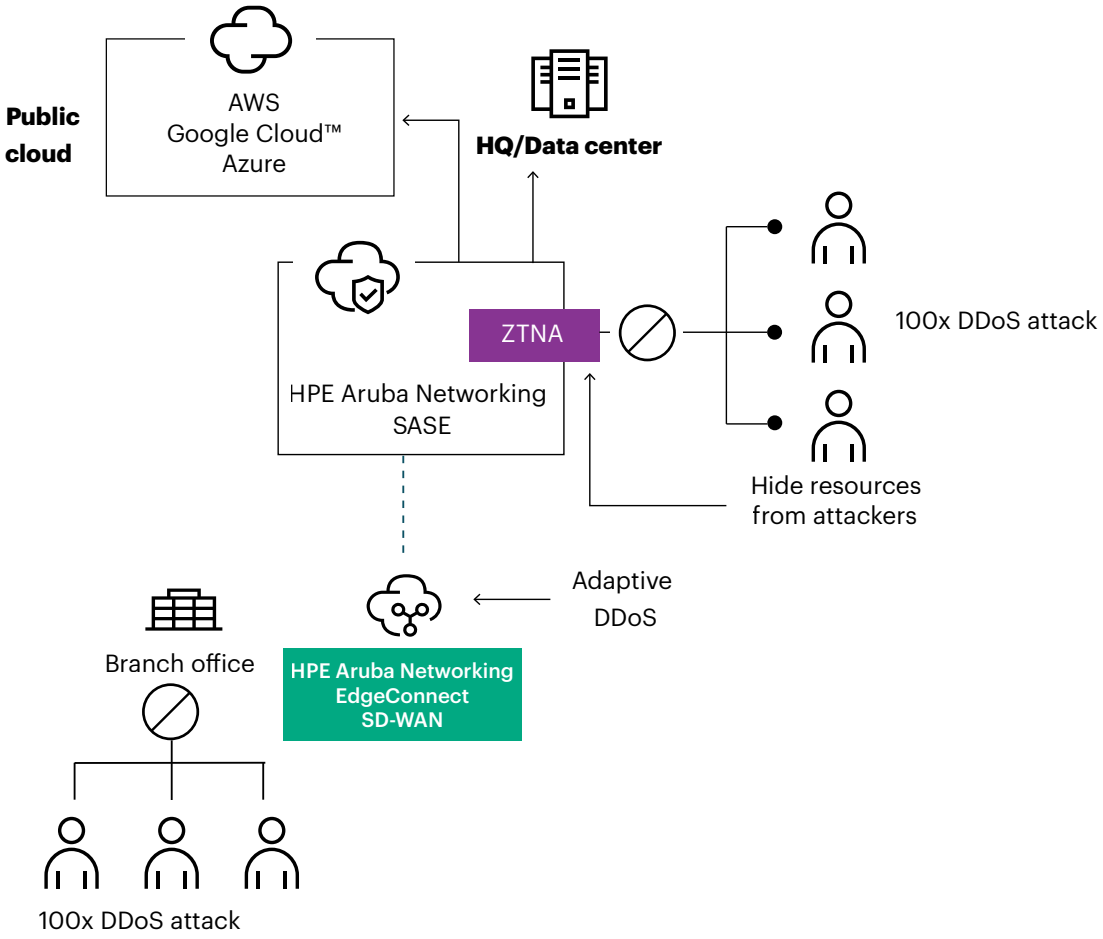

Figure 4. Two-layer DDoS protection using HPE Aruba Networking EdgeConnect SD-WAN Adaptive DDoS paired with HPE Aruba Networking ZTNA

HPE Aruba Networking ZTNA operates on the principle of never trust, always verify. By keeping internal services hidden from the internet, it helps eliminate the common entry points for DDoS attacks. Only authenticated and authorized devices can access specific services, helping ensure that external attackers cannot target these services directly for DDoS exploitation.

Additionally, ZTNA doesn't allow lateral movement. Since ZTNA enforces strict access control policies, users cannot move sideways to other resources. Each connection is formed uniquely, connecting authorized users only to authorized resources. This reduces the overall attack surface, helping ensure that even if one device is compromised, the impact is contained and does not spread to the rest of the network.

Also, unlike VPNs, ZTNA doesn't grant broad access to internal resources. This makes ZTNA an appealing alternative for organizations looking to replace VPNs, which can act as beacons for bad actors by exposing a wide range of network resources.

By continuously verifying user and device identity before granting access, HPE Aruba Networking ZTNA helps ensure that only legitimate traffic can flow to the authorized application while keeping users off the corporate network. This reduces the chances of malicious traffic overwhelming network resources, further mitigating the risks of DDoS attacks. ZTNA effectively narrows the number of devices and services that can be targeted, making large-scale attacks less feasible.

ZTNA's dynamic context-based policies allow network and security administrators to specify different access levels based on user roles, device posture, and location. This granular control further safeguards the network by helping ensure that only authenticated and trusted traffic can interact with critical resources, reducing the risk of malicious traffic slipping through and consuming bandwidth during DDoS attempts (Figure 5).

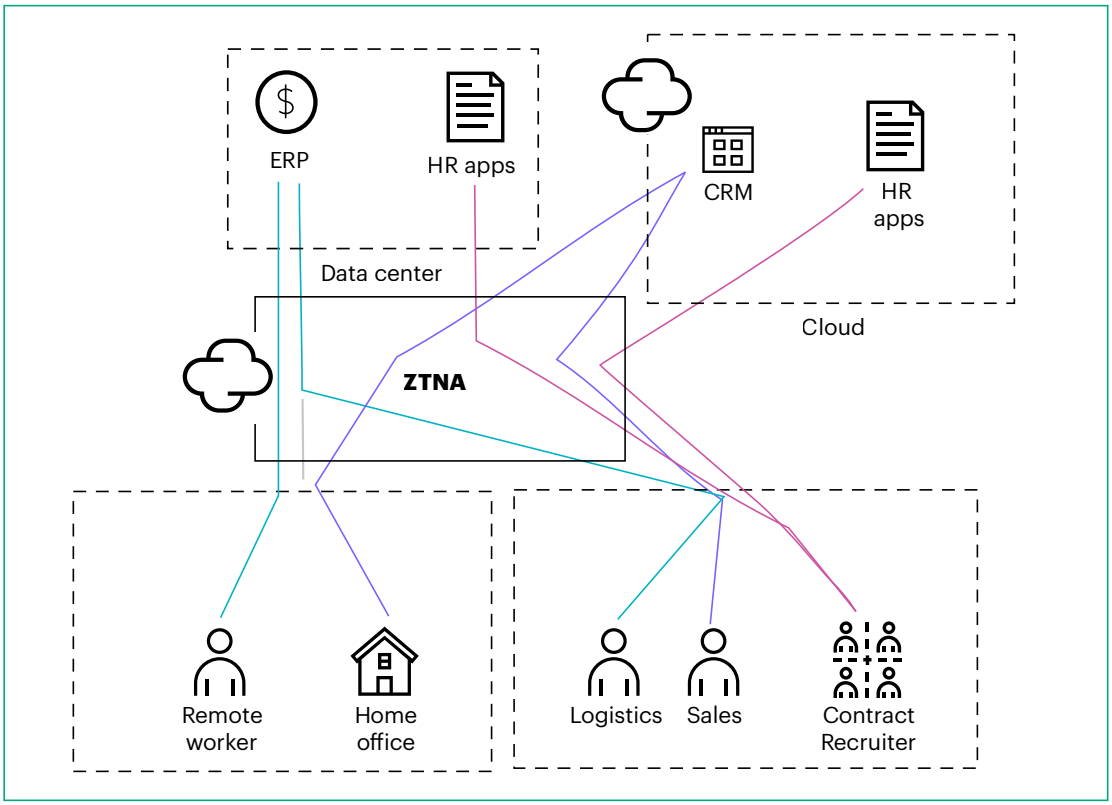

Figure 5. Strict access policy enforcement with ZTNA

HPE Aruba Networking ZTNA supports both remote and on-premises users with the local edge capability, which helps ensure that on-prem traffic remains local, helping eliminate hairpin routing to the cloud. With local edge, ZTNA enforces the same access control policies for on-premises users as it does for remote users, allowing organizations to maintain a single, unified policy across all users. This approach helps minimize complexity and reduces potential security gaps that often arise from managing separate policies for different user types, streamlining security while providing consistent protection.

Comprehensive network security beyond DDoS

While Adaptive DDoS provides dynamic and automated protection against DDoS attacks, HPE Aruba Networking SASE offers a holistic security framework that includes other critical features.

For example, HPE Aruba Networking EdgeConnect SD-WAN's built-in next-generation firewall provides end-to-end network segmentation spanning the LAN, WAN, and even into the cloud. Security policies are defined on a zone-by-zone basis, limiting connectivity with other zones according to predefined security policies. HPE Aruba Networking EdgeConnect SD-WAN also integrates with HPE Aruba Networking ClearPass to provide user and device identity and role-based context, for fine-grained segmentation, helping ensure that users and devices, including IoT, only reach destinations consistent with their role on the network.

HPE Aruba Networking EdgeConnect SD-WAN includes a rule-based IDS/IPS designed to monitor network traffic and identify known attack patterns. This signature-based system can be configured to operate in either in-line mode for greater security or out-of-band mode to prioritize performance. When combined with DDoS protection, IDS/IPS ensures that the network remains secure against a broad range of threats, not just DDoS attacks.

Furthermore, the integration with Splunk offers a comprehensive dashboard for viewing IDS/IPS events, allowing administrators to filter, sort, and analyze security event data efficiently (Figure 6).

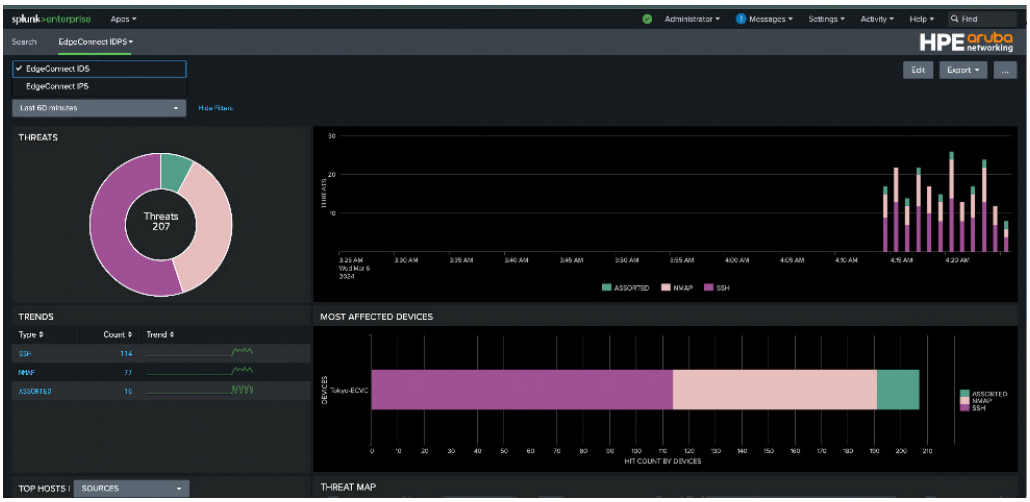

Figure 6. A view of IDS/IPS events in Splunk stemming from HPE Aruba Networking EdgeConnect SD-WAN

Organizations can strengthen their security posture by adding other security service edge (SSE) features such as HPE Aruba Networking Secure Web Gateway (SWG) and cloud access security broker (CASB) to build a single-vendor SASE solution (Figure 7).

SWG is a security solution that protects users from web-based threats by monitoring and filtering internet traffic in real time. It enforces security policies to block access to malicious websites, prevents malware downloads, and filters inappropriate or harmful content. Additionally, HPE Aruba Networking EdgeConnect SD-WAN integrates with our SWG to protect all network devices, including unmanaged devices (for example, guests and IoT devices), without the need for individual agents on each device. This feature is particularly useful for organizations with large numbers of IoT devices, which may not support traditional security agents but still need protection from web-based threats.

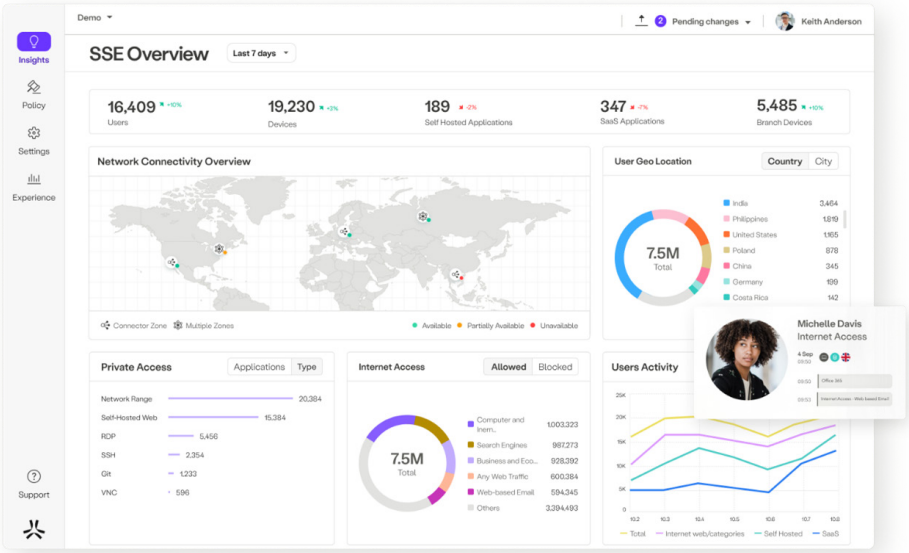

Figure 7. A view of HPE Aruba Networking SSE dashboard to monitor access to private apps, SaaS, and internet

CASB acts as a control point between cloud service users and SaaS applications, helping ensure the secure use of cloud-based resources. CASB provides visibility into cloud usage across an organization, enforces security policies, and protects sensitive data by monitoring access and behavior in cloud applications. CASB helps prevent data leaks by applying encryption, data loss prevention (DLP), and access controls. By offering granular controls over how users interact with cloud services, CASB helps secure sensitive data and ensure compliance with regulatory requirements while enabling safe cloud adoption.

Conclusion

HPE Aruba Networking EdgeConnect SD-WAN, enhanced with Adaptive DDoS protection and HPE Aruba Networking ZTNA, delivers a robust, multilayered defense against DDoS attacks. Adaptive DDoS protection leverages machine learning to dynamically adjust thresholds, preventing disruptions while helping ensure legitimate traffic flows smoothly. ZTNA reduces the attack surface by enforcing strict access controls and preventing unauthorized exposure of network resources. Additionally, organizations can further strengthen their security posture by integrating SWG and CASB, forming a complete SASE architecture. SWG provides protection against web-based threats while CASB secures cloud access, together delivering comprehensive coverage across all entry points and helping ensure a resilient, secure network environment against DDoS and other cyber threats. (Figure 8).

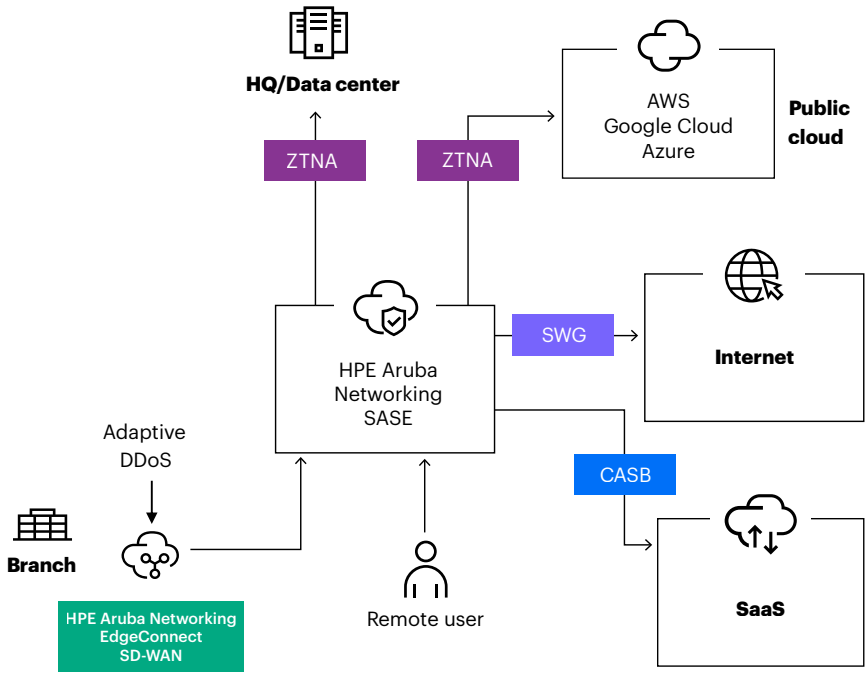

Figure 8. Enhanced DDoS protection and secure access to private apps, SaaS, and internet with HPE Aruba Networking SASE

Learn more at

HPE Aruba Networking SD-WAN

HPE Aruba Networking SSE

HPE Aruba Networking SASE

Visit HPE.com

Chat now

a50011705ENW, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com