



Virtual Private Network Features

This chapter provides high-level information to configure the ASA Virtual Private Network features in Secure Firewall Threat Defense using Secure Firewall Management Center.

- [Site-to-Site VPN, on page 1](#)
- [Remote Access VPN, on page 2](#)

Site-to-Site VPN

Table 1: Site-to-Site VPN

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
LAN-to-LAN IPsec	<p>Policy-based VPN</p> <p>UI path: Devices > Site To Site > Policy Based (Crypto Map).</p> <p>See: Configure a Policy-based Site-to-Site VPN.</p> <p>How-To: Configure a Policy-based Site-to-Site VPN, Customize IKE Options for an Existing Site-to-Site VPN Deployment, Customize IPsec Options for an Existing Site-to-Site VPN Deployment, Customize Advanced Settings for an Existing Site-to-Site VPN Deployment</p>	The management center provides a single wizard to configure VPN on the peers.
Virtual Tunnel Interface (VTI)	<p>Route-based VPN</p> <p>UI path: Devices > Site To Site > Route Based (VTI).</p> <p>See: Create a Route-based Site-to-Site VPN.</p> <p>How-To: Create a route-based VPN (VTI), Configure a Static Route for VTI, Configure BGP routing for VTI, Configure an access control rule to allow encrypted traffic over VTI</p>	<p>Creating a VPN between a hub with a dynamic VTI and spokes with static VTIs is much easier in management center using the wizard.</p> <p>There is no wizard in ASDM.</p>
Umbrella SASE	<p>Deploy a SASE Tunnel on Umbrella</p> <p>UI path: Devices > VPN > Site To Site > +SASE Topology.</p> <p>See: Deploy a SASE Tunnel on Umbrella.</p>	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Monitor Site-to-Site VPN	Monitor the Site-to-Site VPN UI path: Overview > Dashboards > Site to Site VPN. See: Monitor the Site-to-Site VPN.	

Remote Access VPN

Table 2: Remote Access VPN

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
Remote Access IPsec (IKE v2) VPN	Remote Access VPN Policy UI path: Devices > VPN > Remote Access > Policy Assignment > VPN Protocols > IPsec-IKEv2. See: Configuring a Remote Access VPN Connection. How-To: <ul style="list-style-type: none"> Configuring Traffic Filtering for Remote Access (RA) VPN Connections—Creating an Extended Access List for Filtering Traffic on an RA VPN Connection, Adding an Extended Access List to a Group Policy for Filtering Traffic on an RA VPN Connection Certificate Authentication for Remote Access (RA) VPN—Creating a Certificate Map for Certificate Authentication in RA VPN, Associating a Certificate Map to a Connection Profile Create and Install an Identity Certificate on Device for Remote Access VPN Configuration—PKCS12 Cert Enrollment Object, Manual Cert Enrollment Object, Self-signed Cert Enrollment Object, SCEP Cert Enrollment Object, Install Manual Certificate, Install PKCS12, SCEP, or Self-Signed Certificate, Configure Remote Access VPN Configuring VPN—Renew a certificate using manual re-enrollment, Renew a certificate using Self-signed, SCEP, or EST enrollment, Configure LDAP attribute map for remote access VPN, Add SAML Single Sign-On server object, Configure Dynamic Access Policy for Remote Access VPN 	Configuring a connection profile and a group policy object remains the same in the management center as in the ASA. You must create a realm object for creating local users and Active Directory/LDAP. Realms are connections between the management center and the user accounts on the servers.
Remote Access SSL VPN	Remote Access VPN Policy UI path: Devices > VPN > Remote Access > Policy Assignment > VPN Protocols > SSL. See: Configuring a Remote Access VPN Connection. How-To: Configure Remote Access VPN.	

ASA Feature	Threat Defense Feature in Secure Firewall Management Center	Notes
VPN Load Balancing	<p>VPN Load Balancing</p> <p>UI path: Edit the remote access VPN policy.</p> <p>Advanced > Load Balancing.</p> <p>See: Configuring VPN Load Balancing.</p>	VPN load balancing is a mechanism for equitably distributing remote-access VPN traffic among the devices in a VPN load-balancing group.
Dynamic Access Policies	<p>Dynamic Access Policies</p> <p>UI path: Devices > Dynamic Access Policy.</p> <p>See: Dynamic Access Policies.</p> <p>How-To: Configure Dynamic Access Policy for Remote Access VPN.</p>	Enables you to configure authorization that addresses the dynamics of VPN environments.
Monitor VPN	<p>Remote Access VPN Dashboard</p> <p>UI path: Overview > Dashboards > Remote Access VPN</p> <p>See: Remote Access VPN Monitoring.</p>	
Secure Client Hostscan	<p>VPN File Objects</p> <p>UI path: Objects > Object Management > VPN > Secure Client File.</p> <p>See: File Objects.</p>	
Secure Client Custom Attributes	<p>Secure Client Custom Attributes Objects</p> <p>UI path: Objects > Object Management > VPN > Custom Attribute.</p> <p>Secure Client Custom Attributes Objects.</p>	

