

Juniper NCE-511 AI-Driven SD-WAN Reference Architecture User Guide

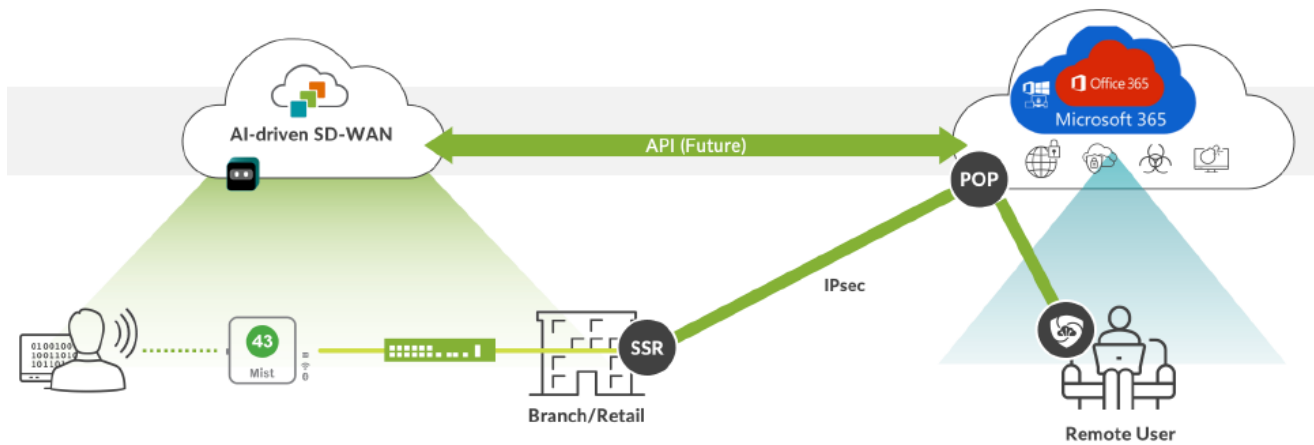
[Home](#) » [JUNIPer](#) » Juniper NCE-511 AI-Driven SD-WAN Reference Architecture User Guide 

Contents

- [1 Juniper NCE-511 AI-Driven SD-WAN Reference Architecture](#)
- [2 Product Usage Instructions](#)
- [3 Configuration Basics](#)
- [4 Configure IPsec Tunnel](#)
- [5 Create Application](#)
- [6 Update WAN Edge Template](#)
- [7 Single WAN Link with Zone Redundancy on the Microsoft SSE Solution](#)
- [8 FAQ](#)
- [9 Documents / Resources](#)
 - [9.1 References](#)



Juniper NCE-511 AI-Driven SD-WAN Reference Architecture



Specifications

- **Product Name:** Juniper AI-Driven SD-WAN
- **Integration:** Microsoft's SSE Solution
- **Published Date:** 2024-12-16

Product Information

The Juniper AI-Driven SD-WAN integrates with Microsoft's SSE Solution to provide network configuration examples for deployment scenarios. The solution offers benefits such as improved network performance and optimized deployment planning.

Product Usage Instructions

Configuration Workflow

The configuration example involves creating and deploying a basic branch template for device connectivity. Prior to configuration, ensure you have the necessary information for each site, including WAN link addresses, BGP peering address ranges, BGP AS number, access permissions, bandwidth requirements, and redundancy model.

Configuration Basics

1. Create a basic branch template for device connectivity.
2. Configure the IPsec tunnel.
3. Associate traffic profiles.
4. View the network profile.
5. Create applications.
6. Update WAN Edge templates.
7. Verify operation.

Configuration Options

Multiple configuration options are available with varying redundancy levels. Depending on the setup, you can configure single or dual WAN links with Microsoft's SSE Solution. Ensure to follow the specified guidelines for WAN Edge and Microsoft's SSE Solution configurations.

Juniper AI-Driven SD-WAN and Microsoft's SSE Solution Integration—Network Configuration Example (NCE)

Juniper Networks Network Configuration Example (NCE) describes how to configure and deploy Juniper products in a typical use case scenario. In this NCE, you'll find use case scenario with the topology, configuration

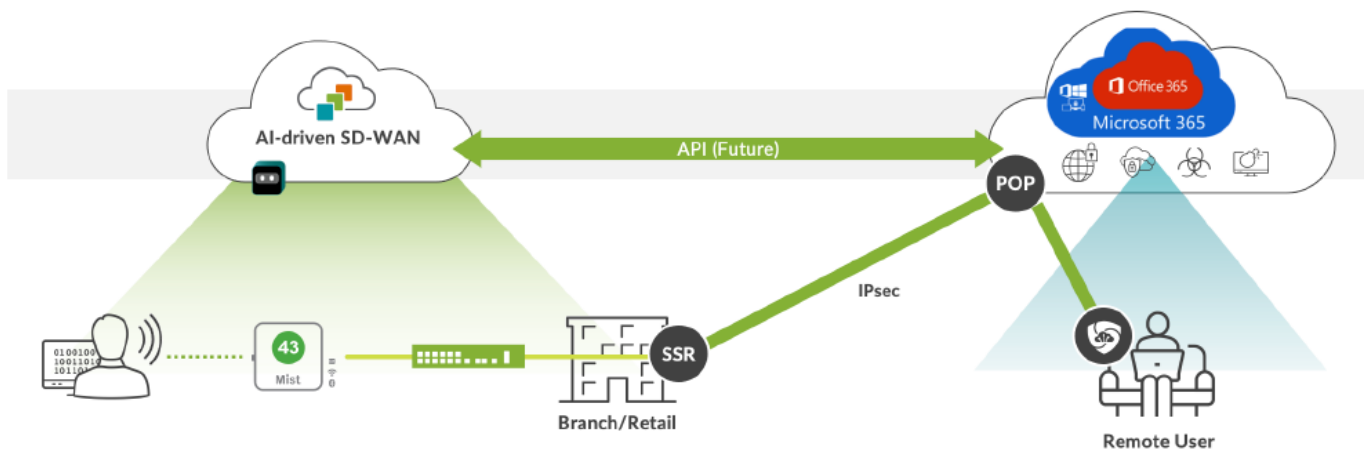
information, and validation output for the configuration. Read further to plan and optimize your network deployment.

Solution Benefits

- This network configuration example (NCE) describes the integration that you can achieve between Juniper AI-Driven SD-WAN and Microsoft's SSE solution. The NCE describes the benefits of integrating the solutions and provides multiple example configurations including verification steps.
- Microsoft's cloud-based Secure Service Edge (SSE) solution includes Microsoft Entra Internet Access and Microsoft Private Access, under the Global Secure Access brand. The Juniper AI-Driven SD-WAN solution provides seamless access to Microsoft's SSE solution from branch and office locations. This integration is automated using scalable device templates to ease the operational burden of deploying the service to many sites. This guide describes how to configure both Microsoft's SSE solution and the Juniper Mist WAN Edge template for connectivity.

This document enables the topology shown in Figure 1 on page 2. An IPsec tunnel is configured between the Juniper AI-Driven SD-WAN device, also known as the Juniper Session Smart Router (SSR), and Microsoft's SSE solution using the Secure Edge Connector within the WAN Edge template. Additionally, a BGP over IPsec connection is configured to dynamically learn routing destinations from Microsoft's SSE solution. When used for Microsoft 365 access, Microsoft's SSE solution-advertised addresses are used to determine the traffic sent to the service rather than the WAN Edge-based application dictionary.

Figure 1: Integration with Microsoft's SSE Solution



Configuration Workflow

The sequence of tasks in this configuration example:

1. Create and deploy a basic branch template for device connectivity. Creation of the basic template is out of scope of this guide, but the WAN Edge template might be stand-alone or SD-WAN with security enabled.
2. Configure a remote network within the Microsoft Entra portal. This defines the IPsec tunnel characteristics and define routing endpoints for reachability.
3. Configure a Secure Edge Connector in the device template. This creates a custom IPsec tunnel to Microsoft's SSE solution and defines encryption parameters.
4. Configure a BGP peer for Microsoft's SSE solution service to learn Microsoft 365 destinations dynamically.
5. Configure an application to allow traffic to be steered toward the IPsec tunnel. This application will be used in

application policy to allow client networks to access the BGP learned routes.

6. Configure an application policy with a network and application, but no traffic steering policy to indicate to the WAN Edge that the routing table should be used for learned destinations.

Configuration Planning

Prior to configuration, the following information must be available for each site:

1. The public address of the WAN links that are used to reach Microsoft's SSE solution service. At this time, only static WAN addresses might be used to reach the service.
2. One or two /29 address ranges that are available for BGP peering between the WAN Edge loopback and Microsoft's SSE solution. When zone redundancy is desired, two address ranges are required.
3. A BGP AS for use by Microsoft's SSE solution. This might be in the private AS range unused elsewhere in the enterprise network.
4. Networks and users that are granted access to Microsoft's SSE solution.
5. Bandwidth desired for each site. This is used in remote network configuration within the Microsoft Entra portal.
6. Desired redundancy model for each site. Options include single/dual WAN for the WAN Edge and single/dual Zone for Microsoft's SSE solution. The single/dual WAN configuration might be used with either a single SSR or HA SSR.

Configuration Options and Workflows

Several configuration options are available with varying levels of redundancy. For the Juniper SSR WAN Edge, it is possible to configure a single node with either one or two WAN interfaces connected to Microsoft's SSE solution. A dual node HA SSR router should be configured with two WAN interfaces connected to Microsoft's SSE solution.

NOTE: When zone redundancy is configured on the Microsoft's SSE solution, then two BGP peers are configured as routing neighbors across a single tunnel.

Three configuration options are covered in this guide:

1. Single WAN link and peer on the Microsoft's SSE solution. This configuration might be used for small deployments and testing when redundancy is not required.
2. Single WAN link with zone redundancy on the Microsoft's SSE solution. This configuration does not provide redundancy on the SSR WAN Edge but does cover failure of an availability zone on the Microsoft's SSE solution. This option is included to illustrate how two BGP peers might be configured across the same IPsec tunnel.
3. Dual WAN link using an HA SSR with zone redundancy per tunnel on the Microsoft's SSE solution. This provides the maximum level of redundancy for both the WAN Edge and Microsoft's SSE solution. Failure of an SSR node, WAN link or Microsoft availability zone does not impact the flow of traffic in this configuration.

Additional redundancy and WAN link variations might be configured using the basic configuration building blocks described for each of these variations.

Single WAN Link and Peer on Microsoft's SSE Solution

This configuration option is illustrated in the diagram below.



Microsoft Entra
SSE

Configuration Basics

Sign into Microsoft Entra portal with this URL, <https://entra.microsoft.com>, using credentials with administrative permissions to configure Microsoft's SSE solution.

1. On the Microsoft Entra Portal, navigate to Global Secure Access > Devices > Remote network.
2. Select Create remote network and provide Name and Region details. Region specifies the Azure region where the other end of your tunnel will be (one end being the WAN Edge SSR router at the branch).
3. Click Next.

CREATE A REMOTE NETWORK

Basics Connectivity Traffic profiles Review + create

Add basic details for your remote network

Name * ⓘ

Region * ⓘ

Configure IPsec Tunnel

1. Select the + Add a link button.
2. **Enter the following details:**
 1. Link name: Name of your WAN Edge device.
 2. Device type: Choose one of the options from the drop-down list (Other or Juniper).
 3. Device IP address: Public IP address of the WAN link used to connect to Microsoft.
 4. Device BGP address: The border gateway protocol address of the WAN Edge. This will be the Local BGP address of the WAN Edge and will be within the /29 range selected for connectivity. The reverse peer configuration will be done in Entra portal.
 5. Device ASN: Provide the autonomous system number of the WAN Edge network. By default, this value is 65000 but might be modified using Mist APIs.
 6. Redundancy: Select either No redundancy or Zone redundancy for your IPsec tunnel. If you select Zone redundancy, then another unique zone redundant local BGP address is configured.
NOTE: Microsoft limits configuration to a list of valid ASNs.
 7. Bandwidth capacity (Mbps): Choose the bandwidth for your IPsec tunnel.
 8. Local BGP address: This is a private IP address outside of the on-premises network within the /29 range selected for connectivity. For example, if the device BGP address selected for the WAN Edge peer above is 10.99.99.1, then use 10.99.99.2.

Microsoft Entra admin center

Search resources, services, and docs (G+D)

External collaboration settings
Cross-tenant synchronization

... Show more

Protection
Identity Governance
Verified ID
Permissions Management
Global Secure Access
Dashboard
Applications
Connect
Traffic forwarding
Client download
Remote networks
Connectors
Secure
Monitor
Alerts
Audit logs
Traffic logs
Deployment logs
Learn & support

... > Audit Log > Provisioning Log > Health > You do not have access > Diagnostic settings | General > You do not have access > Usage & insights | Microsoft Entra application ad

Create a remote network

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 5, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. [Learn more](#)

Basics Connectivity Traffic profiles Review + create

Add links to remote network.

+ Add a link

Link name	Device type	Device IP address	Local BGP address	Device BGP address	Device ASN	Redundancy	Zone Local BGP address	Per tunnel bandwidth

Add a link

Remote network

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 5, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. [Learn more](#)

General Details Security

Link name *

JuniperSSR-WAN1

Enter your device info

Device type *

Other

Device IP address *

13.91.234.228

Device BGP address *

10.47.47.1

Device ASN *

65000

Enter tunnel preference

Redundancy *

Bandwidth capacity (Mbps) *

250 Mbps

Enter a private IP address you want to use for Microsoft gateway

Local BGP address *

10.47.47.2

< Previous Next: Traffic profiles >

Save < Previous Next >

3. Click Next.
4. The IPsec/IKE policy is set to Default but change it to Custom.
5. After selecting Custom, select a combination of settings that match the WAN Edge. In this example, the following settings are selected:
 - Encryption
 - IKEv2 integrity
 - DH Group
 - IPsec encryption
 - IPsec integrity
 - PFS Group
 - SA lifetime

NOTE: The IPsec/IKE policy specified must match the policy on the WAN Edge.
6. Review the remote network valid configurations.
7. Click Next.
8. Enter the pre-shared key (PSK). The same secret key must be used on your CPE.
9. Select Add link.

Add a link

Remote network

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Entra Internet Access will begin to rollout on October 1, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. [Learn more](#)

General
Details
Security

Protocol ⓘ

☒ IKEv2

IPSec/IKE policy ⓘ

☐ Default ☒ Custom

IKE Phase 1 ⓘ

Encryption *

IKEv2 integrity *

DH group *

IKE Phase 2 ⓘ

IPSec encryption *

IPSec integrity *

PFS group *

SA lifetime (seconds) * ⓘ

Add a link

Remote network

General
Details
Security

Enter security information, including a pre-shared key, to establish a secure tunnel.

Pre-shared key (PSK) * ⓘ

Associate Traffic Profile

1. Either click Next or select the Traffic profiles tab.
2. Select the Microsoft 365 traffic profile. This ensures that only Microsoft 365 traffic is forwarded to Microsoft's SSE solution. The rest of the traffic will follow the configured Application Policy.
3. Select Review + Create.

NOTE: Select Create remote network to finalize the remote network configuration.

View the Network Profile

Once the remote network is created, go to the list of remote networks and select View configuration. This displays a task pane with connectivity details for the Microsoft gateway. The details include public endpoints of Microsoft's SSE gateway that are added to the WAN, along with BGP and ASN values.

The screenshot displays the Microsoft Entra admin center interface. On the left, the navigation pane shows various settings like Protection, Identity Governance, and Verified ID. The main area is titled 'Remote network' and lists several remote networks (Juniper-SSR, Juniper-SSR1, Juniper-SSR2) with their regions, links, device types, and forwarding profiles. On the right, a 'Remote network configuration' window for Juniper-SSR is open, showing a JSON configuration snippet. A diagram overlays the JSON, mapping fields to network parameters:

- IP Hostname/Remote ID:** Points to the `"ip": "10.237.132.39"` field.
- BGP Peer AS:** Points to the `"peerAs": "65476"` field.
- BGP Peer Address:** Points to the `"peerAddress": "13.99.224.228"` field.
- WAN Edge Public Address:** Points to the `"wanEdgePublicAddress": "18.49.49.2"` field.
- WAN Edge AS:** Points to the `"wanEdgeAs": "65476"` field.
- WAN Edge Source IP:** Points to the `"wanEdgeSourceIP": "18.49.49.1"` field.

Create Application

- One of the benefits of the Microsoft's SSE solution is that Microsoft 365 applications are advertised dynamically to the WAN Edge. This means that, as protected destinations are updated and service addresses modified over time, the Microsoft's SSE solution can dynamically advertise these routes to the WAN Edge for transport toward the service.
- One of the benefits of Juniper's AI-Driven SD-WAN is that routing policy is "Zero Trust." This means that just because a route was learned, it does not mean a network can access the destinations reachable through the advertised route. An application policy must explicitly permit the Network to access the application.
- A unique characteristic of the Session Smart Router (SSR) is that it might be configured to route unconditionally toward a destination using Steering Policy, or follow routes learned within the RIB (routing information base or route table). When a steering policy is defined for traffic to be forwarded locally toward a WAN or LAN link (for example, DIA), this policy overrides any learned routes. Therefore, an Internet service steered toward a local interface (not dynamically learned routes through the overlay), takes precedence over the learned routes if configured in the WAN Edge template.
- When the Microsoft's SSE solution is used for all Internet traffic, then a simple Internet application with a prefix 0.0.0.0/0 might be used, and the user is granted access without a steering policy as shown below:

The screenshot shows the 'APPLICATION POLICIES' section in the admin center. A table lists application policies. The first policy is 'Internet' with the following details:

NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	IDP	ADVANCED SECURITY SERVICES (SRX ONLY)	TRAFFIC STEERING
1	Internet		Lab	✓	Internet	No...		

- This will tell the WAN edge to allow the Network "Lab" to use any of the learned routes either through overlay or through IPsec to the Microsoft's SSE solution.
- However, if an Internet service is already created and uses DIA policies as shown in the example below, then a separate application must be created to allow the learned routes to be used first.
- The way to do this is define a more specific "IPsec" application than the 0.0.0.0/0 Internet application. When the prefixes to be learned are not known (cannot be configured), then creating an IPsec application with a more

specific prefix ensures the route table is imported from the IPsec BGP peer and used for the allowed networks.

APPLICATION POLICIES Destination zone in SRX is determined by the Traffic Steering path. Please ensure that policies have Traffic Steering assigned.

Search

Displaying 3 of 3 total Application Policies

[Import Application Policy](#) [Add Application Policy](#) [Edit Applications](#)

<input type="checkbox"/>	NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	ID P	ADVANCED SECURITY SERVICES (SRX ONLY)	TRAFFIC STEERING
<input type="checkbox"/>	1	Routed		+ Lab	→	IPSec	No...	+	+
<input type="checkbox"/>	2	Internet		+ Lab	→	Internet	No...	+	DIA

1. In the Mist portal, navigate to Organization > WAN > Applications.
2. Click Add Applications.
3. Define an application name (for example, IPsec). See the image below.
4. Select Custom Apps.
5. Enter the prefixes 128.0.0.0/1 and 0.0.0.0/1 for the IP Addresses. These prefixes are more specific than the default 0.0.0.0/0.

Edit Application

Name *

IPSec

Description

Type

☒ Custom Apps

☐ Apps

☐ URL Categories

☐ Custom URLs

IP Addresses

128.0.0.0/1,
0.0.0.0/1

(comma-separated)

Domain Names

(comma-separated)

Protocol

Any

Protocol Number

Not Applicable

6. Click Save and navigate to Organization > WAN > WAN Edge Templates.

Update WAN Edge Template

In the Mist portal, navigate to the WAN Edge Template for the Session Smart Router WAN Edge device.

1. Select Add Providers under Secure Edge Connectors to open a configuration panel.

SECURE EDGE CONNECTORS

1 Provider

[Add Providers](#)

2. Enter the following entries to match Microsoft's SSE solution:

- Name: (for example, MicrosoftSSE)
- Provider: Custom
- Protocol: IPSec
- LocalID: <WAN Edge Public IP address>
- Pre-shared Key: <Same as MirosoftSSE>
- IP or Hostname: <Microsoft endpoint address>
- Source IP: <WAN Edge Source IP>
- Remote ID:<Microsoft endpoint address>
- WAN Interface:<Interface address with Public IP>
- **IPSec Proposals:**
 - Encryption: aes256
 - Authentication Algorithm: sha2
 - DH Group: 14
- **IPSec Proposals:**
 - Encryption Algorithm: aes_gcm256
 - DH Group: 14
 - SA Lifetime: 1800 seconds

Edit Provider

Note: Please ensure Inbound or Outbound Application Policies are created with Traffic Steering for the Secure Edge Connector to be deployed to devices.

Name *

MicrosoftSSE1

Provider *

Custom

Remote Networks

None

(Select an existing Network or [Create Network](#))

Protocol

☒ IPsec ☐ GRE

Local ID * VAR

13.90.224.228

Pre-Shared Key (Clear Text) * VAR

Show

IP or Hostname * VAR

20.81.84.32

Source IPs VAR

10.40.122.1

Edit Provider

Note: Please ensure Inbound or Outbound Application Policies are created with Traffic Steering for the Secure Edge Connector to be deployed to devices.

IKE V2 PROPOSALS

Encryption Algorithm

aes256

Authentication Algorithm

sha2

DH Group

14

Lifetime

3600

(Number of seconds in range (180, 86400))

IPSEC PROPOSALS

Encryption Algorithm

aes_gcm256

Authentication Algorithm

None

- Click Save at the bottom of the window.
- Create a new BGP Group using the BGP dialog.

Use the values selected previously:

- Name: <name of SSE Connector>
- Type: External
- Local AS: <65000 or non-default AS for WAN Edge>

Add BGP Group

At least one Neighbor must be defined

Name *

MicrosoftSSR

Peering Network

☐ WAN

None

☐ LAN

None

☒ SEC Tunnel

MicrosoftSSE1

BFD

☒ Enabled
☐ Disabled

Type *

External

Local AS *

65000

Hold Time *

90

Graceful Restart Time *

120

- Select Add Neighbor in the BGP dialog box.

NEIGHBORS					Add Neighbor
IP Address	Neighbor AS	Export Policy	Import Policy	Enabled	
10.40.12...	65476	--	--	Yes	

6. Enter the following values for the BGP peer:

- IP Address: BGP peer address of Microsoft's SSE solution
- Optional: Add BGP policy for import/export of routes

NEIGHBORS

Edit Neighbor

☒ Enabled
 ☐ Disabled

IP Address * VAR

10.40.122.2

Neighbor AS *

65476

7. Navigate to Application Policies and click Add Application Policy.

- Import Application Policy
- Add Application Policy
- Edit Applications

8. Using the application name created in the steps above, add a policy to allow the desired networks to reach the more specific "IPSec" application using the route table. Leaving the Steering Policy blank instructs the SSR to use the routing table for prefixes within the defined application range.

APPLICATION POLICIES [Destination zone in SRX is determined by the Traffic Steering path. Please ensure that policies have Traffic Steering assigned.](#)

Search

Displaying 3 of 3 total Application Policies

[Import Application Policy](#) [Add Application Policy](#) [Edit Applications](#)

NO.	NAME	ORG IMPORTED	NETWORK / USER (MATCHING ANY)	ACTION	APPLICATION / DESTINATION (MATCHING ANY)	ISP	ADVANCED SECURITY SERVICES (SRX ONLY)	TRAFFIC STEERING
1	Routed			→	IPsec	No...		

9. Navigate to the top of the Template and click Save.

Verify Operation

- Once the template is updated, an IPsec configuration will be pushed to the WAN Edge device. If this is the first time IPsec deployment, this will take some time to download the software/configuration.
- Once the IPsec configuration is deployed, you can view the IPsec status under WAN Edge > <WAN Edge Name> > Secure Edge Connector Details.

SECURE EDGE CONNECTOR DETAILS

Filter

1 Tunnel

Tunnel Name	Peer Host	Peer IP	Status	Node	RX Bytes	TX Bytes	RX Packets	TX Packets	Last Event	Protocol	Uptime	Priority	WAN Port	Last Seen
MicrosoftSSE1	20.81.84.32	20.81.84.32	Connected	standalone	85.4 MB	73.7 MB	558.9 k	539.1 k	--	IPsec	16d 34m	primary	MPLS	Oct 29, 2024 6:03:19 PM

- BGP neighbor status might be found under Monitor > Insights > WAN Edge.

BGP Summary

Neighbor Information 6:09:34 PM (Updates Every 3 Minutes) [Q](#)

Status	State	Neighbor	Neighbor AS	Local AS	Uptime	RX Routes	TX Routes	RX Packets	TX Packets	VRF Name
Connected	Established	10.40.122.2	65476	65000	16d 40m	32	32	61045	53602	default

- It might be useful to navigate to Testing tools to observe learned routes under WAN Edge > Utilities > Testing Tools > Routes > Show Routes. In the display below, routes learned through IPsec will be

displayed with Microsoft's SSE solution BGP peer as next hop.

WAN Edge Testing Tools

Utility

Applications

Address Resolution Protocol

FIB

Border Gateway Protocol

Ping

WAN DHCP Release

Bounce Port

Traceroute

Path

Sessions

Refresh ARP

Table

FIB Lookup

FIB By Application

Clear BGP

Summary

Routes

Advertised Routes

Received Routes

OSPF

Summary

Interfaces

Neighbors

Database

Routes

Route Prefix

VRF

Route Prefix

VRF

Show Routes

🔍 Search

32 items

VRF NAME	PREFIX	NAME	METRIC	WEIGHT	AS PATH	LOCAL PREFERENCE	STATUS	SELECTION REASON	NEXT HOPS
default	13.107.6.152/31		0	0	65000 65476	100	Valid, Best	First path received	10.40.122.2
default	13.107.6.171/32		0	0	65000 65476	100	Valid, Best	First path received	10.40.122.2
default	13.107.6.192/32		0	0	65000 65476	100	Valid, Best	First path received	10.40.122.2
default	13.107.9.192/32		0	0	65000 65476	100	Valid, Best	First path received	10.40.122.2
default	13.107.18.10/31		0	0	65000 65476	100	Valid, Best	First path received	10.40.122.2
default	13.107.18.15/32		0	0	65000 65476	100	Valid, Best	First path received	10.40.122.2
default	13.107.128.0/22		0	0	65000 65476	100	Valid, Best	First path received	10.40.122.2
default	13.107.136.0/22		0	0	65000 65476	100	Valid, Best	First path received	10.40.122.2
default	13.107.140.6/32		0	0	65000 65476	100	Valid, Best	First path received	10.40.122.2
default	20.20.32.0/19		0	0	65000 65476	100	Valid, Best	First path received	10.40.122.2
default	20.190.128.0/18		0	0	65000 65476	100	Valid, Best	First path received	10.40.122.2

Single WAN Link with Zone Redundancy on the Microsoft SSE Solution

This configuration option is illustrated in the diagram below.



In this configuration, a second BGP peer is created using zone redundancy within the Microsoft SSE solution. Follow the steps described above with the following additions:

1. Ensure to select Zone redundancy when creating the link to the remote network within the Microsoft SSE solution as shown below. This creates a second BGP peer which might be reached through the same remote network link and IPsec tunnel from the SSR.

Redundancy * ⓘ

No redundancy

Zone redundancy

2. Create a second BGP peer using the same BGP group within the device template in Mist. The peer address might be found within the SSE configuration as shown.

```
{
  "@odata.context": "https://graph.microsoft.com/beta/$metadata#netv",
  "remoteNetworkId": "5e6099c8-88ea-4746-bcd5-01c1ca199112",
  "remoteNetworkName": "Juniper-SSR2",
  "links@odata.context": "https://graph.microsoft.com/beta/$metadata#links",
  "links": [
    {
      "id": "5560f6ff-94db-4a99-aef8-c770df3b1dd2",
      "displayName": "JuniperSSR2",
      "localConfigurations": [
        {
          "endpoint": "20.81.84.32",
          "asn": 65476,
          "bgpAddress": "10.40.122.2",
          "region": "eastUS"
        },
        {
          "endpoint": "20.81.84.33",
          "asn": 65476,
          "bgpAddress": "10.40.121.2",
          "region": "eastUS"
        }
      ],
      "peerConfiguration": {
        "endpoint": "13.90.224.228",
        "asn": 65000,
        "bgpAddress": "10.40.122.1"
      }
    }
  ],
  "headerRequestId": "ceea9e2f-ece3-4eab-991d-1450fff7ff5e"
}
```

NEIGHBORS

Add Neighbor

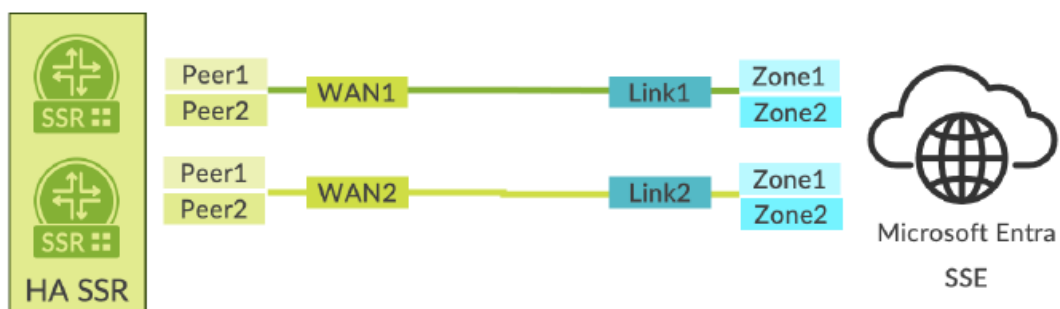
☒ Enabled
☐ Disabled

IP Address *
VAR
10.40.121.2

Neighbor AS *
65476

Dual WAN Link Using an HA SSR with Zone Redundancy Per Tunnel on the Microsoft SSE Solution

This configuration option is illustrated in the diagram below.



In this configuration, both a second link and a second BGP peer per link are created using zone redundancy within the Microsoft SSE solution. Follow the steps described above with the following additions:

1. Ensure to select Zone redundancy when creating links as described above.
2. Create the second BGP peer within the same BGP group configuration that is pointing toward the SEC Tunnel as the peering network.
3. Create a second link within the Microsoft SSE solution for the same Remote network. This link might be added either during initial network configuration or added using the Remote network dialog box shown below. Select Remote network > Remote Network Name > Links > Add a link.
4. Repeat the steps above for addition of another Secure Edge Connector within the device template in Mist. This provides the opportunity to steer the tunnel out a secondary interface in a high availability configuration.
5. Create a second BGP Group that is assigned to the second Secure Edge Connector. This group is assigned to

- the second connector (SEC tunnel) as the outbound interface.
6. Create a second pair of BGP peers within the BGP Group using the additional link and BGP peering configuration within the Microsoft SSR solution.

Home > Remote network > Juniper-SSR2

Juniper-SSR2 | Links

Global Secure Access

Basics

Links

Traffic profiles

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Access will begin with General Availability on July 1st, 2024. [Learn more](#)

+ Add a link

Got feedback?

Link name	Device type	Device IP address	Local BGP address	Device BGP address	Device ASN	Redundancy
JuniperSSR2	Other	13.90.224.228	10.40.122.2	10.40.122.1	65000	Zone redundancy

Add a link

Remote network

Global Secure Access is now in generally available. Licensing requirements have been updated. Licensing enforcement for Microsoft Entra Private Access, Microsoft Access will begin with General Availability on July 1st, 2024. This is following a 90-day trial period that began with General Availability on July 1st, 2024. [Learn more](#)

General

Details

Security

Link name *

JuniperSSR2HA

Enter your device info

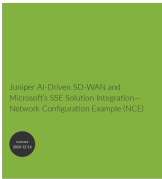
Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice. Copyright © 2024 Juniper Networks, Inc. All rights reserved.

FAQ

Q: What information is required prior to configuring the network?
A: Prior to configuration, you need to have the public addresses of WAN links, BGP peering address ranges, BGP AS number, access permissions, bandwidth requirements, and redundancy model details for each site.

Q: How many configuration options are covered in the guide?
A: The guide covers three configuration options: Single WAN link and peer on Microsoft's SSE Solution, Single WAN link with zone redundancy on Microsoft's SSE Solution, and Dual WAN link using an HA SSR with zone redundancy per tunnel on Microsoft's SSE Solution.

Documents / Resources



[Juniper NCE-511 AI-Driven SD-WAN Reference Architecture \[pdf\]](#) User Guide
NCE-511 AI-Driven SD-WAN Reference Architecture, NCE-511, AI-Driven SD-WAN Reference Architecture, Reference Architecture, Architecture

References

- [User Manual](#)

[Manuals+](#), [Privacy Policy](#)

This website is an independent publication and is neither affiliated with nor endorsed by any of the trademark owners. The "Bluetooth®" word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. The "Wi-Fi®" word mark and logos are registered trademarks owned by the Wi-Fi Alliance. Any use of these marks on this website does not imply any affiliation with or endorsement.