Delivering Secure Internet Service to Data Center, Campus, Branch, and Remote Locations

Arista and Microsoft partnering to integrate Microsoft's Security Service Edge (SSE) Solution into Arista CloudVision Pathfinder Solution

Overview

Arista Networks is partnering with Microsoft to integrate Microsoft's Security Service Edge (SSE) Solution into Arista CloudVision Pathfinder solution, delivering secure Internet service to Data Center, Campus, Branch and remote locations.

Customers that have Arista WAN Routing Systems and CloudEOS routers deployed at the edge of their network can now leverage this new capability to identify and select specific SaaS applications or all Internet-bound traffic and send that traffic to Microsoft Entra Internet Access for security inspection, providing users and workloads secure access to the Internet and software as a service (SaaS) applications.

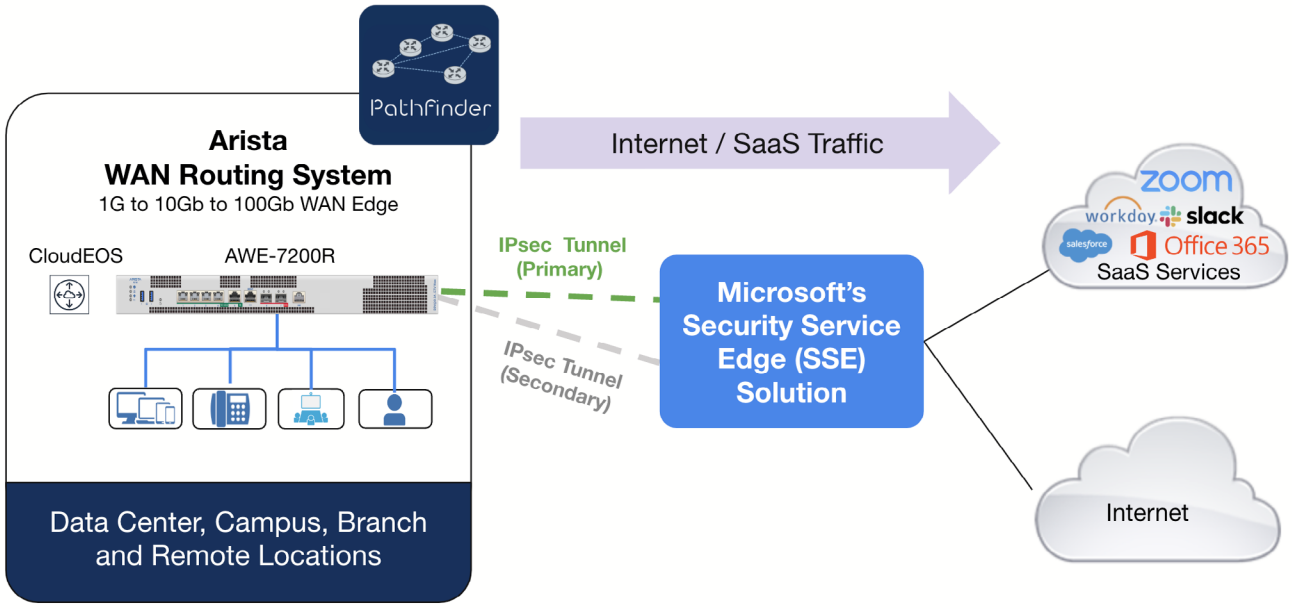

Figure 1: Arista CV-Pathfinder and Microsoft's SSE Solution Integration

The Integration has the following key benefits

- **Centralized Security Control with a Lower WAN Cost** - by sending Internet bound and SaaS applications traffic to Microsoft's SSE Solution, customers can use Microsoft Entra Internet Access to gain central control over security policy management and enforcement with consistency, also avoid backhauling traffic to a data center, reducing the network latency and the need of increasing WAN bandwidth to save cost.
- **Improving Application and User Experience** - the Arista CV Pathfinder solution monitors the health status of the IPsec tunnels to Microsoft Entra Internet Access endpoints to ensure an optimal application and user experience. Furthermore, An Active-Active dual router design option is also available at a site level to increase a reliable connection to Microsoft Entra Internet Access.
- **Enhanced Network Visibility and Monitoring** - on Arista CloudVision, customers can see and monitor the health of all the tunnels to Microsoft Entra Internet Access endpoints to easily identify if there is a network issue going on that might affect users and applications, as well as with the ability to go back to a certain point of time for troubleshooting purposes, and also being able to visualize on the topology page to see all the traffic going from the SD-WAN fabric to the Microsoft Entra Internet Access for Internet and SaaS application access.

Configuration Steps

As part of this integration users will configure a remote network on Microsoft Entra and an Arista Router (AWE-7200R or CloudEOS router). The following sections cover details about the configuration aspect for both.

Configure Remote Network on Microsoft Entra

1. Basics
   a. Sign into Microsoft Entra portal with this URL, https://entra.microsoft.com, with the credentials provided.
   b. Browse to **Global Secure Access -> Connect -> Remote Networks**
   c. Select **Create remote network** button to create a remote network. Add Name and Region for the remote network. Region specified the Azure region to which the other end of the tunnel will connect to. Select Next to configure link connectivity

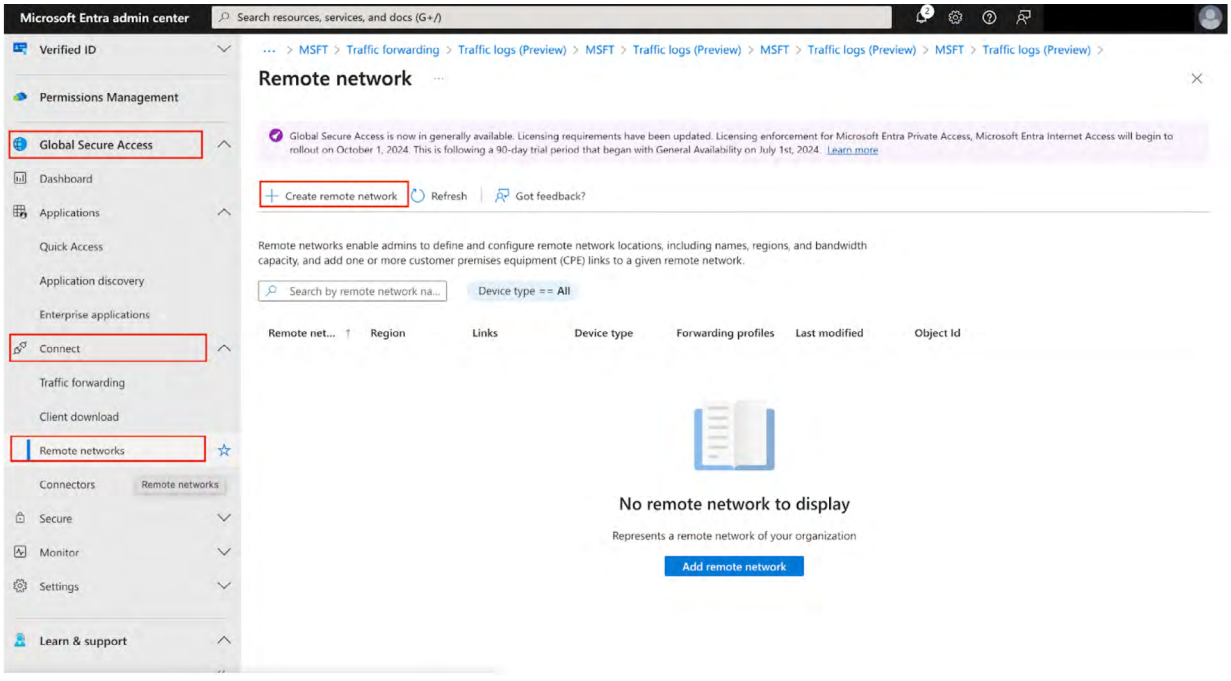

Figure 2: Create a Remote Network

d. Add **Name** and **Region** for the remote network. Region specified the Azure region to which the other end of the tunnel will connect to. Select **Next** to configure link connectivity

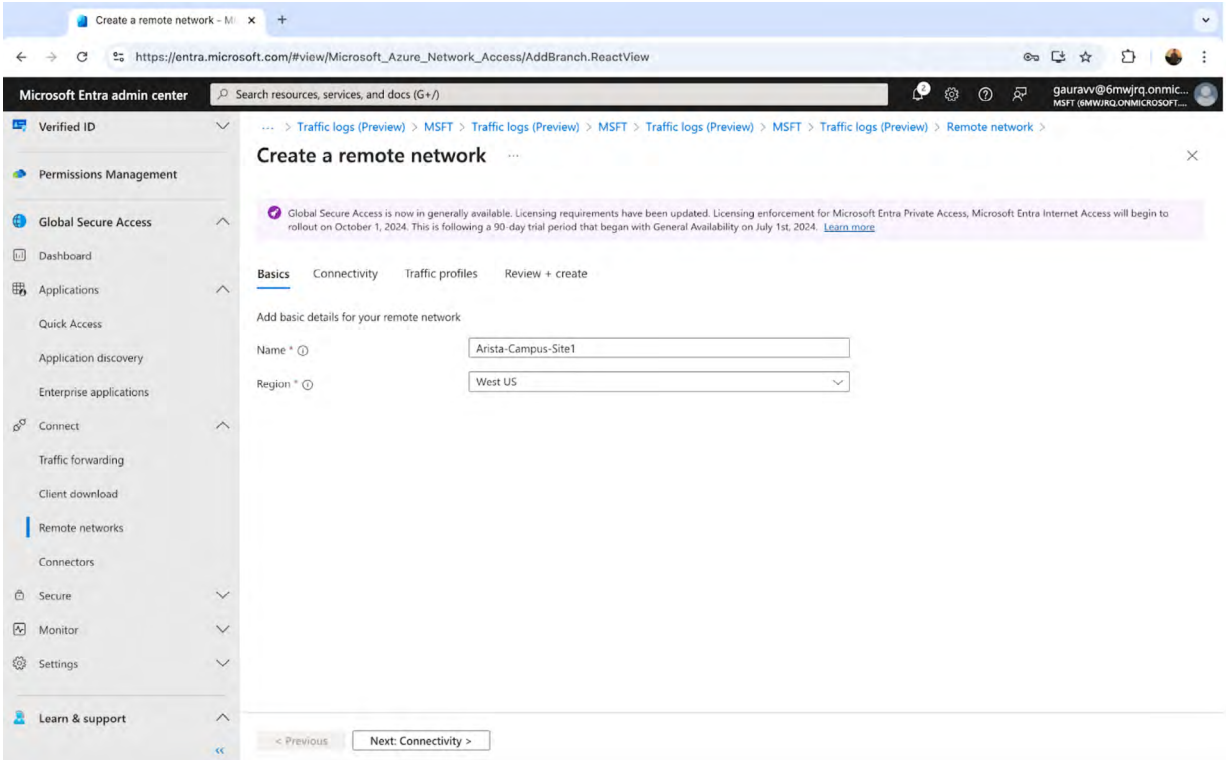

Figure 3: Add Name and Region

2. Setup IPsec tunnel

a. Select **Add a link** and add link name, Device type as other, Device's public IP address. On Arista's branch routers, we use Application Traffic Recognition and Internet Exit features to identify internet bound traffic and redirect it through IPsec tunnels to their appropriate Microsoft Entra endpoints. Therefore, BGP configuration on an Arista router is not required, we recommend using any private IP address in RFC1918 space and ASN here.

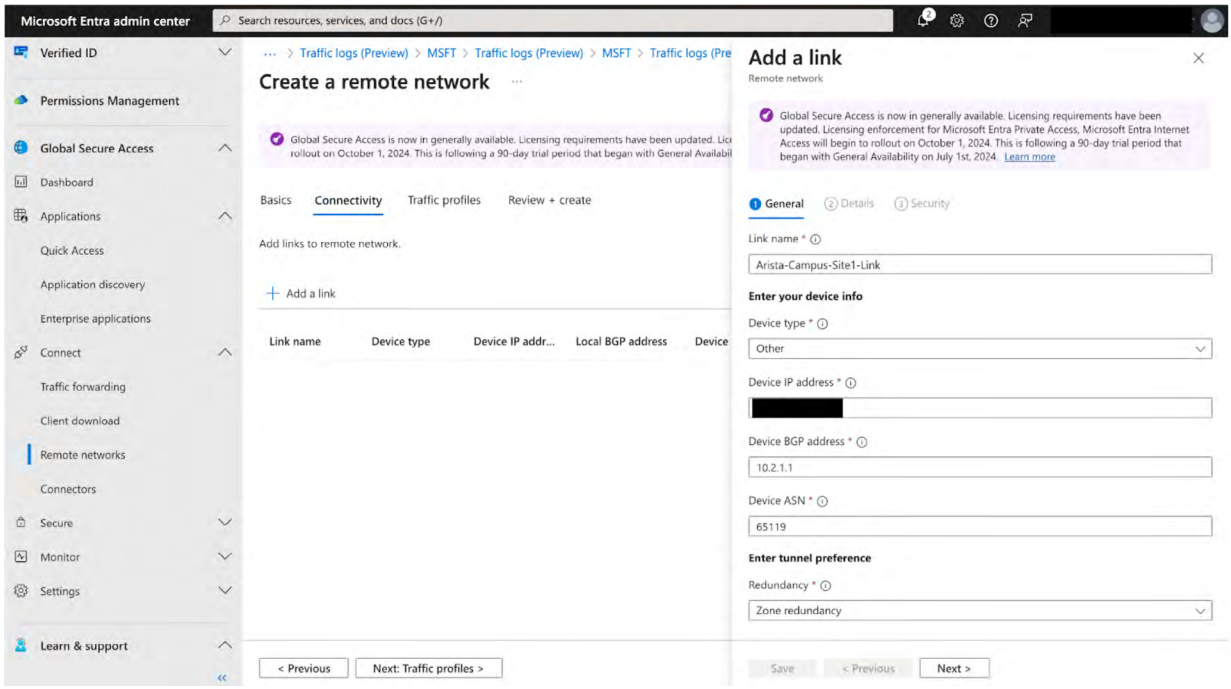

Figure 4: Add a Link

b. Select **Redundancy** option. The recommendation is to select zone-level redundancy so that a primary and secondary tunnel can be configured on the Arista device. Provide a private IP address in RFC1918 space for the local BGP address (This configuration setting was not applied in the Arista router due to the reason previously mentioned.). Select **Next** to configure IPsec tunnel

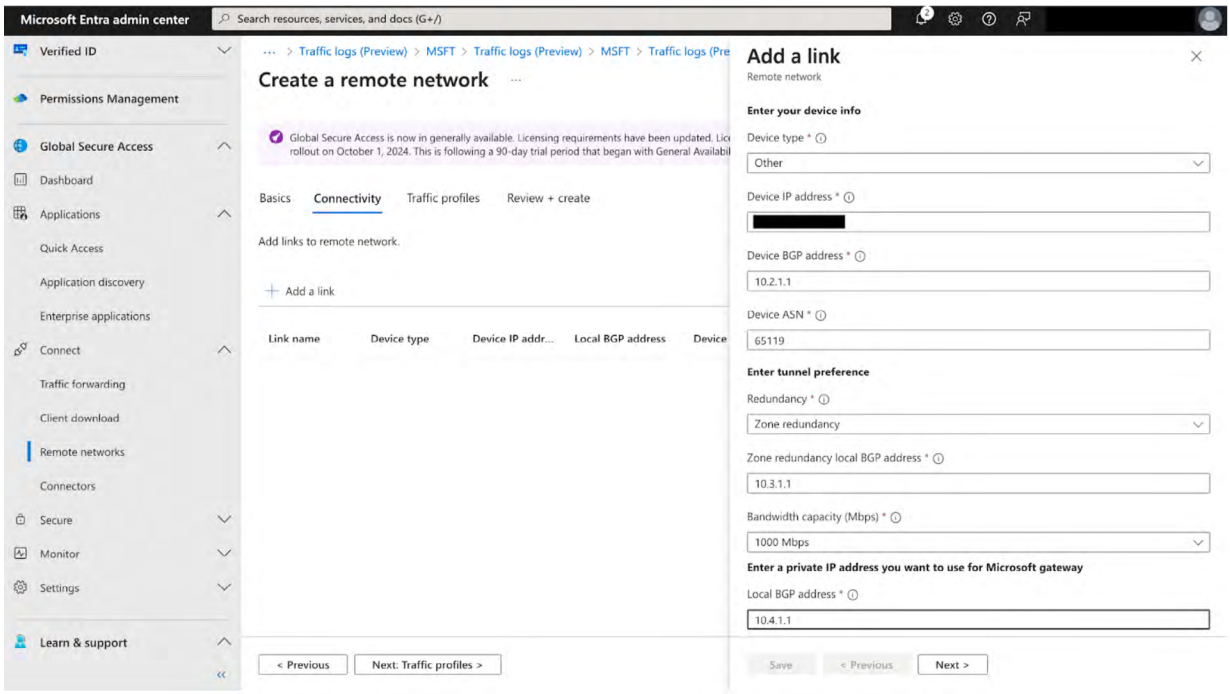

Figure 5: Add BGP

c. Select either a default or a custom IPSec/IKE policy. In the example below we select a default IPSec/IKE policy and use a corresponding encryption profile on the Arista device.

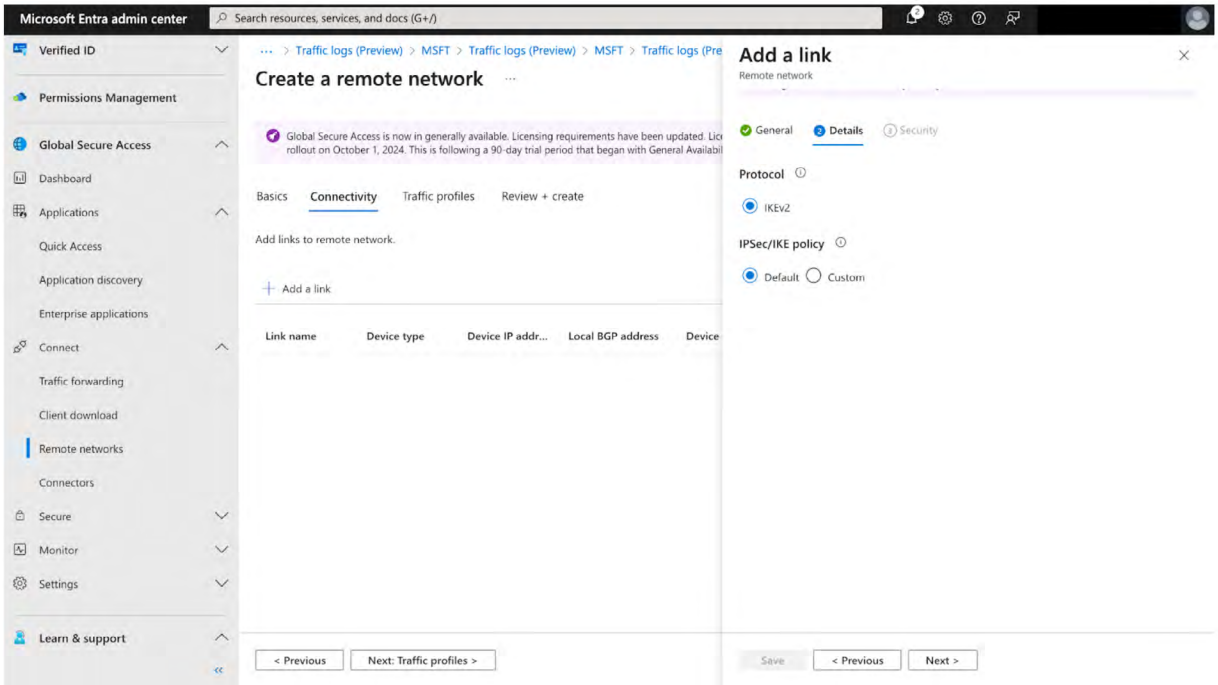

Figure 6: Select IPSec and IKE Policy

d. Click Next to add the **Pre Shared key** for the primary and redundancy. The same Pre Shared key needs to be configured on the Arista device. Click **Save** and associate a traffic profile.

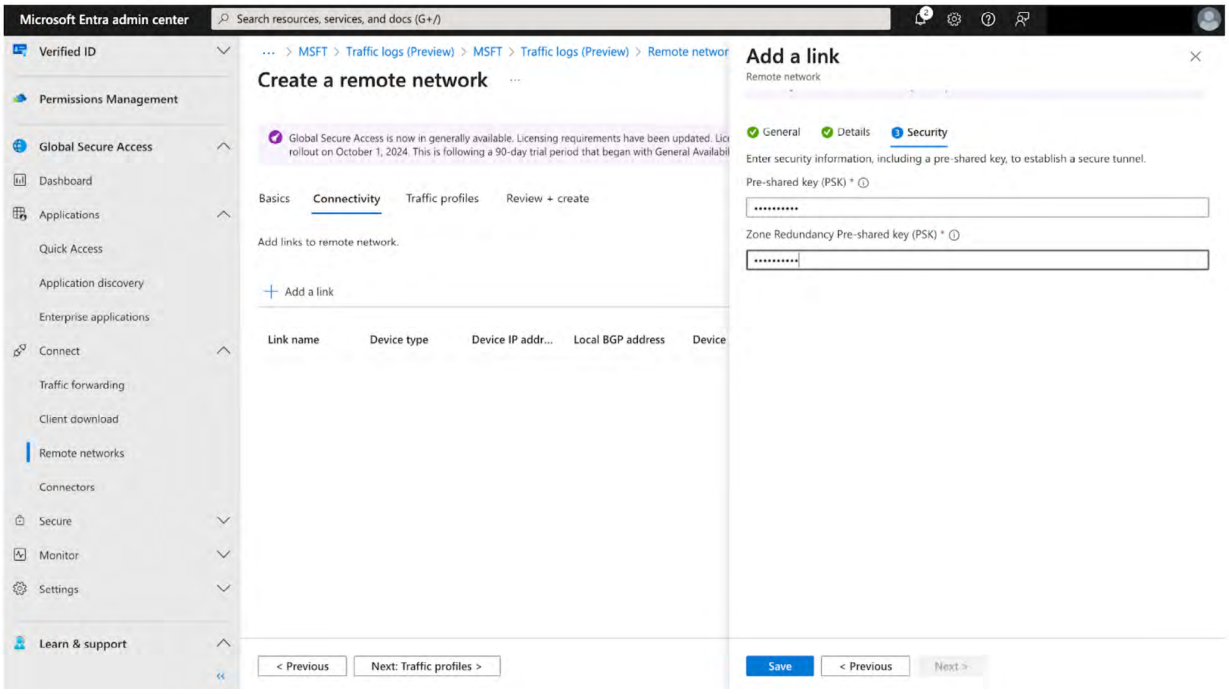

Figure 7: Add Pre-shared Key

3. Associate Traffic Profile

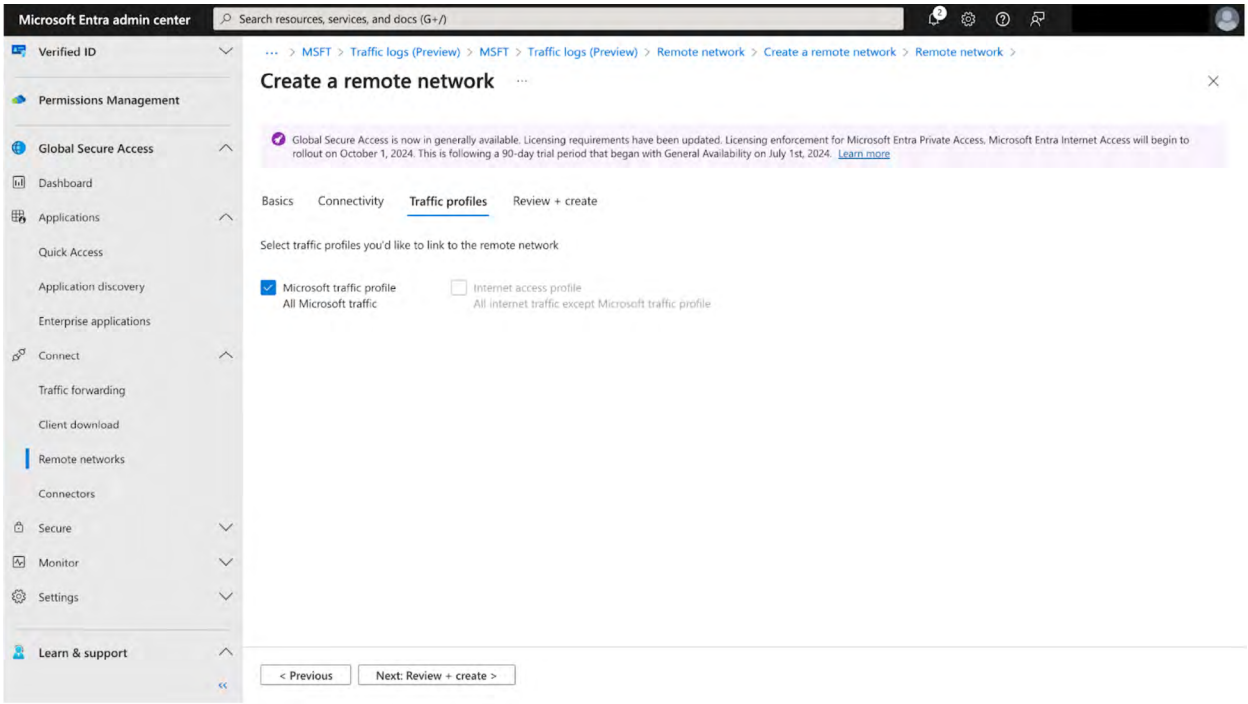

Figure 8: Associate Traffic Profile

4. Review and Create

   a. Click Create Remote network to finally submit the entered configuration and create a remote network.

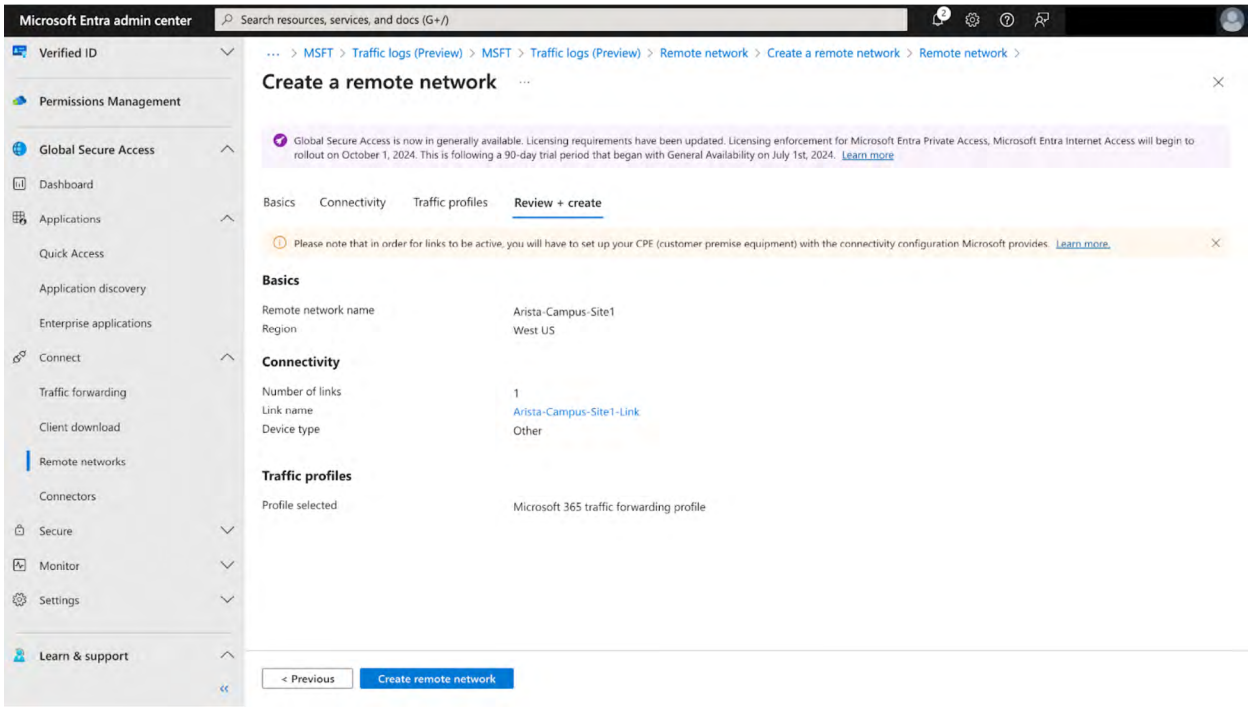

Figure 9: Submit Request

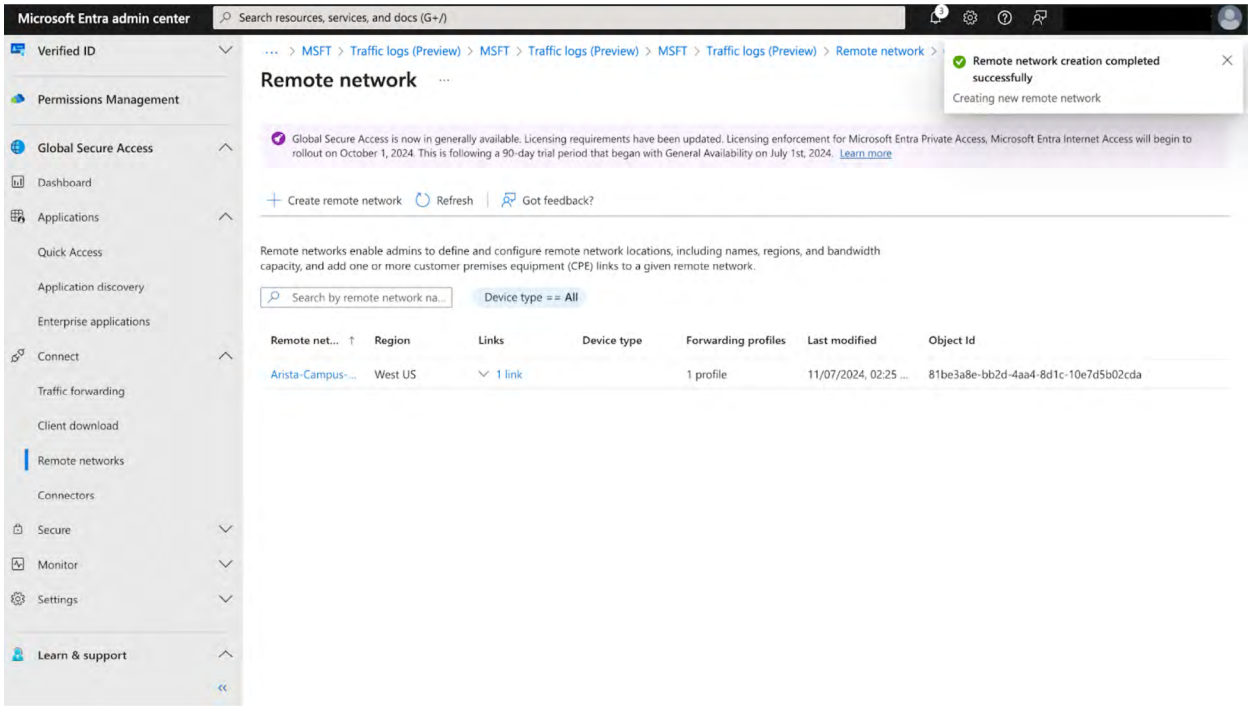

Figure 10: Remote Network Successfully Created

5. Review and Create

   a. Once the remote network has been successfully created, view the list of remote networks and scroll to the right to view the configuration.

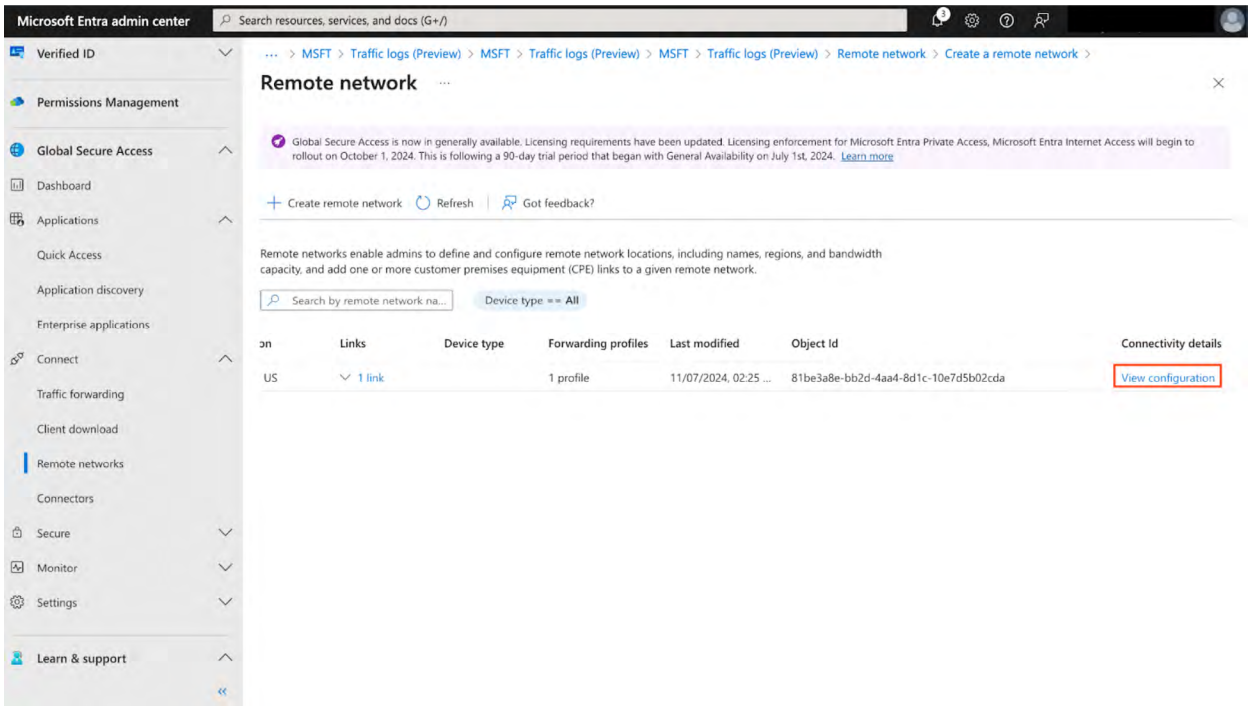

Figure 11: View Remote Network Configuration

   b. Note the two endpoints marked in red. This will be the tunnel destination for the primary and secondary tunnels on Arista's router.

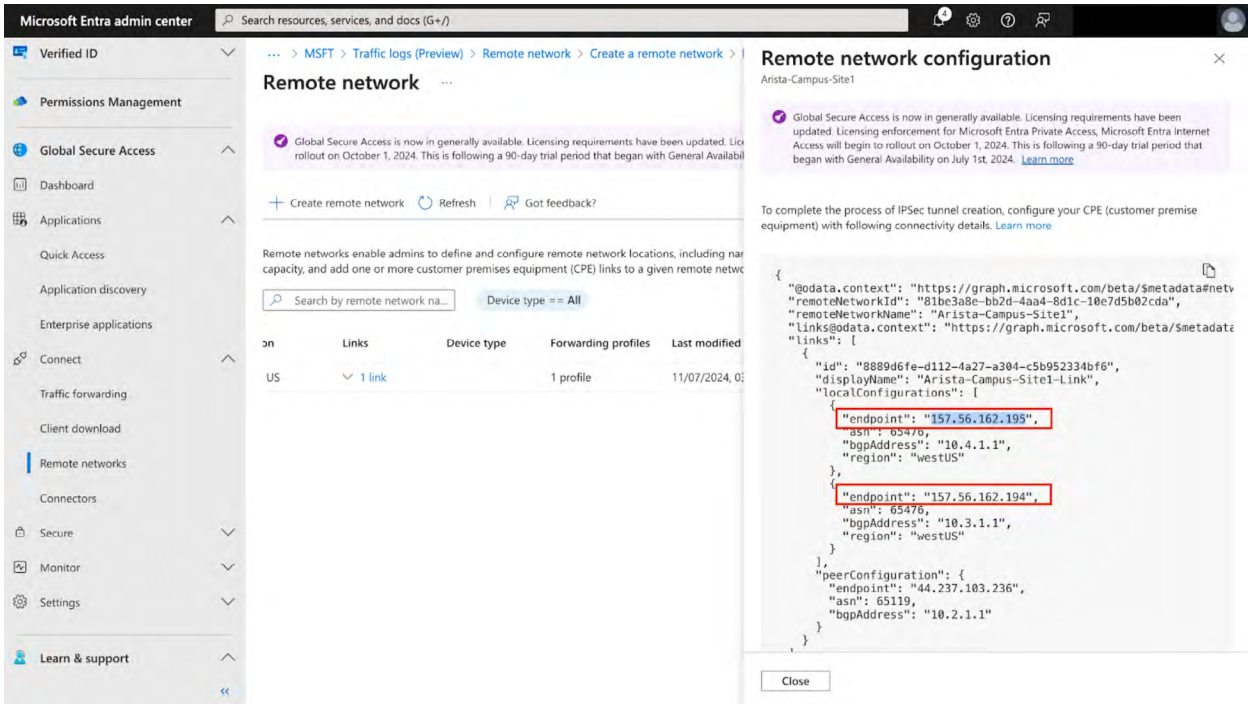

Figure 12: Remote Network Configuration Template

Configure Arista WAN Router

1. Configure Interfaces

   In this example, the LAN network is part of a non-default VRF. Ethernet1 is the WAN interface and Ethernet2 is facing LAN and is in VRF green.

```
interface Ethernet1
   description Internet
   no switchport
   ip address dhcp
   dhcp client accept default-route
!
interface Ethernet2
   no switchport
   vrf green
   ip address dhcp
```

2. Configure port-only NAT

   On Arista routers, port-only NAT is configured to preserve the LAN IP addresses and also map the reverse traffic to the appropriate VRFs. This NAT configuration needs to be applied to the Tunnel interfaces which we will create later in this deployment guide.

```
ip nat profile VRF-AWARE-NAT
   ip nat source dynamic access-list ALLOW-ALL pool PORT-ONLY-POOL
!
ip access-list ALLOW-ALL
   10 permit ip any any
!
ip nat pool PORT-ONLY-POOL port-only
   port range 1500 65535
!
```

3. Configure IPsec

   To configure IPsec on an Arista WAN device, users need to configure IKE and SA policies along with an IPsec profile. For the default configuration on Microsoft Entra, dh-group 24 and encryption as **aes256gcm128** should be configured. In the Ike policy local-id should be set to the public IP address of the WAN interface.

```
ip security
   ike policy ms-ike
      dh-group 24
      local-id 44.237.103.236
   !
   sa policy ms-sa
      esp encryption aes256gcm128
   !
   profile ms-ipsec
      ike-policy ms-ike
      sa-policy ms-sa
      connection start
```

```
      shared-key @TEST-PRESHARED-KEY
      !
      flow entropy udp
   !
```

4. Configure Tunnel Interfaces

   a. Tunnel source : Should be set to the WAN interface name

   b. Tunnel destination: these IP addresses are the same that we get after selecting the **view configuration** link of the remote network on Microsoft Entra login.

   c. Attach the previously configured NAT and IPsec profiles.

   d. Set the IP address to unnumbered Loopback0 so that the tunnel interface uses the same IP address as that of the Loopback interface.

   In the example below, two tunnel interfaces are created one as a primary and the other as a secondary interface.

```
interface Loopback0
   description Router_ID
   ip address 10.254.100.7/32
interface Tunnel100
   mtu 1394
   ip address unnumbered Loopback0
   ip nat service-profile VRF-AWARE-NAT
   tunnel mode ipsec
   tunnel source interface Ethernet1
   tunnel destination 157.56.162.194
   tunnel ipsec profile ms-ipsec
!
interface Tunnel101
mtu 1394
   ip address unnumbered Loopback0
   ip nat service-profile VRF-AWARE-NAT
   tunnel mode ipsec
   tunnel source interface Ethernet1
   tunnel destination 157.56.162.195
   tunnel ipsec profile ms-ipsec
!
```

5. Configure Connectivity Monitor

   For monitoring a host through the IPsec tunnel, users can use the ICMP probes using ip configuration. In the example below we will monitor 8.8.8.8. These hosts will be attached to the service-insertion configuration as shown in the next step.

```
monitor connectivity
   no shutdown
   interface set MS-SSE-PRI Tunnel100
   interface set MS-SSE-SEC Tunnel101
   !
   host MS-SSE-HOST-PRI
```

```
      local-interfaces MS-SSE-PRI
      ip 8.8.8.8
!
   host MS-SSE-HOST-SEC
      local-interfaces MS-SSE-SEC
      ip 8.8.8.8
   !
```

6. Configure Service Insertion

   As part of the service-insertion configuration, add the tunnel interfaces as primary and also attach monitor connectivity configuration.

```
router service-insertion
   connection IE-Tunnel100
      interface Tunnel100 primary
      monitor connectivity host MS-SSE-HOST-PRI
   !
   connection IE-Tunnel101
      interface Tunnel101 primary
      monitor connectivity host MS-SSE-HOST-SEC
   !
```

7. Configure Internet Exit

```
router internet-exit
   exit-group MS-IE-EXIT-PRI
      local connection IE-Tunnel100
   !
   exit-group MS-IE-EXIT-SEC
      local connection IE-Tunnel101
   !
   policy MS-IE-EXIT-POLICY
      exit-group MS-IE-EXIT-PRI
      exit-group MS-IE-EXIT-SEC
      exit-group system-default-exit-group
!
```

8. Configure Application traffic recognition

```
application traffic recognition
   application-profile MSFT
      application microsoft
      application ms_teams
      application office365
   !
```

9. Configure Adaptive virtual topology

```
router adaptive-virtual-topology
   topology role transit region
   region US id 1
   zone US-ZONE id 1
   site Arista-Campus-Site1 id 501
   !
   policy AVT-POLICY-VRF-GREEN
      match application-profile MSFT
         avt profile AVT-POLICY-VRF-GREEN-MSFT
      !
      match application-profile default
         avt profile AVT-POLICY-VRF-GREEN-MSFT
   !
   profile AVT-POLICY-VRF-GREEN-MSFT
      internet-exit policy MS-IE-EXIT-POLICY
      path-selection load-balance LB-AVT-POLICY-VRF-GREEN-DEFAULT
   !
   vrf green
      avt policy AVT-POLICY-VRF-GREEN
      avt profile AVT-POLICY-VRF-GREEN-MSFT id 10
```

Verification

The following section shows different visibility components that are available on Arista's CloudVision Portal as well as on the Microsoft Entra Visibility Dashboard.

For this, we initiated connections from a host connected directly to the Arista router (Arista-Campus-Site1) to two Microsoft services, Microsoft Teams, and Microsoft Outlook.

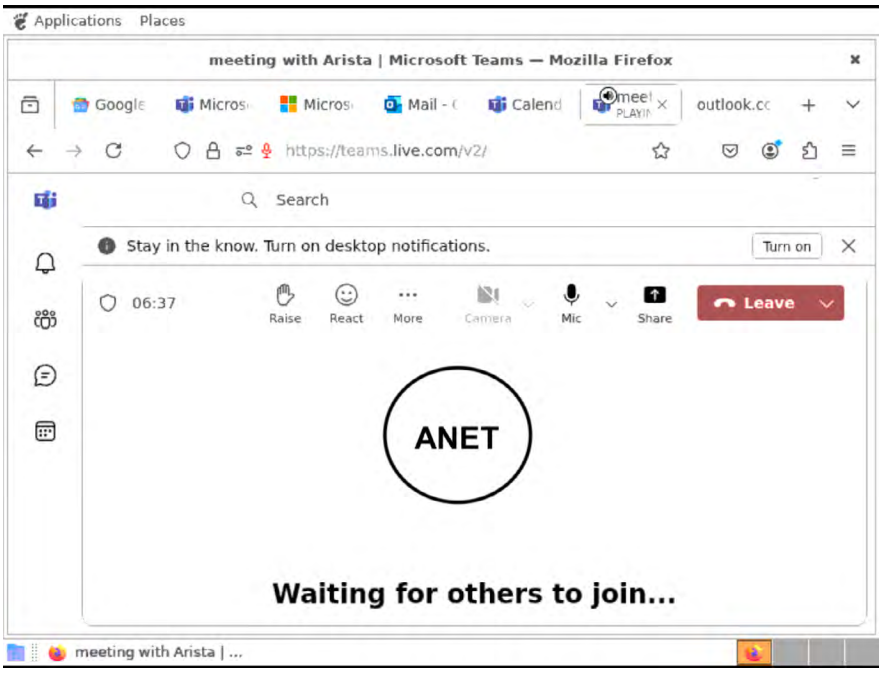

Figure 13: Access Microsoft Teams and Outlook

The images below show traffic logs for Microsoft Teams and Microsoft Outlook access.

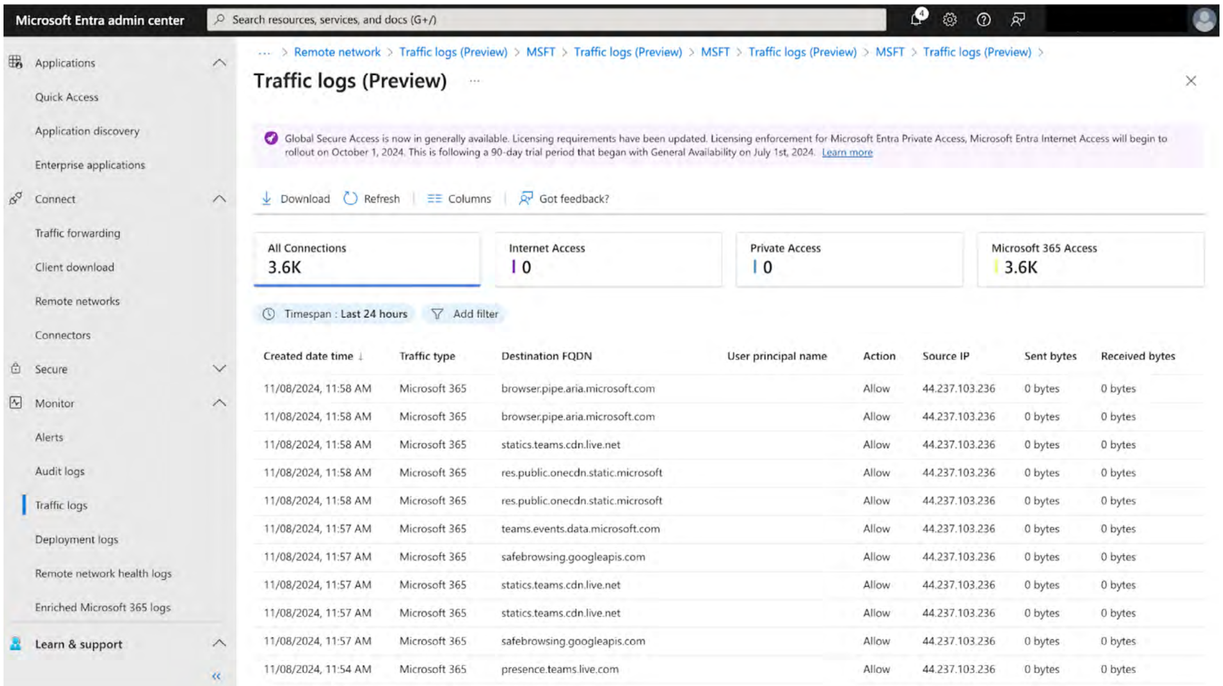

Figure 14: Microsoft Entra Traffic Logs for Microsoft Teams

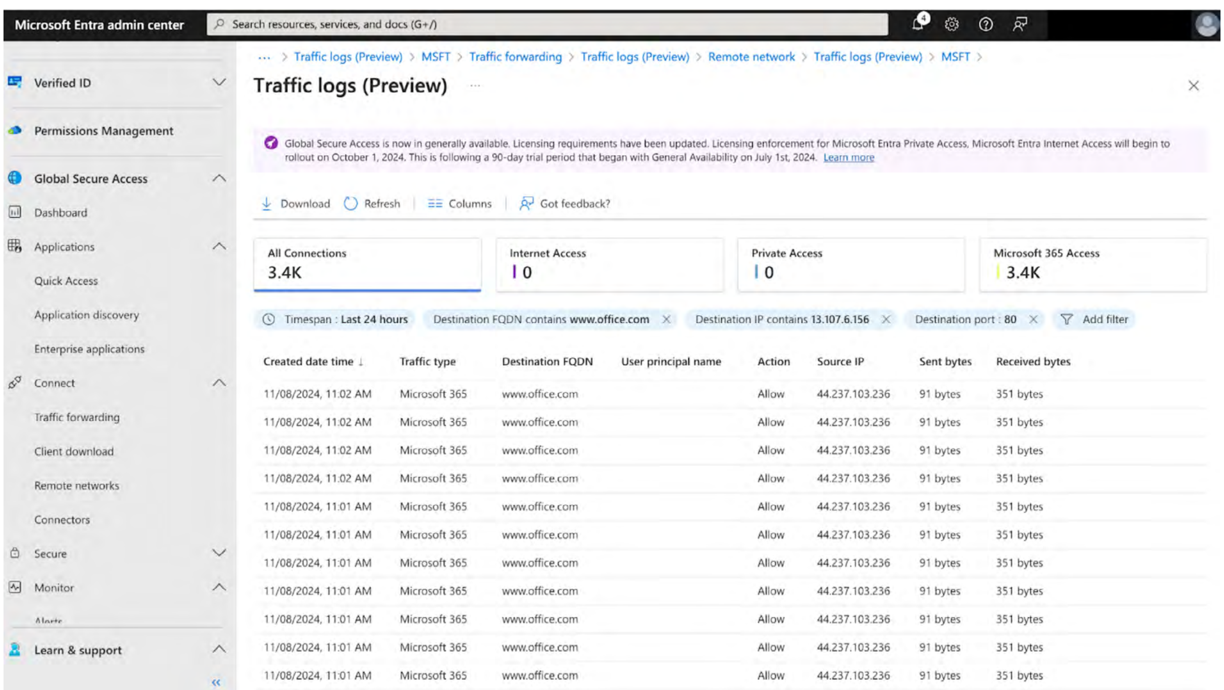

Figure 15: Microsoft Entra Traffic Logs for Microsoft Office

Arista CloudVision Visibility

Viewing IPsec Tunnel to Microsoft Entra on the Topology Page

The image shown below has the topology view where two IPsec tunnels are formed between Arista-Campus-Site1 and the Microsoft Entra IPsec endpoints.

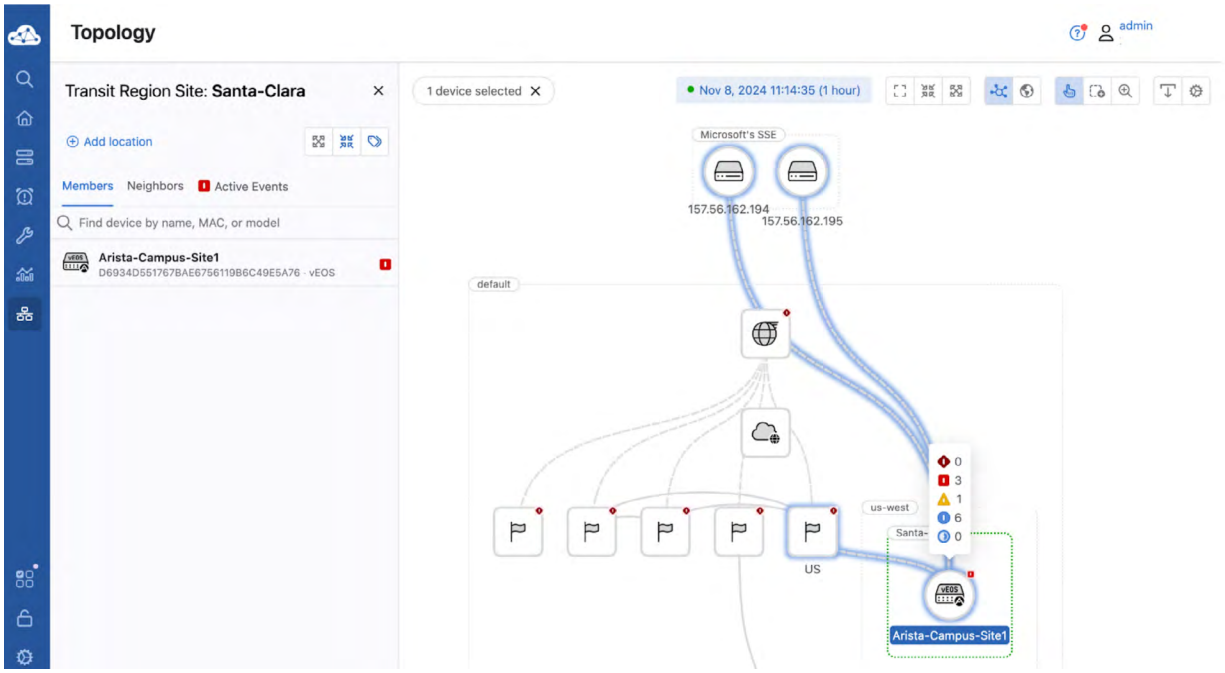

Figure 16: View IPsec Tunnel to Microsoft Entra on CloudVision Topology Page

Viewing Traffic Flows Going to Microsoft Entra via the IPsec Tunnel

The Arista router supports sending IPFIX data to CloudVision for visualization purposes. The image below displays one of the application flows from a host (**10.0.2.196**) to a Microsoft SaaS service that goes over the IPsec tunnel. In the left pane, further details about the flow are shown such as the ingress and egress interfaces and the packet counts.

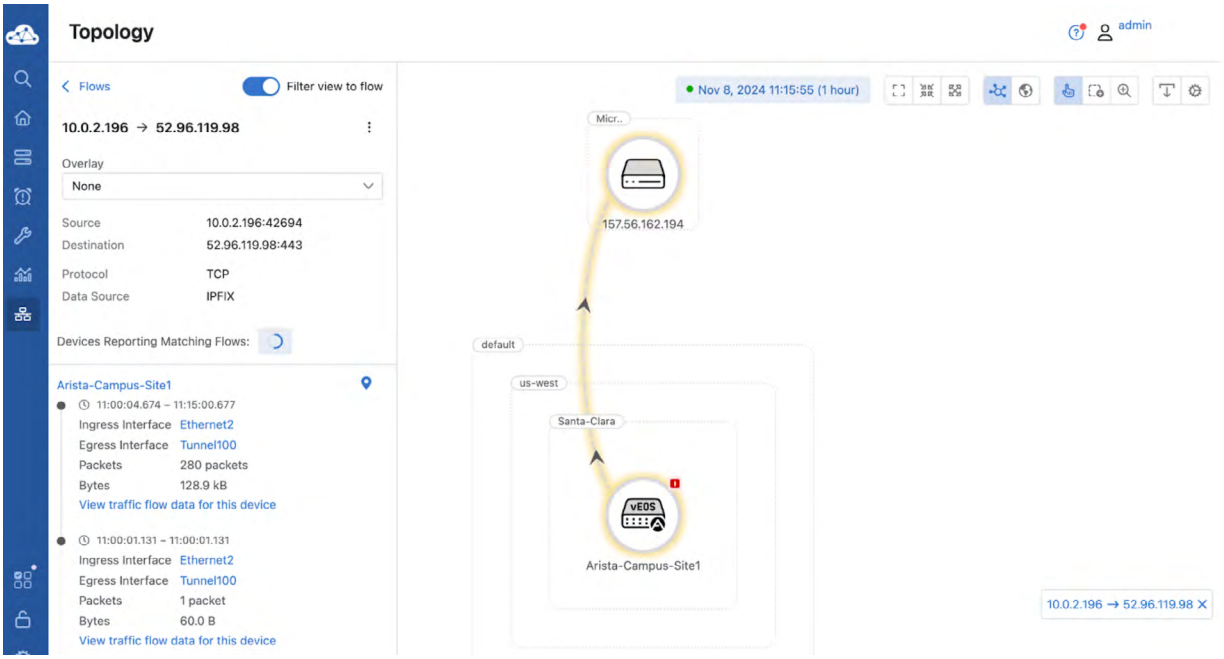

Figure 17: Viewing Traffic Flows Going to Microsoft Entra via the IPsec Tunnel

Check Tunnel Statistics

Customers can monitor the IPsec tunnel status, rates, and counters on CloudVision. The image below shows the tunnel statistics for one of the two tunnels (Tunnel100), formed between the Arista WAN router and Microsoft Entra endpoints.

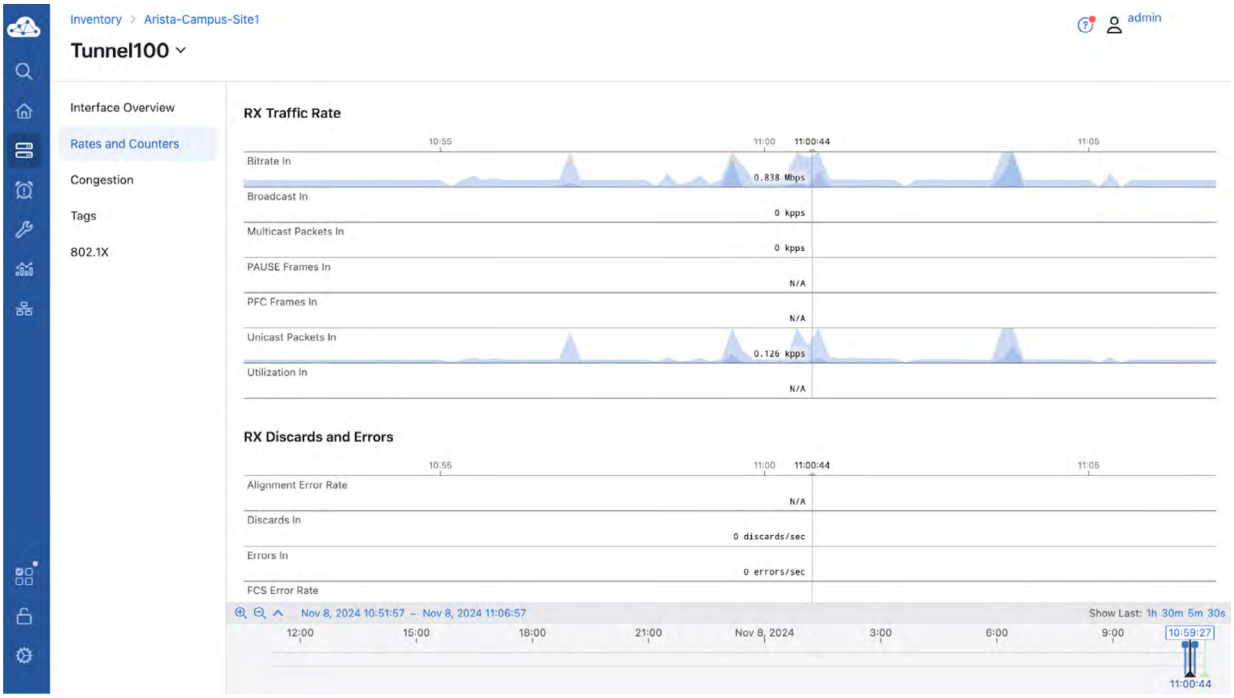

Figure 18: IPsec Tunnel Statistics

Check Tunnel Network Performance

Connectivity Monitor monitors the health status and network performance of the tunnel connecting to the Microsoft Entra endpoint. This includes packet loss, jitter, and latency information. The image below shows the loss percentage (0 percentage) of the two Tunnels.

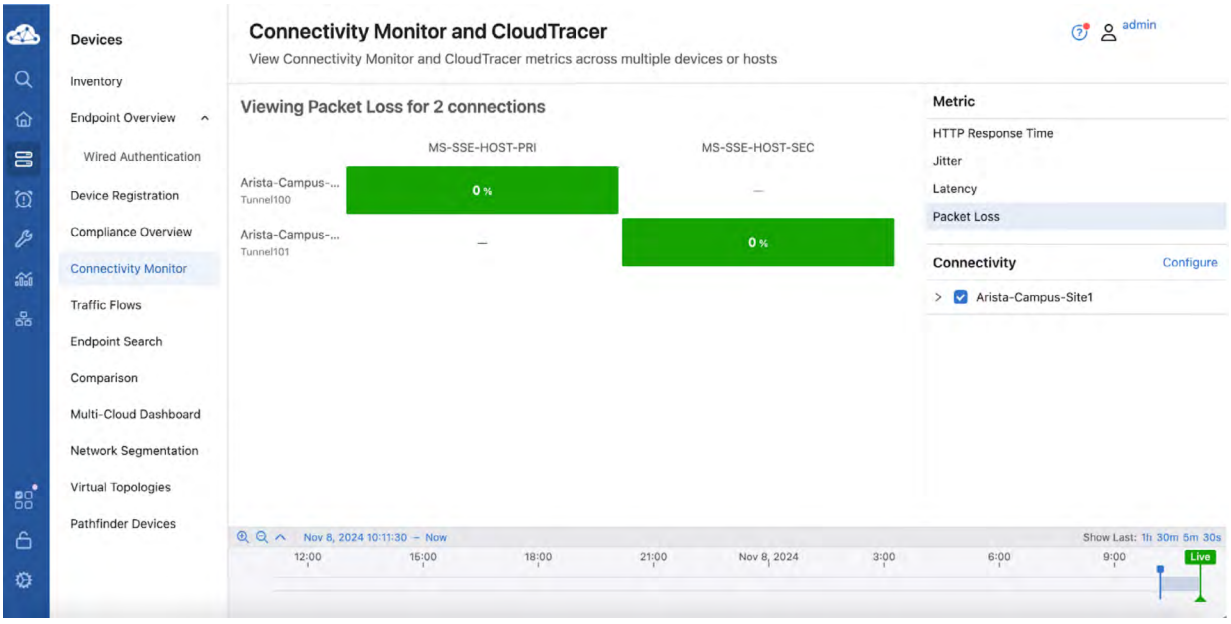

Figure 19: IPsec Tunnel Health and Packet Loss Stats

Summary

With this integration, customers can easily provide secure Internet access to their data centers, campuses, branches, and remote locations using Arista CV-Pathfinder and Microsoft's SSE solution.

Santa Clara—Corporate Headquarters
5453 Great America Parkway,
Santa Clara, CA 95054

Phone: +1-408-547-5500
Fax: +1-408-538-8920
Email: info@arista.com

Ireland—International Headquarters
3130 Atlantic Avenue
Westpark Business Campus
Shannon, Co. Clare
Ireland

Vancouver—R&D Office
9200 Glenlyon Pkwy, Unit 300
Burnaby, British Columbia
Canada V5J 5J8

San Francisco—R&D and Sales Office 1390
Market Street, Suite 800
San Francisco, CA 94102

India—R&D Office
Global Tech Park, Tower A, 11th Floor
Marathahalli Outer Ring Road
Devarabeesanahalli Village, Varthur Hobli
Bangalore, India 560103

Singapore—APAC Administrative Office
9 Temasek Boulevard
#29-01, Suntec Tower Two
Singapore 038989

Nashua—R&D Office
10 Tara Boulevard
Nashua, NH 03062