SASE Quick Start Guide: EdgeConnect SD-WAN Advanced Security & Secure Web Gateway

Contents

Overview

This document is designed to help SD-WAN customers begin their SASE (Secure Access Secure Edge) journey with two powerful new security features that are now part of the SD-WAN standard bandwidth subscription (Tiered Licensing – Foundation or Advanced):

Advanced Security: A suite of threat detection and mitigation tools, including IDS/IPS, Dynamic DDOS protection, and Secure Web Service filtering.

Secure Web Gateway: The Secure Web Gateway license enables IPsec tunnel connectivity to HPE SSE cloud edge points, providing advanced web filtering, data loss prevention, and malware scanning.

This guide introduces these new features, illustrating their application in real-world scenarios. It also includes sample configuration instructions to help you quickly set up and operationalize the capabilities in your environment.

Feature Introduction

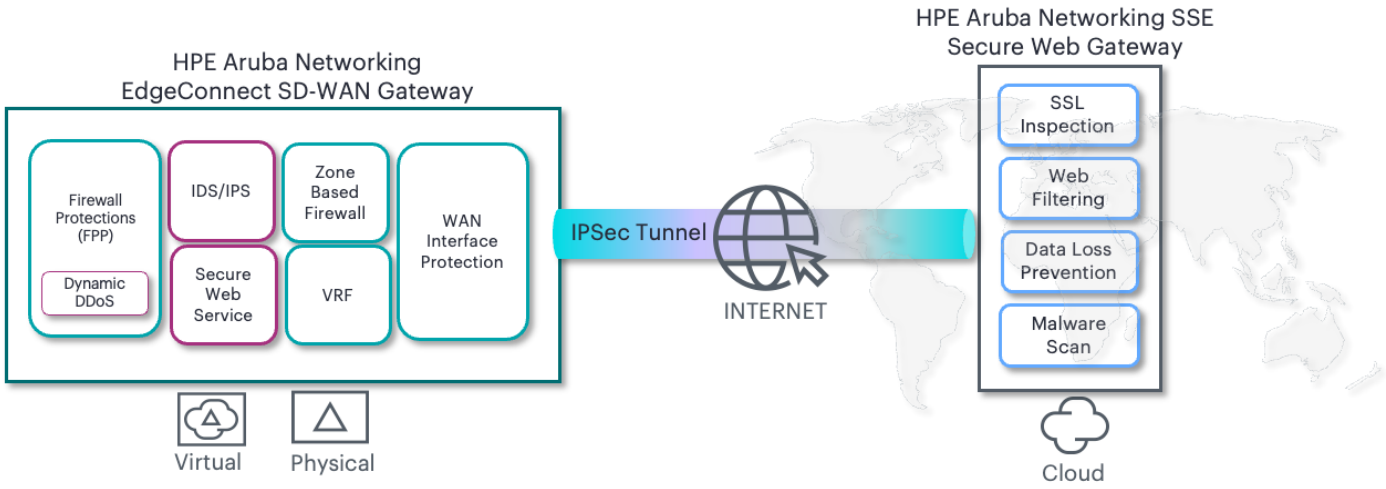


Figure 1 - HPE Aruba Networking SASE - SD-WAN Gateway Security with Cloud-Native SSE Protection

Advanced Security (Dynamic Threat Defense)

Dynamic Threat Defense (DTD) strengthens your EdgeConnect SD-WAN deployment by delivering advanced security directly at the branch gateway. It extends next-generation firewall functions to the WAN edge, providing stronger protection and smarter traffic handling.

The standard SD-WAN subscription ***already includes core firewall capabilities such as***:

- **Zone-based firewall:** Enforces security policies between network zones for granular traffic control. Policies can also be applied based on user or device identity, derived from RADIUS authentication or identity discovery.
- **Firewall Protections (FPP):** Strengthens baseline security with Standard threshold-based DDoS protections, stateful TCP inspection, reverse path forwarding, and limited DPI enforcement.
- **WAN interface protection** – Ensures the WAN edge is secured and blocks any unsolicited connections.
- **Route segmentation (VRF):** Isolates traffic into virtual routing instances to separate and secure network segments.

In addition, features that previously required an Advanced Security license are now included as part of your standard SD-WAN subscription:

- **Secure Web Service** – Filters traffic based on web categories, reputation, and URL intelligence using dynamic threat feeds.
- **IDS/IPS** – Continuously inspects traffic against dynamic signature sets to detect and block known threats.
- **Adaptive DDoS Protection** – Monitors traffic baselines to mitigate denial-of-service attacks, with *Smart Burst* automatically adjusting thresholds to allow legitimate traffic spikes.

Secure Web Gateway

Secure Web Gateway extends security beyond the branch by leveraging the HPE SSE cloud platform. With a Secure Web Gateway Bandwidth License, each EdgeConnect gateway can establish an IPsec tunnel to the HPE SSE cloud edges, redirecting branch traffic for advanced inspection and filtering.

Encrypted traffic analysis **(SSL Inspection)** plays a critical role in this process. By securely decrypting, inspecting, and re-encrypting HTTPS traffic, the SWG provides deep visibility into encrypted threats and ensures that security policies are consistently enforced, even on encrypted web sessions.

Key features of the HPE SSE Secure Web Gateway:

- **SSL Inspection:** Performs decryption and inspection of HTTPS traffic to identify concealed risks.
- **Web Filtering:** Category-based web filtering, Granular URL and sub-URL filtering.
- **DLP:** Data Loss Prevention (DLP) for uploads/downloads.
- **Scanning**: Inspects web traffic and files for hidden threats. Sandboxing is available with an add-on subscription.

Use Cases for Advanced Security on EdgeConnect Gateway

To implement the use cases described in this guide, you first need to enable the Advanced Security license (also known as the Dynamic Threat Detection license), which is now included with the SD-WAN Bandwidth Subscription (AAS). Refer to Appendix A on how to apply the license to your EdgeConnect gateway.

Filtering Guest Web Traffic Based on Web Categories, Reputation

Visitors on a branch guest Wi-Fi try to access gambling or restricted websites. Secure Web Service applies web filtering directly at the gateway, blocking gambling, restricted, and high-risk categories while still allowing safe browsing for guests.

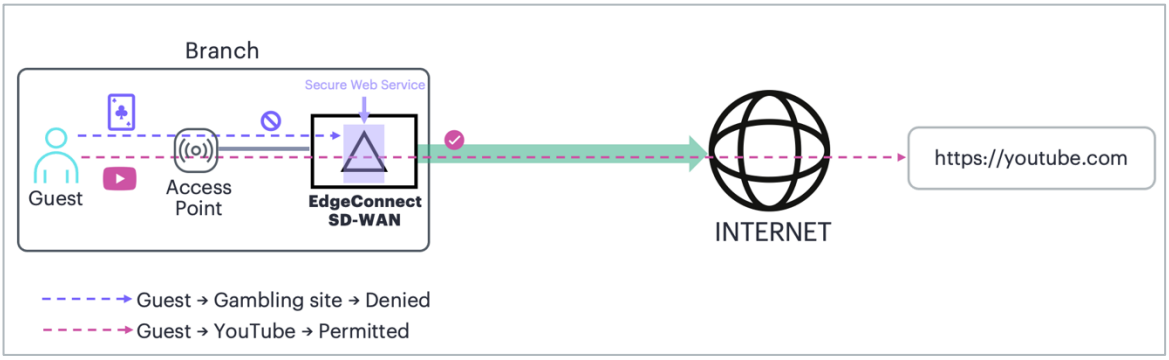


Figure 2 - Secure Web Services in Guest internet traffic drain

The Secure Web Service feature is available starting with the ECOS 9.6.0 release. To access this capability, upgrade your EdgeConnect gateway to version 9.6 and follow the instructions in **Appendix A** and **Appendix B**. If an upgrade to ECOS 9.6 is not feasible, you can achieve a similar level of web filtering by following the instructions for configuring a **Secure Web Gateway (SWG)** below.

Follow these steps to configure a Secure Web Service policy on your EdgeConnect gateway:

- Navigate to **Configuration > Security > Firewall Zone Matrix**.
- Select the intersection between your **Source Zone** and **Destination Zone**.
- In this example, Guest users are segmented using interface Labels. Depending on your design, you can segment in different ways. For example, you can use **LABELS** to distinguish Guest users from Corporate users and use Labels as matching criteria.
- The example below illustrates a policy construct that uses a matching Interface Label for “Guest” and subjects user traffic to the Secure Web Service policy.

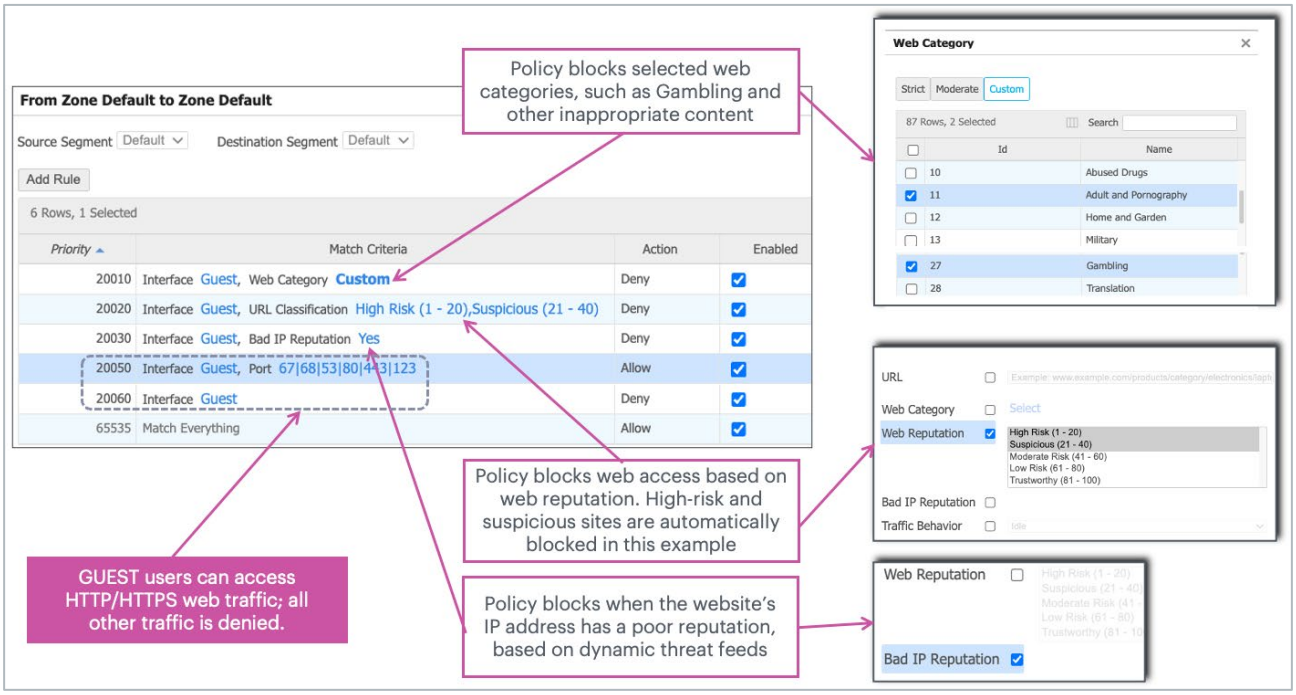


Figure 3 - Security policy to block guest web traffic based on category and reputation

Example of flows dropped at the EdgeConnect gateway due to Web Policy settings (**Monitoring > Bandwidth > Flows > Active & Recent Flows >** *filter for specific user IP address to view the flow details*):

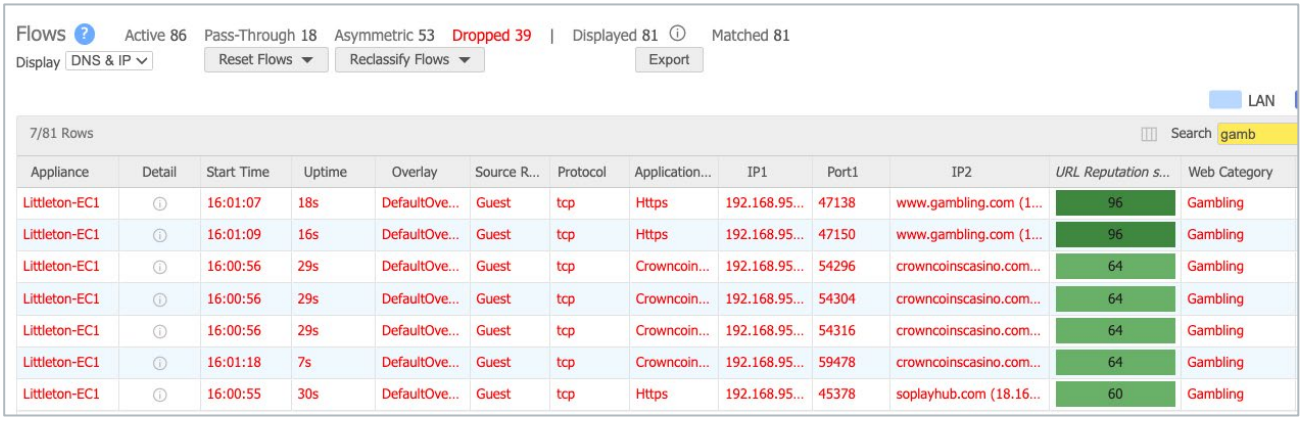


Figure 4 - Flows Blocked Due to Gambling Web Access

Blocking Known Exploit Attempts

An employee at the branch clicks a malicious link. IDS/IPS recognizes the traffic as a known threat and blocks the connection before it leaves the branch network, while permitting traffic to internal apps and other internet traffic post inspection.

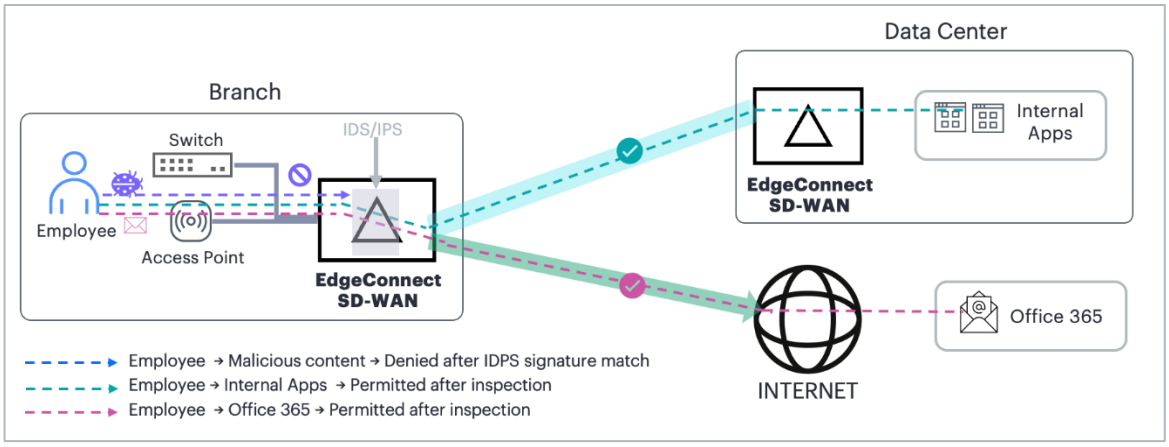


Figure 5 – Enforcing IDS/IPS on employee traffic to block malicious attempts

Follow these steps to configure IDS/IPS inspection on your EdgeConnect gateway:

- Enable IDS/IPS on EdgeConnect gateways by selecting one or all appliances from the Appliances tree and navigating to **Configuration > Overlays & Security > Security > IDS/IPS > Apply IDS/IPS on Appliances**

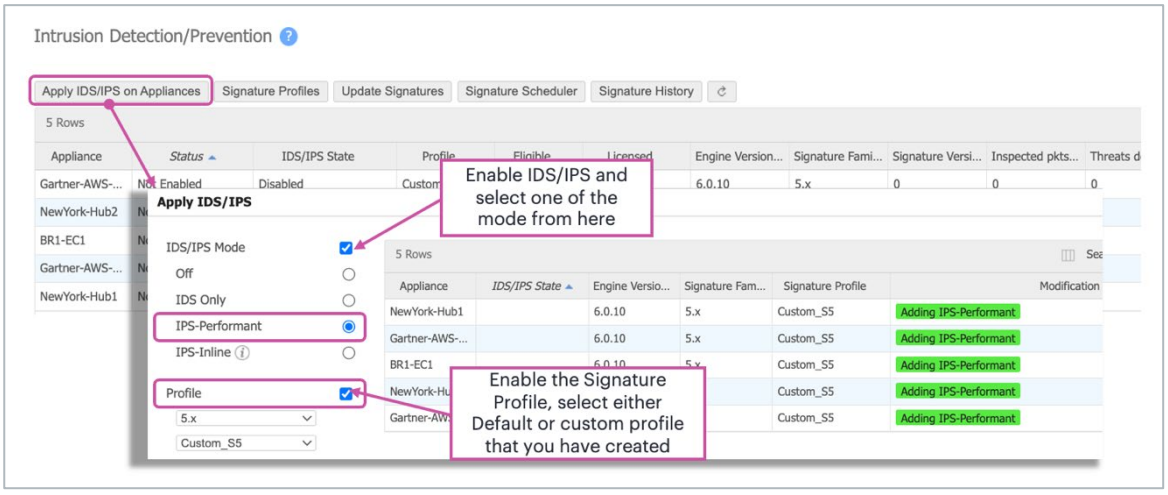


Figure 6 - Enabling IDS/IPS on the EdgeConnect SD-WAN gateway

The example above uses the “IPS-Performant” mode, which is less CPU-intensive and has minimal impact on SD-WAN performance compared to the pure “IPS-Inline” mode. Depending on your security requirements, you can select the appropriate mode. Alternatively, choosing the “IDS Only” mode does not block intrusion attempts; instead, it allows administrators to monitor traffic and receive alerts if suspicious activity is detected.

- After applying IDS/IPS to the EdgeConnect gateways, you can inspect traffic by configuring a security policy. The policy action “**Inspect**” can be applied to all traffic or selectively, based on your requirements.
- Go to **Configuration > Overlays & Security > Security > Firewall Zone Matrix**. Select the relevant zone intersection, then either add a new policy or edit an existing one to apply inspection.
- The example below shows a Default Zone-to-Default Zone policy configuration. It applies the Inspect action to subject all traffic to IDS/IPS inspection.

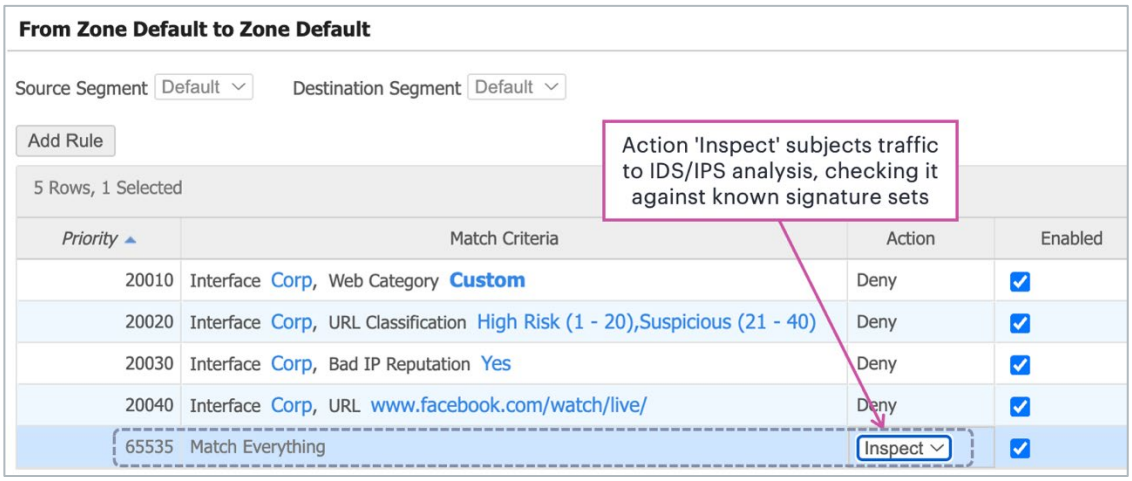


Figure 7 - Firewall Policy subjecting traffic to IDS/IPS inspection

- View IDS/IPS traffic in Orchestrator under **Configuration > Overlays & Security > Security > IDS/IPS**. Monitor **Inspected pkts/sec**, **Threats Detected**, **IPS Flow Drops**, and **Events**. Click the graph icon to see stats trends.

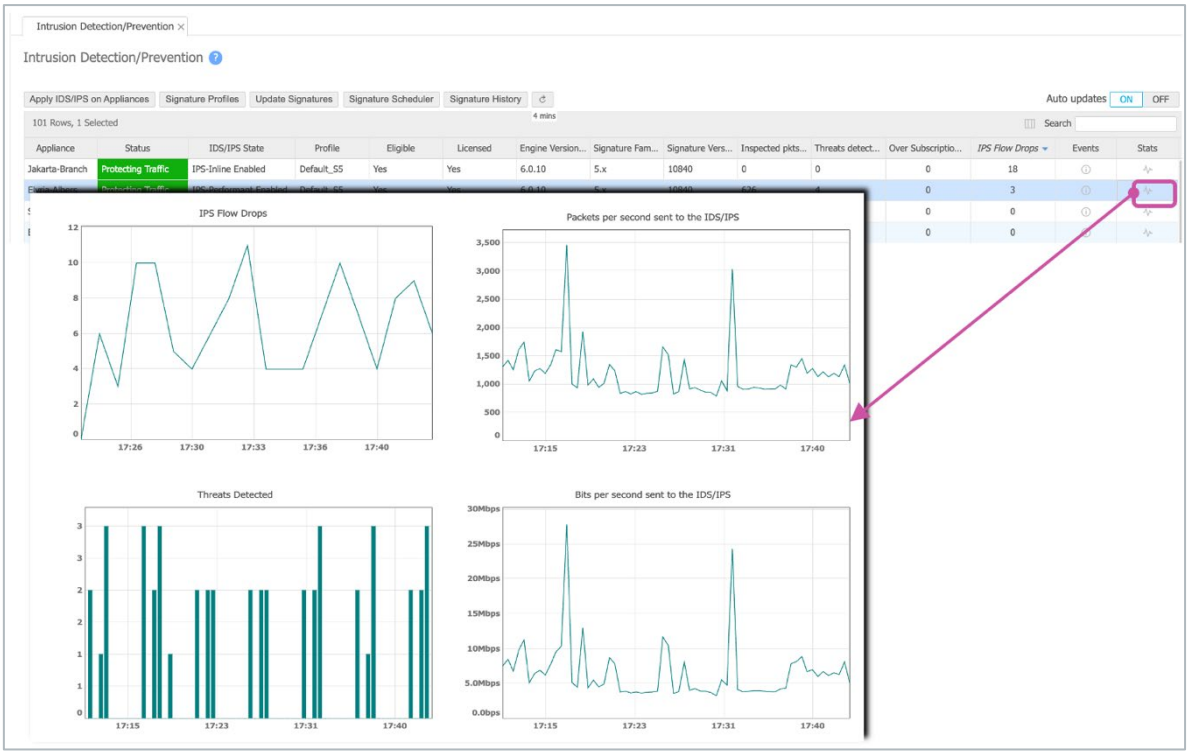


Figure 8 - IDS/IPS inspection trends charts

Stopping Outbound Traffic Floods

A compromised device in the branch begins generating excessive outbound traffic, overwhelming the WAN link and slowing down critical business applications. Dynamic DoS detects abnormal traffic spikes, blocks malicious floods, and uses Smart Burst to ensure that legitimate traffic, such as backups or software updates, continues without interruption.

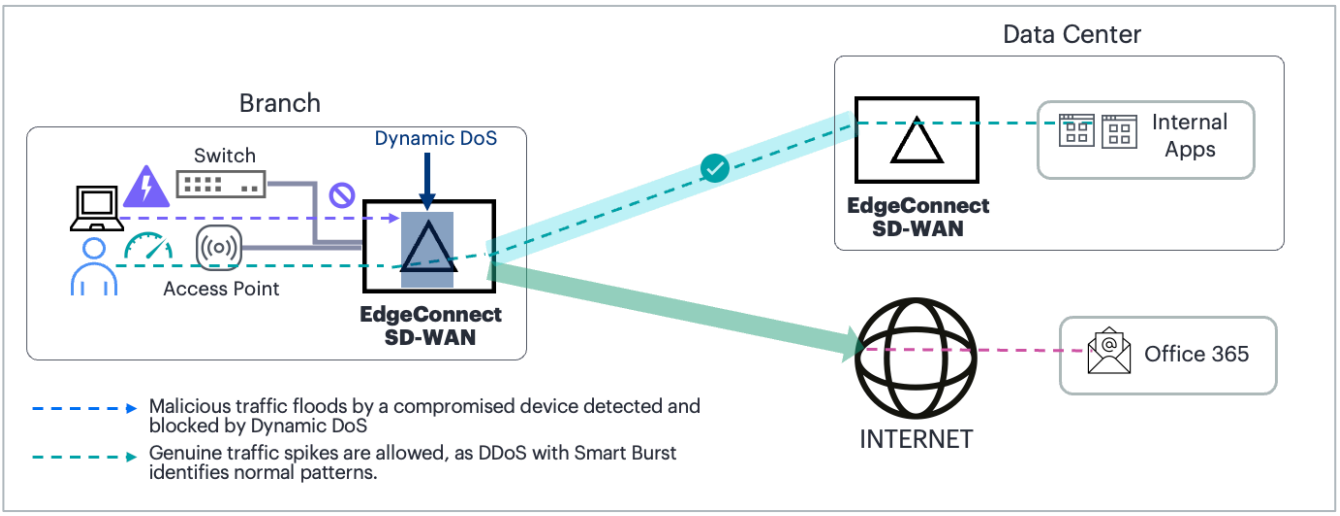


Figure 9 - Preventing volumetric attacks using Dynamic DDoS

Firewall Protection Profile that controls DDoS function and other firewall functions on the EdgeConnect gateway. Follow the steps below to configure the Dynamic DDoS to prevent volumetric DoS attacks in your network:

- In Orchestrator, go to **Configuration > Templates and Policies > Templates**.
- Either use an existing Template Group or create a new one. (In this example, an existing Template Group is used.)
- Drag **Firewall Protection Profile** from *Available Templates* into *Active Templates*.
- Enable the Baseline Learning (default settings use 14 14-day training model to understand the network pattern, you can edit the settings to suit your requirement by clicking on **Baseline Settings**)

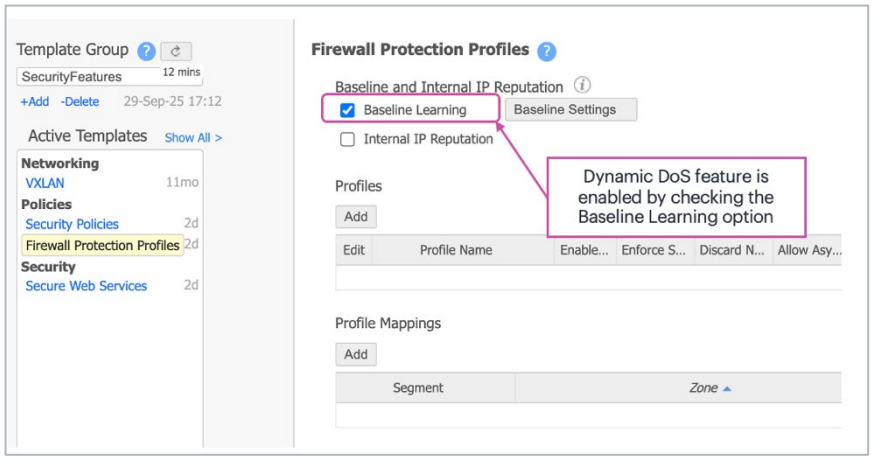


Figure 10 - Enabling Firewall Protection Profiles - Baseline Learning

- Click on ***Add*** under the Profiles section to create a new FPP and define DoS thresholds that control volumetric attacks by setting limits for concurrent flows, embryonic flows, and flows per second.

- Configure the Firewall Protection Profile by enabling Security Settings and DoS Thresholds. In this example, a new profile is created with default security settings and Smart Burst DoS thresholds applied.

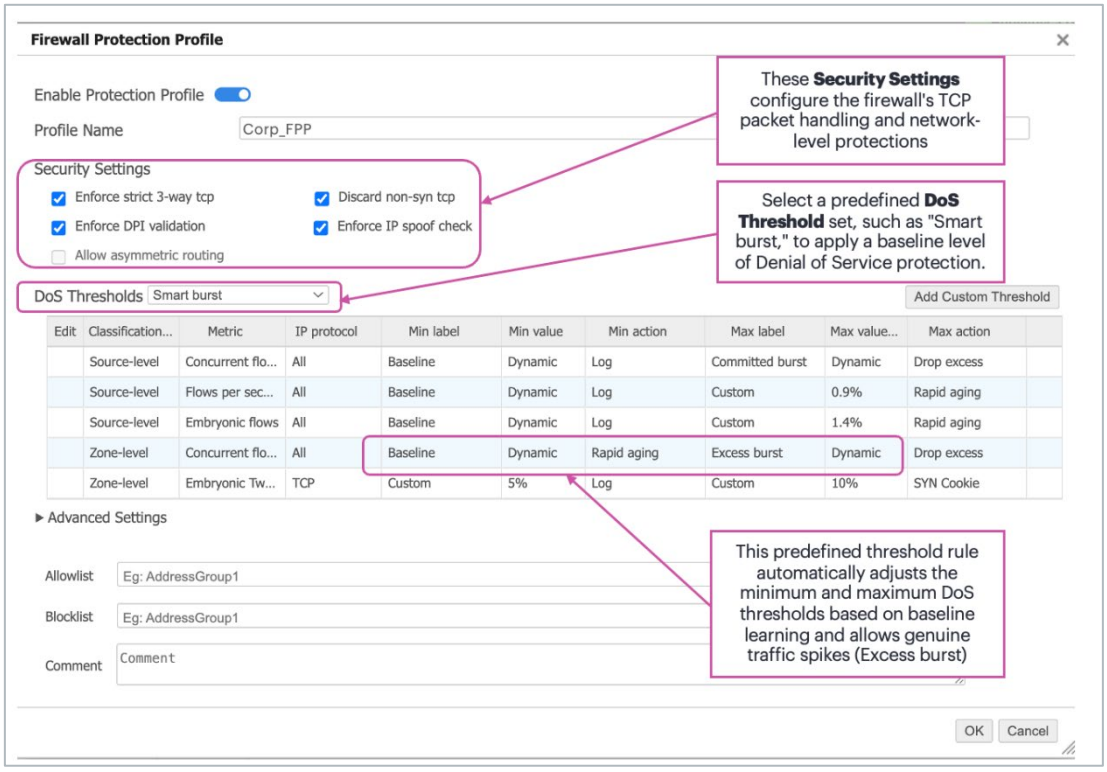


Figure 11 - Firewall Protection Profile Security Settings and DoS Threshold Rules

Predefined thresholds are a good starting point, but you may need to fine-tune them for your network. Custom Threshold Settings enable you to select between classification options (Source-Level or Zone-Level), metrics (Flows/sec, Concurrent, or Embryonic), and IP protocols (TCP, UDP, ICMP, Others, or All). This flexibility allows you to build tailored DoS protection that best fits your environment. You can add a Custom Threshold by clicking on the "**Add Custom Threshold**" option on the FPP.

- Click **OK**
- Click **Add** under **Profile Mappings**
- Select "Segment" and "Zone" from the respective columns and map it to a Firewall Protection Profile that you have created.
- In this example, the newly created "Corp_FPP" is mapped to the Default Segment/Default Zone.

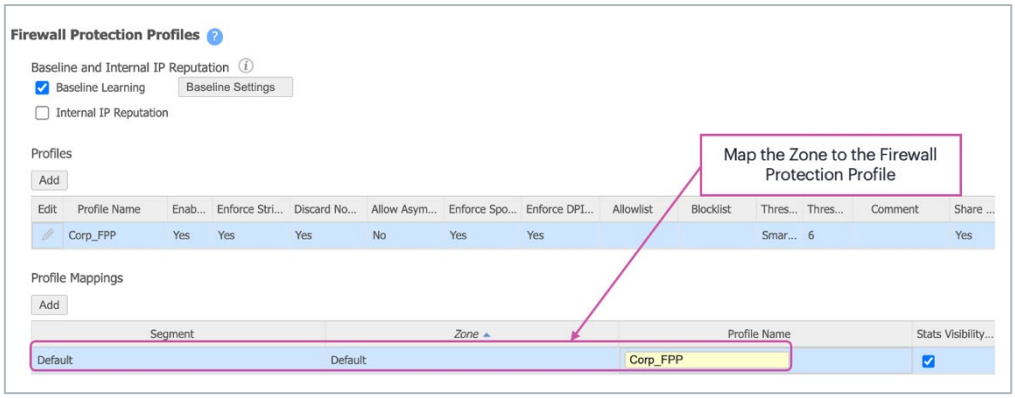


Figure 12 - Profile Mapping to the Zone

- Once the mapping is completed, click on **Save** and **Save Templates Changes**

- Once saved, apply the Template Group to your gateway using **Configuration > Templates and Policies > Apply Template Groups** for the FPP to take effect.

Orchestrator provides visibility into the effectiveness of DDoS through various graphs and charts on the Orchestrator (**Monitoring >Security > Protection Profile Top Talkers, Protection Profile Trends, Flow Baselines, and Flow Baseline Trends**)

- Below is one such chart from the **Monitoring > Security > Protection Profile Top Talkers** showing the violation count based on the thresholds

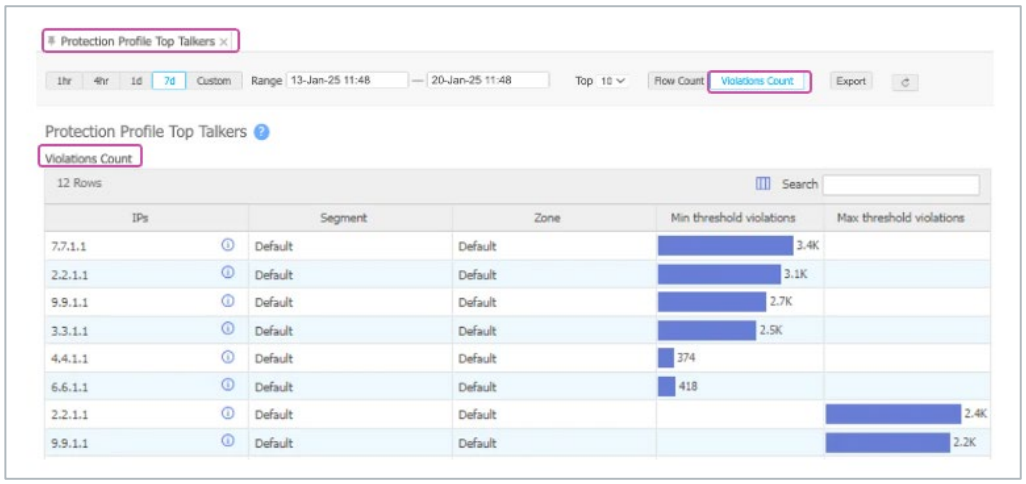


Figure 13 - Denial of Service - Violations Count

Use Cases for Secure Web Gateway on HPE SSE

While the local EdgeConnect SD-WAN gateway provides essential protections such as web filtering, IDS/IPS, and DoS prevention, some advanced security functions require SSL decryption and deeper inspection that cannot be performed locally at the branch. This is where a cloud-based Secure Web Gateway (SWG) becomes valuable.

To enable this, EdgeConnect establishes secure tunnels to the nearest HPE SSE cloud edges. Orchestrator simplifies this process by orchestrating the tunnels to the closest cloud edges and allowing you to redirect selected internet-bound traffic to the SWG for deeper inspection.

You must complete prerequisites, including understanding the SWG bandwidth license, setting up tunnel connectivity between EdgeConnect and the nearest HPE SSE cloud edges, and redirecting branch internet traffic to the HPE SSE secure web gateway. Details are in **Appendix C**.

Controlling Web Access Without SSL Inspection

Guest users at a branch location should access the internet safely through the Secure Web Gateway, utilizing category and reputation-based filtering. In this example, access to high-risk sites, such as gaming and gambling websites, or those with low reputations, is blocked, while general browsing remains allowed.

This policy provides secure internet access for guests **without requiring SSL inspection** or certificate installation on their devices.

NOTE: If your deployment is running **ECOS 9.6 or later**, this use case can be implemented directly on the EdgeConnect gateway using the **Secure Web Service** feature. Suppose your deployment is on an earlier ECOS version that does not support this feature. In that case, it is recommended to use the **HPE SSE Secure Web Gateway** to achieve similar category and reputation-based web filtering results.

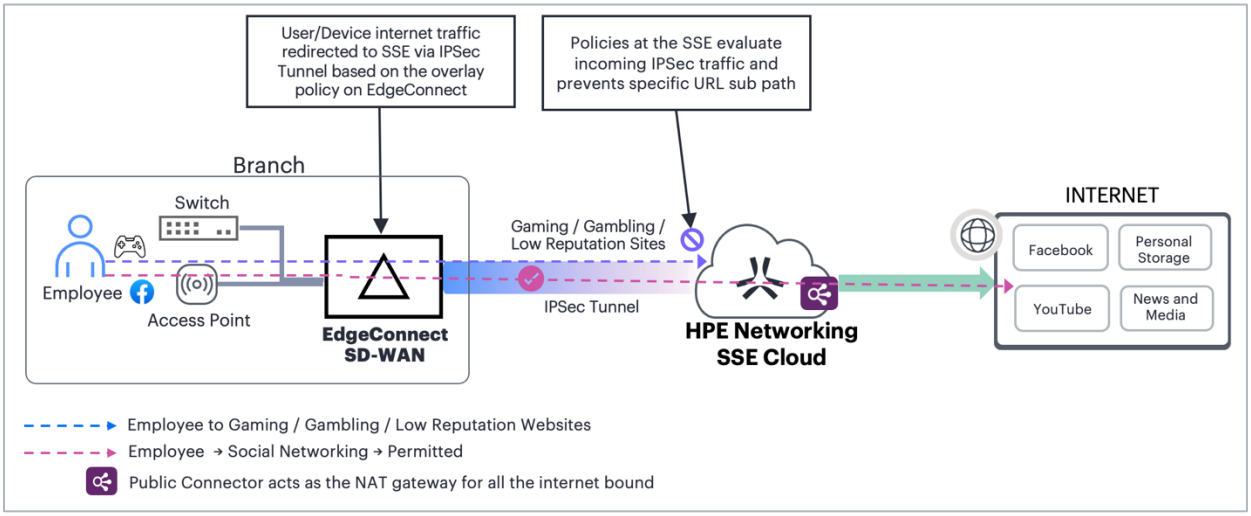


Figure 14 - Categories and Reputation based web filtering without SSL inspection

Creating a web profile and enabling Threat Intelligence Protection is a prerequisite to ensure websites with bad reputations are blocked.

Web Profile: Create or modify a Web Profile and enable Threat Intelligence Protection

- Navigate to **Policy > Profiles > External Web**.
- Create a new profile or edit an existing one (e.g., *Default Web Profile*).
- Check **Enable Threat Intelligence Protection**.
- Click **Submit** and **Apply changes to** save the profile.

Web Policy: Create a web policy that blocks access to categories such as Gaming, Gambling, and other restricted sites, while allowing access to general web browsing:

- Navigate to **Policy > Rules**.
- Add a new rule or modify an existing one (in this example, a new rule is created, **Guest - Restricted Categories**).
- Sample policy:
  - Set **Identity** to **Any**.
  - To apply the policy only to a specific branch location, set **Source** to **Locations** and select the branch from the list. *(This location is automatically created during tunnel orchestration in the Orchestrator.)*
  - Set **Destination** to Gambling, Games, and select desired restricted categories from the list.
  - Leave the other conditions as **Any**.
  - Set the **Action** to **Block**.
  - Under **Profiles**, select the appropriate **Web Profile** that has Threat Intelligence Protection enabled.
- Create another rule that allows all web traffic, since the previous rule already blocks restricted categories. If preferred, you can further limit access by allowing only specific categories. In this use case, the rule enables general web browsing for guest users.
- Sample policy:
  - Set **Identity** to **Any**.
  - To apply the policy only to a specific branch location, set **Source** to **Locations** and select the branch from the list. *(This location is automatically created during tunnel orchestration in the Orchestrator.)*
  - Leave the other conditions as **Any**.

- Set the **Action** to **Allow**.
- Under **Profiles**, select the appropriate **Web Profile** that has Threat Intelligence Protection enabled.

- Click **Submit** and **Apply Changes** to save the policy.

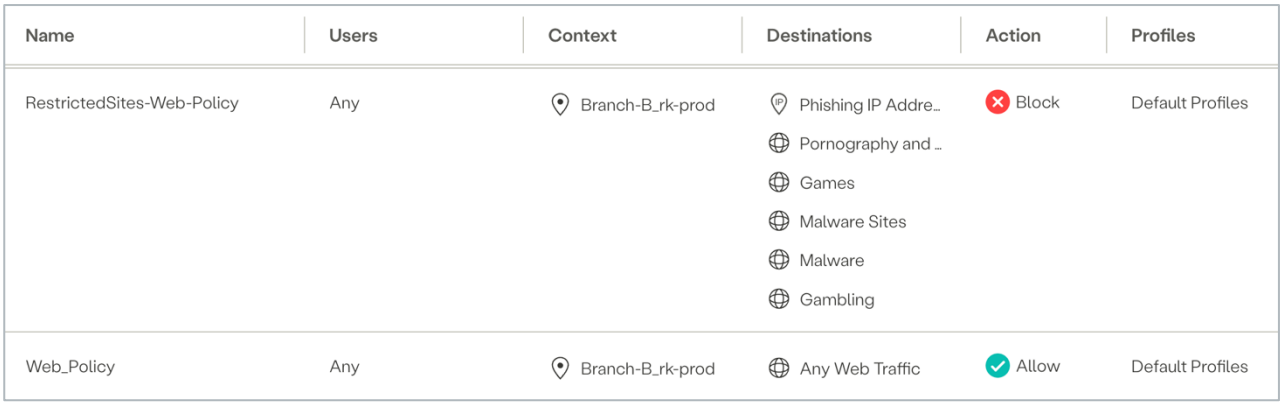


Figure 15 - Sample policy that blocks certain categories and allows general web browsing

To view branch user traffic activity on HPE SSE, navigate to **Insights > Exploration**. Apply filters, such as Integration Type: IPsec, to view all traffic from the EdgeConnect gateway through the IPSec tunnel (as shown in the screenshot below).

The following exploration activity displays blocked branch user traffic when attempting to access a website categorized under “Phishing and Other Frauds.” The block was enforced by the web filtering engine based on the domain’s reputation and category, without requiring SSL inspection.

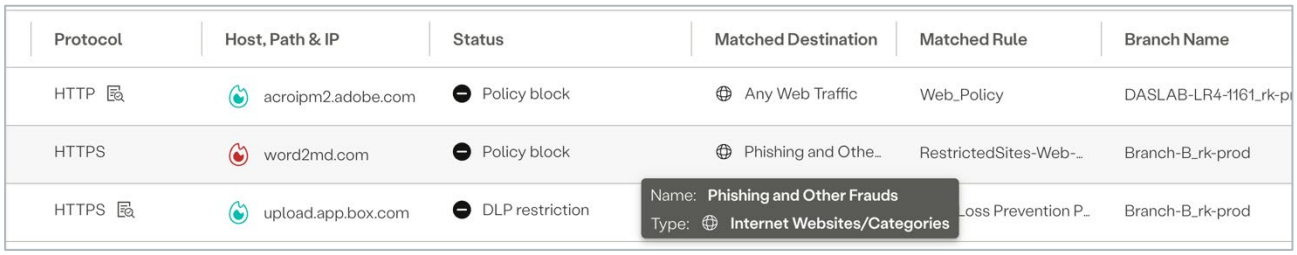


Figure 16 - Insights into user activity showing blocked status when accessing restricted category website

Enforcing Granular Web Access with Advanced Web Filtering

An organization allows access to **Social Networking** sites for marketing and brand engagement, while **blocking high-risk or non-productive subpaths**, such as facebook.com/games or youtube.com/shorts.

- Category: Social Networking → Allowed
- Specific Sub-paths: *facebook.com/games* → **Blocked**

To enforce this distinction, the SWG performs **SSL inspection**, decrypting and analyzing encrypted web traffic to identify specific **URL subpaths** and apply precise controls.

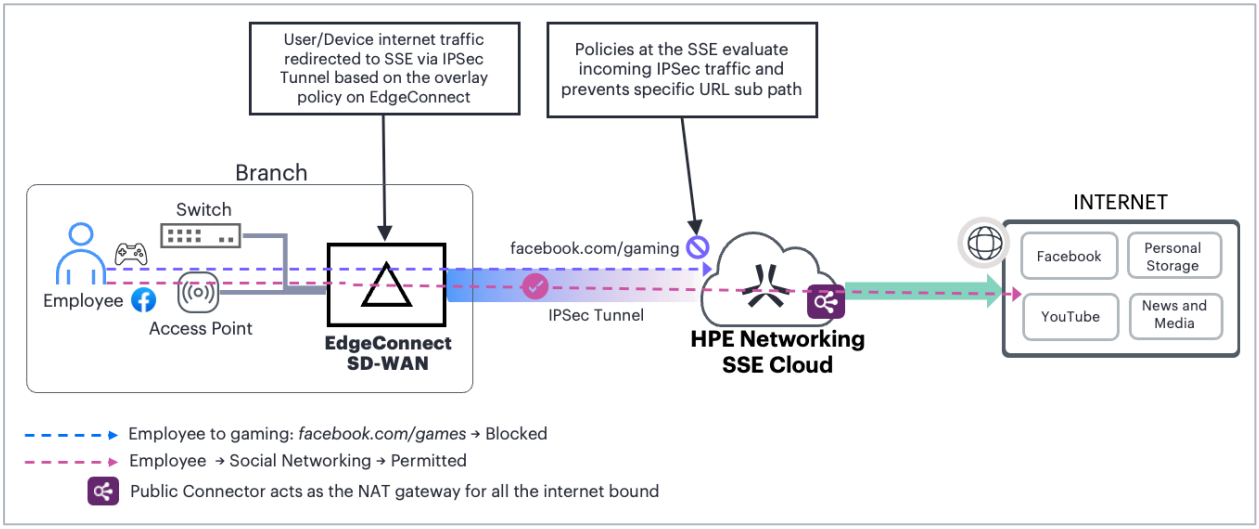


Figure 17 - Granular web control enforcement on SSE Cloud

Granular web access control requires SSL inspection to identify and manage encrypted traffic. Ensure that trusted CA certificates are configured to allow proper SSL decryption. The following procedure outlines how to create a web profile with SSL inspection enabled, configure a custom category to block a specific website sub-path, and upload the necessary CA certificate.

Web Profile: Create or modify a Web Profile and enable SSL inspection:

- Navigate to **Policy > Profiles > External Web**.
- Create a new profile or edit an existing one (e.g., *Default Web Profile*).
- Check **Enable SSL Inspection**.
- Click **Submit** and **Apply changes to** save the profile.

Destination Category: Create or modify a web category to include facebook.com/gaming

- Navigate to **Setting > Destinations > Categories >** *Create a **New Category***.
- Provide a name for this category, e.g: **facebook-gaming**”
- Add **facebook.com/gaming** under the “**include**” section of the category and Submit and Apply Changes to save the changes. This category will be later used in the policy construct to block access.
- Click **Submit** and **Apply changes to** save the category.

Root Certificate: Upload the enterprise CA Root certificate:

- Navigate to **Settings > Configuration > Certificates > CA Certificates**.
- Upload your enterprise CA using the **Upload Certificate** option (pfx format)

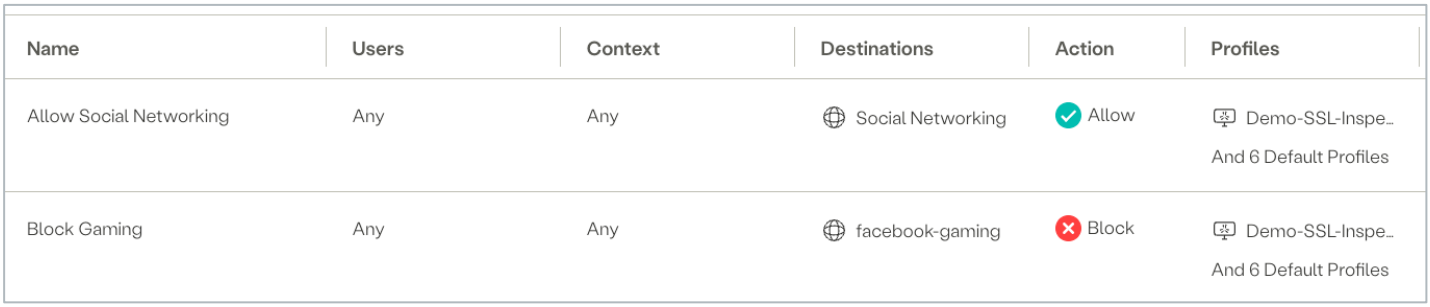
IMPORTANT: In this example, the pre-installed default CA on HPE SSE is used for testing. If you are using the default CA certificate from the HPE SSE management console, you must install the same CA certificate on your test machine for SSL inspection to function correctly.

Web Policy: Create the Web Policy

Finally, create a web policy to block traffic. The **Web Profile** with SSL inspection enabled ensures that SSE can decrypt the packet and extract the full URL, including the subpath.

- Navigate to **Policy > Rules**.
- Add a new rule or modify an existing one (in this example, an existing rule (**Allow Social Networking**) is modified).
- Sample policy:
    - Set **Identity** to **Any**.
    - To apply the policy only to a specific branch location, set **Source** to **Locations** and select the branch from the list. *(This location is automatically created during tunnel orchestration in the Orchestrator.)*
    - Set **Destination** to the newly created category (e.g, **facebook-gaming**)
    - Leave the other conditions as **Any**.
    - Set the **Action** to **Block**.
    - Under **Profiles**, select the appropriate **Web Profile** that has SSL inspection enabled.
- Click **Submit** and **Apply Changes** to save the policy.

The following example illustrates how a policy can permit access to the overall **"Social Networking"** category, including *facebook.com*, while enforcing a more granular rule to block the *facebook.com/gaming* sub-path.

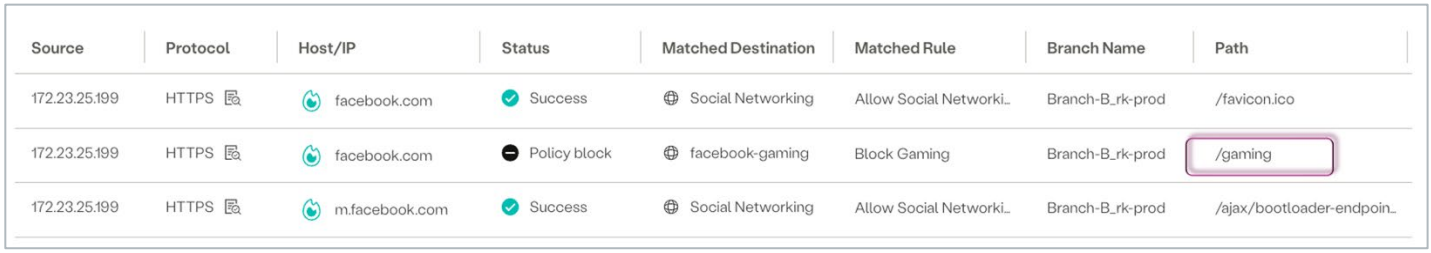


Name	Users	Context	Destinations	Action	Profiles
Allow Social Networking	Any	Any	Social Networking	Allow	Demo-SSL-Inspe… And 6 Default Profiles
Block Gaming	Any	Any	facebook-gaming	Block	Demo-SSL-Inspe… And 6 Default Profiles

Figure 18 - Web policy to block access to sub path of a URL

To view branch user traffic activity on HPE SSE, navigate to **Insights > Exploration**. Apply filters, such as Integration Type: IPsec, to view all traffic from the EdgeConnect gateway through the IPSec tunnel (as shown in the screenshot below).

The following exploration activity shows traffic from a branch user who was allowed to access *facebook.com* but was blocked when attempting to reach the specific sub-path *facebook.com/gaming*. The block was triggered by the web filtering engine during SSL inspection, demonstrating how the SWG enforces granular web access controls based on URL paths.



Source	Protocol	Host/IP	Status	Matched Destination	Matched Rule	Branch Name	Path
172.23.25.199	HTTPS	facebook.com	Success	Social Networking	Allow Social Networki…	Branch-B_rk-prod	/favicon.ico
172.23.25.199	HTTPS	facebook.com	Policy block	facebook-gaming	Block Gaming	Branch-B_rk-prod	/gaming
172.23.25.199	HTTPS	m.facebook.com	Success	Social Networking	Allow Social Networki…	Branch-B_rk-prod	/ajax/bootloader-endpoin…

Figure 19 - Exploration of user activity - showing web control policy actions

Stopping Threats with Malware Scanning

An employee attempts to download third-party software from an untrusted website. The file contains hidden malware. The Secure Web Gateway scans downloads, detects threats, and blocks them, thereby preventing infections while allowing safe browsing.

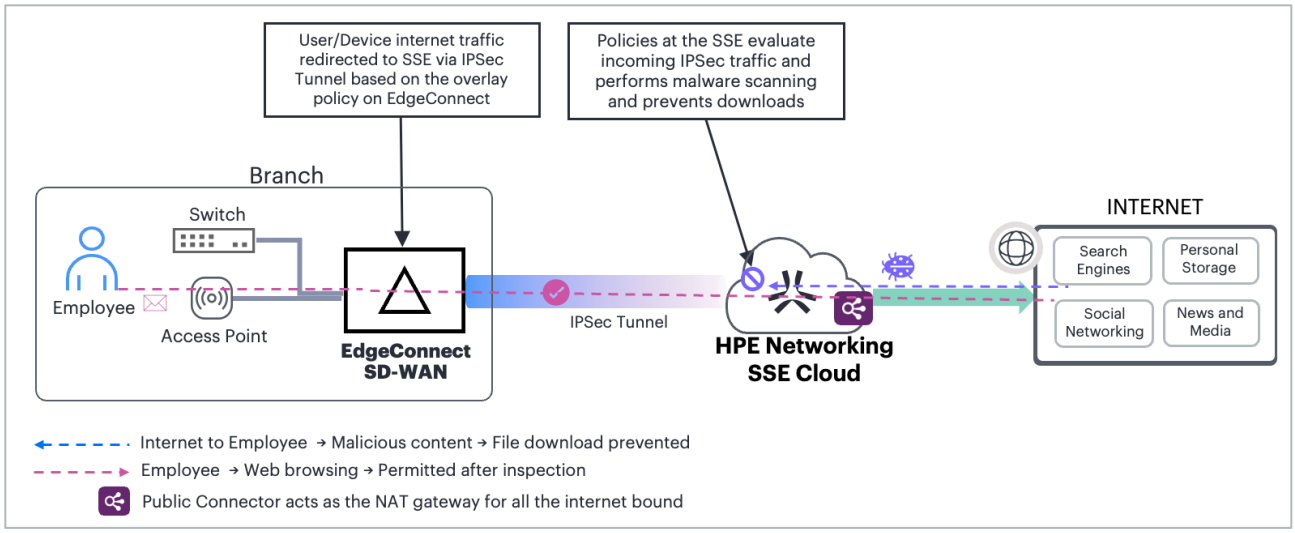


Figure 20 - Performing malware scan at the HPE SSE Cloud

Malware scanning on encrypted web traffic requires SSL inspection to analyze downloaded files for potential threats. The following procedure explains how to enable SSL inspection in a web profile, configure a web policy to scan file downloads for malware, and upload the trusted CA certificate necessary for proper SSL decryption.

Web Profile - Create or modify a Web Profile and enable SSL inspection:

- Navigate to **Policy > Profiles > External Web**.
- Create a new profile or edit an existing one (e.g., *Default Web Profile*).
- Check **Enable SSL Inspection**.
- Click **Submit** and **Apply Changes** to save the profile.

File Security Profile - Create or modify a File Security Profile to enable Scanning:

- Navigate to **Policy > Profiles > File Security Profiles**.
- Create a new profile or edit an existing one (e.g., *Default File Security Profile*).
- Set the **Action** to **Fast Scan** for the chosen file matcher. In this example, all files are scanned by applying the "Any Other File" match criteria with the action set to Fast Scan.
- Click **Submit** and **Apply Changes** to save the profile.

Root Certificate - Upload the enterprise CA Root certificate:

- Navigate to **Settings > Configuration > Certificates > CA Certificates**.
- Upload your enterprise CA using the **Upload Certificate** option (pfx format)

IMPORTANT: In this example, the pre-installed default CA on HPE SSE is used for testing. If you are using the default CA cert from the HPE SSE management console, you will need to install the same CA cert on your test machine for SSL inspection to work.

Web Policy - Create the Web Policy:

Finally, create a web policy to permit traffic. The **Web Profile** and **File Security Profile** will handle malware scanning.

- Navigate to **Policy > Rules**.

- Add a new rule or modify an existing one (in this example, an existing rule is modified to allow **Any Web Traffic**).
- Sample policy:
    - Set **Identity** to **Any**.
    - To apply the policy only to a specific branch location, set **Source** to **Locations** and select the branch from the list. *(This location is automatically created during tunnel orchestration in the Orchestrator.)*
    - Leave the other conditions as **Any**.
    - Set the **Action** to **Allow**.
    - Under **Profiles**, select the appropriate **Web Profile** and **File Security Profile**.
- Click **Submit** and **Apply Changes** to save the policy.

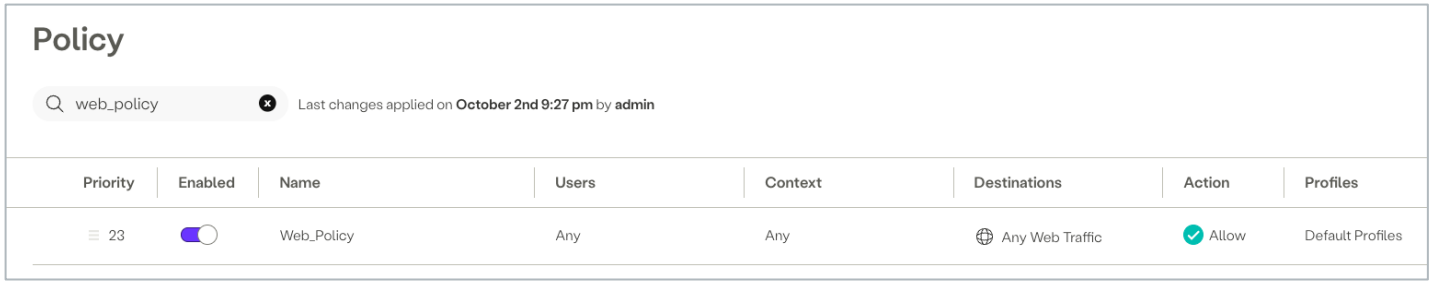


Figure 21 - Sample Web Policy on HPE SSE for malware scan

To view branch user traffic activity on HPE SSE, navigate to **Insights > Exploration**. Apply filters, such as Integration Type: IPsec, to view all traffic from the EdgeConnect gateway through the IPSec tunnel (as shown in the screenshot below).

In this example (Figure 22The report shows traffic from a branch user that was blocked due to a metadata restriction. The block was triggered by the malware scanning engine during inspection, highlighting how the SWG enforces advanced security controls on user traffic.

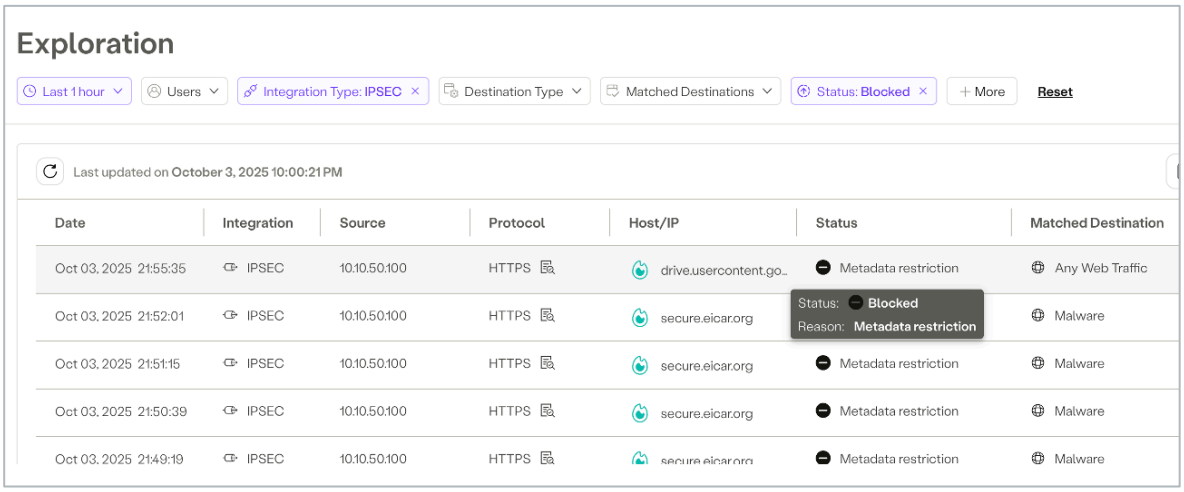


Figure 22 - Insights into user browsing activity showing restriction due to malware scan

Preventing Data Leakage with DLP

An employee attempts to upload a file containing sensitive and financial information to a personal cloud account. The SWG performs SSL inspection, detects sensitive data patterns using its DLP engine, and blocks uploads of sensitive data.

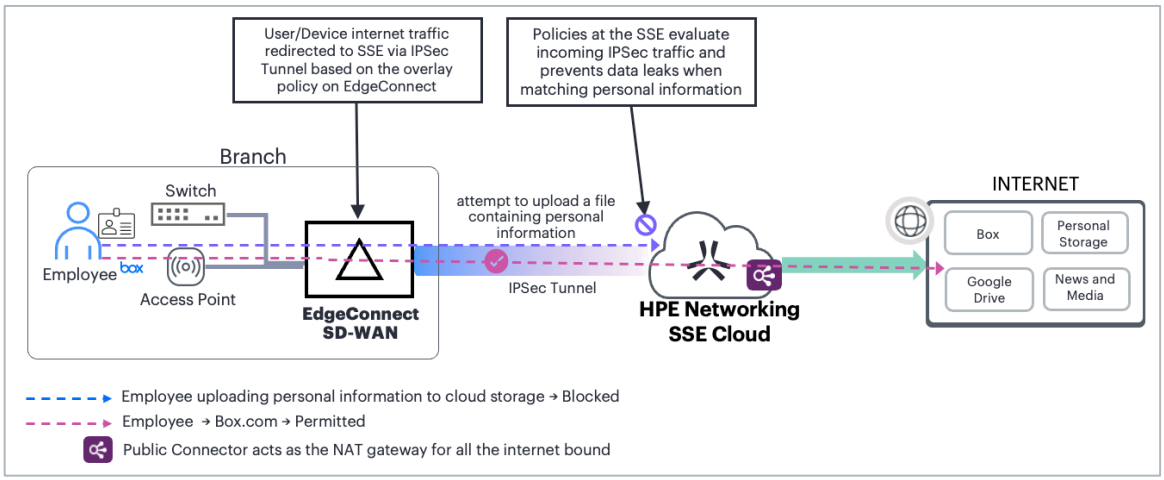


Figure 23 - Data Loss Prevention use case with SWG

DLP inspection of encrypted web traffic requires SSL inspection, allowing the Secure Web Gateway to analyze file uploads for sensitive information such as personal or financial data. The following procedure guides you in enabling SSL inspection in a web profile, creating a File Matcher and a File Security Profile to detect pattern matches for personal or financial data, and uploading a trusted CA certificate to ensure that encrypted traffic is decrypted correctly and inspected.

Web Profile - Create or modify a Web Profile and enable SSL inspection:

- Navigate to **Policy > Profiles > External Web**.
- Create a new profile or edit an existing one (e.g., *Default Web Profile*).
- Check **Enable SSL Inspection**.
- **Submit** and **Apply Changes** to save the profile.

File Matcher - Create or modify a File Matcher to detect the sensitive data pattern

- Navigate to **Policy > Profiles > File Matcher**
- Create a new file matcher or edit an existing one
- In this example, a new file matcher called "*SensitiveData_Matcher*" is created that has the following set of attributes:
    - **Action:** Upload/Download (scans the file for both upload and download activities)
    - **File Type:** Any (All files, you can select a specific file type if needed)
    - **Dictionaries:** Personal Information, SSN, and National Identifiers
    - For simplicity and brevity, this example uses a default dictionary. To better align with your organization's specific sensitive data patterns, you can create custom dictionaries using regular expressions (RegEx) and apply them in a file matcher profile to detect sensitive data during file inspection.
- **Submit** and **Apply Changes** to save the policy.

NOTE: HPE SSE supports pattern matching using Optical Character Recognition (OCR) to detect and prevent data leaks from image-based content. This capability is **not included** in the standard SWG Bandwidth (BW) subscription and requires an add-on license to enable OCR-based data loss prevention.

File Security Profile - Create or modify a File Security Profile for DLP:

- Navigate to **Policy > Profiles > File Security Profiles**.
- Create a new profile or edit an existing one (e.g., *Default File Security Profile*).
- Click on Add File Rules
    - **File Matcher**: Select the file matcher that identifies your data (e.g, *SensitivieData_Matcher*)
    - **Action:** Block
- Set the **Submit** and **Apply Changes** to save the profile

Root Certificate - Upload the enterprise CA Root certificate:

- Navigate to **Settings > Configuration > Certificates > CA Certificates**.
- Upload your enterprise CA using the **Upload Certificate** option (pfx format)

IMPORTANT: In this example, the pre-installed default CA on HPE SSE is used for testing. If you are using the default CA cert from the HPE SSE management console, you will need to install the same CA cert on your test machine for SSL inspection to work.

Web Policy - Create the Web Policy

Finally, create a web policy that permits access to cloud storage destinations. The **Web Profile** and **File Security Profile** will handle Data Loss Prevention, preventing any data leaks based on the file matcher definitions.

- Navigate to **Policy > Rules**.
- Add a new rule or modify an existing one (in this example, an existing rule is modified to allow **Any Web Traffic**).
- Sample policy:
    - Set **Identity** to **Any**.
    - To apply the policy only to a specific branch location, set **Source** to **Locations** and select the branch from the list. *(This location is automatically created during tunnel orchestration in the Orchestrator.)*
    - **Destination**: Personal Storage
    - Leave the other conditions as **Any**.
    - Set the **Action** to **Allow**.
    - Under **Profiles**, select the appropriate **Web Profile** and **File Security Profile**.
- Click **Submit** and **Apply Changes** to save the policy.

Figure 24 - Sample policy that includes profiles to detect data loss preventions

To view branch user traffic activity on HPE SSE, navigate to **Insights > Exploration**. Apply filters, such as Integration Type: IPsec, to view all traffic from the EdgeConnect gateway through the IPSec tunnel. The following insight (Figure

25) shows that a user's attempt to upload a spreadsheet file was blocked due to a policy match that detected personal information patterns, such as date of birth (DOB) and social security number (SSN), as defined in the file matcher policy.

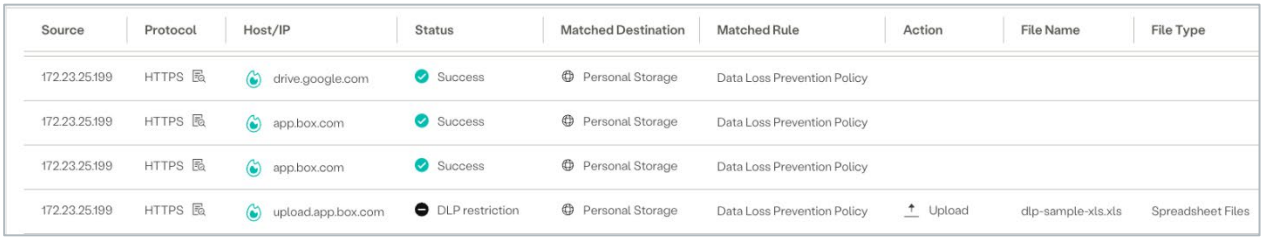


Figure 25 - Insight showing file upload blocked due to sensitive data match

Appendix A

Applying the Advanced Security (DTD) license to EdgeConnect gateways

The Advanced Security license is automatically available only to Tiered Licensing SD-WAN customers (AAS) across both Foundation and Advanced subscriptions.

With this enablement, customers are provisioned with Advanced Security (DTD) licenses equal to the number of their SD-WAN bandwidth subscriptions. For example, if you have 100 SD-WAN subscriptions (Foundation or Advanced), you will see 100 Advanced Security licenses listed in your Orchestrator license page. These licenses appear automatically, and no additional action is required to make them visible.

Viewing security license: **Configuration > Overlays & Security > Licensing > Licenses >** *select the Summary tab*

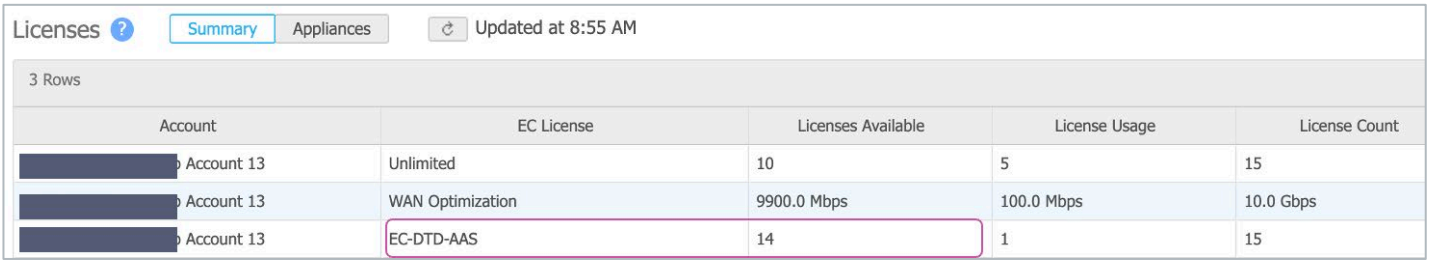


Figure 26 - Viewing Newly Enabled Security Licenses

Before applying a license, select **All** or the specific appliances from the left-hand appliances tree.

To apply a security license, navigate to: **Configuration > Overlays & Security > Licensing > Licenses >** *select Appliances tab* **>** *click on* **Assign Licenses to Appliances >** "Assign Licenses to Appliances" wizard will open:

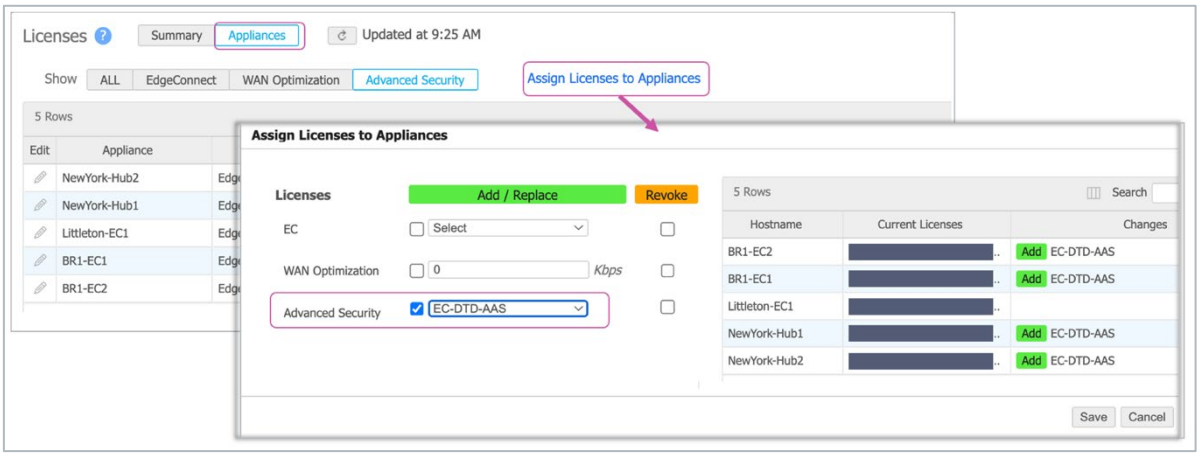


Figure 27 - Assigning Security License to Gateways

Check the box next to **Advanced Security** and click on **Save**

This completes the Advanced Security enablement on the EdgeConnect gateways. The gateways are now equipped with the advanced security functions outlined in this document, enabling you to implement the described use cases.

Appendix B

Enable Secure Web Service via Template Groups

- In Orchestrator, go to **Configuration > Templates and Policies > Templates**.
- Either use an existing Template Group or create a new one. (In this example, an existing Template Group is used.)
- Drag **Secure Web Services** from *Available Templates* into *Active Templates*.
- Enable the available Secure Web Services settings.
- Click **Save** and **Save Template Changes**.

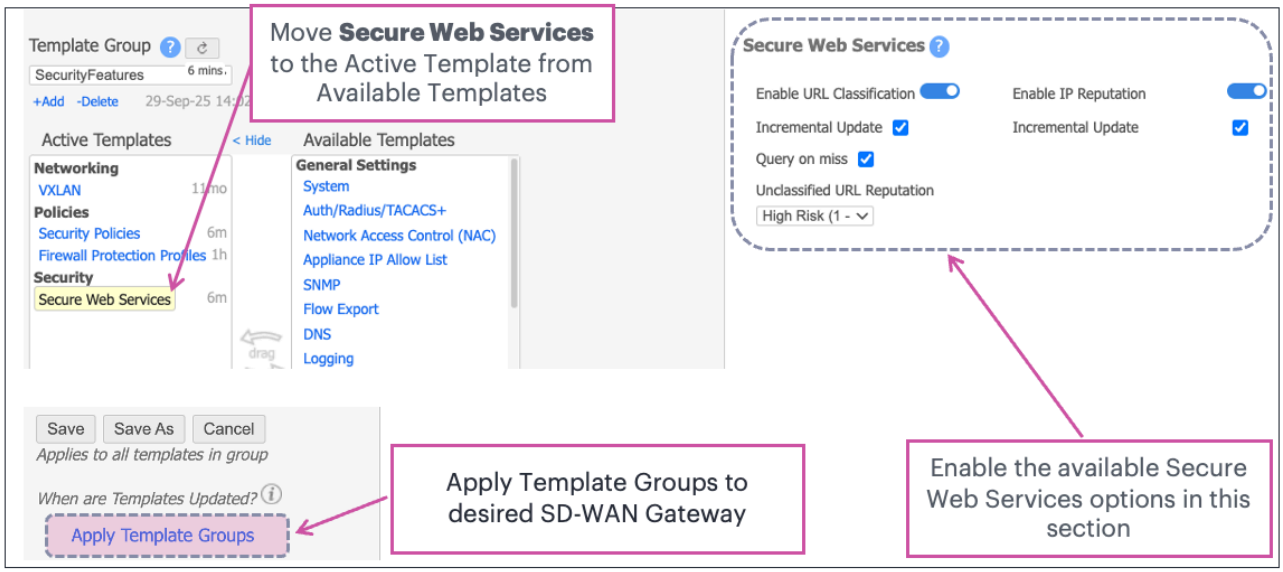


Figure 28 - Enabling Secure Web Services on gateways using Templates Group

- Once saved, apply the Template Group to your gateway using **Configuration > Templates and Policies > Apply Template Groups**.

Enabling secure web services on the EdgeConnect gateways is now complete. You may proceed to implement web security policies using the match criteria in the firewall policy.

Appendix C

SWG Bandwidth license

Your SSE tenant should have been created automatically. You may need to complete a few simple steps to set up credentials for logging into the HPE SSE management portal. The SWG bandwidth license is activated in the backend, so it will not be visible in the console.

Each SD-WAN bandwidth license includes 10 Mbps of SWG bandwidth. For instance, purchasing 100 SD-WAN licenses provides 100 10 Mbps SWG licenses, enabling easy testing of secure web gateway features in the cloud. For production use, plan for extra SWG subscriptions based on user numbers and site bandwidth requirements. Every 10 Mbps SWG subscription includes a 30 GB monthly fair-use policy allowance.

Connecting the EdgeConnect gateway to the HPE SSE cloud edge

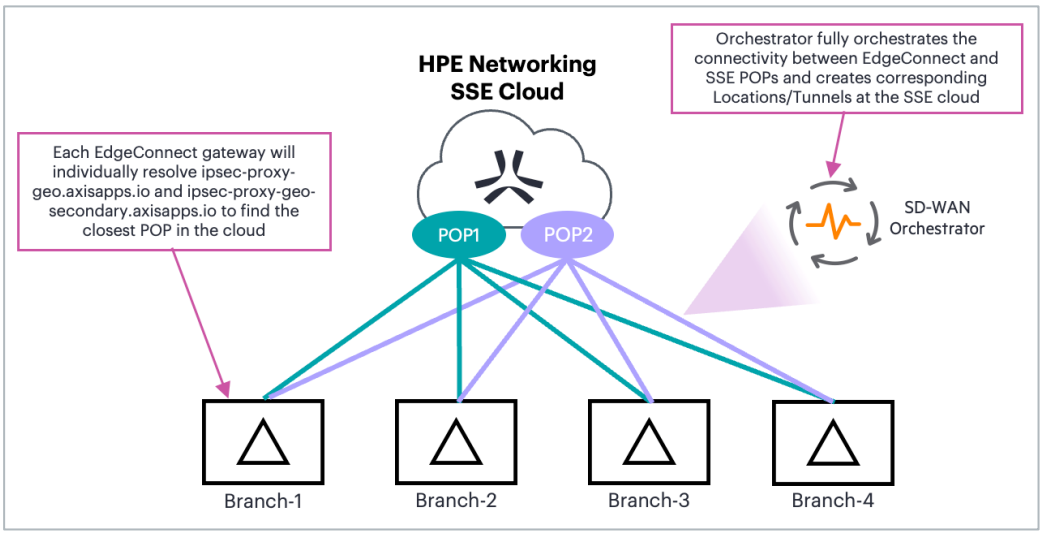


Figure 29 - Orchestrating connectivity to HPE SSE Cloud Edge

Log in to the HPE SSE Management Portal and navigate to **Settings > Admin API > New API Token**.

- Ensure the **Token Permission** is set to **Read and Write**.
- **Check all options** under **Token Scopes**.
- Set the **Token Expiration to 12 months** (maximum allowed).
- Click **Submit**.
- **Copy the token** before clicking OK.

If you miss copying it, you will not be able to retrieve the API key, and you will need to create a new one.

- Click on the **Apply Changes** on the top right of the management UI
- Click on **Commit Changes**

Log in to the SD-WAN **Orchestrator** and navigate to **Configuration > Cloud Services > HPE SSE.**

Click on the **Subscription** tab

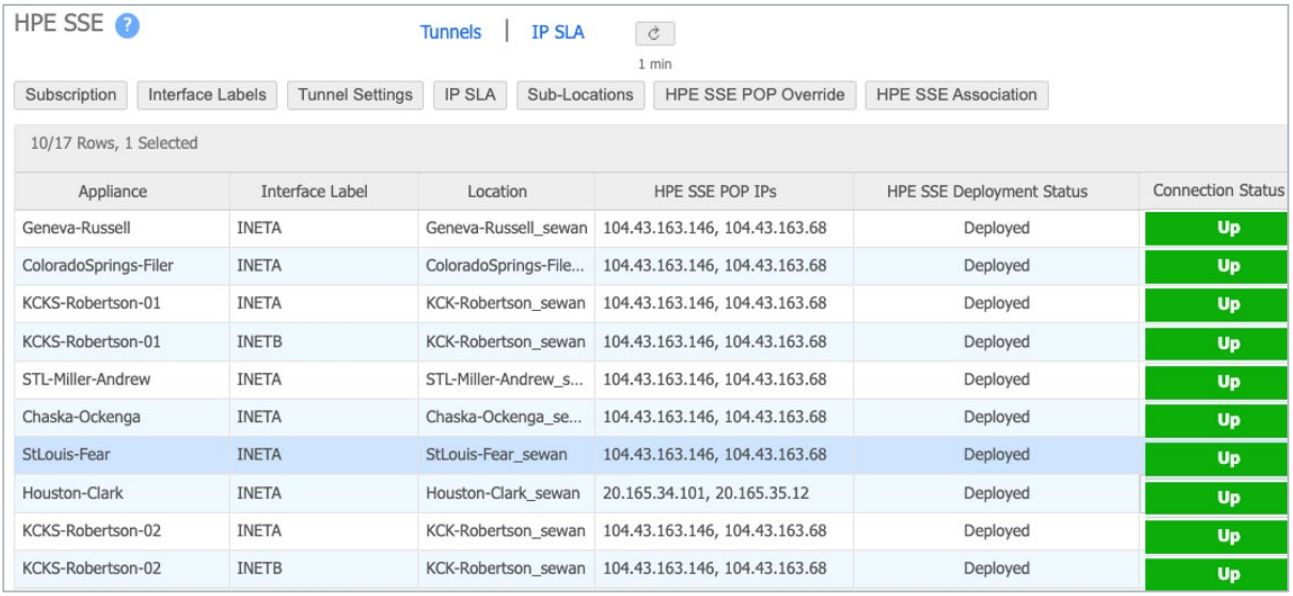
- Enter a name for the **API token**.
- Paste the API token key copied from HPE SSE.
- The API Domain will populate automatically.
- Enter the Tunnel Identifier in domain format (e.g., demo.com).
- Click **Save** to save the settings and exit Subscription

Click on the **Interface Labels** tab.

- Drag and drop **WAN labels** into the **Primary** (if needed, add labels to the **Backup** section)
- This ensures Orchestrator correctly orchestrates tunnels for the designated WAN interfaces.
- Marking a WAN label as Primary ensures tunnels built on that interface are preferred for traffic path selection.
- Click **Save** to apply the settings and exit the Interface Labels configuration.

Finally, from the Appliances tree on the left, select all appliances or the specific appliance(s) for which you want to build tunnels to HPE SSE.

- Click on the **HPE SSE Association** tab.
- Check the box next to **Add**.
- Click **Save** to apply the settings and exit the HPE SSE Appliance Association dialog.
- Once the association is complete, Orchestrator will begin orchestrating tunnel configuration for each selected gateway.
- The page will display the deployment status. If the status shows **'Deployed' and the connection status is 'UP'**, the tunnels have been successfully created and are active.



Appliance	Interface Label	Location	HPE SSE POP IPs	HPE SSE Deployment Status	Connection Status
Geneva-Russell	INETA	Geneva-Russell_sewan	104.43.163.146, 104.43.163.68	Deployed	Up
ColoradoSprings-Filer	INETA	ColoradoSprings-File...	104.43.163.146, 104.43.163.68	Deployed	Up
KCKS-Robertson-01	INETA	KCK-Robertson_sewan	104.43.163.146, 104.43.163.68	Deployed	Up
KCKS-Robertson-01	INETB	KCK-Robertson_sewan	104.43.163.146, 104.43.163.68	Deployed	Up
STL-Miller-Andrew	INETA	STL-Miller-Andrew_s...	104.43.163.146, 104.43.163.68	Deployed	Up
Chaska-Ockenga	INETA	Chaska-Ockenga_se...	104.43.163.146, 104.43.163.68	Deployed	Up
StLouis-Fear	INETA	StLouis-Fear_sewan	104.43.163.146, 104.43.163.68	Deployed	Up
Houston-Clark	INETA	Houston-Clark_sewan	20.165.34.101, 20.165.35.12	Deployed	Up
KCKS-Robertson-02	INETA	KCK-Robertson_sewan	104.43.163.146, 104.43.163.68	Deployed	Up
KCKS-Robertson-02	INETB	KCK-Robertson_sewan	104.43.163.146, 104.43.163.68	Deployed	Up

Figure 30 - EdgeConnect gateway tunnel state with HPE SSE Cloud

What is the best practice for SWG?

Not all network traffic needs to be routed through the cloud Secure Web Gateway. Many business applications already include robust native security controls and can be accessed safely directly. Sending such trusted traffic through the SWG introduces unnecessary processing and may increase latency without adding significant protection.

The recommended best practice is to direct only untrusted or unknown internet traffic, such as general web browsing, to the SWG. This approach ensures advanced security inspection is applied where it is most needed, while maintaining optimal performance for trusted applications.

Traffic redirection from EdgeConnect gateway to Secure Web Gateway

Once you determine which traffic should be sent to the HPE SSE Cloud for advanced inspection, redirect it using a Business Intent Overlay on the Orchestrator:

- Navigate to **Configuration > Overlays and Security > Business Intent Overlays**.
- Modify an existing overlay or add a new overlay to identify SSE-bound traffic and direct it through tunnels to HPE SSE.
- Click the **pencil** icon next to the **Match** section to edit the Overlay ACL.
- On the Overlay ACL page, add a policy that identifies the traffic to be sent to the HPE SSE Cloud.
- Example: In this scenario, an existing overlay called “HPE_SSE” is modified with a policy to send traffic from the “Corp” label interface. More specifically, traffic-matching websites with medium- to high-risk reputations.

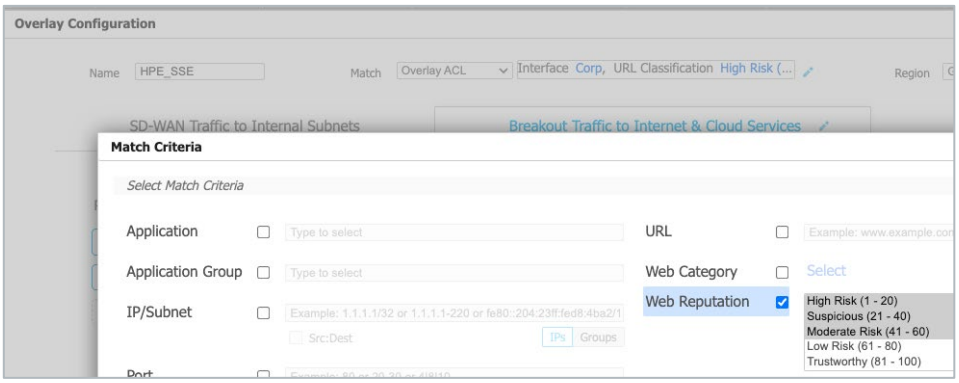


Figure 31 - Selecting traffic to redirect to SWG

- Click **Save** to confirm the ACL settings.
- Go to the **Breakout Traffic to Internet & Cloud Services** tab in the Overlay Configuration page.
- Drag the **HPE SSE Cloud icon** from Available Policies to Preferred Policy Order, ensuring it is at the top of the list.

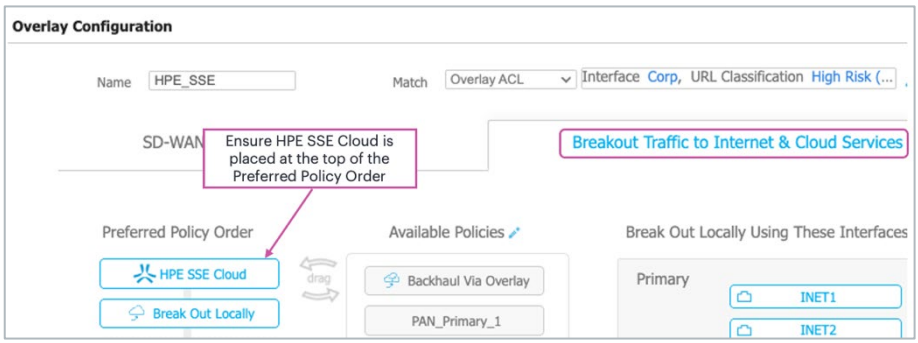


Figure 32 - Configuring Business Internet Overlay to send HPE SSE Cloud

- Click **OK** to close the Overlay Configuration page.
- Finally, click **Save and Apply Changes to Overlays** to confirm the updates to the Business Intent Overlay.

IMPORTANT: Ensure that EdgeConnect has a firewall policy allowing user traffic to access the internet. In this example, internet traffic from the “Corp” labeled interface is already permitted.

To Learn More

Security Features Guide – Overview of all security features available in the EdgeConnect SD-WAN gateway.

EdgeConnect SD-WAN with SWG: Blog post explaining the fundamental components of SASE.

What is SWG – A quick video introducing HPE SSE’s Secure Web Gateway capabilities.

Identity-Based Traffic Management – Explains user-identity–based security policies and use cases.

Orchestrator Administration Guide – Admin guide that provides

SSE Administrator Guide – Admin guide that outlines all the features of SSE and navigating various menus.