

ASA 8.x : ASA で AnyConnect VPN Client のスプリット トンネリングを許可するための設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[ASDM 6.0\(2\) を使用した ASA 設定](#)

[ASA CLI 設定](#)

[SVC との SSL VPN 接続の確立](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、Cisco Adaptive Security Appliance (ASA; 適応型セキュリティ アプライアンス) 8.0.2 にトンネリングされているときに、Cisco AnyConnect VPN クライアントのインターネットへのアクセスを許可する方法の段階的な手順を説明します。この設定では、スプリットトンネリングを使用したインターネットへのセキュアではないアクセスを提供する一方で、SSL 経由で社内のリソースへのクライアントのセキュアなアクセスが可能になります。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- ASA セキュリティ アプライアンスはバージョン 8.x を稼動する必要があります。
- Cisco AnyConnect VPN Client 2.x注: シスコの「[ソフトウェアダウンロード](#)」ページ ([登録ユーザ専用](#)) から、AnyConnect VPN Client パッケージ (anyconnect-win*.pkg) をダウンロードします。AnyConnect VPN Client を ASA のフラッシュ メモリにコピーします。これは、ASA との SSL VPN 接続を確立するためにリモート ユーザ コンピュータにダウンロードされます。詳細については、ASA のコンフィギュレーション ガイドの「[AnyConnect Client のインストール](#)」セクション (英語) 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。

- ソフトウェア バージョン 8.0(2) が稼働している Cisco 5500 シリーズ ASA
- Windows 2.0.0343 用のバージョンの Cisco AnyConnect SSL VPN Client
- Microsoft Installer バージョン 3.1 によって Microsoft Vista、Windows XP SP2、または Windows 2000 Professional SP4 が稼働している PC
- Cisco Adaptive Security Device Manager (ASDM) バージョン 6.0(2)

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。

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

Cisco AnyConnect VPN Client は、リモート ユーザのためにセキュリティ アプライアンスへのセキュアな SSL 接続を提供しています。以前にインストールしたクライアントがない場合、リモート ユーザは SSL VPN 接続を受け入れるように設定したインターフェイスのブラウザに IP アドレスを入力します。セキュリティ アプライアンスが http:// 要求を https:// にリダイレクトするように設定されていない場合、ユーザは https://<address> の形式で URL を入力する必要があります。

URL を入力した後、ブラウザは、そのインターフェイスに接続し、ログイン画面を表示します。ユーザがログインと認証を満たし、セキュリティ アプライアンスがそのユーザをクライアントを要求しているものと認識した場合、セキュリティ アプライアンスはリモート コンピュータのオペレーティング システムに一致するクライアントをダウンロードします。ダウンロード後、クライアントは自身をインストールして設定し、セキュアな SSL 接続を確立して、接続が終了したときに自身を残すか、アンインストールします (これは、セキュリティ アプライアンスの設定に従います)。

以前にインストールされているクライアントの場合、ユーザが認証を行うと、セキュリティ アプライアンスはクライアントのリビジョンを調査して、必要に応じてクライアントをアップグレードします。

クライアントは、セキュリティ アプライアンスと SSL VPN 接続をネゴシエートすると、Transport Layer Security (TLS) を使って接続し、オプションで Datagram Transport Layer Security (DTLS) に接続します。DTLS は、SSL 接続の一部に関連する遅延と帯域幅の問題を回避し、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスを向上させます。

AnyConnect クライアントは、セキュリティ アプライアンスからダウンロードすることも、システム管理者がリモートの PC に手動でインストールすることもできます。クライアントを手動でインストールする方法に関する詳細については [Cisco AnyConnect VPN Client 管理者ガイド](#)を参照して下さい。

セキュリティ アプライアンスは、グループ ポリシーや接続を確立するユーザのユーザ名属性に基づいてクライアントをダウンロードします。セキュリティ アプライアンスは、クライアントを自動的にダウンロードするように設定することも、クライアントをダウンロードするかどうかをユーザにプロンプトで表示してから設定することもできます。後者の場合、ユーザが応答しないときには、タイムアウト期間が経過した後にクライアントをダウンロードするか、ログイン ページを表示するか、いずれかを実行するようにセキュリティ アプライアンスを設定できます。

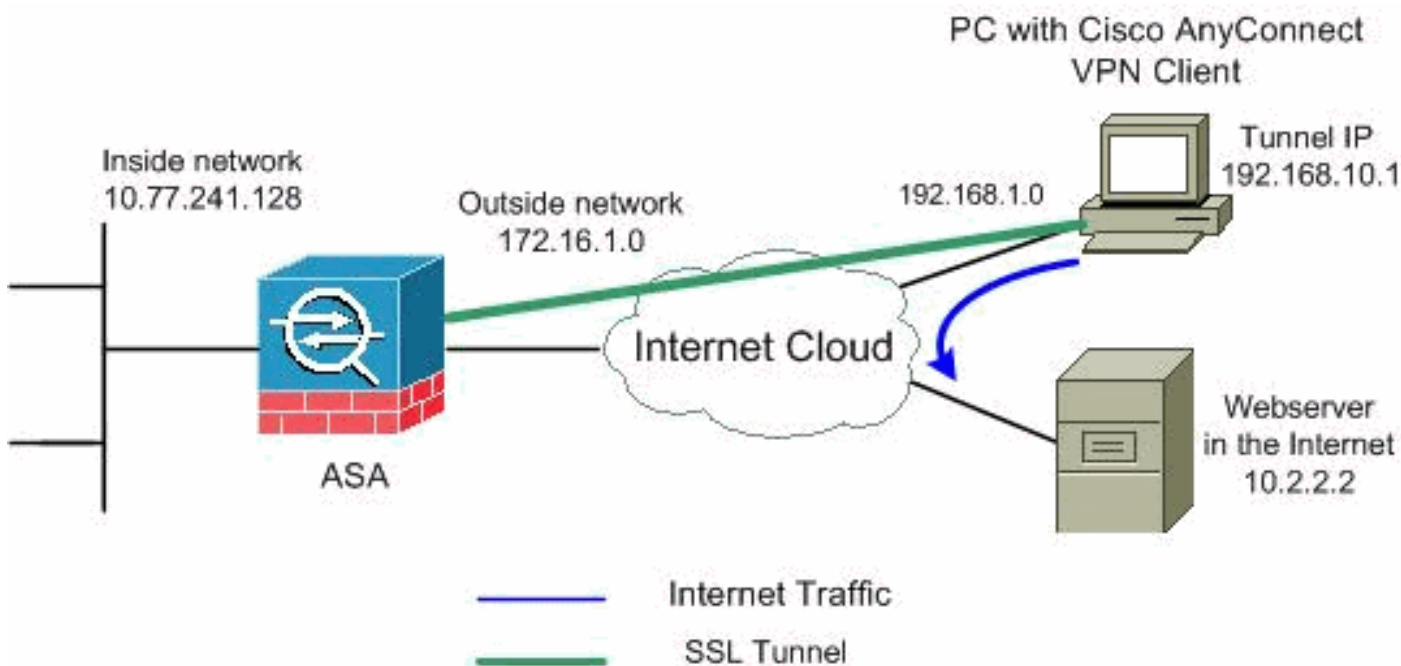
設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

注: このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) ([登録ユーザ専用](#)) を使用してください。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



注: この設定で使用している IP アドレススキームは、インターネット上で正式にルーティング可能なものではありません。これらは、ラボ環境で使用された [RFC 1918](#) のアドレスです。

[ASDM 6.0\(2\) を使用した ASA 設定](#)

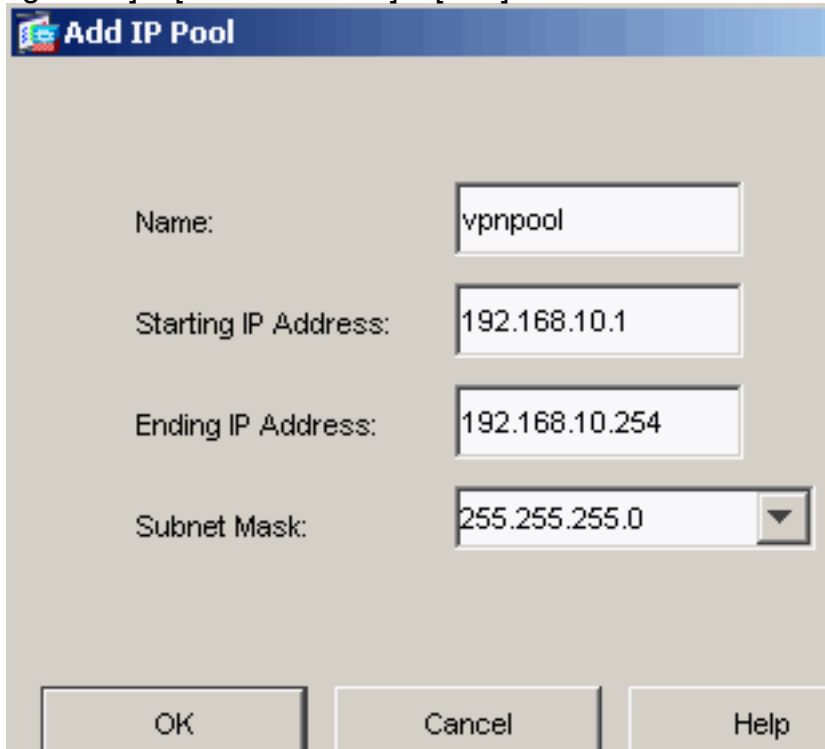
このドキュメントは、インターフェイス設定などの基本設定がすでに行われていて適切に動作していることを前提としています。

注: 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。

注: 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。詳細については、『[ASA の同じインターフェイスで有効になる ASDM および WebVPN](#)』 (英語) を参照してください。

次の手順を実行すると、ASA 上でスプリット トンネリングを備えた SSL VPN を設定できます。

1. [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Address Management] > [Address Pools] > [Add] を選択し、IP アドレス プール vpnpool を作成しま



The screenshot shows a configuration window titled "Add IP Pool". It contains the following fields and values:

Field	Value
Name:	vpnpool
Starting IP Address:	192.168.10.1
Ending IP Address:	192.168.10.254
Subnet Mask:	255.255.255.0

At the bottom of the window, there are three buttons: "OK", "Cancel", and "Help".

す。

2. [Apply] をクリックします。同等の CLI 設定 :
3. WebVPN をイネーブルにします。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [SSL VPN Connection Profiles] を選択し、[Access Interfaces] の下で、外部インターフェイスに対して [Allow Acces] と [Enable DTLS] のチェックボックスをオンにします。また、[Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interface selected in the table below] チェックボックスをオンにし、外部インターフェイスで SSL VPN を有効にします。

Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at [Client Settings](#))

Access Interfaces

Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the

Interface	Allow Access	Require Client Certificate	Enable DTLS
outside	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Access Port:

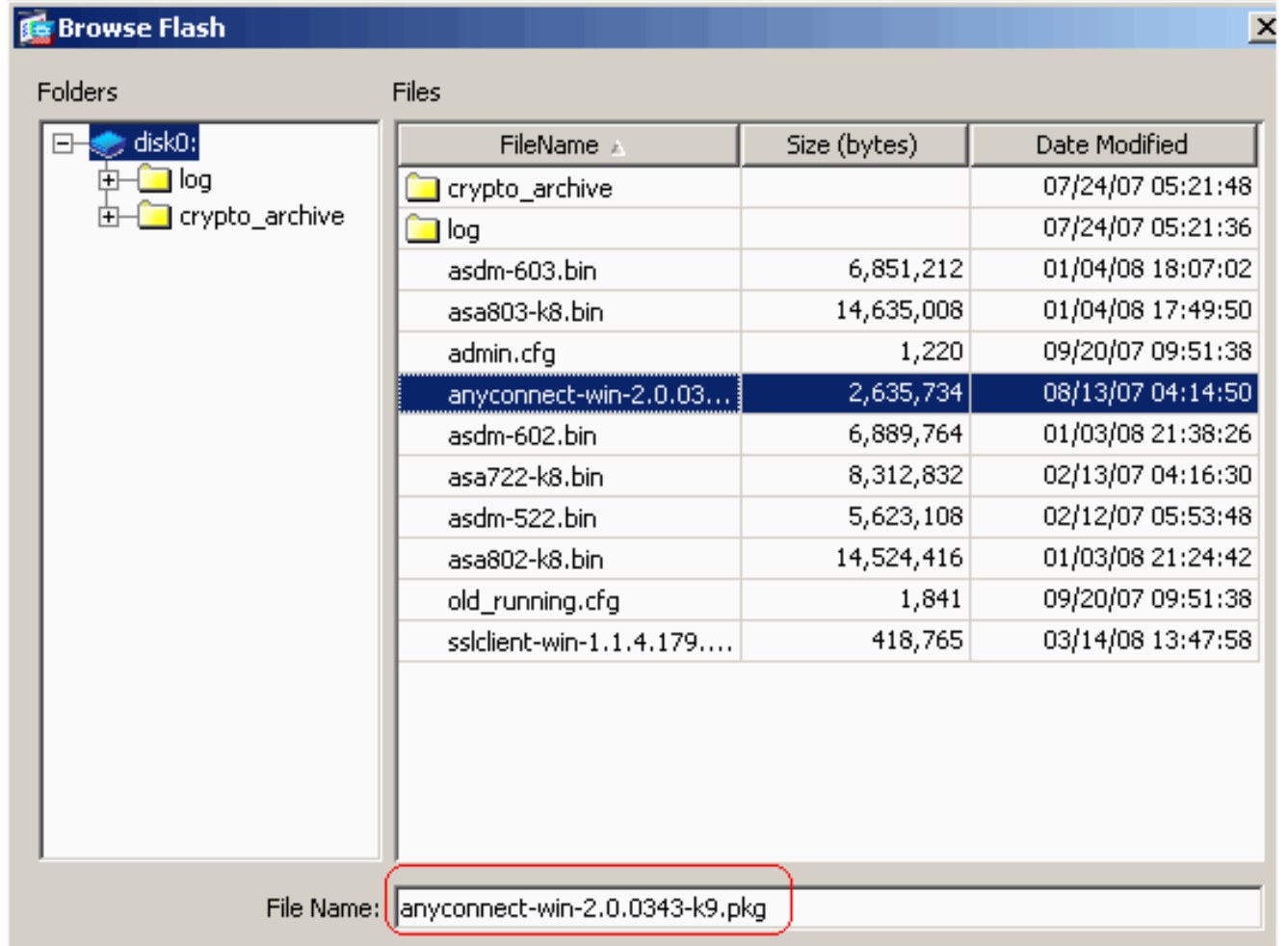
443

DTLS Port:

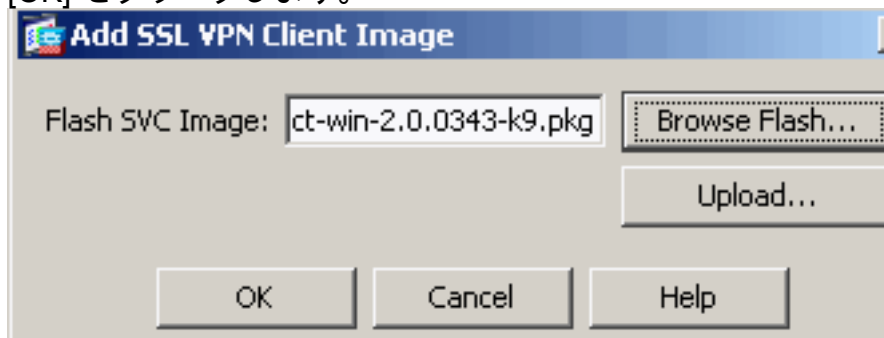
443

Click here to [Assign Certificate to Interface](#).

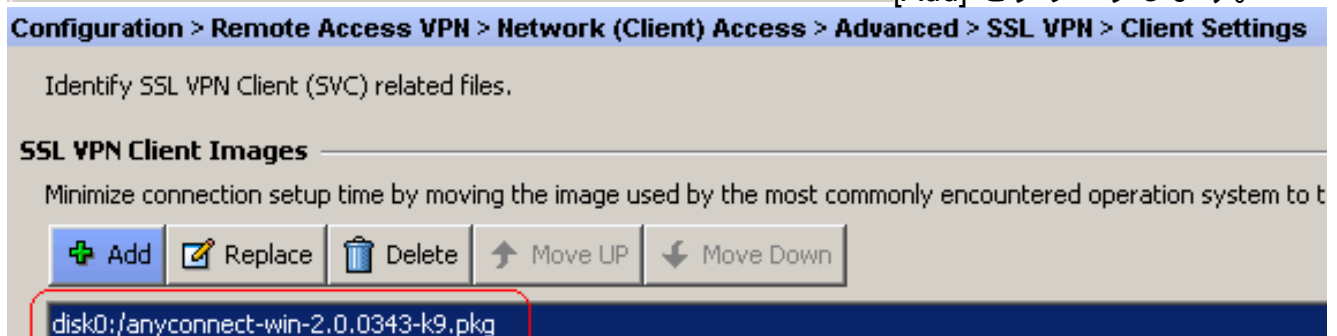
[Apply] をクリックします。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Advanced] > [SSL VPN] > [Client Settings] > [Add] を選択し、次に示すように Cisco AnyConnect VPN のクライアント イメージを ASA のフラッシュ メモリから追加します。



[OK] をクリックします。

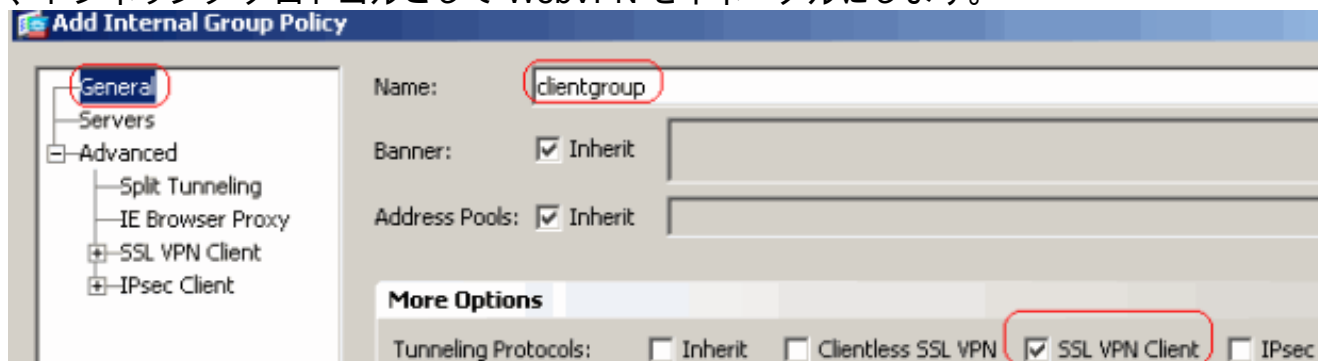


[Add] をクリックします。

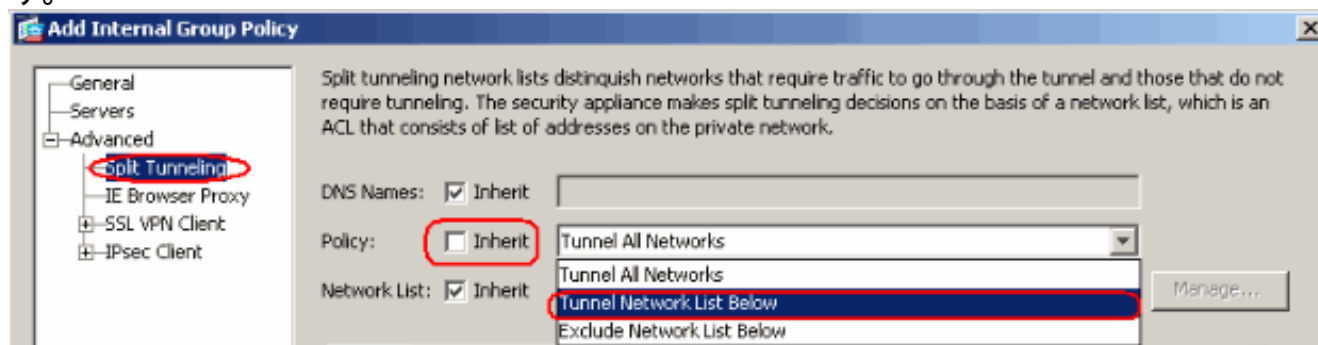


同等の CLI 設定：

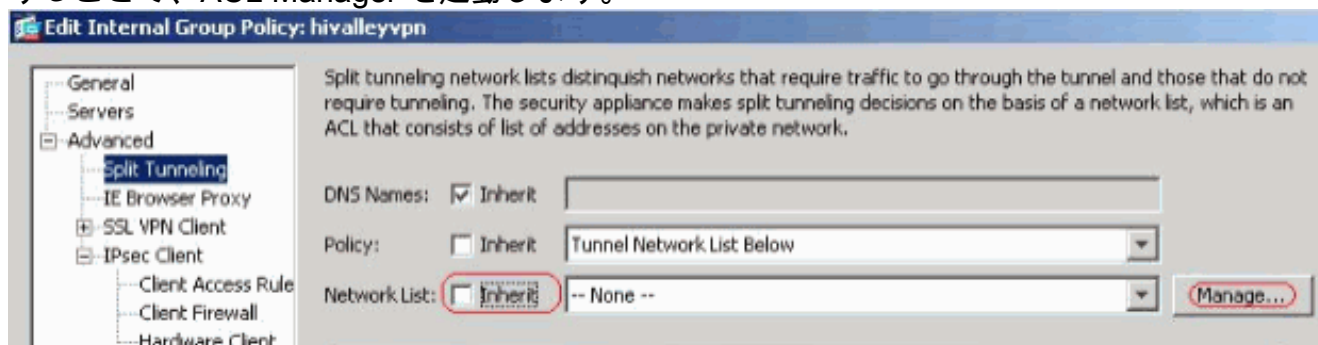
4. グループ ポリシーを設定します。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択し、内部グループ ポリシー **clientgroup** を作成します。[General] タブの下で、[SSL VPN Client] チェックボックスにチェック マークを付けて、トンネリング プロトコルとして WebVPN をイネーブルにします。



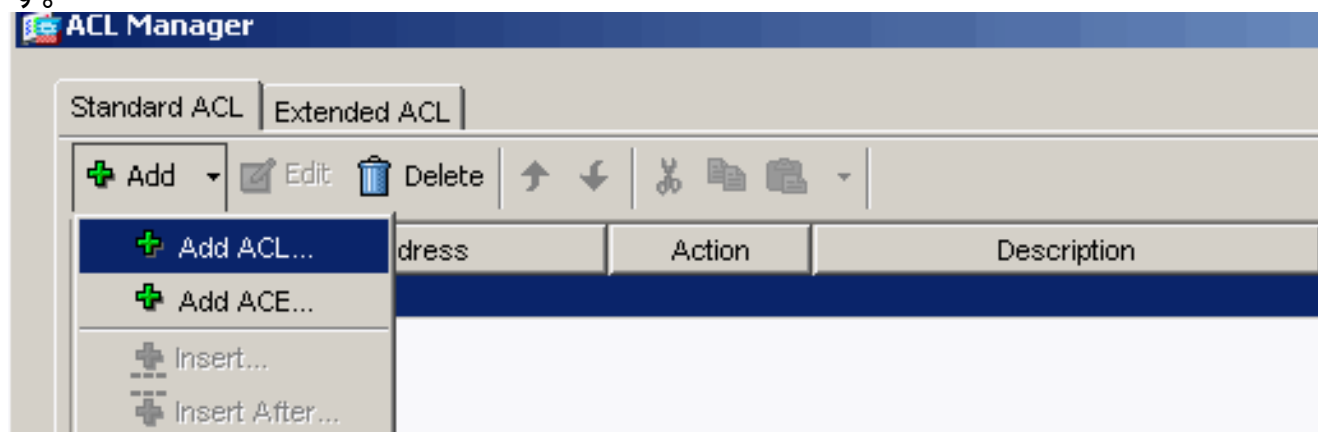
[Advanced] > [Split Tunneling] タブで、スプリット トンネル ポリシー用の [Inherit] チェックボックスをオフにして、ドロップダウン リストから [Tunnel Network List Below] を選択します。



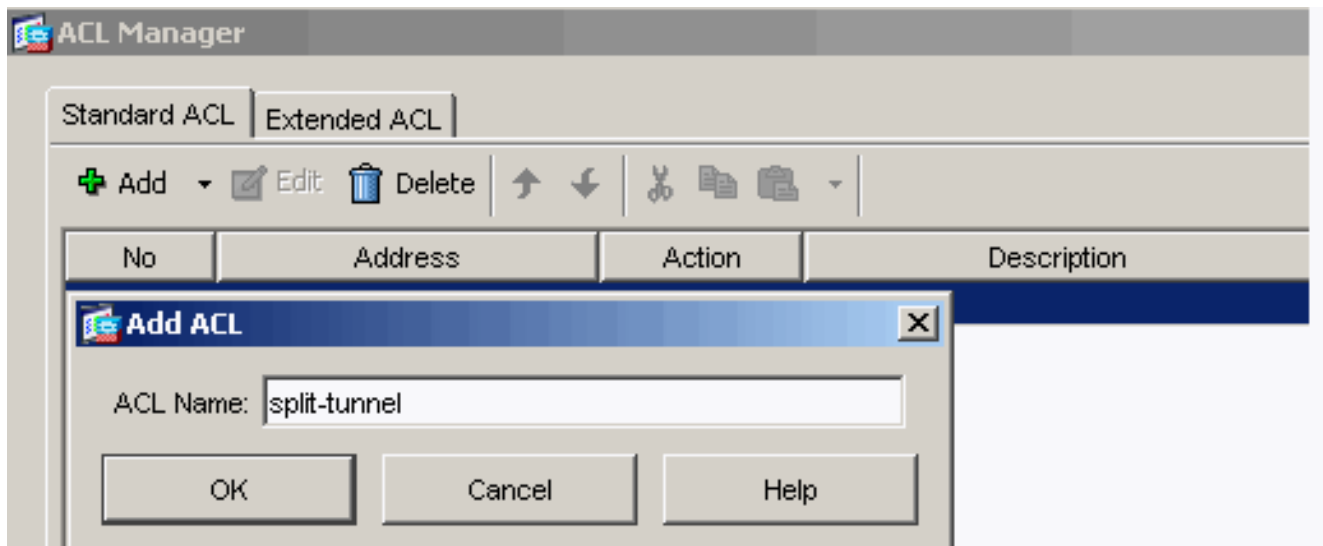
[Split Tunnel Network List] の [Inherit] チェック ボックスをオフにして [Manage] をクリックすることで、ACL Manager を起動します。



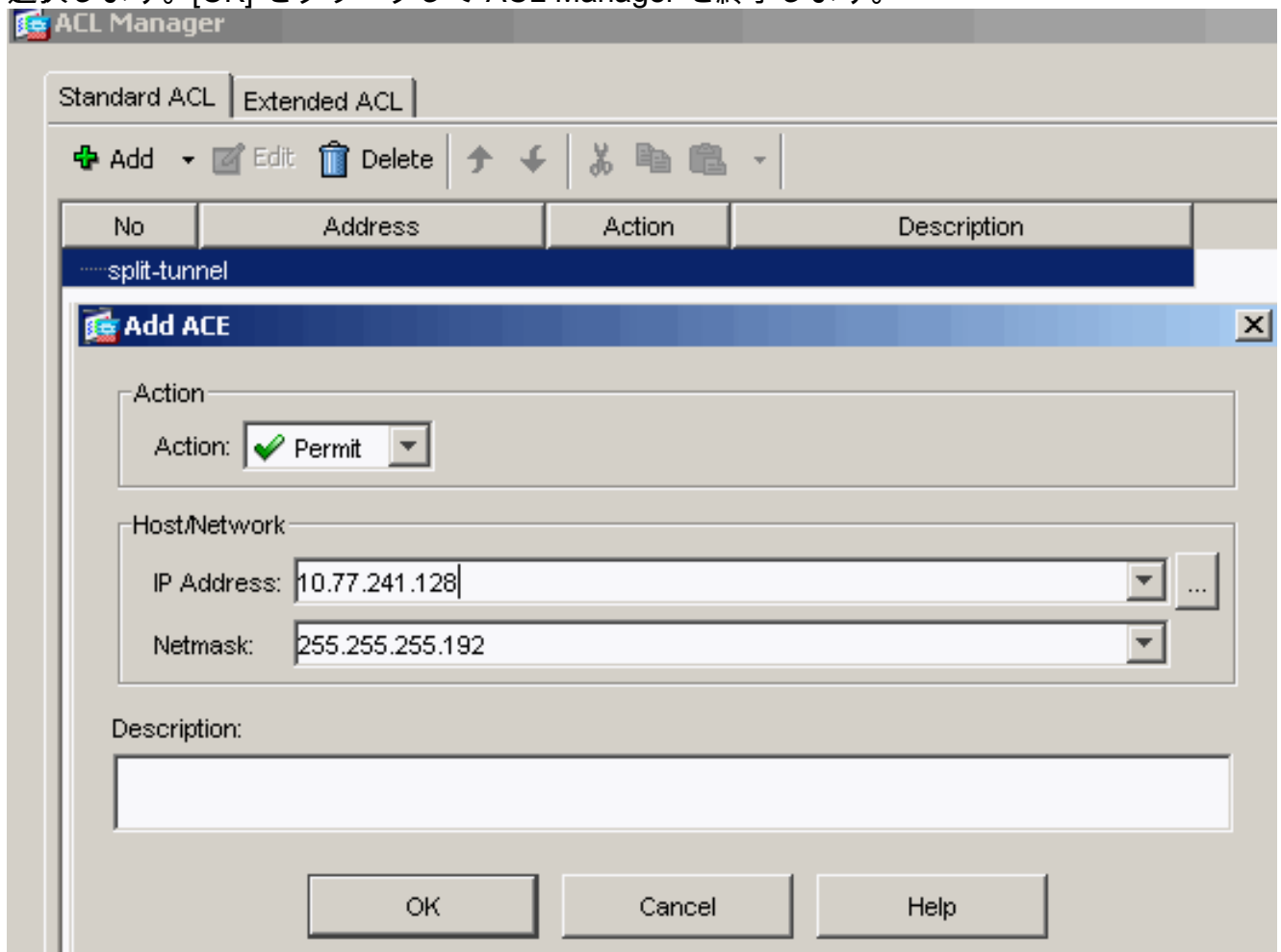
ACL Manager で、[Add] > [Add ACL...] の順に選択して、新しいアクセス リストを作成します。



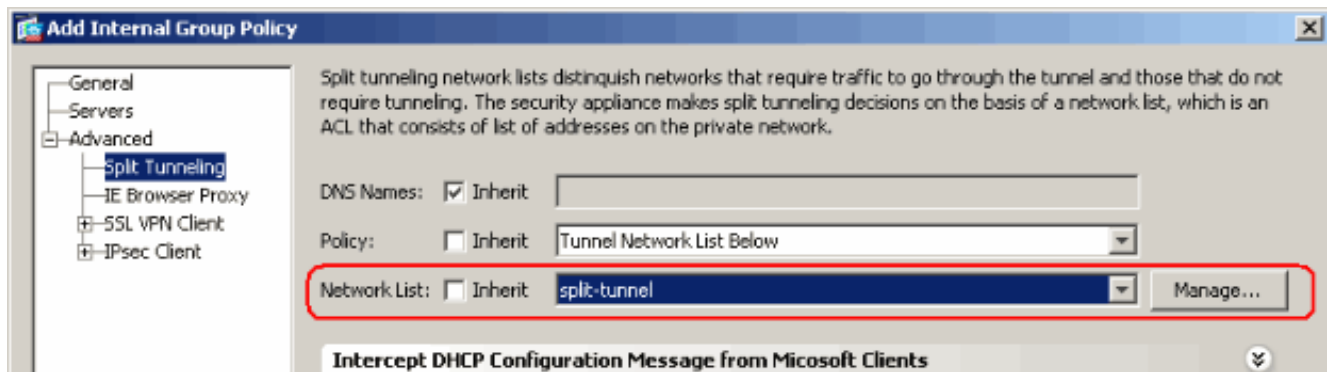
ACL に名前を指定して [OK] をクリックします。



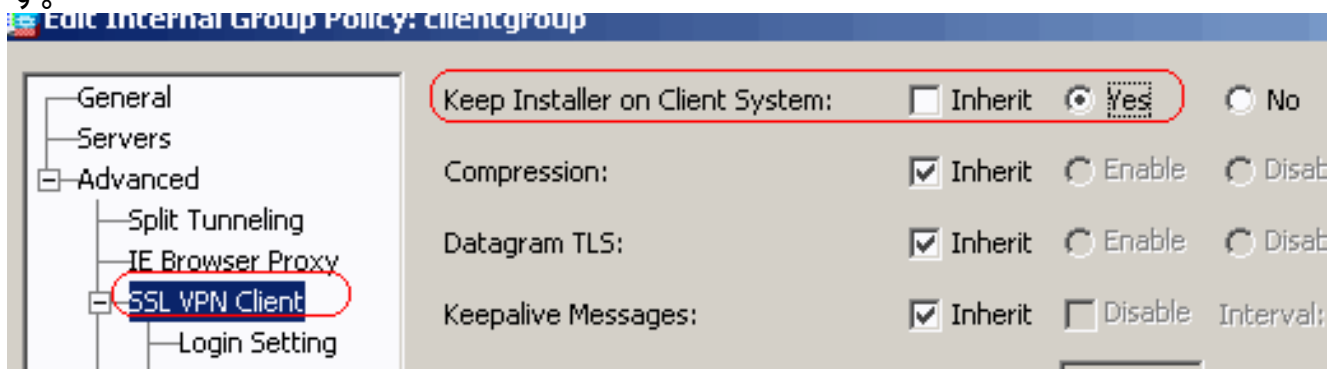
ACL 名が作成されてから、[Add] > [Add ACE] を選択して Access Control Entry (ACE; アクセスコントロール エントリ) を追加します。ASA の背後にある LAN に対応する ACE を定義します。この場合、ネットワークは 10.77.241.128/26 であり、[Action] として [Permit] を選択します。[OK] をクリックして ACL Manager を終了します。



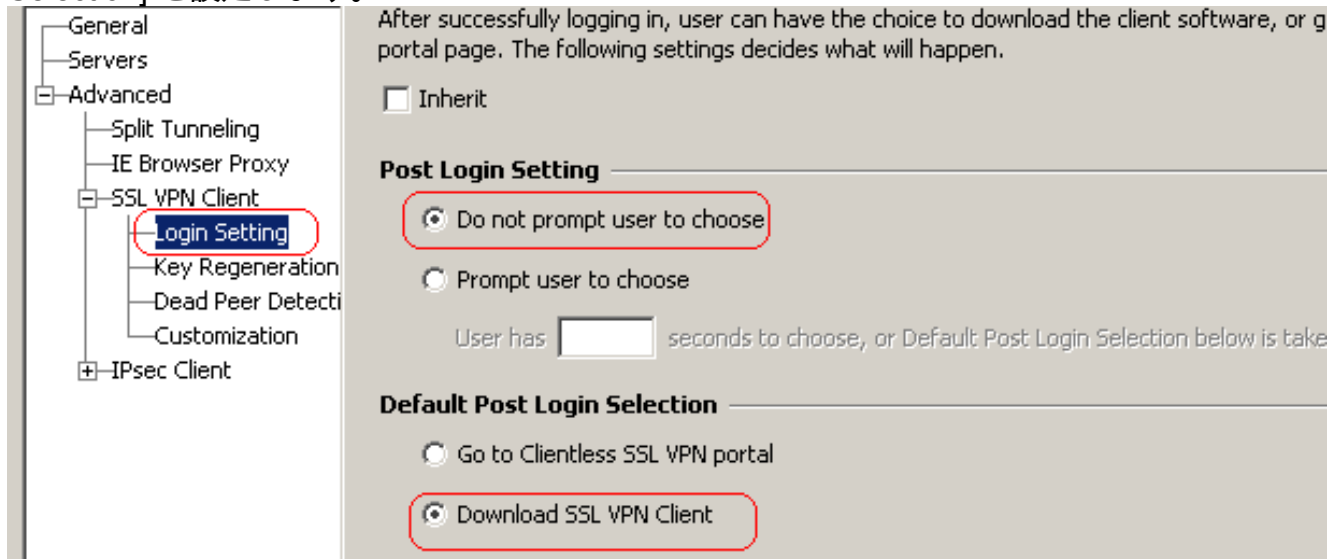
作成したばかりの ACL が split-tunnel ネットワーク リスト用に選択されていることを確認します。[OK] をクリックして、グループ ポリシー設定に戻ります。



メイン ページで、[Apply] をクリックしてから [Send] (必要な場合) をクリックして、コマンドを ASA に送信します。グループ ポリシー モードで SSL VPN を設定します。[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。



[Login Setting] をクリックして、次に示すように [Post Login Setting] と [Default Post Login Selection] を設定します。



[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。

General
Servers
Advanced

- Split Tunneling
- IE Browser Proxy
- SSL VPN Client
 - Login Setting
 - Key Regeneration**

Renegotiation Interval: Inherit Unlimited minutes

Renegotiation Method: Inherit None **SSL** New Tunnel

[OK] をクリックし、次に [Apply] をクリックします。

Configuration > Remote Access VPN > Network (Client) Access > Group Policies

Manage VPN group policies. A VPN group policy is a collection of user-oriented attribute/value pairs that may be stored inter-externally on a RADIUS/LDAP server. The group policy information is referenced by VPN tunnel groups and user accounts.

Name	Type	Tunneling Protocol	
clientgroup	Internal	svc	-- N/A --
DfltGrpPolicy (System Default)	Internal	L2TP-IPSec,IPSec,webvpn	-- N/A --

同等の CLI 設定 :

- [Configuration] > [Remote Access VPN] > [AAA Setup] > [Local Users] > [Add] を選択し、新しいユーザ アカウント **ssluser1** を作成します。[OK] をクリックし、次に [Apply] をクリックします。

Add User Account

Identity

- VPN Policy

Username:

Password:

Confirm Password:

User authenticated using MSCHAP

Member-of

Member-of:

Access Restriction

Select one of the options below to restrict ASDM, SSH, Telnet and Console access.
Note: All users have network access, regardless of these settings.

Full access(ASDM, SSH, Telnet and Console)
Privilege level is used with command authorization.
Privilege Level:

CLI login prompt for SSH, Telnet and console (no ASDM access)
This setting is effective only if AAA authenticate console command is configured.

No ASDM, SSH, Telnet or Console access
This setting is effective only if AAA authenticate console command is configured.

同等の CLI 設定 :

6. [Configuration] > [Remote Access VPN] > [AAA Setup] > [AAA Servers Groups] > [Edit] を選択し、[Enable Local User Lockout] チェック ボックスをオンにして最大試行値の 16 に設定することで、デフォルトのサーバグループ LOCAL を変更します。

Configuration > Remote Access VPN > AAA Setup > AAA Server Groups

AAA Server Groups

Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		

Edit LOCAL Server Group

This feature allows you to specify the maximum number of failed attempts to allow before locking out and denying access to the user. This limit is applicable only when the local database is used for authentication.

Enable Local User Lockout

Maximum Attempts:

OK Cancel Help

7. [OK] をクリックし、次に [Apply] をクリックします。同等の CLI 設定：

8. トンネルグループを設定します。[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [SSL VPN Connection Profiles Connection Profiles] > [Add] を選択し、新しいトンネルグループ **sslgroup** を作成します。[Basic] タブで、次に示すように設定のリストを実行できます。トンネルグループに **sslgroup** という名前を付けます。[Client Address Assignment] の下でドロップダウンリストからアドレスプール **vpnpool** を選択します。[Default Group Policy] の下でドロップダウンリストからグループポリシー **clientgroup** を選択します。

Add SSL VPN Connection Profile

Basic Advanced

Name:

Aliases:

Authentication

Method: AAA Certificate Both

AAA Server Group: Manage

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools: Select

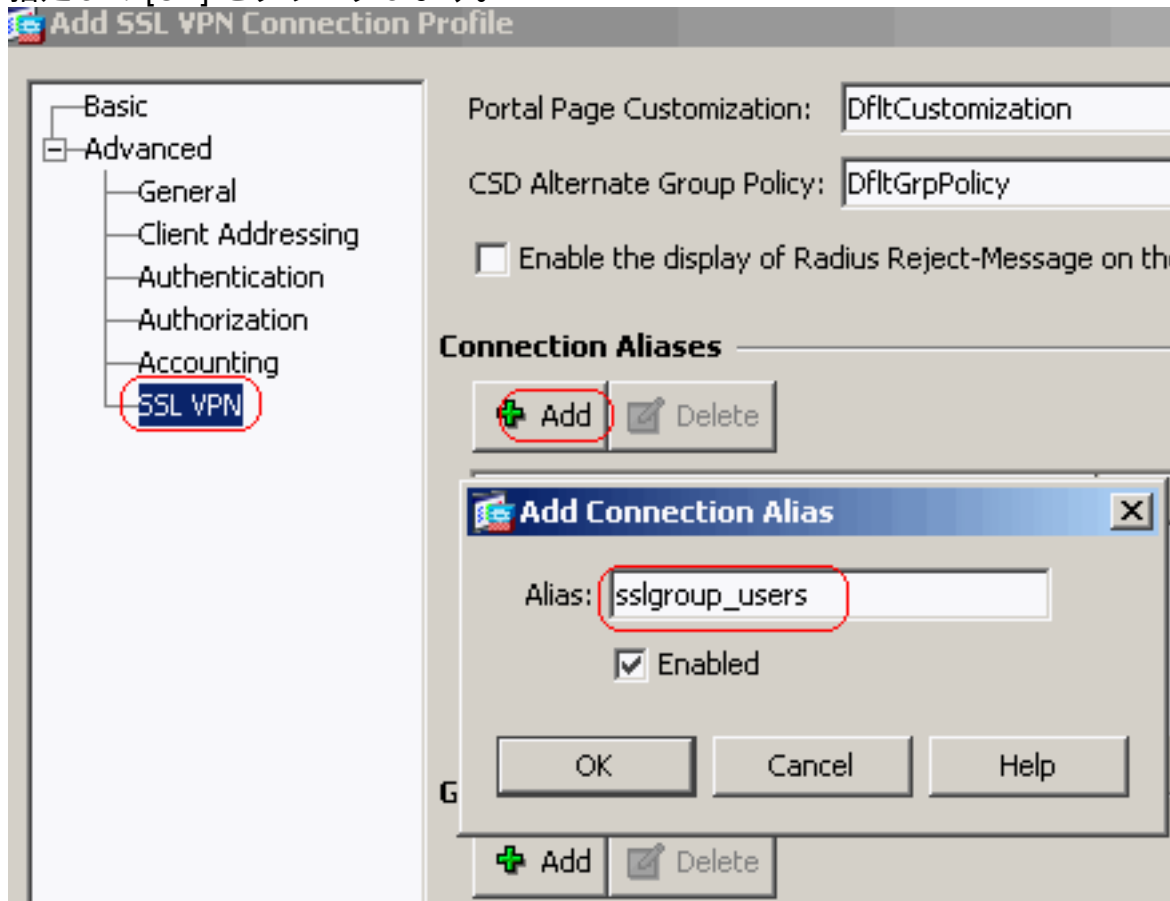
Default Group Policy

Group Policy: Manage

SSL VPN Client Protocol: Enabled

OK Cancel Help

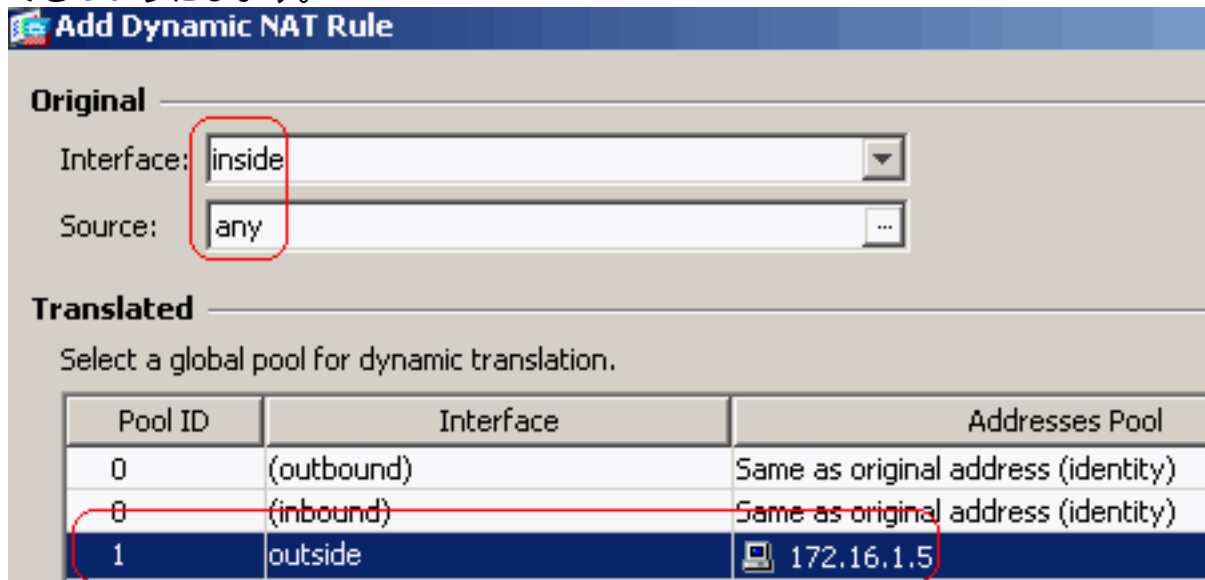
[SSL VPN] > [Connection Aliases] タブの下で、グループエイリアス名に `sslgroup_users` と指定して [OK] をクリックします。



[OK] をク

リックし、次に [Apply] をクリックします。同等の CLI 設定：

9. NAT を設定します。[Configuration] > [Firewall] > [NAT Rules] > [Add Dynamic NAT Rule] を選択し、Inside ネットワークからのトラフィックが Outside IP アドレス 172.16.1.5 で変換できるようにします。



[OK] を

クリックします。[OK] をクリックします。

Configuration > Firewall > NAT Rules						
#	Type	Original			Interface	
		Source	Destination	Service		
[-] inside (1 Dynamic rules)						
1	Dynamic	any			outside	

[Apply] をクリックします。同等の CLI 設定 :

10. VPN クライアントにネットワーク内から戻るトラフィックの NAT 免除を設定します。

```
ciscoasa(config)#access-list nonat permit ip 10.77.241.0 192.168.10.0
```

```
ciscoasa(config)#access-list nonat permit ip 192.168.10.0 10.77.241.0 ciscoasa(config)#nat
(inside) 0 access-list nonat
```

ASA CLI 設定

Cisco ASA 8.0(2)

```
ciscoasa(config)#show running-config : Saved : ASA
Version 8.0(2) ! hostname ciscoasa domain-name
default.domain.invalid enable password 8Ry2YjIyt7RRXU24
encrypted names ! interface Ethernet0/0 nameif inside
security-level 100 ip address 10.77.241.142
255.255.255.192 ! interface Ethernet0/1 nameif outside
security-level 0 ip address 172.16.1.1 255.255.255.0 !
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 boot system
disk0:/asa802-k8.bin ftp mode passive clock timezone IST
5 30 dns server-group DefaultDNS domain-name
default.domain.invalid access-list split-tunnel standard
permit 10.77.241.128 255.255.255.192 !--- ACL for Split
Tunnel network list for encryption. access-list nonat
permit ip 10.77.241.0 192.168.10.0 access-list nonat
permit ip 192.168.10.0 10.77.241.0 !--- ACL to define
the traffic to be exempted from NAT. pager lines 24
logging enable logging asdm informational mtu inside
1500 mtu outside 1500 ip local pool vpnpool
192.168.10.1-192.168.10.254 mask 255.255.255.0 !--- The
address pool for the Cisco AnyConnect SSL VPN Clients no
failover icmp unreachable rate-limit 1 burst-size 1 asdm
image disk0:/asdm-602.bin no asdm history enable arp
timeout 14400 global (outside) 1 172.16.1.5 !--- The
global address for Internet access used by VPN Clients.
!--- Note: Uses an RFC 1918 range for lab setup. !---
Apply an address from your public range provided by your
ISP. nat (inside) 0 access-list nonat !--- The traffic
permitted in "nonat" ACL is exempted from NAT. nat
(inside) 1 0.0.0.0 0.0.0.0 route outside 0.0.0.0 0.0.0.0
172.16.1.2 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 dynamic-access-policy-record
DfltAccessPolicy http server enable http 0.0.0.0 0.0.0.0
inside no snmp-server location no snmp-server contact
snmp-server enable traps snmp authentication linkup
linkdown coldstart no crypto isakmp nat-traversal telnet
```

```

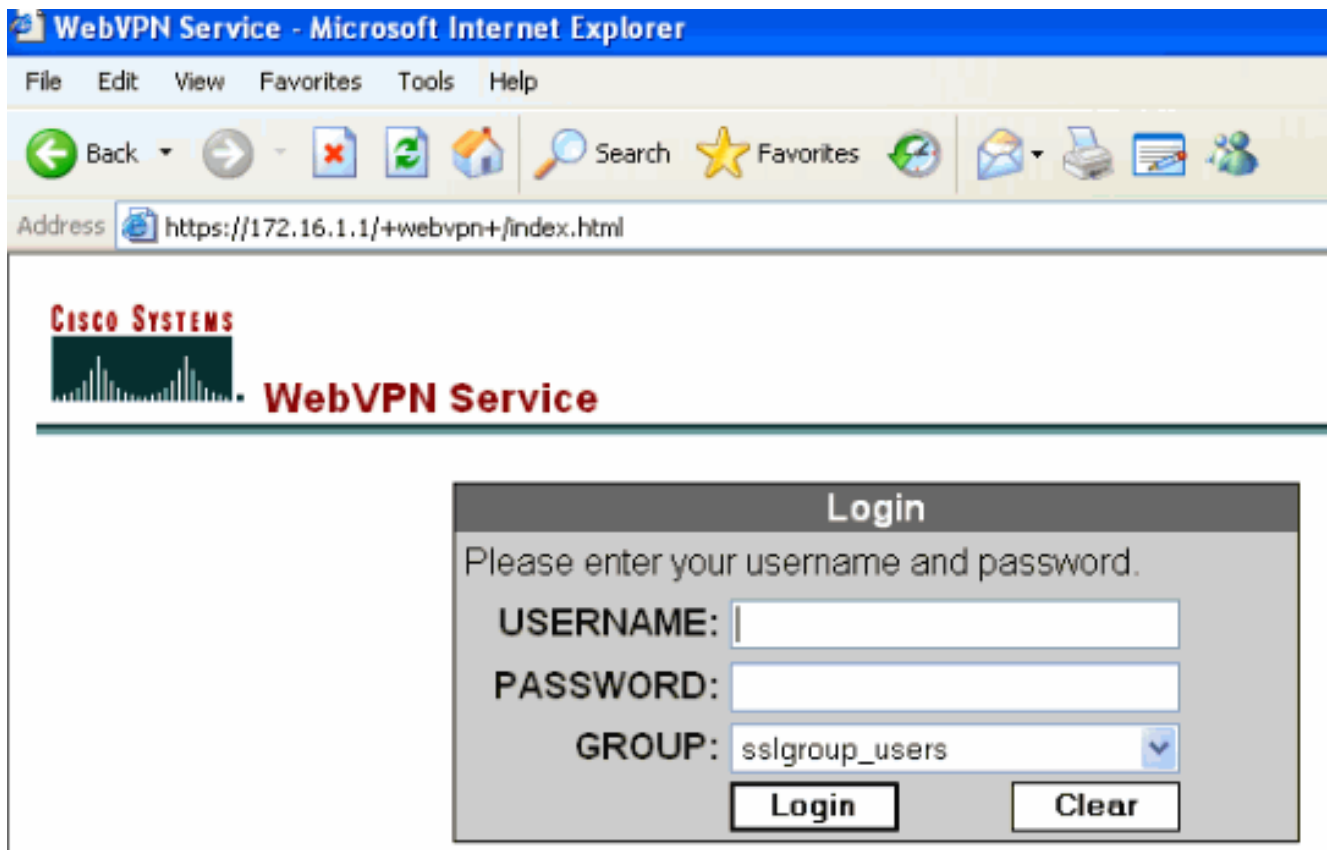
timeout 5 ssh timeout 5 console timeout 0 threat-
detection basic-threat threat-detection statistics
access-list ! class-map inspection_default match
default-inspection-traffic ! ! policy-map type inspect
dns preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
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 webvpn enable outside !---
Enable WebVPN on the outside interface svc image
disk0:/anyconnect-win-2.0.0343-k9.pkg 1 !--- Assign an
order to the AnyConnect SSL VPN Client image svc enable
!--- Enable the security appliance to download SVC
images to remote computers tunnel-group-list enable !---
Enable the display of the tunnel-group list on the
WebVPN Login page group-policy clientgroup internal !---
Create an internal group policy "clientgroup" group-
policy clientgroup attributes vpn-tunnel-protocol svc !-
-- Specify SSL as a permitted VPN tunneling protocol
split-tunnel-policy tunnelspecified split-tunnel-
network-list value split-tunnel !--- Encrypt the traffic
specified in the split tunnel ACL only webvpn svc keep-
installer installed !--- When the security appliance and
the SVC perform a rekey, they renegotiate !--- the
crypto keys and initialization vectors, increasing the
security of the connection. svc rekey time 30 !---
Command that specifies the number of minutes from the
start of the !--- session until the rekey takes place,
from 1 to 10080 (1 week). svc rekey method ssl !---
Command that specifies that SSL renegotiation takes
place during SVC rekey. svc ask none default svc
username ssluser1 password ZRhW85jZqEaVd5P. encrypted !-
-- Create a user account "ssluser1" tunnel-group
sslgroup type remote-access !--- Create a tunnel group
"sslgroup" with type as remote access tunnel-group
sslgroup general-attributes address-pool vpnpool !---
Associate the address pool vpnpool created
default-
group-policy clientgroup !--- Associate the group policy
"clientgroup" created tunnel-group sslgroup webvpn-
attributes group-alias sslgroup_users enable !---
Configure the group alias as sslgroup-users prompt
hostname context
Cryptochecksum:af3c4bfc4ffc07414c4dfbd29c5262a9 : end
ciscoasa(config)#

```

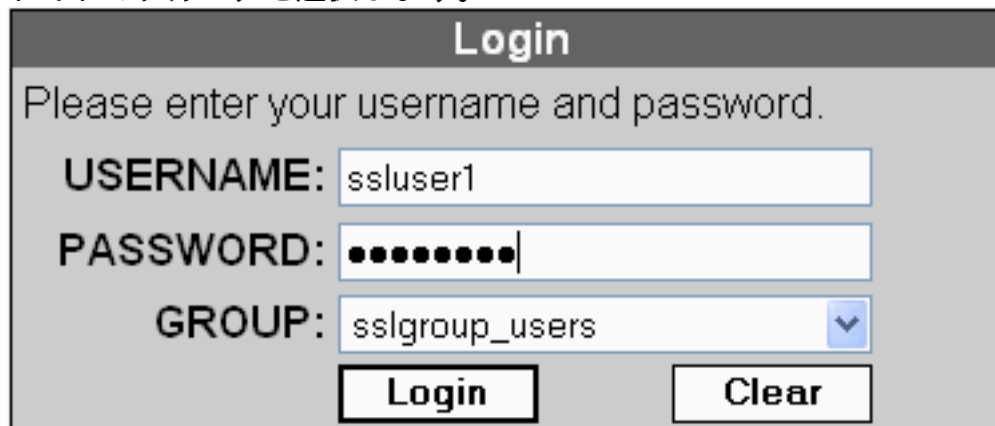
SVC との SSL VPN 接続の確立

次の手順を実行して、ASA との SSL VPN 接続を確立します。

1. 次に示す形式で、Web ブラウザ内で ASA の WebVPN インターフェイスの URL または IP アドレスを入力します。https://url または https://<IP address of the ASA WebVPN interface>



2. ユーザ名とパスワードを入力します。また、次に示すようにドロップダウン リストからそれぞれのグループを選択します。

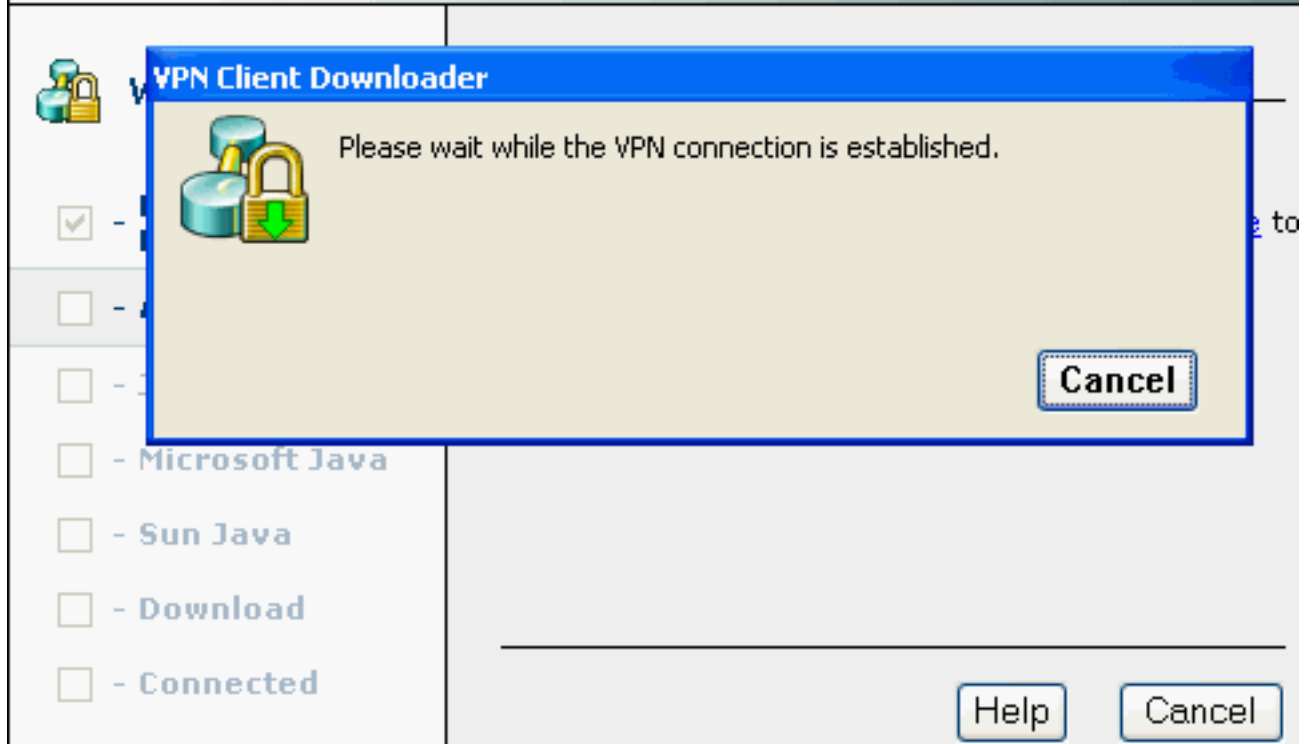


SSL VPN 接続が確立

される前に次のウィンドウが表示されます。



Cisco AnyConnect VPN Client



注: SVC をダウンロードする前に ActiveX ソフトウェアをコンピュータにインストールしておく必要があります。接続が確立されると、このウィンドウが表示されます。



Cisco AnyConnect VPN Client



WebLaunch

- Platform Detection
- ActiveX
- Java Detection
- Microsoft Java
- Sun Java
- Download
- Connected

Connection Established

The Cisco AnyConnect VPN Client has successfully connected.

The connection can be controlled from the tray icon, circled in the image below:



Help

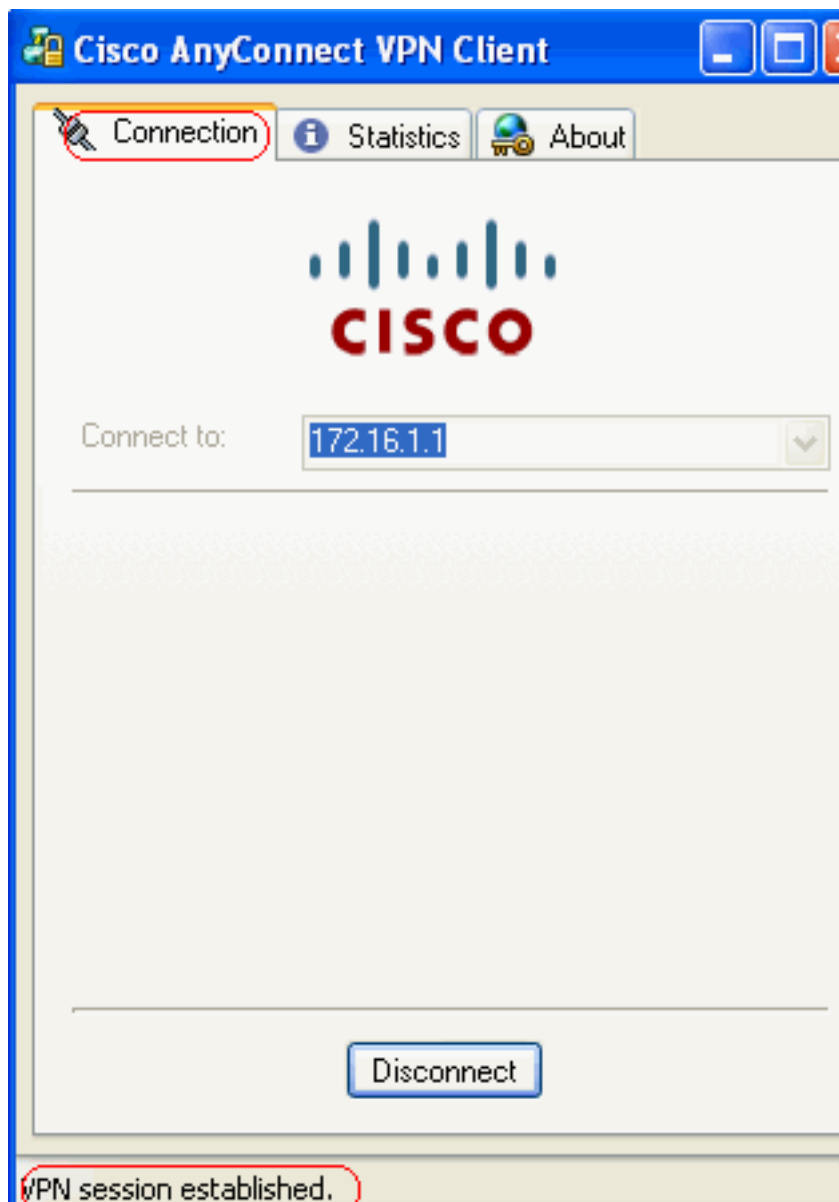
Cancel

system...

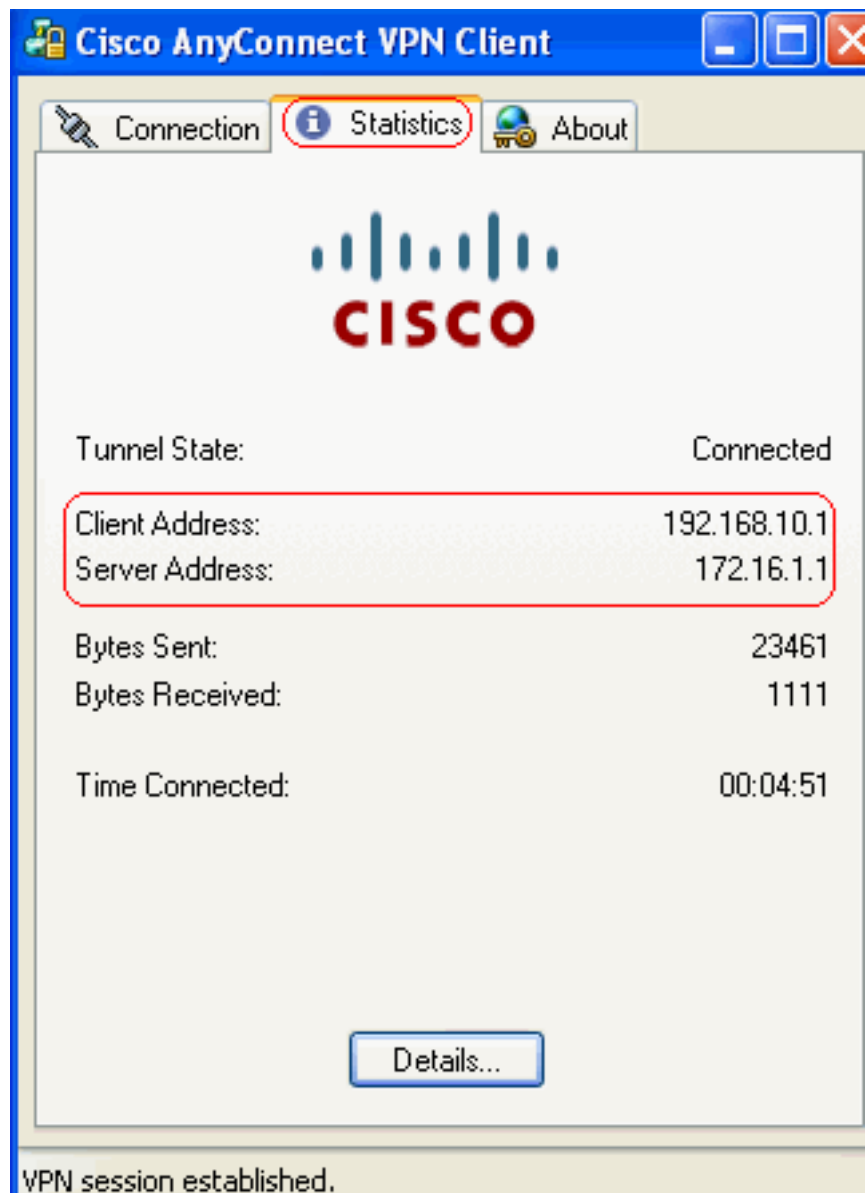
anyconnect - Paint

Cisco AnyConnect
Connected

3. コンピュータのタスクバーに表示される錠をクリックします。



このウィンドウが表示され、SSL 接続についての情報が提供されます。たとえば、192.168.10.1 は ASA によって割り当てら



れた IP であるなどです。このウ
インドウは、Cisco AnyConnect VPN Client バージョンの情報を示しています。



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。

[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。

- **show webvpn svc** : ASA フラッシュ メモリに格納された SVC イメージを表示します。
`ciscoasa#show webvpn svc 1. disk0:/anyconnect-win-2.0.0343-k9.pkg 1 CISCO STC win2k+2,0,0343 Mon 04/23/2007 4:16:34.63 1 SSL VPN Client(s) installed`
- **show vpn-sessiondb svc** : 現在の SSL 接続についての情報を表示します。 `ciscoasa#show vpn-sessiondb svc` Session Type: SVC Username : **ssluser1** Index : 12 Assigned IP : **192.168.10.1** Public IP : **192.168.1.1** Protocol : **Clientless SSL-Tunnel DTLS-Tunnel** Encryption : **RC4 AES128** Hashing : **SHA1** Bytes Tx : 194118 Bytes Rx : 197448 Group Policy : **clientgroup** Tunnel Group : **sslgroup** Login Time : 17:12:23 IST Mon Mar 24 2008 Duration : 0h:12m:00s NAC Result : Unknown VLAN Mapping : N/A VLAN : none
- **show webvpn group-alias** : さまざまなグループに対する設定済みのエイリアスを表示します
◦ `ciscoasa#show webvpn group-alias` Tunnel Group: **sslgroup** Group Alias: **sslgroup_users** enabled
- ASDM で、[Monitoring] > [VPN] > [VPN Statistics] > [Sessions] を選択すると、ASA の現在の WebVPN セッションがわかります。

Monitoring > VPN > VPN Statistics > Sessions

Remote Access	Site-to-Site	SSL VPN			E-mail Proxy	VPN Load Balancing
		Clientless	With Client	Total		
0	0	0	0	0	0	0

Filter By: **SSL VPN Client** -- All Sessions -- Filter

Username IP Address	Group Policy Connection	Protocol Encryption	Login Time Duration	Byt Byt
ssluser1 192.168.10.1	clientgroup sslgroup	Clientless SSL-Tunnel DT... RC4 AES128	17:12:23 IST Mon Mar 24 2008 0h:03m:31s	194118 192474

トラブルシューティング

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

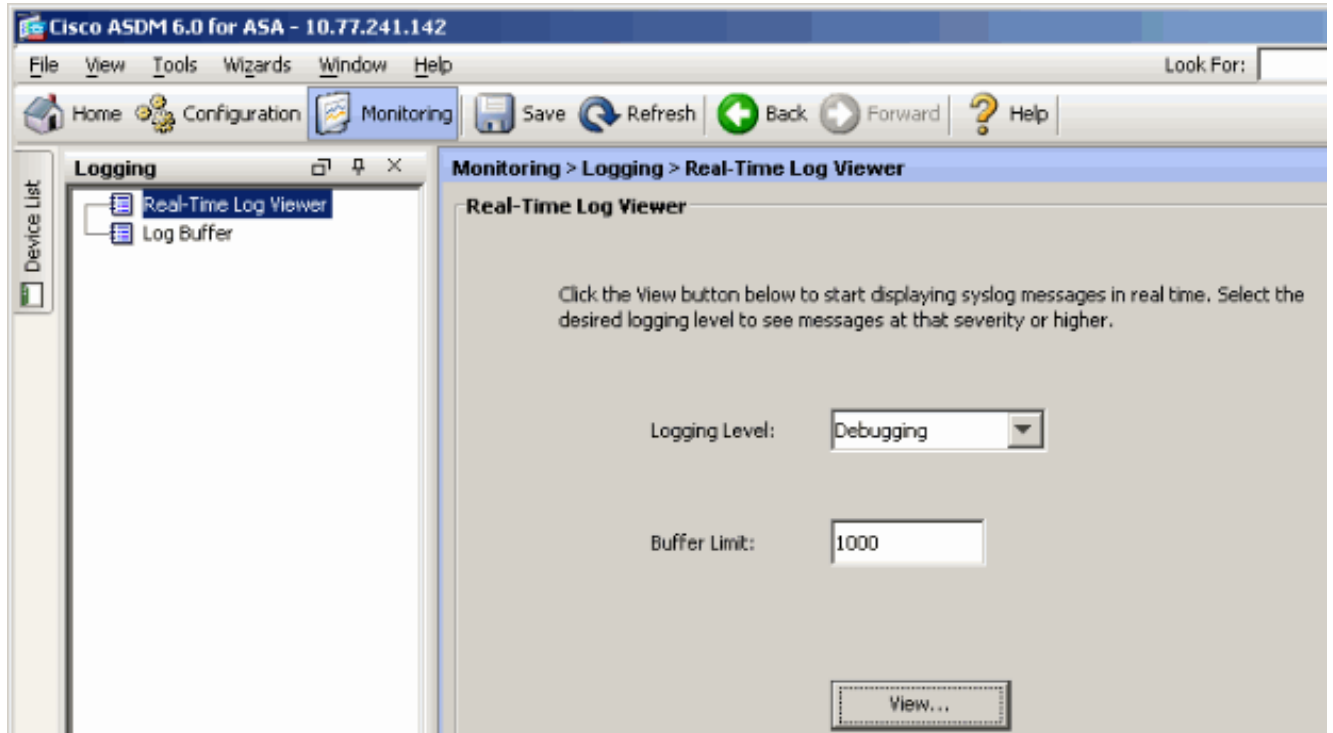
- vpn-sessiondb logoff name <ユーザ名>** : 特定のユーザ名の SSL VPN セッションをログオフするコマンドです。 `ciscoasa#vpn-sessiondb logoff name ssluser1` Do you want to logoff the VPN session(s)? [confirm] Y INFO: Number of sessions with name "ssluser1" logged off : 1 `ciscoasa#Called vpn_remove_uauth: success! webvpn_svc_np_tear_down: no ACL webvpn_svc_np_tear_down: no IPv6 ACL np_svc_destroy_session(0xB000)` 同様に、**vpn-sessiondb logoff svc** コマンドを使用すると、すべての SVC セッションを終了できます。
- 注:** PC がスタンバイ モードまたは休止状態モードになった場合、SSL VPN 接続を終了することができます。 `webvpn_rx_data_cstp webvpn_rx_data_cstp: got message SVC message: t/s=5/16: Client PC is going into suspend mode (Sleep, Hibernate, e tc) Called vpn_remove_uauth: success! webvpn_svc_np_tear_down: no ACL webvpn_svc_np_tear_down: no IPv6 ACL np_svc_destroy_session(0xA000) ciscoasa#show vpn-sessiondb svc` INFO: There are presently no active sessions
- debug webvpn svc <1-255>** : セッションを確立するために、リアルタイムの webvpn イベントを提供します。 `Ciscoasa#debug webvpn svc 7 webvpn_rx_data_tunnel_connect` CSTP state = HEADER_PROCESSING http_parse_cstp_method() ...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1' `webvpn_cstp_parse_request_field() ...input: 'Host: 172.16.1.1'` Processing CSTP header line: 'Host: 172.16.1.1' `webvpn_cstp_parse_request_field() ...input: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343'` Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Client 2, 0, 0343' Setting user-agent to: 'Cisco AnyConnect VPN Client 2, 0, 0343' `webvpn_cstp_parse_request_field() ...input: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B 7D75F4EDEF26'` Processing CSTP header line: 'Cookie: webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D75F4EDEF26' Found WebVPN cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B 08B7D75F4EDEF26' WebVPN Cookie: 'webvpn=16885952@12288@1206098825@D251883E8625B92C1338D631B08B7D7 5F4EDEF26' `webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Version: 1'` Processing CSTP header line: 'X-CSTP-Version: 1' Setting version to '1' `webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Hostname: tacweb'` Processing CSTP header line: 'X-CSTP-Hostname: tacweb' Setting hostname to: 'tacweb' `webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Accept-Encoding: deflate;q=1.0'` Processing CSTP header line: 'X-CSTP-Accept-Encoding: deflate;q=1.0' `webvpn_cstp_parse_request_field() ...input: 'X-CSTP-MTU: 1206'` Processing CSTP header line: 'X-CSTP-MTU: 1206' `webvpn_cstp_parse_request_field() ...input: 'X-CSTP-Address-Type: IPv4'` Processing CSTP header line: 'X-CSTP-Address-Type: IPv4' `webvpn_cstp_parse_request_field() ...input: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40 642E22C6AF9501758FF3B7B5545973C06F6393C92E59693'` Processing CSTP header line: 'X-DTLS-Master-Secret: CE151BA2107437EDE5EC4F5EE6AEBAC12031550B1812D40642E22C6AF9501758FF3B7B5545973C06F6393C92E59693' `webvpn_cstp_parse_request_field() ...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-`

```

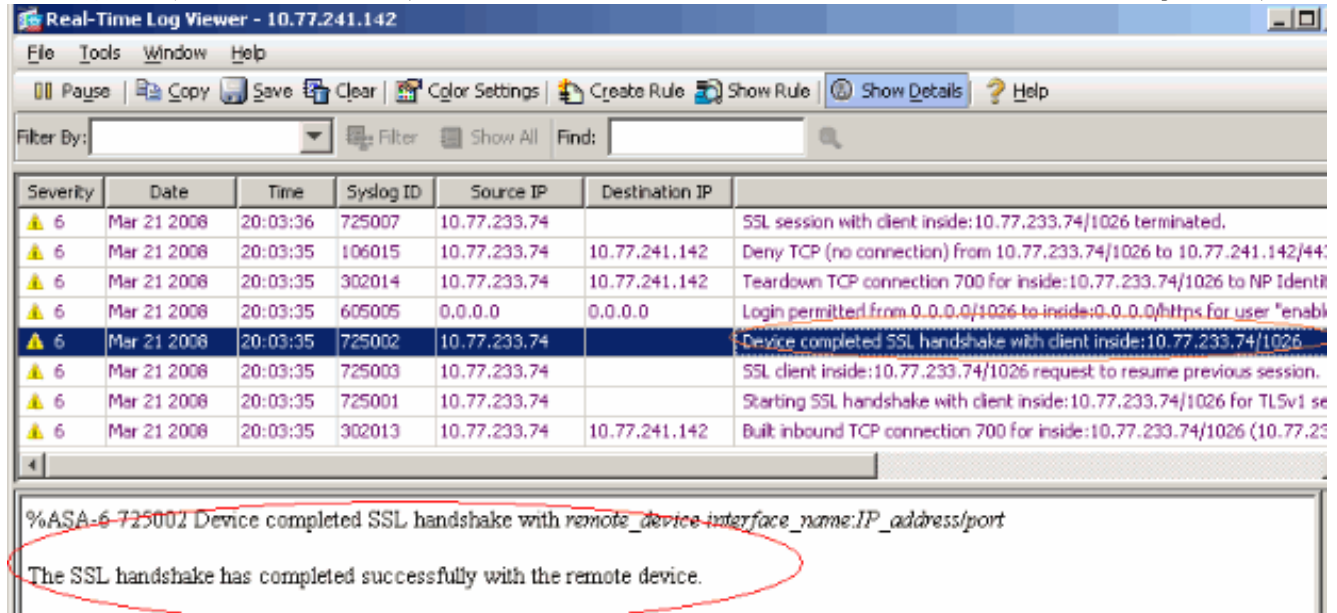
CBC3-SHA:DES-CBC-SHA' Processing CSTEP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-
SHA:DES-CBC3 -SHA:DES-CBC-SHA' Validating address: 0.0.0.0 CSTEP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/0.0.0.0 CSTEP state = HAVE_ADDRESS No subnetmask...
must calculate it SVC: NP setup np_svc_create_session(0x3000, 0xD41611E8, TRUE)
webvpn_svc_np_setup SVC ACL Name: NULL SVC ACL ID: -1 SVC ACL ID: -1 vpn_put_uauth success!
SVC IPv6 ACL Name: NULL SVC IPv6 ACL ID: -1 SVC: adding to sessgmt SVC: Sending response
Unable to initiate NAC, NAC might not be enabled or invalid policy CSTEP state = CONNECTED
webvpn_rx_data_cstp webvpn_rx_data_cstp: got internal message Unable to initiate NAC, NAC
might not be enabled or invalid policy

```

4. ASDM で、[Monitoring] > [Logging] > [Real-time Log Viewer] > [View] を選択してリアルタイム イベントを表示します。



この例では、ヘッドエンドデバイスで SSL セッションが確立されていることを示します。



関連情報

- [Cisco 5500 シリーズ適応型セキュリティ アプライアンスに関するサポート ページ](#)
- [AnyConnect VPN クライアント リリース 2.0 のリリース ノート](#)

- [ASA/PIX : ASA で VPN クライアントのスプリット トンネリングを許可するための設定例](#)
- [スプリット トンネリングを使用する VPN クライアントが IPSec とインターネットに接続するのをルータで許可する設定例](#)
- [公衆インターネット VPN on a Stick のための PIX/ASA 7.x および VPN クライアント間の設定例](#)
- [ASDM を使用した ASA での SSL VPN Client \(SVC \) の設定例](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)