Cisco RVルータVPNの概要とベストプラクティス

目的

このドキュメントの目的は、Cisco RVシリーズルータを初めて使用するすべてのユーザに仮想プライベートネットワーク(VPN)のベストプラクティスの概要を説明することです。

目次

はじめに

昔は働ける場所は会社しかなかったようですね。仕事の問題を解決するために週末にオフィスに向かう必要があったことを覚えているかもしれません。社内のリソースからデータを取得するには、オフィス内に物理的に配置する必要がありました。その日々は終わった。今日の時代では、外出先で、自宅、別のオフィス、コーヒーショップ、または別の国からビジネスを行うことができます。欠点は、ハッカーが常に機密データを取得しようとしていることです。公共のインターネットを使用するだけでは安全ではありません。柔軟性とセキュリティを確保するには、どうすればよいか？VPNをセットアップします。

VPN接続を使用すると、ユーザは、インターネットなどのパブリックまたは共有ネットワークを経由してプライベートネットワークとの間でデータにアクセスし、データを送受信できます。ただし、プライベートネットワークとそのリソースを保護するために、基盤となるネットワークインフラストラクチャへの安全な接続を確保できます。

VPNトンネルは、暗号化を使用してデータをエンコードし、認証を使用してクライアントのIDを保証することで、データを安全に送信できるプライベートネットワークを確立します。従業員がオフィスの外にいてもプライベートネットワークにアクセスできるようにするのは便利で必要であるため、企業オフィスではVPN接続がよく使用されます。

通常、サイト間VPNはネットワーク全体を相互に接続します。ネットワークを拡張し、ある場所のコンピュータリソースを別の場所で使用できるようにします。VPN対応ルータを使用することで、企業はインターネットなどのパブリックネットワークを介して複数の固定サイトを接続できます。

VPN用にクライアントとサイト間を設定すると、リモートホストまたはクライアントが同じローカルネットワーク上に配置されているかのように動作できます。ルータがインターネット接続用に設定された後で、ルータとエンドポイントの間にVPN接続を設定できます。VPNクライアントは、接続を確立するための一致した設定の要件に加えて、VPNルータの設定に依存します。また、一部のVPNクライアントアプリケーションはプラットフォーム固有であり、オペレーティングシステム(OS)のバージョンにも依存します。設定は完全に同じである必要があり、そうでないと通信できません。

VPNは、次のいずれかを使用して設定できます。

- Secure Socket Layer (SSL)
- IPSec（Internet Protocol Security）
- Point to Point Tunneling Protocol(PPTP):SSLやIPSecほど安全ではない
- 総称ルーティング カプセル化（GRE）
- Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）

これまでにVPNを設定したことがない場合は、この記事を通じて多くの新しい情報を受け取ります。これは手順ごとのガイドではなく、参考のための概要です。したがって、ネットワーク上にVPNをセットアップする前に、この記事を一通り読んでおくと便利です。この記事では、特定の手順に関するリンクを紹介しています。

TheGreenBow、OpenVPN、Shrew Soft、EZ VPNなどのシスコ以外のサードパーティ製品はシスコでサポートされていません。これらはガイダンスの目的でのみ含まれています。上記のサポートが必要な場合は、サードパーティに連絡してサポートを受けてください。

VPN接続を使用する利点

- VPN接続を使用すると、機密のネットワークデータとリソースを保護するのに役立ちます。
- リモートワーカーや企業の従業員は、物理的な場所にいなくても本社のリソースに簡単にアクセスでき、プライベートネットワークとそのリソースのセキュリティを維持できるので、利便性とアクセス性が向上します。
- VPN接続を使用した通信は、他のリモート通信方法に比べて高いレベルのセキュリティを提供します。高度な暗号化アルゴリズムによってこれを可能にし、プライベートネットワーク

を不正アクセスから保護します。
- ユーザの実際の地理的な場所は保護されており、インターネットなどのパブリックネットワークや共有ネットワークには公開されません。
- VPNを使用すると、コンポーネントを追加したり複雑な設定を行ったりすることなく、新しいユーザまたはユーザグループを追加できます。

VPN接続を使用する際のリスク

- 設定ミスによるセキュリティリスクが存在する可能性があります。VPNの設計と実装は複雑になる可能性があるため、プライベートネットワークのセキュリティが侵害されないようにするために、接続の設定のタスクを知識と経験のある専門家に委託する必要があります。
- 信頼性が低くなる可能性があります。VPN接続にはインターネット接続が必要なため、実績のあるテスト済みのレピュテーションを持つプロバイダーを利用して、優れたインターネットサービスを提供し、ダウンタイムを最小限に抑えることが重要です。
- 新しいインフラストラクチャや新しい構成セットを追加する必要が生じた場合、互換性がないために技術的な問題が発生する可能性があります。特に、使用中の製品やベンダーとは異なる製品やベンダーが関係している場合には、この問題が発生する可能性があります。
- 接続速度が遅くなる可能性があります。無料のVPNサービスを提供するISP接続を使用している場合は、これらのプロバイダーが接続速度を優先しないため、接続が遅くなることが予想されます。VPNのスループットは、ルータのハードウェア機能によって異なることに注意してください。

VPNの動作の詳細については、ここをクリックしてください。

VPNの設定時に使用するヒント

1. 異なるサイト間でVPNを設定しながら、両端で異なるLAN IPサブネットを使用します。たとえば、接続先のサイトで192.168.x.xのアドレス計画を使用する場合は、10.x.x.xまたは172.16.x.x - 172.31.x.xのサブネットを使用します。別のオプションとして、異なるサブネットマスクを設定することもできます。ルータのIPアドレスを変更すると、Dynamic Host Configuration Protocol(DHCP)上のデバイスはそのサブネットのIPアドレスを自動的に取得します。
2. 安定したVPN接続のためにルータのWANインターフェイスでスタティックパブリックIPを使用します。
3. 選択した暗号化および認証レベルが、VPNのVPNトンネルを確立するルータと同じであることを確認します。
4. 入力したPSKとKey Lifetimeがリモートルータと同じであることを確認します。PSKは、クライアントが自分のコンピュータ上でクライアントとして設定するときに、サイトとクライアントで一致する必要があります。デバイスによっては、使用できない禁止された記号がある場合があります。Key Lifetimeは、システムが鍵を変更する頻度です。証明書はより安全であると考えられるため、推奨されます。
5. ほとんどのVPNでは、クライアントはVPNを使用するために証明書を必要としません。これは単にルータを介した検証のためです。たとえば、OpenVPNにはクライアント証明書とサイト証明書の両方が必要です。
6. SAライフタイムをフェーズIIのSAライフタイムよりも長くフェーズIに設定します。フェー

ズIをフェーズIIより短くすると、データトンネルとは対照的に、トンネルを頻繁に再ネゴシエートする必要があります。データトンネルにはより多くのセキュリティが必要なため、フェーズIよりもフェーズIIのライフタイムを短くすることをお勧めします。
7. すべてのパスワードをより複雑なものに変更します。

VPNのタイプ

セキュアソケットレイヤ(SSL)

Cisco RV34xシリーズルータは、AnyConnectを使用したSSL VPNをサポートしています。RV160およびRV260には、別のSSL VPNであるOpenVPNを使用するオプションがあります。SSL VPNサーバを使用すると、リモートユーザはWebブラウザを使用してセキュアなVPNトンネルを確立できます。この機能により、ネイティブのHypertext Transfer Protocol(HTTP)over SSL Hypertext Transfer Protocol Secure(HTTPS)ブラウザサポートを使用して、さまざまなWebリソースやWeb対応アプリケーションに簡単にアクセスできます。

SSL VPNを使用すると、ネットワークトラフィックを暗号化することにより、セキュアで認証済みのパスを使用して、制限されたネットワークにリモートからアクセスできます。

SSLでアクセスを設定するには、次の2つのオプションがあります。

1. 自己署名証明書：自身の作成者によって署名された証明書。これは推奨されず、テスト環境でのみ使用してください。
2. CA署名付き証明書：これはより安全であり、強く推奨されます。サードパーティは有償でネットワークが正当なものであることを検証し、CA証明書を作成してサイトに添付します。CA証明書の詳細については、この記事の「証明書」セクションを参照してください。

このドキュメントには、AnyConnectに関する記事へのリンクがあります。AnyConnectの概要については、ここをクリックしてください。

IPsec プロファイル

Easy VPN(EZVPN)、TheGreenBow、およびShrew Softは、インターネットプロトコルセキュリティ(IPSec)VPNです。IPSec VPNは、2つのピア間またはクライアントとサイト間の安全なトンネルを提供します。センシティブと見なされるパケットは、これらの安全なトンネルを通じて送信される必要があります。これらの機密パケットを保護するために、ハッシュアルゴリズム、暗号化アルゴリズム、キーの有効期間、モードなどのパラメータを使用する必要があります。これらのパラメータは、これらのトンネルの特性を指定して定義する必要があります。次に、IPSecピアはこのような機密パケットを検出すると、適切なセキュアトンネルをセットアップし、このトンネル経由でリモートピアにパケットを送信します。

IPSecをファイアウォールまたはルータに実装すると、境界を通過するすべてのトラフィックに適用できる強力なセキュリティが提供されます。企業またはワークグループ内のトラフィックは、セキュリティ関連の処理のオーバーヘッドを受けません。

VPNトンネルの両端が正常に暗号化されて確立されるためには、両方とも暗号化、復号化、およ

び認証の方法について合意する必要があります。IPSecプロファイルはIPSecの中心設定で、自動モードおよび手動キーイングモードでのフェーズIおよびIIネゴシエーションに対して、暗号化、認証、およびDiffie-Hellman(DH)グループなどのアルゴリズムを定義します。

IPSecの重要なコンポーネントには、インターネットキーエクスチェンジ(IKE)フェーズ1とフェーズ2があります。

IKEフェーズ1の基本的な目的は、IPSecピアを認証し、ピア間にセキュアなチャネルを設定してIKE交換を有効にすることです。IKEフェーズ1は次の機能を実行します。

- IPSecピアのIDの認証と保護
- ピア間で一致するIKEセキュリティアソシエーション(SA)ポリシーをネゴシエートして、IKE交換を保護します
- 一致する共有秘密キーを持つ最終結果を使用して、認証されたDiffie-Hellman交換を実行します
- IKEフェーズ2パラメータをネゴシエートするためのセキュアトンネルを設定します
- メインモードとアグレッシブモードの2つのモードで発生する

IKEフェーズ2の目的は、IPSec SAをネゴシエートしてIPSecトンネルを設定することです。IKEフェーズ2は、次の機能を実行します。

- 既存のIKE SAによって保護されているIPSec SAパラメータをネゴシエートします。
- IPSecセキュリティアソシエーションを確立します。
- セキュリティを確保するためにIPSec SAを定期的に再ネゴシエートする
- オプションで、追加のDiffie-Hellman交換を実行します。
- 使用するモードは1つのみ、クイックモード

IPSecポリシーでPerfect Forward Secrecy (PFS)が指定されている場合は、各クイックモードで新しいDH交換が実行され、エントロピー（鍵材料の寿命）が高く、暗号攻撃に対する耐性が高い鍵材料が提供されます。各DH交換は大きな累乗を必要とするため、CPU使用率が増加し、パフォーマンスコストが増大します。

- RV34xシリーズルータでのインターネットプロトコルセキュリティ(IPSec)プロファイルの設定
- RV160およびRV260でのIPSecプロファイル（自動キーイングモード）の設定
- RV160およびRV260ルータでのIPsecプロファイルの手動キーイングモードの設定

Point-to-Point Tunneling Protocol（PPTP）

PPTPは、パブリックネットワーク間にVPNトンネルを作成するために使用されるネットワークプロトコルです。PPTPサーバは、Virtual Private Dialup Network(VPDN)サーバとも呼ばれます。PPTPは他のプロトコルよりも高速で、モバイルデバイスで動作できるため、他のプロトコルよりも使用されることがあります。ただし、他のタイプのVPNほど安全ではないことに注意してください。PPTPタイプのアカウントで接続する方法は複数あります。リンクをクリックして、詳細を確認してください。

- Rv34xシリーズルータでのPoint-to-Point Tunneling Protocol(PPTP)サーバの設定

- WindowsでのRV320およびRV325 VPNルータシリーズでのポイントツーポイントトンネリングプロトコル(PPTP)サーバの設定

総称ルーティング カプセル化

Generic Routing Encapsulation(GRE)は、カプセル化によって1つのプロトコルのパケットを別のプロトコルのパケットに転送するためのシンプルで一般的なアプローチを提供するトンネリングプロトコルです。

GREはペイロード、つまり、外部IPパケット内の宛先ネットワークに配信する必要がある内部パケットをカプセル化します。GREトンネルは、トンネルの送信元アドレスと宛先アドレスによって識別される2つのエンドポイントを持つ仮想ポイントツーポイントリンクとして動作します。

トンネルエンドポイントは、カプセル化されたパケットを中間のIPネットワークを介してルーティングすることで、ペイロードをGREトンネル経由で送信します。途中にある他のIPルータは、ペイロード（内部パケット）を解析しません。外部IPパケットを解析するのは、GREトンネルエンドポイントに転送するときだけです。トンネルのエンドポイントに到達すると、GREカプセル化が削除され、ペイロードはパケットの最終的な宛先に転送されます。

ネットワーク内のデータグラムのカプセル化は、複数の理由で行われます。たとえば、送信元サーバが、パケットが宛先ホストに到達するために通るルートに影響を与える必要がある場合などです。送信元サーバは、カプセル化サーバとも呼ばれます。

IP-in-IPカプセル化では、既存のIPヘッダーに外部IPヘッダーを挿入します。外部IPヘッダーの送信元アドレスと宛先アドレスは、IP-in-IPトンネルのエンドポイントを指しています。パケットを転送しているルータのループバックアドレスをネットワーク管理者が把握している場合は、IPヘッダーのスタックを使用して、パケットはあらかじめ決められたパスを経由して宛先に送信されます。

このトンネリングメカニズムは、ほとんどのネットワークアーキテクチャのアベイラビリティと遅延の決定に使用できます。送信元から宛先までのパス全体をヘッダーに含める必要はありませんが、パケットを転送するためにネットワークのセグメントを選択できることに注意してください。

レイヤ 2 トンネリング プロトコル

L2TPは、トンネリングするトラフィックに暗号化メカニズムを提供しません。代わりに、IPSecなどの他のセキュリティプロトコルに依存してデータを暗号化します。

L2TPトンネルは、L2TP Access Concentrator(LAC)とL2TP Network Server(LNS)の間に確立されます。IPSec トンネルもこれらのデバイス間で確立され、すべての L2TP トンネルのトラフィックは IPSec を使用して暗号化されます。

L2TPの主な用語は次のとおりです。

- CHAP:Challenge Handshake Authentication Protocol（チャレンジハンドシェイク認証プロトコル）。ポイントツーポイント認証プロトコル(PPP)。

- L2TPアクセスコンセントレータ(LAC):LACは、公衆電話交換網(PSTN)に接続されたCiscoネットワークアクセスサーバです。LACは、L2TP上で動作するメディアを実装するだけで済みます。LACは、ローカルエリアネットワークまたはパブリックフレームリレーやプライベートフレームリレーなどのワイドエリアネットワークを使用してLNSに接続できます。LACは着信コールの発信側および発信コールの受信側です。
- L2TPネットワークサーバ(LNS):ローカルエリアネットワークまたはワイドエリアネットワーク（パブリックまたはプライベートフレームリレーなど）に接続されているほぼすべてのCiscoルータは、LNSとして機能できます。これはL2TPプロトコルのサーバ側であり、PPPセッションを終了するすべてのプラットフォームで動作する必要があります。LNSは発信コールの発信側および着信コールの受信側です。図1は、LACとLNS間のコールルーチンを示しています。
- バーチャルプライベートダイヤルネットワーク(VPDN):サービスを提供するためにPPPを使用するアクセスVPNのタイプ。

L2TPの詳細については、次のリンクをクリックしてください。

- RV34xルータでのL2TP WANの設定
- Wide-Area Networking Configuration Guide：レイヤ2サービス、Cisco IOS XEリリース3S

Cisco RVシリーズVPNルータと互換性のあるVPN

	RV34X	RV32X	RV160X/RV260X
IPSec(IKEv1)			
シュラウソフト	Yes	Yes	Yes
グリーンボウ	Yes	Yes	Yes
Mac組み込みクライアント	Yes	Yes	いいえ
iPhone/iPad	Yes	Yes	いいえ
Android	Yes	Yes	Yes
L2TP/IPSec	あり(PAP)	いいえ	いいえ
PPTP	あり(PAP)	可能*	あり(PAP)
その他			
AnyConnect	Yes	いいえ	いいえ
Openvpnの場合	いいえ	Yes	Yes
IKEv2			
Windows	可能*	いいえ	可能*
Mac	Yes	いいえ	Yes
iPhone	Yes	いいえ	Yes
Android	Yes	いいえ	Yes

VPNテクノロジ	サポートされて	サポートされるク	詳細と警告

ー	いるデバイス	ライアント*	
IPSec(IKEv1)	RV34X、RV32X、RV160X/RV260X	ネイティブ：Mac、iPhone、iPad、Android その他：EasyVPN(Cisco VPN Client)、ShrewSoft、Greenbow	セットアップ、トラブルシューティング、サポートが最も簡単です。すべてのルータで使用でき、設定が簡単で（ほとんどの場合）、トラブルシューティングに最適なロギングを備えています。最も多くのデバイスが含まれます。このため、ShrewSoft（無料で動作する）とGreenbow（無料ではなく動作する）をお勧めします。 Windowsの場合、Windowsには純粋なIPSecネイティブVPNクライアントがないため、オプションとしてShrewSoftクライアントとGreenbowクライアントがあります。ShrewSoftとGreenbowにとっては、もう少し複雑ですが、難しくありません。最初のセットアップ後に、クライアントプロファイルをエクスポートし、他のクライアントにインポートできます。 RV160X/RV260Xルータの場合、Easy VPNオプションがないため、Mac、iPhone、またはiPadで動作しないサードパーティクライアントオプションを使用する必要があります。ただし、ShrewSoft、Greeenbow、およびAndroidクライアントを接続するように設定できます。Mac、iPhone、およびiPadクライアントには、IKEv2（以下を参照）を推奨します。
AnyConnect	RV34X	Windows、Mac、iPhone、iPad、Android	お客様の中には、完全なシスコソリューションを求めているお客様もいます。設定は簡単で、ログも記録されますが、ログを理解するのは困難な場合があります。クライアントのライセンス要件を満たすコストが必要です。これはシスコの包括的なソリューションであり、更新されています。トラブルシューティングはIPSecほど簡単ではありませんが、他のVPNオプションよりも優れています。
L2TP/IPSec	RV34X	ネイティブ	これは、Windowsに組み込みのVPNクライ

		：Windows	アントを使用する必要があるお客様に推奨するものです。これに関する2つの注意点は次のとおりです。 1.ローカル認証を使用する場合のみ、PAP認証をサポートします。各クライアントにアクセスして、オプションまたは暗号化なしを選択し、MS-CHAPオプションを無効にして、PAPを有効にする必要があります。これは、ユーザ名/パスワードがクリアテキストで送信されることを意味します。すべてがIPSecで暗号化され、各クライアントで設定する必要があるため、大したことではありません。Windowsでは、これは設定可能ですが、Mac、iPhone、iPad、Androidデバイスでは設定できません。そのため、Windowsクライアントは、RadiusやLDAPなどの外部認証サーバを持たない限り、Windowsクライアントでのみ使用できます。 2.ルータがNATデバイスの背後にある場合、Windowsマシンでは接続が失敗します。回避策は、クライアントとルータの両方でNATを許可するために、各クライアントでレジストリキーを作成することです。
IPSec(IKEv2)	RV34X、RV160X/RV260X	ネイティブ：Windows、Mac、iPhone、iPad、Android	IKEv2用のWindowsネイティブクライアントでは、証明書認証が必要です。ルータとすべてのクライアントの両方が同じCA（または別の信頼できるCA）からの証明書を持つ必要があるため、証明書認証にはPKIインフラストラクチャが必要です。 IKEv2を使用する場合は、Mac、iPhone、iPad、およびAndroidデバイス用に設定し、通常はWindowsマシン（ShrewSoft、Greenbow、またはL2TP/IPSec）用にIKEv1を設定します。
オープンVPN	RV32X、RV160X/RV260X	クライアントはオープンVPN	セットアップが難しく、トラブルシューティングやサポートも難しい。RV160X/RV260XおよびRV320でサポートされます。セットアップはIPSecやAnyConnectよりも複雑で、特に証明書を使

用する場合は複雑です。証明書の多くは証明書を使用します。ルータには有用なログがなく、クライアントログに依存しているため、トラブルシューティングはより困難です。また、OpenVPNクライアントのバージョンの更新により、警告なしで、受け入れた証明書が変更されています。また、これはChromebookでは動作せず、IPSecソリューションを使用する必要があることがわかりました。

*可能な限り多くの組み合わせをテストします。特定のハードウェアとソフトウェアの組み合わせがある場合は、こちらにご連絡ください。それ以外の場合は、関連する『デバイス別コンフィギュレーションガイド、テスト済みの最新バージョン』を参照してください。

証明書

Webサイトにアクセスして、安全ではないという警告を受けたことはありますか。プライベート情報が安全であるという確信は持てず、安全ではありません。サイトがセキュリティで保護されている場合は、サイト名の前に閉じたロックアイコンが表示されます。これは、サイトが安全であることが確認されたことを示す記号です。このロックアイコンが閉じていることを確認します。同じことがVPNにも当てはまります。

VPNを設定する際には、認証局(CA)から証明書を取得する必要があります。証明書はサードパーティサイトから購入され、認証に使用されます。それはあなたのサイトが安全であることを証明するための公式の方法です。基本的に、CAは、ユーザが正当な企業であり、信頼できることを検証する信頼できる送信元です。VPNの場合、最小のコストで低レベルの証明書のみが必要です。CAによってチェックアウトされ、CAが情報を確認すると、証明書が発行されます。この証明書は、コンピュータ上にファイルとしてダウンロードできます。その後、ルータ（またはVPNサーバ）に移動し、そこでアップロードできます。

CAは、デジタル証明書の発行時に公開キーインフラストラクチャ(PKI)を使用します。デジタル証明書は、セキュリティを確保するために公開キーまたは秘密キーの暗号化を使用します。CAは、証明書要求の管理とデジタル証明書の発行を担当します。一部のサードパーティCAには、Identrust、Comodo、GoDaddy、GlobalSign、GeoTrust、およびVerisignが含まれます。

VPN内のすべてのゲートウェイが同じアルゴリズムを使用することが重要です。アルゴリズムを使用しないと、通信できません。シンプルにするために、すべての証明書を同じ信頼できるサードパーティから購入することをお勧めします。これにより、複数の証明書を手動で更新する必要があるため、管理が容易になります。

注：通常、クライアントはVPNを使用するために証明書を必要としません。これは単にルータを介した検証のためのものです。ただし、OpenVPNの場合は例外で、クライアント証明書が必要です。

一部の小規模企業では、簡単にするために、証明書の代わりにパスワードまたは事前共有キーを使用することを選択します。これは安全性が低くなりますが、無料で設定できます。

証明書の詳細については、次のリンクを参照してください。

- RV160およびRV260シリーズルータの証明書(Import/Export/Generate CSR)
- RV34xシリーズルータでデフォルトの自己署名証明書をサードパーティのSSL証明書で置き換える

ルータ上のサイト間VPN

ローカルルータとリモートルータでは、VPN接続に使用される事前共有キー(PSK)、パスワード、証明書、およびセキュリティ設定がすべて一致していることを確認することが重要です。1つ以上のルータでネットワークアドレス変換(NAT)が使用されている場合は（ほとんどのCisco RVシリーズルータで使用）、ローカルルータとリモートルータのVPN接続に対してファイアウォール除外を実行する必要があります。

詳細については、次のサイト間記事を参照してください。

- RV34xでのサイト間VPNの設定
- RV340またはRV345ルータでのサイト間VPNの設定
- Cisco Tech Talk:RV340シリーズルータでのサイト間VPNの設定（ビデオ）
- RV160およびRV260ルータでのサイト間VPNの設定（基本設定）
- RV160およびRV260ルータでのサイト間VPN（詳細設定およびフェールオーバー）

ルータ上のクライアントとサイト間VPN

クライアント側でVPNを設定する前に、ルータ上でVPNを設定する必要があります。

クリックすると、次のルータ設定の記事が表示されます。

- RV160およびRV260ルータでのVPNセットアップウィザードの設定
- RV160およびRV260でのShrew Soft VPN Clientの設定
- Cisco Tech Talk:RV160およびRV260でのShrew Soft VPNの設定（ビデオ）
- RV160およびRV260ルータに接続するためのGreenBow IPsec VPNクライアントのセットアップと使用

クライアントとサイト間のプロファイルの作成

クライアントとサイト間VPN接続では、インターネットからのクライアントはサーバに接続して、サーバの背後にある企業ネットワークまたはLANにアクセスできますが、ネットワークとそのリソースのセキュリティは維持されます。この機能は、新しいVPNトンネルを作成し、テレワーカーや出張者がプライバシーやセキュリティを損なうことなくVPNクライアントソフトウェアを使用してネットワークにアクセスできるようにするため、非常に便利です。次の文書は、RV34xシリーズルータに固有のものです。

- RV34xシリーズルータでのクライアントとサイト間のバーチャルプライベートネットワーク(VPN)接続の設定
- RV34x シリーズ ルータでの AnyConnect バーチャル プライベート ネットワーク（ VPN ）接続の設定

送信元 All Trafficと宛先 All Trafficにポート転送が設定されている場合、クライアントからサイトへのVPNは機能しません。

ユーザグループ

ユーザグループは、同じサービスセットを共有するユーザの集合に対してルータ上に作成されます。これらのユーザグループには、VPNへのアクセス方法に関する権限のリストなど、グループのオプションが含まれます。デバイスに応じて、PPTP、サイト間IPSec VPN、およびクライアント間IPSec VPNを許可できます。たとえば、RV260にはOpenVPNを含むオプションがありますが、L2TPはサポートされていません。RV340シリーズには、SSL VPN用のAnyConnectと、キャプティブポータルまたはEZ VPNが搭載されています。

これらの設定により、管理者は権限のあるユーザだけがネットワークにアクセスできるように制御およびフィルタリングできます。Shrew SoftとTheGreenBowは、ダウンロード可能な最も一般的なVPN Clientの2つです。ルータのVPN設定に基づいて設定しないと、VPNトンネルを正常に確立できません。次の記事では、特にユーザグループの作成について説明します。

- RV34xルータでのVPNセットアップ用のユーザグループの作成

VPNのユーザグループを設定する際には、必ずadminグループにデフォルトのadminアカウントを残し、VPN用に新しいユーザアカウントとユーザグループを作成してください。管理者アカウントを別のグループに移動すると、自分自身がルータにログインできなくなります。その結果、工場出荷時の状態にリセットしてルータの設定を再度行う必要が生じ、デフォルトのadminアカウントはadminグループに残されます。

ユーザアカウント

ユーザアカウントは、PPTP、VPNクライアント、Web Graphical User Interface（GUI；グラフィカルユーザインターフェイス）ログイン、Secure Sockets Layer Virtual Private Network（SSLVPN；セキュアソケットレイヤ仮想プライベートネットワーク）などのさまざまなサービスに対してローカルデータベースを使用するローカルユーザの認証を可能にするために、ルータ上に作成されます。これにより、管理者はネットワークにアクセスする権限を持つユーザだけを制御およびフィルタリングできます。次の記事では、特にユーザアカウントの作成について説明します。

- RV34xルータでのVPN Clientセットアップ用のユーザアカウントの作成

クライアントの場所でのクライアントとサイト間

クライアントとサイト間VPN接続では、インターネットからのクライアントはサーバに接続して、サーバの背後にある企業ネットワークまたはLANにアクセスできますが、ネットワークとその

リソースのセキュリティは維持されます。この機能は、新しいVPNトンネルを作成し、在宅勤務者や出張者がプライバシーやセキュリティを損なうことなくVPNクライアントソフトウェアを使用してネットワークにアクセスできるようにするため、非常に便利です。VPNは、データの送受信時にデータを暗号化および復号化するように設定されています。

AnyConnectアプリケーションはSSL VPNで動作し、特にRV34xルータで使用されます。他のRVシリーズルータでは使用できません。バージョン1.0.3.15以降では、ルータライセンスは不要になりましたが、VPNのクライアント側でライセンスを購入する必要があります。Cisco AnyConnectセキュアモビリティクライアントの詳細については、ここをクリックしてください。インストールの手順については、次の記事を参照してください。

- Mac コンピュータへの Cisco AnyConnect セキュア モビリティ クライアントのインストール
- Windows コンピュータへの Cisco AnyConnect セキュア モビリティ クライアントのインストール

すべてのRVシリーズルータでクライアントとサイト間のVPNに使用できるサードパーティ製アプリケーションがいくつかあります。前述のとおり、シスコはこれらのアプリケーションをサポートしていません。この情報はガイダンス用に提供されています。

GreenBow VPN Clientは、ホストデバイスがクライアント間IPsecトンネルまたはSSLのセキュアな接続を設定できるようにするサードパーティのVPNクライアントアプリケーションです。これはサポートを含む有料のアプリケーションです。

- RV160およびRV260ルータに接続するためのGreenBow IPsec VPNクライアントのセットアップと使用

OpenVPNは、SSL VPN用に設定して使用できる無料のオープンソースアプリケーションです。クライアント/サーバ接続を使用して、インターネット経由でサーバとリモートクライアントロケーション間のセキュアな通信を提供します。

- RV160およびRV260ルータでのOpenVPN

Shrew Softは、IPsec VPN用にも設定して使用できるフリーのオープンソースアプリケーションです。クライアント/サーバ接続を使用して、インターネット経由でサーバとリモートクライアントロケーション間のセキュアな通信を提供します。

- RV160およびRV260でのShrew Soft VPN Clientの設定

Easy VPNはRV32xルータで一般的に使用されていました。次に、参考になる情報を示します。

- RV320およびRV325 VPNルータシリーズでのEasy Client to Gatewayバーチャルプライベートネットワーク(VPN)の設定
- Cisco Easy VPN に関する Q&A
- Cisco IOSソフトウェアベースのルータでのEasy VPN

セットアップウィザード

最新のCisco RVシリーズルータには、セットアップ手順を示すVPN Setup Wizardが付属しています。VPN Setup Wizardでは、基本的なLAN-to-LANおよびリモートアクセスVPN接続を設定し、認証用に事前共有キーまたはデジタル証明書を割り当てることができます。詳細については、次の記事を参照してください。

- RV160およびRV260でのVPNセットアップウィザードの設定
- RV34xシリーズルータのセットアップウィザードを使用してバーチャルプライベートネットワーク(VPN)接続を設定する

結論

この記事では、VPNをより深く理解するためのヒントを紹介しています。これで、独自の設定を行う準備が整いました。時間をかけてリンクを表示し、Cisco RVシリーズルータにVPNを設定する最適な方法を決定します。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。