拡張認証を備えたリモート VPN サーバとしての PIX/ASA の CLI と ASDM を使用した設定例

目次

概要

このドキュメントでは、Adaptive Security Device Manager（ASDM）か CLI を使用して、リモート VPN サーバとして機能するように Cisco 5500 シリーズ Adaptive Security Appliance（ASA）を設定する方法について説明しています。 ASDM では、直感的で使用が容易な Web ベースの管理インターフェイスにより、ワールドクラスのセキュリティ管理と監視機能が提供されています。 Cisco ASA の設定が完了すると、Cisco VPN Client を使用して、これを確認できます。

Cisco VPN Client（4.x for Windows）と PIX 500 シリーズ セキュリティ アプライアンス 7.x との間にリモート アクセス VPN 接続を設定する方法については、「PIX/ASA 7.x および Cisco VPN Client 4.x で Active Directory に対する Windows 2003 IAS RADIUS 認証を使用するための設定例」を参照してください。 リモートの VPN Client ユーザは Microsoft Windows 2003 Internet Authentication Service（IAS）RADIUS サーバを使用して Active Directory に対する認証を行います。

Cisco Secure Access Control Server（ACS バージョン 3.2）を使用して拡張認証（Xauth）用に、Cisco VPN Client（4.x for Windows）と PIX 500 シリーズ セキュリティ アプライアンス 7.x との間にリモート アクセス VPN 接続を設定する方法については、「PIX/ASA 7.x と Cisco VPN Client 4.x の Cisco Secure ACS 認証用の設定例」を参照してください。

前提条件

要件

このドキュメントでは、ASA が完全に動作していて、Cisco ASDM か CLI で設定を変更できるように設定されていることを想定しています。

注: 「ASDM 用の HTTPS アクセスの許可」または「PIX/ASA 7.x： 内部および外部インターフェイスの SSH の設定例」を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 適応型セキュリティ アプライアンス ソフトウェア バージョン 7.x 以降
- Adaptive Security Device Manager バージョン 5.x 以降
- Cisco VPN Client バージョン 4.x 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

関連製品

この設定は、Cisco PIX セキュリティ アプライアンス バージョン 7.x 以降にも適用できます。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

リモート アクセス設定により、モバイル ユーザなどの Cisco VPN Client にセキュアなリモート アクセスが提供されます。 リモート アクセス VPN により、リモート ユーザが中央のネットワーク リソースに安全にアクセスできるようになります。 Cisco VPN Client は IPSec プロトコルに準拠しており、特にセキュリティ アプライアンスと連動する設計になっています。 一方、セキュリティ アプライアンスは、多様なプロトコルに準拠するクライアントと IPSec 接続を確立できます。 IPSec についての詳細は、『ASA 設定ガイド』を参照してください。

グループとユーザは、VPN のセキュリティの管理とセキュリティ アプライアンスの設定では中心となる概念です。 これらにより、ユーザによる VPN へのアクセスと使用を決定する属性が指定されます。 グループはユーザの集合で、単一のエンティティとして扱われます。 ユーザは自身の属性をグループのポリシーから取得します。 トンネル グループでは、具体的な接続のグループ ポリシーが識別されます。 特定のグループ ポリシーをユーザに割り当てない場合は、その接続のデフォルト グループ ポリシーが適用されます。

トンネル グループは、トンネル接続のポリシーを決定するレコードのセットで構成されています。 これらのレコードにより、トンネルのユーザが認証されるサーバが判別され、さらに、接続情報が送信されるアカウンティング サーバが存在する場合は、これも判別されます。 接続のデフォ

ルトのグループ ポリシーも識別されます。レコードには、プロトコル固有の接続パラメータも含まれています。 トンネル グループには、トンネル自体の作成に適切な属性が少数含まれています。 トンネル グループには、ユーザ指向の属性を定義するグループ ポリシーに対するポインタが含まれています。

注: このドキュメントのサンプル設定では、認証にローカル ユーザ アカウントが使用されています。 LDAP と RADIUS のような他のサービスを使用する場合は、『認可と認証用の外部 RADIUS サーバの設定』を参照してください。

Internet Security Association and Key Management Protocol（ISAKMP）、別名 IKE はホストどうしが IPSec セキュリティ アソシエーションの構築方法について同意を行うネゴシエーション プロトコルです。 各 ISAKMP ネゴシエーションは、Phase1 と Phase2 の 2 つのセクションに分けられます。 Phase1 では、以降の ISAKMP ネゴシエーション メッセージを保護するための最初のトンネルが作成されます。 Phase2 では、セキュアな接続で送信されるデータを保護するトンネルが作成されます。 ISAKMP についての詳細は、『CLI コマンドのための ISAKMP ポリシーのキーワード』を参照してください。

設定

リモート VPN サーバとしての PIX/ASA の ASDM を使用した設定

ASDM を使用して Cisco ASA をリモート VPN サーバとして設定するには、次の手順を実行します。

1. Home ウィンドウで、**Wizards > VPN Wizard** の順に選択します。
2. **Remote Access** VPN Tunnel Type を選択して、VPN Tunnel Interface が意図どおりに設定されていることを確認します。
3. 利用可能な唯一の VPN Client Type がすでに選択されています。 [Next] をクリックします。
4. Tunnel Group Name の名前を入力します。 使用する認証方式を入力します。この例では **Pre-shared Key** が選択されています。**注:** ASDM では、事前共有キーを非表示にしたり、暗号化したりする方法はありません。 この理由は、ASDM を使用するのは ASA を設定する担当者か、この設定でカスタマーをサポートする担当者に限定されるためです。
5. リモート ユーザの認証用にローカル ユーザのデータベースか外部 AAA サーバ グループを選択します。**注:** ステップ 6 で、ローカル ユーザのデータベースにユーザを追加します。**注:** ASDM で外部 AAA サーバ グループを設定する方法についての詳細は、『PIX/ASA 7.x：ASDM での VPN ユーザの認証と認可のサーバ グループの設定例』を参照してください。
6. 必要な場合は、ローカル データベースにユーザを追加します。**注:** このウィンドウで既存のユーザを削除しないようにしてください。 データベースの既存のエントリを編集するか、データベースから既存のエントリを削除するには、**Configuration > Device Administration > Administration > User Accounts in the main ASDM window** の順に選択します。
7. 接続時にリモート VPN クライアントにダイナミックに割り当てられるローカル アドレスのプールを定義します。
8. *オプション：* DNS と WINS のサーバ情報、およびリモート VPN Client にプッシュするデフォルトのドメイン名を指定します。
9. IKE のパラメータを指定します。これは IKE フェーズ 1 とも呼ばれます。トンネルの両側の設定は完全に一致している必要があります。 ただし、Cisco VPN Client では適切な設定が自動的に選択されます。 そのため、クライアント PC で IKE を設定する必要はありません。
10. IPSec のパラメータを指定します。これは IKE Phase 2 とも呼ばれます。トンネルの両側

の設定は完全に一致している必要があります。 ただし、Cisco VPN Client では適切な設定が自動的に選択されます。 そのため、クライアント PC で IKE を設定する必要はありません。

11. リモート VPN ユーザに公開するホストやネットワークが存在する場合は、これを指定します。このリストを空白にしておくと、リモート VPN ユーザは ASA の Inside ネットワーク全体にアクセスできることになります。このウィンドウでは、スプリット トンネリングを有効にすることもできます。 スプリット トンネリングでは、ここまでで指定したリソースへのトラフィックは暗号化されますが、一般にインターネットに対してはトラフィックのトンネル化は行われず、非暗号化アクセスが行われます。 スプリット トンネリングが *有効にされていない* 場合、リモート VPN ユーザからのすべてのトラフィックは ASA に対してトンネリングされます。 この場合、設定によっては、帯域幅とプロセッサへの負荷が増大する可能性があります。
12. このウィンドウにはユーザが行った操作の概要が表示されます。 設定に問題がなければ、[Finish] をクリックします。

リモート VPN サーバとしての PIX/ASA の CLI を使用した設定

次の手順を実行して、コマンドラインからリモート VPN Access Server を設定します。 使用する各コマンドについての詳細は、『リモート アクセス VPN の設定』または『Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス、コマンド リファレンス』を参照してください。

1. VPN リモート アクセス トンネルに使用する IP アドレス プールを設定するには、グローバル設定モードで **ip local pool** コマンドを入力します。 アドレス プールを削除するには、このコマンドの no 形式を発行します。セキュリティ アプライアンスでは、接続用のトンネル グループに基づいたアドレス プールが使用されます。 トンネル グループ用に複数のアドレス プールを設定すると、セキュリティ アプライアンスでは、設定されている順序でアドレス プールが使用されます。 次のコマンドを発行して、リモートアクセスの VPN クライアントへのダイナミック アドレスの割り当てに使用できるローカル アドレスのプールを作成します。`ASA-AIP-CLI(config)#`**`ip local pool vpnpool 172.16.1.100-172.16.1.199 mask 255.255.255.0`**
2. 次のコマンドを発行します。`ASA-AIP-CLI(config)#`**`username marty password 12345678`**
3. 具体的なトンネルを設定するには、次の一連のコマンドを発行します。ASA-AIP-CLI(config)**#isakmp policy 1 authentication pre-share**ASA-AIP-CLI(config)**#isakmp policy 1 encryption 3des**ASA-AIP-CLI(config)**#isakmp policy 1 hash sha**ASA-AIP-CLI(config)**#isakmp policy 1 group 2**ASA-AIP-CLI(config)**#isakmp policy 1 lifetime 43200**ASA-AIP-CLI(config)**#isakmp enable outside**ASA-AIP-CLI(config)**#crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac**ASA-AIP-CLI(config)**#crypto dynamic-map outside_dyn_map 10 set transform-set ESP-3DES-SHA**ASA AIPCLI (config) #crypto **ダイナミック マップ outside_dyn_map 10 セット反転ルート**ASA-AIP-CLI(config)**#crypto dynamic-map outside_dyn_map 10 set security-association lifetime seconds 288000**ASA AIPCLI (config) #crypto **マップ outside_map 10 ipsecisakmp ダイナミック outside_dyn_map**ASA-AIP-CLI(config)**#crypto map outside_map interface outside**ASA-AIP-CLI(config)**#crypto isakmp nat-traversal**
4. *オプション：* インターフェイスに適用されているアクセスリストを接続で迂回させるには、次のコマンドを発行します。`ASA-AIP-CLI(config)#`**`sysopt connection permit-ipsec`** **注:** このコマンドが有効なのは、7.2(2) よりも前の 7.x イメージです。 7.2(2) のイメージを使用している場合は、ASA-AIP-CLI(config)#sysopt connection permit-vpn コマンドを発行します。
5. 次のコマンドを発行します。`ASA-AIP-CLI(config)#`**`group-policy hillvalleyvpn internal`**

6. クライアント接続を設定するには、次のコマンドを発行します。ASA-AIP-CLI(config)#**group-policy hillvalleyvpn attributes**ASA-AIP-CLI(config)#(config-group-policy)#**dns-server value 172.16.1.11**ASA-AIP-CLI(config)#(config-group-policy)#**vpn-tunnel-protocol IPSec**ASA-AIP-CLI(config)#(config-group-policy)#**default-domain value test.com**
7. 次のコマンドを発行します。ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-ra**
8. 次のコマンドを発行します。ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn ipsec-attributes**
9. 次のコマンドを発行します。ASA-AIP-CLI(config-tunnel-ipsec)#**pre-shared-key cisco123**
10. 次のコマンドを発行します。ASA-AIP-CLI(config)#**tunnel-group hillvalleyvpn general-attributes**
11. 認証用にローカル ユーザ データベースを参照するには、次のコマンドを発行します。ASA-AIP-CLI(config-tunnel-general)#**authentication-server-group LOCAL**
12. グループ ポリシーをトンネル グループに関連付けます。ASA-AIP-CLI(config-tunnel-ipsec)#**default-group-policy hillvalleyvpn**
13. ステップ 1 で作成された vpnpool を hillvalleyvpn グループに割り当てるには、hillvalleyvpn トンネルグループの general-attributes モードで次のコマンドを発行します。ASA-AIP-CLI(config-tunnel-general)#**address-pool vpnpool**

ASA デバイスでの設定の実行

```
ASA-AIP-CLI(config)#show running-config ASA Version
7.2(2) ! hostname ASAwAIP-CLI domain-name corp.com
enable password WwXYvtKrnjXqGbu1 encrypted names !
interface Ethernet0/0 nameif outside security-level 0 ip
address 10.10.10.2 255.255.255.0 ! interface Ethernet0/1
nameif inside security-level 100 ip address 172.16.1.2
255.255.255.0 ! interface Ethernet0/2 shutdown no nameif
no security-level no ip address ! interface Ethernet0/3
shutdown no nameif no security-level no ip address !
interface Management0/0 shutdown no nameif no security-
level no ip address ! passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive dns server-group DefaultDNS domain-name
corp.com pager lines 24 mtu outside 1500 mtu inside 1500
ip local pool vpnpool 172.16.1.100-172.16.1.199 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 no asdm history enable arp timeout 14400
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
group-policy hillvalleyvpn1 internal group-policy
hillvalleyvpn1 attributes dns-server value 172.16.1.11
vpn-tunnel-protocol IPSec default-domain value test.com
username marty password 6XmYwQOO9tiYnUDN encrypted no
snmp-server location no snmp-server contact snmp-server
enable traps snmp authentication linkup linkdown
coldstart crypto ipsec transform-set ESP-3DES-SHA esp-
3des esp-sha-hmac crypto dynamic-map outside_dyn_map 10
set transform-set ESP-3DES-SHA crypto dynamic-map
outside_dyn_map 10 set security-association lifetime
seconds 288000 crypto map outside_map 10 ipsec-isakmp
dynamic outside_dyn_map crypto map outside_map interface
outside crypto isakmp enable outside crypto isakmp
policy 10 authentication pre-share encryption 3des hash
sha group 2 lifetime 86400 crypto isakmp nat-traversal
20 tunnel-group hillvalleyvpn type ipsec-ra tunnel-group
hillvalleyvpn general-attributes address-pool vpnpool
default-group-policy hillvalleyvpn tunnel-group
hillvalleyvpn ipsec-attributes pre-shared-key * telnet
timeout 5 ssh timeout 5 console timeout 0 ! class-map
```

```
inspection_default match default-inspection-traffic ! !
policy-map type inspect dns preset_dns_map parameters
message-length maximum 512 policy-map global_policy
class inspection_default inspect dns preset_dns_map
inspect ftp inspect h323 h225 inspect h323 ras inspect
netbios inspect rsh inspect rtsp inspect skinny inspect
esmtp inspect sqlnet inspect sunrpc inspect tftp inspect
sip inspect xdmcp ! service-policy global_policy global
prompt hostname context
Cryptochecksum:0f78ee7ef3c196a683ae7a4804ce1192 : end
ASA-AIP-CLI(config)#
```

Cisco VPN Client Password Storage の設定

膨大な Cisco VPN Client を導入している場合、すべての VPN Client のユーザ名とパスワードを把握しておくのは非常に困難です。 VPN Client マシンにパスワードを保存するには、ASA/PIX と VPN Client をこのセクションで説明されているように設定します。

ASA/PIX

次のように、グローバル設定モードで **group-policy attributes** コマンドを使用します。

```
group-policy VPNusers attributes password-storage enable
```

Cisco VPN クライアント

.pcf file を編集して、次のパラメータを変更します。

```
SaveUserPassword=1 UserPassword= <type your password>
```

拡張認証をディセーブルにする

拡張認証をディセーブルにするには、tunnel group モードで次のコマンドを入力します。 PIX/ASA 7.x では、これはデフォルトでイネーブルにされています。

```
asa(config)#tunnel-group client ipsec-attributes asa(config-tunnel-ipsec)#isakmp ikev1-user-authentication none
```

拡張認証をディセーブルにすると、VPN Client では認証（Xauth）用のユーザ名/パスワードがポップアップ表示されなくなります。 このため、ASA/PIX では、VPN Client を認証するのにユーザ名とパスワードの設定が不要になります。

確認

ASA の設定に成功したことを確認するには、Cisco VPN Client を使用して Cisco ASA に接続してみます。

1. **Connection Entries > New** の順に選択します。
2. 新しい接続の詳細情報を入力します。Host フィールドには、設定済みの Cisco ASA の IP アドレスかホスト名が含まれている必要があります。 グループ 認証情報はステップ 4.で使用されるそれに終了したら『SAVE』 をクリック します対応する必要があります。
3. 新しく作成した接続を選択し、**Connect** をクリックします。
4. 拡張認証用のユーザ名とパスワードを入力します。 この情報はステップ 5 と 6 で指定されたものと一致している必要があります。

5. 接続が正常に確立されたら、Status メニューから **Statistics** を選択し、トンネルの詳細情報を確認します。次のウィンドウには、トラフィックと暗号の情報が表示されています。次のウィンドウには、スプリット トンネリング情報が表示されています。

トラブルシューティング

ここでは、設定に関するトラブルシューティングについて説明します。

誤った暗号化 ACL

ASDM 5.0(2) では、スプリット トンネリングを使用する VPN Client、および、network-extension モードのハードウェア クライアントに問題を発生させる暗号化 Access Control List（ACL）が作成され、適用されることが判明しています。 この問題を回避するには、ASDM バージョン 5.0(4.3) 以降を使用してください。 詳細は、Cisco Bug ID CSCsc10806（ ）を参照してください。

関連情報

- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- 一般的な L2L およびリモート アクセス IPSec VPN のトラブルシューティング方法について
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス（ASA）のトラブルシューティングとアラート
- テクニカルサポートとドキュメント - Cisco Systems