仮想プライベートネットワーク機能

この章では、Secure Firewall Management Center を使用して Secure Firewall Threat Defense で ASA 仮想プライベートネットワーク機能を設定するための高レベルの情報を提供します。

サイト間 VPN

表 *1*：サイト間 *VPN*

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
LAN-to-LAN IPsec	**ポリシーベース VPN** UI パス：[デバイス（Devices）]>[サイト間（Site To Site）] > [ポリシーベース（暗号マップ）（Policy Based (Crypto Map)）]。 「Configure a Policy-based Site-to-Site VPN」を参照してください。 手順：ポリシーベースのサイト間 VPN の設定、既存のサイト間 VPN 展開の IKE オプションのカスタマイズ、既存のサイト間VPN展開のIPsecオプションのカスタマイズ、既存のサイト間 VPN 展開の詳細設定のカスタマイズ	Management Center は、ピアで VPN を設定するための単一のウィザードを提供します。

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
仮想トンネルインターフェイス（VTI）	**ルートベース VPN** UI パス：[デバイス（Devices）] > [サイト間（Site To Site）] > [ルートベース（VTI）（Route Based (VTI)）]。 「Create a Route-based Site-to-Site VPN」を参照してください。 手順：ルートベース VPN（VTI）の作成、VTI の静的ルートの設定、VTI の BGP ルーティングの設定、VTI 経由の暗号化トラフィックを許可するアクセスコントロールルールの設定	動的 VTI を持つハブと静的 VTI を持つスポークの間に VPN を作成することは、ウィザードを使用して Management Center で作成するよりずっと簡単です。 ASDM にはウィザードがありません。
Umbrella SASE	**Umbrella に SASE トンネルを展開する** UI パス：[デバイス（Devices）] > [VPN] > [サイト間（Site To Site）] > [+SASE トポロジ（+SASE Topology）]。 「Umbrella に SASE トンネルを展開する」を参照してください。	
サイト間 VPN のモニタリング	**サイト間 VPN のモニタリング** UI パス：[概要（Overview）] > [ダッシュボード（Dashboards）] > [サイト間VPN（Site to Site VPN）]。 「サイト間 VPN のモニタリング」を参照してください。	

リモート アクセス VPN

表 *2*：リモート アクセス *VPN*

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
リモートアクセス IPsec（IKE v2）VPN	**リモートアクセス VPN ポリシー** UI パス：[デバイス（Devices）] > [VPN] > [リモートアクセス（Devices）] > [ポリシーの割り当て（Policy Assignment）] > [VPNプロトコル（VPN Protocols）] > [IPsec-IKEv2]。 「Configuring a Remote Access VPN Connection」を参照してください。 手順： • リモートアクセス（RA）VPN 接続のトラフィックフィルタリングの設定：RA VPN 接続のトラフィックをフィルタリングするための拡張アクセスリストの作成、RA VPN接続のトラフィックをフィルタリングするためのグループポリシーへの拡張アクセスリストの追加 • リモートアクセス（RA）VPN の証明書認証：RA VPN での証明書認証用の証明書マップの作成、接続プロファイルへの証明書マップの関連付け • リモートアクセス VPN 設定用のデバイスでの ID 証明書の作成とインストール：PKCS12 証明書登録オブジェクト、手動証明書登録オブジェクト、自己署名証明書登録オブジェクト、SCEP 証明書登録オブジェクト、手動証明書のインストール、PKCS12、SCEP、または自己署名証明書のインストール、リモートアクセス VPN の設定 • VPN の設定：手動再登録を使用した証明書の更新、自己署名、SCEP、または EST 登録を使用した証明書の更新、リモートアクセス VPN の LDAP 属性マップの設定、SAML シングル サインオン サーバー オブジェクトの追加、リモートアクセス VPN の動的アクセスポリシーの設定	接続プロファイルとグループ ポリシー オブジェクトの設定は、Management Center でも ASA と同じままです。 ローカルユーザーと Active Directory/LDAP を作成するためのレルムオブジェクトを作成する必要があります。レルムとは、Management Center とサーバー上にあるユーザーアカウントの間の接続です。
リモートアクセス SSL VPN		

ASA 機能	Secure Firewall Management Center での Threat Defense 機能	注記
	リモートアクセス VPN ポリシー UI パス：[デバイス（Devices）] > [VPN] > [リモートアクセス（Devices）] > [ポリシーの割り当て（Policy Assignment）] > [VPNプロトコル（VPN Protocols）] > [SSL]。 「Configuring a Remote Access VPN Connection」を参照してください。 手順：リモートアクセス VPN を設定します。	
VPN ロード バランシング	**VPN ロード バランシング** UI パス：リモートアクセス VPN ポリシーを編集します。 [詳細設定（Advanced）] > [ロードバランシング（Load Balancing）] 「Configuring VPN Load Balancing」を参照してください。	VPN ロードバランシングは、VPN ロードバランシンググループ内のデバイス間でリモートアクセス VPN トラフィックを均一に分散するメカニズムです。
ダイナミック アクセス ポリシー	**ダイナミック アクセス ポリシー** UI パス：[デバイス（Devices）] > [ダイナミックアクセスポリシー（Dynamic Access Policy）]。 「Dynamic Access Policies」を参照してください。 手順：リモートアクセス VPN のダイナミック アクセス ポリシーを設定します。	VPN 環境のダイナミクスに対応する許可を構成できます。
VPN の監視	**リモートアクセス VPN ダッシュボード** UI パス：[概要（Overview）] > [ダッシュボード（Dashboards）] > [リモートアクセスVPN（Remote Access VPN）] 「Remote Access VPN Monitoring」を参照してください。	
セキュアクライアント Hostscan	**VPN ファイルオブジェクト** UI パス：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [セキュアクライアントファイル（Secure Client File）]。 「File Objects」を参照してください。	
セキュアクライアント カスタム属性	**セキュアクライアント カスタム属性オブジェクト** UI パス：[オブジェクト（Objects）] > [オブジェクト管理（Object Management）] > [VPN] > [カスタム属性（Custom Attribute）]。 Secure Client カスタム属性オブジェクト	

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。