{:new_window: target="_blank"} {:shortdesc: .shortdesc} {:screen: .screen} {:codeblock: .codeblock} {:pre: .pre} {:tip: .tip} {:note: .note} {:preview: .preview} {:important: .important} {:deprecated: .deprecated} {:external: target="_blank" .external}

Managing VPN connections

{: #VPN-connections}

Use Virtual Private Networking (VPN) to manage the Power Systems Virtual Servers remotely and securely over the IBM Cloud® private network. You can use VPN to log in to the private network, complete your work securely, and log out. This capability offers you site-to-site IP security (IPsec) VPN between your on-premises location and the Power Systems Virtual Servers to enable low-cost secure connectivity.

With VPN access, you can:

- Establish a VPN connection to the private network via Secure Sockets Layer (SSL) or IPsec.
- Access your Virtual Servers through the primary private IP address by Secure Shell (SSH) or Remote Desktop Protocol (RDP).
- Connect to your Virtual Server’s Intelligent Platform Management Interface (IPMI) IP address for low-level server management or rescue needs.

Each of your accounts can be provided with VPN access and it can be limited to the subnets to which it needs access. You must have VPN access that is enabled and a VPN password that is specified before you attempt to log in to the VPN services. You can use VPN for Virtual Private Cloud (VPC) to securely connect your VPC to an on-premises network through a VPN tunnel, for more information see Connecting to your on-premises network.

A maximum of four VPN connections are supported for one account. Maximum number of policies (IKE and IPsec) is limited to four. {: important}

To learn more about using the command-line interface for VPN connections, see IBM Power Systems Virtual Servers CLI Reference.

Creating VPN connections

{: #creating-VPN-connections}

You can create a new VPN connection by using the `ibmcloud pi vpn-connection-create` command. For more information on creating, viewing, updating, or deleting a VPN section, see VPN connections.

You can view allowable and default values for attributes when you are creating Internet Key Exchange (IKE) and IPsec policies for a VPN connection.

IKE Policy version 2 is not compatible with policy-based VPN connections. If you attempt to combine the two, it results in an error. {: important}

Creating IKE and IPsec policies

{: #creating-IKE-policies}

When you create your VPN connection, you must set the IKE policy and IPsec policy. IBM provides default IKE policy and IPsec policy. You can also create your custom policies based on your requirements.

Adding a VPN IKE policy

{: #adding-IKE-policies}

You can use the default or custom IKE policies to define security parameters to use during Phase 1 of IKE negotiation. In this phase, the VPN and peer device exchange credentials and security policies to authenticate each other and establish a secure communication channel to be used for Phase 2 negotiation.

You can add an IKE policy by using the `ibmcloud pi vpn-ike-policy-add` command. For more information on adding, viewing, updating, or deleting an IKE policy, see VPN IKE policy.

Adding and configuring IPsec policy

{: #adding-IPsec-policies}

You can use default or custom IPsec policies to define security parameters to use during Phase 2 of IKE negotiation. In this phase, the VPN and peer device use the security association that is established during Phase 1 to negotiate what traffic to send and how to authenticate and encrypt that traffic.

You can add an IPsec policy by using the `ibmcloud pi vpn-ipsec-policy-add` command. For more information on adding, viewing, updating, or deleting an IPsec policy, see the VPN IPsec policy.

Attaching subnets to VPN connections

{: #attach_subnets_VPN}

If you create a Power Systems Virtual Servers service that contains VPN connections, you also have Local subnets and Peer subnets that are connected to the VPN connection.

You must route Power Systems Virtual Server private network subnets over VPN connections to allow access to your Power Systems Virtual Server over private network. When you create subnet or edit details of subnet, you can attach an existing VPN connection to the subnet.

For more information on attaching or detaching subnets, see the VPN subnets.