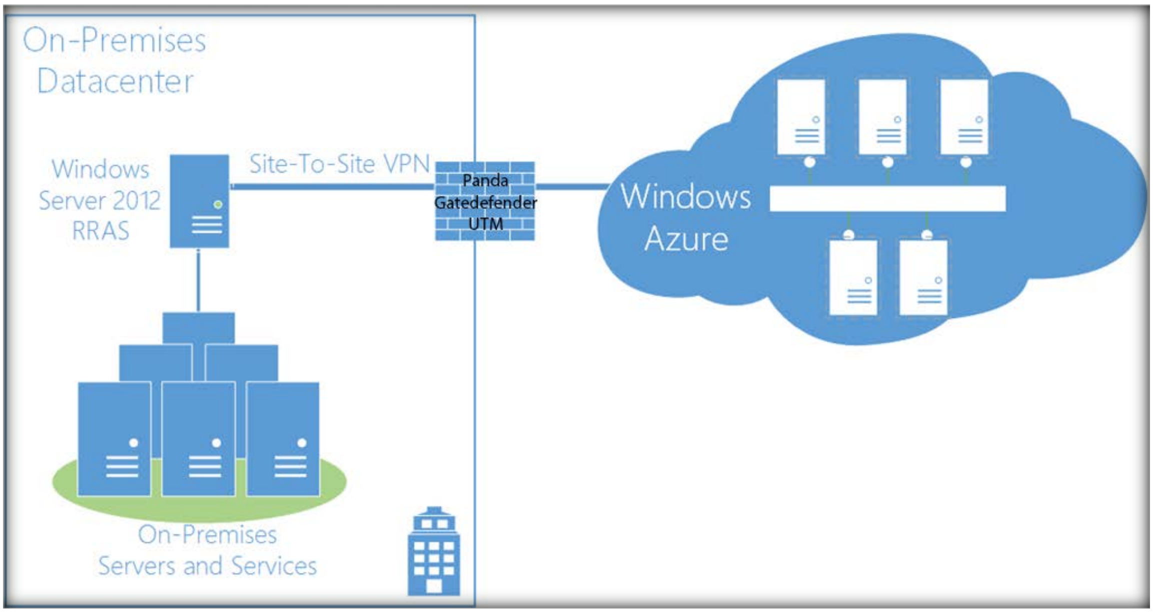
How to configure an IPSec VPN site-to-site with Microsoft Azure and Gatedefender v5.50.50

TechSupport Articles



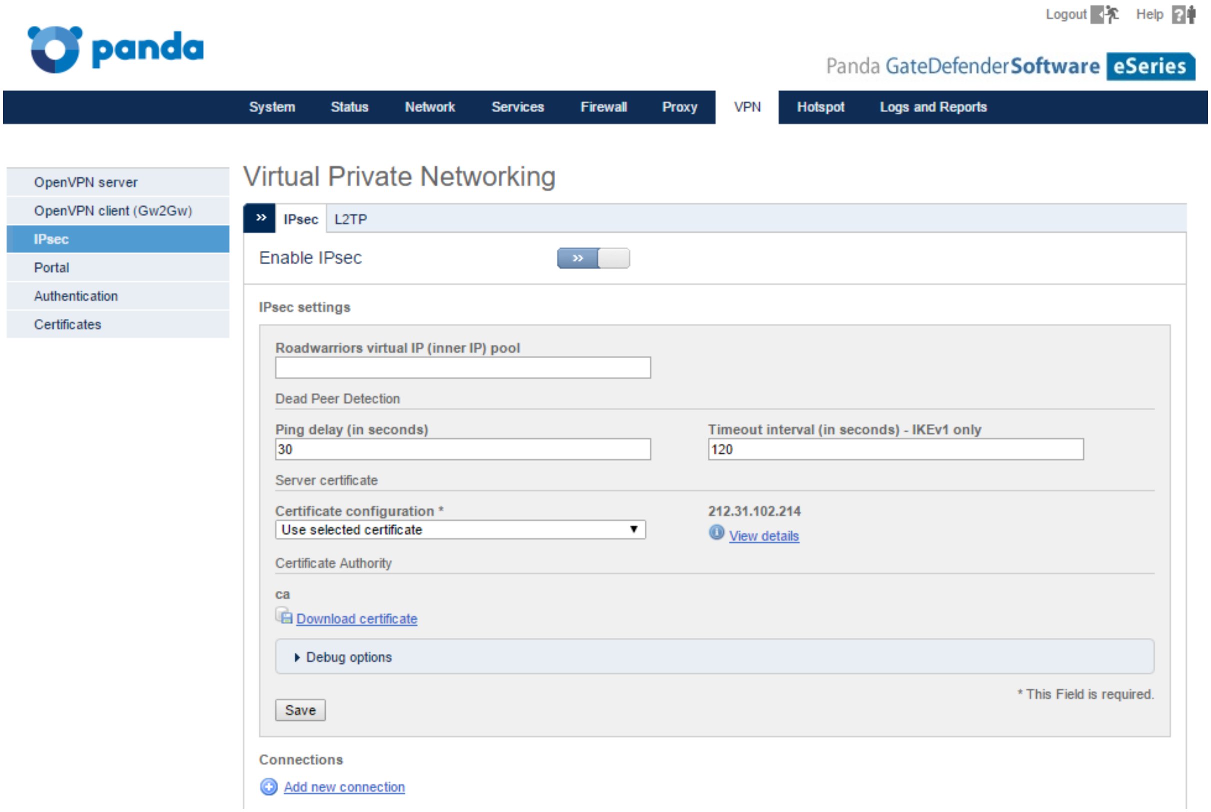
This HowTo explains how to configure a site-to-site with Microsoft Azure and Gatedefender eSeries v5.50.50

Before you begin:

1. Create and configure a Microsoft Azure static VPN Gateway for your virtual network.

Configure IPsec VPN site-to-site on the Gatedefender Appliance

1. Go to **VPN** menu → **IPsec**
2. Enable the IPsec.



Virtual Private Networking

Enable IPsec

IPsec settings

Roadwarriors virtual IP (inner IP) pool

Dead Peer Detection

Ping delay (in seconds): 30

Timeout interval (in seconds) - IKEv1 only: 120

Server certificate

Certificate configuration *: Use selected certificate

212.31.102.214

Certificate Authority

ca

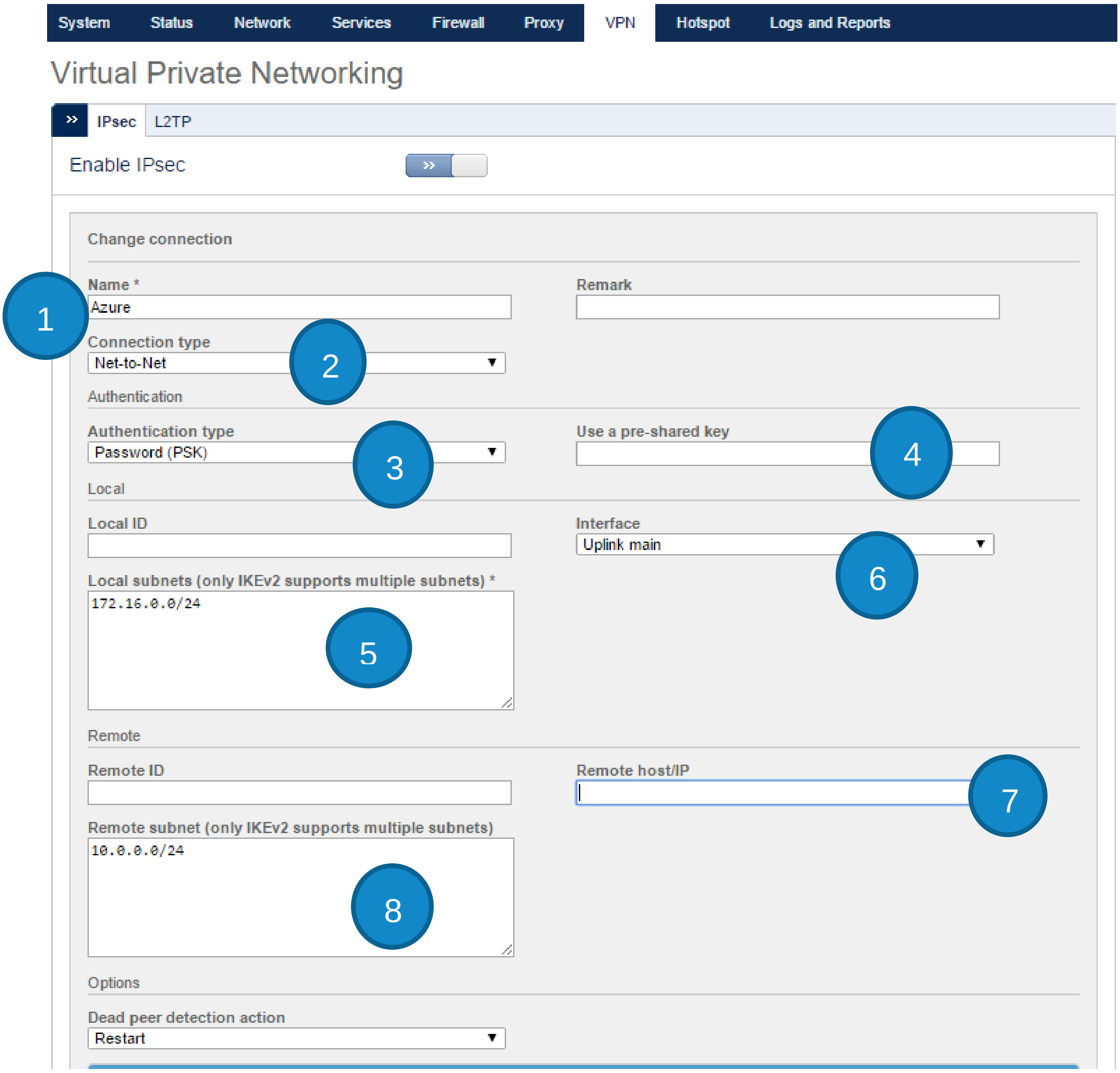
* This Field is required.

Connections

3. Press **Add new connection**.
4. On the new window you will to have configure the VPN connection according to the configuration that MS Azure portal will provide to you.

By default the MS VPN Portal will export a configuration file to import on a Cisco Device.

Since the VPN connection is an IPsec VPN tunnel, it will work with any devices that support the type of configuration that is required for MS Azure VPN Gateway.



Virtual Private Networking

Enable IPsec

Change connection

Name * Azure

Remark

Connection type Net-to-Net

Authentication

Authentication type Password (PSK)

Use a pre-shared key

Local

Local ID

Interface Uplink main

Local subnets (only IKEv2 supports multiple subnets) * 172.16.0.0/24

Remote

Remote ID

Remote host/IP

Remote subnet (only IKEv2 supports multiple subnets) 10.0.0.0/24

Options

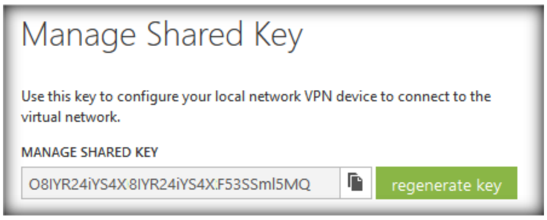
Dead peer detection action Restart

1: Type a name for this VPN connection. eg: Azure

2: Select **Net-to-Net** (Site to Site) VPN

3: **Authentication type:** select the Password (PSK)

4: **Pre-shared key:** Enter the shared key generated by your Azure VPN Gateway. *To view the shared key go to the DASHBOARD of your Azure network and click on the **Manage Key** icon in the bottom pane.



Manage Shared Key

Use this key to configure your local network VPN device to connect to the virtual network.

MANAGE SHARED KEY

O8IYR24iYS4X8IYR24iYS4XF53SSml5MQ

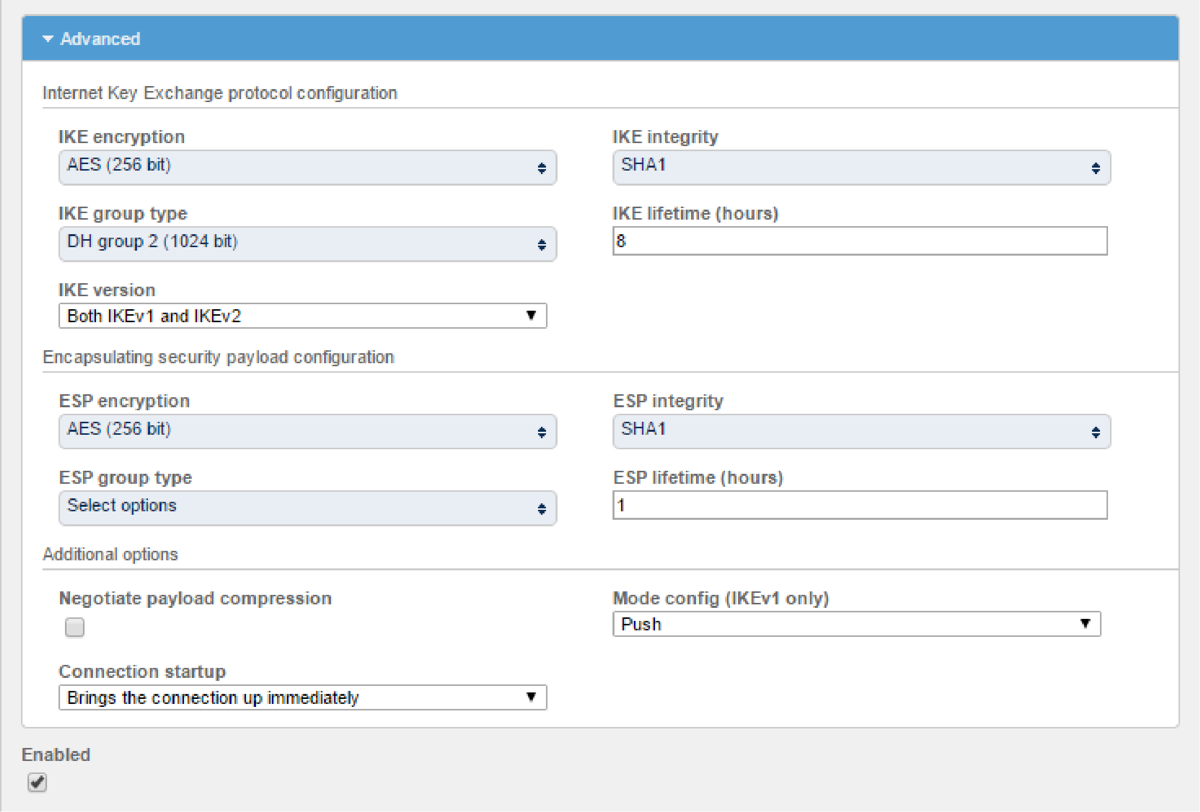
5: **Local subnet:** The subnet of the on premises network where the Gatedefender appliance is installed.

6: **Interface:** Select the interface that is associated with the public IP that you defined on the MS Azure VPN Gateway.

7: **Remote host/IP:** The Public of MS Azure VPN Gateway

8: **Remote subnet:** The subnet of the virtual network on MS Azure infrastructure.

Advanced Settings



Advanced

Internet Key Exchange protocol configuration

IKE encryption: AES (256 bit)

IKE integrity: SHA1

IKE group type: DH group 2 (1024 bit)

IKE lifetime (hours): 8

IKE version: Both IKEv1 and IKEv2

Encapsulating security payload configuration

ESP encryption: AES (256 bit)

ESP integrity: SHA1

ESP group type: Select options

ESP lifetime (hours): 1

Additional options

Negotiate payload compression: □

Mode config (IKEv1 only): Push

Connection startup: Brings the connection up immediately

Enabled: ☑

Internet Key Exchange protocol configuration

IKE Encryption: AES (256 bit)

IKE Integrity: SHA1

IKE group type: DH group 2 (1024 bit)

IKE lifetime: 8 hours

IKE version: By Default it's IKEv1.

Encapsulating security payload configuration

ESP encryption: AES (256 bit)

ESP Integrity: SHA1

ESP group type: NONE

ESP Lifetime (hours): 1

Mode config (IKEv1 only): Push

Connection startup: Bring the connection up immediately.

Finally, click **ADD**.

Example of the VPN Configuration file generated by MS Azure VPN Portal:

```
! Microsoft Corporation
! Windows Azure Virtual Network
! This configuration template applies to Cisco ASA 5500 Series Adaptive Security Appliances running ASA Software 8.3.
! It configures an IPSec VPN tunnel connecting your on-premise VPN device with the Azure gateway.

! ---------------------------------------------------------------------------------------------------------------------
! ACL and NAT rules
!
! Proper ACL and NAT rules are needed for permitting cross-premise network traffic.
! You should also allow inbound UDP/ESP traffic for the interface which will be used for the IPSec tunnel.
object-group network azure-networks
network-object 10.0.0.0 255.255.255.192
exit
object-group network onprem-networks
network-object 172.16.0.0 255.255.255.0
network-object 172.16.50.0 255.255.255.0
network-object 172.16.40.0 255.255.255.0
network-object 172.16.60.0 255.255.255.0
exit
```

```
access-list azure-vpn-acl extended permit ip object-group onprem-networks object-group azure-networks

nat (inside,outside) source static onprem-networks onprem-networks destination static azure-networks azure-networks


! ---------------------------------------------------------------------------------------------------------------

! Internet Key Exchange (IKE) configuration

!

! This section specifies the authentication, encryption, hashing, Diffie-Hellman, and lifetime parameters for the Phase

! 1 negotiation and the main mode security association. We have picked an arbitrary policy # "10" as an example. If

! that happens to conflict with an existing policy, you may choose to use a different policy #.

crypto isakmp enable outside

crypto isakmp policy 10

authentication pre-share

encryption aes-256

hash sha

group 2

lifetime 28800

exit


! ---------------------------------------------------------------------------------------------------------------

! IPSec configuration

!

! This section specifies encryption, authentication, and lifetime properties for the Phase 2 negotiation and the quick

! mode security association.

crypto ipsec transform-set azure-ipsec-proposal-set esp-aes-256 esp-sha-hmac

crypto ipsec security-association lifetime seconds 3600

crypto ipsec security-association lifetime kilobytes 102400000
```

```
! ---------------------------------------------------------------------------------------------------------------

! Crypto map configuration

!

! This section defines a crypto map that binds the cross-premise network traffic to the

! IPSec transform set and remote peer. We have picked an arbitrary ID # "10" as an example. If

! that happens to conflict with an existing crypto map, you may choose to use a different ID #.

crypto map azure-crypto-map 10 match address azure-vpn-acl

crypto map azure-crypto-map 10 set peer Public IP of MS Azure VPN Gateway*

crypto map azure-crypto-map 10 set transform-set azure-ipsec-proposal-set

! Note that you can only bind one crypto map to the "outside" interface. You can, however, define

! different peer/transform-set within a crypto map and identify them with different IDs.

crypto map azure-crypto-map interface outside


! ---------------------------------------------------------------------------------------------------------------

! Tunnel configuration

!

! This section defines an IPSec site-to-site tunnel connecting to the Azure gateway and specifies the
pre-shared key

! value used for Phase 1 authentication.

tunnel-group Public IP of MS Azure VPN Gateway*type ipsec-l2l

tunnel-group Public IP of MS Azure VPN Gateway*ipsec-attributes

pre-shared-key ********

exit


! ---------------------------------------------------------------------------------------------------------------

! TCPMSS clamping

!

! Adjust the TCPMSS value properly to avoid fragmentation

sysopt connection tcpmss 1350
```

```
exit
```

VPN Configuration from the Gatedefender Site:

```
2,on,Azure,,net,psk,Preshared Key,,,172.16.0.0/24,,Public IP of MS Azure VPN
Gateway,10.0.0.0/24,off,off,off,off,8,1,aes256,sha1,1024,aes256,sha1,,off,,UPLINK:
main,restart,off,,,push,start
```