

---

# Forcepoint ONE Integrated with Aruba SD-WAN

**Forcepoint**

# Introduction

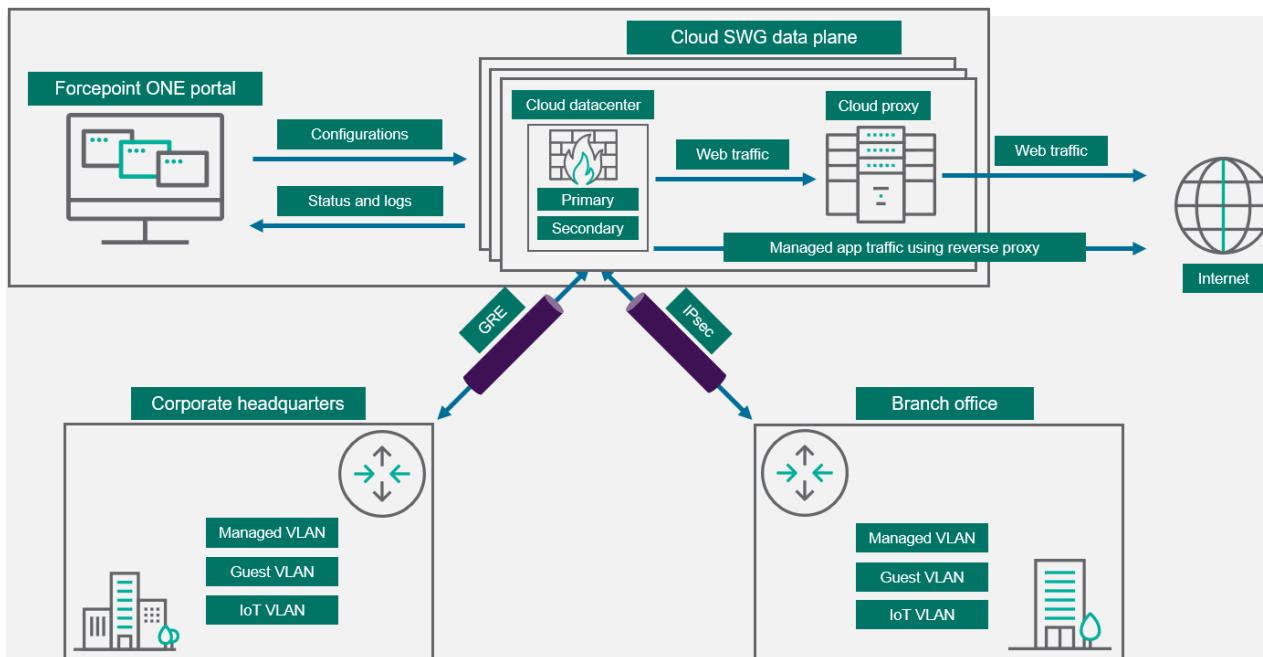
The Forcepoint ONE cloud SWG solution enables web traffic filtering when a SmartEdge agent cannot be deployed on the end-user's machine such as for guest users, IoT devices or when the organization chooses not to deploy an agent.

To filter the web traffic, the Forcepoint ONE SWG routes the customer's web traffic from one or more location(s) over the tunnel to Forcepoint ONE where the SWG functionality is implemented. The Forcepoint ONE SWG implements a transparent proxy, meaning that a PAC file is not required on the end users' devices to forward traffic to it. The Forcepoint ONE SWG solution supports GRE and IPsec modes of tunneling as some network devices only support IPsec tunneling, and others support GRE tunneling.

## IPSec Overview

IPsec is an extension of the IP protocol that provides secure traffic tunneling by authenticating and encrypting information sent over a network. The IPsec protocol uses Internet Key Exchange (IKE) to establish session keys for encryption and decryption and Encapsulating Security Payload (ESP) to provide data confidentiality and integrity. Traffic to the Forcepoint ONE Cloud SWG service can be fully encapsulated in tunnel mode, providing complete traffic encryption. IPsec connectivity can also support sites that connect to the Internet with a dynamic IP address, using a fully qualified domain name (FQDN) as the device IKE ID.

Forcepoint ONE Cloud recommends that you configure edge devices with 2 tunnel connections, using different Forcepoint ONE data center addresses for geographic redundancy. Tunnels should be configured in an active/standby configuration with automatic failover. Each data center has a tunnel monitoring address that can be used to monitor the status of the connection. The Edge device (firewall or router) at the customer's site must be configured to send only web traffic on TCP ports 80 and 443 over the tunnel to SWG. All other traffic should be routed direct to the Internet. If traffic is sent over the tunnel using any other port(s), it will be discarded. This guide describes how to configure HPE Aruba SD-WAN using the Forcepoint ONE IPsec tunnel configurations. The IPsec configuration below utilizes the HPE Aruba SD-WAN commands and concepts.



## This document is for users

- Who are expert network engineers and have prior experience in configuring GRE and IPsec tunnels on various edge devices (firewalls and routers).
- Who would like to know about GRE or IPsec tunnel configurations on the Forcepoint ONE portal and on the edge devices.

## Related Documents

Aruba SD-WAN Documents: <https://www.arubanetworks.com/techdocs/sdwan/>

# Forcepoint ONE Configuration

This section details the configuration requirements to set-up the IPsec tunnel in the Forcepoint ONE portal.

## Creating Sites

A site represents a corporate location from which traffic will originate. While creating a site, you can configure either a GRE or IPsec tunnel through which traffic should be routed to the cloud and create or add subnet groups within the site.

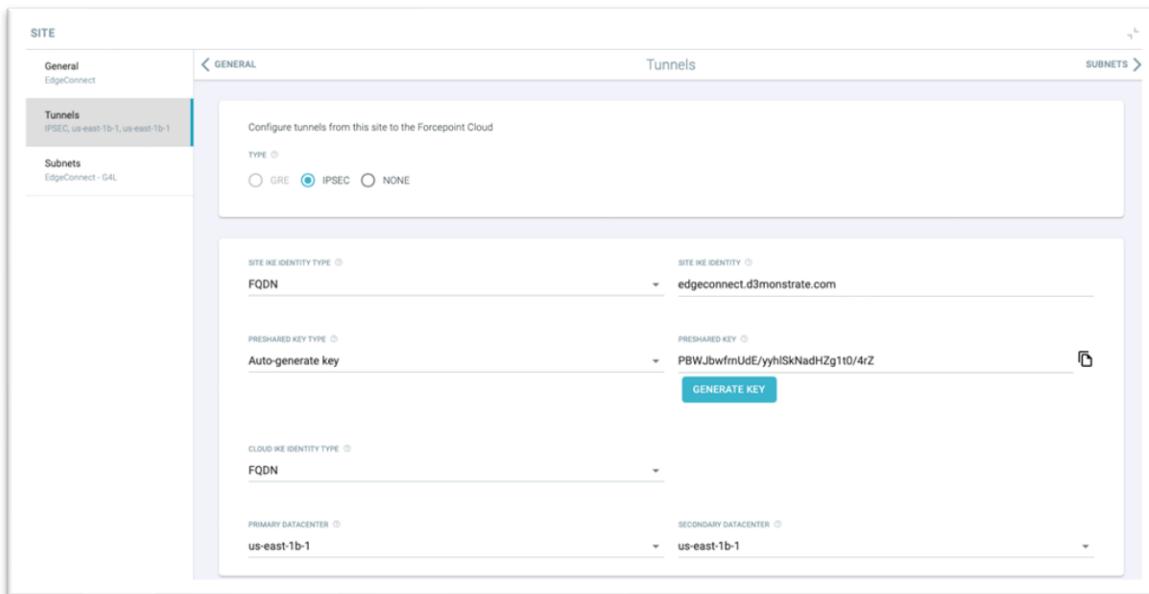
To create a new corporate site, follow these steps:

1. Navigate to **Protect> Objects> Sites**.
2. On the **Sites** page, click the green plus icon.
3. On the **General** tab.
  - a) Enter a unique **Name** for the site.
  - b) Select the appropriate **Time Zone** of the corporate IP location.
  - c) Enter a **Description** for the Site.
  - d) Enter the **Public IP** address of the site.
    - Forcepoint ONE validates the IP address to make sure that the value is an IP address and not a duplicate of another site with the same IP address.
  - e) Set the **Identify Coordinates** to **Automatic** to identify the location of the site based on the entered IP address when you click **Detect Location**.
    - **Location** will display the location name of the entered IP address.
  - f) If you need a finer coordinate or Forcepoint ONE is unable to identify the location of the entered IP address, then set the **Identify Coorindates** to **Maunal** and enter the **Latitude** and **Longitude**.

The screenshot shows the 'General' configuration page for a site named 'EdgeConnect'. The 'General' tab is active in the sidebar. The main form includes fields for 'NAME' (EdgeConnect), 'TIMEZONE' (America/Montreal), and 'PUBLIC IP' (51.161.19.112). Below these, there's a 'IDENTIFY LOCATION' section with 'AUTOMATIC' selected and a 'DETECT LOCATION' button. The 'TUNNELS >' tab is visible at the top right of the page.

#### 4. On the **Tunnels** tab

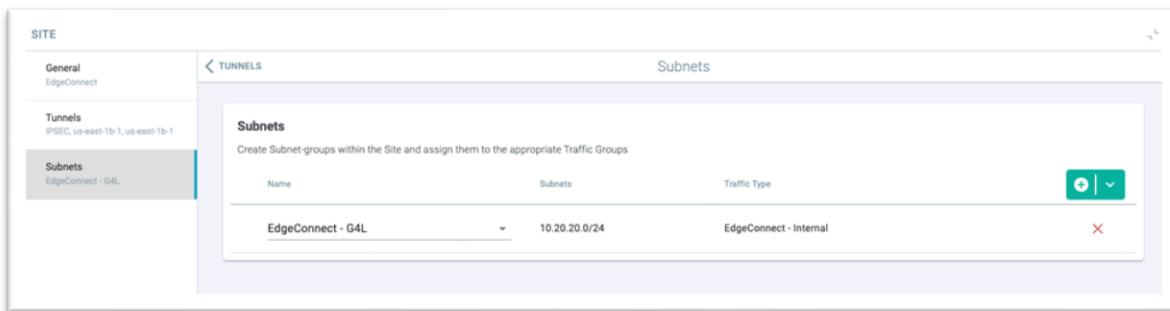
- Select the **Type** as **IPsec**.
- Select whether the site uses its **Public IP address** or a **FQDN** from the **Site IKE Identity Type**.
- Enter either the Public IP address or a FQDN in the Site IKE Identity as from the Site IKE Identity Type selection.
  - When the Site IKE Identity Type is set to a Public IP address you can also enter a Dynamic IP address. The IP address that was assigned dynamically by any one of the ISPs connected to the site in the Site IKE Identity field. This Dynamic IP address can change over time and is used as a tag to match any Location Policies for the site on the Protect > Policies page.
- Select whether you will **Use Your Own Key** or an **Auto-generated Key** from the **Preshared Key Type**.
- Enter the **Preshared Key** configured on the site firewall or router OR click the **Generate Key** to auto-generate a key to use while configuring the site firewall or router.
  - The Preshared Key is case sensitive and must be a minimum of 8 characters.
- Select the **Data Center** where the primary tunnel from the site is terminated.
- Select the **Data Center** where the secondary tunnel from the site is terminated.
  - Select a Data Center that is in a different region or zone than the Primary Data Center. If you do not want to assign a Secondary Data Center then select None from the Secondary Data Center drop-down list.



#### 5. On the **Subnets** tab (Optional)

- Define the Subnets or reuse the configured Subnets with the site. Subnets are unique within a site. However, in large cookie cutter network deployments the same Subnet may be used in multiple sites. Combination of Site and Subnet is globally unique.
- To add Subnet(s) defined in **Protect > Objects > Custom Locations** page click the green plus icon and a Subset will appear.
- From the **Name** drop-down list select the applicable Subset. The details of the selected Subset will appear, and you can add as many Subsets as required.

- c) To create a new Subset for the site
  - o Click the arrow button and select **Create New** and then the **Create Subnet** dialog will open.
  - o Enter a unique **Name** of the location for easy identification.
  - o Select the **Traffic Type** for the subnet addresses in the custom location.
  - o Enter the **IP Address**, one per line in CIDR notation. Custom locations should be external internet facing addresses and can be an IP address, subnets or ranges on individual lines.
  - o Leave the **Trustd IP Addresses** checkbox unchecked. Then click **Save** to save the custom location details.
- ci) To configure a site with selected information, click **OK**.
  - o As soon as the Site is created, the status of the Site will be **Configuring**. After some time, the status of the Site will change to **Provisioned** or **Failed**. A tunnel takes approximately 3 minutes for it to be Provisioned.



## Viewing Tunnels

After creating tunnels, you can monitor the status of each tunnel under the **Analyze> Tunnels** page. The status of the tunnel can be **Configuring**, **Provisioned**, **Failed**, **Up** or **Down**.

A tunnel typically takes approximately 3 minutes to be **Provisioned**, and then the status will change to **Down**. Once the status of the tunnel is **Down**, the IPsec tunnel status will change to **Up** only when customer's firewall or router is correctly configured and there is successful communication between router and cloud.

| <b>Tunnels</b>    |       |           |        |                            |
|-------------------|-------|-----------|--------|----------------------------|
| SITE              | TYPE  | LINK      | STATUS | CONFIGURATION              |
| Cisco-Azure-Site4 | IPsec | Secondary | Up     | <a href="#">Setup Info</a> |
| Cisco-Azure-Site4 | IPsec | Primary   | Up     | <a href="#">Setup Info</a> |

To view the configuration details of the tunnel, click the **Setup Info** link for the tunnel in question. These details are useful for configuring the customer's firewall or router. The customer's Edge device (firewall or router) must be configured to send only web traffic on TCP ports 80 and 443 over the tunnel to the cloud SWG. All other traffic should be routed direct to the Internet. If traffic over any other port(s) is sent over the tunnel, it will be discarded.

When clicking on the **Setup Info** link for the **Primary IPsec** tunnel the following details are displayed

|   |   |                              |
|---|---|------------------------------|
| SITE IKE ID   | edgeconnect.d3monstrate.com               |                              |
| CLOUD FQDN  | dynamics3curity-4.va.us.vpn.forcepoint.io |                              |
| CLOUD IKE ID  | dynamics3curity-4.va.us.vpn.forcepoint.io |                              |
| PRE-SHARED KEY  | 4acb3b4GCWBztuf6djXRYcgUJCchYVo3          |                              |
| MONITORING IP   | 116.50.59.230                             |                              |
| <b>Supported Settings:</b>  |   |                              |
| IKE Parameters (Version supported: IKEv2) ( <b>Bold = recommended</b> ) |   |                              |
| Ciphers: AES-128, AES-256   | Digest: SHA2 256bit                       | DH Groups: <b>14, 19, 20</b> |
| Auth Method: Pre-shared key   | Lifetime: 24 hours                        | PFS: Not Supported           |
| IKE ID Support: FQDN (hostname), Public IP Address                      |   |                              |
| <b>IPsec Parameters</b>   |   |                              |
| Type: ESP   | Digest: SHA2 256bit                       | Lifetime: 8 hours            |
| Ciphers: <b>AES-GCM-128, AES-GCM-256</b> , AES-128, AES-256, Null       |   |                              |

When clicking on the **Setup Info** link for the **Secondary IPsec** tunnel the following details are displayed

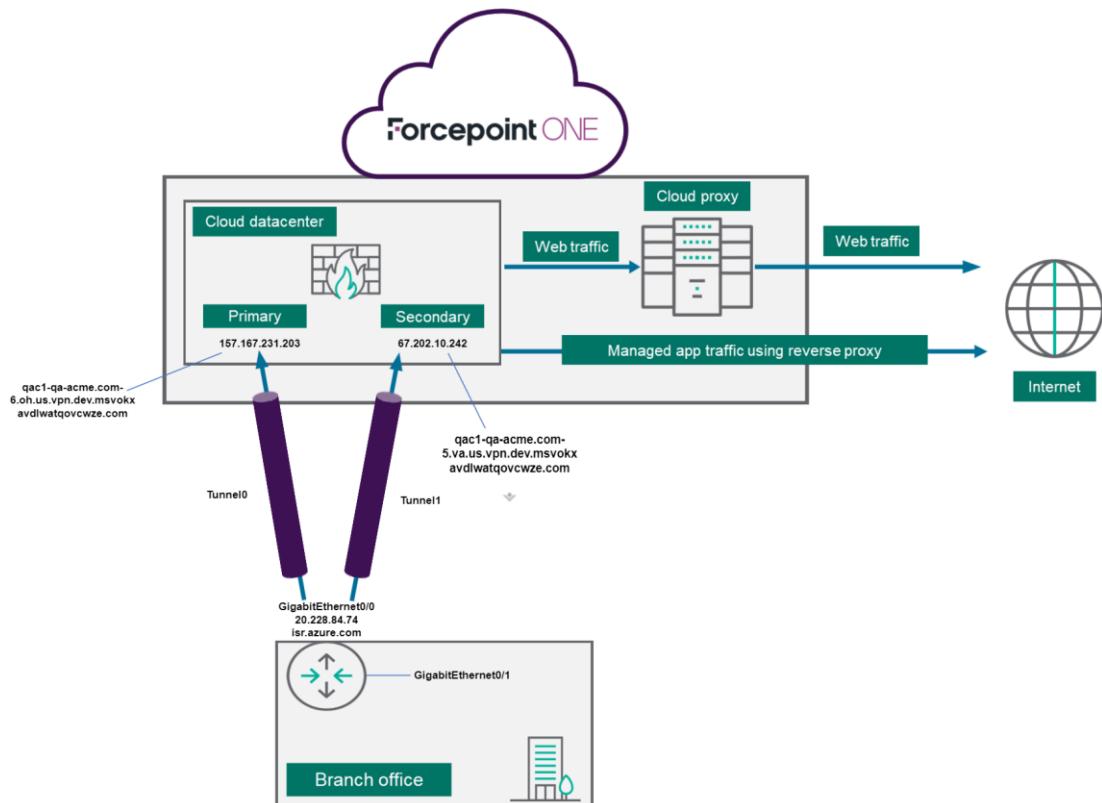
|   |                                  |                              |
|---|----------------------------------|------------------------------|
| SITE IKE ID   | edgeconnect.d3monstrate.net      |                              |
| CLOUD FQDN  | fp-se-4.va.us.vpn.forcepoint.io  |                              |
| CLOUD IKE ID  | fp-se-4.va.us.vpn.forcepoint.io  |                              |
| PRE-SHARED KEY  | j3ddS49zFvnWrLXIBOVelnP/KjYf+6+f |                              |
| MONITORING IP   | 116.50.59.230                    |                              |
| <b>Supported Settings:</b>  |                                  |                              |
| IKE Parameters (Version supported: IKEv2) ( <b>Bold = recommended</b> ) |                                  |                              |
| Ciphers: AES-128, AES-256   | Digest: SHA2 256bit              | DH Groups: <b>14, 19, 20</b> |
| Auth Method: Pre-shared key   | Lifetime: 24 hours               | PFS: Not Supported           |
| IKE ID Support: FQDN (hostname), Public IP Address                      |                                  |                              |
| <b>IPsec Parameters</b>   |                                  |                              |
| Type: ESP   | Digest: SHA2 256bit              | Lifetime: 8 hours            |
| Ciphers: <b>AES-GCM-128, AES-GCM-256</b> , AES-128, AES-256, Null       |                                  |                              |

| Sites   |             |               |             |   |
|---|-------------|---------------|-------------|---|
| A Site represents a corporate location from which traffic will originate.<br>Create sites for each of your locations here |             |               |             |   |
| Site  | Description | Public IP     | Status      |   |
| REMOTE-SITE-01 - IPSec  |             | 1.1.1.1       | Provisioned | X |
| REMOTE-SITE-01 - GRE  |             | 1.1.1.2       | Provisioned | X |
| SEU Lab Tunnel - Chris  |             | 51.79.47.109  | Provisioned | X |
| EdgeConnect - Timo  |             | 51.161.19.112 | Provisioned | X |
| EdgeConnect - Jonathan  |             | 72.214.27.139 | Provisioned | X |

## Aruba SD-WAN Configuration

This section details the required configuration that must be applied on the Edge device using the details from the **Analyze> Tunnels** page in the Forcepoint ONE portal.

This document shows an example environment for information and guidance only. While every effort has been made to ensure the accuracy of this information, we advise to consult the latest documentation for your Edge device and test your configuration thoroughly. For detailed information on Aruba SD-WAN refer to the [Aruba SD-WAN Documentation](#).



## Maximum Segment Size (MSS)

The encapsulation overhead of the IPsec tunnel means that TCP sessions sent over the tunnel must be limited to the lower MSS than usual. Most TCP clients will propose an MSS value of 1460 bytes when connecting over an Ethernet network.

Forcepoint ONE recommends setting an MSS value of no more than 1360 bytes in order to leave overhead for IPsec encapsulation. This can often be achieved by using the MSS clamping feature of a firewall or router to ensure that any TCP traffic sent down the tunnel is limited to an MSS value of 1360.

Where the WAN connection to the Forcepoint ONE data center, uses the IPoE or PPPoE protocol, the MSS value may need to be lowered to account for the encapsulation overhead of the WAN connection. To display the current MSS setting for your tunnel interface, use the appropriate **show interface** command on your Edge device.

## Supported IPSec Settings

For IPsec connectivity, your Edge device must be configured to use the Forcepoint supported IKE tunnel negotiation and IPsec encryption settings.

### Supported tunnel negotiation and encryptions settings

| Setting                       | Supported (Recommended in Bold)                                |
|-------------------------------|--|
| IKE version                   | IKEv2 – (RFC 7296, October 2014)                               |
| IKE cipher                    | AES-128<br>AES-256   |
| IKE message digest            | SHA2, length 256   |
| DH groups                     | 14<br>19<br>20   |
| IPsec type                    | ESP  |
| IPsec cipher                  | <b>AES-GCM-128</b><br><b>AES-GCM-256</b><br>AES-128<br>AES-256 |
| IPsec message digest          | SHA2, length 256   |
| Authentication method         | Pre-shared key   |
| IKE lifetime                  | 24 hours   |
| IPsec lifetime                | 8 hours  |
| IKE ID support                | FQDN (hostname)<br>Public IP address                           |
| Perfect Forward Secrecy (PFS) | Not supported  |

## Abbreviations for Configuration Parameters in IPsec Examples

Abbreviations are used for configuration parameters in the configuration examples. Replace the abbreviations with the appropriate addresses and values for your configuration.

| Parameter                       | Description  |
|---------------------------------|--|
| <supported_ipsec_cipher>        | Select an IPsec cipher supported by the service.   |
| <supported_ike_cipher>          | Select an IKE cipher supported by the service.   |
| <supported_dh_group>            | Select a DH group supported by the service.  |
| <primary_destination_address>   | The Cloud FQDN of the Forcepoint ONE data center for your primary tunnel. Displayed for the connection in the <b>Analyze &gt; Tunnels &gt; Setup Info</b> in Forcepoint ONE portal. To know the public IP address of the primary data center, you need to look up using the Cloud FQDN.            |
| <Secondary_destination_address> | The Cloud FQDN of the Forcepoint ONE data center for your secondary tunnel. Displayed for the connection in the <b>Analyze &gt; Tunnels &gt; Setup Info</b> in Forcepoint ONE portal.<br><br>To know the public IP address of the secondary data center, you need to look up using the Cloud FQDN. |
| <outgoing_interface>            | The name of the egress interface on your edge device.  |
| <pre-shared_key>                | The pre-shared key configured for the tunnel. Must match the key configured for the connection and can be found under the <b>Analyze &gt; Tunnels &gt; Setup Info</b> in Forcepoint ONE portal.  |
| <local_fqdn_id>                 | The FQDN (DNS hostname) of the edge device.  |
| <public_egress_IP>              | The public egress IP address of the edge device.   |
| <primary_cloud_ike_id>          | The Cloud IKE ID for the Forcepoint ONE primary data center. Displayed for the connection under the <b>Analyze &gt; Tunnels &gt; Setup Info</b> in Forcepoint ONE portal.  |
| <secondary_cloud_ike_id>        | The Cloud IKE ID for the Forcepoint ONE secondary data center. Displayed for the connection under the <b>Analyze &gt; Tunnels &gt; Setup Info</b> in Forcepoint ONE portal.  |
| <primary_monitoring_address>    | The tunnel monitoring IP address for the primary tunnel connection. Displayed for the connection under the <b>Analyze &gt; Tunnels &gt; Setup Info</b> in Forcepoint ONE portal.   |
| <secondary_monitoring_address>  | The tunnel monitoring IP address for the secondary tunnel connection. Displayed for the connection under the <b>Analyze &gt; Tunnels &gt; Setup Info</b> in Forcepoint ONE portal.   |
| <client_subnet>                 | IP address range for the internal subnet whose traffic will be forwarded to the tunnel.  |
| <dummy_subnet#_ip#>             | Dummy private IP addresses used as the inner tunnel IP addresses for routing traffic to the tunnel interface.  |

## Resolve Forcepoint Cloud FQDN

Forcepoint ONE SSE provides FQDN endpoint. Utilizing the ping utility in the Edge Connection you can resolve the FQDN into an IP address. In this example below the FQDN **fp-se4.va.us.vpn.forcepoint.io** resolves into **52.210.134.75**. Perform this step for the Primary and Secondary Tunnel.

The screenshot shows the Aruba Network Connectivity interface. The top navigation bar includes Monitoring, Configuration, Administration, Maintenance, and Support. Below the navigation is a sub-header for 'Ping/Traceroute' with a question mark icon. The main section is titled 'Network Connectivity' with tabs for 'Ping' and 'Traceroute' (selected). The 'IP/Hostname' field contains 'fp-se-4.va.us.vpn.forcepoint.io'. A 'Segment' dropdown is set to 'Default'. Under the 'Options' section, there is a large text input area. Below it are 'Start' and 'Clear' buttons. The 'Output' section displays the results of a ping command:

```
PING fp-se-4.va.us.vpn.forcepoint.io (52.201.134.75) 56(84) bytes of data.
--- fp-se-4.va.us.vpn.forcepoint.io ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 160ms
```

## Configure Primary Tunnel

In the Aruba Navigate to the Tunnel configuration to configure both Primary and Secondary Tunnel.

### General Tunnel Settings

Alias: <your descriptive name>

Mode: IPSec

IPsec Suite B Preset: None

Local IP: <edgeconnect IP>

Remote IP: <FONE IP-address>

NAT: None

Peer/Service: <label to use in overlays>

Auto Max BW: 1000000(Auto)

| General              |                                     |
|----------------------|-------------------------------------|
| Setting              | Value                               |
| Alias                | Forcepoint-ONE-US-EAST-1A           |
| Mode                 | IPSec                               |
| IPsec Suite B Preset | None                                |
| Admin                | up                                  |
| Local IP             | 192.168.123.254 - Default           |
| Remote IP            | 107.23.63.125                       |
| NAT                  | none                                |
| Peer/Service         | FONE-US-EAST-1A                     |
| Auto Max BW Enabled  | <input checked="" type="checkbox"/> |
| Max BW Kbps          | 1000000(Auto)                       |
| Kbps                 |                                     |

## IKE Settings

Preshared Key: <PSK from FONE>  
 Authentication Algorithm: SHA2-256  
 Encryption Algorithm: AES-CBC-256  
 Diffie-Hellman Group: 19  
 Lifetime: 1440 minutes  
 Dead Peer Detection: 10 seconds / 3 retries  
 Local IKE Identifier: <FONE SITE IKE ID>  
 Remote IKE Identifier: <FONE SITE Cloud ID>  
 Phase-1 Mode: N.A  
 KE Version: IKE v2

| IKE                            |                         |
|--------------------------------|-------------------------|
| Preshared Key                  | *****                   |
| Authentication Algorithm       | SHA2-256                |
| Encryption Algorithm           | AES-CBC-256             |
| Diffie-Hellman Group           | 19                      |
| Lifetime                       | 1440 Mins               |
| Dead Peer Detection            |                         |
| Delay time                     | 10 Secs                 |
| Retry Count                    | 3                       |
| DPD effective timeout 34 Secs. |                         |
| Local IKE Identifier           | edgeconnect.d3monstra   |
| Remote IKE Identifier          | dynamics3curity-4.va.us |
| Phase 1 Mode                   | Aggressive              |
| IKE Version                    | IKE v2                  |

## IPSec Settings

Authentication Algorithm: N/A  
 Encryption Algorithm: AES-GCM-256  
 IPSec Anti-replay Window: Disable  
 Lifetime: 480 minutes  
 Perfect Forward Security Group: Disable

| IPsec                         |             |
|-------------------------------|-------------|
| Authentication Algorithm      | NA          |
| Encryption Algorithm          | AES-GCM-256 |
| IPsec Anti-replay Window      | Disable     |
| Lifetime                      | 480         |
| Mins (0 = disabled)           | 0           |
| MegaBytes (0 = disabled)      | 0           |
| Perfect Forward Secrecy Group | disabled    |

## Configure Secondary Tunnel

Follow the same process for the secondary tunnel as outlined for the Primary Tunnel. Use the Secondary Tunnel Setup Info in Forcepoint ONE.

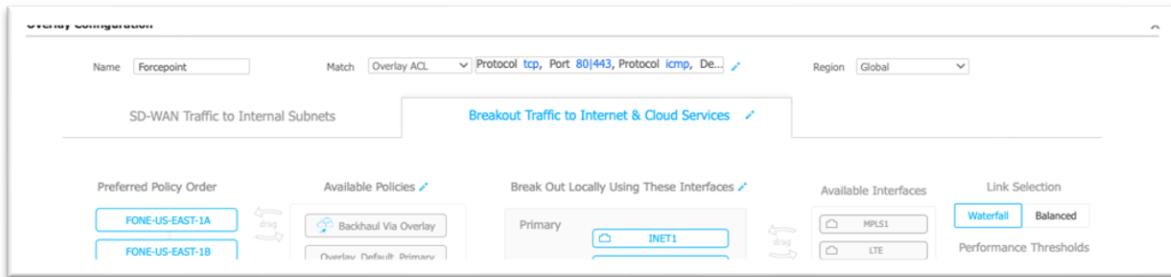
Note: You must use different Peer/Service tablet for the Secondary Tunnel than the Primary Tunnel.

## Configure Business Intent Overlay

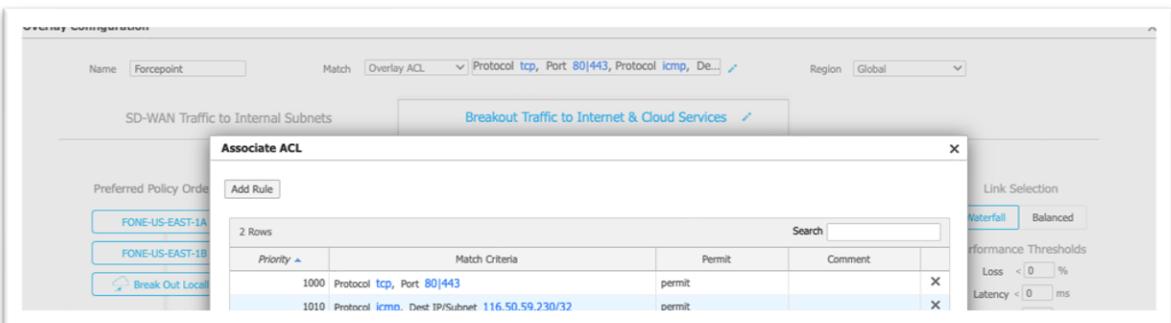
Forcepoint One accepts HTTP/HTTPS traffic on ports 80 and 443. You can send the ICMP Echo Request probes to the Anycast Monitoring IP address.

Note: To ensure that all HTTP(S) traffic is processed by Forcepoint ONE SSE, it is recommended to block QUIC and HTTP(S) on any other port than 80 or 443. Drag the Primary and Secondary Tunnel as preferred policies.

- Drag the **Primary** and **Secondary Tunnel** as preferred policies.



- Create an **Overlay ACL** rule to match Transmission Control Protocol (TCP) ports 80 and 443 and other rules to match ICMP protocol with Anycast Monitoring IP.



- Complete changes by **Saving** and **Deploying** them in the EdgeConnect appliance.

## Configure IP SLA

Configure the IP SLA where the Secondary Tunnel is only enabled when the Primary Tunnel is down. Forcepoint ONE supports Anycast IP monitoring using ICMP echo probes.

Note: It is recommended to create a loopback pool to be used by the EdgeConnect appliances as the source IP for the IP SLA probes.

The screenshot shows the IP SLA configuration page for an EdgeConnect device. On the left, a table lists three monitors: one for the primary tunnel (IP 116.50.59.230) which is Up, and two for the secondary tunnel (IP 192.168.123.254) which are also Up. The primary tunnel monitor has a Keep Alive Time of 5 seconds. On the right, the configuration details for the primary tunnel monitor are shown:

- Monitor:** Ping (ON)
- Address:** 116.50.59.230
- Source:** Tunnel
- Source Interface:** Forcepoint-ONE-US-EAST-1A
- Ping Interval:** 5 Sec
- Sampling Window:** 300 Sec
- Reachability:** Mark Up after X Pings (2), Mark Down after X Failed Pings (3)
- Loss:** Mark Up after loss below X %, Mark Down after loss above X %
- Latency:** Mark Up after average latency below X Milli Sec, Mark Down after average latency above X Milli Sec
- Metric Combination:** OR
- Monitor sampling interval:** 60 Sec
- Actions:** Down action: Enable Tunnel (Forcepoint-ONE-US-EAST-1B), Up action: Disable Tunnel (Forcepoint-ONE-US-EAST-1B)
- Comment:** optional

A modal window titled "Up Stats" is open, displaying statistics for the tunnel monitor. It shows the last 17 hours and 8 minutes of activity, with 1 total up and 1 total down event. The modal includes "Save" and "Cancel" buttons.

## Verify Tunnel Status in Aruba SD-WAN

The screenshot shows the Aruba SD-WAN Tunnel Exception table. The table displays two rows of tunnel information:

| Appliance   | Segment | Passthrough Tunnel        | Admin Status | Charts | Status                | Local IP        | Remote IP     | Mode  | NAT  | Peer/Service    | Max BW K... | Advanc... |
|-------------|---------|---------------------------|--------------|--------|-----------------------|-----------------|---------------|-------|------|-----------------|-------------|-----------|
| edgeconnect | Default | Forcepoint-ONE-US-EAST-1A | up           | up /   | up - active           | 192.168.123.254 | 107.23.63.125 | IPSec | none | FONE-US-EAST-1A | 1000000(... | (i)       |
| edgeconnect | Default | Forcepoint-ONE-US-EAST-1B | up           | up /   | up + in site disabled | 192.168.123.254 | 52.201.134.75 | IPSec | none | FONE-US-EAST-1B | 1000000(... | (i)       |



[forcepoint.com/contact](http://forcepoint.com/contact)

## About Forcepoint

Forcepoint simplifies security for global businesses and governments. Forcepoint's all-in-one, truly cloud-native platform makes it easy to adopt Zero Trust and prevent the theft or loss of sensitive data and intellectual property no matter where people are working. Based in Austin, Texas, Forcepoint creates safe, trusted environments for customers and their employees in more than 150 countries. Engage with Forcepoint on [www.forcepoint.com](http://www.forcepoint.com), [Twitter](#) and [LinkedIn](#).