CHAPTER 34

ASA 5505 上での Easy VPN サービスの設定

この章では、Easy VPN ハードウェア クライアントとして ASA 5505 を設定する方法について説明します。ここでは、ASA 5505 のスイッチ ポートと VLAN インターフェイスが設定されていることを前提としています（第 4 章「Cisco ASA 5505 適応型セキュリティ アプライアンス用スイッチ ポートおよび VLAN インターフェイスの設定」を参照）。

（注） Easy VPN ハードウェア クライアントのコンフィギュレーションでは、プライマリとセカンダリ（バックアップ）の Easy VPN サーバの IP アドレスを指定します。ヘッドエンドとして設定した別の ASA 5505、VPN 3000 シリーズ コンセントレータ、IOS ベースのルータ、またはファイアウォールなどの任意の ASA は、Easy VPN サーバとして動作することができます。ただし ASA 5505 は、同時にクライアントとサーバの両方として機能できません。ASA 5505 をサーバとして設定するには、「Cisco ASA 5505 のクライアント / サーバの役割の指定」（P.34-1）を参照してください。次に、このマニュアルの 「はじめに」（P.2-1）に記載されている他の ASA と同様に ASA 5505 を設定します。

この章は、次の項で構成されています。

Cisco ASA 5505 のクライアント / サーバの役割の指定

Cisco ASA 5505 は、Cisco Easy VPN ハードウェア クライアント（「Easy VPN Remote」とも呼ばれる）またはサーバ（「ヘッドエンド」とも呼ばれる）として機能しますが、同時に両方を機能させることはできません。デフォルトの役割はありません。グローバル コンフィギュレーション モードで次のコマンドのいずれかを使用して、役割を指定します。

- vpnclient enable：ASA 5505 の役割を Easy VPN Remote として指定します。
- **no vpnclient enable**：ASA 5505 の役割をサーバとして指定します。

次の例では、ASA 5505 を Easy VPN ハードウェア クライアントとして指定する方法について示します。

```
hostname(config)# vpnclient enable
hostname(config)#
```

サーバからハードウェア クライアントに切り替える場合、該当の要素がコンフィギュレーションに存在するかどうかによって、特定のデータ要素を削除する必要があることを示すエラー メッセージが CLI に表示されます。表 34-1 に、クライアントおよびサーバの両方のコンフィギュレーションで許可されていて、クライアント コンフィギュレーションで許可されていないデータ要素を示します。

表 34-1　ASA 5505 での特権と制限の設定

クライアントとサーバの両方で許可されている構成	クライアント コンフィギュレーションで許可されていない
crypto ca trustpoints	tunnel-groups
digital certificates	isakmp policies
group-policies	crypto maps
crypto dynamic-maps	
crypto ipsec transform-sets	
crypto ipsec security-association lifetime	
crypto ipsec fragmentation before-encryption	
crypto ipsec df-bit copy-df	

Easy VPN ハードウェア クライアントとして設定された ASA 5505 は、コンフィギュレーション内の最初のカラムにリストされたコマンドを保持します。ただし、クライアントの役割が機能しないものもあります。

次の例では、ASA 5505 を Easy VPN サーバとして指定する方法を示します。

```
hostname(config)# no vpnclient enable
hostname(config)#
```

このコマンドの no 形式を入力してから、このマニュアルの 「はじめに」（P.2-1）に記載されている別の ASA と同様に ASA 5505 を設定します。

プライマリおよびセカンダリ サーバの指定

Easy VPN ハードウェア クライアントとの接続を確立する前に、接続先の Easy VPN サーバの IP アドレスを指定する必要があります。ヘッドエンドとして設定した別の ASA 5505、VPN 3000 シリーズ コンセントレータ、IOS ベースのルータ、またはファイアウォールなどの任意の ASA は、Easy VPN サーバとして動作することができます。

ASA 5505 のクライアントは、ヘッドエンド プライマリ VPN サーバへのトンネルを設定するように常に試みます。プライマリ サーバへのトンネルを設定できない場合は、secondary_1 VPN サーバへの接続を試行し、その後は VPN サーバのリストの上から順に 8 秒間隔で接続を試行します。secondary_1 サーバへの設定済みトンネルに障害が発生すると、この間にプライマリがオンラインになり、ASA は secondary_2 VPN サーバへのトンネルを設定します。

次のように、グローバル コンフィギュレーション モードで **vpnclient server** コマンドを使用します。

[**no**] **vpnclient server** *ip_primary* [*ip_secondary_1…ip_secondary_10*]

no を使用すると、実行コンフィギュレーションからこのコマンドが削除されます。

ip_primary_address は、プライマリ Easy VPN サーバの IP アドレスまたは DNS 名です。

ip_secondary_address_n（任意）は、最大 10 のバックアップ Easy VPN サーバの IP アドレスまたは DNS 名のリストです。スペースを使用して、リスト内の項目を区切ります。

たとえば、次のコマンドを入力して VPN クライアントを設定し、Easy VPN サーバ 10.10.10.15 をプライマリ サーバ、10.10.10.30 および 192.168.10.45 を代替サーバとしてそれぞれ使用します。

```
hostname(config)# vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
hostname(config)#
```

モードの指定

Easy VPN クライアントは、クライアント モードまたは Network Extension Mode（NEM; ネットワーク拡張モード）のいずれかの操作モードをサポートします。操作モードによって、Easy VPN クライアントに関連する内部ホストがトンネルを経由して企業ネットワークからアクセスできるかどうかが決まります。Easy VPN クライアントにはデフォルト モードがないため、接続前に動作モードを指定する必要があります。

クライアント モードは、ポート アドレス変換（PAT）モードとも呼ばれ、Easy VPN クライアント プライベート ネットワーク上のすべてのデバイスの IP アドレスを企業ネットワークの IP アドレスから分離します。Easy VPN クライアントは、内部ホストのすべての VPN トラフィックに対して PAT を実行します。Easy VPN クライアント内部インターフェイスまたは内部ホストで、IP アドレスの管理は必要ではありません。

NEM は、内部インターフェイスとすべての内部ホストに対して、トンネルを介して企業ネットワークをルーティングできるようにします。内部ネットワークのホストは、スタティック IP アドレスで事前設定されたアクセス可能なサブネット（スタティックまたは DHCP を介して）から IP アドレスを取得します。NEM では、PAT は VPN トラフィックに適用されません。このモードでは、各クライアントに VPN を設定する必要がありません。NEM モード用に設定された Cisco ASA 5505 では、自動トンネル起動をサポートしています。コンフィギュレーションには、グループ名、ユーザ名、およびパスワードを保存する必要があります。セキュア ユニット認証がイネーブルの場合は、トンネルの自動開始がディセーブルになります。

（注） Easy VPN ハードウェア クライアントが NEM を使用し、セカンダリ サーバに接続している場合は、各ヘッドエンド デバイスで **crypto map set reverse-route** コマンドを使用して、Reverse Route Injection（RRI; 逆ルート注入）によるリモート ネットワークのダイナミック通知を設定します。

Easy VPN クライアントのモードを指定するには、コンフィギュレーション モードで次のコマンドを入力します。

[**no**] **vpnclient mode** {**client-mode** | **network-extension-mode**}

no を使用すると、実行コンフィギュレーションからこのコマンドが削除されます。

複数のインターフェイスでの NEM

ASA 5505 セキュリティ アプライアンス（バージョン 7.2(3) 以降）を、複数のインターフェイスが設定されているネットワーク拡張モードで Easy VPN クライアントとして設定した場合、セキュリティ アプライアンスは、セキュリティ レベルが最高のインターフェイスからだけのローカルに暗号化されたトラフィック用のトンネルを構築します。

たとえば、次のようなコンフィギュレーションがあるものとします。

```
vlan1 security level 100 nameif inside
vlan2 security level 0 nameif outside
vlan12 security level 75 nameif work
```

このシナリオでは、セキュリティ アプライアンスはセキュリティ レベルが最高のインターフェイスである vlan1 に対してだけトンネルを作成します。vlan12 からのトラフィックを暗号化するには、インターフェイス vlan1 のセキュリティ レベルを、vlan12 より低い値に変更する必要があります。

自動 Xauth 認証の設定

Easy VPN ハードウェア クライアントとして設定された ASA 5505 は、次の条件がすべて真である場合、Easy VPN サーバへの接続を自動的に認証します。

- サーバ上で、セキュア ユニット認証がディセーブルになっている。
- サーバが IKE 拡張認証（Xauth）クレデンシャルを要求する。

  Xauth には、TACACS+ または RADIUS を使用して IKE 内のユーザを認証する機能があります。Xauth は、RADIUS または別のサポートされているユーザ認証プロトコルを使用して、ユーザを認証します（この場合、Easy VPN ハードウェア クライアント）。
- クライアント コンフィギュレーションには、Xauth ユーザ名とパスワードが含まれる。

グローバル コンフィギュレーション モードで次のコマンドを入力して Xauth ユーザ名とパスワードを設定します。

vpnclient username *xauth_username* **password** *xauth password*

それぞれに、最大 64 文字使用できます。

たとえば、次のコマンドを使用して Easy VPN ハードウェア クライアントを設定し、XAUTH ユーザ名として testuser、パスワードとして ppurkm1 を使用します。

```
hostname(config)# vpnclient username testuser password ppurkm1
hostname(config)#
```

実行コンフィギュレーションからユーザ名とパスワードを削除するには、次のコマンドを入力します。

no vpnclient username

次に例を示します。

```
hostname(config)# no vpnclient username
hostname(config)#
```

IPSec Over TCP の設定

デフォルトでは、Easy VPN ハードウェア クライアントとサーバは IPSec をユーザ データグラム プロトコル（UDP）パケット内でカプセル化します。一部の環境（特定のファイアウォール ルールが設定されている環境など）または NAT デバイスや PAT デバイスでは、UDP を使用できません。そのような環境で標準の Encapsulating Security Protocol（ESP; カプセル化セキュリティ プロトコル、プロトコル 50）または Internet Key Exchange（IKE; インターネット キー交換、UDP 500）を使用するには、TCP パケット内に IPSec をカプセル化してセキュアなトンネリングをイネーブルにするようにクライアントとサーバを設定します。ただし、UDP が許可されている環境では、IPSec over TCP を設定すると不要なオーバーヘッドが発生します。

Easy VPN ハードウェア クライアントが TCP カプセル化 IPSec を使用するように設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

vpnclient ipsec-over-tcp [**port** *tcp_port*]

Easy VPN ハードウェア クライアントは、コマンドがポート番号を指定しない場合、ポート 10000 を使用します。

TCP カプセル化 IPSec を使用するように ASA 5505 を設定する場合は、次のコマンドを入力して、外部インターフェイスを介して大きなパケットを送信できるようにします。

```
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

このコマンドは、Don't Fragment（DF）ビットをカプセル化されたヘッダーからクリアします。DF ビットは、パケットを断片化できるかどうかを決定する IP ヘッダー内のビットです。このコマンドを使用すると、Easy VPN ハードウェア クライアントは MTU サイズよりも大きいパケットを送信できます。

次に、デフォルト ポート 10000 を使用して TCP カプセル化 IPSec を使用するように Easy VPN ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにする例を示します。

```
hostname(config)# vpnclient ipsec-over-tcp
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

次に、ポート 10501 を使用して TCP カプセル化 IPSec を使用するように Easy VPN ハードウェア クライアントを設定し、外部インターフェイスを介して大きなパケットを送信できるようにする例を示します。

```
hostname(config)# vpnclient ipsec-over-tcp port 10501
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

この属性を実行コンフィギュレーションから削除するには、次のように、このコマンドの **no** 形式を使用します。

no vpnclient ipsec-over-tcp

次に例を示します。

```
hostname(config)# no vpnclient ipsec-over-tcp
hostname(config)#
```

トンネリング オプションの比較

Easy VPN ハードウェア クライアントとして設定された Cisco ASA 5505 が設定するトンネル タイプは、次の要素の組み合わせによって異なります。

- ヘッドエンド上で **split-tunnel-network-list** コマンドと **split-tunnel-policy** コマンドを使用して、スプリット トンネリングを許可、制限、または禁止します（「スプリット トンネリング用のネットワーク リストの作成」（P.30-43）および「スプリット トンネリング ポリシーの設定」（P.30-42）をそれぞれ参照してください）。

  スプリット トンネリングは、リモートアクセス クライアントがセキュアな VPN トンネルを経由して暗号化して送信するネットワークを判別します。また、そのままインターネットに送信するトラフィックも判別します。

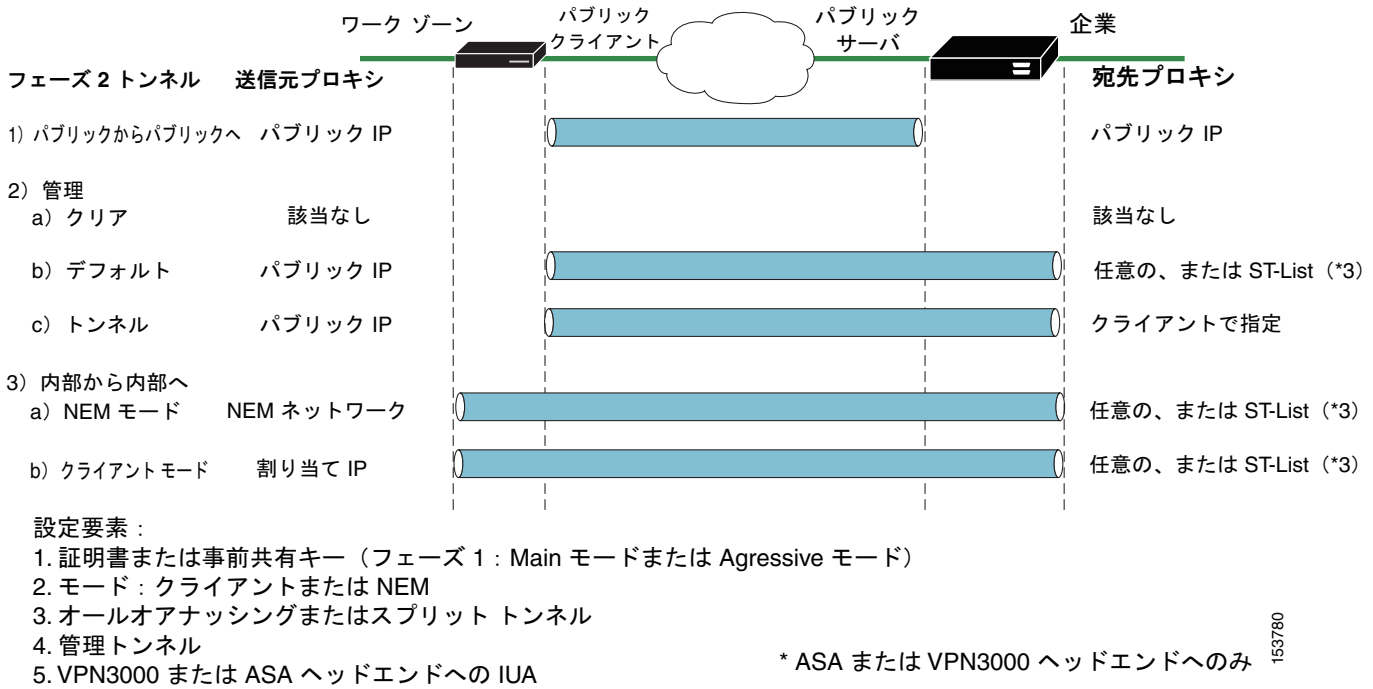
- **vpnclient management** コマンドを使用して、次の自動トンネル起動オプションのいずれかを指定します。
  - **tunnel** は、特定のホストまたは企業側のネットワークによるクライアント側への管理アクセスを制限し、IPSec を使用して、すでに存在している HTTPS または SSH 暗号化を介して暗号化レイヤを管理セッションに追加します。
  - **clear** は、管理セッションが使用する HTTPS または SSH 暗号化を使用して管理アクセスを許可します。
  - **no** は、管理アクセスを禁止します。

注意　シスコは、NAT デバイスがクライアントとインターネット間に存在する場合、vpnclient management コマンドの使用をサポートしません。

- **vpnclient mode** コマンドを使用して、次の操作モードのいずれかを指定します。
  - **client** は、ポート アドレス変換（PAT）モードを使用して、クライアントに関連する内部ホストのアドレスを企業ネットワークから分離します。
  - **network-extension-mode** は、このようなアドレスを企業ネットワークからアクセス可能にします。

図 34-1 に、ユーザが入力したコマンドの組み合わせに基づいて Easy VPN クライアントが起動するトンネルのタイプを示します。

図 34-1　Cisco ASA 5505 用の Easy VPN ハードウェア クライアント トンネリング オプション



「All-Or-Nothing」という用語は、スプリット トンネリングのアクセス リストの有無を意味します。アクセス リスト（「ST-list」）は、トンネリングを必要とするネットワークと必要としないネットワークを識別します。

トンネル グループまたはトラストポイントの指定

Cisco ASA 5505 を Easy VPN ハードウェア クライアントとして設定する場合、Easy VPN サーバのコンフィギュレーションに応じて、Easy VPN サーバ上に設定されるトンネル グループまたはトラストポイントを指定することができます。次の項で、使用するオプションを確認してください。

- トンネル グループの指定
- トラストポイントの指定

トンネル グループの指定

グローバル コンフィギュレーション モードで次のコマンドを入力し、Easy VPN クライアントがサーバに接続するための VPN トンネル グループの名前とパスワードを指定します。

vpnclient vpngroup *group_name* **password** *preshared_key*

group_name は、Easy VPN サーバ上に設定された VPN トンネル グループの名前です。接続を確立する前に、このトンネル グループをサーバ上に設定する必要があります。

preshared_key は、Easy VPN サーバ上の認証に使用される IKE 事前共有キーです。

たとえば、次のコマンドを入力して、TestGroup1 と呼ばれる VPN トンネル グループと IKE 事前共有キー my_key123 を指定します。

```
hostname(config)# vpnclient vpngroup TestGroup1 password my_key123
```

```
hostname(config)#
```

実行コンフィギュレーションからこの属性を削除するには、次のコマンドを入力します。

no vpnclient vpngroup

Easy VPN クライアントとして動作している ASA 5505 のコンフィギュレーションでトンネル グループが指定されていない場合、クライアントは RSA 証明書を使用しようとします。

次に例を示します。

```
hostname(config)# no vpnclient vpngroup
hostname(config)#
```

トラストポイントの指定

トラストポイントは、CA が発行する証明書に基づいた CA のアイデンティティとデバイスのアイデンティティを表します。これらのパラメータはセキュリティ アプライアンスが CA から証明書を取得する方法を指定し、CA が発行するユーザ証明書の認証ポリシーを定義します。

まず、「トラストポイントの設定」（P.39-7）のとおりに、**crypto ca trustpoint** コマンドを使用してトラストポイントを定義します。次に、グローバル コンフィギュレーション モードで次のコマンドを入力して、認証に使用する RSA 証明書を識別するトラストポイントを指定します。

vpnclient trustpoint *trustpoint_name* [**chain**]

trustpoint_name は、認証に使用する RSA 証明書を識別するトラストポイントを指定します。

（任意）**chain** は証明書チェーン全体を送信します。

たとえば、次のコマンドを入力して central という名前の証明書を指定し、証明書チェーン全体を送信します。

```
hostname(config)# crypto ca trustpoint central
hostname(config)# vpnclient trustpoint central chain
hostname(config)#
```

実行コンフィギュレーションからこの属性を削除するには、次のコマンドを入力します。

no vpnclient trustpoint

次に例を示します。

```
hostname(config)# no vpnclient trustpoint
hostname(config)#
```

スプリット トンネリングの設定

スプリット トンネリングを使用すると、リモートアクセス IPSec クライアントは、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリア テキスト形式でネットワーク インターフェイスに誘導したりすることができます。

Easy VPN サーバは、グループ ポリシーからスプリット トンネリング属性を、ワーク ゾーンだけで使用するために Easy VPN クライアントに配信します。Cisco ASA 5505 にスプリット トンネリングを設定するには、「スプリット トンネリング属性の設定」（P.30-42）を参照してください。

グローバル コンフィギュレーション モードで次のコマンドを入力して、NEM とスプリット トンネリングの設定時に IPSec トンネルの自動起動をイネーブルにします。

[**no**] **vpnclient nem-st-autoconnect**

no を使用すると、実行コンフィギュレーションからこのコマンドが削除されます。

次に例を示します。

```
hostname(config)# vpnclient nem-st-autoconnect
hostname(config)#
```

デバイス パススルーの設定

Cisco IP Phone、無線アクセス ポイント、およびプリンタなどのデバイスは認証を実行できません。個々のユーザの認証がイネーブルになっている場合、グローバル コンフィギュレーション モードで次のコマンドを入力し、このようなデバイスの認証を免除してネットワーク アクセスを可能にします。

[**no**] **vpnclient mac-exempt** *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]

no を使用すると、実行コンフィギュレーションからこのコマンドが削除されます。

mac_addr は、個々のユーザ認証をバイパスするデバイスのドット付き 16 進数表記の MAC アドレスです。

mac_mask は、対応する MAC アドレスのネットワーク マスクです。MAC マスク ffff.ff00.0000 は、同一の製造業者が製造したすべてのデバイスに対応します。MAC マスク ffff.ffff.ffff は 1 つのデバイスに対応します。

MAC マスク ffff.ff00.0000 を使用して同一の製造業者が製造したすべてのデバイスを指定する場合、特定の MAC アドレスの最初の 6 文字だけが必要です。たとえば、Cisco IP Phone に製造業者 ID 00036b が設定されている場合、次のコマンドでは、将来的に追加される可能性があるものも含め、すべての Cisco IP Phone が免除されます。

```
hostname(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
hostname(config)#
```

次に、1 つの特定の Cisco IP Phone を免除する例を示します。このようにすると、セキュリティは向上しますが、柔軟性が低くなります。

```
hostname(config)# vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
hostname(config)#
```

リモート管理の設定

Easy VPN ハードウェア クライアントとして動作する Cisco ASA 5505 は、レイヤ 2 の暗号化の有無にかかわらず、SSH または HTTPS を使用して管理アクセスをサポートします。SSH または HTTPS 暗号化で IPSec 暗号化を要求するように Cisco ASA 5505 を設定できます。

グローバル コンフィギュレーション モードで **vpnclient management clear** コマンドを使用して、通常のルーティングにより企業ネットワークから ASA 5505 の外部インターフェイスに管理アクセスを提供します（トンネリング管理パケットなし）。

注意　NAT デバイスが Easy VPN ハードウェア クライアントとインターネットの間で動作している場合、Easy VPN ハードウェア クライアントとして設定されている Cisco ASA 5505 上に管理トンネルを設定しないでください。そのコンフィギュレーションでは、**vpnclient management clear** コマンドを使用します。

IPSec トンネルの作成を自動化して、企業ネットワークから ASA 5505 の外部インターフェイスに管理アクセスを提供する場合、グローバル コンフィギュレーション モードで **vpnclient management tunnel** コマンドを使用します。Easy VPN ハードウェア クライアントとサーバは、**vpnclient server** コマンドの実行後にトンネルを自動的に作成します。vpnclient management tunnel コマンドの構文は次のとおりです。

vpnclient management tunnel *ip_addr_1 ip_mask_1* [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

たとえば、次のコマンドを入力して IPSec トンネルの作成を自動化し、IP アドレス 192.168.10.10 のホストに管理アクセスを提供します。

```
hostname(config)# vpnclient management tunnel 192.198.10.10 255.255.255.0
hostname(config)#
```

このコマンドの **no** 形式は、**split-tunnel-policy** コマンドと **split-tunnel-network-list** コマンドに従って管理トンネル用の IPSec を設定します。

no vpnclient management

次に例を示します。

```
hostname(config)# no vpnclient management
hostname(config)#
```

Easy VPN サーバの設定用ガイドライン

次の項では、Easy VPN サーバに適用される Easy VPN ハードウェア クライアントに関する注意事項を説明します。

- クライアントに配信されるグループ ポリシーとユーザ属性
- 認証のオプション

クライアントに配信されるグループ ポリシーとユーザ属性

トンネルの確立後、Easy VPN サーバは、そのコンフィギュレーションに保存されているグループ ポリシーまたはユーザ属性の値を Easy VPN ハードウェア クライアントに配信します。したがって、Easy VPN ハードウェア クライアントに配信された特定の属性を変更するには、プライマリおよびセカンダリ Easy VPN サーバとして設定されているセキュリティ アプライアンス上で、それらの属性を変更する必要があります。この項では、Easy VPN ハードウェア クライアントに配信されたグループ ポリシーとユーザ属性について説明します。

（注）　この項は参照用です。グループ ポリシーとユーザの設定手順については、「トンネル グループ、グループ ポリシーおよびユーザの設定」（P.30-1）を参照してください。

表 34-2 は、グループ ポリシーまたはユーザ属性を変更するためのコマンドを指定するガイドとして使用してください。

表 34-2　Easy VPN ハードウェア クライアントとして設定されている Cisco ASA 5505 に配信されたグループ ポリシーとユーザ属性

コマンド	説明
backup-servers	プライマリ サーバが応答に失敗した場合、クライアント上にバックアップ サーバを設定します。
banner	トンネルの確立後、バナーをクライアントに送信します。
client-access-rule	アクセス ルールを適用します。
client-firewall	VPN クライアント上にファイアウォール パラメータを設定します。
default-domain	クライアントにドメイン名を送信します。
dns-server	プライマリおよびセカンダリ DNS サーバの IP アドレスを指定するか、または DNS サーバの使用を禁止します。
dhcp-network-scope	DHCP サーバがこのグループ内のユーザにアドレスを割り当てる IP サブネットワークを指定します。
group-lock	ユーザがそのグループに接続していることを確認するトンネル グループを指定します。
ipsec-udp	IPSec トンネルに UDP カプセル化を使用します。
ipsec-udp-port	IPSec over UDP のポート番号を指定します。
nem	ネットワーク拡張モードをイネーブルまたはディセーブルにします。
password-storage	VPN ユーザがユーザ プロファイルにパスワードを保存できるようにします。
pfs	VPN クライアントに Perfect Forward Secrecy（PFS; 完全転送秘密）を使用するように指示します。
re-xauth	IKE キーの再生成時に、XAUTH 認証を要求します。 （注）セキュア ユニット認証がイネーブルの場合、re-xauth をディセーブルにします。
secure-unit-authentication	VPN ハードウェア クライアントの対話型認証をイネーブルにします。
split-dns	名前解決用のドメインのリストを配信します。
split-tunnel-network-list	次のいずれかを指定します。 • スプリット トンネリングにはアクセス リストがありません。トラフィックはすべてトンネルを通過します。 • トンネリングを要求するネットワークと要求しないネットワークを識別するためにセキュリティ アプライアンスが使用するアクセス リストを特定します。 スプリット トンネリングを使用すると、リモート アクセス IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようになります。スプリット トンネリングをイネーブルにすると、宛先が IPSec トンネルの反対側ではないパケットでは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングは必要なくなります。

表 34-2　Easy VPN ハードウェア クライアントとして設定されている Cisco ASA 5505 に配信されたグループ ポリシーとユーザ属性 （続き）

コマンド	説明
split-tunnel-policy	リモートアクセス IPSec クライアントは、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにします。オプションには、次のものが含まれます。 • split-tunnel-policy：トンネリング トラフィックにルールを設定していることを示します。 • excludespecified：トラフィックがクリア テキストで送信されるネットワークのリストを定義します。 • tunnelall：トラフィックがクリア テキストで通過しないように、または Easy VPN サーバ以外の宛先に送信されないように指定します。リモート ユーザは企業ネットワークを経由してインターネットにアクセスしますが、ローカル ネットワークにはアクセスできません。 • tunnelspecified：指定のネットワークから、または指定のネットワークに、すべてのトラフィックをトンネリングします。このオプションによって、スプリット トンネリングが有効になります。トンネリングするアドレスのネットワーク リストを作成できるようになります。その他のすべてのアドレスへのデータは暗号化しないで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。
user-authentication	ハードウェアベースの VPN クライアントに対する個々のユーザ認証をイネーブルにします。
vpn-access-hours	VPN アクセス時間を制限します。
vpn-filter	フィルタを VPN トラフィックに適用します。
vpn-idle-timeout	セッションがタイムアウトになるまでのアイドル時間を分単位で指定します。
vpn-session-timeout	VPN 接続の最長時間を分単位で指定します。
vpn-simultaneous-logins	同時ログインの最大数を指定します。
vpn-tunnel-protocol	許可されたトンネリング プロトコルを指定します。
wins-server	プライマリおよびセカンダリ WINS サーバの IP アドレスを指定します。または WINS サーバの使用を禁止します。

（注）　IPSec NAT-T 接続は、Cisco ASA 5505 のホーム VLAN 上でサポートされる唯一の IPSec 接続タイプです。IPSec over TCP およびネイティブ IPSec 接続はサポートされていません。

認証のオプション

ASA 5505 は、Easy VPN サーバ上に格納されたグループ ポリシーから取得する次の認証メカニズムをサポートします。次のリストは、Easy VPN ハードウェア クライアントでサポートされる認証オプションを示します。ただし、それらのオプションは Easy VPN サーバ上で設定する必要があります。

- セキュア ユニット認証（SUA、対話型ユニット認証とも呼ばれる）

vpnclient username Xauth コマンド（「自動 Xauth 認証の設定」（P.34-4）を参照）を無視し、ユーザにパスワードを入力して ASA 5505 を認証するように要求します。デフォルトでは、SUA はディセーブルになっています。グループ ポリシー コンフィギュレーション モードで **secure-unit-authentication enable** コマンドを使用して、SUA をイネーブルにすることができます。「セキュア ユニット認証の設定」（P.30-46）を参照してください。

- 個々のユーザ認証

  ASA 5505 の背後のユーザに対して、企業 VPN ネットワークにアクセスする前に認証を要求します。デフォルトでは、IUA はディセーブルになっています。グループ ポリシー コンフィギュレーション モードで **user-authentication enable** コマンドを使用して、IUA をイネーブルにすることができます。「ユーザ認証の設定」（P.30-46）を参照してください。

  セキュリティ アプライアンスは NAT デバイスの背後から正常に動作していて、また、ASA 5505 が NAT モードに設定されている場合、（すべての PAT のクライアントに）プロビジョニングされた IP は中央サイトのデバイス上のルーティング テーブルに挿入されます。

注意　1 つの NAT デバイスがサーバと Easy VPN ハードウェア クライアントの間で動作している場合、Easy VPN サーバとして設定された Cisco ASA 5505 上に IUA を設定しないでください。

Easy VPN サーバがクライアントのアクセスを終了した後のアイドル タイムアウト時間を設定または削除するには、**user-authentication-idle-timeout** コマンドを使用します。「アイドル タイムアウトの設定」（P.30-47）を参照してください。

- HTTP リダイレクションによる認証

  Cisco Easy VPN サーバは HTTP トラフィックを代行受信し、次のいずれかが真の場合、ユーザをログイン ページにリダイレクトします。

  - SUA またはユーザ名とパスワードが、Easy VPN ハードウェア クライアント上で設定されていない。
  - IAU がイネーブルになっている。

  HTTP リダイレクションが自動で、Easy VPN サーバ上のコンフィギュレーションが必要ない。

- 事前共有キー、デジタル証明書、トークン、非認証

  ASA 5505 は、ユーザ認証で、事前共有キー、トークンベース（SDI ワンタイム パスワードなど）、および「非ユーザ認証」をサポートしています。（注）Cisco Easy VPN サーバでは、ユーザ認証の一環としてデジタル証明書を使用できます。手順については、第 27 章「IPsec と ISAKMP の設定」を参照してください。