IPsec VPN to Azure with virtual network gateway

https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/255100/ipsec-vpn-to-azure-with-virtual-network-gateway

Prerequisites

- A FortiGate with an Internet-facing IP address
- A valid Microsoft Azure account

Sample topology

Image not found or type unknown

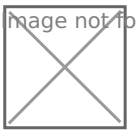
Sample configuration

This sample configuration shows how to:

1. Configure an Azure virtual network.
2. Specify the Azure DNS server.
3. Configure the Azure virtual network gateway.
4. Configure the Azure local network gateway.
5. Configure the FortiGate tunnel.
6. Create the Azure firewall object.
7. Create the FortiGate firewall policies.
8. Create the FortiGate static route.

9. Create the Azure site-to-site VPN connection.
10. Check the results.

To configure an Azure virtual network:

1. Log in to Azure and click *New*.
2. In *Search the Marketplace*, type *Virtual network*.
3. Click *Virtual network* to open the *Virtual network* pane.


4. At the bottom of the *Virtual network* pane, click the *Select a deployment model* dropdown list and select *Resource Manager*.
5. Click *Create*.

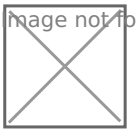

6. On the *Create virtual network* pane, enter you virtual network settings, and click *Create*.

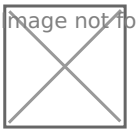

To specify the Azure DNS server:

1. Open the virtual network you just created.
2. Click *DNS servers* to open the *DNS servers* pane.
3. Enter the IP address of the DNS server and click *Save*.


To configure the Azure virtual network gateway:

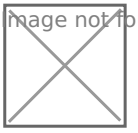
1. In the portal dashboard, go to *New*.
2. Search for *Virtual Network Gateway* and click it to open the *Virtual network gateway* pane.


3. Click *Create Virtual network gateways* and enter the settings for your virtual network gateway.


4. If needed, create a Public IP address.


5. Click *Create*.

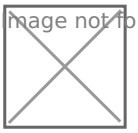
Creating the virtual network gateway might take some time. When the provisioning is done, you'll receive a notification.



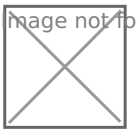
To configure the Azure local network gateway:

1. In the portal dashboard, click *All resources*.
2. Click *Add* and then click *See all*.

3. In the *Everything* pane, search for *Local network gateway* and then click *Create local network gateway*.



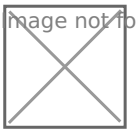
4. For the *IP address*, enter the local network gateway IP address, that is, the FortiGate's external IP address.



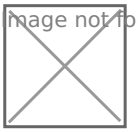
5. Set the remaining values for your local network gateway and click *Create*.

To configure the FortiGate tunnel:

1. In the FortiGate, go to *VPN > IP Wizard*.
2. Enter a *Name* for the tunnel, click *Custom*, and then click *Next*.



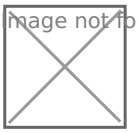
3. Configure the *Network* settings.
   - For *Remote Gateway*, select *Static IP Address* and enter the IP address provided by Azure.
   - For *Interface*, select *wan1*.
   - For *NAT Traversal*, select *Disable*,
   - For *Dead Peer Detection*, select *On Idle*.
   - In the Authentication section, select
4. Configure the *Authentication* settings.
   - For *Method*, select *Pre-shared Key* and enter the *Pre-shared Key*.
   - For *IKE*, select *2*.



5. Configure the *Phase 1 Proposal* settings.
   - Set the Encryption and Authentication combination to the three supported encryption algorithm combinations accepted by Azure.

    - AES256 and SHA1
    - 3DES and SHA1
    - AES256 and SHA256
  - For *Diffie-Hellman Groups*, select *2*.
  - Set *Key Lifetime (seconds)* to *28800*.

Image not found or type unknown



6. In *Phase 2 Selectors*, expand the *Advanced* section to configure the *Phase 2 Proposal* settings.
   - Set the Encryption and Authentication combinations.
     - AES256 and SHA1
     - 3DES and SHA1
     - AES256 and SHA256
   - Uncheck *Enable Perfect Forward Secrecy (PFS)*.
   - Set *Key Lifetime (seconds)* to *27000*.

Image not found or type unknown

7. Click *OK*.

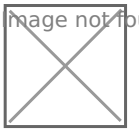
To create the Azure firewall object:

1. In the FortiGate, go to *Policy & Objects* > *Addresses*.
2. Create a firewall object for the Azure VPN tunnel.

To create the FortiGate firewall policies:

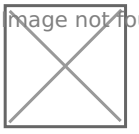
1. In the FortiGate, go to *Policy & Objects* > *IPv4 Policy*.
2. Create a policy for the site-to-site connection that allows outgoing traffic.
   - Set the *Source* address and *Destination* address using the firewall objects you just created.
   - Disable *NAT*.

Image not found or type unknown



3. Create another policy that allows incoming traffic.
   - For this policy, reverse the *Source* address and *Destination* address.

Image not found or type unknown



4. We recommend limiting the TCP maximum segment size (MSS) being sent and received so as to avoid packet drops and fragmentation.
   To do this, use the following CLI commands on both policies.

```
config firewall policy
  edit <policy-id>
    set tcp-mss-sender 1350
```

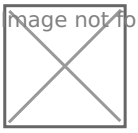
```
    set tcp-mss-receiver 1350
  next
end
```

To create the FortiGate static route:

1. In the FortiGate, go to *Network > Static Routes*.
2. Create an IPv4 Static Route that forces outgoing traffic going to Azure to go through the route-based tunnel.
3. Set the *Administrative Distance* to a value lower than the existing default route value.

To create the Azure site-to-site VPN connection:

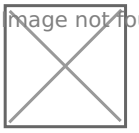
1. In the Azure portal, locate and select your virtual network gateway.
2. In the *Settings* pane, click *Connections* and then click *Add*.



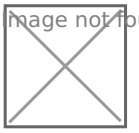
3. Enter the settings for your connection. Ensure the *Shared Key (PSK)* matches the *Pre-shared Key* for the FortiGate tunnel.

To check the results:

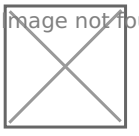
1. In the FortiGate, go to *Monitor > IPsec Monitor*.
   - Check that the tunnel is up.



   - If the tunnel is down, right-click the tunnel and select *Bring Up*.



2. In the FortiGate, go to *Log & Report > Events*.
   - Select an event to view more information and verify the connection.
3. In the Azure portal dashboard, click *All resources* and locate your virtual network gateway.
   1. In your virtual network gateway pane, click *Connections* to see the status of each connection.



   2. Click a connection to open the *Essentials* pane to view more information about that connection.
      - If the connection is successful, the *Status* shows *Connected*.
      - See the *ingress* and *egress* bytes to confirm traffic flowing through the tunnel.

Revision #1
Created 14 October 2024 16:30:08 by ColtM

Updated 14 October 2024 16:30:38 by ColtM