ASA 9.XでのAnyConnect VPNクライアントUターンのトラフィックの設定

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[Uターン型リモートアクセストラフィックの設定](#)
[公衆インターネット VPN on a Stick のための AnyConnect VPN Client の設定例](#)
[ネットワーク図](#)
[ASDM リリース 7.1(6) での ASA リリース 9.1(2) の設定](#)
[CLI の ASA リリース 9.1(2) の設定](#)
[TunnelAll 設定の実施による AnyConnect VPN Client 間の通信の許可](#)
[ネットワーク図](#)
[ASDM リリース 7.1(6) での ASA リリース 9.1(2) の設定](#)
[CLI の ASA リリース 9.1(2) の設定](#)
[スプリットトンネルを使用した AnyConnect VPN Client 間の通信](#)
[ネットワーク図](#)
[ASDM リリース 7.1(6) での ASA リリース 9.1(2) の設定](#)
[CLI の ASA リリース 9.1(2) の設定](#)
[確認](#)
[トラブルシュート](#)
[関連情報](#)

概要

このドキュメントでは、Cisco適応型セキュリティアプライアンス(ASA)リリース9.Xをセットアップして、VPNトラフィックをUターンできるようにする方法について説明します。次の設定シナリオについて説明します。リモートアクセスクライアントからのUターンのトラフィック。

> **注：** ネットワークでの IP アドレスのオーバーラップを避けるために、IP アドレスの完全に異なるプールを VPN Client に割り当ててください（たとえば、10.x.x.x、172.16.x.x および 192.168.x.x）。 このIPアドレス方式は、ネットワークのトラブルシューティングに役立ちます。

ヘアピンまたはUターン

この機能は、あるインターフェイスに着信した後に同じインターフェイスからルーティングされる VPN トラフィックに対して便利な機能です。たとえば、ハブ アンド スポークの VPN ネットワークを構築していて、セキュリティ アプライアンスがハブであり、リモート VPN ネットワークがスポークであるとします。あるスポークが他のスポークと通信するためには、トラフィック

がセキュリティ アプライアンスに着信した後、他のスポーク宛てに再び発信される必要があります。

次を入力します。 **same-security-traffic** コマンドを発行して、トラフィックが同じインターフェイスで発着信できるようにします。

```
ciscoasa(config)#same-security-traffic permit intra-interface
```

前提条件

要件

この設定を行う前に、以下の要件を満たしていることを確認してください。

- ハブ ASA セキュリティ アプライアンスはリリース 9.x を稼働する必要があります。
- Cisco AnyConnect VPN Client 3.x**注：**AnyConnect VPN Clientパッケージ(anyconnect-win*.pkg)からダウンロードできます(登録ユーザ専用)。 AnyConnect VPNクライアントをCisco ASAフラッシュメモリにコピーします。このフラッシュメモリは、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コンフィギュレーションガイドの「AnyConnect VPNクライアント接続」セクション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いています。

- ソフトウェア バージョン 9.1(2) が稼働している Cisco 5500 シリーズ ASA
- Windows 3.1.05152 用のバージョンの Cisco AnyConnect SSL VPN Client
- 「サポートされているVPNプラットフォーム、Cisco ASAシリーズ」に従ってサポートされているOSが稼働するPC。
- Cisco Adaptive Security Device Manager（ASDM）バージョン 7.1(6)

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

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リダイレクトするように設定されていない場合 **http://** 要求 **https://**ユーザは次の形式でURLを入力する必要があります。 **https://**

.URL が入力されると、ブラウザはそのインターフェイスに接続し、ログイン画面が表示されます。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が必要であると識別した場合、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。クライアントがセキュリティ アプライアンスとの SSL VPN 接続をネゴシエートする場合は、Transport Layer Security (TLS) や Datagram Transport Layer Security (DTLS) を使用して接続します。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、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が向上します。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の詳細については、『Cisco AnyConnectセキュアモビリティクライアント管理者ガイド』を参照してください。セキュリティ アプライアンスは、接続を確立するユーザのグループ ポリシーまたは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。**注：**このドキュメントで使用されている例では、IPv4を使用しています。IPv6 Uターンのトラフィックの場合、手順は同じですが、IPv4の代わりにIPv6アドレスを使用します。

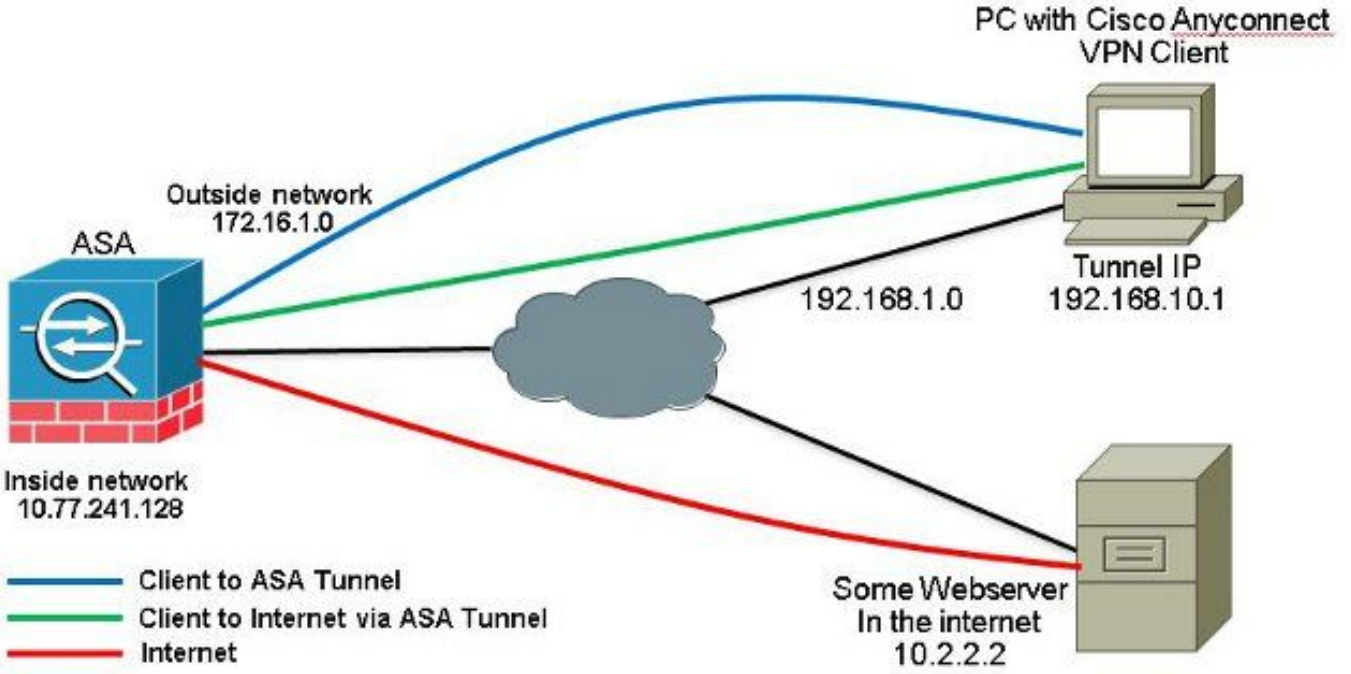
Uターン型リモートアクセストラフィックの設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。**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、コマンドリファレンスガイドを使用してください。

公衆インターネット VPN on a Stick のための AnyConnect VPN Client の設定例

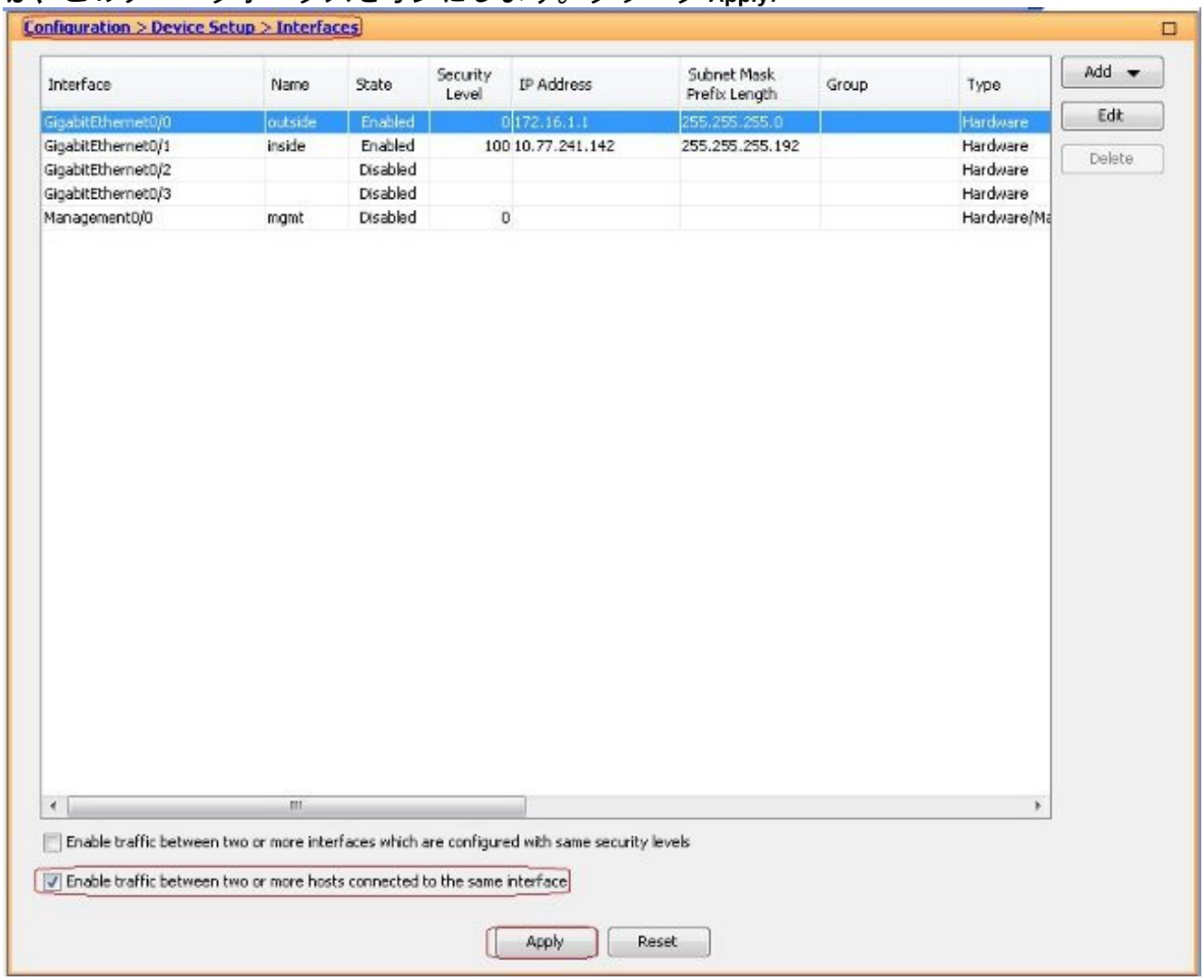
ネットワーク図

このドキュメントでは、次のネットワークセットアップを使用します。



ASDM リリース 7.1(6) での ASA リリース 9.1(2) の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完了し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、『管理アクセスの設定』を参照してください。**注：**リリース 8.0(2) 以降、ASA はクライアントレス SSL VPN (WebVPN) セッションと ASDM 管理セッションを外部インターフェイスのポート 443 で同時にサポートします。8.0(2) 以前のバージョンでは、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有効にはできません。詳細は、『ASAの同じインターフェイスでイネーブルになるASDMとWebVPN』を参照してください。ASA 上で SSL VPN on a stick を設定するには、次の手順を実行します。

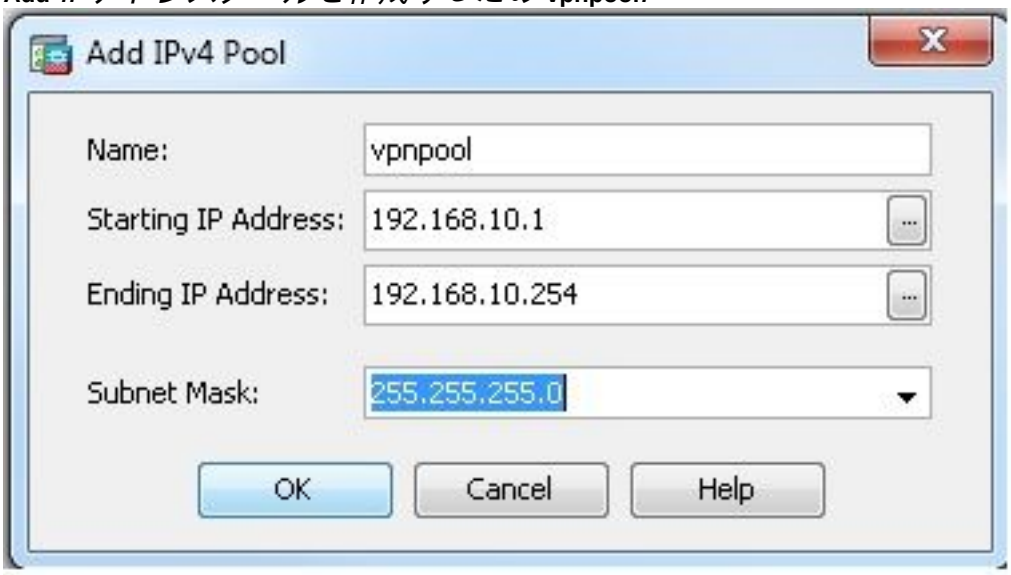
1. *選択* **Configuration > Device Setup > Interfaces** *および* **Enable traffic between two or more hosts connected to the same interface** *SSL VPNトラフィックが同じインターフェイスで発着信できるようにするには、このチェックボックスをオンにします。クリック* **Apply**.



同等の CLI 設定

```
ciscoasa(config)#same-security-traffic permit intra-interface
```

2. *選択* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools > Add** *IPアドレスプールを作成するため* **vpnpool**.

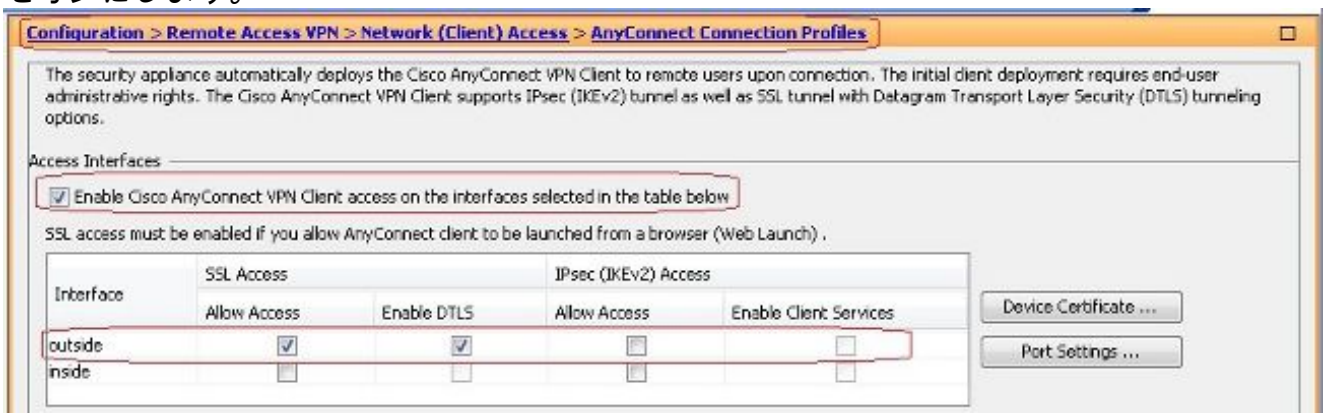


3. *クリック* **Apply**. ***同等の CLI 設定***

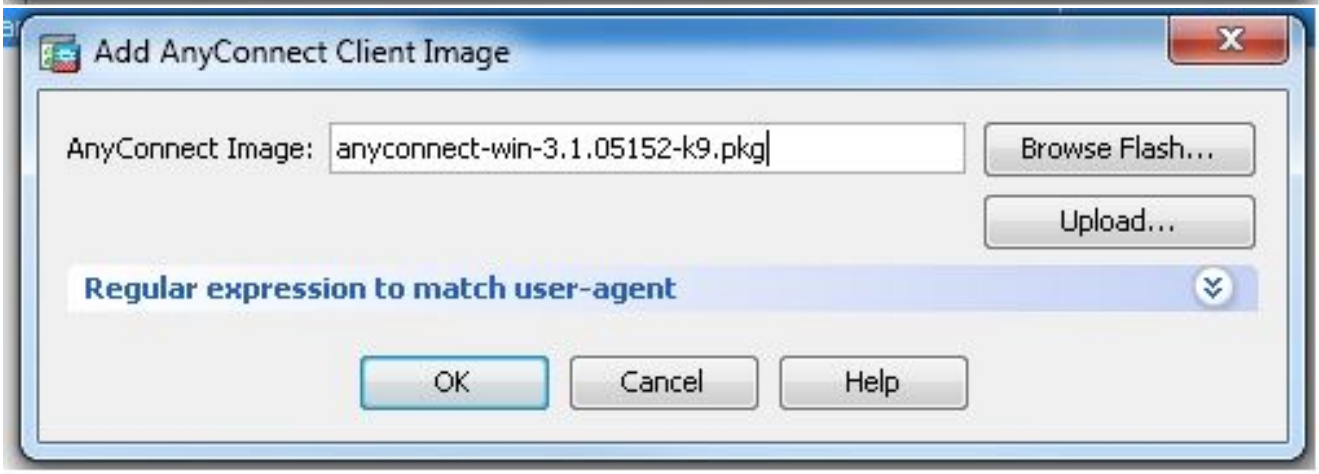
```
ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
```

4. *WebVPN をイネーブルにします。 選択* **Configuration > Remote Access VPN > Network (Client) Access >**

SSL VPN Connection Profiles *以下* **Access Interfaces***チェックボックスをクリックします* **Allow Access** *と* **Enable DTLS** *設定します。また、* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *外部インターフェイスでSSL VPNを有効にするには、このチェックボックスをオンにします。*



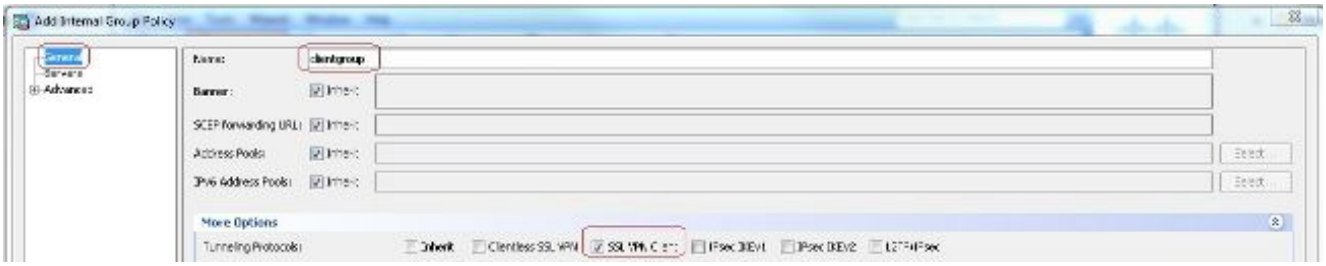
クリック **Apply**.*選択* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** *Cisco AnyConnect VPNクライアントイメージをASAのフラッシュメモリから次のように追加します。*



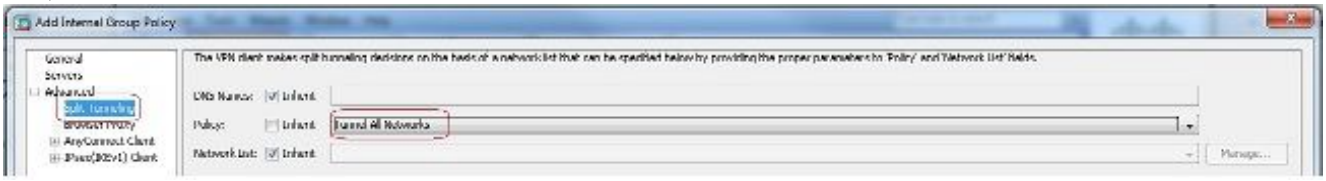
同等の CLI 設定

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable
```

5. *グループ ポリシーを設定します。 選択* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *内部グループポリシーを作成するため* **clientgroup**.*下* **General** *タブで、* **SSL VPN Client** *トンネルプロトコルとしてWebVPNを有効にするには、このチェックボックスをオンにします。*



内 **Advanced > Split Tunneling** *タブ、選択* **Tunnel All Networks** *リモートPCからのすべてのパケットがセキュアトンネルを通過するように、ポリシーの[Policy]ドロップダウンリストから設定します。*



同等の CLI 設定

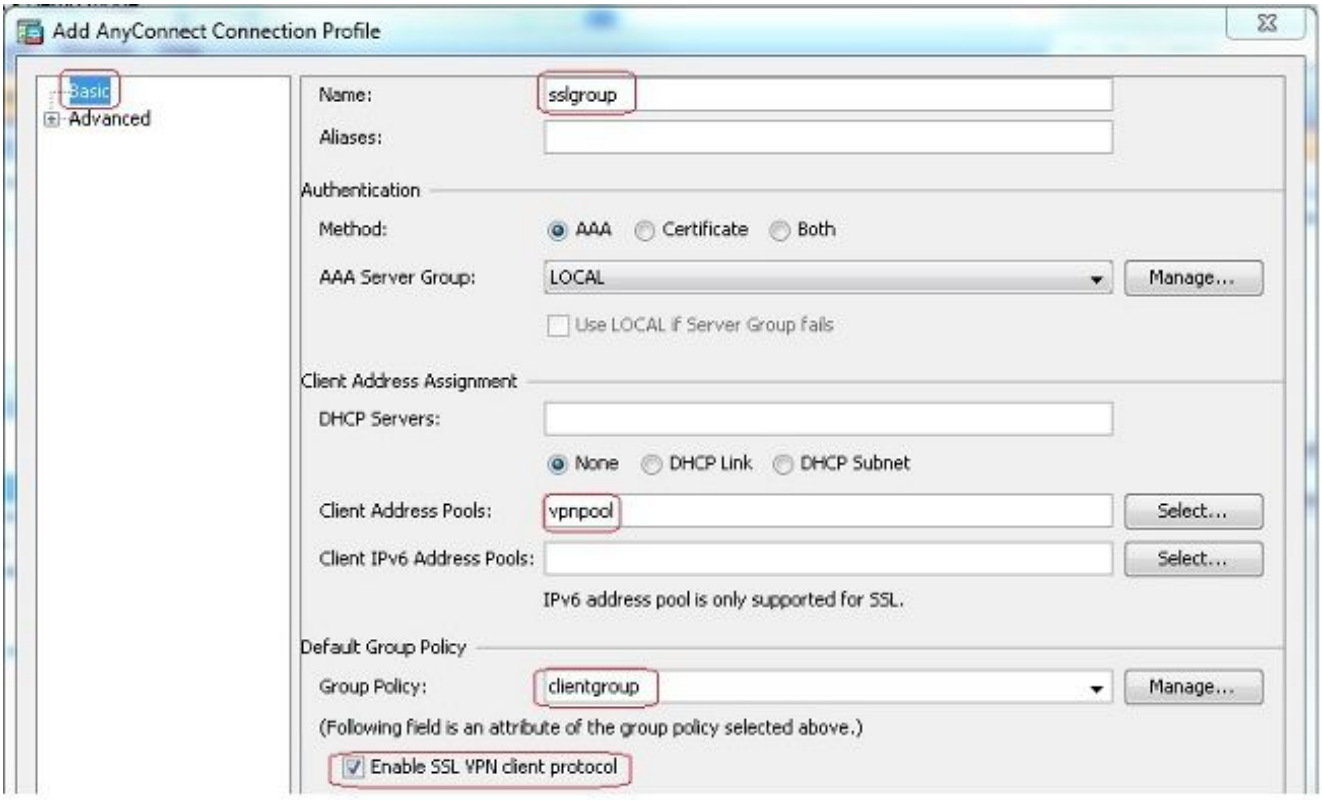
```
ciscoasa(config)#group-policy clientgroup internal
ciscoasa(config)#group-policyclientgroup attributes
ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client
ciscoasa(config-group-policy)#split-tunnel-policy tunnelall
```

6. *選択* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *新しいユーザアカウントを作成するため* **ssluser1**. *クリック* **OK** *それから* **Apply**.

同等の CLI 設定

```
ciscoasa(config)#username ssluser1 password asdmASA@
```

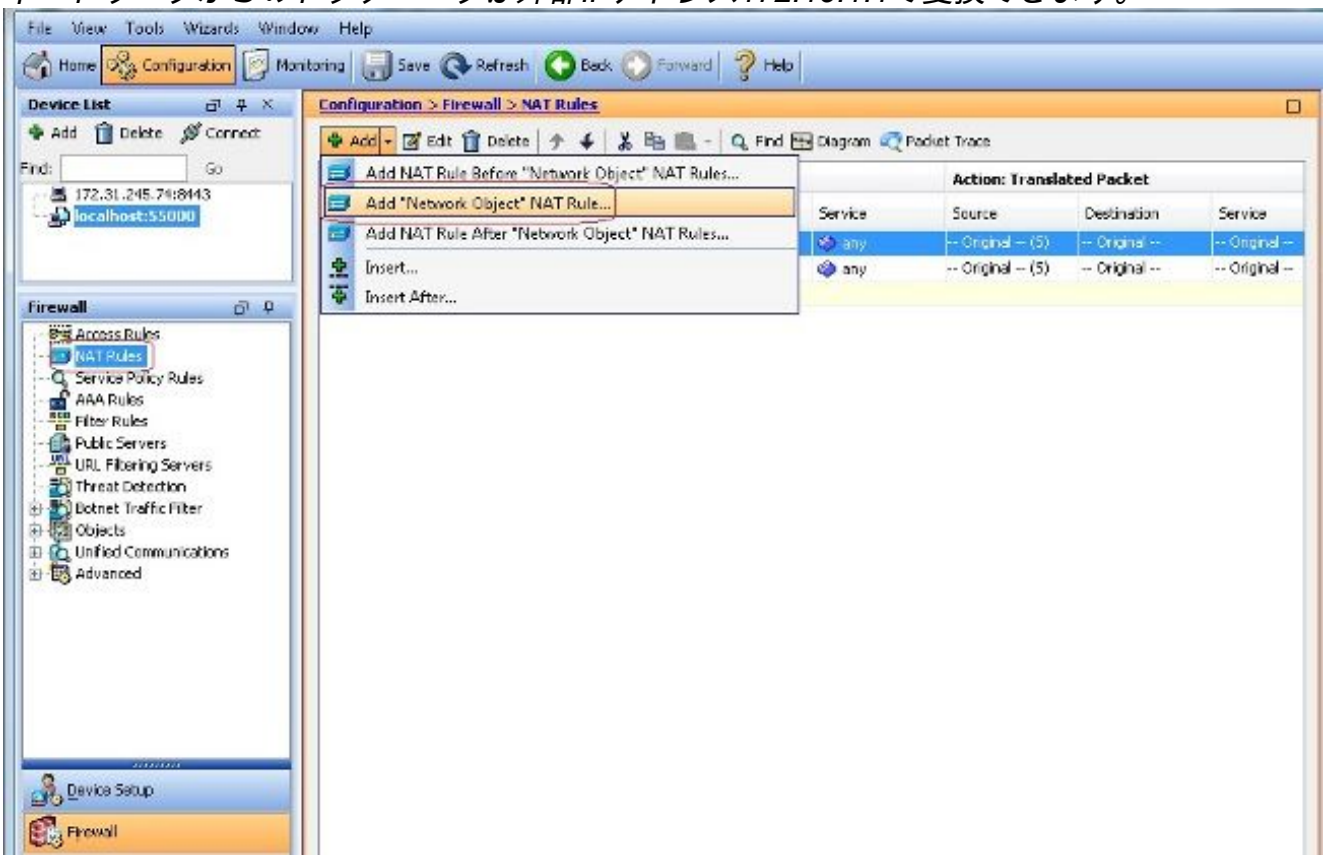
7. *トンネル グループを設定します。 選択* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *新しいトンネルグループを作成するため* **sslgroup**.*内* **Basic** *タブをクリックすると、次に示すように設定のリストを実行できます。 トンネルグループに次の名前を付けます。* **sslgroup**.*通常の* **Client Address Assignment** *アドレスプールを選択します。* **vpnpool Client Address Pools** *選択します。通常の* **Default Group Policy** *グループポリシーを選択します* **clientgroup Group Policy** *選択します。*

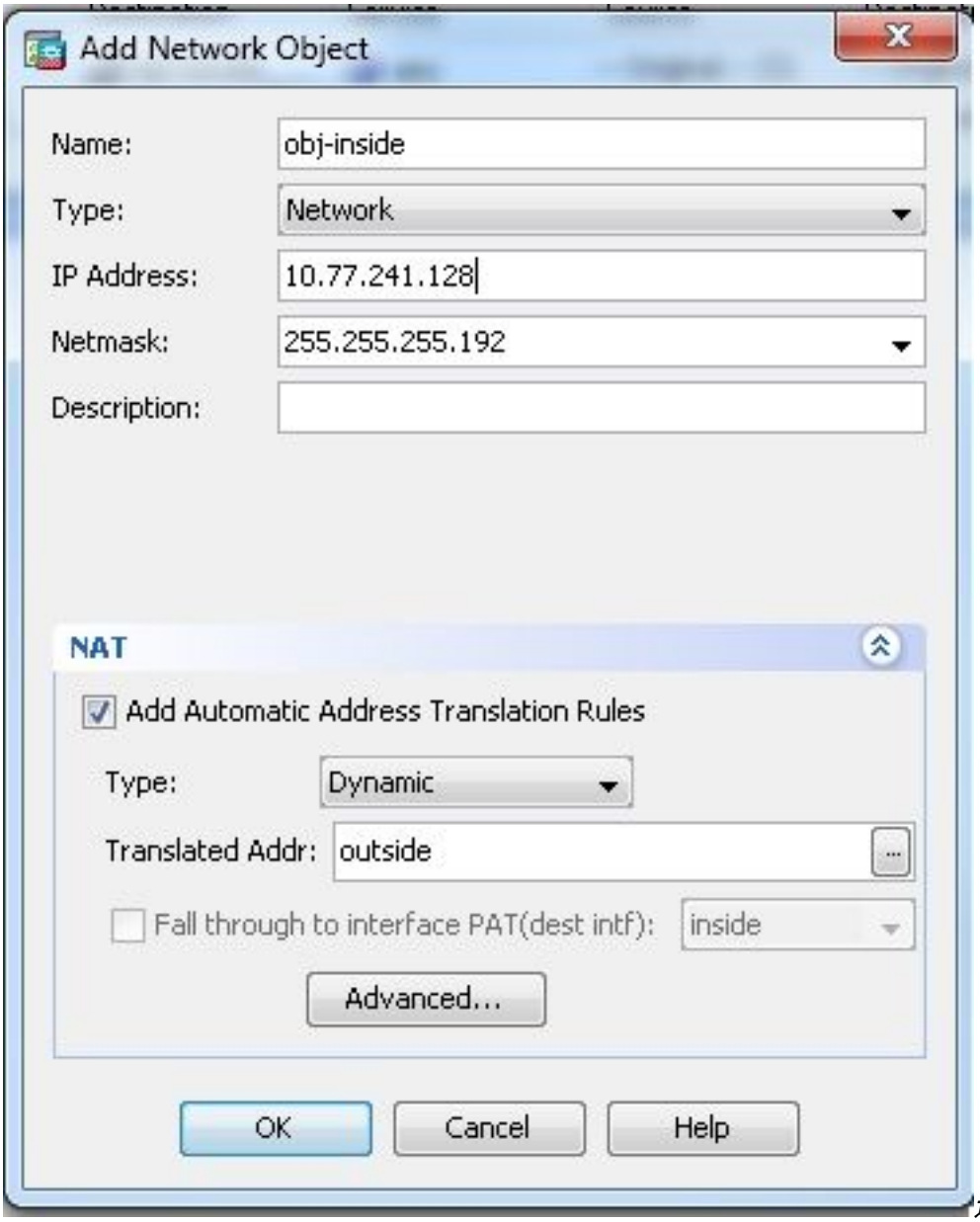


下 **Advanced > Group Alias/Group URL** *タブをクリックし、グループエイリアス名を* **sslgroup_users** *をクリックし、* **OK**. ***同等の CLI 設定***

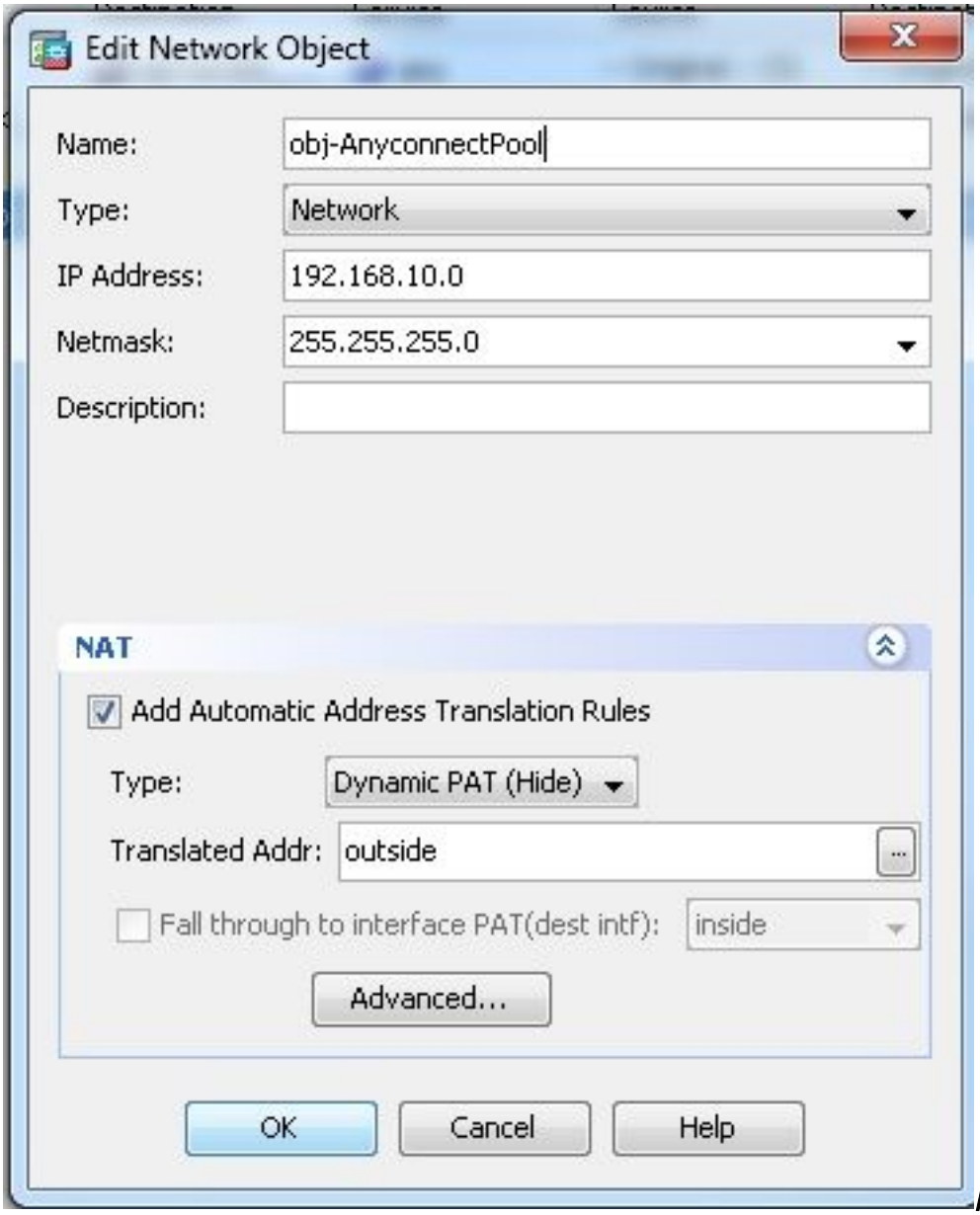
```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

8. *NAT の設定 選択* **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *そのため、内部ネットワークからのトラフィックは外部IPアドレス172.16.1.1で変換できます。*





選択 **Configuration > Firewall > NAT Rules > Add "Network Object" NAT Rule** *そのため、外部ネットワークからのVPNトラフィックに対するトラフィックは、外部IPアドレス172.16.1.1で変換できます。*



同等の CLI 設定

```
ciscoasa(config)# object network obj-inside
ciscoasa(config-network-object)# subnet 10.77.241.128 255.255.255.192
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
ciscoasa(config)# object network obj-AnyconnectPool
ciscoasa(config-network-object)# subnet 192.168.10.0 255.255.255.0
ciscoasa(config-network-object)# nat (outside,outside) dynamic interface
```

CLI の ASA リリース 9.1(2) の設定

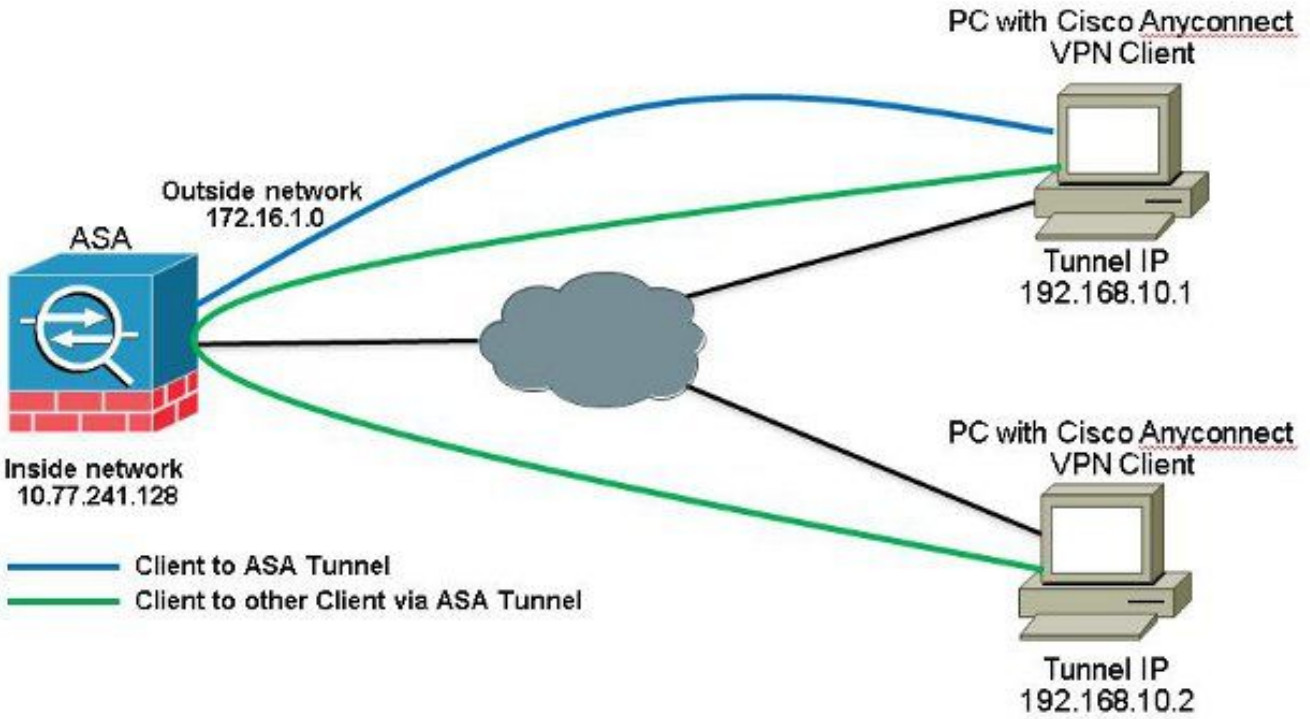
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
```

```
ip address 10.77.241.142 255.255.255.192
!
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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool
subnet 192.168.10.0 255.255.255.0
object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

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

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated
when going to the Anyconnect Pool.

object network obj-AnyconnectPool
nat (outside,outside) dynamic interface
object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and
Anyconnect Clients.
!--- Note: Uses an RFC 1918 range for lab setup.

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
```

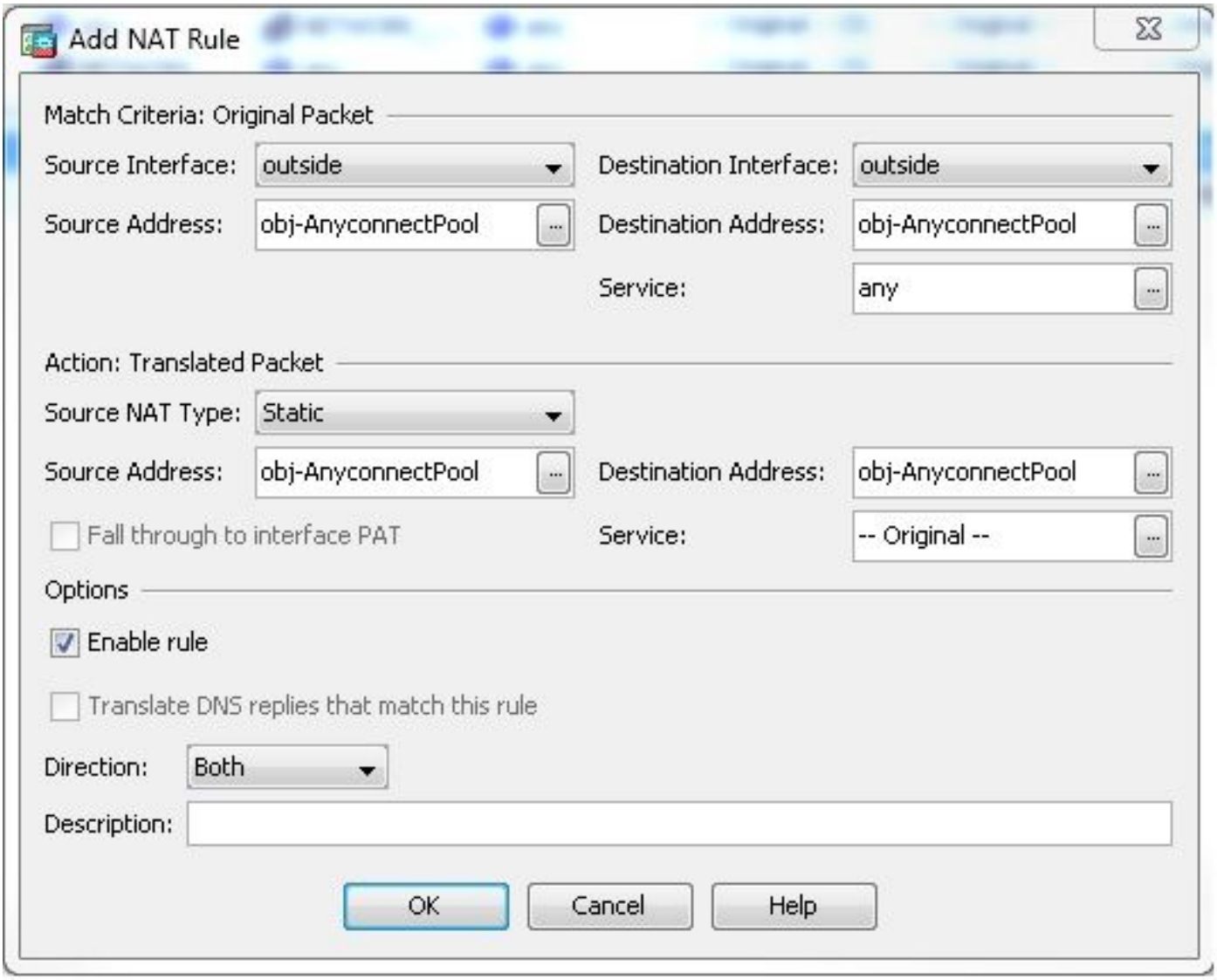
```
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection 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


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect 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 ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol


split-tunnel-policy tunnelall


!--- Encrypt all the traffic from the SSL VPN Clients.

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)#
```

TunnelAll 設定の実施による AnyConnect VPN Client 間の通信の許可ネットワーク図



AnyConnect Client 間の通信が必要で、公衆インターネット on a Stick 用の NAT が実施されている場合は、双方向通信を可能にするために手動 NAT も必要になります。これは、Anyconnectクライアントが電話サービスを使用し、相互にコールできる必要がある場合の一般的なシナリオです。ASDM リリース 7.1(6) での ASA リリース 9.1(2) の設定選択 Configuration > Firewall > NAT Rules > Add NAT Rule Before "Network Object" NAT Rules そのため、外部ネットワーク（Anyconnectプール）から送信され、同じプールから別のAnyconnectクライアントに送信されるトラフィックは、外部IPアドレス172.16.1.1で変換されません。



同等の CLI 設定

```
nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool destination
static obj-AnyconnectPool obj-AnyconnectPool
```

CLI の ASA リリース 9.1(2) の設定

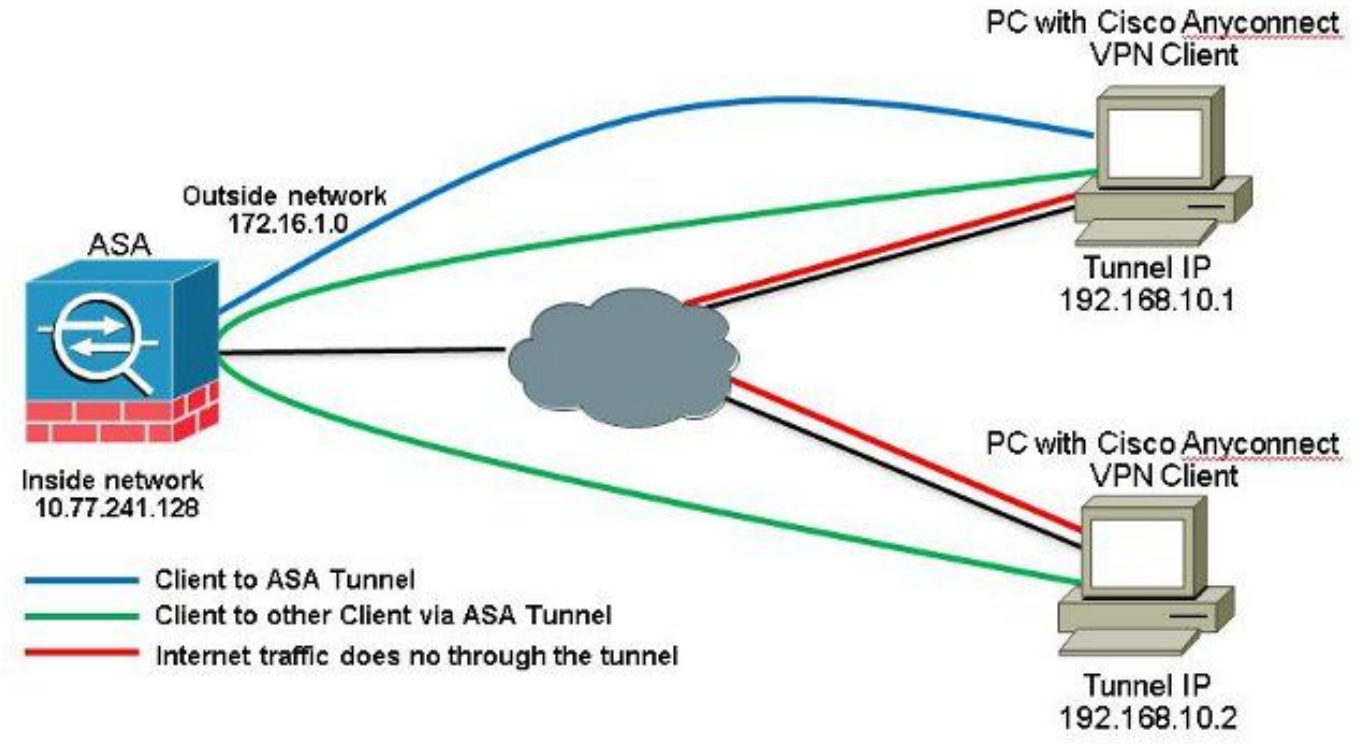
```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-AnyconnectPool
subnet 192.168.10.0 255.255.255.0
object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

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

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool
nat (outside,outside) source static obj-AnyconnectPool obj-AnyconnectPool
destination static obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT statements used so that traffic from the inside network
destined to the Anyconnect Pool and traffic from the Anyconnect Pool destined
to another Client within the same pool does not get translated.

object network obj-AnyconnectPool
nat (outside,outside) dynamic interface
object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users and
Anyconnect Clients.
!--- Note: Uses an RFC 1918 range for lab setup.

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


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect 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"
```

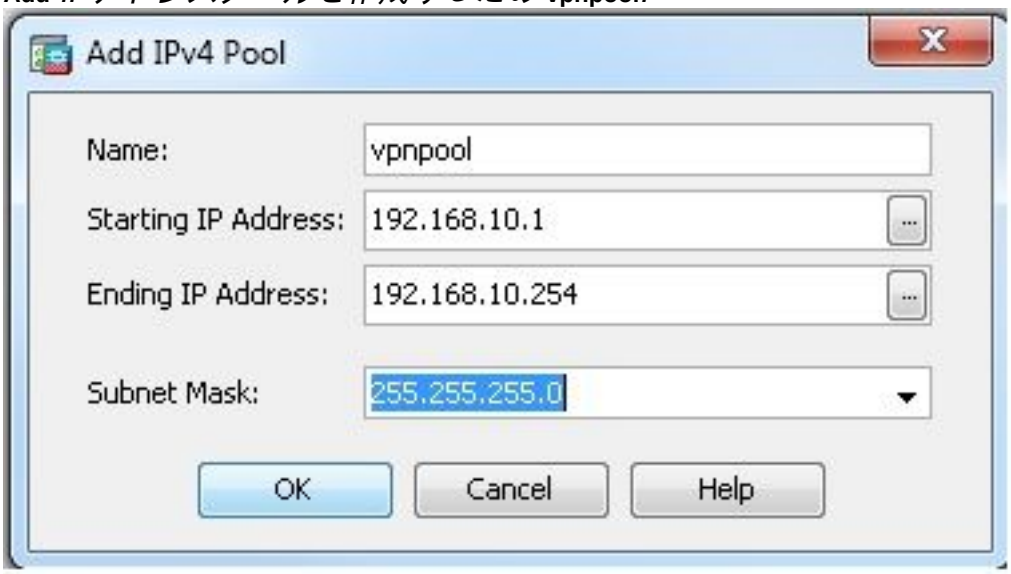
```
group-policy clientgroup attributes
vpn-tunnel-protocol ssl-client

!--- Specify SSL as a permitted VPN tunneling protocol

split-tunnel-policy tunnelall

!--- Encrypt all the traffic from the SSL VPN Clients.

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)#
```

スプリットトンネルを使用した AnyConnect VPN Client 間の通信ネットワーク図



Anyconnectクライアント間の通信が必要で、スプリットトンネルが使用される場合。このトラフィックの設定に影響を与える NAT ルールがない限り、双方向通信を可能にするために手動 NAT を使用する必要はありません。ただし AnyConnect VPN Pool はスプリットトンネル ACL に含む必要があります。これは、Anyconnectクライアントが電話サービスを使用し、相互にコールできる必要がある場合の一般的なシナリオです。ASDM リリース 7.1(6) での ASA リリース 9.1(2) の設定

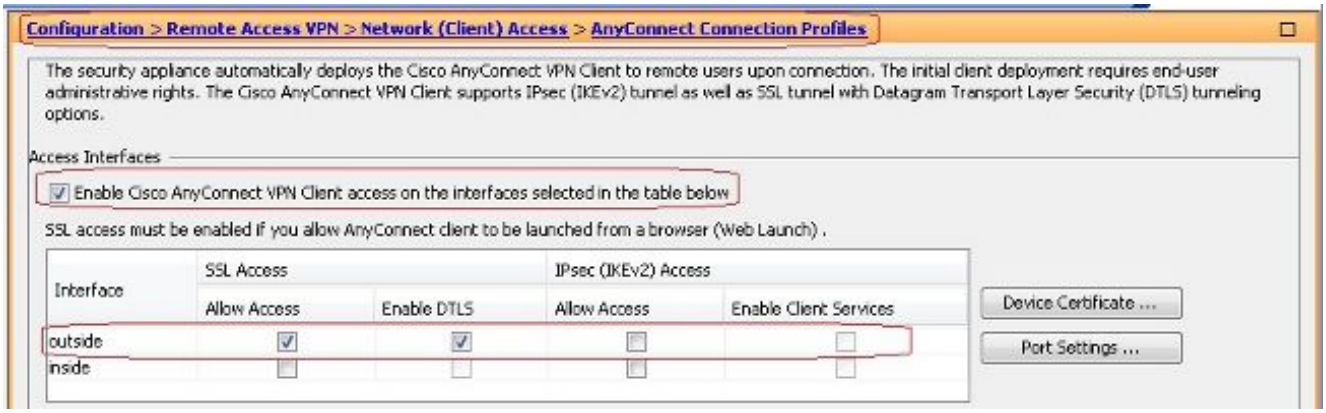
1. *選択* **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment> Address Pools > Add** *IPアドレスプールを作成するため* **vpnpool**.



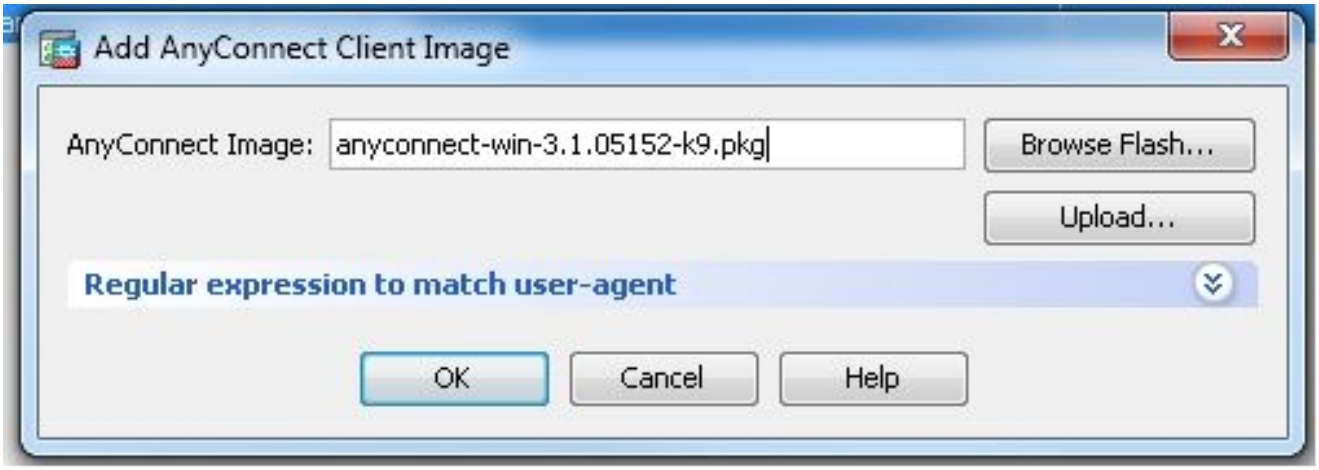
2. *クリック* **Apply**. ***同等の CLI 設定***

```
ciscoasa(config)#ip local pool vpnpool 192.168.10.1-192.168.10.254 mask 255.255.255.0
```

3. *WebVPN をイネーブルにします。 選択* **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles** *以下* **Access Interfaces***チェックボックスをクリックします* **Allow Access** *と* **Enable DTLS** *設定します。また、* **Enable Cisco AnyConnect VPN Client access on the interfaces selected in the table below** *外部インターフェイスでSSL VPNを有効にするには、このチェックボックスをオンにします。*



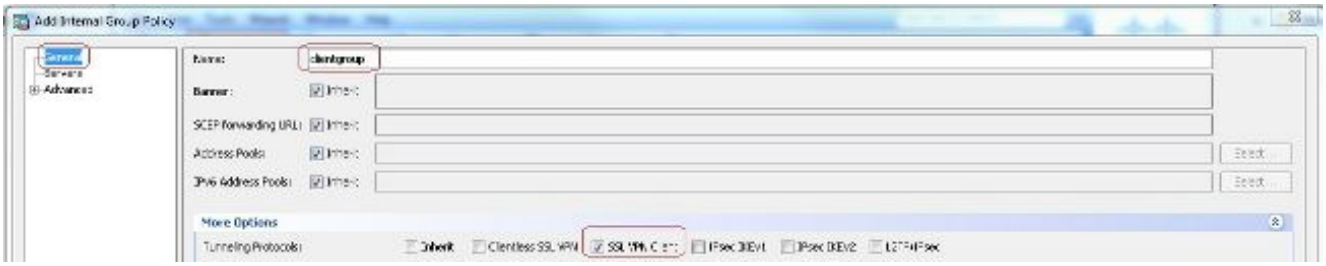
クリック **Apply.***選択* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Client Software > Add** *Cisco AnyConnect VPNクライアントイメージをASAのフラッシュメモリから次のように追加します。*



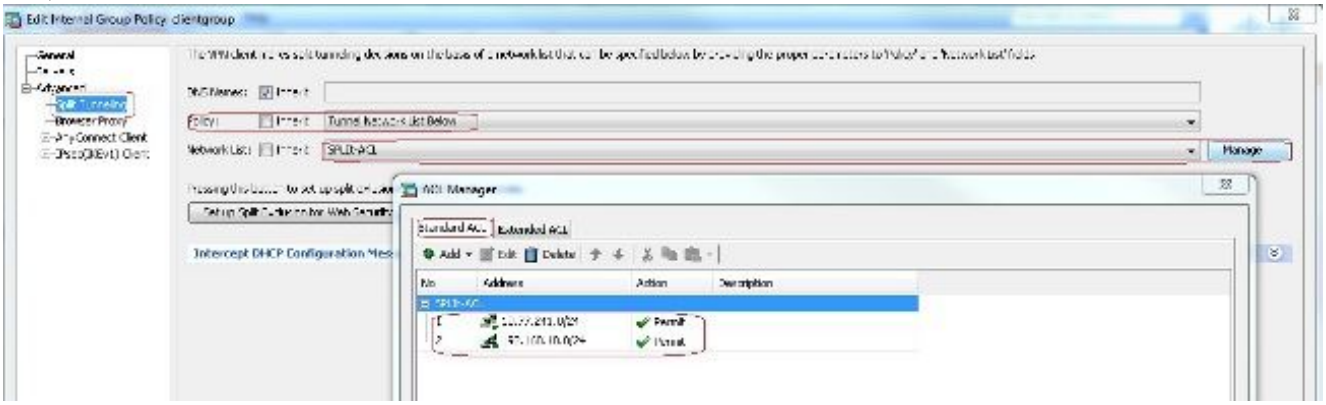
同等の CLI 設定

```
ciscoasa(config)#webvpn
ciscoasa(config-webvpn)#enable outside
ciscoasa(config-webvpn)#anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
ciscoasa(config-webvpn)#tunnel-group-list enable
ciscoasa(config-webvpn)#anyconnect enable
```

4. *グループ ポリシーを設定します。 選択* **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** *内部グループポリシーを作成するため* **clientgroup.***下* **General** *タブで、* **SSL VPN Client** *チェックボックスをオンにして、WebVPNを許可されたトンネルプロトコルとして有効にします。*



内 **Advanced > Split Tunneling** *タブ、選択* **Tunnel Network List Below** *[Policy]ドロップダウンリストから選択して、リモートPCからのすべてのパケットがセキュアトンネルを通過するようにします。*



同等の CLI 設定

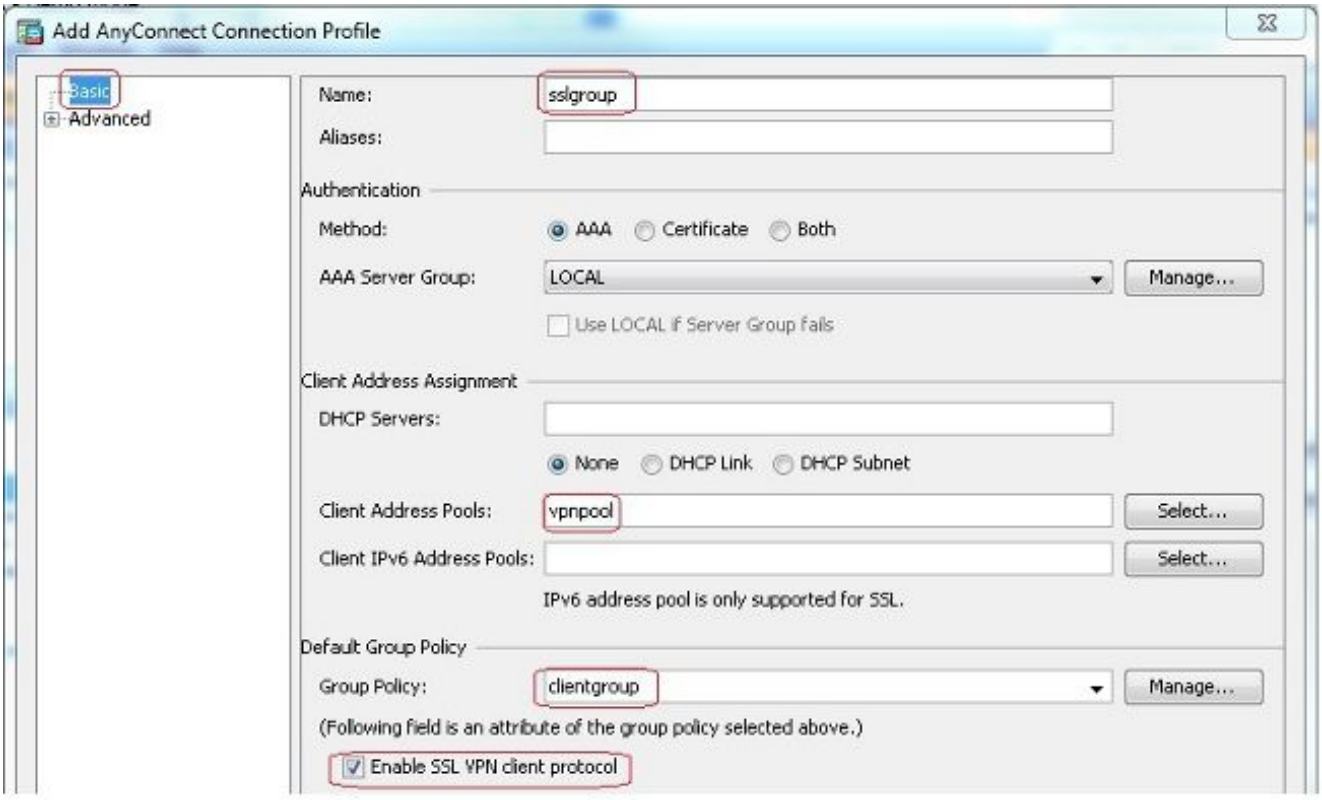
```
ciscoasa(config)#access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0
ciscoasa(config)#access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

ciscoasa(config)#group-policy clientgroup internal
ciscoasa(config)#group-policy clientgroup attributes
ciscoasa(config-group-policy)#vpn-tunnel-protocol ssl-client
ciscoasa(config-group-policy)#split-tunnel-policy tunnelspecified
ciscoasa(config-group-policy)#split-tunnel-network-list SPLIt-ACL
```

5. *選択* **Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add** *新しいユーザアカウントを作成するため* **ssluser1**. *クリック* **OK** *それから* **Apply**.

同等の CLI 設定

```
ciscoasa(config)#username ssluser1 password asdmASA@
```

6. *トンネル グループを設定します。 選択* **Configuration > Remote Access VPN > Network (Client) Access > Anyconnect Connection Profiles > Add** *新しいトンネルグループを作成するため* **sslgroup**.*内* **Basic** *タブをクリックすると、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次の名前を付けます。* **sslgroup**.*通常の* **Client Address Assignment** *アドレスプールを選択します。* **vpnpool Client Address Pools** *選択します。通常の* **Default Group Policy** *グループポリシーを選択します* **clientgroup Group Policy** *選択します。*



下 **Advanced > Group Alias/Group URL** タブをクリックし、グループエイリアス名を **sslgroup_users** をクリックし、 **OK**. *同等の CLI 設定*

```
ciscoasa(config)#tunnel-group sslgroup type remote-access
ciscoasa(config)#tunnel-group sslgroup general-attributes
ciscoasa(config-tunnel-general)#address-pool vpnpool
ciscoasa(config-tunnel-general)#default-group-policy clientgroup
ciscoasa(config-tunnel-general)#exit
ciscoasa(config)#tunnel-group sslgroup webvpn-attributes
ciscoasa(config-tunnel-webvpn)#group-alias sslgroup_users enable
```

CLI の ASA リリース 9.1(2) の設定

```
ciscoasa(config)#show running-config
: Saved
:
ASA Version 9.1(2)
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.77.241.142 255.255.255.192
!
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
same-security-traffic permit intra-interface

!--- Command that permits the SSL VPN traffic to enter and exit the same interface.

object network obj-inside
subnet 10.77.241.128 255.255.255.192

!--- Commands that define the network objects we will use later on the NAT section.

access-list SPLIt-ACL standard permit 10.77.241.0 255.255.255.0
access-list SPLIt-ACL standard permit 192.168.10.0 255.255.255.0

!--- Standard Split-Tunnel ACL that determines the networks that should travel the
Anyconnect tunnel.

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

nat (inside,outside) source static obj-inside obj-inside destination static
obj-AnyconnectPool obj-AnyconnectPool

!--- The Manual NAT that prevents the inside network from getting translated when
going to the Anyconnect Pool

object network obj-inside
nat (inside,outside) dynamic interface

!--- The Object NAT statements for Internet access used by inside users.
!--- Note: Uses an RFC 1918 range for lab setup.

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


anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1


!--- Assign an order to the AnyConnect SSL VPN Client image


anyconnect 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 ssl-client


!--- Specify SSL as a permitted VPN tunneling protocol
```

```
split-tunnel-policy tunnelspecified

!--- Encrypt only traffic specified on the split-tunnel ACL coming from the SSL
VPN Clients.

split-tunnel-network-list value SPLIt-ACL

!--- Defines the previosly configured ACL to the split-tunnel policy.

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)#
```

確認 ここでは、設定が正常に機能しているかどうかを確認します。

- **show vpn-sessiondb svc** – 現在のSSL接続に関する情報を表示します。

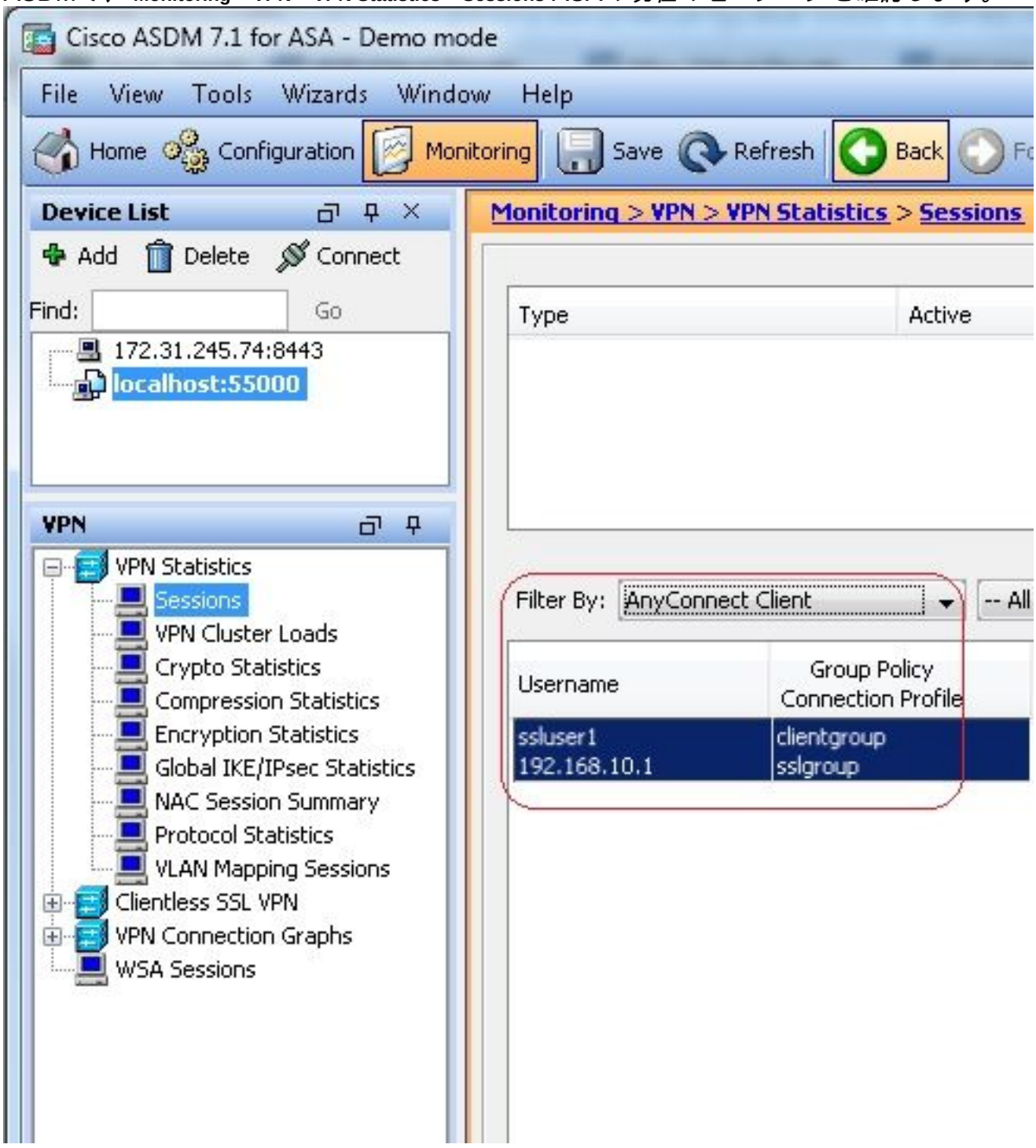
```
ciscoasa#show vpn-sessiondb anyconnect

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の設定済み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** ASAの現在のセッションを確認します。



トラブルシュート ここでは、設定のトラブルシューティングに使用できる情報を示します。

- **vpn-sessiondb logoff name** – 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。

```
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)
```

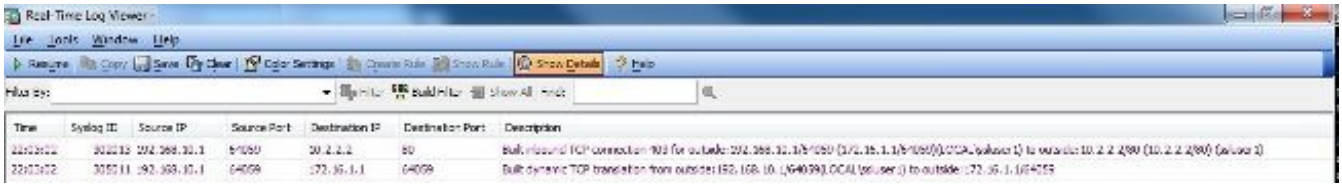
同様に、 **vpn-sessiondb logoff anyconnect** すべてのAnyConnectセッションを終了します。

- **debug webvpn anyconnect <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 anyconnect 7

CSTP state = HEADER_PROCESSING
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: 10.198.16.132'
Processing CSTP header line: 'Host: 10.198.16.132'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 3.1.05152'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows
3.1.05152'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 3.1.05152'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Processing CSTP header line: 'Cookie: webvpn=
146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
Found WebVPN cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
WebVPN Cookie: 'webvpn=146E70@20480@567F@50A0DFF04AFC2411E0DD4F681D330922F4B21F60'
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: WCRSJOW7Pnbc038'
Processing CSTP header line: 'X-CSTP-Hostname: WCRSJOW7Pnbc038'
Setting hostname to: 'WCRSJOW7Pnbc038'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1280'
Processing CSTP header line: 'X-CSTP-MTU: 1280'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1300'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1300'
webvpn_cstp_parse_request_field()
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0A602CF075972F91EAD1
9BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
Processing CSTP header line: 'X-DTLS-Master-Secret: F1810A764A0646376F7D254202A0
A602CF075972F91EAD19BB6BE387BB8C6F893BFB49886D47F9A4BE2EA2A030BF620D'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3-SHA:DES-CBC-SHA'
Processing CSTP header line: 'X-DTLS-CipherSuite: AES256-SHA:AES128-SHA:DES-CBC3
-SHA:DES-CBC-SHA'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
```

```
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Validating address: 0.0.0.0
CSTP state = WAIT_FOR_ADDRESS
webvpn_cstp_accept_address: 192.168.10.1/255.255.255.0
webvpn_cstp_accept_ipv6_address: No IPv6 Address
CSTP state = HAVE_ADDRESS
SVC: Sent gratuitous ARP for 192.168.10.1.
SVC: NP setup
np_svc_create_session(0x5000, 0xa930a180, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
vpn_put_uauth success for ip 192.168.10.1!
No SVC ACL
Iphdr=20 base-mtu=1300 def-mtu=1500 conf-mtu=1406
tcp-mss = 1260
path-mtu = 1260(mss)
mtu = 1260(path-mtu) - 0(opts) - 5(ssl) - 8(cstp) = 1247
tls-mtu = 1247(mtu) - 20(mac) = 1227
DTLS Block size = 16
mtu = 1300(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1243
mod-mtu = 1243(mtu) & 0xfff0(complement) = 1232
dtls-mtu = 1232(mod-mtu) - 1(cdtp) - 20(mac) - 1(pad) = 1210
computed tls-mtu=1227 dtls-mtu=1210 conf-mtu=1406
DTLS enabled for intf=2 (outside)
tls-mtu=1227 dtls-mtu=1210
SVC: adding to sessmgmt

Unable to initiate NAC, NAC might not be enabled or invalid policy
CSTP 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
```

- ASDMで、 **Monitoring > Logging > Real-time Log Viewer > View** リアルタイムのイベントを表示します。次に、ASA 172.16.1.1 経由のインターネットにおける、AnyConnect 192.168.10.1 と Telnet Server 10.2.2.2 の間のセッション情報の例を示します。



関連情報

- Cisco ASA 5500-Xシリーズファイアウォール
- 公衆インターネット VPN on a Stick のための PIX/ASA および VPN Client 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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。