paloalto TECHDOCS

IPSec VPN 管理

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2023-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

June 9, 2023

Table of Contents

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

IPSec VPN の基本

これはどこで使えますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

仮想プライベート ネットワーク（VPN）は、ユーザー/システムをローカル エリア ネットワーク（LAN）で接続している場合と同様に、パブリック ネットワークでも安全に接続することができるトンネルを作成します。VPN トンネルをセットアップするには、互いに認証し、両者間の情報の流れを暗号化できるデバイスのペアが必要です。デバイスとして使用できるのは、Palo Alto Networks ファイアウォールのペア、または Palo Alto Networks ファイアウォールと他ベンダーの VPN 対応デバイスです。

VPN の基本概念について学びます。

- IPsec VPN
- IPSec トンネル モード
- IPSec VPN の種類
- IPSec VPN トンネル数
- VPN デプロイメント
- VPN 用の Internet Key Exchange（IKE）

IPsec VPN

これはどこで使えますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

IPSec VPN は、パブリック ネットワーク インフラストラクチャ (インターネットなど) 上でプライベートで安全な IP 通信を提供します。このテクノロジーを使用すると、地理的に異なる地域の異なるサイトやユーザーがネットワーク経由で通信できるため、リソースを安全に使用できます。IPSec は、認証、整合性チェック、暗号化などのデータの機密性と整合性を提供します。

IPSec VPN は、2 つの一般的な VPN プロトコル、つまり VPN 接続の確立に使用される標準セットの 1 つです。IP 層では、IPSec は (単一のデバイスだけでなく) ネットワーク全体への安全なリモート アクセスを提供します。

IPSec VPN には 2 つのタイプがあります。

- トンネルモード
- トランスポートモード

IPSec と **VPN** の違い

IP セキュリティ (IPSec)	**VPN**
IP ネットワーク上で送信されるデータを暗号化および認証する方法を IP ホストに提供します。	暗号化を使用して、VPN クライアントとサーバー間で送信されるすべてのデータを隠蔽します。
IPSec を使用すると、IP アドレスを持つエンティティは安全なトンネルを作成できます。	多くの種類の VPN プロトコルは、さまざまなレベルのセキュリティやその他の機能を提供します。VPN 業界で最も一般的に使用されているトンネリング プロトコルは、ポイントツーポイント トンネル プロトコル (PPTP)、レイヤー 2 トンネリング プロトコル (L2TP) または IPSec、セキュア ソケット トンネリング プロトコル (SSTP)、および OpenVPN です。

©2024 Palo Alto Networks, Inc.

IPSec トンネル モード

どこで使用できますか?	何が必要ですか?
• Prisma Access (IPSec トンネル トランスポート モードは、Prisma Access ではまだサポートされていません) • PAN-OS	ライセンスは必要ありません

IPSec 標準では、トンネル モードとトランスポート モードという、IPSec 動作の 2 つの異なるモードが定義されています。トランスポート モードとトンネル モードの主な違いは、ポリシー ルールが適用される場所です。トンネル モードでは、元のパケットは別の IP ヘッダーにカプセル化されますが、どちらのモードでも、パケットは認証ヘッダー (AH)、カプセル化セキュリティ ペイロード (ESP)、またはその両方によって保護できます。

- 整合性は *IP* ヘッダーの一部のフィールドを使用して計算されるため、*AH* は *NAT* では機能しません。*AH* はハッシュベースのメッセージ認証コード（*HMAC*）の計算に外側の*IP*ヘッダーを含むため、*NAT*がそれを破ってしまうためです。
- *IPSec* トランスポート モードは、クライアントとサーバーの間、またはゲートウェイがホストとして扱われている場合はワークステーションとゲートウェイの間など、エンドツーエンドの通信に使用されます。良い例としては、ワークステーションからサーバーへの暗号化された *Telnet* またはリモート デスクトップ セッションが挙げられます。
- *PAN-OS* ® はデフォルトでトンネルモードをサポートしていますが、トランスポート モード のサポートは *PAN-OS 11.0* リリースから導入されています。

©2024 Palo Alto Networks, Inc.

IPSec VPN の種類

どこで使用できますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

サイト間 (またはゲートウェイ間) VPN とリモート アクセス (クライアントからサイト) VPN は、VPN の 2 つの異なるタイプです。クライアントからサイトへの VPN が単一のユーザー接続を表すのに対し、サイト間 VPN はネットワーク全体のリモート接続を処理します。

サイト間 VPN では、IPSec セキュリティ メソッドを使用して、あるカスタマー ネットワークからカスタマーのリモート サイトへの暗号化されたトンネルを作成します。Palo Alto Networks のVPNトンネルは、パートナー間でも使用できます。

サイト間VPN では、複数のエンドポイントは許可されません。

リモート アクセス VPN では、個々のエンドポイントがプライベート ネットワークに接続され、そのプライベート ネットワークのサービスとリソースにリモートでアクセスします。リモート アクセスVPNは、複数のエンドポイントを許可するため、ビジネスユーザーとホームユーザーに最適です。

©2024 Palo Alto Networks, Inc.

IPSec VPN トンネル数

どこで使用できますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

IPSec トンネルを作成するプロセスでは、最初に暗号化されセキュリティで保護された準備用トンネルの確立が開始され、次にそのセキュア トンネル内から IPSec トンネルの暗号化キーとパラメータがネゴシエートされます。

VPN ネゴシエーションは、フェーズ 1 とフェーズ 2 という 2 つの定義されたフェーズで行われます。フェーズ 1 の主な目的は、2 つのピアがネゴシエートできる安全な暗号化チャネルを設定することです。フェーズ 1 が正常に終了すると、ピアはすぐにネゴシエーションのためにフェーズ 2 に進みます。

トンネルインターフェイスがトラフィックの発信元または発信元のゾーンとは異なるゾーンにある場合は、送信元ゾーンからトンネル インターフェイスを含むゾーンへのトラフィックのフローを許可するポリシー ルールを定義します。トンネル インターフェイスでの IP アドレスの構成はオプションです。トンネル インターフェイス上で動的ルーティング プロトコルを実行する場合は、この IP アドレスが必要になります。

IPSec には多くのコンポーネント テクノロジが組み込まれており、複数の暗号化オプションが提供されていますが、基本的な操作には次の 5 つの主要な手順が含まれます。

- 対象トラフィックまたはオンデマンド- IPSec トンネル ポリー ルールとルートテーブルによって、どのタイプのトラフィックが「対象」とみなされるか、または「オンデマンド」でキャプチャされ、保護されるかが決まります。PAN-OS VPN セキュリティ ポリシーがどのように実装されるかは、デバイス プラットフォームによって異なります。アクセス リストは IPSec ポリシー ルールを解釈して、どのトラフィックが IPSec によって保護されるかを決定します。

  IPSec トンネルは、そのトンネル宛ての興味深いトラフィックがある場合にのみ起動します。トンネルを手動で開始するには、CLI を使用したサイト間 VPN の問題のトラブルシューティングを参照して、トンネルのステータスを確認し、トンネルをクリアします。
- **IKE** フェーズ **1**- IKE は、IPSec で使用されるキー管理プロトコル標準です。IKE は、IPSec セッション内の各ピアを認証し、2 つのレベルの SA を自動的にネゴシエートし、フェーズ 1 とフェーズ 2 の 2 つのフェーズで実行されるセッション キーの交換を処理します。

  IKE フェーズ 1 の主な目的は、IPSec ピアを認証し、ピア間に安全なチャネルを確立することです。
- **IKE** フェーズ **2**- IKE は、ピア間でより厳密な IPSec セキュリティ アソシエーション (SA) パラメータをネゴシエートします。

©2024 Palo Alto Networks, Inc.

- **IPSec** データ転送 ：対象となるデータが IPSec ピア間で転送されます。情報は、対象トラフィックを定義する方法に基づいて、IPSec セッションを通じて交換されます。パケットは、IPSec SA で指定された暗号化を使用して、IPSec ピアで暗号化および復号化されます。
- **IPSec** トンネル セッションの終了-トラフィックが終了して IPSec SA が削除されたため、IPSec セッションが終了するか、いずれかの SA ライフタイム設定に基づいて SA がタイムアウトする可能性があります。SA タイムアウトは、指定された秒数または接続を通過した指定されたバイト数が経過した後に発生します。

  SA が終了するとキーは破棄され、IKE は新しいフェーズ 2 と、場合によっては新しいフェーズ 1 ネゴシエーションを実行する必要があります。現在の SA が期限切れになる前に新しい SA を確立でき、中断のないデータ フローを維持できます。

  IPSec セッションは、削除またはタイムアウトによって終了します。

パロアルトネットワークスの次世代ファイアウォールへの **IPSec** トンネル ポリシー ルールの実装

ネットワーク上で安全に転送するためのパケットのカプセル化は、IPsec プロトコルによって実行されます。例えば、サイト間 VPN の場合、ネットワーク内の送信元ホストが IP パケットを送信します。そのパケットがネットワークのエッジに到達すると、VPN ゲートウェイと通信します。そのネットワークに対応する VPN ゲートウェイはプライベート IP パケットを暗号化し、ESP トンネルを介して次のネットワークのエッジにあるピア VPN ゲートウェイに中継します。そのゲートウェイはパケットを復号化して宛先ホストに配信します。

ポリシーベースの VPN には、IPSec トンネルを通過する対象のトラフィックを許可するように設定された特定のセキュリティ ルール、ポリシー ルール、またはアクセス リスト（送信元アドレス、宛先アドレス、ポートなど）があります。これらのルールはクイック モード (または IPSec フェーズ 2) 中に参照され、最初または 2 番目のメッセージでプロキシ ID として交換されます。Palo Alto Networks ファイアウォールがプロキシ ID 設定で構成されていない場合、ファイアウォールはプロキシ ID をデフォルト値 (送信元 IP = 0.0.0.0/0、宛先 IP = 0.0.0.0/0、アプリケーション:任意) で設定します。クイック モードの最初または 2 番目のメッセージ中にピアとそれを交換します。

 ©2024 Palo Alto Networks, Inc.

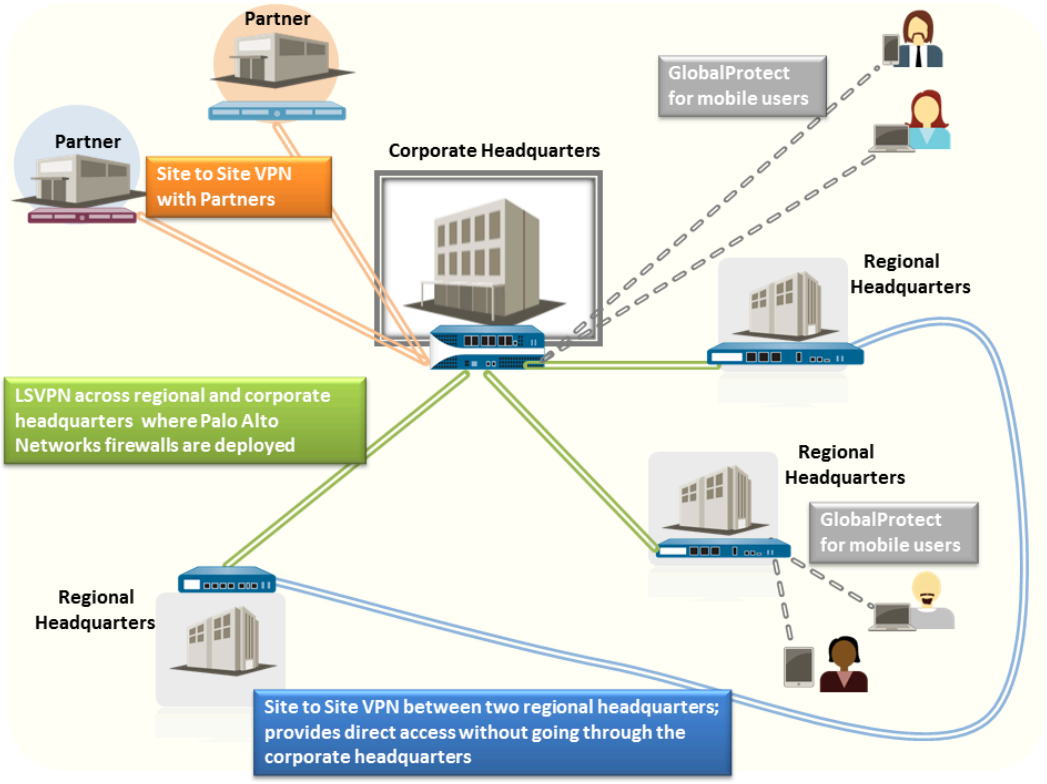
VPN デプロイメント

どこで使用できますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

Palo Alto Networks ファイアウォールでは、以下の VPN デプロイメントをサポートしています。

- サイト間 **VPN** — 中央サイトとリモート サイトを接続する簡易 VPN、または中央サイトと複数のリモート サイトを接続するハブ アンド スポーク VPN。ファイアウォールは、インターネット プロトコル セキュリティ (IPSec) のプロトコル セットを使用して、2 つのサイト間のトラフィック用に安全なトンネルを設定します。サイト間 VPN の概要を参照してください。
- リモート ユーザーからサイトへの **VPN** — GlobalProtect エージェントを使用してリモート ユーザーがファイアウォール経由で安全な接続を確立できるようにするソリューション。このソリューションは、SSL および IPSec を使用してユーザーとサイト間の安全な接続を確立します。『GlobalProtect 管理者ガイド』を参照してください。
- 大規模 **VPN** — Palo Alto Networks の GlobalProtect 大規模 VPN （LSVPN）は、最大 1,024 のサテライト オフィスまで拡張可能なハブ アンド スポーク VPN を展開するための簡略化されたメカニズムを提供します。このソリューションを使用するには、Palo Alto Networks ファイアウォールをハブおよびすべてのスポークでデプロイする必要があります。デバイスの認証に証明書を、すべてのコンポーネント間の安全な通信のために SSL を、データの保護のために IPSec を使用します。大規模 VPN （LSVPN）を参照してください。
- リモート サイト **VPN**-リモート サイトは IPSec トンネルを使用して、 リモート ネットワークの場所にあるユーザーとデバイスを保護します。さらに、GlobalProtect で保護されたモバイル ユーザーとリモート サイトのユーザーは、IPSec トンネル (サービス接続 または ZTNA コネクタ用) または GRE トンネル (Colo-Connect 接続用) を使用してプライベート アプリケーションにアクセスします。

©2024 Palo Alto Networks, Inc.

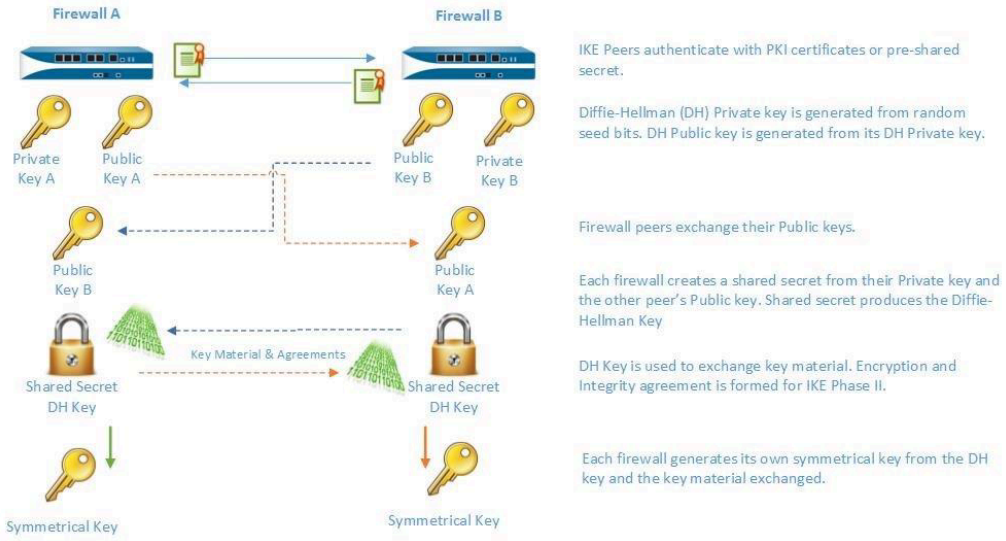


 ©2024 Palo Alto Networks, Inc.

VPN 用の Internet Key Exchange（IKE）

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

IKE プロセスにより、トンネル両端の VPN ピアは、相互に合意したキーまたは証明書、および暗号化方法を使用して、パケットを暗号化および復号化することができます。IKE プロセスは、2 つのフェーズで行われます。IKE フェーズ 1 および IKE フェーズ 2。各フェーズは、暗号プロファイル（IKE 暗号プロファイルおよび IPSec 暗号プロファイル）を使用して定義されたキーと暗号化アルゴリズムを使用し、IKE ネゴシエーションの結果が Security Association （SA）です。SA は相互に合意されたキーとアルゴリズムのセットで、VPN トンネルでのデータのフローを許可するため両方の VPN ピアによって使用されます。以下の図は、VPN トンネルをセットアップするための鍵交換プロセスを示しています。



IKE ゲートウェイ

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

Palo Alto Networks ファイアウォール同士、またはファイアウォールと別のセキュリティ デバイスが 2 つのネットワーク間で VPN 接続を開始して終了する場合、これらは IKE ゲートウェイと呼ばれます。VPN トンネルをセットアップして IKE ゲートウェイ間でトラフィックを送信するには、各ピアにスタティックまたはダイナミックな IP アドレスまたは FQDN が必要です。VPN ピアは事前共有鍵または証明書を使用して相互に認証します。

©2024 Palo Alto Networks, Inc.

ピアは、VPN トンネルをセットアップするためのモード（main または aggressive）と IKE フェーズ 1 における SA のライフタイムをネゴシエートする必要があります。main モードはピアの ID を保護し、トンネルをセットアップするときにより多くのパケットが交換されるため安全性が高いモードです。両方のピアでサポートされている場合、IKE ネゴシエーションのための推奨モードは main モードです。aggressive モードは VPN トンネルをセットアップするために使用するパケットが少ないため、高速ですが VPN トンネルをセットアップする場合に安全性が劣る選択肢です。

構成の詳細については、IKE ゲートウェイのセットアップを参照してください。

IKE フェーズ 1

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

このフェーズでは、ファイアウォールは IKE ゲートウェイ設定で定義されたパラメータおよび IKE 暗号プロファイルを使用して相互に認証し、安全な制御チャネルをセットアップします。IKE フェーズは、VPN ピアの相互認証に事前共有鍵またはデジタル証明書（公開鍵インフラストラクチャ（PKI）を使用）の使用をサポートしています。事前共有鍵は PKI インフラストラクチャのサポートを必要としないため、小規模なネットワークを保護するための単純なソリューションです。大規模なネットワーク、またはより堅牢な認証セキュリティが必要な実装では、デジタル証明書の方が適しています。

証明書を使用する場合、証明書を発行する CA が両方のゲートウェイ ピアによって信頼されており、証明書チェーン内の証明書の最大長が 5 以下であることを確認します。IKE フラグメンテーションを有効にすると、ファイアウォールは証明書チェーン内の最大 5 つの証明書を使用して IKE メッセージを再構築し、VPN トンネルを正常に確立できます。

IKE 暗号プロファイルは、IKE SA ネゴシエーションで使用される以下のオプションを定義します。

- IKE 用の対象鍵を生成するための Diffie-Hellman（DH）グループ。

  Diffie-Hellman アルゴリズムは、一方の秘密鍵ともう一方の公開鍵を使用して共有のシークレットを作成します。これは、両方の VPN トンネル ピアによって共有される暗号化鍵です。ファイアウォールでサポートされている DH グループ：

グループ番号	ビット数
グループ1	768 ビット
グループ2	1,024ビット（デフォルト）
グループ 5	1,536ビット

©2024 Palo Alto Networks, Inc.

グループ番号	ビット数
グループ 14	2,048ビット
グループ 15	(PAN-OS 10.2.0以降のリリース) 3072 ビットのモジュラー指数グループ
グループ 16	(PAN-OS 10.2.0以降のリリース) 4096 ビットのモジュラー指数グループ
グループ 19	256 ビット楕円曲線グループ
グループ 20	384 ビット楕円曲線グループ
グループ 21	(PAN-OS 10.2.0 以降のリリース) 512 ビットランダム楕円曲線群

- 認証アルゴリズム — sha1、sha 256、sha 384、sha 512、または md5。
- 暗号化アルゴリズム - aes-256-gcm、aes-128-gcm、3des、aes-128-cbc、aes-192-cbc、 aes-256-cbc、またはデス。

  - *PAN-OS 10.0.3* 以降のリリースは、*aes-256-gcm* および *aes-128-gcm* アルゴリズムをサポートします。
  - *PAN-OS 10.1.0* 以前のリリースは、*des* 暗号化アルゴリズムをサポートしています。

IKE フェーズ 2

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

トンネルが保護されて認証されると、フェーズ 2 では、ネットワーク間でのデータ送受信のためにチャネルがさらに保護されます。IKE フェーズ 2 では、プロセスのフェーズ 1 で確立されたキーと、IKE フェーズ 2 の SA で使用する IPSec プロトコルとキーを定義する IPSec 暗号プロファイルを使用します。

IPSec は、以下のプロトコルを使用して安全な通信を可能にします。

- Encapsulating Security Payload （ESP） — IP パケット全体を暗号化し、送信元を認証してデータの整合性を確認できます。ESP ではパケットを暗号化して認証する必要がありますが、暗号化オプションを Null （ヌル）に設定することで暗号化のみまたは認証のみを行うように設定できます。認証をせずに暗号化を使用するのは推奨されません。

©2024 Palo Alto Networks, Inc.

- Authentication Header （AH） — パケットの送信元を認証し、データの整合性を確認します。AH はデータ ペイロードを暗号化しないため、データ保護が重要なデプロイメントには適していません。AH は、データ保護が必要でなく、主な懸念がピアの正当性を確認することである場合によく使用されます。

表 **1 : IPSec** 認証および暗号化でサポートされるアルゴリズム

エスケープ	**AH**
サポートされる **Diffie Hellman** （**DH**）交換オプション	
• グループ 1 — 768 ビット • グループ 2 - 1024 ビット(デフォルト) • グループ 5 — 1536 ビット • グループ 14:2048 ビット • (PAN-OS 10.2.0 以降のリリース) グループ 15—3072 ビットのモジュラー指数グループ • （PAN-OS 10.2.0 以降）グループ 16—4096 ビット モジュラ指数グループ • グループ 19 - 256 ビット楕円曲線グループ • グループ 20 — 384 ビット楕円曲線グループ • （PAN-OS 10.2.0以降）グループ21—512ビットのランダム楕円曲線グループ • no-pfs — デフォルトでは、Perfect Forward Secrecy が有効化され、上記いずれかのグループを使用して IKE フェーズ 2 で新しい DH キーが生成されます。このキーは IKE フェーズ 1 で交換されるキーとは関係なく、より堅牢なデータ転送セキュリティが提供されます。no-pfs を選択すると、フェーズ 1 で作成された DH キーが更新されず、1 つのキーが IPSec SA ネゴシエーションに使用されます。両方の VPN ピアを PFS について有効化または無効化する必要があります。	
サポートされる暗号化アルゴリズム	
• des	（PAN-OS 10.1.0以前）セキュリティ強度56ビットのデータ暗号化規格（DES）。
• 3desIPv6	セキュリティ強度が 112 ビットの Triple Data Encryption Standard （トリプル DES 暗号化）。
• aes-128-cbc	セキュリティ強度が 128 ビットの暗号ブロック チェーン（CBC）を使用した Advanced Encryption Standard （AES）。
• aes-192-cbc	セキュリティ強度が 192 ビットの CBC を使用した AES。

©2024 Palo Alto Networks, Inc.

エスケープ	AH
• aes-256-cbc	セキュリティ強度が 256 ビットの CBC を使用した AES。
• aes-128-ccm	セキュリティ強度が 128 ビットの CBC-MAC （CCM）を使用した AES。
• aes-128-gcm	セキュリティ強度が 128 ビットの Galois/Counter Mode （GCM）を使用した AES。
• aes-256-gcm	セキュリティ強度が 256 ビットの GCM を使用した AES。
サポートされる認証アルゴリズム	
• md5	• md5
• sha 1	• sha 1
• sha 1	• sha 1
• sha 1	• sha 1
• SHA512	• sha 512

IPSec VPN トンネルを保護するための方法（**IKE** フェーズ **2**）

IPSec VPN トンネルは、手動キーまたは自動キーを使用して保護できます。さらに、IPSec の設定オプションには、Diffie-Hellman グループによる鍵共有、暗号化アルゴリズム、およびメッセージ認証のためのハッシュなどがあります。

- 手動キー — 手動キーは一般に、Palo Alto Networks ファイアウォールがレガシー デバイスとの VPN トンネルを確立しているか、セッション キーを生成するオーバーヘッドを軽減する場合に使用されます。手動キーを使用する場合、同じキーを両方のピアで設定する必要があります。

  ピア間でキー情報をリレーする際にセッション キーが解読されるおそれがあるため、VPN トンネルを確立する場合、手動キーは推奨されません。キーが解読されると、データの送受信が保護されなくなります。
- 自動キー — 自動キーを使用すると、IPSec 暗号プロファイルで定義されたアルゴリズムに基づいて IPSec トンネルをセットアップしてメンテナンスするためにキーを自動的に生成できます。

©2024 Palo Alto Networks, Inc.

IKEv2

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

IPSec VPN ゲートウェイは、IKEv1 または IKEv2 を使用して IKE Security Association （SA）および IPSec トンネルをネゴシエートします。IKEv2 は RFC 5996 で定義されています。

フェーズ 1 SA とフェーズ 2 SA を使用する IKEv1 とは異なり、IKEv2 は IKE SA で設定された Encapsulating Security Payload （ESP）または Authentication Header （AH）の子 SA を使用します。

2 つのゲートウェイ間に配置されたデバイスで発生する NAT がある場合は、両方のゲートウェイで NAT トラバーサル（NAT-T）を有効にする必要があります。ゲートウェイは、NAT デバイスの（グローバルにルーティング可能な）パブリック IP アドレスのみを確認できます。

IKEv2 には、IKEv1 に比べて以下の利点があります。

- トンネル確立時にエンドポイント間で交わされるメッセージ数が少なくなります。IKEv2 は 4 個のメッセージを使用し、IKEv1 は 9 個（main モードの場合）または 6 個のメッセージ（aggressive モードの場合）を使用します。
- 組み込み NAT-T 機能により、ベンダー間の互換性が向上します。
- トンネルがダウンした場合でも、組み込みのヘルスチェックが自動的にトンネルを再確立します。IKEv1 で使用されていた Dead Peer Detection の代替として、存続性チェックを使用できます。
- トラフィック セレクターがサポートされます (1 交換につき 1 つ)。IKE ネゴシエーションではトラフィック セレクターを使用して、トンネルへのアクセスを許可するトラフィックを決定します。
- フラグメンテーションを軽減するためのハッシュおよび URL 証明書の交換がサポートされています。
- 向上したピア検証による DoS 攻撃に対する耐障害性。ハーフオープン SA が過剰に検出されると、cookie 検証が実行されます。

IKEv2 を設定する前に、以下の概念を把握する必要があります。

- ライブネス チェック
- Cookie アクティベーションのしきい値と Cookie の厳密な検証
- トラフィック セレクタ
- ハッシュおよび URL 証明書の交換
- SA キーの有効期間と再認証間隔

©2024 Palo Alto Networks, Inc.

IKE ゲートウェイのセットアップ後、IKEv2 を選択した場合は、ご使用の環境で要求されているように、IKEv2 に関連する以下のオプション・タスクを実行します。

- ハッシュおよび URL を使用してアクセスするピアの証明書のエクスポート
- IKEv2 ゲートウェイ認証の証明書のインポート
- IKEv2 のキーの有効期間または認証間隔の変更
- IKEv2 の Cookie アクティベーションのしきい値の変更
- IKEv2 トラフィック セレクタの設定

ライブネス チェック

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

IKEv2 のライブネス チェックは、IKEv1 でピアがまだ使用可能かどうかを判断するために使用されるデッド ピア検出（DPD）と似ています。

IKEv2 では、ライブネス チェックはすべての IKEv2 パケット送信、または設定可能な間隔（デフォルトは 5 秒）でゲートウェイがピアに送信する空の情報メッセージで実行されます。必要に応じて、送信側が最大 10 回まで再送信を試行できます。応答が得られない場合、送信側は IKE_SA および対応する CHILD_SA を閉じて削除します。送信側は、別の IKE_SA_INIT メッセージを送信して、もう一度やり直します。

Cookie アクティベーションのしきい値と Cookie の厳密な検証

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

Cookie の検証は IKEv2 では常に有効化され、ハーフオープン SA DoS 攻撃に対する保護に役立ちます。Cookie の検証をトリガーするハーフオープン SA のグローバルしきい値を設定できます。新しい IKEv2 SA ごとに Cookie の検証を適用するように、個々の IKE ゲートウェイを設定することもできます。

- **Cookie Activation Threshold (Cookie** アクティベーションのしきい値**)** は、同時に発生するハーフオープン IKE SA の数（デフォルトは 500）を制限するグローバル VPN セッション設定です。ハーフオープン IKE SA の数が **Cookie Activation Threshold** [Cookie アクティベーションのしきい値]を超えると、レスポンダが Cookie を要求し、イニシエータは接続を検証する

©2024 Palo Alto Networks, Inc.

Cookie が含まれる IKE_SA_INIT で応答する必要があります。Cookie の検証に成功すると、別の SA を開始できます。値を 0 にすると、Cookie の検証が常にオンになります。

レスポンダはイニシエータが Cookie を返すまで、イニシエータの状態を管理せず、Diffie-Hellman キーの交換も実行しません。IKEv2 の Cookie の検証は、多数の接続をハーフオープンのままにしようとする DoS 攻撃を軽減します。

Cookie Activation Threshold[Cookie アクティベーションのしきい値] は、**Maximum Half Opened SA** [ハーフ オープン SA の最大数]設定を超えないようにする必要があります。非常に高い数値 (65534 など) にIKEv2 の Cookie アクティベーションのしきい値の変更し、**Maximum Half Open SA** 設定がデフォルト値の 65535 のままの場合、Cookie の検証はに無効になります。

- グローバルしきい値に関係なく、ゲートウェイが受信するすべての新しい IKEv2 SA に対して Cookie の検証を実行するには、**Strict Cookie Validation** [Cookie の厳密な検証]を有効にします。**Strict Cookie Validation** [Cookie の厳密な検証]は設定されいる IKE ゲートウェイにのみ影響し、デフォルトでは無効になっています。**Strict Cookie Validation (Cookie** の厳密な検証**)** が無効な場合、システムは **Cookie Activation Threshold (Cookie** アクティベーションのしきい値**)** を使用して Cookie が必要かどうかを判断します。

トラフィック セレクタ

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

IKEv1 では、ルートベースの VPN があるファイアウォールで IPSec トンネルをセットアップするには、ローカルおよびリモート プロキシ ID を使用する必要があります。各ピアは、IKE フェーズ 2 を正常にネゴシエートするために、プロキシIDをパケットで受信したものと比較します。IKE フェーズ 2 は、SA をネゴシエートして IPSec トンネルをセットアップします(Proxy ID について詳しくは、トンネルインターフェイスを参照してください。

IKEv2 では、IKE ネゴシエーション時に使用されるネットワーク・トラフィックのコンポーネントであるIKEv2 トラフィック セレクタの設定できます。トラフィック セレクタは、トンネルをセットアップし、トンネルの通過が許可されるトラフィックを判断するために、CHILD_SA （トンネル作成）フェーズ 2 で使用されます。2 つの IKE ゲートウェイ ピアがネゴシートしてトラフィック セレクタについて合意する必要があります。合意しなかった場合、一方がアドレス範囲を絞り込んで合意に達します。1 つの IKE 接続で複数のトンネルを使用できます。たとえば、各部門に異なるトンネルを割り当ててトラフィックを分離することができます。トラフィックの分離によって、QoS などの機能も実装できます。

IPv4 および IPv6 トラフィック セレクタは以下のとおりです。

- 送信元 **IP** アドレス — ネットワーク プレフィックス、アドレス範囲、特定のホスト、またはワイルドカード。

 ©2024 Palo Alto Networks, Inc.

- 宛先 **IP** アドレス — ネットワーク プレフィックス、アドレス範囲、特定のホスト、またはワイルドカード。
- プロトコル — 転送プロトコル（TCP または UDP など）。
- 送信元ポート — パケットの送信元ポート。
- 宛先ポート — パケットの宛先ポート。

IKE ネゴシエーション中、異なるネットワークとプロトコル用に複数のトラフィック セレクタを使用できます。たとえば、イニシエータがトンネルを介して 172.168.0.0/16 からそのピアの宛先 198.5.0.0/16 に TCP パケットを送信するとします。さらに、同じトンネルを介して 172.17.0.0/16 から同じゲートウェイの宛先 0.0.0.0 に UDP パケットを送信します。ピア ゲートウェイは、この送信を承諾するためにこれらのトラフィック セレクタに同意する必要があります。

ゲートウェイは、他のゲートウェイの IP アドレスよりも具体的な IP アドレスのトラフィック セレクタを使用してネゴシエーションを開始できます。

- たとえば、ゲートウェイ A は 172.16.0.0/16 の送信元 IP アドレスと 192.16.0.0/16 の宛先 IP アドレスを提供します。一方、ゲートウェイ B は送信元 IP アドレスとして 0.0.0.（任意の送信元）、宛先 IP アドレスとして 0.0.0.（任意の宛先）が設定されています。したがって、ゲートウェイ B は送信元 IP アドレスを 192.16.0.0/16、宛先アドレスを 172.16.0.0/16 に絞り込みます。この絞り込みによって、ゲートウェイ A のアドレスに対応し、2 つのゲートウェイのトラフィック セレクタが同意に達します。
- （送信元 IP アドレスとして 0.0.0.0 が設定された）ゲートウェイ B はレスポンダではなくイニシエータになり、ゲートウェイ A はより具体的な IP アドレスで応答し、ゲートウェイ B がアドレスを絞り込んで合意に達します。

ハッシュおよび URL 証明書の交換

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

IKEv2 では、ハッシュおよび URL 証明書の交換がサポートされています。この交換は、SA の IKEv2 ネゴシエーション中に使用されます。証明書は、URL で指定された HTTP サーバーに保存します。ピアはサーバーへの URL の受信に基づいて、サーバーから証明書をフェッチします。ハッシュは、証明書のコンテンツが有効であるかどうかの確認に使用されます。したがって、2 つのピアは証明書を相互に交換する代わりに、HTTP CA を使用して交換します。

ハッシュおよび URL のハッシュ部分によってメッセージ サイズが削減されるため、IKE ネゴシエーション中のパケット フラグメンテーションの発生確率が低くなります。ピアは期待される証明書とハッシュを受信するため、IKE フェーズ 1 でピアが検証されます。フラグメンテーションの発生の削減は、DoS 攻撃に対する保護に役立ちます。

©2024 Palo Alto Networks, Inc.

ハッシュおよび URL 証明書の交換は、IKE ゲートウェイの設定時に **HTTP Certificate Exchange** [HTTP 証明書の交換]を選択し、**Certificate URL** [証明書 URL]を入力することで有効にできます。交換が正常に行われるには、ピアもハッシュおよび URL 証明書の交換を使用する必要があります。ピアがハッシュおよび URL を使用できない場合、X.509 証明書が IKEv1 での交換方法と同様に交換されます。

ハッシュおよび URL 証明書の交換を有効にする場合、独自の証明書を証明書サーバーにエクスポートする必要があります（サーバーにまだ存在しない場合）。証明書をエクスポートするときに、ファイル フォーマットを **Binary Encoded Certificate (DER)** [バイナリ エンコード済み証明書 (DER)]にする必要があります。ハッシュおよび URL を使用してアクセスするピアの証明書のエクスポートを参照してください。

SA キーの有効期間と再認証間隔

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

IKEv2 では、**Key Lifetime** [キーの有効期間]と **IKEv2 Authentication Multiple** [IKEv2 多重認証]の 2 つの IKE 暗号プロファイル値を使用して、IKEv2 IKE SA の確立を制御します。キーの有効期間は、ネゴシエートされた IKE SA キーが有効な期間です。キーの有効期間が切れる前に、SA のキーを再生成する必要があります。そうしないと、有効期限が切れたときに、SA は新しい IKEv2 IKE SA キーの再生成を開始する必要があります。デフォルト値は 8 時間です。

再認証間隔は、**Key Lifetime (**キーの有効期間**)** に **IKEv2 Authentication Multiple (IKEv2** 多重認証**)** を乗算して求められます。多重認証のデフォルトは、再認証機能が無効になる 0 に設定されています。

多重認証の範囲は 0 ～ 50 です。たとえば、多重認証を 20 に設定すると、システムは 20 回のキーの再生成（160 時間）ごとに再認証を実行します。この場合、ゲートウェイが IKE を再認証して IKE SA を最初から作り直す前に、160 時間、子 SA の作成を実行できます。

IKEv2 では、イニシエータ ゲートウェイとレスポンダ ゲートウェイに独自のキーの有効期間値が設定され、キーの有効期間が短い方のゲートウェイが SA キーの再生成を要求します。

 ©2024 Palo Alto Networks, Inc.

IPSec VPN（サイト間）について

これはどこで使えますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

VPN 接続により、2 つ以上のサイト間で安全に情報にアクセスできるようになります。リソースへの安全なアクセスと信頼性の高い接続を実現するには、VPN 接続には次のコンポーネントが必要です。IKE ゲートウェイ、トンネルインターフェース、トンネルモニタリング、VPN 用 Internet Key Exchange (IKE)、および IKEv2。

IPSec VPN トンネルのセットアップを計画する前に、次の事項について確認しておくことが重要です

- トンネルインターフェイス
- トンネル モニタ
- IPsec VPN のプロキシ ID

サイト間 VPN の概要

どこで使用できますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

2 つのローカル エリア ネットワーク（LAN）を接続できるようにする VPN 接続はサイト間 VPN と呼ばれます。ルートベースの VPN を設定すると、2 つのサイトに設置された Palo Alto Networks ファイアウォール間、または Palo Alto Networks ファイアウォールと別の場所に設置されたサードパーティのセキュリティ デバイスを接続できます。ファイアウォールは、サードパーティのポリシーベースの VPN デバイスとの相互運用性も確保しています。Palo Alto Networks ファイアウォールはルートベースの VPN をサポートしています。

Palo Alto Networks ファイアウォールはルートベースの VPN をセットアップし、ファイアウォールは宛先 IP アドレスに基づいてルーティングの判断を行います。トラフィックがVPNトンネルを介して特定の宛先にルーティングされる場合、VPNトラフィックとして処理されます。

プロトコルの Internet Protocol Security （IPSec）セットを使用して VPN トラフィックに安全なトンネルをセットアップすると、TCP/IP パケットの情報の安全が確保されます（トンネル タイプが ESP の場合は暗号化されます）。IP パケット（ヘッダーおよびペイロード）は別の IP ペイロードに埋め込まれ、新しいヘッダーが適用され、IPSec トンネルを経由して送信されます。新しいヘッダーの送信元 IP アドレスはローカル VPN ピアのアドレスであり、宛先 IP アドレスはトンネルの反対側の VPN ピアのアドレスです。パケットがリモート VPN ピア（トンネルの反対側のファイアウォール）に達すると、外部ヘッダーが削除され、元のパケットがその宛先に送信されます。

VPN トンネルをセットアップするには、最初にピアを認証する必要があります。認証に成功したら、ピアは暗号化メカニズムおよびアルゴリズムをネゴシエートして、通信を安全にします。Internet Key Exchange （IKE）プロセスが VPN ピアの認証に使用され、VPN 通信を保護するために IPSec Security Associations （SA）がトンネルの両端で定義されます。IKE はデジタル証明書または事前共有鍵、および Diffie Hellman 鍵を使用して IPSec トンネル用の SA をセットアップします。SA は、セキュリティパラメータインデックス (SPI)、セキュリティプロトコル、暗号化キー、および宛先 IP アドレス (暗号化、データ認証、データ整合性、エンドポイント認証) を含む、安全な伝送に必要なすべてのパラメータを指定します。

以下の図は、2 つのサイト間の VPN トンネルを示しています。VPN ピア A によって保護されたクライアントが他のサイトに設置されたサーバーのコンテンツを必要とする場合、VPN ピア A は VPN ピア B への接続要求を開始します。セキュリティ ポリシーによって接続が許可される場合、VPN ピア A は IKE 暗号のプロファイル パラメータ（IKE フェーズ 1）を使用して安全な接続を確立し、VPN ピア B を認証します。次に、VPN ピア A は IPSec 暗号のプロファイルを使用して VPN トンネルを確立し、これによって IKE フェーズ 2 パラメータを定義して、2 つのサイト間の安全なデータ転送を可能にします。

©2024 Palo Alto Networks, Inc.

トンネルインターフェイス

どこで使用できますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

VPN トンネルをセットアップするには、両端のレイヤー 3 インターフェイスに VPN トンネルを接続して確立するためのファイアウォール用の論理トンネル インターフェイスが必要です。トンネル インターフェイスとは、2 つのエンドポイント間でトラフィックを配信するために使用される論理（仮想）インターフェイスです。設定済みのプロキシ ID がある場合、IPSec トンネルの容量にプロキシ ID が加味されます。

トンネル インターフェイスはポリシー ルールを適用するセキュリティ ゾーンに属する必要があり、既存のルーティング インフラストラクチャを使用するには仮想ルーターに割り当てる必要があります。ファイアウォールがルート検索を実行して、使用する適切なトンネルを判断できるように、トンネル インターフェイスと物理インターフェイスが同じ仮想ルーターに割り当てられるようにします。

一般に、トンネル インターフェイスが接続されたレイヤー 3 インターフェイスは、たとえば Untrust ゾーンなどの外部ゾーンに属します。トンネル インターフェイスは物理インターフェイスと同じセキュリティ ゾーンに配置できますが、安全性と可視性を高めるため、トンネル インターフェイス用に別個のゾーンを作成することができます。トンネル インターフェイス用に、たとえば VPN ゾーンなどの別個のゾーンを作成する場合、VPN ゾーンと Trust ゾーン間でトラフィックが流れるようにセキュリティ ポリシーを作成する必要があります。

サイト間のトラフィックをルーティングするために、トンネル インターフェイスには IP アドレスは必要ありません。IP アドレスが必要になるのは、トンネル モニタリングを有効にする場合か、トンネル間のトラフィックをルーティングするためにダイナミック ルーティング プロトコルを使用している場合のみです。ダイナミック ルーティングでは、トンネル IP アドレスは VPN トンネルへのトラフィックをルーティングするためのネクスト ホップ IP アドレスとして機能します。

ポリシーベースの VPN を実行する VPN ピアで Palo Alto Networks ファイアウォールを設定している場合、IPSec トンネルをセットアップするときにローカルおよびリモートのプロキシ ID を設定する必要があります。各ピアは、IKE フェーズ 2 ネゴシエーションを成功させるために、ここで設定したプロキシ ID をパケットで受信する ID と比較します。複数のトンネルが必要な場合、各トンネル インターフェイスに一意のプロキシ ID を設定します。1 つのトンネル インターフェイスに最大 250 個のプロキシ ID を設定できます。各プロキシ ID はファイアウォールの

©2024 Palo Alto Networks, Inc.

IPSec VPN トンネル容量にカウントされ、トンネル容量はファイアウォール モデルによって異なります。

設定の詳細については、「IPSec トンネルのセットアップ」を参照してください。

トンネル モニタ

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

VPN トンネルでは、トンネルを経由して宛先 IP アドレスへの接続を確認できます。ファイアウォールでネットワーク モニタリング プロファイルを使用することで、宛先 IP アドレスへの接続（ICMP を使用）または指定したポーリング間隔でネクスト ホップを確認し、モニタリング対象 IP アドレスへのアクセスで障害が発生した場合のアクションを指定できます。

宛先 IP アドレスにアクセスできない場合、トンネルが回復するのを待機するようにファイアウォールを設定するか、別のトンネルへの自動フェイルオーバーを設定できます。どちらの場合も、ファイアウォールはトンネル障害を警告するシステム ログを生成し、IPSec 鍵を再ネゴシエートして回復を加速させます。

構成の詳細については、IPSec VPN トンネルを監視するを参照してください。

IPsec VPN のプロキシ ID

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

プロキシ ID またはプロキシ ID は、ピア間でネゴシエートされる (またはネゴシエーションが成功した後のセットアップ) SA の対象となる、IPSec VPN に属する一連のトラフィックを指します。

これにより、トラフィックを識別して誘導することができます。

- 同じ IKE ゲートウェイを共有する同じ 2 つのピア間で複数のトンネルが共存する適切なトンネルに接続します。
- 異なるパラメータを持つ固有の SA と共有 SA を共存させることができます。

同じ *2* つのピア間に *VPN* トンネルが設定されている構成では、プロキシ *ID* を使用します。

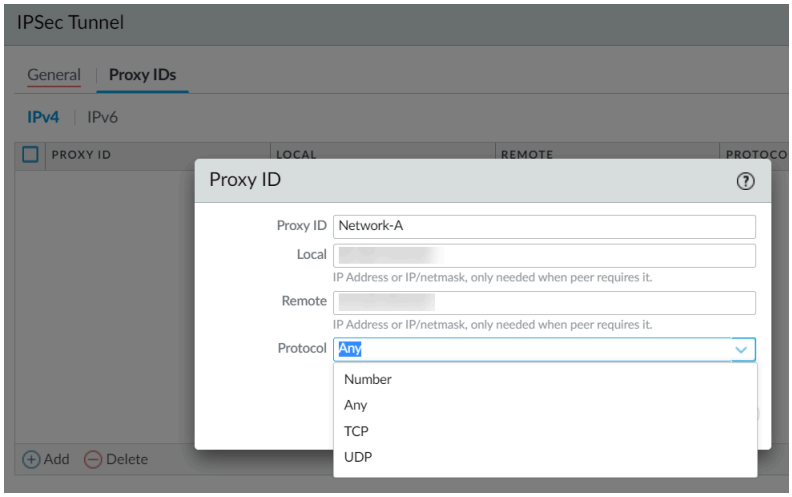
プロキシ ID は、どのトラフィックが特定の IPSec VPN に属しているかを識別するのに役立ちます。これにより、オペレーティング システムは適切なフックをインストールして、プロキシ ID

 ©2024 Palo Alto Networks, Inc.

(クライアント ID) の送信元アドレスと宛先アドレスに一致するトラフィックを、一致する IPSec SA または VPN に誘導し、一致する IPSec SA に出入りできるようになります。

プロキシ**ID**の設定

Palo Alto Networks は、プロキシ ID を使用する他のベンダーの 1 つです。次の図は、Palo Alto Networks プロキシ ID ウィンドウとそのオプションを示しています。



Network (ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)** > **Proxy IDs (**プロキシ **ID)** を選択します。プロキシ ID 名、ローカル IP アドレス、ピアで必要な場合はリモート IP アドレス、プロトコル タイプとローカルおよびリモートのポート番号を入力します。

各プロキシ *ID* は *VPN* トンネルとみなされ、ファイアウォールの *IPSec VPN* トンネル容量にカウントされます。例えば、サイト間 *IPSec VPN* トンネルの最大制限は、*PA-3020* の場合は *1000*、*PA-2050* の場合は *100*、*PA-200* の場合は *25* です。

プロキシ ID は IKE バージョンによって動作が異なります。

- **IKEv1**—Palo Alto Networks デバイスは、プロキシ ID の完全一致のみをサポートします。ピアのプロキシ ID が一致しない場合、VPN は正しく機能しません。
- **IKEv2**-プロキシ ID 設定が 2 つの VPN ゲートウェイで異なる場合のトラフィック セレクターの絞り込みをサポートします。

プロキシ **ID** の使用

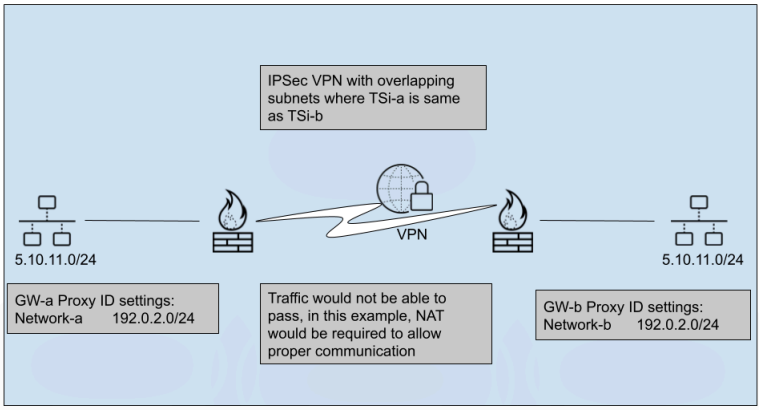
次の例は、2 つの VPN ゲートウェイを示しています。AとB。

IKE ネゴシエーションは、VPN GW-az、i=イニシエーター、r=レスポンダーによって開始されます。VPN GW-a はトラフィック セレクタ TSi-a/TSr-a を定義し、VPN GW-b はトラフィック セレクタ TSi-b/TSr-b を指定します。TSr-a は TSr-b と同じであるため無視できますが、TSi-a は TSi-b と異なる場合があります。

この場合、トンネルの両側に同じネットワークが存在するため、トラフィックは VPN トンネルを介してルーティングできません。

©2024 Palo Alto Networks, Inc.

ただし、以下に示すように、この問題を解決する唯一の方法は、両方のピア ゲートウェイが NAT を作成し、新しい一意のネットワーク サブネットを内部ネットワークに変換することです。そうでない場合は、一方がサブネット IP を変更する必要があります。



このようにして、どちらかの側のすべてのトラフィックは、他の同様のネットワークではなく、新しい NAT アドレスに送信されます。これを適切に機能させるには、両方のゲートウェイで NAT を実行 し、どちらのネットワークがどちら側にあるかについての混乱を取り除く必要があります。

Palo Alto Networks ファイアウォール用の **IPSec VPN** の構成

トンネルの反対側がサードパーティの VPN デバイスである場合、または非 PAN-OS ファイアウォールである場合は、一致するローカル プロキシ ID とリモート プロキシ ID (通常はローカル LAN サブネットとリモート LAN サブネット) を指定する必要があります。

NAT 処理されるトラフィックのローカルおよびリモート IP ネットワークを識別するために IPSec トンネル プロキシ ID を構成する場合、NAT 後の IP ネットワーク情報を使用して IPSec トンネルのプロキシ ID 構成を構成する必要があります。これはプロキシID情報が、IPSec設定の両側でトンネルの通過を許可するネットワークを定義するためです。

©2024 Palo Alto Networks, Inc.

IPSec VPN トンネルのセットアップを計画する

どこで使用できますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

IPSec トンネルをセットアップする前に、次の要素を決定し、IPSec トンネルのセットアップを適切に計画することが重要です。

STEP 1 | **VPN** のタイプを決定します。サイト間アクセスまたはリモート アクセス

サイト間 VPN では、IPSec セキュリティ方式を使用して、1 つの顧客ネットワークから顧客のリモート サイトへの暗号化されたトンネルを作成できます。ただし、リモート アクセス VPN を使用すると、個々のユーザーがプライベート ネットワークに接続して、そのサービスやリソースにアクセスできます。

STEP 2 | **VPN** のセキュリティ方式を選択してください

サイト間 VPN では、IPSec セキュリティ方式を使用して、1 つの顧客ネットワークから顧客のリモート サイトへの暗号化されたトンネルを作成します。

リモート アクセス VPN では、個々のユーザーがプライベート ネットワークに接続されます。

STEP 3 | **VPN** クライアントを決定する

サイト間 VPN は、各クライアントでセットアップする必要はありません。リモート アクセス VPN は、各クライアントでのセットアップが必要な場合と必要ない場合があります。

STEP 4 | **VPN** トンネルの設定を決定する

サイト間 VPN では、すべてのユーザーが VPN トンネルのセットアップを開始する必要はありません。リモート アクセス VPN では、すべてのリモート アクセス ユーザーが VPN トンネルのセットアップを開始する必要があります。

STEP 5 | セキュリティ テクノロジを決定する

サイト間 VPN は IPSec テクノロジーをサポートしますが、リモート アクセス VPN は IPSec テクノロジーだけでなく SSL もサポートします。

STEP 6 | **VPN** に単一ユーザーを使用するか複数ユーザーを使用するかを決定します

サイト間 VPN では、複数のユーザーは許可されません。ただし、リモート アクセス VPN では、複数のユーザーが許可されます。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

IPSec VPN トンネルの構成 (サイト間)

どこで使用できますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

サイト間 VPN をセットアップするには、以下の手順を実行します。

- Ethernet インターフェイス、仮想ルーター、およびゾーンが正しく設定されていることを確認してください。詳細は、「インターフェイスとゾーンの設定」を参照してください。
- トンネル インターフェイスを作成します。トンネル インターフェイスを別のゾーンに置き、トンネル対象トラフィックで異なるポリシー ルールを使用できるようにするのが理想的です。
- スタティック ルートをセットアップするか、またはルーティング プロトコルを割り当て、VPN トンネルにトラフィックを転送します。ダイナミック ルーティング（OSPF、BGP、RIP がサポートされます）をサポートするには、IP アドレスをトンネル インターフェイスに割り当てる必要があります。
- VPN トンネルの両端にあるピア間の通信を確立するために IKE ゲートウェイを定義します。また、IKEv1 フェーズ 1 で VPN トンネルをセットアップするために使用する ID、認証、暗号化のプロトコルおよびアルゴリズムを指定する暗号プロファイルも定義します。IKE ゲートウェイのセットアップおよびIKE 暗号プロファイルの定義を参照してください。
- VPN を経由してデータを転送する IPSec 接続を確立するために必要なパラメータを設定します。 IPSec トンネルのセットアップを参照してください。IKEv1 Phase-2 についてはIPSec 暗号プロファイルの定義を参照してください。
- （任意）ファイアウォールによる IPSec トンネルのモニター方法を指定します。IPSec VPN トンネルを監視するを参照してください。

- セキュリティ ポリシーを定義し、トラフィックのフィルタリングおよび検証を行います。

  セキュリティ ルールベースの最後に拒否ルールがある場合、許可されていない限りゾーン内のトラフィックはブロックされます。*IKE* および *IPsec* アプリケーションを許可するルールは、上記の拒否ルールに明示的に含まれている必要があります。

  VPN トラフィックが *PA-7000 Series* あるいは *PA-5200 Series* ファイアウォールを通過（送信元でも宛先でもなく）する場合、*ESP* あるいは *AH* トラフィックを双方向で許可する双方向セキュリティポリシールールを設定します。

以上の作業を実行すると、トンネルを使用できるようになります。ポリシー ルールで定義されるゾーン/アドレスを宛先とするトラフィックは、ルーティング テーブルの宛先ルートに基づいて自動的に適切にルーティングされ、VPN トラフィックとして処理されます。サイト間 VPN の例は、サイト間 VPN の設定例を参照してください。

©2024 Palo Alto Networks, Inc.

IKE ゲートウェイのセットアップ

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

VPN トンネルをセットアップするには、VPN ピアまたはゲートウェイが事前共有鍵またはデジタル証明書を使用して相互に認証し、安全なチャネルを確立して、両側のホスト間でトラフィックを保護するために使用される IPSec Security Association （SA）をネゴシエートします。

STEP 1 | IKE ゲートウェイを定義します。

1. **Network**（ネットワーク） > **Network Profiles**（ネットワークのプロファイル） > **IKE Gateways**（**IKE** ゲートウェイ）を選択して、ゲートウェイを **Add**（追加）し、そのゲートウェイの **Name**（名前）を入力します（**General**（全般）タブ）。
2. **Version**（バージョン）を、**IKEv1 only mode**（**IKEv1** 専用モード）、**IKEv2 only mode**（**IKEv2** 専用モード）、または **IKEv2 preferred mode**（**IKEv2** 優先モード） を選択します。ここで指定したモードで、IKE ゲートウェイがピアとのネゴシエーションを開始します。**IKEv2 preferred mode** [IKEv2 優先モード]を選択すると、リモート ピアで IKEv2 がサポートされている場合は 2 つのピアで IKEv2 が使用され、サポートされていない場合は IKEv1 が使用されます。

   Version (バージョン**)** の選択に応じて、**Advanced Options (**詳細オプション**)** タブの設定で使用可能なオプションも決定されます。

STEP 2 | トンネルのローカル エンドポイント（ゲートウェイ）を確立します。

1. **Addres Type**（アドレス タイプ）を選択します。**IPv4**または**IPv6**
2. ローカル ゲートウェイが存在するファイアウォールで物理的な発信 **Interface (**インターフェイス**)** を選択します。
3. **Local IP Address (**ローカル **IP** アドレス**)** リストから、VPN 接続がエンドポイントとして使用する IP アドレスを選択します。これは、ファイアウォール上の公的にルーティング可能な IP アドレスを持つ外部向きのインターフェイスです。

STEP 3 | トンネルの反対側のピア（ゲートウェイ）を確立します。

Peer IP Address Type（ピア **IP** アドレス タイプ）の場合、次のいずれかを選択し、ピアの対応する情報を入力します：

- **IP** — IPv4 または IPv6 アドレスのいずれかである **Peer Address** を入力するか、IPv4 または IPv6 アドレスであるアドレス オブジェクトを入力します。
- **FQDN** — FQDN 文字列または FQDN 文字列を使用するアドレス オブジェクトである **Peer Address** を入力します。FQDN または FQDN アドレス オブジェクトが複数の IP アドレス

©2024 Palo Alto Networks, Inc.

に解決される場合、ファイアウォールは、IKE ゲートウェイの Address Type (IPv4 または IPv6) に一致するアドレスのセットから、次のように優先アドレスを選択します。

- IKE セキュリティ アソシエーション (SA) がネゴシエートされていない場合、優先アドレスは最小値を持つ IP アドレスです。
- IKE ゲートウェイが返されたアドレスのセット内のアドレスを使用する場合、ファイアウォールはそのアドレスを (セット内の最小のアドレスであるかどうかにかかわらず) 選択します。
- IKE ゲートウェイが返されたアドレスのセットに含まれていないアドレスを使用する場合、ファイアウォールは新しいアドレスを選択し、それがセット内の最小のアドレスになります。

- **Dynamic** — ピア IP アドレスまたは FQDN 値が不明な場合、ピアがネゴシエーションを開始する際**Dynamic** を選択します。

FQDN または *FQDN* アドレス オブジェクトを使用すると、ピアが動的 *IP* アドレスの変更を受ける *(*それ以外の場合はこの *IKE* ゲートウェイ ピア アドレスを再構成する必要がある*)* 環境での問題が軽減されます。

STEP 4 | ピアの認証方法を指定します。

Authentication [認証]の方法を選択します。**Pre-Shared Key** [事前共有鍵]あるいは**Certificate** [認証]です。事前共有鍵を選択した場合は、次のステップに進みます。証明書を選択した場合は、ステップ 6 の証明書ベースの認証を設定までスキップします。

STEP 5 | 事前共有鍵を設定します。

1. **Pre-shared Key**（事前共有鍵）に、トンネル間の認証用のセキュリティ キーを入力します。**Confirm Pre-shared Key** [再入力 事前共有鍵]に値を再入力します。最大 255 文字の ASCII 文字または非 ASCII 文字を使用してください。

   辞書攻撃で解読されにくいキーを生成します。必要に応じて、事前共有鍵生成プログラムを使用します。

2. **Local Identification** [ローカル ID]で次のタイプの中から選択を行い、決定した値を入力します。**FQDN (hostname)**（**FQDN**（ホスト名））、**IP address**（**IP** アドレス）、**KEYID (binary format ID string in HEX)**（**HEX** のバイナリフォーマット **ID** 文字列）、**User FQDN (email address)**（ユーザー **FQDN**（電子メール アドレス））。ローカル ID は、ローカル ゲートウェイのフォーマットと ID を定義します。値を指定しない場合は、ローカル IP アドレスがローカル ID 値として使用されます。
3. **Peer Identification**（ピア **ID**）で次のタイプの中から選択を行い、決定した値を入力します。**FQDN (hostname)**（**FQDN**（ホスト名））、**IP address**（**IP** アドレス）、**KEYID (binary format ID string in HEX)**（**HEX** のバイナリフォーマット **ID** 文字列）、**User FQDN (email address)**（ユーザー **FQDN**（電子メール アドレス））。ピア ID は、ピア ゲートウェイのフォーマットと ID を定義します。値を指定しない場合、ピア IP アドレスがピア識別値として使用されます。

©2024 Palo Alto Networks, Inc.

4. ステップ 7 (ゲートウェイの詳細オプションを設定) に進みます。

STEP 6 | 証明書ベースの認証を設定します。

トンネルの反対側にあるピア ゲートウェイの認証方式として **Certificate** [証明書]を選択した場合、この手順の残りのステップを実行します。

1. すでにファイアウォールにある **Local Certificate (**ローカル証明書**)** を選択するか、証明書を **Import (**インポート**)** するか、新しい証明書を **Generate (**生成**)** します。
   - 証明書を **Import (**インポート**)** する必要がある場合は、はじめに IKEv2 ゲートウェイ認証の証明書のインポート を行ってから、このタスクに戻ってください。
   - 新しい証明書を **Generate**（生成）する場合は、はじめにファイアウォールでの証明書の生成を行ってから、このタスクに戻ります。
2. (任意) **HTTP Certificate Exchange (HTTP** 証明書の交換**)** を有効化 (選択) して、ハッシュと URL (IKEv2 限定) を設定します。HTTP 証明書の交換を行う **Certificate URL** [証明書 URL]を入力します。詳細についてはハッシュおよび URL 証明書の交換を参照してください。
3. **Local Identification**（ローカル **ID**）タイプを **Distinguished Name** （**Subject**）（識別名（サブジェクト）、FQDN （ホスト名）、**IP address** （**IP** アドレス）、または **User FQDN** （**email address**）（ユーザー **FQDN** （電子メール アドレス））から選択してから、値を入力します。ローカル ID は、ローカル ゲートウェイのフォーマットと ID を定義します。
4. **Peer Identification**（ピア **ID**） タイプを **Distinguished Name** （**Subject**）（識別名（サブジェクト）、FQDN （ホスト名）、**IP address** （**IP** アドレス）、または **User FQDN**（**email address**）（ユーザー **FQDN** （電子メール アドレス））から選択してから、値を入力します。ピア ID は、ピア ゲートウェイのフォーマットと ID を定義します。
5. **Peer ID Check**（ピア **ID** チェック）で以下のいずれかのタイプを指定します。
   - **Exact**（完全）— ローカル設定とピア IKE ID ペイロードが完全に一致するピア ID のみを許可します。
   - **Wildcard**（ワイルドカード）— （*）より前のすべての文字に一致するピア ID を許可します。ワイルドカードより後の文字が一致する必要はありません。
6. （任意）ピア ID が証明書のピア ID に一致しなくても IKE SA を正常に確立できるようにするには、**Permit peer identification and certificate payload identification mismatch**（ピア **ID** と証明書ペイロード **ID** の不一致を許可する）をクリックします。
7. **Certificate Profile (**証明書プロファイル**)** を選択します。証明書プロファイルには、ピア ゲートウェイの認証方法に関する情報が含まれています。
8. （任意）鍵の使用方法を厳密に制御する場合は、**Enable strict validation of peer's extended key use**（ピアの拡張鍵使用の厳密な検証を有効にする）をクリックします。

 ©2024 Palo Alto Networks, Inc.

STEP 7 | ゲートウェイの詳細オプションを設定します。

1. ファイアウォールが IKE 接続リクエストにのみ応答し、それらを開始させないように指定するには、（任意）共通オプション（**Advanced Options**（詳細オプション））で **Enable Passive Mode**（パッシブ モードを有効にする）を行います。
2. ゲートウェイ間で NAT を実行しているデバイスがあり、IKE および UDP プロトコルで UDP カプセル化が使用され、中間 NAT デバイスを通過できるようにするには、**Enable NAT Traversal**（**NAT** トラバーサルを有効にする） を使用します。
3. ステップ 1 で **IKEv1 only mode (IKEv1** 専用モード**)** を設定した場合は、IKEv1 タブで以下の設定を指定します：

   - **Exchange Mode**（交換モード）を選択します： **auto**（自動）、**aggressive**（アグレッシブ）、または **main**（メイン）。ファイアウォールが **auto (**自動**)** の交換モードを使用するように設定されている場合、**main (**メイン**)** モードと **aggressive (**アグレッシブ**)** モードの両方のネゴシエーション要求を受け入れることができますが、可能な場合は常にネゴシエーションを開始して **main (**メイン**)** モードで交換ができるようにします。

     交換モードを ***auto***（自動） に設定しない場合、各ピアがネゴシエーション要求を受け入れることができるように、両方のピアを同じ交換モードで設定する必要があります。

   - **IKE Crypto Profile (IKE** 暗号プロファイル**)** リストから既存のプロファイルを選択するか、デフォルト プロファイルのままにします。必要に応じて、 IKE 暗号プロファイルを定義することができます。
   - （証明書ベースの認証を使用していて交換モードが aggressive モードに設定されていない場合のみ）ファイアウォールが IKE フラグメンテーションで動作するようにするには、**Enable Fragmentation (**フラグメンテーションを有効にする**)** をクリックします。
   - **Dead Peer Detection**（デッド ピア検出）をクリックして **Interval**（間隔）（範囲は 2 ～ 100 秒）を入力します。**Retry**には、IKE ピアから切断するまでの再試行回数 (範囲は 2 ～ 100) を指定します。デッド ピア検出は、IKE フェーズ 1 通知ペイロードをピアに送信して確認を待機することで、無効または使用できない IKE ピアを識別します。
4. ステップ 1 で **IKEv2 only mode (IKEv2** 専用モード**)** あるいは **IKEv2 preferred mode (IKEv2** 優先モード**)** を設定した場合は、IKEv2 タブで：

   - **IKE Crypto Profile (IKE** 暗号プロファイル**)** を選択します。このプロファイルは、DH グループ、ハッシュ アルゴリズム、ESP 認証などの IKE フェーズ 1 オプションを設定します。IKE 暗号化プロファイルの詳細は、IKE フェーズ 1を参照してください。
   - （任意） **Strict Cookie Validation(Cookie** アクティベーションのしきい値**)** Cookie アクティベーションのしきい値と Cookie の厳密な検証を有効にします。

©2024 Palo Alto Networks, Inc.

- （任意）ゲートウェイからそのゲートウェイ ピアに応答を要求するメッセージ要求を送信する場合は、**Enable Liveness Check (**ライブネス チェックを有効化**)** して **Interval （sec） (**間隔（秒）**)**（デフォルトは 5）を入力します。必要に応じて、イニシエータが最大 10 回までライブネス チェックを試行できます。応答が得られない場合、イニシエータは IKE_SA および CHILD_SA を閉じて削除します。イニシエータは、別の IKE_SA_INIT を送信して、もう一度やり直します。

STEP 8 | **OK** をクリックし、変更を **Commit (**コミット**)** します。

ハッシュおよび URL を使用してアクセスするピアの証明書のエクスポート

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

IKEv2 は、トンネルのリモート エンドのピアが証明書をエクスポートしたサーバーから証明書をフェッチする方法として、ハッシュおよび URL 証明書の交換をサポートしています。このタスクを実行して、証明書をそのサーバーにエクスポートします。**Device (**デバイス**)** > **Certificate Management (**証明書管理**)**を使用して、すでに証明書を作成済みである必要があります。

STEP 1 | **Device (**デバイス**)** > **Certificates (**証明書**)** を選択し、プラットフォームで複数の仮想システムがサポートされている場合は、**Location (**場所**)** で適切な仮想システムを選択します。

STEP 2 | **Device Certificates**[デバイス証明書] タブで、サーバーに **Export**[エクスポート] する証明書を選択します。

証明書の状態は失効ではなく有効である必要があります。ファイアウォールは、無効な証明書のエクスポートを阻止しません。

STEP 3 | **File Format** [ファイル フォーマット]で、**Binary Encoded Certificate （DER）** [バイナリ エンコード済み証明書（DER）]を選択します。

STEP 4 | **Export private key** [秘密鍵のエクスポート]はオフのままにします。秘密鍵のエクスポートは、ハッシュおよび URL には不要です。

STEP 5 | **OK** をクリックします。

IKEv2 ゲートウェイ認証の証明書のインポート

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

©2024 Palo Alto Networks, Inc.

IKEv2 ゲートウェイのピアを認証するときに、ファイアウォールにすでに存在するローカル証明書を使用せずに他の場所から証明書をインポートする場合は、このタスクを実行します。

このタスクは、**Network (**ネットワーク**)** > **IKE Gateways (IKE** ゲートウェイ**)** の順に選択してゲートウェイを追加し、**Local Certificate (**ローカル証明書**)** で **Import (**インポート**)** をクリックしていることを前提としています。

STEP 1 | 証明書をインポートします。

1. **Network (**ネットワーク**)** > **IKE Gateways (IKE** ゲートウェイ**)** の順に選択してゲートウェイを **Add (**追加**)** し、**General** （全般） タブの **Authentication (**認証**)** で **Certificate (**証明書**)** を選択します。**Local Certificate** [ローカル証明書]で、**Import** [インポート]をクリックします。
2. Import Certificate [証明書のインポート]ウィンドウで、インポートする証明書の **Certificate Name** [証明書名]を入力します。
3. この証明書を複数の仮想システムで共有する場合は、**Shared** [共有]を選択します。
4. **Certificate File** [証明書ファイル]で、証明書ファイルを **Browse** [参照]します。ファイル名をクリックして **Open** [開く]をクリックすると、**Certificate File** [証明書ファイル]フィールドに証明書ファイルが設定されます。
5. **File Format** [ファイル フォーマット]で、以下のいずれかを選択します。
   - **Base64 Encoded Certificate (PEM)**[Base64 エンコード済み証明書 (PEM)] — 鍵ではなく、証明書が含まれます。クリアテキストです。
   - **Encrypted Private Key and Certificate (PKCS12)**[暗号化された秘密鍵と証明書 (PKCS12)] — 証明書と鍵の両方が含まれます。
6. 証明書ファイルとは別のファイル内に秘密鍵がある場合は、**Import private key** [秘密鍵のインポート]を選択します。秘密鍵は任意ですが、以下の例外があります。
   - **File Format** [ファイル フォーマット]を **PEM** に設定した場合は、秘密鍵をインポートする必要があります。**Browse** [参照]をクリックしてインポートするキー ファイルに移動し、**Key file** [キー ファイル]を入力します。
   - **Passphrase** [パスフレーズ]と **Confirm Passphrase** [パスフレーズの確認]を入力します。
7. **OK** をクリックします。

STEP 2 | 次のタスクに進みます。

証明書ベースの認証の設定ステップ。

IKEv2 のキーの有効期間または認証間隔の変更

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

©2024 Palo Alto Networks, Inc.

このタスクは任意です。IKEv2 IKE SA キー再生成の有効期間のデフォルト設定は 8 時間です。IKEv2 認証マルチのデフォルト設定は 0 です。つまり、再認証機能は無効です。詳細については、SA キーの有効期間と再認証間隔を参照してください。

デフォルト値を変更するには、以下のタスクを実行します。前提条件として、IKE 暗号プロファイルがすでに存在する必要があります。

STEP 1 | IKE 暗号プロファイルの SA キーの有効期間または認証間隔を変更します。

1. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IKE Crypto (IKE** 暗号**)** の順に選択し、ローカル ゲートウェイに適用する IKE 暗号プロファイルを選択します。
2. **Key Lifetime** [キーの有効期間]で、単位（**Seconds** [秒]、**Minutes** （分）、**Hours** [時間]、または **Days** [日]）を選択して値を入力します。最短は 3 分です。
3. **IKE Authentication Multiple** [IKE 多重認証]に値を入力します。この値は、再認証間隔を決定するために有効期間で乗算されます。

STEP 2 | 変更をコミットします。

OK、**Commit (**コミット**)** の順にクリックします。

IKEv2 の Cookie アクティベーションのしきい値の変更

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

Cookie の検証が必要になる前に、ファイアウォールに 500 ハーフオープン SA セッションのデフォルト設定とは異なるしきい値を設定する場合は、以下のタスクを実行します。Cookie 検証の詳細については、Cookie アクティベーションのしきい値と Cookie の厳密な検証を参照してください。

STEP 1 | Cookie アクティベーションのしきい値を変更します。

1. **Device (**デバイス**)** > **Setup (**セットアップ**)** > **Session (**セッション**)** を選択して VPN Session Settings (VPN セッション設定) を編集します。**Cookie Activation Threshold (Cookie** アクティベーションのしきい値**)** で、レスポンダがイニシエータから Cookie を要求する前に許可される、ハーフオープン SA の最大数を入力します（範囲は 0 ～ 65535、デフォルトは 500）。
2. **OK** をクリックします。

STEP 2 | 変更をコミットします。

OK、**Commit (**コミット**)** の順にクリックします。

©2024 Palo Alto Networks, Inc.

IKEv2 トラフィック セレクタの設定

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

IKEv2 では、IKE ネゴシエーション中に使用されるネットワーク トラフィックのコンポーネントであるトラフィック セレクタを設定することができます。トラフィック セレクタは、トンネルをセットアップし、トンネルの通過が許可されるトラフィックを判断するために、CHILD_SA（トンネル作成）フェーズ 2 で使用されます。2 つの IKE ゲートウェイ ピアがネゴシートしてトラフィック セレクタについて合意する必要があります。合意しなかった場合、一方がアドレス範囲を絞り込んで合意に達します。1 つの IKE 接続で複数のトンネルを使用できます。たとえば、各部門に異なるトンネルを割り当ててトラフィックを分離することができます。トラフィックの分離によって、QoS などの機能も実装できます。以下の流れでトラフィック セレクタを設定します。

STEP 1 | **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)** > **Proxy IDs (**プロキシ **ID)** を選択します。

STEP 2 | **IPv4** または **IPv6** タブを選択します。

STEP 3 | **Add** [追加]をクリックし、**Proxy ID** [プロキシ ID]フィールドの **Name** [名前]に入力します。

STEP 4 | **Local** [ローカル]フィールドで、**Source IP Address** [送信元 IP アドレス]を入力します。

STEP 5 | **Remote** [リモート]フィールドで、**Destination IP Address** [宛先 IP アドレス]を入力します。

STEP 6 | **Protocol (**プロトコル**)** フィールドで、トランスポート プロトコル (**TCP** または **UDP**) を選択します。

STEP 7 | **OK** をクリックします。

©2024 Palo Alto Networks, Inc.

暗号プロファイルの定義

これはどこで使えますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

暗号プロファイルは、2 つの IKE ピア間の認証や暗号化に使用される暗号と、キーのライフタイムを指定します。各再ネゴシエーション間の期間はライフタイムとして知られます。指定した時間が経過すると、ファイアウォールは新しいキーのセットを再ネゴシエートします。

VPN トンネルを経由した通信を保護するため、ファイアウォールでは、IKE フェーズ 1 とフェース 2 のネゴシエーションの完了に、それぞれ IKE と IPSec 暗号プロファイルが必要です。ファイアウォールには、すぐに使用できるデフォルトの IKE 暗号化プロファイルとデフォルトの IPSec 暗号化プロファイルが含まれています。

- IKE 暗号プロファイルの定義
- IPSec 暗号プロファイルの定義

IKE 暗号プロファイルの定義

これはどこで使えますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

IKE 暗号プロファイルは、IKE フェーズ 1 の鍵交換プロセスに使用される暗号化および認証アルゴリズムと、キーが有効な期間を指定するキーのライフタイムをセットアップするために使用されます。プロファイルを呼び出すには、IKE ゲートウェイ設定に関連付ける必要があります。

IKE ゲートウェイの ***Peer IP Address Type (***ピア ***IP***アドレス タイプ***)***が***Dynamic (***ダイナミック***)*** として設定され、*IKEv1* メイン モードまたは *IKEv2* が適用されている場合、同じインターフェースまたはローカル *IP*アドレスで設定されたすべての *IKE* ゲートウェイは同じ暗号プロファイルを使用する必要があります。ゲートウェイ上の暗号プロファイルが同じであれば、初期接続は別のゲートウェイで開始される可能性がありますが、事前共有鍵、証明書、およびピア *ID* が交換されると、接続は適切なゲートウェイに移行します。

VPN ピアが同じベンダーのものであるかどうかにかかわらず、IKE ネゴシエーションを正常に実行するには、VPN ピアに同じ IKE パラメータが設定されている必要があります。

IKE ネゴシエーションを成功させるには、次のパラメータが一致する必要があります。

©2024 Palo Alto Networks, Inc.

- キー交換用 DH グループ
- 暗号化アルゴリズム
- 認証アルゴリズム

例えば、**VPN** ピア **1** を **DH** グループにはグループ **20**、認証には **sha384**、暗号化には **aes-256-gcm** を設定したとします。次に、IPSec トンネルを確立する VPN ピア 2 にも同じ値が設定されている必要があります。

- PAN-OS 10.1 以降および Prisma Access (パノラマ管理)
- #unique_39

IPSec 暗号プロファイルの定義

どこで使用できますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

IPSec 暗号プロファイルは IKE フェーズ 2 で呼び出されます。IKE SA のキーを自動的に生成するために自動キー IKE を使用する場合にトンネル内でデータを保護する方法を指定します。

VPN ピアが同じベンダーのものであるかどうかにかかわらず、IPSec ネゴシエーションを正常に実行するには、VPN ピアに同じ IPSec　パラメータが設定されている必要があります。

IPSec ネゴシエーションは、VPN ピア間で次のパラメータが一致すると成功します。

- IPsec プロトコル (ESP または AH)
- キー交換用 DH グループ (または PFS)
- 暗号化アルゴリズム
- 認証アルゴリズム

例えば、VPN ピア 1 を IPsec プロトコルに **ESP**、DH グループにはグループ **20**、認証には **sha384**、暗号化には **aes-256-gcm**を設定したとします。次に、IPSecトンネルを確立する VPNピア 2 にも、まったく同じ値で設定されている必要があります。

デフォルトでは、IPsec トンネルでは完全な前方秘匿性 (PFS) が有効になっており、よりランダム化されたキーが生成されます。PFS は、IPSec SA ネゴシエーション中に追加のキー交換を行い、新しい共有シークレットを生成して新しい IPSec SA キーに結合することでこれを行います。PFS を設定するときは、両方の VPN ピアに同じ PFS 設定があることを確認してください。IPSec SA ネゴシエーションに失敗すると、IPSec トンネルの確立に失敗します。

- PAN-OS 10.1 以降および Prisma Access (パノラマ管理)
- Prisma Access (Cloud Management)

©2024 Palo Alto Networks, Inc.

IPSec トンネルのセットアップ

どこで使用できますか?	何が必要ですか?
• Prisma Access (IPSec トンネル トランスポート モードは、Prisma Access ではまだサポートされていません) • PAN-OS	ライセンスは必要ありません

IPSec は、ピア間の通信を保護するために使用される一連のプロトコルです。IPSec では、暗号化および認証アルゴリズム、セキュリティ アソシエーションのタイムアウトなど、さまざまな設定を構成できます。そのような構成の 1 つが IPSec モード (トンネル モードまたはトランスポート モード) です。

IPsec トンネルを設定するときに、IPsec モードを [トンネル] または [トランスポートモード] として選択して、安全な接続を確立できます。つまり、トンネルモード またはトランスポートモードのどちらでパケットを暗号化するか、認証するかを選択できます。PAN-OS® はデフォルトでトンネル モードをサポートし、データ (IP パケット) がトンネルを通過するときに認証または暗号化します。PAN-OS 11.0以降.0、トランスポートモードを使用できます。

トンネルモードとトランスポートモードの違い

トンネル モード	トランスポートモード
IP ヘッダーを含むパケット全体を暗号化します。暗号化後、新しい IP ヘッダーがパケットに追加されます。	ペイロードのみを暗号化し、元の IP ヘッダーは保持します。
トンネルモニタリングでは、トンネルインターフェイスの IP アドレスを使用します。	トンネル監視では、物理インターフェースの IP アドレス (ゲートウェイインターフェースの IP アドレス) が自動的に使用され、トンネルインターフェースの IP アドレスは無視されます。
二重カプセル化をサポートします。	二重カプセル化はサポートされていません。
このモードは、一般的にサイト間通信に使用されます。	このモードは通常、ホスト間の通信に使用されます。

©2024 Palo Alto Networks, Inc.

IPSec トンネルの設定 (トンネル モード)

どこで使用できますか?	何が必要ですか?
• Prisma Access • PAN-OS	ライセンスは必要ありません

IPSec トンネル設定により、データ (IP パケット) がトンネルを通過するときに、データの認証や暗号化を行うことができます。

ポリシーベースの VPN をサポートするピアと連携するようにファイアウォールを設定している場合は、プロキシ ID を定義する必要があります。ポリシーベースの VPN をサポートするデバイスは、関連するトラフィックが IPSec トンネルを通過するのを許可するために特定のセキュリティ ルール/ポリシーまたはアクセスリスト（送信元アドレス、宛先アドレス、およびポート）を使用します。これらのルールはクイック モード/IKE フェーズ 2 ネゴシエーション中に参照され、プロセスの最初または 2 番目のメッセージのプロキシ ID として交換されます。したがって、ポリシーベースの VPN ピアと連携するようにファイアウォールを設定している場合は、フェーズ 2 ネゴシエーションを成功させるために、両方のピアの設定が同じになるように Proxy-ID を定義する必要があります。ファイアウォールがルートベースの VPN をサポートしているために Proxy-ID が設定されていない場合、Proxy-ID として使用されるデフォルト値は source ip です。0.0.0.0/0、宛先 IP が0.0.0.0/0およびアプリケーションが「任意」になります。これらの値がピアと交換されると、VPN 接続のセットアップに失敗します。

IPSec トンネルを正常に確立するには、IKE と IPSec の両方のネゴシエーションが成功する必要があります。

- IKE ネゴシエーションは、両方の VPN ピアが設定された同じ IKE パラメータを交換する場合にのみ成功します。
- IPSec ネゴシエーションは、両方の VPN ピアが設定された同じ IPSec パラメータを交換する場合にのみ成功します。
- （PAN-OS 10.1 以降）
- #unique_43
- #unique_44

IPSec トンネルのセットアップ (トランスポートモード)

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

トランスポート モードは、PAN-OS 11.0.0 リリースから新しく追加され、以下をサポートします。

©2024 Palo Alto Networks, Inc.

- IPv4 アドレスのみ。
- セキュリティペイロード (ESP) プロトコルのみをカプセル化します。
- IKEv2 のみ。
- DH グループ 20 Diffie-Hellman (DH) グループおよび PFS の場合。
- GCM モードで 256 ビットのキーを持つ AES のみ。

ネットワーク要件に基づいて IPsec モードを選択できます。

- 次世代ファイアウォールとトンネル エンドポイント間で交換される管理プレーン プロトコル (BGP など) パケットを暗号化する場合は、IPSec トランスポート モードを構成する必要があります。トランスポートモードでは、制御トラフィック (ルーティングプロトコルやシグナライゼーションメッセージなど) を最も堅牢なプロトコルで暗号化できます。トランスポートモードを使用すると、ファイアウォールの IP アドレスに属するポイントツーポイント トラフィックを暗号化できます。
- 次世代ファイアウォールとトンネル エンドポイントの間で交換されるデータプレーン トラフィックを暗号化する場合は、IPSec トンネル モードを構成する必要があります。

トランスポートモードを有効にする前に覚えておくべき重要な点:

- NAT-T が有効になっている場合、トランスポート モードは選択できません。
- トランスポート モードの IPSec トンネルへのループバック インターフェイス上に IKE ゲートウェイを構成することはできません。
- IPSec トランスポート モードは、ネゴシエーションにプロキシ ID 設定を使用しません。したがって、トランスポート モードではプロキシ ID を設定できません。他の方法でプロキシ ID を設定しようとすると、自動的に 0.0.0.0/0 に置き換えられます。
- トランスポートモードは、オートキー交換でのみ使用できます。
- IPSec トンネルなしで IKE ゲートウェイを設定すると、デフォルトで IKE はトンネルモードのチャイルドセキュリティアソシエーション（SA）をネゴシエートします。
- GRE カプセル化を使用しない IPSec トランスポート モードでは、関連するトンネル インターフェイスを介してユーザー トラフィックをルーティングしないでください。制御プロトコル (BGP ピアリング セッションなど) をトンネル インターフェイスではなく物理インターフェイス (ethernet1/1 など) に設定します。BGP ルートの IPsec トンネルモードはトンネルインターフェイスで動作しますが、BGP ルートの IPsec トランスポートモードは物理インターフェイスでのみ機能します。
- デフォルトでは、IPsec トンネルはトンネルモードで動作します。
- マルチキャストパケットをカプセル化するには、トランスポートモードで **[GRE**カプセル化の追加**]** を有効にする必要があります。

PAN-OS 10.2 以前のバージョンはトランスポートモードをサポートしていないため、以前のバージョンにダウングレードすると互換性の問題が発生します。ダウングレードする前に、トランスポートモードのトンネルを手動で削除するか、トンネルモードに切り替える必要があります。そうしないと、ダウングレードが失敗します。

©2024 Palo Alto Networks, Inc.

- PAN-OS 11.0以降

©2024 Palo Alto Networks, Inc.

IPSec VPN トンネルを監視する

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンス不要

中断のない VPN サービスを提供するには、デッド ピア ディテクション機能とファイアウォールのトンネル モニタリング機能を使用できます。トンネルの状態をモニタリングすることもできます。これらのモニタリング タスクについては、以下のセクションで説明します。

- トンネル モニタリング プロファイルの定義
- #unique_47

トラブルシューティングのために、IKE ゲートウェイまたは IPSec トンネルの有効化/無効化、更新、または再起動を行えます。

トンネル モニタリング プロファイルの定義

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

トンネル モニタリング プロファイルにより、VPN ピア間の接続を確認できます。トンネル インターフェイスが指定した間隔で宛先 IP アドレスに ping を送信するように設定し、トンネル間の通信が切断された場合のアクションを指定できます。

STEP 1 | **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **Monitor (**監視**)** を選択します。デフォルトのトンネル モニタリング プロファイルが使用できます。

STEP 2 | **[**追加**]** をクリックし、プロファイルの **[**名前**]** を入力します。

STEP 3 | 宛先 IP アドレスに到達できない場合に実行する **Action (**アクション**)** を選択します。

- 回復を待機 — ファイアウォールはトンネルが回復するのを待機します。ファイアウォールでは、トンネルがまだアクティブであるかのようにして、そのトンネル インターフェイスをルート決定で使用し続けます。
- フェイル オーバー — バックアップ パスが使用できる場合、強制的にトラフィックをバックアップ パスに誘導します。ファイアウォールはトンネル インターフェイスを無効化し、それによってそのインターフェイスを使用するルーティング テーブルのルートが無効になります。

いずれの場合でも、ファイアウォールは新しい IPSec キーをネゴシエートすることで回復を早めようとします。

STEP 4 | 指定したアクションをトリガーする**Interval (sec) (**間隔（秒）**)** と **Threshold (**しきい値**)** を指定します。

- **Threshold (**しきい値**)** は、指定したアクションがファイアウォールによって実行されまでに待機するハートビートの数（範囲は 2～100、デフォルトは 5）を指定します。
- **Interval (sec) (**間隔（秒）**)** は、ハートビート間隔（範囲は2～ 10、デフォルトは3）を指定します。

STEP 5 | モニタリング プロファイルを IPsec トンネル設定に関連付けます。トンネル モニタリングの有効化を参照してください。

©2024 Palo Alto Networks, Inc.

トンネルの[状態]を確認します。

どこで使用できますか?	何が必要ですか?
• PAN-OS • Cloud Management	❑ ライセンスは必要ありません ❑ AIOps for NGFW プレミアム ライセンス

トンネルの状態から、有効な IKE フェーズ 1 およびフェーズ 2 SA が確立されているかどうか、トンネル インターフェイスが起動していてトラフィックを通過させることができるかどうかが分かります。

トンネル インターフェイスは論理インターフェイスであるため、物理リンクの状態を示すことはできません。したがって、トンネル モニタリングを有効にして、トンネル インターフェイスで IP アドレスへの接続を確認し、パスが使用できるかどうかを判断できるようにする必要があります。IP アドレスに到達できない場合、ファイアウォールはトンネルが回復するのを待機するか、フェイルオーバーします。フェイルオーバーが行われると、既存のトンネルはダウンして、ルーティング変更がトリガーされ、新しいトンネルがセットアップされてトラフィックが転送されます。

- PAN-OS
- クラウド管理

IPSec VPN トンネルのステータスを表示する

STEP 1 | **Network (**ネットワーク**) > IPSec Tunnels (IPSec** トンネル**)**の順に選択します。

STEP 2 | トンネルの **[**状態**]** を確認します。

- 緑は、有効な IPSec SA トンネルがあることを表します。
- 赤は、IPSec SA が使用できないか、有効期限が切れていることを表します。

STEP 3 | IKE ゲートウェイの **[**状態**]** を確認します。

- 緑は、有効な IKE フェーズ 1 SA があることを表します。
- 赤は、IKE フェーズ 1 SA が使用できないか、有効期限が切れていることを表します。

©2024 Palo Alto Networks, Inc.

STEP 4 | **Tunnel Interface Status**（トンネル インターフェイスの状態）を確認します。

- 緑は、トンネル インターフェイスが起動していることを表します。
- 赤は、トンネル インターフェイスがダウンしている（トンネル モニタリングが有効になっていて状態がダウンであるため）ことを表します。

まだ稼働していない VPN トンネルのトラブルシューティングを行うには、VPN エラー メッセージの解釈を参照してください。

IPSec VPN トンネルのステータスの表示

STEP 1 | Strata Cloud Manager にログインします。

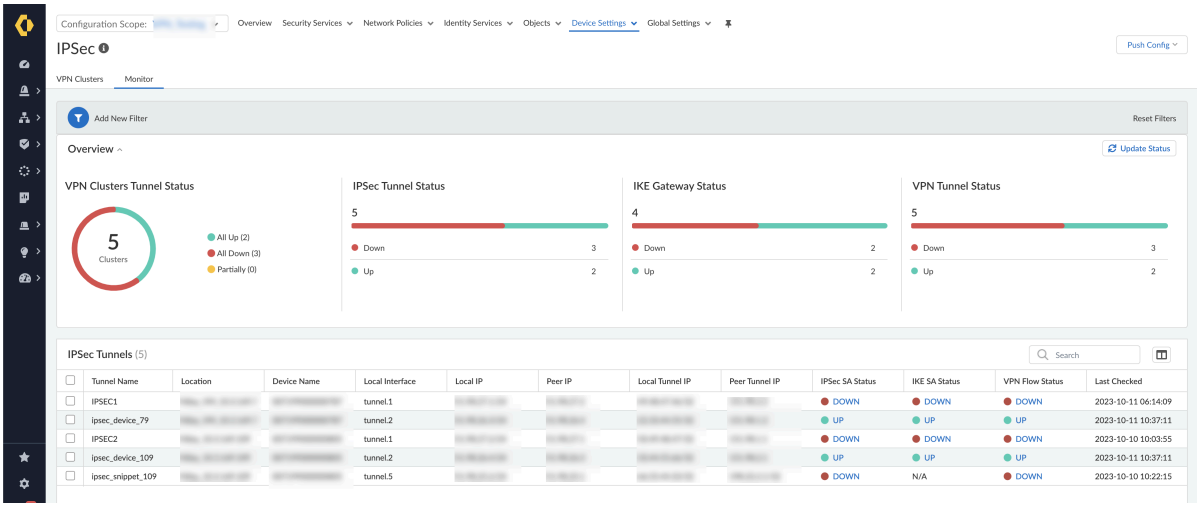
STEP 2 | [**Manage (**管理**)** > **Configuration (**設定**)** > **NGFW** と **Prisma Access** > **Device Settings (**デバイス設定**)** > **IPSec Tunnels (IPSec** トンネル**)**]を選択し、[**Monitor (**監視**)**]を選択します。

©2024 Palo Alto Networks, Inc.

STEP 3 | [**Configuration Scope (範囲の設定)]**を選択すると、IPSec VPNトンネルのステータスが表示されます。［フォルダ］からフォルダまたはファイアウォールを選択して、ファイアウォール上に作成した IPSec VPN トンネルを監視できます。

- すべてのファイアウォールの IPSec トンネルのステータスを表示するには、[すべてのファイアウォール]フォルダを選択します。
- フォルダに関連付けられたファイアウォールグループの IPSec トンネルのステータスを表示するには、特定のフォルダを選択します。
- 特定のファイアウォールのIPSecトンネルのステータスを表示するには、ファイアウォールを選択します。

- *AutoVPN* を使用して *VPN* クラスタを作成した場合は、それらのファイアウォールの *IPSec* トンネルの状態を監視できません。
- 監視できるのはオンプレミスのファイアウォールのみで、*Prisma Access* が管理するコンポーネントは監視できません。
- グローバルレベルとスニペットレベルで監視が無効になります。したがって、グローバルまたはスニペット設定スコープで *IPSec* トンネルを作成できますが、*IPSec* トンネルを監視できるのはフォルダまたはファイアウォールレベルだけです。



STEP 4 | アップしているトンネル数、ダウンしているトンネル数、および部分的にアップしているトンネル数のグラフ表示を提供する **VPN** クラスタトンネルステータスを表示します。

 ©2024 Palo Alto Networks, Inc.

STEP 5 | **IPSec** トンネルの **IPSec SA** ステータスを表示する。

- 緑（**UP**）は、有効なIPSec SAトンネルであることを示します。**UP** を選択すると、IPSec トンネルに関する詳細情報が表示されます。
- 赤（**DOWN**）は、IPSec SAが利用できないか、有効期限が切れていることを示します。**DOWN**を選択すると、失敗の理由を解釈するための詳細情報が表示されます。

STEP 6 | **IPSec** トンネルの **IKE SA** ステータスを表示する。

- 緑（**UP**）は、有効な IKE フェーズ 1 SA があることを示します。**UP** を選択すると、IKE ゲートウェイに関する詳細情報が表示されます。
- 赤（**DOWN**）は、IKE フェーズ 1 SA が使用できないか、有効期限が切れていることを表します。**DOWN**を選択すると、失敗の理由を解釈するための詳細情報が表示されます。

STEP 7 | **IPSec**トンネル内のVPNトラフィックフロー情報の**VPN**フローステータスを表示する。

- 緑（**UP**）は、IPSec トンネルがアップしていることを示します。**UP** を選択すると、VPN トラフィック フローに関する詳細情報が表示されます。
- 赤（**DOWN**）は、IPSec トンネルがダウンしていることを示します。**DOWN**を選択すると、失敗の理由を解釈するための詳細情報が表示されます。

STEP 8 | [新しいフィルタを追加]を選択し、選択したフィールドに基づいて結果を表示するフィールドを選択します。例えば、リストからデバイス名を選択し新しいフィルタを追加すると、選択したデバイスの IPSec トンネルステータスが表示されます。

1つ以上のフィルタを削除するには、[フィルタをリセットReset Filters]を選択します。

STEP 9 | ［ステータスを更新］ を選択すると、そのレベル（ファイアウォール、フォルダ、またはすべてのファイアウォール）に存在するすべての IPSec トンネル監視データが更新されます。

©2024 Palo Alto Networks, Inc.

IKE ゲートウェイまたは IPSec トンネルの有効化/無効化、更新、または再起動

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

IKE ゲートウェイまたは VPN トンネルを有効化、無効化、更新、または再起動できます。

- IKE ゲートウェイまたは IPSec トンネルの有効化または無効化
- IKE ゲートウェイまたは IPSec トンネルの更新または再起動

IKE ゲートウェイまたは IPSec トンネルの有効化または無効化

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンス不要

IKE ゲートウェイまたは IPSec トンネルを有効または無効にして、トラブルシューティングを容易にします。

IKE ゲートウェイを有効または無効にします。

1. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IKE Gateways (IKE** ゲートウェイ**)** の順に選択し、有効または無効にするゲートウェイを選択します。
2. 画面の下部で **Enable** [有効化]または **Disable** [無効化]をクリックします。

IPSec トンネルを有効または無効にします。

1. **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)** の順に選択し、有効または無効にするトンネルを選択します。
2. 画面の下部で **Enable** [有効化]または **Disable** [無効化]をクリックします。

IKE ゲートウェイまたは IPSec トンネルの更新または再起動

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

©2024 Palo Alto Networks, Inc.

IKE ゲートウェイまたは IPSec トンネルを更新または再起動できます。IKE ゲートウェイと IPSec トンネルの更新および再起動の動作は以下のようになります。

フェーズ	**Refresh**（更新）	再起動
IKE ゲートウェイ（IKE フェーズ 1）	選択した IKE ゲートウェイの画面上の統計を更新します。 CLI で 2 番目の `show` コマンド（最初の `show` コマンドの後）を発行することと同じです。	選択した IKE ゲートウェイを再起動します。 **IKEv2**：関連付けられた子 IPSec Security Associations （SA）も再起動されます。 **IKEv1**:関連付けられた IPSec SA を再起動しません。 再起動は既存のすべてのセッションに影響します。 CLI で **`clear`**、**`test`**、**`show`** コマンドを連続して発行することと同じです。
IPSec トンネル（IKE フェーズ 2）	選択した IPSec トンネルの画面上の統計を更新します。 CLI で 2 番目の `show` コマンド（最初の `show` コマンドの後）を発行することと同じです。	IPSec トンネルを再起動します。 再起動は既存のすべてのセッションに影響します。 CLI で **`clear`**、**`test`**、**`show`** コマンドを連続して発行することと同じです。

IKE ゲートウェイを再起動した結果は、それが IKEv1 か IKEv2 かによって異なりますので、ご注意ください。

IKE ゲートウェイを更新または再起動します。

1. **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)** の順に選択し、更新または再起動するゲートウェイのトンネルを選択します。
2. そのトンネルの行の Status [状態]列で、**IKE Info** [IKE 情報]をクリックします。
3. IKE Info （IKE 情報）画面の下部で、以下のいずれかのアクションをクリックします。
   - **Refresh** [更新] — 画面上の統計を更新します。
   - **Restart** [再起動] — SA をクリアします。これにより、IKE ネゴシエーションをやり直してトンネルが再作成されるまでトラフィックはドロップされます。

©2024 Palo Alto Networks, Inc.

IPSec トンネルを更新または再起動します。

トンネル モニターを使用したトンネル状態のモニタリング、または外部ネットワーク モニターを使用した IPSec トンネル経由のネットワーク接続のモニタリングを行うときに、トンネルを更新するか再起動するかの判断が必要な場合があります。

1. **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)** の順に選択し、更新または再起動するトンネルを選択します。
2. そのトンネルの行の Status [状態]列で、**Tunnel Info** [トンネル情報]をクリックします。
3. Tunnel Info （トンネル情報）画面の下部で、以下のいずれかのアクションをクリックします。
   - **Refresh** [更新] — 画面上の統計を更新します。
   - **Restart** [再起動] — SA をクリアします。これにより、IKE ネゴシエーションをやり直してトンネルが再作成されるまでトラフィックはドロップされます。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

サイト間 VPN の構成例

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

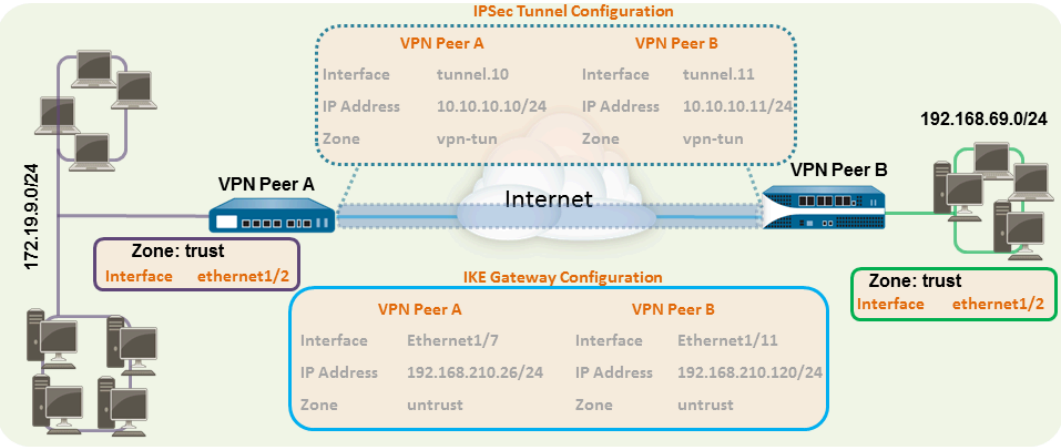
以下のセクションでは、一般的な VPN デプロイメントのための手順を説明します。

- スタティック ルーティングを使用したサイト間 VPN
- OSPF を使用したサイト間 VPN
- スタティック ルーティングおよびダイナミック ルーティングを使用したサイト間 VPN

スタティック ルーティングを使用したサイト間 VPN

これはどこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

以下の例は、スタティック ルートを使用する 2 つのサイト間の VPN 接続を示しています。ダイナミック ルーティングを使用しない場合、VPN ピア A および VPN ピア B のトンネル インターフェイスに IP アドレスは必要ありません。これは、ファイアウォールが、サイト間のトラフィックのルーティングのために自動的にトンネル インターフェイスをネクスト ホップとして使用するためです。ただし、トンネル モニタリングを有効化するために、スタティック IP アドレスが各トンネル インターフェイスに割り当てられています。



©2024 Palo Alto Networks, Inc.

STEP 1 | レイヤー 3 インターフェイスを設定します。

このインターフェイスが IKE フェーズ 1 トンネルに使用されます。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** > **Ethernet (**イーサネット**)** の順に選択し、VPN について設定するインターフェイスを選択します。
2. **Interface Type (**インターフェイス タイプ**)** で **Layer3 (**レイヤー **3)** を選択します。
3. **Config (**設定**)** タブでインターフェイスが属する **Security Zone (**セキュリティ ゾーン**)** を選択します。
   - インターフェイスは、信頼されるネットワークの外部のゾーンからアクセスできる必要があります。VPN トラフィックを可視化して制御するために、専用の VPN ゾーンを作成することを検討してください。
   - まだゾーンを作成していない場合は、**Security Zone (**セキュリティ ゾーン**)** から **New Zone (**新規ゾーン**)** を選択し、新規ゾーンの **Name (**名前**)** を定義してから **OK** をクリックします。
4. 使用する **Virtual Router (**仮想ルーター**)** を選択します。
5. IP アドレスをインターフェイスに割り当てるには、**IPv4** タブを選択してから IP セクションで **Add**（追加）をクリックし、インターフェイスに割り当てる IP アドレスとネットマスク（例: 192.168.210.26/24）を入力します。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(**インターフェイス**)**—ethernet1/7
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 192.168.210.26/24

   VPN ピア B の設定は以下のようになります。

   - **Interface(**インターフェイス**)**—ethernet1/11
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 192.168.210.120/24

©2024 Palo Alto Networks, Inc.

STEP 2 | トンネル インターフェイスを作成し、仮想ルーターおよびセキュリティ ゾーンに関連付けます。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** > **Tunnel (**トンネル**)** の順に選択し、**Add(**追加**)** をクリックします。
2. **Interface Name**（インターフェイス名）フィールドで、**.1**などの数値のサフィックスを指定します。
3. **Config (**設定**)** タブで、**Security Zone (**セキュリティ ゾーン**)** を展開して以下のようにゾーンを定義します。
   - トンネルの終端点として信頼されたゾーンを使用するには、そのゾーンを選択します。
   - （推奨）VPN トンネルの終端のゾーンを別に作成するには、**New Zone**（新規ゾーン）をクリックします。[ゾーン] ダイアログの **[**名前**]** で「*vpn-tun*」などの名前を付けて新しいゾーンを定義し、**[OK]** をクリックします。
4. **Virtual Router**[仮想ルーター] を選択します。
5. （任意）トンネル インターフェイスに IP アドレスを割り当て、**IPv4** タブまたは **IPv6** タブを選択してから IP セクションで **Add** [追加]をクリックし、インターフェイスに割り当てる IP アドレスとネットマスクを入力します。

   スタティック ルートでは、トンネル インターフェイスに IP アドレスは必要ありません。指定したサブネット/IP アドレスを宛先とするトラフィックでは、トンネル インターフェイスが自動的にネクスト ホップになります。トンネル モニタリングを有効化する場合、IP アドレスの追加を検討してください。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。
   - インターフェイス — tunnel.10
   - セキュリティ ゾーン — vpn_tun
   - 仮想ルーター — デフォルト
   - **IPv4** — 172.19.9.2/24

   VPN ピア B の設定は以下のようになります。
   - インターフェイス — tunnel.11
   - セキュリティ ゾーン — vpn_tun
   - 仮想ルーター — デフォルト
   - **IPv4** — 192.168.69.2/24

©2024 Palo Alto Networks, Inc.

STEP 3 | 仮想ルーターで宛先サブネットへのスタティック ルートを設定します。

1. **Network (**ネットワーク**)** > **Virtual Router (**仮想ルーター**)** の順に選択し、前のステップで定義したルーターをクリックします。
2. **[**スタティック ルート**]** を選択し、追加 をクリックして、トンネルの反対側にあるサブネットにアクセスする新しいルートを入力します。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Destination**（宛先） — 192.168.69.0/24
   - インターフェイス — tunnel.10

   VPN ピア B の設定は以下のようになります。

   - 宛先 — 172.19.9.0/24
   - インターフェイス — tunnel.11

STEP 4 | 暗号プロファイル（フェーズ 1 では IKE 暗号プロファイル、フェーズ 2 では IPSec 暗号プロファイル）をセットアップします。

両方のピアでこのタスクを実行し、必ず同じ値を設定します。

1. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IKE** 暗号化を選択します。この例では、デフォルトのプロファイルを使用します。
2. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IPSec Crypto (IPSec** 暗号**)** を選択します。この例では、デフォルトのプロファイルを使用します。

©2024 Palo Alto Networks, Inc.

STEP 5 | IKE ゲートウェイをセットアップします。

1. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IKE Gateway (IKE** ゲートウェイ**)** を選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(**インターフェイス**)**—ethernet1/7
   - ローカル **IP** アドレス — 192.168.210.26/24
   - ピア **IP** タイプ/アドレス — スタティック/192.168.210.120
   - 事前共有鍵 — 値を入力
   - ローカル **ID** — なし。ローカル ID 値としてローカル IP アドレスが使用されます。
   - VPN ピア B の設定は以下のようになります。
   - **Interface(**インターフェイス**)**—ethernet1/11
   - ローカル **IP** アドレス — 192.168.210.120/24
   - ピア **IP** タイプ/アドレス — スタティック/192.168.210.26
   - 事前共有鍵 — ピア A と同じ値を入力
   - ローカル **ID** — なし
3. **[**詳細フェーズ **1** のオプション**]** を選択し、IKE フェーズ 1　で使用するために以前に作成した IKE 暗号プロファイルを選択します。

©2024 Palo Alto Networks, Inc.

STEP 6 | IPSec トンネルをセットアップします。

1. **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)**の順に選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Tunnel Interface(**トンネル インターフェイス)—tunnel.10
   - タイプ — 自動キー
   - **IKE** ゲートウェイ — 上で定義した IKE ゲートウェイを選択します。
   - **IPSec Crypto Profile**—ステップ 4 で定義した IPSec Crypto プロファイルを選択して下さい。

   VPN ピア B の設定は以下のようになります。

   - **Tunnel Interface(**トンネル インターフェイス)—tunnel.11
   - タイプ — 自動キー
   - **IKE** ゲートウェイ — 上で定義した IKE ゲートウェイを選択します。
   - **IPSec Crypto Profile** - 手順 4 で定義した IPSec Crypto を選択します。
3. （任意）**Show Advanced Options**（詳細オプションの表示）をオンにし、**Tunnel Monitor**（トンネル監視）をオンにして、接続を確認するために ping を送信する宛先 IP アドレスを指定します。一般に、VPN ピアのトンネル インターフェイス IP アドレスが使用されます。
4. （任意）接続の確立に失敗した場合のアクションを定義する方法については、トンネル モニタリング プロファイルの定義を参照してください。

STEP 7 | トラフィックをサイト（サブネット）間で許可するためのポリシー ルールを作成します。

1. **Policies** > **Security**を選択します。
2. 指定した送信元および宛先 IP アドレスから発信されるトラフィックについて、トラフィックを Uuntrust ゾーンと vpn-tun ゾーン間および vpn-tun ゾーンと Untrust ゾーン間で許可するためのルールを作成します。

STEP 8 | 保留中の設定の変更をすべてコミットします。

Commit（コミット）をクリックします。

STEP 9 | 「VPN 接続のテスト」を行います。

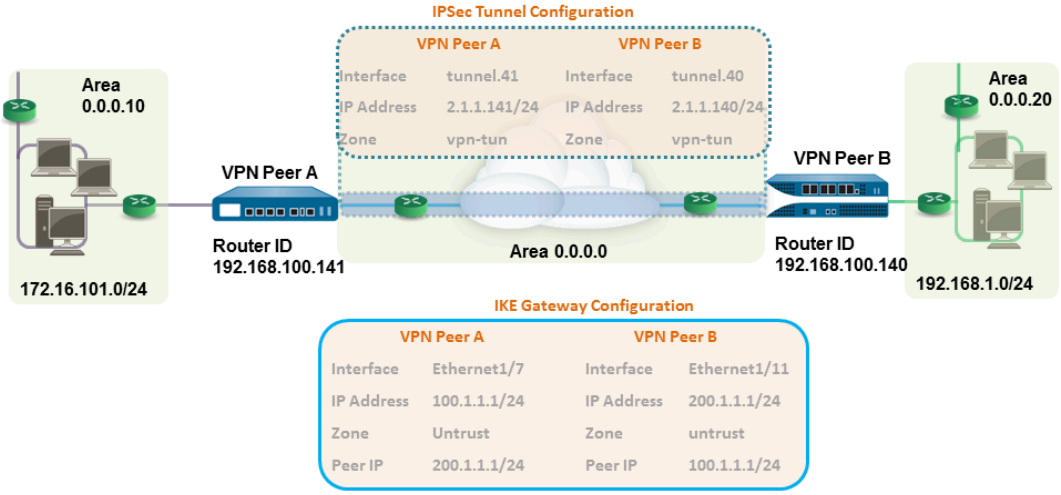
トンネルの状態の表示も参照してください。

 ©2024 Palo Alto Networks, Inc.

OSPF を使用したサイト間 VPN

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

この例では、各サイトはトラフィックのダイナミック ルーティングに OSPF を使用します。各 VPN ピアのトンネル IP アドレスは静的に割り当てられ、2 つのサイト間でトラフィックをルーティングするためのネクスト ホップとして機能します。



©2024 Palo Alto Networks, Inc.

STEP 1 | 各ファイアウォールでレイヤー 3 インターフェイスを設定します。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** > **Ethernet (**イーサネット**)** の順に選択し、VPN について設定するインターフェイスを選択します。
2. **Interface Type (**インターフェイス タイプ**)** リストから **Layer3 (**レイヤー **3)** を選択します。
3. **Config (**設定**)** タブでインターフェイスが属する **Security Zone (**セキュリティ ゾーン**)** を選択します。
   - インターフェイスは、信頼されるネットワークの外部のゾーンからアクセスできる必要があります。VPN トラフィックを可視化して制御するために、専用の VPN ゾーンを作成することを検討してください。
   - ゾーンをまだ作成していない場合は、**[**セキュリティ ゾーン**]** リストから **[**新しいゾーン**]** を選択し、新しいゾーンの 名前 を定義して、**[OK]**をクリックします。
4. 使用する **Virtual Router (**仮想ルーター**)** を選択します。
5. IP アドレスをインターフェイスに割り当てるには、**IPv4** タブを選択してから IP セクションで **Add**（追加）をクリックし、インターフェイスに割り当てる IP アドレスとネットマスク（例: 192.168.210.26/24）を入力します。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(**インターフェイス**)**—ethernet1/7
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 100.1.1.1/24

   VPN ピア B の設定は以下のようになります。

   - **Interface(**インターフェイス**)**—ethernet1/11
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 200.1.1.1/24

©2024 Palo Alto Networks, Inc.

STEP 2 | トンネル インターフェイスを作成し、仮想ルーターおよびセキュリティ ゾーンに関連付けます。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** > **Tunnel (**トンネル**)** の順に選択し、**Add(**追加**)** をクリックします。
2. **Interface Name (**インターフェイス名**)** フィールドで、**.11** などの数値のサフィックスを指定します。
3. **Config (**設定**)** タブで、**Security Zone (**セキュリティ ゾーン**)** を展開して以下のようにゾーンを定義します。
   - トンネルの終端点として信頼されたゾーンを使用するには、そのゾーンを選択します。
   - （推奨）VPN トンネルの終端のゾーンを別に作成するには、**New Zone**（新規ゾーン）をクリックします。[ゾーン] ダイアログの **[**名前**]** で「vpn-tun」などの名前を付けて新しいゾーンを定義し、**[OK]** をクリックします。
4. **Virtual Router**[仮想ルーター] を選択します。
5. IP アドレスをトンネル インターフェイスに割り当て、**[IPv4]** または **[IPv6]** タブを選択します。[IP] セクションで **[**追加**]** をクリックし、インターフェイスに割り当てる IP アドレスとネットワーク マスク/プレフィックス（例: 172.19.9.2/24）を入力します。

   この IP アドレスは、トンネルにトラフィックをルーティングするためにネクスト ホップ IP アドレスとして使用され、トンネルの状態をモニタリングするために使用することもできます。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。
   - **Interface**[インターフェイス] — tunnel.41
   - セキュリティ ゾーン — vpn_tun
   - 仮想ルーター — デフォルト
   - **IPv4** — 2.1.1.141/24

   VPN ピア B の設定は以下のようになります。
   - **Interface**[インターフェイス] — tunnel.40
   - セキュリティ ゾーン — vpn_tun
   - 仮想ルーター — デフォルト
   - **IPv4** — 2.1.1.140/24

©2024 Palo Alto Networks, Inc.

STEP 3 | 暗号プロファイル（フェーズ 1 では IKE 暗号プロファイル、フェーズ 2 では IPSec 暗号プロファイル）をセットアップします。

両方のピアでこのタスクを実行し、必ず同じ値を設定します。

1. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IKE** 暗号化を選択します。この例では、デフォルトのプロファイルを使用します。
2. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IPSec Crypto (IPSec** 暗号**)** を選択します。この例では、デフォルトのプロファイルを使用します。

STEP 4 | 仮想ルーターで OSPF 設定をセットアップし、OSPF エリアをファイアウォール上の適切なインターフェイスに関連付けます。

ファイアウォールで使用可能な OSPF オプションの詳細は、「OSPF の設定」を参照してください。

ルーティング情報を交換する必要がある OSPF ルートが 2 つ以上ある場合、リンク タイプとして Broadcast （ブロードキャスト）を使用します。

1. **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)** の順に選択し、デフォルトのルーターを選択するか新しいルーターを追加します。
2. **OSPF**（IPv4 の場合）または **OSPFv3** （IPv6 の場合）を選択し、**Enable**（有効）をオンにします。
3. この例では、VPN ピア A の OSPF 設定は以下のようになります。
   - ルーター**ID**：192.168.100.141
   - エリア **ID**：0.0.0.0 — リンク タイプ「p2p」で、インターフェイス tunnel.1 に割り当てられている
   - エリア **ID**：インターフェイス Ethernet1/1およびリンク タイプに0.0.0.10 が割り当てられているブロードキャスト

   VPN ピア B の OSPF 設定は以下のようになります。
   - ルーター**ID**：192.168.100.140
   - エリア **ID**：0.0.0.0 — リンク タイプ「p2p」で、インターフェイス tunnel.1 に割り当てられている
   - エリア **ID**：インターフェイス Ethernet1/15およびリンク タイプに0.0.0.20 が割り当てられているブロードキャスト

 ©2024 Palo Alto Networks, Inc.

STEP 5 | IKE ゲートウェイをセットアップします。

この例では、両方の VPN ピアに静的 IP アドレスを使用します。一般に、企業オフィスでは静的に設定された IP アドレスを使用し、支社側をダイナミック IP アドレスにできます。ダイナミック IP アドレスは、VPN などの安定したサービスの設定には適しません。

1. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IKE Gateway (IKE** ゲートウェイ**)** を選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(**インターフェイス**)**—ethernet1/7
   - ローカル **IP** アドレス — 100.1.1.1/24
   - ピア **IP** アドレス — 200.1.1.1/24
   - 事前共有鍵 — 値を入力

   VPN ピア B の設定は以下のようになります。

   - **Interface(**インターフェイス**)**—ethernet1/11
   - ローカル **IP** アドレス — 200.1.1.1/24
   - ピア **IP** アドレス — 100.1.1.1/24
   - 事前共有鍵 — ピア A と同じ値を入力
3. IKE フェーズ 1 で使用するために以前に作成した IKE 暗号プロファイルを選択します。

©2024 Palo Alto Networks, Inc.

STEP 6 | IPSec トンネルをセットアップします。

1. **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)**の順に選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - トンネル インターフェイス — tunnel.41
   - タイプ — 自動キー
   - **IKE** ゲートウェイ — 上で定義した IKE ゲートウェイを選択します。
   - **IPSec** 暗号プロファイル — 上で定義した IKE ゲートウエィを選択します。

   VPN ピア B の設定は以下のようになります。

   - **Tunnel Interface(**トンネル インターフェイス**)**—tunnel.40
   - タイプ — 自動キー
   - **IKE** ゲートウェイ — 上で定義した IKE ゲートウェイを選択します。
   - **IPSec** 暗号プロファイル — 上で定義した IKE ゲートウエィを選択します。
3. **Show Advanced Options** [詳細オプションの表示]をオンにし、**Tunnel Monitor** [トンネル モニター]をオンにして、接続を確認するために ping を送信する宛先 IP アドレスを指定します。
4. 接続の確立に失敗した場合のアクションを定義する方法については、トンネル モニタリング プロファイルの定義を参照してください。

STEP 7 | トラフィックをサイト（サブネット）間で許可するためのポリシー ルールを作成します。

1. **Policies** > **Security**を選択します。
2. 指定した送信元および宛先 IP アドレスから発信されるトラフィックについて、トラフィックを Uuntrust ゾーンと vpn-tun ゾーン間および vpn-tun ゾーンと Untrust ゾーン間で許可するためのルールを作成します。

 ©2024 Palo Alto Networks, Inc.

STEP 8 | OSPF 隣接および CLI からのルートを確認します。

両方のファイアウォールが互いにネイバーとして完全な状態で表示できることを確認します。また、VPN ピアのトンネル インターフェイスの IP アドレスおよび OSPF ルーター ID も確認します。各 VPN ピアで以下の CLI コマンドを使用します。

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route type ospf**

```
admin@FW-A> show routing route type ospf

flags: A:active, ?:loose, C:connect, H:host, S:static, ~:internal, R:rip, O:ospf, B:bgp,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface          next-AS
2.1.1.0/24              0.0.0.0                 10   Oi       6760  tunnel.41
172.16.101.0/24         0.0.0.0                 10   Oi       6854  ethernet1/1
192.168.1.0/24          2.1.1.140               20 A Oo       6754  tunnel.40
total routes shown: 3
```

```
admin@FW-B> show routing route type ospf

flags: A:active, C:connect, H:host, S:static, R:rip, O:ospf,
       Oi:ospf intra-area, Oo:ospf inter-area, O1:ospf ext-type-1, O2:ospf ext-type-2


VIRTUAL ROUTER: vr1 (id 1)
  ==========
destination             nexthop             metric flags      age   interface
2.1.1.0/24              0.0.0.0                 10   Oi       20033 tunnel.40
172.16.101.0/24         2.1.1.141               20   AOo      6896  tunnel.40
192.168.1.0/24          0.0.0.0                 10   Oi       8058  ethernet1/15
total routes shown: 3
```


©2024 Palo Alto Networks, Inc.

STEP 9 | 「VPN 接続のテスト」を行います。

トンネル モニタリングのセットアップおよびトンネルの状態の表示を参照してください。

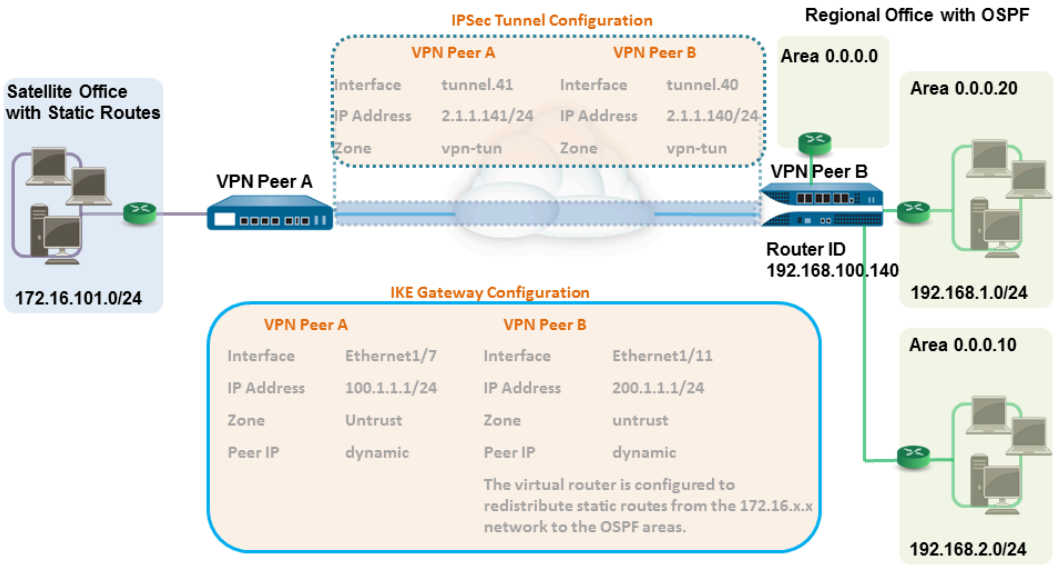
©2024 Palo Alto Networks, Inc.

スタティック ルーティングおよびダイナミック ルーティングを使用したサイト間 VPN

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

この例では、一方のサイトでスタティック ルートを使用し、もう一方のサイトで OSPF を使用しています。ルーティング プロトコルが場所間で同じでない場合、各ファイアウォールのトンネル インターフェイスはスタティック IP アドレスで設定する必要があります。次に、ルーティング情報の交換を可能にするために、スタティック ルーティングとダイナミック ルーティングの両方のプロセスに参加するファイアウォールを再配信プロファイルで設定する必要があります。再配信プロファイルを設定すると、仮想ルーターはプロトコル間のルート（スタティック ルート、接続済みルート、ホスト）をスタティック Autonomous System から OSPF Autonomous System に再配信してフィルタリングできます。この再配信プロファイルがない場合、各プロトコルは独自に機能し、同じ仮想ルーターを実行している他のプロトコルとルート情報を交換しません。

この例では、サテライト オフィスはスタティック ルートを持ち、192.168.x.x ネットワークを宛先とするすべてのトラフィックは tunnel.41 にルーティングされます。VPN ピア B の仮想ルーターはスタティック ルーティングとダイナミック ルーティングの両方のプロセスに参加し、スタティック ルートを OSPF Autonomous System に配信（エクスポート）するために再配信プロファイルで設定されます。



©2024 Palo Alto Networks, Inc.

STEP 1 | 各ファイアウォールでレイヤー 3 インターフェイスを設定します。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** > **Ethernet (**イーサネット**)** の順に選択し、VPN について設定するインターフェイスを選択します。
2. **Interface Type (**インターフェイス タイプ**)** で **Layer3 (**レイヤー **3)** を選択します。
3. **Config (**設定**)** タブでインターフェイスが属する **Security Zone (**セキュリティ ゾーン**)** を選択します。
   - インターフェイスは、信頼されるネットワークの外部のゾーンからアクセスできる必要があります。VPN トラフィックを可視化して制御するために、専用の VPN ゾーンを作成することを検討してください。
   - まだゾーンを作成していない場合は、**Security Zone (**セキュリティ ゾーン**)** から **New Zone (**新規ゾーン**)** を選択し、新規ゾーンの **Name (**名前**)** を定義してから **OK** をクリックします。
4. 使用する **Virtual Router (**仮想ルーター**)** を選択します。
5. IP アドレスをインターフェイスに割り当てるには、**IPv4** タブを選択してから IP セクションで **Add**（追加）をクリックし、インターフェイスに割り当てる IP アドレスとネットマスク（例: 192.168.210.26/24）を入力します。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(**インターフェイス**)**—ethernet1/7
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 100.1.1.1/24

   VPN ピア B の設定は以下のようになります。

   - **Interface(**インターフェイス**)**—ethernet1/11
   - セキュリティ ゾーン — Untrust
   - 仮想ルーター — デフォルト
   - **IPv4** — 200.1.1.1/24

STEP 2 | 暗号プロファイル（フェーズ 1 では IKE 暗号プロファイル、フェーズ 2 では IPSec 暗号プロファイル）をセットアップします。

両方のピアでこのタスクを実行し、必ず同じ値を設定します。

1. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IKE** 暗号化を選択します。この例では、デフォルトのプロファイルを使用します。
2. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IPSec Crypto (IPSec** 暗号**)** を選択します。この例では、デフォルトのプロファイルを使用します。

©2024 Palo Alto Networks, Inc.

STEP 3 | IKE ゲートウェイをセットアップします。

IKE フェーズ 1 トンネルをセットアップするときに認証の精度を高めるために事前共有鍵を使用すると、ローカルおよびピア ID 属性、および IKE ネゴシエーション プロセスで照合される対応する値をセットアップできます。

1. **Network (**ネットワーク**)** > **Network Profiles (**ネットワーク プロファイル**)** > **IKE Gateway (IKE** ゲートウェイ**)** を選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - **Interface(**インターフェイス**)**—ethernet1/7
   - ローカル **IP** アドレス — 100.1.1.1/24
   - ピア **IP** タイプ — ダイナミック
   - 事前共有鍵 — 値を入力
   - ローカル **ID** — **[FQDN (hostname)]** を選択し、VPN ピア A の値を入力します。
   - ピア **ID** — **[FQDN (hostname)]** を選択し、VPN ピア B の値を入力します。

   VPN ピア B の設定は以下のようになります。

   - **Interface(**インターフェイス**)**—ethernet1/11
   - ローカル **IP** アドレス — 200.1.1.1/24
   - ピア **IP** アドレス — ダイナミック
   - 事前共有鍵 — ピア A と同じ値を入力
   - ローカル **ID** — **[FQDN (hostname)]** を選択し、VPN ピア B の値を入力します。
   - ピア **ID** — **[FQDN (hostname)]** を選択し、VPN ピア A の値を入力します。
3. IKE フェーズ 1 で使用するために以前に作成した IKE 暗号プロファイルを選択します。

©2024 Palo Alto Networks, Inc.

STEP 4 | トンネル インターフェイスを作成し、仮想ルーターおよびセキュリティ ゾーンに関連付けます。

1. **Network (**ネットワーク**)** > **Interfaces (**インターフェイス**)** > **Tunnel (**トンネル**)** の順に選択し、**Add(**追加**)** をクリックします。
2. **[**インターフェイス名**]** フィールドで、**.41** などの数値のサフィックスを指定します。
3. **Config (**設定**)** タブで、**Security Zone (**セキュリティ ゾーン**)** を展開して以下のようにゾーンを定義します。
   - トンネルの終端点として信頼されたゾーンを使用するには、そのゾーンを選択します。
   - （推奨）VPN トンネルの終端のゾーンを別に作成するには、**New Zone**（新規ゾーン）をクリックします。[ゾーン] ダイアログの **[**名前**]** で「*vpn-tun*」などの名前を付けて新しいゾーンを定義し、**[OK]** をクリックします。
4. **Virtual Router**[仮想ルーター] を選択します。
5. IP アドレスをトンネル インターフェイスに割り当て、**[IPv4]** または **[IPv6]** タブを選択します。[IP] セクションで **[**追加**]** をクリックし、インターフェイスに割り当てる IP アドレスとネットワーク マスク/プレフィックス（例: 172.19.9.2/24）を入力します。

   この IP アドレスは、トンネルにトラフィックをルーティングするため、およびトンネルの状態をモニタリングするために使用されます。
6. インターフェイス設定を保存するには、**OK** をクリックします。

   この例では、VPN ピア A の設定は以下のようになります。
   - **Interface**[インターフェイス] — tunnel.41
   - セキュリティ ゾーン — vpn_tun
   - 仮想ルーター — デフォルト
   - **IPv4** — 2.1.1.141/24

   VPN ピア B の設定は以下のようになります。
   - インターフェイス — tunnel.42
   - セキュリティ ゾーン — vpn_tun
   - 仮想ルーター — デフォルト
   - **IPv4** — 2.1.1.140/24

STEP 5 | 192.168.x.x ネットワーク上の宛先にトラフィックをルーティングするインターフェイスを指定します。

1. VPN ピア A で、仮想ルーターを選択します。
2. **[**スタティック ルート**]** を選択し、192.168.x.x ネットワークを**[**宛先**]** とするトラフィックをルーティングするために **[**インターフェイス**]** として tunnel.41 を **[**追加**]** します。

©2024 Palo Alto Networks, Inc.

STEP 6 | 仮想ルーターでスタティック ルートと OSPF 設定をセットアップし、OSPF エリアをファイアウォール上の適切なインターフェイスに関連付けます。

1. VPN ピア B で **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)** の順に選択し、デフォルトのルーターを選択するか新しいルーターを追加します。
2. **Static Routes**（静的ルート） を選択し、172.168.x.x. ネットワークでトラフィックのネクスト ホップとしてトンネル IP アドレスを **Add**（追加） します。

   目的のルート メトリックを割り当てます。低い値を使用すると、テーブルの転送におけるルート選択で優先順位が高くなります。
3. **OSPF**（IPv4 の場合）または **OSPFv3** （IPv6 の場合）を選択し、**Enable**（有効）をオンにします。
4. この例では、VPN ピア B の OSPF 設定は以下のようになります。
   - ルーターID：192.168.100.140
   - エリア ID：インターフェイス Ethernet 1/12およびリンク タイプに0.0.0.0 が割り当てられているブロードキャスト
   - エリア ID：インターフェイス Ethernet1/1およびリンク タイプに0.0.0.10 が割り当てられているブロードキャスト
   - エリア ID：インターフェイス Ethernet1/15およびリンク タイプに0.0.0.20 が割り当てられているブロードキャスト

©2024 Palo Alto Networks, Inc.

STEP 7 | スタティック ルートを OSPF Autonomous System に注入するための再配信プロファイルを作成します。

1. VPN ピア B で再配信プロファイルを作成します。
   1. **Network (**ネットワーク**)** > **Virtual Routers (**仮想ルーター**)** の順に選択し、上で使用したルーターを選択します。
   2. **Redistribution Profiles**（再配信プロファイル）を選択し、**Add**（追加）をクリックします。
   3. [名前] フィールドにプロファイル名を入力し、**[**再配信あり**]** を選択して **[**優先順位**]** の値を割り当てます。複数のプロファイルを設定している場合、優先順位の最も低い値を持つプロファイルが最初に一致されます。
   4. **Source Type (**送信元タイプ**)** を **static**（静的） に設定し、**OK** をクリックします。ステップ 6 で定義した静的ルートが再配信に使用されます。
2. スタティック ルートを OSPF システムに挿入します。
   1. **OSPF** > **Export Rules (**ルールのエクスポート**)**（IPv4 の場合）または **OSPFv3** > **Export Rules (**ルールのエクスポート**)**（IPv6 の場合）の順に選択します。
   2. **[**追加**]**をクリックし、作成した再配布プロファイルを選択します。
   3. 外部ルートを OSPF システムに誘導する方法を選択します。デフォルト オプションである **Ext2** は、外部メトリックのみを使用したルートの総コストを計算します。内部と外部の両方の OSPF メトリックを使用するには、**Ext1** を使用します。
   4. OSPF システムに注入されるルートについて、**Metric**（メトリック） コスト値）を割り当てます。このオプションを使用すると、注入されたルートが OSPF システムに到達したときにそのメトリックを変更できます。
   5. **OK** をクリックします。

©2024 Palo Alto Networks, Inc.

STEP 8 | IPSec トンネルをセットアップします。

1. **Network (**ネットワーク**)** > **IPSec Tunnels (IPSec** トンネル**)**の順に選択します。
2. **Add**（追加） をクリックして、**General**（全般） タブでオプションを設定します。

   この例では、VPN ピア A の設定は以下のようになります。

   - トンネル インターフェイス — tunnel.41
   - タイプ — 自動キー
   - **IKE** ゲートウェイ — 上で定義した IKE ゲートウェイを選択します。
   - **IPSec** 暗号プロファイル — 上で定義した IKE ゲートウエィを選択します。

   VPN ピア B の設定は以下のようになります。

   - **Tunnel Interface(**トンネル インターフェイス**)**—tunnel.40
   - タイプ — 自動キー
   - **IKE** ゲートウェイ — 上で定義した IKE ゲートウェイを選択します。
   - **IPSec** 暗号プロファイル — 上で定義した IKE ゲートウエィを選択します。
3. **Show Advanced Options** [詳細オプションの表示]をオンにし、**Tunnel Monitor** [トンネル モニター]をオンにして、接続を確認するために ping を送信する宛先 IP アドレスを指定します。
4. 接続の確立に失敗した場合のアクションを定義する方法については、トンネル モニタリング プロファイルの定義を参照してください。

STEP 9 | トラフィックをサイト（サブネット）間で許可するためのポリシー ルールを作成します。

1. **Policies** > **Security**を選択します。
2. 指定した送信元および宛先 IP アドレスから発信されるトラフィックについて、トラフィックを Uuntrust ゾーンと vpn-tun ゾーン間および vpn-tun ゾーンと Untrust ゾーン間で許可するためのルールを作成します。

©2024 Palo Alto Networks, Inc.

STEP 10 | OSPF 隣接および CLI からのルートを確認します。

両方のファイアウォールが互いにネイバーとして完全な状態で表示できることを確認します。また、VPN ピアのトンネル インターフェイスの IP アドレスおよび OSPF ルーター ID も確認します。各 VPN ピアで以下の CLI コマンドを使用します。

- **show routing protocol ospf neighbor**

```
admin@FW-A> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.140
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.140
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no

admin@FW-B> show routing protocol ospf neighbor

  Options: 0x80:reserved, O:Opaq-LSA capability, DC:demand circuits, EA:Ext-Attr LSA capability,
           N/P:NSSA option, MC:multicase, E:AS external LSA capability, T:TOS capability
  ==========
  virtual router:               vr1
  neighbor address:             2.1.1.141
  local address binding:        0.0.0.0
  type:                         dynamic
  status:                       full
  neighbor router ID:           192.168.100.141
  area id:                      0.0.0.0
  neighbor priority:            1
  lifetime remain:              39
  messages pending:             0
  LSA request pending:          0
  options:                      0x42: O E
  hello suppressed:             no
```

- **show routing route**

以下は、各 VPN ピアの出力例です。

```
VPN PeerA

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          2.1.1.141       20      A S             tunnel.41
192.168.2.0/24          2.1.1.141       20      A S             tunnel.41
172.16.101.0/24         0.0.0.0         1       A H             ethernet1/1
2.1.1.140/24            2.1.1.141       20      A S             tunnel.41

VPN PeerB

destination             next hop        metric  flags   age     interface       next-AS
192.168.1.0/24          0.0.0.0         10      A Oo            ethernet1/1
192.168.2.0/24          0.0.0.0         10      A Oo            ethernet1/15
172.16.101.0/24         2.1.1.140       20      A H             tunnel.40
2.1.1.141/24            2.1.1.140       10      A C             tunnel.40
```

STEP 11 | 「VPN 接続のテスト」を行います。

トンネル モニタリングのセットアップおよびトンネルの状態の表示を参照してください。

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

トラブルシューティング

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

この章では、VPN 接続のテストと、VPN エラー メッセージが発生した場合の解釈に関するタスクについて説明します。CLI コマンドを使用して、サイト間 VPN 接続を監視およびトラブルシューティングします。

- IPSec VPN トンネル接続のトラブルシューティング
- CLI を使用したサイト間 IPSec VPN トンネル問題のトラブルシューティング

IPSec VPN トンネル接続のトラブルシューティング

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

IPSec VPN 接続のパフォーマンスを最大限に引き出すためのテストとトラブルシューティング:

- VPN 接続のテスト
- VPN エラー メッセージの解釈

VPN 接続のテスト

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンス不要

VPN 接続をテストするには、このタスクを実行します。

STEP 1 | トンネルを経由してホストに ping 送信するか、以下の CLI コマンドを使用して IKE フェーズ 1 を開始します。

```
test vpn ike-sa gateway <gateway_name>
```

STEP 2 | 以下のコマンドを入力して IKE フェーズ 1 がセットアップされているかどうかをテストします。

```
show vpn ike-sa gateway <gateway_name>
```

出力で、セキュリティ アソシエーションが表示されるかどうかを確認します。表示されていない場合、システム ログ メッセージを確認して失敗の理由を見直します。

STEP 3 | トンネルを経由してホストに ping 送信するか、以下の CLI コマンドを使用して IKE フェーズ 2 を開始します。

```
test vpn ipsec-sa tunnel <tunnel_name>
```


©2024 Palo Alto Networks, Inc.

STEP 4 | 以下のコマンドを入力して IKE フェーズ 2 がセットアップされているかどうかをテストします。

```
show vpn ipsec-sa tunnel <tunnel_name>
```

出力で、セキュリティ アソシエーションが表示されるかどうかを確認します。表示されていない場合、システム ログ メッセージを確認して失敗の理由を見直します。

STEP 5 | VPN トラフィック フロー情報を表示するには、以下のコマンドを使用します。

```
show vpn flow total tunnels configured:             1 filter - type
 IPSec, state any total IPSec tunnel configured:       1 total
 IPSec tunnel shown:                 1 name                    id
      state      local-ip       peer-ip       tunnel-i/f
 ------------------------------------------------------------------------------
 vpn-to-siteB       5       active
    100.1.1.1     200.1.1.1     tunnel.41
```

VPN エラー メッセージの解釈

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

以下の表に、システム ログに記録される一般的な VPN エラー メッセージの一部を示します。

表 **2 : VPN** に問題がある場合の **Syslog** エラー メッセージ

エラーが次の場合:	対処法
IKE フェーズ 1 ネゴシエーションは、イニシエーター、メイン・モードとして失敗します。失敗した SA: x.x.x.x[500]-y.y.y.y[500] cookie:84222f276c2fa2e9:0000000000000000 タイムアウトのため。 もしくは IKE フェーズ 1 ネゴシエーションが失敗しました。ピア IP x.x.x.x に対する IKE フェーズ 1 要求の構成が見つかりませんでした[1929]	• IKE ゲートウェイ設定で各 VPN ピアのパブリック IP アドレスが正しいことを確認します。 • IP アドレスに ping を送信可能であり、接続の失敗の原因がルーティングの問題ではないことを確認します。
Received unencrypted notify payload (no proposal chosen) from IP x.x.x.x[500] to y.y.y.y[500], ignored...	IKE 暗号プロファイル設定で、両側のプロポーザルに共通の暗号化、認

©2024 Palo Alto Networks, Inc.

エラーが次の場合:	対処法
もしくは IKE フェーズ 1 ネゴシエーションが失敗しました。ピアの SA ペイロードを処理できません。	証、および DH グループ プロポーザルがあることを確認します。
pfs グループが一致しない:my:2ピア:0 もしくは SA ペイロードの処理中に IKE フェーズ 2 ネゴシエーションが失敗しました。ピアの SA ペイロードに適切な提案が見つかりません。	IPSec 暗号プロファイル設定で、以下を確認します。 • PFS が両方の VPN ピアで有効または無効のいずれかであること • 各ピアによって提案される DH グループに少なくとも 1 つ共通の DH グループがあること
Proxy ID の処理中に IKE フェーズ 2 ネゴシエーションが失敗しました。受信したローカル ID x.x.x.x/x タイプ IPv4 アドレス プロトコル 0 ポート 0、リモート ID y.y.y.y/y タイプ IPv4 アドレス プロトコル 0 ポート 0 を受信しました。	一方の VPN ピアがポリシーベースの VPN を使用しています。Palo Alto Networks ファイアウォールでプロキシ ID を構成する必要があります。VPN ピアを識別するためのプロキシ ID の作成を参照してください。
コミットエラー:トンネルインターフェイス tunnel.x の複数バインディング制限(xx)に達しました。	ファイアウォールでサポートされている最大プロキシ ID に達している必要があります。IPSec トンネルを確立する前に、ファイアウォールでサポートされている最大プロキシ ID を確認してください。 VPN ピアのプロキシ ID を構成する前に、ファイアウォールでサポートされている最大プロキシ ID を確認することをお勧めします。ファイアウォールでサポートされている最大プロキシ ID を超える IPSec VPN トンネルを実装するユースケースがある場合は、次の手順に従います。 • 同じフェーズ 1 およびフェーズ 2 構成で別のトンネルを構成します。 • SuperNet プロキシ ID の IP アドレス。例えば、複数

©2024 Palo Alto Networks, Inc.

エラーが次の場合:	対処法
	のエントリを避けるために、10.1.0.0/16、10.2.0.0/16 を使用する代わりに、範囲を 10.0.0.0/8 にスーパーネットします。
プロキシ ID の不一致	プロキシ ID が一致しないと、サイト間の IPSec VPN トンネルの確立に失敗します。したがって、サイト間の IPSec VPN トンネルを正常に確立するには、両方の VPN ピアに同一のプロキシ ID を設定します。 以下に例を示します。サイト間 IPSec トンネル構成では、1 つの VPN ピアがネットマスク /32 の IP アドレスで構成され、リモート VPN ピアが同じ IP アドレスで異なるネットマスク /16 で構成されている場合、 VPN トンネルの確立に失敗します。 他のファイアウォール ベンダーのプロキシ *ID* は、アクセス リストまたはアクセス コントロール リスト *(ACL)* と呼ばれます。 VPN ピア内のプロキシ ID は、互いの正確なミラー (つまり、反対) である必要がありますが、一致する必要はありません。 IPSec VPN トンネルを確立するための VPN ピアのプロキシ ID 設定の例: VPN ファイアウォール 1 がローカル ID として 192.0.2.0/24、ピア ID として 192.0.2.25/24 を使用して構成されている場合。次に、VPN ファイアウォール 2 は、ローカル ID と

©2024 Palo Alto Networks, Inc.

エラーが次の場合:	対処法
	して 192.0.2.25/24、ピア ID として 192.0.2.0/24 を使用して構成する必要があります。

©2024 Palo Alto Networks, Inc.

CLI を使用したサイト間 VPN の問題のトラブルシューティング

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

次の CLI コマンドを使用して、フェーズ 1 およびフェーズ 2 のサイト間 VPN の問題をトラブルシューティングします。

- 表示コマンド
- コマンドをクリア
- テストコマンド
- コマンドのデバッグ

表示コマンド

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

実行したい内容	以下を使用
• すべての VPN トンネルの基本統計を表示します。	`> 実行中のトンネル フロー情報を表示`
• 特定のゲートウェイの IKE SA を表示します。	`>VPN IKE-SA ゲートウェイを表示 <gateway> | マッチ <x.x.x.x/Y>`
• 特定のトンネルの IKE SA を表示します。	`>VPN IKE-SA トンネルを表示 <tunnel>`
• IPSec カウンタを表示する	`>VPN フローを表示`

©2024 Palo Alto Networks, Inc.

実行したい内容	以下を使用
• すべての IPSec ゲートウェイとその構成のリストを表示します。	**>VPN** ゲートウェイを表示
• IKE フェーズ 1 SA を表示する	**>VPN IKE-SA** を表示
• IKE フェーズ 2 SA を表示する	**>VPN IPSec-SA** を表示
• 自動キー IPSec トンネル構成のリストを表示する	**> VPN** トンネルを表示

コマンドをクリア

どこで使用できますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

実行したい内容	以下を使用
• 特定のゲートウェイの IKEv1 IKE SA を削除する	**> VPN IKE-SA** トンネル をクリアする ***<gateway>***
• 特定のトンネルの IKEv1 IKE SA を削除する	**> VPN IKE-SA** トンネルをクリアする ***<tunnel>***
• 特定のトンネルの IKEv1 IPSec SA を削除します	**> VPN IPsec-SA** トンネルをクリアする ***<tunnel>***

テストコマンド

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

©2024 Palo Alto Networks, Inc.

実行したい内容	以下を使用
• 指定されたゲートウェイとの IKE ネゴシエーションを開始します。	**>VPN IKE-SA** ゲートウェイをテストする ***<gateway>***
• 指定されたトンネルの IPSec ネゴシエーションを開始します。	**>VPN IPSec-SA** トンネルをテストします ***<tunnel>***

コマンドのデバッグ

これはどこで使えますか?	何が必要ですか?
• PAN-OS	ライセンスは必要ありません

実行したい内容	以下を使用
• デバッグをオンにして、詳細なログとステータスを表示します	**> debug ike global on debug less mp-log ikemgr.log debug ike stat**
• メイン、アグレッシブ、クイック モードのネゴシエーションを表示およびキャプチャするための packet capture (パケットキャプチャ - pcap)。	**>view-pcap** で **IKE pcap** をデバッグ **no-dns-lookup** はい **no-port-lookup** はい **debug-pcap ikemgr.pcap**
• デバッグをオフにする	**>IKE pcap** をオフにしてデバッグします

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.