Cisco RV320ギガビットデュアルWAN VPNルータとCisco 500シリーズサービス統合型アダプタ間のサイト間VPNトンネルの設定

目的

バーチャルプライベートネットワーク(VPN)は、リモートネットワークをメインのプライベートネットワークに接続するために広く使用されているテクノロジーとして存在し、パブリックライン上で暗号化されたチャネルの形でプライベートリンクをシミュレートします。VPNトラフィックを暗号化する2段階のネゴシエーションにより、VPNエンドポイントのみが復号化を認識できる方法で行われるため、リモートネットワークはセキュリティ上の問題なく、プライベートのメインネットワークの一部として存在するように接続できます。
この短いガイドでは、Cisco 500シリーズサービス統合型アダプタとCisco RVシリーズルータの間にサイト間IPsec VPNトンネルを構築するための設計例を示します。

該当するデバイス

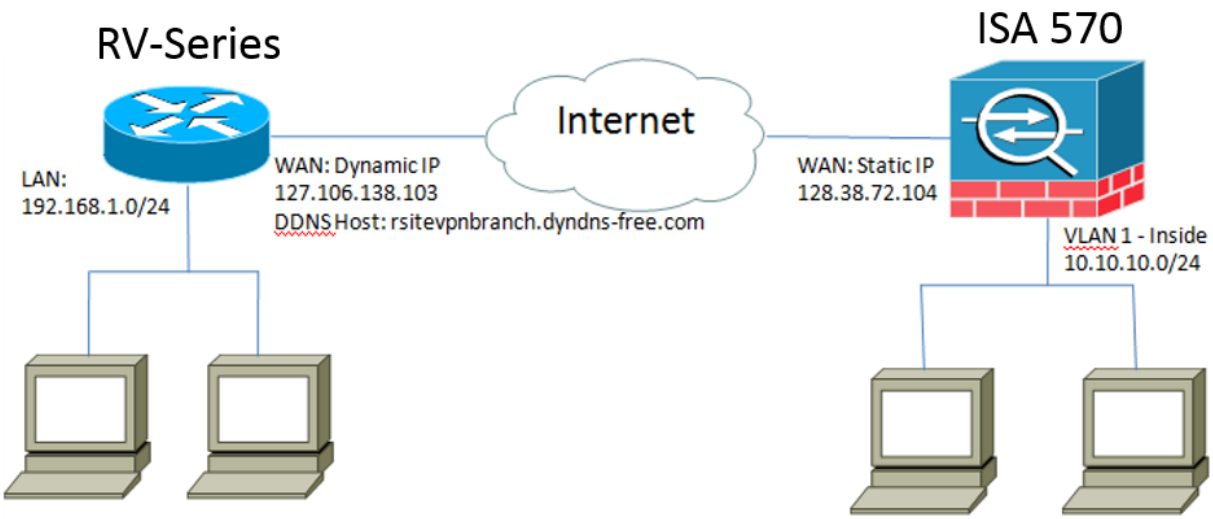
- Cisco RVシリーズルータ(RV320)
- Cisco 500シリーズサービス統合型アダプタ(ISA570)

[Software Version]

- 4.2.2.08 [Cisco RV0xxシリーズVPNルータ]

事前設定

ネットワーク図
次に、サイト間VPNトポロジを示します。



サイト間IPsec VPNトンネルは、リモートオフィスのCisco RVシリーズルータと本社のCisco 500シリーズISAの間で設定および確立されます。
この設定では、リモートオフィスのLAN 192.168.1.0/24のホストと、本社のLAN 10.10.10.0/24のホストが、VPNを介して互いに安全に通信できます。

コアコンセプト

ンターネット キー交換（IKE）

Internet Key Exchange（IKE；インターネットキーエクスチェンジ）は、IPsecプロトコルスイートでセキュリティアソシエーション(SA)をセットアップするために使用されるプロトコルです。IKEは、Oakleyプロトコル、Internet Security Association、およびKey Management Protocol(ISAKMP)に基づいて構築され、Diffie-Hellman(DH)キー交換を使用して共有セッションシークレットを設定し、そこから暗号キーを取得します。

Internet Security Association and Key Management Protocol（ISAKMP）

Internet Security Association and Key Management Protocol(ISAKMP)は、2つのVPNエンドポイント間でVPNトンネルをネゴシエートするために使用されます。認証、通信、およびキー生成の手順を定義し、IKEプロトコルで暗号キーを交換してセキュア接続を確立します。

IPSec（Internet Protocol Security）

IP Security Protocol(IPsec)は、データストリームの各IPパケットを認証および暗号化することによって、IP通信を保護するためのプロトコルスイートです。IPsecには、セッションの開始時にエージェント間で相互認証を確立するためのプロトコルや、セッション中に使用される暗号キーのネゴシエーションも含まれます。 IPsecは、ホスト、ゲートウェイ、またはネットワークのペア間のデータフローを保護するために使用できます。

設計のヒント

VPNトポロジ：ポイントツーポイントVPNトポロジとは、メインサイトとリモートサイト

の間にセキュアなIPsecトンネルが設定されていることを意味します。
企業では、多くの場合、マルチサイトトポロジで複数のリモートサイトを必要とし、ハブアンドスポークVPNトポロジまたはフルメッシュVPNトポロジを実装します。ハブアンドスポークVPNトポロジとは、リモートサイトが他のリモートサイトと通信する必要がなく、各リモートサイトはメインサイトとのセキュアなIPsecトンネルのみを確立することを意味します。フルメッシュVPNトポロジは、リモートサイトが他のリモートサイトと通信する必要があることを意味し、各リモートサイトはメインサイトおよびその他すべてのリモートサイトとのセキュアなIPsecトンネルを確立します。
VPN認証:VPNトンネルの確立時にVPNピアを認証するためにIKEプロトコルが使用されます。さまざまなIKE認証方式が存在し、事前共有キーが最も便利な方式です。シスコでは、強力な事前共有キーの適用を推奨しています。
VPN暗号化:VPN経由で転送されるデータの機密性を確保するために、暗号化アルゴリズムを使用してIPパケットのペイロードを暗号化します。DES、3DES、およびAESは、3つの一般的な暗号化規格です。AESは、DESおよび3DESと比較して最も安全であると考えられています。シスコでは、AES-128ビット以上の暗号化（AES-192やAES-256など）を適用することを強く推奨しています。 ただし、強力な暗号化アルゴリズムでは、ルータからより多くの処理リソースが必要になります。
ダイナミックWAN IPアドレッシングおよびダイナミックドメインネームサービス(DDNS):2つのパブリックIPアドレス間でVPNトンネルを確立する必要があります。WANルータがインターネットサービスプロバイダー(ISP)からスタティックIPアドレスを受信する場合、スタティックなパブリックIPアドレスを使用してVPNトンネルを直接実装できます。しかし、ほとんどの小規模企業は、DSLやケーブルなどのコスト効率の高いブロードバンドインターネットサービスを使用し、ISPからダイナミックIPアドレスを受信しています。このような場合、ダイナミックドメインネームサービス(DDNS)を使用して、ダイナミックIPアドレスを完全修飾ドメイン名(FQDN)にマッピングできます。
LAN IPアドレッシング：各サイトのプライベートLAN IPネットワークアドレスは重複しないようにしてください。各リモートサイトのデフォルトLAN IPネットワークアドレスは、常に変更する必要があります。

設定のヒント

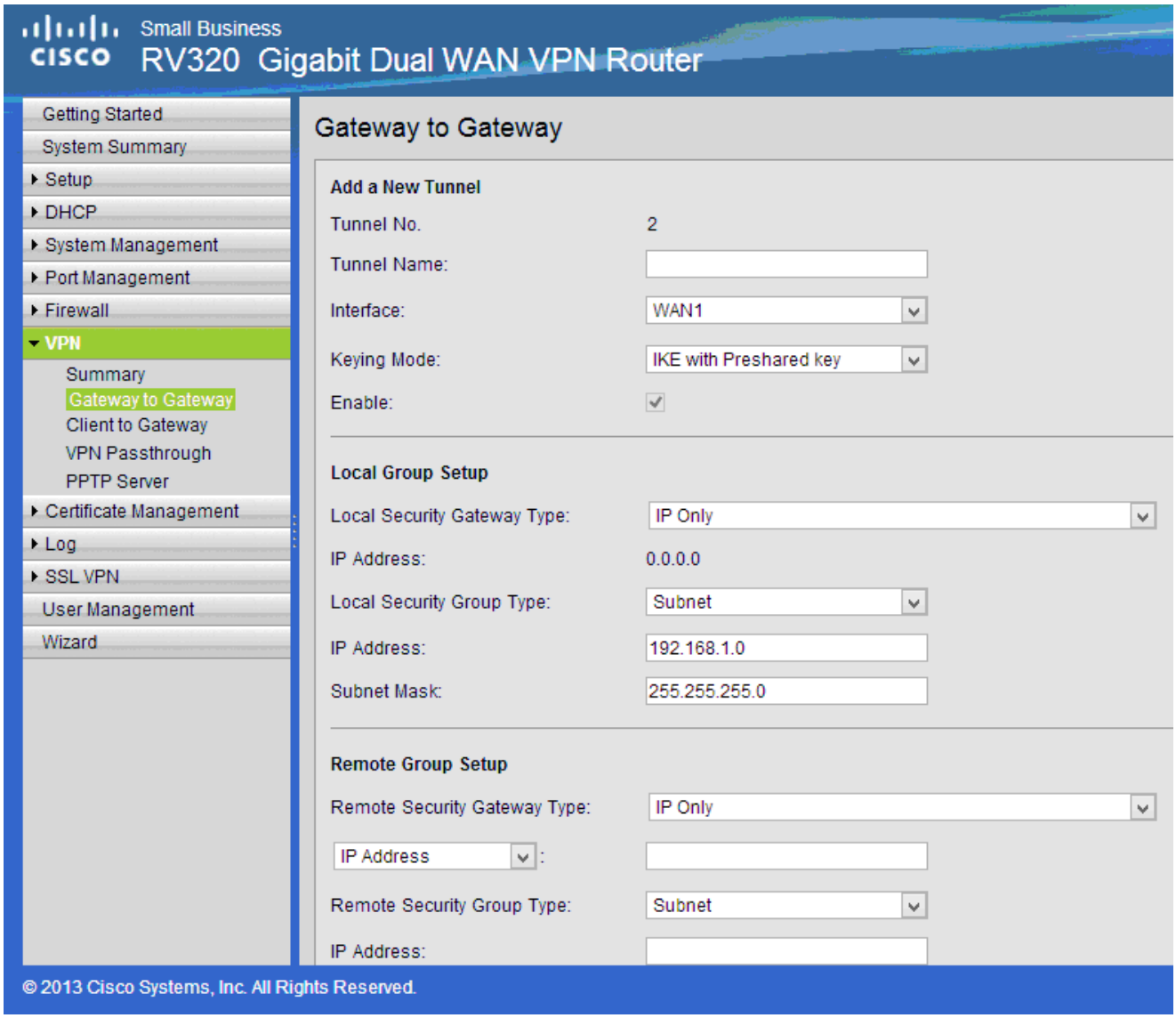
設定前チェックリスト
ステップ1:RV320とDSLまたはケーブルモデムの間にイーサネットケーブルを接続し、ISA570とDSLまたはケーブルモデムの間にイーサネットケーブルを接続します。
ステップ2:RV320をオンにし、内部PC、サーバ、およびその他のIPデバイスをRV320のLANポートに接続します。
ステップ3:ISA570をオンにし、内部PC、サーバ、およびその他のIPデバイスをISA570のLANポートに接続します。
手順4：異なるサブネット上の各サイトでネットワークIPアドレスを設定します。この例では、リモートオフィスLANは192.168.1.0を使用し、本社LANは10.10.10.0を使用しています。
ステップ5：ローカルPCがそれぞれのルータと、同じLAN上の他のPCに接続できることを確認します。

WAN接続の特定

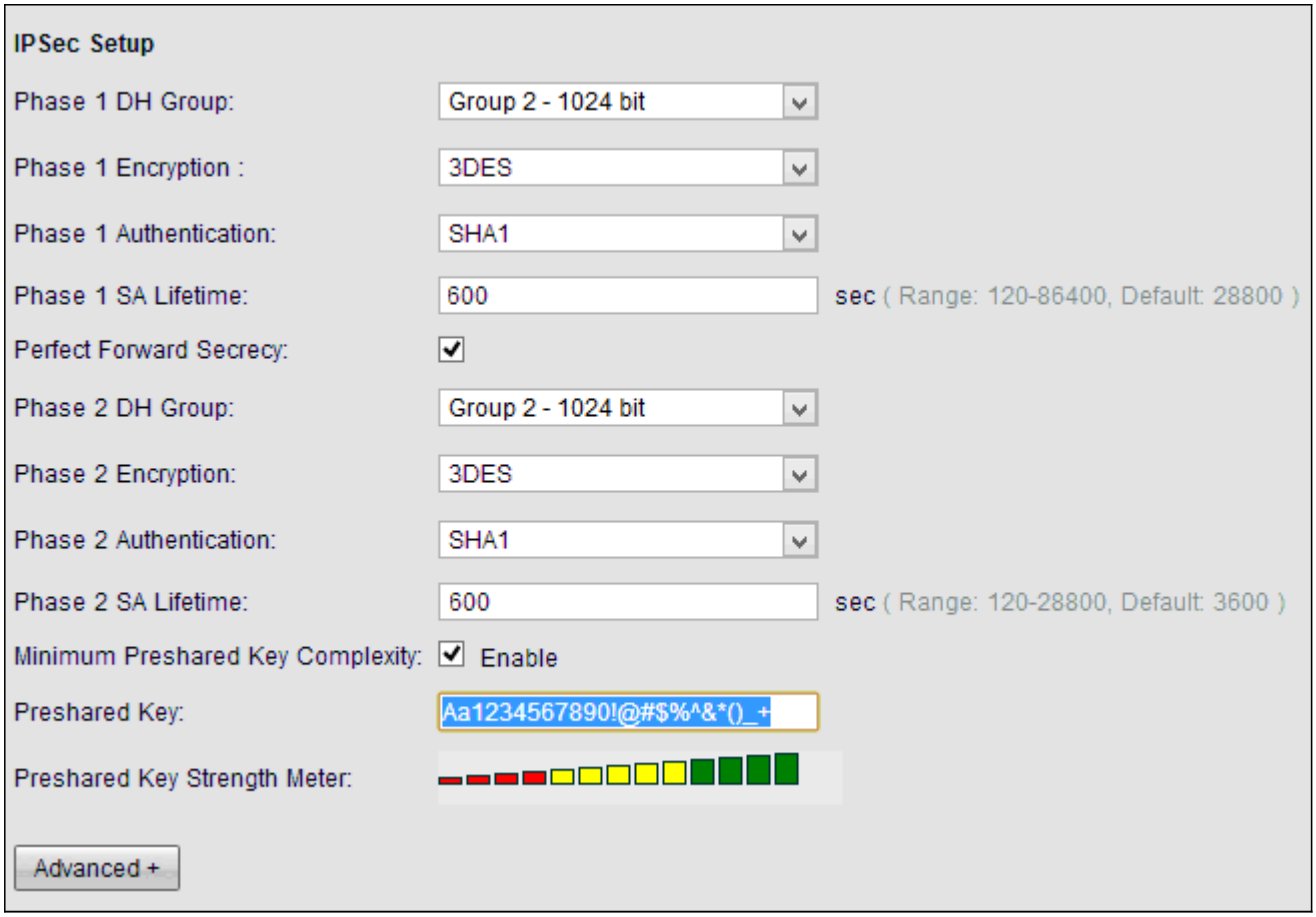
ISPがダイナミックIPアドレスまたはスタティックIPアドレスを提供しているかどうかを確認する必要があります。通常、ISPはダイナミックIPアドレスを提供しますが、サイト間VPNトンネル設定を完了する前に、これを確認する必要があります。

リモートオフィスでのRV320用のサイト間IPsec VPNトンネルの設定

ステップ1:[VPN] > [Gateway-to-Gateway]に移動します（図を参照）
a.) トンネル名（RemoteOfficeなど）を入力します。
b.) インターフェイスをWAN1に設定します。
c.) 事前共有キーを使用して、キーイングモードをIKEに設定します。
d.) [Local IP Address]と[Remote IP Address]を入力します。
次の図は、[RV320 Gigabit Dual WAN Router Gateway to Gateway]ページを示しています。



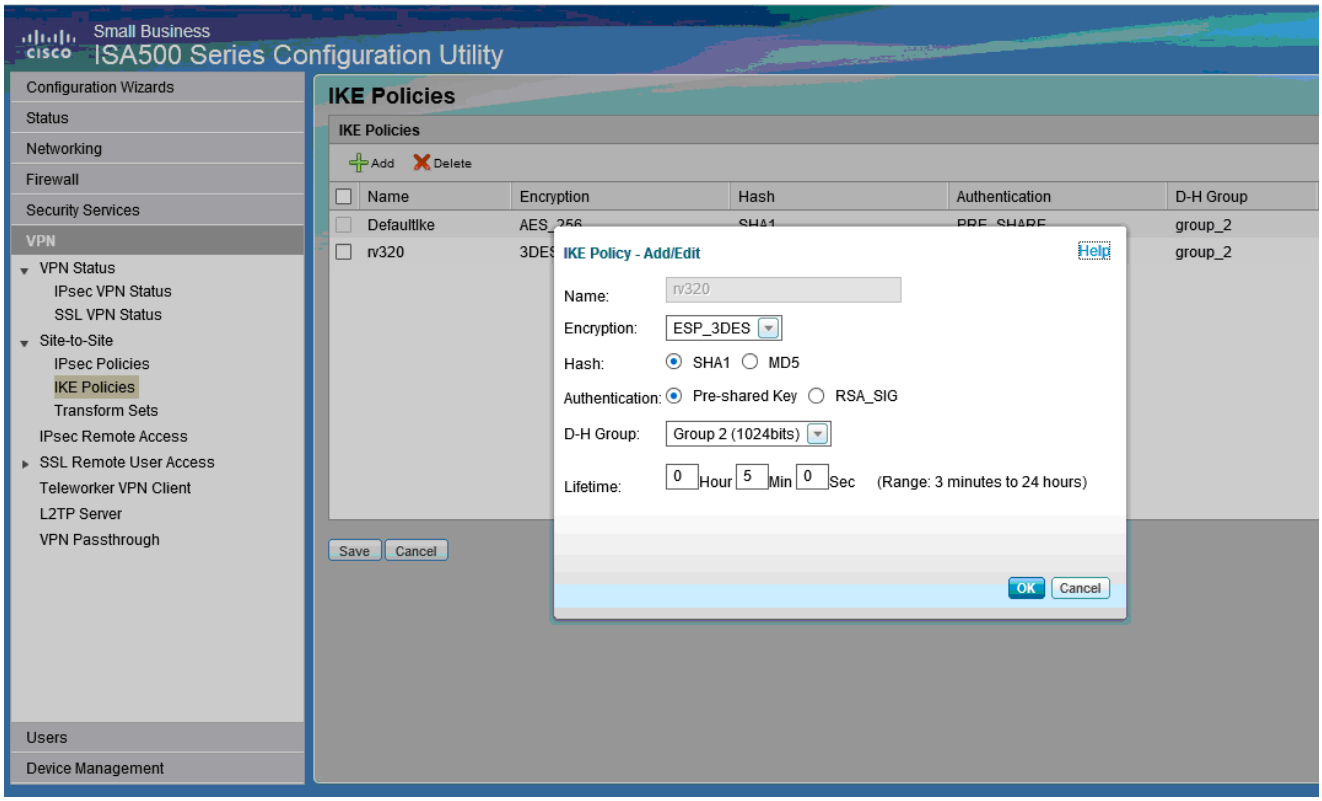
ステップ2:IPSecトンネル設定の設定（図を参照）
a.) [暗号化]を3DESに設定します。
b.) [Authentication]を/SHA1]に設定します。
c.) Perfect *Forward Secrecy*をチェックします。
d.) 事前共有キーを設定します（両方のルータで同じにする必要があります）。
次に、IPSecセットアップ（フェーズ1および2）を示します。



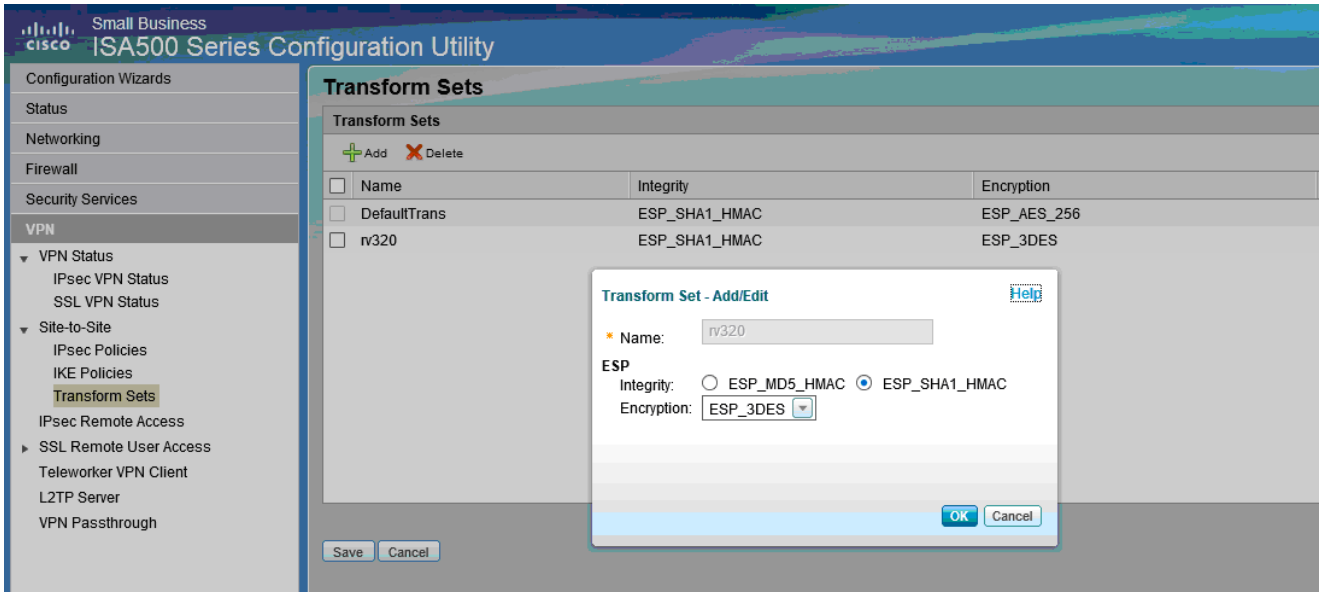
注：サイト間IPsec VPNトンネルの両側のIPsecトンネル設定が一致する必要があることに注意してください。RV320とISA570のIPsecトンネル設定に不一致がある場合、両方のデバイスが暗号化キーのネゴシエートに失敗し、接続に失敗します。
ステップ3:[Save]をクリックし、設定を完了します。

本社のISA570用サイト間IPsec VPNトンネルの設定

ステップ1:[VPN] > [IKE Policies]に移動します（図を参照）。
a.) 暗号化をESP_3DESに設定します。
b.) ハッシュをSHA1に設定します。
c.) [Authentication]を[Pre-shared Key]に設定します。
d.) [D-H Group]を[Group 2（1024ビット）]に設定します。
次の図に、IKEポリシーを示します。



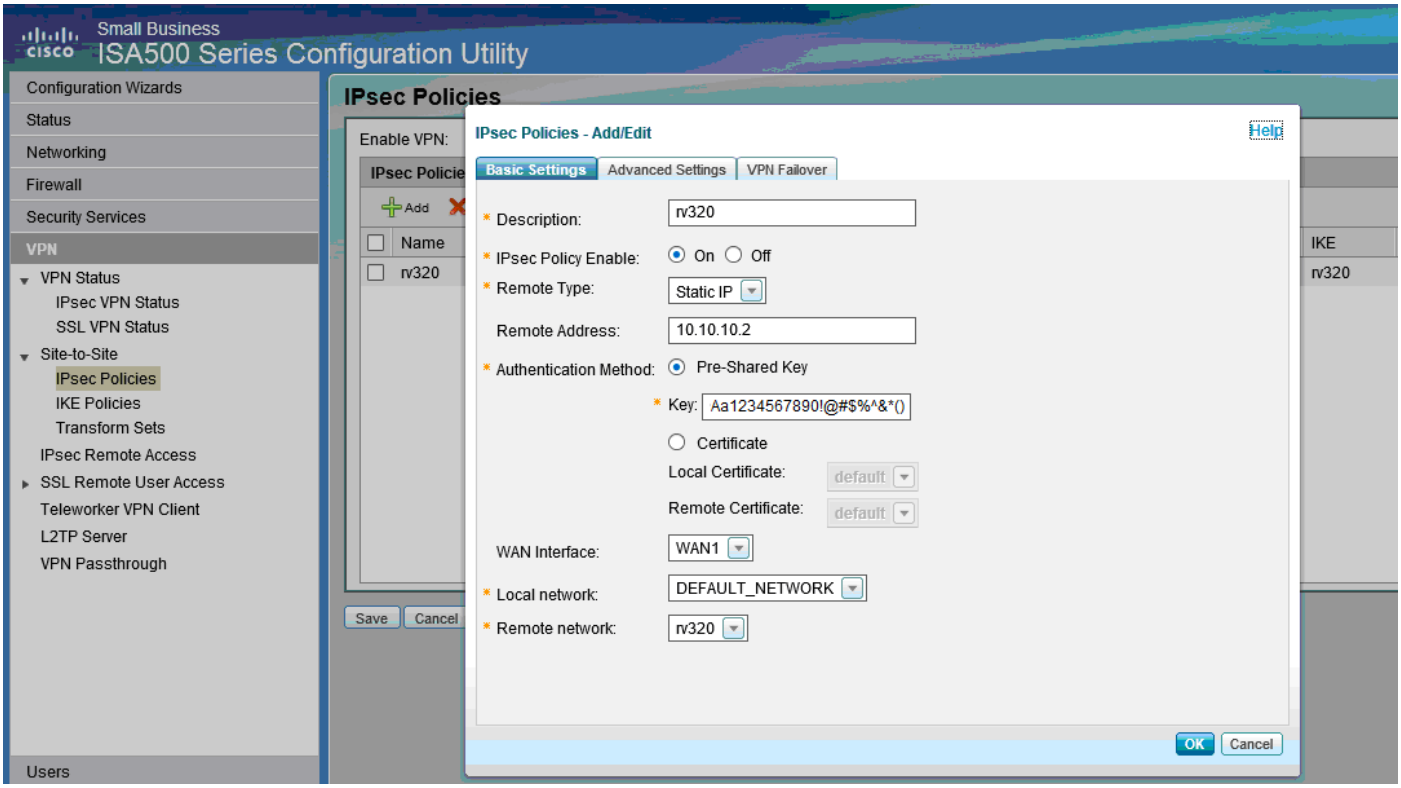
ステップ2:[VPN] > [IKE Transform Sets]に移動します（図を参照）
a.) [Integrity] を[ESP_SHA1_HMAC]に設定します。
b.) [Encryption]を[ESP_DES]に設定します。
次に、IKEトランスフォームセットを示します。



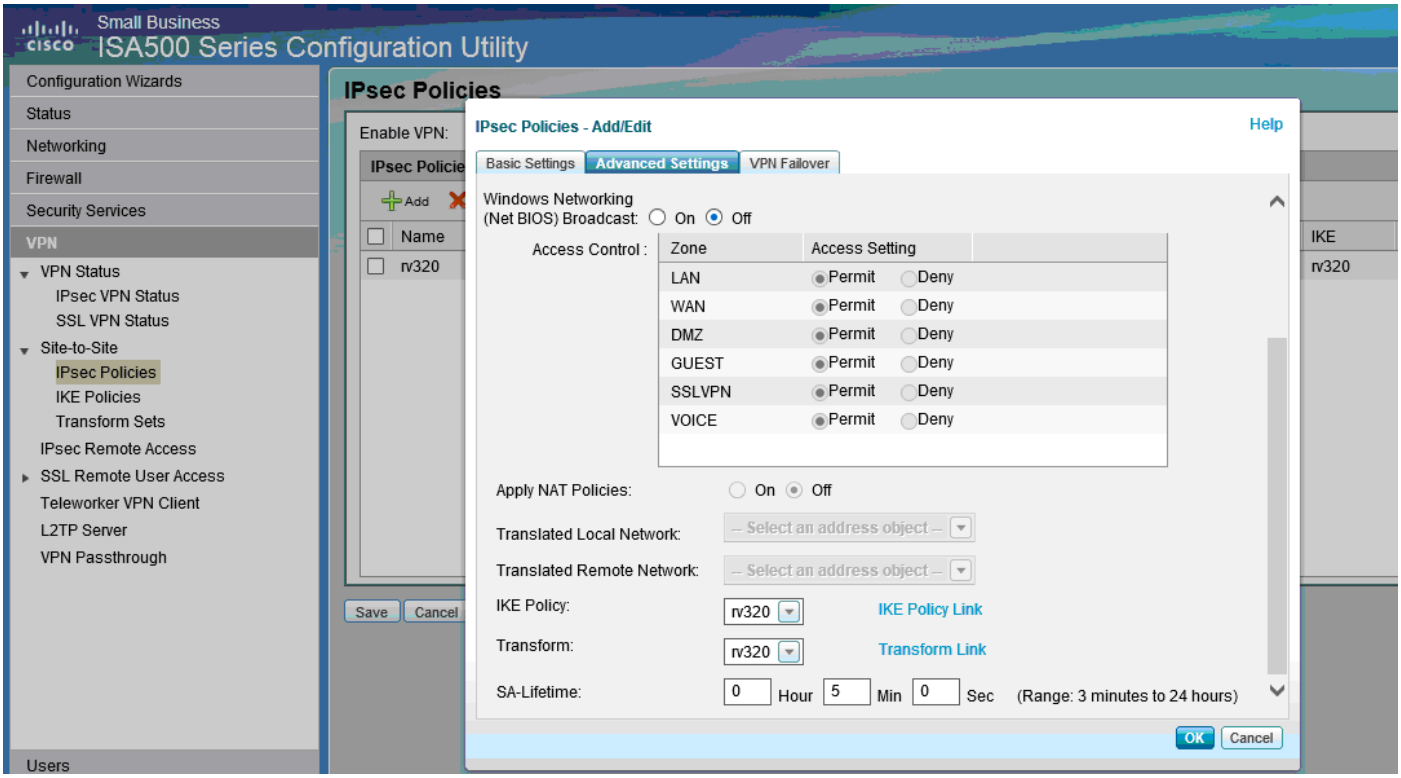
ステップ3:[VPN] > [IPsec Policies] > [Add] > [Basic Settings]に移動します（図を参照）。

a.) RV320など、説明を入力します。
b.) IPsecポリシーの有効化をオンに設定します。
c.) [Remote Type] を[Static IP]に設定します。
d.) リモートアドレスを入力。
e.) [Authentication Method] を[Pre-Shared Key]に設定します。
f) WANインターフェイスをWAN1に設定します。
g.) ローカル・ネットワークをDEFAULT_NETWORKに設定します。

h.) リモートネ ットワークをRV320に設定します。
次の図に、IPsecポリシーの基本設定を示します。



ステップ4:[VPN] > [IPsec Policies] > [Add] > [Advanced Settings]に移動します（図を参照）。
a.) IKEポリ シーと *IKE*トランスフォームセットを、手順1と2で作成したセットにそれぞれ設定します。
b.) *SA- Lifetime*を*0*時間5分0秒に設定します。
c.) [OK] をクリックします。
次に、IPsecポリシーの詳細設定を示します。



ステップ5：サイト間IPsec VPNトンネルの接続（図を参照）
a.) [Enable VPN] を*[*On *]*に設定します。
b.) [接続]ボタ **ンをクリッ**クします。
次の図は、[Connect]ボタンを示しています。