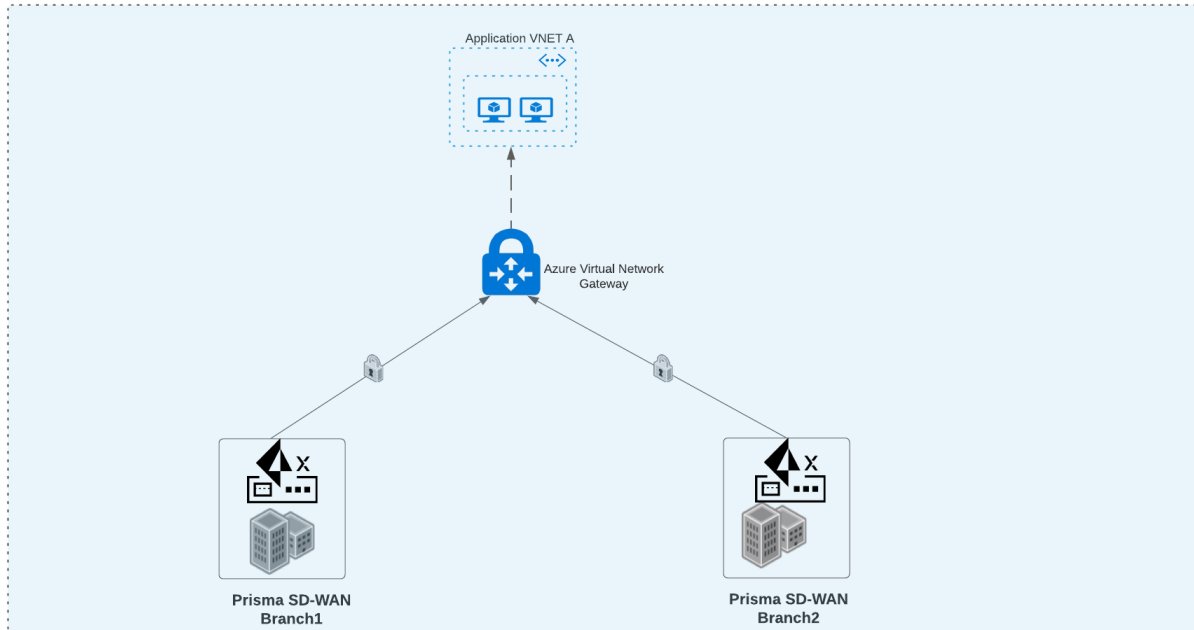


Establishing an IPSEC tunnel to Azure VPN Gateway

Multiple remote networks can connect to an Azure Virtual Network Gateway over site to site IPSEC VPN to send encrypted traffic to an Azure virtual network.




Below are the steps to configure a Prisma SD-WAN branch ION to send traffic to Azure VNETs over an IPSEC tunnel:

1. Create a Virtual Network Gateway on Azure

[Home](#) > [Meena-VPN-GW-Test](#) > [Meena-Test-VPN-GW](#) > [Create a resource](#) >

Virtual network gateway

Microsoft



Virtual network gateway [Add to Favorites](#)

Microsoft
★★★★☆ 4.0 (3 ratings)

[Create](#)

[Overview](#) [Plans](#) [Usage Information + Support](#) [Reviews](#)

A virtual network gateway is the software VPN device for your Azure virtual network. Use this with a [connection](#) to set up a site-to-site VPN connection between an Azure virtual network and your local network, or a VNet-to-VNet VPN connection between two Azure virtual networks. It can also be used to connect a virtual network to an ExpressRoute circuit.

Microsoft Azure provides a [99.9% uptime SLA](#) for virtual network gateways.

2. Create a Local Network Gateway on Azure. This is the remote network configuration. Provide the public IP address of the Prisma SD-WAN ION and the Address Space indicates the branch LAN subnet. Without the Address space config, the tunnel will not come up.

Create local network gateway ...

Name *
Meena-Local-GW-Test ✓

Endpoint ⓘ
IP address FQDN

IP address * ⓘ
65.70.99.112 ✓

Address space ⓘ
192.168.20.0/24 ...
Add additional address range ...

☐ Configure BGP settings

Subscription *
AzureCGXTME ✓

Resource group * ⓘ
Meena-Test-VPN-GW ✓
[Create new](#)

Location *
East US ✓

Create [Automation options](#)

3. Navigate to the Virtual Network Gateway that was just created and add a new Site-Site IPSEC connection



4. Configure the right Virtual Network Gateway and the local network Gateway. Make sure the PSK matches at the remote end.

Home > Meena-VPN-GW-Test >

Add connection

Meena-VPN-GW-Test

Name *
Meena-Test-Connection ✓

Connection type ⓘ
Site-to-site (IPsec) ✓

*Virtual network gateway ⓘ
Meena-VPN-GW-Test 🔒

*Local network gateway ⓘ
(new) Meena-Test-Local-Gateway >

Shared key (PSK) * ⓘ
PaloAltoNetworks!123 ✓

☐ Use Azure Private IP Address ⓘ

☐ Enable BGP ⓘ

IKE Protocol ⓘ
☐ IKEv1 ☒ IKEv2

Subscription ⓘ
AzureCGXTME ✓

Resource group ⓘ
✓

Location ⓘ
East US ✓

5. Change the configuration of the connection to match the crypto profile at the remote end

Home > Meena-VPN-GW-Test > Meena-Test-Connection

Meena-Test-Connection | Configuration

Connection

Search (Cmd+/) Save Discard

- Overview
- Activity log
- Access control (IAM)
- Tags

Settings

- Shared key
- Configuration**
- Properties
- Locks

Monitoring

- Metrics

Automation

- Tasks (preview)
- Export template

Support + troubleshooting

- Resource health
- VPN troubleshoot

BGP [?]

Disabled Enabled

IPsec / IKE policy [?]

Default Custom

IKE Phase 1 [?]

Encryption * Integrity/PRF * DH Group *

IKE Phase 2(IPsec) [?]

IPsec Encryption * IPsec Integrity * PFS Group *

IPsec SA lifetime in KiloBytes * [?]

102400000

IPsec SA lifetime in seconds * [?]

27000

Use policy based traffic selector [?]

Enable Disable

DPD timeout in seconds * [?]

45

Connection Mode [?]

Default InitiatorOnly ResponderOnly

Save the public IP of the VPN Gateway to configure as Peer on the Prisma SD-WAN side.

Home > Meena-VPN-GW-Test >

Meena-Test-Connection

Connection

Search (Cmd+/) Refresh Move Download configuration Delete

- Overview**
- Activity log
- Access control (IAM)
- Tags

Settings

- Shared key
- Configuration
- Properties
- Locks

Essentials

Resource group (change) : Meena-Test-VPN-GW

Status : Not connected

Location : East US

Subscription (change) : AzureCGXTME

Subscription ID : 80c49be4-fee2-45b6-9180-0a9b0fbee491

Tags (change) : Click here to add tags

Data in : 0 B

Data out : 0 B

Virtual network : Meena-VPN-GW-TEST-VNET

Virtual network gateway : Meena-VPN-GW-Test (20.185.80.230)

Local network gateway : Meena-Test-Local-Gateway (64.112.59.10)

JSON View

- On the Prisma SD-WAN ION, make sure the right public IP is configured on the parent interface

PRISMA SD-WAN BY PALO ALTO NETWORKS

Dashboard Map Policies Activity CloudBlades

Prisma SD-WAN Branch1 @Prisma-sdwan-Branch1

Basic Info Device Toolkit **Interfaces** Routing SNMP Syslog Export NTP Client DNS Service IPFIX

CONTROLLER C1

VIRTUAL PORTS 1 2 3 4 5 6 7 8 9

Configure Interface: 1

Main Configuration Sub-Interfaces (0) PPPoE

IPFIX COLLECTOR CONTEXT --

IPFIX FILTER CONTEXT --

> NAT Configuration - Clear

> Security Configuration

Advanced Options

MAC optional

EXTERNAL NAT ADDRESS & PORT 64 . 124 . 115 . 162 : 4500

IP MTU (552 - 1500) 1500

PHYSICAL Auto

7. Create a standard VPN interface

Prisma SD-WAN Branch1 @Prisma-sdwan-Branch1

Basic Info Device Toolkit **Interfaces** Routing SNMP Syslog Export NTP Client DNS Service IPFIX

CONTROLLER C1

VIRTUAL PORTS 1 2 3 4 5 6 7 8 9

CREATE A NEW INTERFACE

☐ Loopback

☒ Standard VPN

☐ Virtual Interface

☐ Port Channel

Cancel Add

- Configure the standard VPN interface with the peer IP from Azure Virtual Network Gateway and associate an IPSEC profile to this interface.

PRISMA SD-WAN BY PALO ALTO NETWORKS

Dashboard Map Policies Activity CloudBlades

Basic Info Device Toolkit **Interfaces** Routing SNMP Syslog Export NTP Client DNS Service IPFIX

Configure Interface: Azure VPN

Main Configuration Sub-Interfaces (0) PPPoE

INTERFACE TYPE Standard VPN

STANDARD VPN TYPE IPsec

PARENT INTERFACE Port 2

SCOPE Local

INNER TUNNEL IP ADDRESS/MASK (REQUIRED) 10 . 0 . 0 . 4 / 24

Configuration

ENDPOINT -- Update

PEER HOSTNAME optional

PEER IP 52 . 255 . 149 . 103

IPSEC PROFILE Azure Edit | Add

9. This should automatically bring up the site to site connection. The status on Azure should show connected and the Operational state of the VPN interface on the Prisma SD-WAN ION should show “Up”

Home > Meena-VPN-GW-Test

Meena-VPN-GW-Test | Connections

Virtual network gateway

Search (Cmd+/) Add Refresh

Overview Activity log Access control (IAM) Tags Diagnose and solve problems

Search connections

Name	Status	Connection type	Peer
Meena-VIRTUAL-GW	Connected	Site-to-site (IPsec)	Meena-Local-NW-GW

Interface Status: [redacted] Azure VPN

Last Edited: Jul 23, 2021 - 2:00pm

ITEM	VALUE
Operational State:	up
Extended State:	tunnel_up
Last State Change:	Aug 12 2021, 08:46:43.364
Admin Up?:	Yes
IPv4 Addresses:	10.0.0.4/24
Secondary IPv4 Addresses:	None
Routes:	10.0.0.4 (destination: 0.0.0.0/0)