ASDM を使用した ASA での SSL VPN Client（SVC）の設定例

目次

概要

Secure Socket Layer（SSL）Virtual Private Network（VPN; バーチャル プライベート ネットワーク）テクノロジーを使用すると、次の方法のいずれかを使用して、あらゆる場所から企業ネットワークに安全に接続できます。

- **クライアントレス SSL VPN（WebVPN）**：企業のローカル エリア ネットワーク（LAN）上の HTTP サーバまたは HTTPS Web サーバへアクセスする際に SSL 対応の Web ブラウザが必要となるリモート クライアントです。 また、クライアントレス SSL VPN は、Common Internet File System（CIFS）プロトコルによる Windows ファイル ブラウジングへのアクセスも提供します。 Outlook Web Access（OWA）は、HTTP アクセスの一例です。クライアントレス SSL VPN の詳細は、『ASA でのクライアントレス SSL VPN（WebVPN）の設定例』を参照してください。
- **シンクライアント SSL VPN（ポート転送）**：小規模な Java ベースのアプレットをダウンロードし、スタティックなポート番号を使用する Transmission Control Protocol（TCP; 伝送制御プロトコル）アプリケーションのセキュアなアクセスを可能にするリモート クライアントです。 Post Office Protocol（POP3）、Simple Mail Transfer Protocol（SMTP）、Internet Message Access Protocol（IMAP）、Secure Shell（ssh; セキュア シェル）、および Telnet は、セキュアなアクセスの例です。 ローカル マシン上のファイルが変更されるため、この方法を使用するには、ユーザにローカル管理者特権が必要です。 SSL VPN のこの方法は、一部の File Transfer Protocol（FTP; ファイル転送プロトコル）アプリケーションなど、ダイナミックなポート割り当てを使用するアプリケーションでは使用できません。クライアントレス SSL VPN の詳細については、『ASDM を使った ASA でのシンクライアント SSL VPN（WebVPN）の設定例』を参照してください。**注:** User Datagram Protocol（UDP; ユーザ データグラム プロトコル）はサポートされていません。
- **SSL VPN Client（トンネル モード）**：リモート ワークステーションに小規模なクライアントをダウンロードし、社内ネットワーク上のリソースへの完全なセキュア アクセスを可能にします。 SSL VPN Client（SVC; SSL VPN クライアント）をリモート ワークステーションへ永続的にダウンロードすることも、セキュアなセッションが閉じられた後にクライアントを削除することもできます。

このドキュメントでは、Adaptive Security Device Manager（ASDM）を使用して、Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）で SVC を設定する方法について説明します。 この設定によってコマンドラインに表示される内容は、「結果」の項に示します。

前提条件

要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

- 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 7.1.x 以降では SVC がサポートされています。
- すべてのリモート ワークステーション上でのローカルな管理者権限
- リモート ワークステーションでの Java コントロールおよび ActiveX コントロール
- 接続パス上のどの場所でも、ポート 443 がブロックされていないこと

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 Adaptive Security Appliance Software Version 7.2(1)
- Cisco Adaptive Security Device Manager 5.2(1)

- Cisco 適応型セキュリティ アプライアンス 5510 シリーズ
- Microsoft Windows XP Professional SP 2

このドキュメントに記載されている情報は、ラボ環境で作成されたものです。 このドキュメントで使用されるデバイスはすべてデフォルト設定にリセットされました。 対象のネットワークが実稼動中である場合には、どのような作業についても、その潜在的な影響について確実に理解しておく必要があります。 この設定で使用される IP アドレスはすべてラボ環境の RFC 1918 アドレスから選択されました。 これらの IP アドレスはインターネット上でルーティングできず、テスト専用です。

ネットワーク図

このドキュメントでは、このセクションで示すネットワーク設定を使用しています。

リモート ユーザは SSL 対応の Web ブラウザを使用して ASA の IP アドレスに接続します。 認証が成功した後、クライアント コンピュータに SVC をダウンロードします。ユーザは社内ネットワーク上のアクセスが許可されているすべてのリソースに対して、暗号化されたセキュア セッションを使用して完全なアクセスを行えます。

設定前の作業

開始する前に、次の作業を実行してください。

- ASA を ASDM で設定できるようにするには、『ASDM 用の HTTPS アクセスの許可』を参照してください。ASDM アプリケーションにアクセスするには、管理ステーションから SSL 対応の Web ブラウザを使用して ASA デバイスの IP アドレスを入力します。 次に、例を示します。 **https://*inside_ip_address*** ここで *inside_ip_address* は ASA のアドレスです。 ASDM がロードされれば、SVC の設定を開始できます。
- シスコのソフトウェア ダウンロード（登録ユーザ専用）Web サイトから、ASDM アプリケーションにアクセスする管理ステーションローカル ハードドライブに、SSL VPN クライアント パッケージ（sslclient-win*.pkg）をダウンロードします。

WebVPN と ASDM は、ポート番号を変更しない限り、同じ ASA インターフェイス上では有効にできません。 これら 2 つのテクノロジーを同じデバイスの同じポート（ポート 443）で使用する場合は、*inside インターフェイス*では ASDM をイネーブルにし、*outside インターフェイス*では WebVPN をイネーブルにします。

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。

ASA での SSL VPN クライアントの設定

ASA での SSL VPN クライアントを設定するには、次の手順を実行します。

1. ASA で WebVPN アクセスをイネーブルにする
2. ASA に SSL VPN クライアントをインストールし、イネーブルにする
3. クライアントにインストールした SVC をイネーブルにする
4. キーの再生成パラメータをイネーブルにする

手順 1：ASA で WebVPN アクセスをイネーブルにする

ASA で WebVPN アクセスをイネーブルにするには、次の手順を実行します。

1. ASDM アプリケーション内で [Configuration] をクリックし、次に [VPN] をクリックします。
2. [WebVPN] を展開して、[WebVPN Access] を選択します。
3. WebVPN をイネーブルにするインターフェイスを選択して、Enable をクリックします。

手順 2：ASA に SSL VPN クライアントをインストールし、イネーブルにする

ASA に SSL VPN クライアントをインストールしてイネーブルにするには、次の手順を実行します。

1. [Configuration] をクリックし、次に [VPN] をクリックします。
2. ナビゲーション ペインで [WebVPN] を展開し、[SSL VPN Client] を選択します。
3. [Add] をクリックします。Add SSL VPN Client Image ダイアログ ボックスが表示されます。
4. [Upload] ボタンをクリックします。Upload Image ダイアログ ボックスが表示されます。
5. [Browse Local Files] ボタンをクリックして、ローカル コンピュータにあるファイルを指定するか、[Browse Flash] ボタンをクリックして、フラッシュ ファイル システムにあるファイルを指定します。
6. アップロードするクライアント イメージ ファイルを指定して、[OK] をクリックします。
7. [Upload File] をクリックした後に、[Close] をクリックします。
8. クライアント イメージがフラッシュにロードされたら、**Enable SSL VPN Client** チェック ボックスにチェックマークを入れてから、**Apply** をクリックします。**注:** エラー メッセージが表示された場合は、WebVPN アクセスがイネーブルになっていることを確認してください。 ナビゲーション ペインで [WebVPN] を展開し、[WebVPN Access] を選択します。 アクセスを設定するインターフェイスを選択して、[Enable] をクリックします。
9. [Save] をクリックし、[Yes] をクリックして変更を確定します。

手順 3：クライアントにインストールした SVC をイネーブルにする

クライアントにインストールした SVC をイネーブルにするには、次の手順を実行します。

1. ナビゲーション ペインで [IP Address Management] を展開し、[IP Pools] を選択します。
2. [Add] をクリックし、[Name]、[Starting IP Address]、[Ending IP Address]、および [Subnet Mask] の各フィールドに値を入力します。 Starting IP Address と Ending IP Address のフィールドに入力した IP アドレスは、内部ネットワークのサブネットに含まれている必要があります。
3. [OK] をクリックして、[Apply] をクリックします。
4. [Save] をクリックし、[Yes] をクリックして変更を確定します。
5. ナビゲーション ペインで [IP Address Management] を展開し、[Assignment] を選択します。
6. [Use internal address pools] チェック ボックスをオンにし、次に [Use authentication server] チェック ボックスと [Use DHCP] チェック ボックスをオフにします。
7. [Apply] をクリックします。
8. [Save] をクリックし、[Yes] をクリックして変更を確定します。

9. ナビゲーション ペインで [General] を展開し、[Tunnel Group] を選択します。
10. 管理するトンネル グループを選択して、[Edit] をクリックします。
11. [Client Address Assignment] タブをクリックして、新しく作成した IP アドレス プールを [Available Pools] リストから選択します。
12. [Add] をクリックし、次に [OK] をクリックします。
13. ASDM アプリケーションのウィンドウで、[Apply] をクリックします。
14. [Save] をクリックし、[Yes] をクリックして変更を確定します。

手順 4：キーの再生成パラメータをイネーブルにする

キーの再生成パラメータをイネーブルにするには、次の手順を実行します。

1. ナビゲーション ペインで [General] を展開し、[Group Policy] を選択します。
2. このグループのクライアントに適用するポリシーを選択して、[Edit] をクリックします。
3. [General] タブで、[Tunneling Protocols Inherit] チェック ボックスをオフにし、[WebVPN] チェック ボックスをオンにします。
4. [WebVPN] タブをクリックし、[SSLVPN Client] タブをクリックして、次のオプションを選択します。[Use SSL VPN Client] オプションで、[Inherit] チェック ボックスをオフにし、[Optional] オプション ボタンをクリックします。これを選択すると、リモート クライアントが SVC をダウンロードするかどうかを選択できるようになります。 [Always] を選択すると、SSL VPN 接続のたびにリモート ワークステーションに SVC がダウンロードされるようになります。[Keep Installer on Client System] オプションについては、**[Inherit]** チェック ボックスのチェックマークを外して、**[Yes]** オプション ボタンをクリックします。この操作によって、SVC ソフトウェアはクライアント マシン上に留まります。 これにより、ASA は接続が確立するたびに SVC ソフトウェアをクライアントにダウンロードする必要がなくなります。 このオプションは、社内ネットワークに頻繁にアクセスするリモート ユーザが選択するのに適しています。[Renegotiation Interval] オプションで、[Inherit] チェック ボックスをオフにし、[Unlimited] チェック ボックスをオフにし、キーの再生成が行われるまでの時間（分）を入力します。セキュリティは、キーが有効である時間に制限を設けることで強化されます。[Renegotiation Method] オプションで、[Inherit] チェック ボックスをオフにして、[SSL] オプション ボタンをクリックします。 再ネゴシエーションは、現在の SSL トンネルまたは再ネゴシエーション用に明示的に作成された新しいトンネルを使用できます。SSL VPN クライアントの属性は次の図で示すように設定することになります。
5. [OK] をクリックして、[Apply] をクリックします。
6. [Save] をクリックし、[Yes] をクリックして変更を確定します。

結果

ASDM は次のコマンドライン設定を作成します。

ciscoasa

```
ciscoasa(config)#show run
ASA Version 7.2(1)
!
hostname ciscoasa
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
```

```
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask
255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 1
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 Statements group-policy GroupPolicy1
internal group-policy GroupPolicy1 attributes vpn-
tunnel-protocol IPSec l2tp-ipsec webvpn !--- Enable the
SVC for WebVPN webvpn svc enable svc keep-installer
installed svc rekey time 30 svc rekey method ssl !
username cisco password 53QNetqK.Kqqfshe encrypted
privilege 15 ! http server enable http 10.2.2.0
255.255.255.0 inside ! no snmp-server location no snmp-
server contact snmp-server enable traps snmp
authentication linkup linkdown coldstart !--- Tunnel
Group and Group Policy using the defaults here tunnel-
group DefaultWEBVPNGroup general-attributes address-pool
CorporateNet default-group-policy GroupPolicy1 ! no vpn-
addr-assign aaa no vpn-addr-assign dhcp ! telnet timeout
5 ssh 172.22.1.0 255.255.255.0 outside 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 rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp !
service-policy global_policy global !--- Enable webvpn
and the select the SVC client webvpn enable outside svc
```

```
image disk0:/sslclient-win-1.1.1.164.pkg 1 svc enable !-
-- Provide list for access to resources url-list
ServerList "E-Commerce Server1" http://10.2.2.2 1 url-
list ServerList "BrowseServer" cifs://10.2.2.2 2 tunnel-
group-list enable prompt hostname context
Cryptochecksum:80a1890a95580dca11e3aee200173f5f : end
```

設定のカスタマイズ

「ASA での SSL VPN クライアントの設定」で説明する手順では、次の図に示すグループ ポリシーの ASA デフォルト名（*GroupPolicy1*）とトンネル グループのデフォルト名（*DefaultWebVPNGroup*）を使用します。

この手順では、組織のセキュリティ ポリシーに従って、独自のカスタム グループ ポリシーとトンネル グループを作成し、これらをリンクさせる方法について説明します。

設定のカスタマイズを行うには、次のステップを実行します。

1. カスタム グループ ポリシーの作成
2. カスタム トンネル グループの作成
3. ユーザの作成とそのユーザのカスタム グループ ポリシーへの追加

手順 1：カスタム グループ ポリシーの作成

カスタム グループ ポリシーを作成するには、次の手順を実行します。

1. [Configuration] をクリックし、次に [VPN] をクリックします。
2. [General] を展開して、[Group Policy] を選択します。
3. [Add] をクリックして、[Internal Group Policy] を選択します。
4. Name フィールドにグループ ポリシーの名前を入力します。この例では、グループ ポリシーの名前を *SalesGroupPolicy* に変更しています。
5. [General] タブで、[Tunneling Protocols Inherit] チェック ボックスをオフにし、[WebVPN] チェック ボックスをオンにします。
6. [WebVPN] タブをクリックし、[SSLVPN Client] タブをクリックします。このダイアログ ボックスでは、SSL VPN クライアントの動作も選択できます。
7. [OK] をクリックして、[Apply] をクリックします。
8. [Save] をクリックし、[Yes] をクリックして変更を確定します。

手順 2：カスタム トンネル グループの作成

カスタム トンネル グループを作成するには、次の手順を実行します。

1. [Configuration] ボタンをクリックし、次に [VPN] をクリックします。
2. [General] を展開して、[Tunnel Group] を選択します。
3. **[Add]** をクリックし、**[WebVPN Access]** を選択します。
4. Name フィールドにトンネル グループの名前を入力します。この例では、トンネル グループの名前を *SalesForceGroup* に変更しています。
5. [Group Policy] ドロップダウン矢印をクリックし、新しく作成したグループ ポリシーを選択します。これでグループ ポリシーとトンネル グループがリンクされました。

6. [Client Address Assignment] タブをクリックして、DHCP サーバの情報を入力するか、ローカルに作成されている IP アドレス プールから選択します。
7. [OK] をクリックして、[Apply] をクリックします。
8. [Save] をクリックし、[Yes] をクリックして変更を確定します。

手順 3：ユーザの作成とそのユーザのカスタム グループ ポリシーへの追加

ユーザを作成し、そのユーザをカスタム グループ ポリシーに追加するには、次の手順を実行します。

1. [Configuration] をクリックし、次に [VPN] をクリックします。
2. [General] を展開して、[Users] を選択します。
3. [Add] をクリックして、ユーザ名とパスワードを入力します。
4. [VPN Policy] タブをクリックします。 Group Policy フィールドに新しく作成したグループ ポリシーが表示されていることを確認します。このユーザは新しいグループ ポリシーの特性をすべて継承します。
5. [OK] をクリックして、[Apply] をクリックします。
6. [Save] をクリックし、[Yes] をクリックして変更を確定します。

確認

ここでは、設定が正常に動作していることを確認します。

認証

SSL VPN クライアントの認証は、次の方法のいずれかを使用して行います。

- Cisco Secure ACS Server（Radius）
- NT ドメイン
- Active Directory
- ワンタイム パスワード
- デジタル証明書
- スマートカード
- ローカル AAA 認証

このドキュメントでは、ASA デバイスで作成されたローカルのアカウントを使用しています。

注: 適応型セキュリティ アプライアンスに同じ CA を共有するトラストポイントが複数ある場合、CA を共有するトラストポイントのうち、ユーザ証明書の検証に使用できるのは 1 つだけです。

設定

リモート クライアントを使用して ASA に接続するには、SSL 対応の Web ブラウザのアドレス フィールドに **https://ASA_outside_address** と入力します。 *ASA_outside_address* は ASA の外部 IP アドレスです。 設定が正常に行われると、Cisco Systems SSL VPN Client ウィンドウが表示されます。

注: Cisco Systems SSL VPN Client ウィンドウは、ASA からの認証を受け入れ、SSL VPN クライ

アントがリモート ステーションにダウンロードされた後に表示されます。 ウィンドウが表示されない場合は、ウィンドウが最小化されていないかどうか確認してください。

コマンド

いくつかの **show** コマンドは WebVPN に関連しています。 これらのコマンドをコマンドラインインターフェイス（CLI）で実行して、統計情報や他の情報を表示できます。 **show コマンド**の詳細については、『WebVPN 設定の確認』を参照してください。

注: Output Interpreter Tool（OIT）（登録ユーザ専用）では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

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。

SVC エラー

問題

認証中に、次のようなエラー メッセージを受信する場合があります。

```
ciscoasa(config)#show run
ASA Version 7.2(1)
!
hostname ciscoasa
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
```

```
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 1
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 Statements group-policy GroupPolicy1 internal group-policy GroupPolicy1
attributes vpn-tunnel-protocol IPSec l2tp-ipsec webvpn !--- Enable the SVC for WebVPN webvpn svc
enable svc keep-installer installed svc rekey time 30 svc rekey method ssl ! username cisco
password 53QNetqK.Kqqfshe encrypted privilege 15 ! http server enable http 10.2.2.0
255.255.255.0 inside ! no snmp-server location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart !--- Tunnel Group and Group Policy using the
defaults here tunnel-group DefaultWEBVPNGroup general-attributes address-pool CorporateNet
default-group-policy GroupPolicy1 ! no vpn-addr-assign aaa no vpn-addr-assign dhcp ! telnet
timeout 5 ssh 172.22.1.0 255.255.255.0 outside 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 rsh inspect rtsp
inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp ! service-policy global_policy global !--- Enable webvpn and the select the
SVC client webvpn enable outside svc image disk0:/sslclient-win-1.1.1.164.pkg 1 svc enable !---
Provide list for access to resources url-list ServerList "E-Commerce Server1" http://10.2.2.2 1
url-list ServerList "BrowseServer" cifs://10.2.2.2 2 tunnel-group-list enable prompt hostname
context Cryptochecksum:80a1890a95580dca11e3aee200173f5f : end
```

解決策

ファイアウォール サービスが PC で稼働している場合は、このサービスによって認証が中断している可能性があります。 サービスを停止し、クライアントを再接続します。

SVC によって ASA とのセキュアなセッションが確立されているかどうか

SSL VPN クライアントによって ASA とのセキュアなセッションが確立されているかどうかを確認するには、次の手順に従います。

1. [Monitoring] をクリックします。
2. [VPN Statistics] を展開し、[Sessions] を選択します。
3. [Filter By] ドロップダウン メニューから、[SSL VPN Client] を選択して、[Filter] ボタンをクリックします。設定がセッション リストに表示されます。

セキュアなセッションが確立されていて、正しく終端されているかどうか

リアルタイムのログを表示すると、セキュアなセッションが確立されていて、正しく終端されているかどうかを確認できます。 セッション ログを表示するには、次の手順に従ってください。

1. [Monitoring] をクリックし、次に [Logging] をクリックします。
2. [Real-time Log Viewer] または [Log Buffer] を選択し、次に [View] をクリックします。**注:** 特定のアドレスを持つセッションだけを表示するには、アドレスでフィルタリングします。

WebVPN プロファイルの IP プールの確認

```
ciscoasa(config)#show run
```

```
ASA Version 7.2(1)
!
hostname ciscoasa
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 1
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 Statements group-policy GroupPolicy1 internal group-policy GroupPolicy1
attributes vpn-tunnel-protocol IPSec l2tp-ipsec webvpn !--- Enable the SVC for WebVPN webvpn svc
enable svc keep-installer installed svc rekey time 30 svc rekey method ssl ! username cisco
password 53QNetqK.Kqqfshe encrypted privilege 15 ! http server enable http 10.2.2.0
255.255.255.0 inside ! no snmp-server location no snmp-server contact snmp-server enable traps
snmp authentication linkup linkdown coldstart !--- Tunnel Group and Group Policy using the
defaults here tunnel-group DefaultWEBVPNGroup general-attributes address-pool CorporateNet
default-group-policy GroupPolicy1 ! no vpn-addr-assign aaa no vpn-addr-assign dhcp ! telnet
timeout 5 ssh 172.22.1.0 255.255.255.0 outside 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 rsh inspect rtsp
inspect esmtp inspect sqlnet inspect skinny inspect sunrpc inspect xdmcp inspect sip inspect
netbios inspect tftp ! service-policy global_policy global !--- Enable webvpn and the select the
SVC client webvpn enable outside svc image disk0:/sslclient-win-1.1.1.164.pkg 1 svc enable !---
Provide list for access to resources url-list ServerList "E-Commerce Server1" http://10.2.2.2 1
url-list ServerList "BrowseServer" cifs://10.2.2.2 2 tunnel-group-list enable prompt hostname
context Cryptochecksum:80a1890a95580dca11e3aee200173f5f : end
```

SVC 接続への割り当てに使用できるアドレスがありません。 このため、プロファイルの IP プール アドレスを割り当てます。

新しい接続プロファイルを作成する場合は、この接続プロファイルにアクセスするためのエイリアスまたはグループ URL を設定します。 作成しない場合は、SSL の試行は IP プールが関連付けられていないすべてデフォルト WebVPN 接続プロファイルにヒットします。 デフォルト接続プロファイルを使用し、IP プールをこのプロファイルに追加するためにこのように設定します。

ヒント

- リモート クライアントに割り当てた IP アドレス プールを使用してルーティングが正しく動作していることを確認してください。 この IP アドレス プールは、使用している LAN のサブネットに属している必要があります。 また、IP アドレスの割り当てには DHCP サーバや認証サーバも使用できます。
- ASA ではデフォルトのトンネル グループ（*DefaultWebVPNGroup*）とデフォルトのグループ ポリシー（*GroupPolicy1*）が作成されます。 新しいグループとポリシーを作成した場合は、必ず使用しているネットワークのセキュリティ ポリシーに従って値を割り当てるようにしてください。
- CIFS による Windows ファイル ブラウジングをイネーブルにするには、[Configuration] > [VPN] > [WebVPN] > [Servers and URLs] で WINS（NBNS）サーバを入力します。 このテクノロジーでは CIFS の一部を使用しています。

コマンド

いくつかの **debug** コマンドは、WebVPN に関連しています。 これらのコマンドの詳細については、「WebVPN の Debug コマンドの使用」を参照してください。

注: debug コマンドを使用すると、Cisco デバイスに悪影響が及ぶ可能性があります。 **debug** コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

関連情報

- ASA でのクライアントレス SSL VPN（WebVPN）の設定例
- ASDM を使った ASA でのシンクライアント SSL VPN（WebVPN）の設定例
- ASDM および NTLMv1 を使用した WebVPN およびシングル サインオン機能付き ASA の設定例
- Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス
- テクニカル サポートとドキュメント – Cisco Systems