Firepower Threat Defense VPN Deployments

About Firepower Threat Defense Site-to-site VPNs

Firepower Threat Defense site-to-site VPN supports the following features:

- Both IPsec IKEv1 & IKEv2 protocols are supported.
- Automatic or manual preshared keys for authentication.
- IPv4 & IPv6. All combinations of inside and outside are supported.
- Static and Dynamic Interfaces.
- Support for both Firepower Management Center and Firepower Threat Defense HA environments.
- VPN alerts when the tunnel goes down.
- Tunnel statistics available using the Firepower Threat Defense Unified CLI.

VPN Topology

To create a new site-to-site VPN topology you must, at minimum, give it a unique name, specify a topology type, choose the IKE version that is used for IPsec IKEv1 or IKEv2, or both. Also, designate a preshared key. Once configured, you deploy the topology to Firepower Threat Defense devices. The Firepower Management Center configures site-to-site VPNs on Firepower Threat Defense devices only.

You can select from three types of topologies, containing one or more VPN tunnels:

- Point-to-point (PTP) deployments establish a VPN tunnel between two endpoints.
- Hub and Spoke deployments establish a group of VPN tunnels connecting a hub endpoint to a group of spoke nodes.
- Full Mesh deployments establish a group of VPN tunnels among a set of endpoints.

IPsec and IKE

In the Firepower Management Center, site-to-site VPNs are configured based on IKE policies and IPsec proposals that are assigned to VPN topologies. Policies and proposals are sets of parameters that define the characteristics of a site-to-site VPN, such as the security protocols and algorithms that are used to secure traffic in an IPsec tunnel. Several policy types may be required to define a full configuration image that can be assigned to a VPN topology.

Authentication

Define a preshared key for VPN authentication. You can manually specify a default key to use in all the VPN nodes in a topology, or have the Firepower Management Center automatically generate one.

Extranet Devices

Each topology type can include Extranet devices, devices that you do not manage in Firepower Management Center. These include:

- Cisco devices that Firepower Management Center supports, but for which your organization is not responsible. Such as spokes in networks managed by other organizations within your company, or a connection to a service provider or partner's network.
- Non-Cisco devices. You cannot use Firepower Management Center to create and deploy configurations to non-Cisco devices.

Add non-Cisco devices, or Cisco devices not managed by the Firepower Management Center, to a VPN topology as "Other" devices. Also specify the IP address of each remote device.

VPN Licensing

There is no specific licensing for enabling Firepower Threat Defense VPN, it is available by default.

The Firepower Management Center determines whether to allow or block the usage of strong crypto on a Firepower Threat Defense device based on attributes provided by the smart licensing server.

This is controlled by whether you selected the option to allow export-controlled functionality on the device when you registered with Cisco Smart License Manager. If you are using the evaluation license, or you did not enable export-controlled functionality, you cannot use strong encryption.

Firepower Threat Defense Site-to-site VPN Guidelines and Limitations

- PKI Certification is not supported. Only preshared keys are supported for authentication.
- A VPN connection can only be made across domains by using an extranet peer for the endpoint not in the current domain.
- A VPN topology cannot be moved between domains.
- Network objects with a 'range' option are not supported in VPN
- Firepower Threat Defense VPNs are only be backed up using the Firepower Management backup.

- The Firepower Threat Defense VPNs do not currently support PDF export and policy comparison.
- There is no per-tunnel or per-device edit option for Firepower Threat Defense VPNs, only the whole topology can be edited.
- Firepower Threat Defense VPNs are not supported in clustered environment.
- Tunnel status is not updated in realtime, but at an interval of 5 minutes in the Firepower Management Center.
- Transport mode is not supported, only tunnel mode. IPsec tunnel mode encrypts the entire original IP datagram which becomes the payload in a new IP packet. Use tunnel mode when the firewall is protecting traffic to and from hosts positioned behind a firewall. Tunnel mode is the normal way regular IPsec is implemented between two firewalls (or other security gateways) that are connected over an untrusted network, such as the Internet.