BIG-IP Secure IPsec Tunneling: From a Data Center Network to a Microsoft Azure Network

Overview: Using IPsec on the BIG-IP system to establish a secure network

This document guides you through the steps to configure a site-to-site (S2S) VPN tunnel connection from a corporate data center to an Microsoft Azure virtual network (VNet).

Watch an overview of BIG-IP IPsec tunneling and how to set up a secure tunnel to an Azure virtual network

Before you can set up a S2S VPN tunnel, you need to create a virtual network, gateway subnet in Azure, and complete other Azure VPN configuration steps. These are all beyond the scope of this document. For details, see *Create a VNet with a Site-to-Site connection using PowerShell* at `https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-create-site-to-site-rm-powershell/`

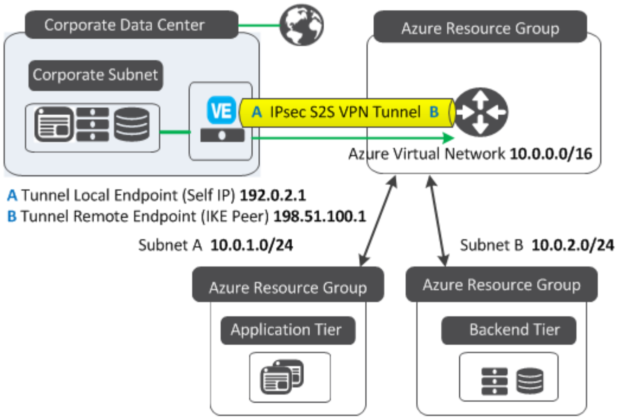

Figure 1: Sample configuration of a corporate data center and Azure resource groups connected by an IPsec site-to-site VPN tunnel

This illustration shows:

- A corporate data center, which includes a BIG-IP® VE and is where databases live.
- An Azure resource group, which contains a VNet. This VNet acts as a central hub for taking care of routing out to additional subnets.
- Additional Azure resource groups, which host applications and appliances.

In order for the databases in the corporate data center to contact the applications in Azure, you need to set up a VPN tunnel between the BIG-IP VE and Azure VNet.

How do I set up a secure tunnel to an Azure virtual network?

You should follow all of the tasks in this document, in the order shown.

Define an IKE Phase 2 security policy

Use these steps to configure the Internet Key Exchange (IKE) Phase 2 settings (authentication & encryption algorithms and perfect forward secrecy) for tunnel traffic.

In case you are not familiar with IKE, *IKE Phase 2* is where *security associations* (a set of policy and key[s] used to protect information) are negotiated on behalf of services such as IPsec, or any other service that needs key material and/or parameter negotiation.

Watch how to define an IKE Phase 2 security policy

1. On the Main tab, click **Network** > **IPsec** > **IPsec Policies**.
   The IPsec Policies screen opens.
2. Click the **Create** button.
   The New Policy screen opens.
3. Configure the settings described in this table. For all other settings, use the defaults.

Section	Setting	Details
General Properties	**Name**	Type a unique name for the IPsec policy, such as `my_ipsec_policy`.
Configuration	**Mode**	Select **IPsec Interface**.
IKE Phase 2	**Authentication Algorithm**	Select **SHA-1**.
IKE Phase 2	**Encryption Algorithm**	Select **AES-256**.
IKE Phase 2	**Perfect Forward Secrecy**	Select **MODP1024**.

4. Click **Finished**.
   The screen refreshes and displays the new IPsec policy in the list.

Define eligible web traffic for the secure tunnel

Use these steps to direct web traffic into the secure tunnel.

The *traffic selector* (a packet filter that defines which traffic should be handled by an IPsec policy) filters traffic based on the IP addresses and port numbers that you specify, as well as the custom IPsec policy you assign.

Watch how to define eligible web traffic for the secure tunnel

1. On the Main tab, click **Network** > **IPsec** > **Traffic Selectors**.
   The Traffic Selector screen opens.
2. Click **Create**.

The New Traffic Selector screen opens.

3. Configure the settings described in this table. For all other settings, use the defaults.

Section	Setting	Details
General Properties	**Name**	Type a unique name for the traffic selector, such as `my_traffic_selector`.
General Properties	**Order**	Specify the order in which traffic is matched. For example, select **Specify** and type `1`.
Configuration	**Source IP Address or CIDR**	Type the host or network address from which the application traffic originates. For example, `192.168.60.0/24`.
Configuration	**Destination IP Address or CIDR**	Type the final host or network address to which the application traffic is destined. For example, `172.16.101.0/24`.
Configuration	**IPsec Policy Name**	Select the name of the IPsec policy that you created. For example, `my_ipsec_policy`.

4. Click **Finished**.
   The screen refreshes and displays the new IPsec traffic selector in the list.

Define IKE Phase 1 tunnel negotiation parameters

Use these steps to configure negotiation to authenticate Internet Key Exchange (IKE) peers and to encrypt IKE communication.

During IKE Phase 1, *IKE peers*, a configuration object of the IPsec protocol that represents a BIG-IP® system on each side of the IPsec tunnel, allow two systems to authenticate each other.

▶ *Watch how to define IKE Phase 1 tunnel negotiation parameters*

1. On the Main tab, click **Network** > **IPsec** > **IKE Peers**.
   The IKE Peers screen opens.
2. Click the **Create** button.
   The New IKE Peer screen opens.
3. Configure the settings described in this table. For all other settings, use the defaults.

Section	Setting	Details
General Properties	**Name**	Type a unique name for the IKE peer, such as `my_ike_peer`.
General Properties	**Remote Address**	Type the IP address of the device that is remote to the system you are configuring. For example, `198.51.100.1`.
General Properties	**Version**	Select the **Version 2** check box.
IKE Phase 1 Algorithms	**Encryption Algorithm**	Select **AES256**.
IKE Phase 1 Credentials	**Authentication Method**	Select **Preshared Key**.
IKE Phase 1 Credentials	**Preshared Key** and **Verify Preshared Key**	Type a string that the IKE peers share for authenticating each other.

Section	Setting	Details
Common Settings	**Traffic Selector**	Under the **Available** setting, select a **Traffic Selector**, and move it under **Selected**. For example, select and move `my_traffic_selector`.
Common Settings	**Presented ID Value**	Type the IP address for **Override** For example, `192.0.2.1`.
Common Settings	**Verified ID Value**	Type the IP address for **Override** For example, `198.51.100.1`.

4. Click **Finished**.
   The screen refreshes and displays the new IKE peer in the list.

Create a virtual interface for routing traffic through the tunnel

Use these steps to create an IPsec interface profile to filter traffic through the tunnel according to the traffic selector you specify.

The *parent profile* specifies the profile from which the newly created profile inherits settings.

▶ *Watch how to create a virtual interface for routing traffic through the tunnel*

1. On the Main tab, click **Network** > **Tunnels** > **Profiles** > **IPsec Interface**.
   The IPsec Interface screen opens.
2. Click the **Create** button.
   The New Policy screen opens.
3. In the **Name** field, type a unique name for the profile, such as `my_ipsec_profile`.
4. From the **Parent Profile** list, retain the default selection, **ipsec**.
5. On the right side of the screen, select the **Custom** check box.
6. In the Settings area, from the **Traffic Selector** list, select the traffic selector for the IPsec interface tunnel to which the profile is applied, such as `my_traffic_selector`.
7. Click **Finished**.
   The screen refreshes and displays the new IPsec policy in the list.

Create a tunnel by assigning endpoints and direction

Use these steps to create an IPsec tunnel on the BIG-IP® system and specify how the tunnel carries traffic.

When configuring a new tunnel, the default setting for **Mode** is **Bidirectional**, but this document only describes how to set up a tunnel for *outbound* traffic; that is, IPsec tunneling from a corporate data center network to a Microsoft Azure network.

▶ *Watch how to create a tunnel by assigning endpoints and direction*

1. On the Main tab, click **Network** > **Tunnels** > **Tunnel List** > **Create**.
   The New Tunnel screen opens.
2. Configure the settings described in this table. For all other settings, use the defaults.

Setting	Details
Name	Type a unique name for the tunnel, such as `my_tunnel`.

Setting	Details
Profile	Select the profile associated with the tunnel for handling traffic, such as `my_ipsec_profile`.
Local Address	Type the IP address of the local endpoint of the tunnel. For example, `192.0.2.1`.
Remote Address	Type the IP address of the remote endpoint of the tunnel. For example, `198.51.100.1`.

3. Click **Finished**.
   The screen refreshes and displays the new tunnel in the list.

Create IP addresses for local and remote tunnel endpoints

Before starting, make sure you have created a tunnel.

Use these steps to create tunnel endpoints. You start by first creating a tunnel local endpoint and then repeat the steps a second time to create a tunnel remote endpoint.

Watch how to create IP addresses for local and remote tunnel endpoints

1. On the Main tab, click **Network** > **Self IPs**.
   The Self IP screen opens.
2. Click **Create**.
   The New Self IP screen opens.
3. Configure the settings described in this table. For all other settings, use the defaults.

Setting	Details
Name	Type a unique name for the self IP address, such as `my_self_ip`.
IP Address	Type the IP address of the tunnel local endpoint. For example, `192.0.2.1`.
Netmask	Type the netmask for the specified IP address. For example, `255.255.255.0`.
Port Lockdown	Select **Allow All**.

4. Click **Finished**.
   The screen refreshes, and displays the new self IP address in the list.
5. Repeat the previous steps, but this time type a name and an IP address for a remote tunnel endpoint. For example, you can type `my_ipesec_tunnel`, and `10.23.54.2`. When repeating the steps, for the **VLAN/Tunnel** setting, select the name of the tunnel you created, such as `my_tunnel`. The first time through, for the **VLAN/Tunnel** setting, you retained the default setting (**External**).

Add a static route for web traffic

Before you start this task, make sure you've created a tunnel and have assigned a self IP address to the tunnel.

Use these steps to route traffic from a BIG-IP® system to an Azure virtual network and to specify the virtual interface as the gateway for the route.

A *static route* with the newly created tunnel allows any traffic hitting the BIG-IP system and destined for the specified subnet to be routed through the tunnel.

Watch how to add a static route for web traffic

1. On the Main tab, click **Network** > **Routes**.
   The Routes screen opens.
2. Click **Add**.
   The New Route screen opens.
3. Configure the settings described in this table. For all other settings, use the defaults.

Setting	Details
Name	Type a unique name for the static route, such as `my_static_route`.
Destination	Type a destination IP address for the route. For example, `172.16.101.0`.
Netmask	Type the netmask for the destination IP address. For example, `255.255.255.0`.
Resource	Select **Use VLAN/Tunnel**.
VLAN/Tunnel	Select the VLAN associated for the specified self IP address, such as `my_tunnel`.

4. Click **Finished**.
   The screen refreshes and displays the new static route in the list.

Disable load balancing and forward web traffic through the tunnel

Use these steps to create a forwarding virtual server to move traffic to the destination address.

Selecting **Forwarding (IP)** for **Type** specifies a virtual server like other virtual servers, except that the virtual server has no pool members to load balance. The virtual server forwards the packet directly to the destination IP address specified in the client request.

Watch how to forward web traffic through the tunnel

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the **Create** button.
   The New Virtual Server screen opens.
3. Configure the settings described in this table. For all other settings, use the defaults.

Section	Setting	Details
General Properties	**Name**	Type a unique name for the virtual server, such as `my_forwarding_vs`.
General Properties	**Type**	Select **Forwarding (IP)**.
General Properties	**Source Address**	Type an IP address from which the virtual server accepts traffic. For example, `0.0.0.0/0`.
General Properties	**Destination Address/ Mask**	Type an IP address to which the virtual server sends traffic. For example, `0.0.0.0/0`.
General Properties	**Service Port**	Type a service port number and select *** All Ports**. For example, `0`.
Configuration	**Protocol**	Select **All Protocols**.

4. Click **Finished**.

The screen refreshes and displays the virtual server in the list.

5. Select the check box for the virtual server and click **Enable**.

Other resources

For information about IKE or related industry-standard technologies, see the relevant IETF RFCs (Request for Comments).

For information about the F5 BIG-IP® platform and Microsoft Azure, see *The BIG-IP® Platform and Microsoft Azure: Application Services in the Cloud* whitepaper at `https://f5.com`.

For information about the F5 BIG-IP Virtual Edition and Azure, see *BIG-IP® Virtual Edition and Microsoft Azure: Setup* on the AskF5™ Knowledge Base at `http://support.f5.com`.

For information about Azure VPN Gateway documentation, see *Create a VNet with a Site-to-Site connection using PowerShell* at `https://azure.microsoft.com/en-us/documentation/articles/vpn-gateway-create-site-to-site-rm-powershell/`.

For videos that walk you through common business tasks, see: `https://www.youtube.com/playlist?list=PLyqga7AXMtPPi-MPCs8eC2b3EZDNqHuBO`

Or, search for *F5: Make It Work!* on our DevCentral™ YouTube™ channel.