IPSec VPN Configuration Reference

VMware Integrations

Table of contents

IPSec VPN Configuration Reference 3
Introduction 3
SDDC - Cisco CSR (IOS XR) with IKEv1 4
SDDC Configuration 4
Cisco CSR Configuration (IOS-XR) 4
SDDC - Cisco CSR (IOS XR) with IKEv2 6
SDDC Configuration 6
Cisco CSR (IOS-XR) configuration 6
SDDC - Ubiquiti EdgeMax with IKEv2 8
SDDC Configuration 8
Ubiquiti EdgeMax Configuration 8
SDDC - VyOS (vyatta) with IKEv2 (no NAT; both endpoints on public IP) 9
SDDC Configuration 9
VyOS with a DHCP interface for IPSec endpoint 9
SDDC - VyOS (vyatta on private IP, NAT) with IKEv2 10
SDDC Configuration 10
VyOS with Private IP 10
SDDC - Azure VPN Endpoint with IKEv2 (public IPs on both ends) 12
SDDC Configuration 12
Azure Configuration 13
Authors and Contributors 16

IPSec VPN Configuration Reference

Introduction

In the IPSec implementation for VMware Cloud on AWS article , we discussed the architecture, use cases, and design considerations for IPSec between on-premises and VMware Cloud on AWS. The VPN endpoint at the other end could be an on-premises router and or a VPN endpoint hosted in other public cloud.

This document provides information about the configuration of Cisco (IOS-XR) devices, VyOS virtual router, Azure VPN endpoint etc. These different VPN endpoints were setup in AWS using EC2 instances for test purpose (except for Azure VPN endpoint that was hosted in Azure itself). EC2 instances use NAT, so you must be sure to open up UDP 500/4500 (for NAT-t) inbound in the security group for the device. However, note that the actual VPN endpoints in your on-prem may require modification or additional configuration to your specific environment in order to actually work.

SDDC - Cisco CSR (IOS XR) with IKEv1

In this configuration, Cisco CSR (IOS-XR) is one VPN endpoint and the other VPN endpoint resides on the SDDC running in VMware Cloud on AWS SDDC. Both the endpoints are configured with IKE version as IKEv1. Following is the configuration for VPN endpoint in VMware Cloud on AWS SDDC and Cisco CSR.

VPN Type: Route-Based VPN, IKEv1

SDDC Configuration

```
Local IP Address : edge public IP 203.0.113.10
IKE Type:  IKEv1
Tunnel Encryption:  AES 256
Tunnel Digest Algorithm:  SHA2
IKE Encryption:  AES 256
IKE Digest Algorithm:  SHA2
Perfect Forward Secrecy:  enabled
Pre-shared Key:  myverysecretkey
Diffie Hellman:  Group 14
BGP Local IP/Prefix Length:  169.254.255.1/30
BGP Remote IP:  169.254.255.2
BGP Remote ASN:  64512
SDDC ASN Setting:  64513
```

Cisco CSR Configuration (IOS-XR)

In this configuration also, Cisco CSR (IOS-XR) is one VPN endpoint and the other VPN endpoint resides on the SDDC running in VMware Cloud on AWS SDDC. Both the endpoints are configured with IKE version as IKEv2.

Following is the configuration for VPN endpoint in VMware Cloud on AWS SDDC and Cisco CSR.

```
! specify the pre-share key for the remote sddc edge
crypto keyring sddc
! the local private ip address
local-address 192.168.250.43
! pre-shared key with sddc edge
pre-shared-key address 203.0.113.10 key myverysecretkey
exit

! phase1 crypto - AES 256 SHA2-256
crypto isakmp policy 1
encryption aes 256
hash sha256
authentication pre-share
group 14
! this is typically a default setting
lifetime 86400
exit

! create a profile for the remote sddc edge
crypto isakmp profile isakmp-sddc
keyring sddc
! ip of sddc edge
match identity address 203.0.113.10
! the local private ip address
local-address 192.168.250.43
exit

! phase2 crypto - AES 256 SHA2-256. always use tunnel mode
crypto ipsec transform-set ipsec-sddc esp-aes 256 esp-sha256-hmac
mode tunnel
exit

! phase2 ipsec profile
crypto ipsec profile ipsec-profile-sddc
set transform-set ipsec-sddc
```

```
set pfs group14
! this is typically a default setting
set security-association lifetime seconds 3600
exit

crypto ipsec df-bit clear
crypto isakmp keepalive 60 2 on-demand
crypto ipsec security-association replay window-size 128
crypto ipsec fragmentation before-encryption

! a fake network we will use for testing. this is definitely optional
interface Loopback0
ip address 192.168.251.1 255.255.255.0
exit

! the VTI interface for route-based vpn
interface Tunnel0
! can use link-local address range here. use a range which is not currently in use on this router or the sddc edge
ip address 169.254.255.2 255.255.255.252
ip virtual-reassembly
! use the local private ip
tunnel source 192.168.250.43
! ip of the sddc edge
tunnel destination 203.0.113.10
tunnel mode ipsec ipv4
! this enables ipsec encryption for the VTI
tunnel protection ipsec profile ipsec-profile-sddc
ip tcp adjust-mss 1379
no shutdown
exit

! enable bgp with local asn
router bgp 64512
! the neighbor should be the VTI address of the sddc edge. use the asn specified in the vmc console
neighbor 169.254.255.1 remote-as 64513
neighbor 169.254.255.1 activate
neighbor 169.254.255.1 timers 60 180 180
address-family ipv4 unicast
! as a test, we will advertise the fake network we created on Loopback 0
network 192.168.251.0 mask 255.255.255.0
neighbor 169.254.255.1 activate
neighbor 169.254.255.1 soft-reconfiguration inbound

exit
```

SDDC - Cisco CSR (IOS XR) with IKEv2

In this configuration also, Cisco CSR (IOS-XR) is one VPN endpoint and the other VPN endpoint resides on the SDDC running in VMware Cloud on AWS SDDC. Both the endpoints are configured with IKE version as IKEv2. Following is the configuration for VPN endpoint in VMware Cloud on AWS SDDC and Cisco CSR.

Type: Route-Based VPN, IKEv2

SDDC Configuration

```
Local IP Address: edge public IP 203.0.113.10
IKE Type: IKEv2
Tunnel Encryption: AES 256
Tunnel Digest Algorithm: SHA2
IKE Encryption: AES 256
IKE Digest Algorithm: SHA2
Perfect Forward Secrecy: enabled
Preshared Key: myverysecretkey
Diffie Hellman: Group 14
BGP Local IP/Prefix Length: 169.254.255.1/30
BGP Remote IP: 169.254.255.2
BGP Remote ASN: 64512
SDDC ASN Setting: 64513
```

Cisco CSR (IOS-XR) configuration

```
! ikev2 crypto - AWS-256-CBC SHA-256
crypto ikev2 proposal ikev2-prop-sddc
encryption aes-cbc-256
integrity sha256
group 14
exit

! define an ikev2 policy
crypto ikev2 policy ikev2-policy-sddc
match fvrf any
proposal ikev2-prop-sddc
exit

! define keyring for pre-shared key
crypto ikev2 keyring ikev2-keyring-sddc
peer sddc
! ip of sddc edge
address 203.0.113.10
pre-shared-key myverysecretkey
exit
exit

! ikev2 profile
crypto ikev2 profile ikev2-profile-sddc
! ip of sddc edge
match identity remote address 203.0.113.10 255.255.255.255
! local private ip of this router
identity local address 192.168.250.43
authentication remote pre-share
authentication local pre-share
keyring local ikev2-keyring-sddc
exit

crypto ikev2 dpd 60 2 on-demand
crypto ipsec security-association replay window-size 128
crypto ipsec df-bit clear

! ipsec proposal - AES-256 SHA-256
crypto ipsec transform-set ipsec-sddc esp-aes 256 esp-sha256-hmac
```

```
mode tunnel
exit

! ipsec profile using previously configured parameters
crypto ipsec profile ipsec-profile-sddc
set transform-set ipsec-sddc
set pfs group14
set ikev2-profile ikev2-profile-sddc
exit

! a fake network we will use for testing. this is definitely optional
interface Loopback0
ip address 192.168.251.1 255.255.255.0
exit

! the VTI interface for route-based vpn
interface Tunnel0
! can use link-local address range here. use a range which is not currently in use on this router or the sddc edge
ip address 169.254.255.2 255.255.255.252
ip virtual-reassembly
! use the local private ip
tunnel source 192.168.250.43
! ip of the sddc edge
tunnel destination 203.0.113.10
tunnel mode ipsec ipv4
! this enables ipsec encryption for the VTI
tunnel protection ipsec profile ipsec-profile-sddc
ip tcp adjust-mss 1379
no shutdown
exit

! enable bgp with local asn
router bgp 64512
! the neighbor should be the VTI address of the sddc edge. use the asn specified in the vmc console
neighbor 169.254.255.1 remote-as 64513
neighbor 169.254.255.1 activate
neighbor 169.254.255.1 timers 60 180 180
address-family ipv4 unicast
! as a test, we will advertise the fake network we created on Loopback 0
network 192.168.251.0 mask 255.255.255.0
neighbor 169.254.255.1 activate
neighbor 169.254.255.1 soft-reconfiguration inbound
exit
```

SDDC - Ubiquiti EdgeMax with IKEv2

In this configuration, Ubiquiti EdgeMax is one VPN endpoint and the other VPN endpoint resides on the SDDC running in VMware Cloud on AWS SDDC. Both the endpoints are configured with IKE version as IKEv2. Following is the configuration for VPN endpoint in VMware Cloud on AWS SDDC and Ubiquiti EdgeMax.

VPN Type: Route-Based VPN, IKEv2

SDDC Configuration

```
Local IP Address: edge public IP 203.0.113.10
IKE Type: IKEv2
Tunnel Encryption: AES 256
Tunnel Digest Algorithm: SHA1
IKE Encryption: AES 256
IKE Digest Algorithm: SHA1
Perfect Forward Secrecy: enabled
Preshared Key: myverysecretkey
Diffie Hellman: Group 14
BGP Local IP/Prefix Length: 169.254.255.1/30
BGP Remote IP: 169.254.255.2
BGP Remote ASN: 64512
SDDC ASN Setting: 64513
```

Ubiquiti EdgeMax Configuration

```
set vpn ipsec ike-group vmc key-exchange ikev2
set vpn ipsec ike-group vmc lifetime 28800
set vpn ipsec ike-group vmc proposal 1 dh-group 14
set vpn ipsec ike-group vmc proposal 1 encryption aes256
set vpn ipsec ike-group vmc proposal 1 hash sha1

set vpn ipsec esp-group vmc lifetime 27000
set vpn ipsec esp-group vmc pfs enable
set vpn ipsec esp-group vmc proposal 1 encryption aes256
set vpn ipsec esp-group vmc proposal 1 hash sha1

set interfaces vti vti1 address 169.254.255.2/30

set firewall options mss-clamp interface-type vti
set firewall options mss-clamp mss 1379

set vpn ipsec site-to-site peer 203.0.113.10 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 203.0.113.10 authentication pre-shared-secret myverysecretkey
set vpn ipsec site-to-site peer 203.0.113.10 description "VMware Cloud on AWS"
set vpn ipsec site-to-site peer 203.0.113.10 local-address 203.0.113.30

set vpn ipsec site-to-site peer 203.0.113.10 ike-group vmc
set vpn ipsec site-to-site peer 203.0.113.10 vti bind vti0
set vpn ipsec site-to-site peer 203.0.113.10 vti esp-group vmc

set protocols bgp 64512 neighbor 169.254.255.1 remote-as 64513
set protocols bgp 64512 redistribute connected
set protocols bgp timers holdtime 30
set protocols bgp timers keepalive 10
```

SDDC - VyOS (vyatta) with IKEv2 (no NAT; both endpoints on public IP)

In this configuration, Vyatta device running VyOS is one VPN endpoint and the other VPN endpoint resides on the SDDC running in VMware Cloud on AWS SDDC. Both the endpoints are configured with IKE version as IKEv2. There is no NAT involved here as the connectivity between both the endpoints is on Public IP addresses. Following is the configuration for VPN endpoint in VMware Cloud on AWS SDDC and VyOS device.

VPN Type: Route-Based VPN, IKEv2

SDDC Configuration

```
Local IP Address: edge public IP 203.0.113.20
Remote IP Address: public IP of VyOS 203.0.113.30
IKE Type: IKEv2
Tunnel Encryption: AES 256
Tunnel Digest Algorithm: SHA2
IKE Encryption: AES 256
IKE Digest Algorithm: SHA2
Perfect Forward Secrecy: enabled
Preshared Key: myverysecretkey
Diffie Hellman: Group 14
BGP Local IP/Prefix Length: 169.254.255.1/30
BGP Remote IP: 169.254.255.2
BGP Remote ASN: 64512
SDDC ASN Setting: 64513
```

VyOS with a DHCP interface for IPSec endpoint

```
set vpn ipsec esp-group VMC compression 'disable'
set vpn ipsec esp-group VMC lifetime '3600'
set vpn ipsec esp-group VMC mode 'tunnel'
set vpn ipsec esp-group VMC pfs 'dh-group14'
set vpn ipsec esp-group VMC proposal 1 encryption 'aes256'
set vpn ipsec esp-group VMC proposal 1 hash 'sha256'
set vpn ipsec ike-group VMC dead-peer-detection action 'restart'
set vpn ipsec ike-group VMC dead-peer-detection interval '15'
set vpn ipsec ike-group VMC dead-peer-detection timeout '30'
set vpn ipsec ike-group VMC ikev2-reauth 'yes'
set vpn ipsec ike-group VMC key-exchange 'ikev2'
set vpn ipsec ike-group VMC lifetime '28800'
set vpn ipsec ike-group VMC proposal 1 dh-group '14'
set vpn ipsec ike-group VMC proposal 1 encryption 'aes256'
set vpn ipsec ike-group VMC proposal 1 hash 'sha256'
set vpn ipsec ipsec-interfaces interface 'eth0'
set vpn ipsec site-to-site peer 203.0.113.20 authentication id '203.0.113.30'
set vpn ipsec site-to-site peer 203.0.113.20 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 203.0.113.20 authentication pre-shared-secret 'myverysecretkey'
set vpn ipsec site-to-site peer 203.0.113.20 authentication remote-id '203.0.113.20'
set vpn ipsec site-to-site peer 203.0.113.20 connection-type 'respond'
set vpn ipsec site-to-site peer 203.0.113.20 description 'VMC PRIMARY TUNNEL'
set vpn ipsec site-to-site peer 203.0.113.20 ike-group 'VMC'
set vpn ipsec site-to-site peer 203.0.113.20 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 203.0.113.20 dhcp-interface eth0
set vpn ipsec site-to-site peer 203.0.113.20 vti bind 'vti1'
set vpn ipsec site-to-site peer 203.0.113.20 vti esp-group 'VMC'
set interfaces vti vti1 address '169.254.255.2/30'
set interfaces vti vti1 description 'VMC Tunnel'
set protocols bgp 65002 address-family ipv4-unicast
set protocols bgp 65002 neighbor 169.254.255.1 remote-as '65001'
```

SDDC - VyOS (vyatta on private IP, NAT) with IKEv2

In this configuration, Vyatta device running VyOS is one VPN endpoint and the other VPN endpoint resides on the SDDC running in VMware Cloud on AWS SDDC. Both the endpoints are configured with IKE version as IKEv2. The VyOS device has NAT enabled (note the remote private IP address field populated with the private IP of VyOS device).

Following is the configuration for VPN endpoint in VMware Cloud on AWS SDDC and VyOS device.

VPN Type: Route-Based VPN, IKEv2

SDDC Configuration

```
Local IP Address: edge public IP 203.0.113.20
Remote IP Address: Public IP of VyOS 203.0.113.30
Remote Private IP: 192.168.10.101
IKE Type: IKEv2
Tunnel Encryption: AES 256
Tunnel Digest Algorithm: SHA2
IKE Encryption: AES 256
IKE Digest Algorithm: SHA2
Perfect Forward Secrecy: enabled
Preshared Key: myverysecretkey
Diffie Hellman: Group 14
BGP Local IP/Prefix Length: 169.254.255.1/30
BGP Remote IP: 169.254.255.2
BGP Remote ASN: 65002
SDDC ASN Setting: 65001
```

VyOS with Private IP

```
set interfaces ethernet eth5 address '192.168.10.101/24'
set interfaces vti vti1 address '169.254.255.2/30'
set interfaces vti vti1 description 'VMC Tunnel'
set protocols bgp address-family ipv4-unicast
set protocols bgp local-as '65002'
set protocols bgp neighbor 169.254.255.1 remote-as '65001'
set vpn ipsec esp-group VMC compression 'disable'
set vpn ipsec esp-group VMC lifetime '3600'
set vpn ipsec esp-group VMC mode 'tunnel'
set vpn ipsec esp-group VMC pfs 'dh-group14'
set vpn ipsec esp-group VMC proposal 1 encryption 'aes256'
set vpn ipsec esp-group VMC proposal 1 hash 'sha256'
set vpn ipsec ike-group VMC close-action 'none'
set vpn ipsec ike-group VMC dead-peer-detection action 'restart'
set vpn ipsec ike-group VMC dead-peer-detection interval '15'
set vpn ipsec ike-group VMC dead-peer-detection timeout '30'
set vpn ipsec ike-group VMC ikev2-reauth 'yes'
set vpn ipsec ike-group VMC key-exchange 'ikev2'
set vpn ipsec ike-group VMC lifetime '28800'
set vpn ipsec ike-group VMC mobike 'disable'
set vpn ipsec ike-group VMC proposal 1 dh-group '14'
set vpn ipsec ike-group VMC proposal 1 encryption 'aes256'
set vpn ipsec ike-group VMC proposal 1 hash 'sha256'
set vpn ipsec ipsec-interfaces interface 'eth5'
set vpn ipsec nat-traversal 'enable'
set vpn ipsec site-to-site peer 203.0.113.20 authentication id '192.168.10.101'
set vpn ipsec site-to-site peer 203.0.113.20 authentication mode 'pre-shared-secret'
set vpn ipsec site-to-site peer 203.0.113.20 authentication pre-shared-secret 'myverysecretkey'
set vpn ipsec site-to-site peer 203.0.113.20 authentication remote-id '203.0.113.20'
set vpn ipsec site-to-site peer 203.0.113.20 connection-type 'respond'
set vpn ipsec site-to-site peer 203.0.113.20 description 'VMC PRIMARY TUNNEL'
set vpn ipsec site-to-site peer 203.0.113.20 ike-group 'VMC'
set vpn ipsec site-to-site peer 203.0.113.20 ikev2-reauth 'inherit'
set vpn ipsec site-to-site peer 203.0.113.20 local-address '192.168.10.101'
set vpn ipsec site-to-site peer 203.0.113.20 vti bind 'vti1'
```

```
set vpn ipsec site-to-site peer 203.0.113.20 vti esp-group 'VMC'
```

SDDC - Azure VPN Endpoint with IKEv2 (public IPs on both ends)

In this configuration, VPN gateway in Azure is one VPN endpoint and the other VPN endpoint resides on the SDDC running in VMware Cloud on AWS SDDC. Both the endpoints are configured with IKE version as IKEv2. Both the endpoints use Public IP addresses for establishing the IPSec tunnel. Following is the configuration for VPN endpoint in VMware Cloud on AWS SDDC and Azure VPN gateway.

VPN Type: Route-Based VPN, IKEv1

SDDC Configuration

```
Local IP Address: edge public IP 203.0.113.20
Remote IP Address: 198.51.100.20
IKE Type: IKEv2
Tunnel Encryption: AES 256
Tunnel Digest Algorithm: SHA2
IKE Encryption: AES 256
IKE Digest Algorithm: SHA2
Perfect Forward Secrecy: enabled
Preshared Key: myverysecretkey
Diffie Hellman: Group 14
BGP Local IP/Prefix Length: 169.254.98.10/30
BGP Remote IP: 169.254.98.9
BGP Remote ASN: 65515
SDDC ASN Setting: 65001
```

The following images show the different Azure configurations.

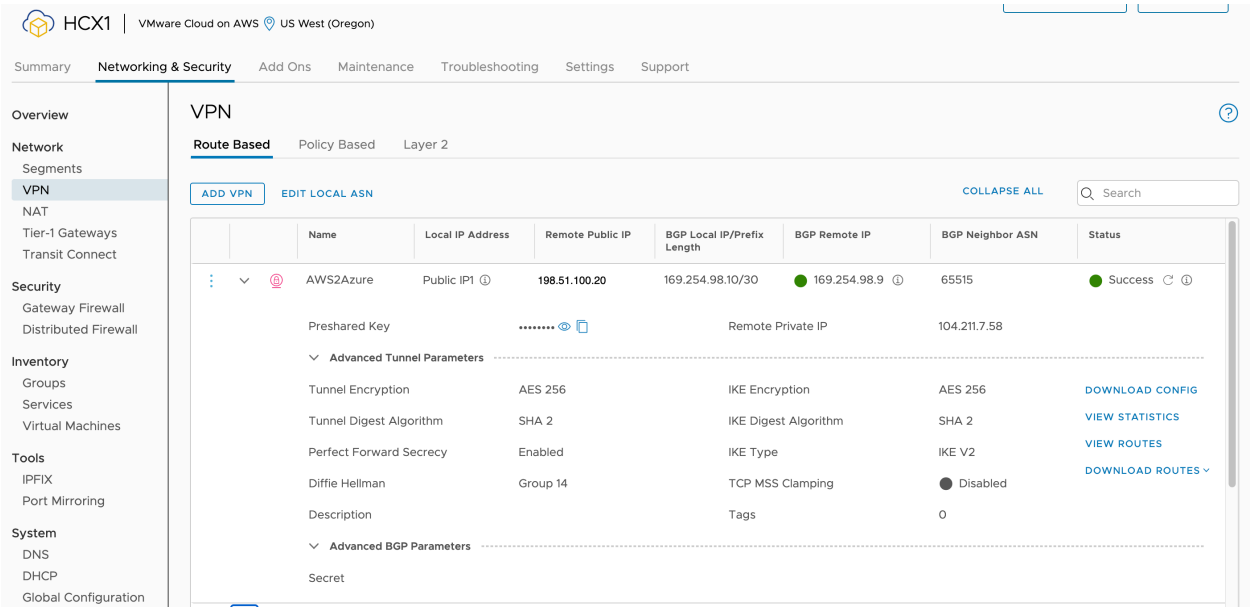

Figure 1 - VMware Cloud on AWS SDDC VPN configuration

Azure Configuration

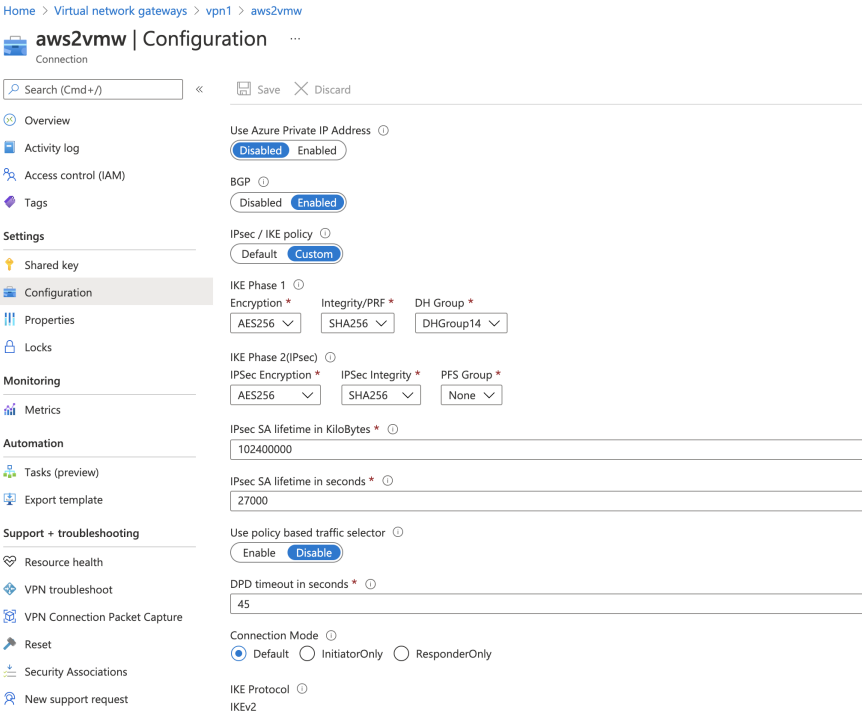

Figure 2 - Generic IPSec Configuration in Azure

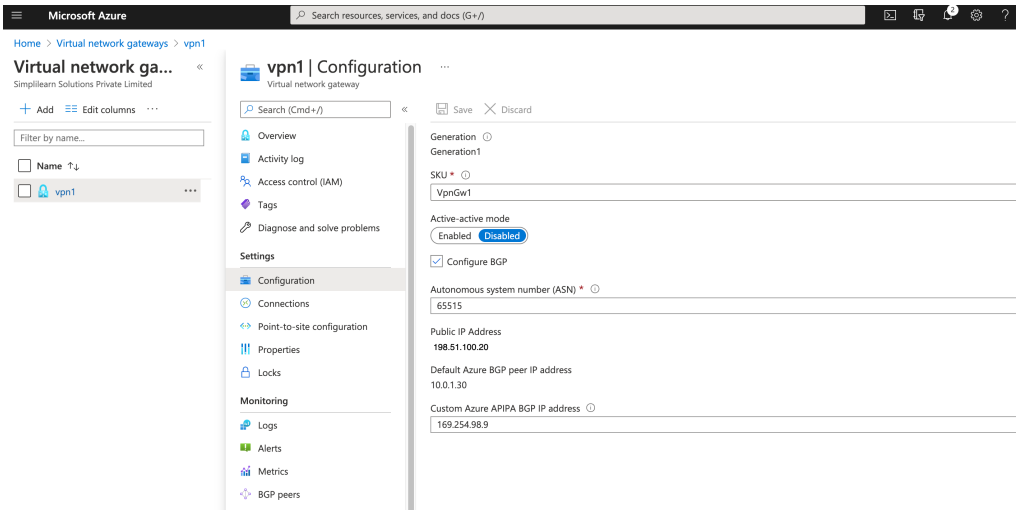

Figure 3 - VPN gateway configuration in Azure

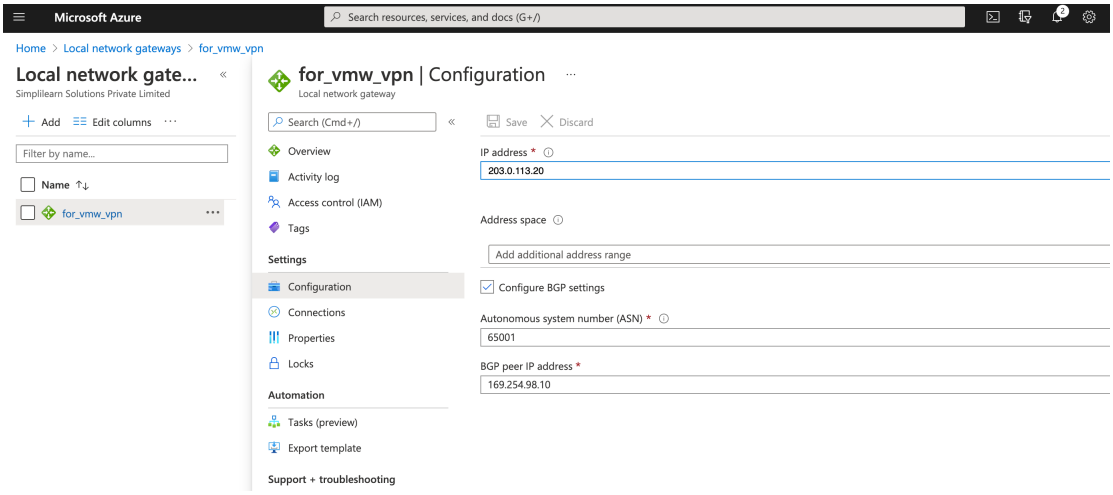

Figure 4 - Local network gateway configuration in Azure

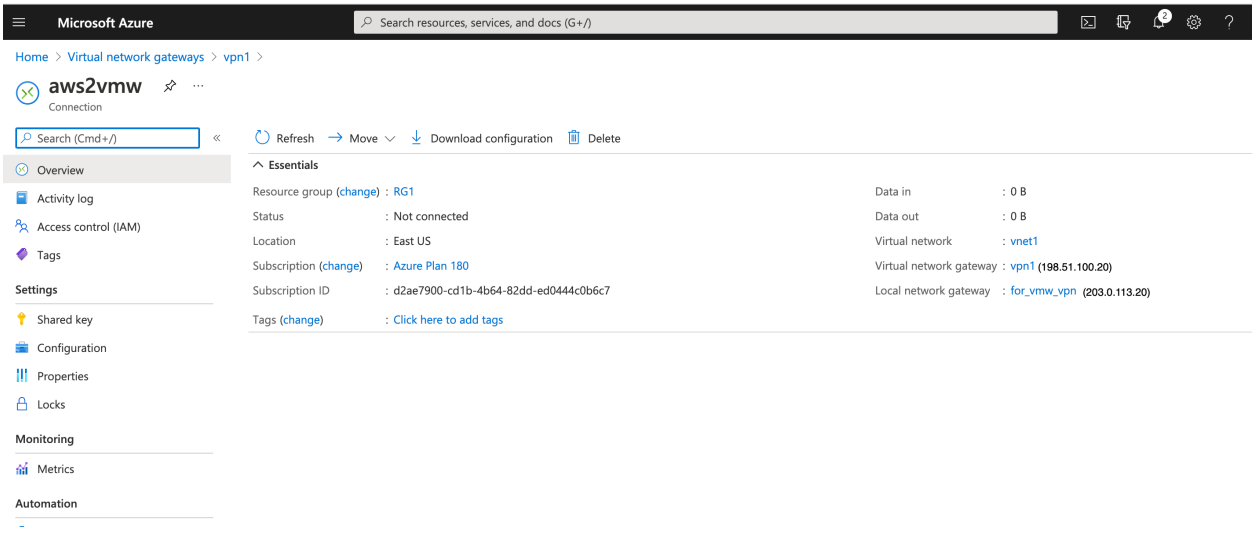

Figure 5 - Connection overview for IPSec in Azure

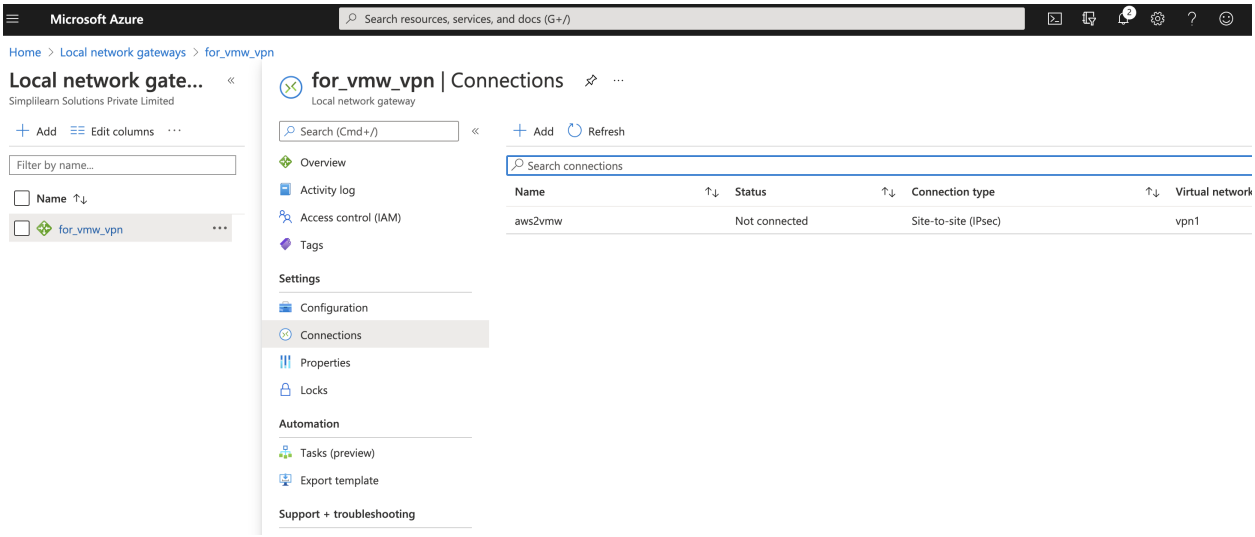

Figure 6 - IPSec connection status at local network gateway in Azure

Authors and Contributors

The following people have contributed the configuration included in this article:

Dustin Spinhirne

Sharath BN

Mithil Rangdale

Z House