アドレス割り当て DHCP を使用した ASA への AnyConnect クライアント

目次

概要

この資料に DHCPサーバに Anyconnect すべてのクライアントにクライアントIPアドレスを提供させます Adaptive Security Device Manager （ASDM）または CLI の使用で Cisco 5500-X シリーズを（ASA）適応型セキュリティ アプライアンス（ASA）ソフトウェア設定する方法を記述されています。

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:** [本 1 を](#)参照して下さい[: Cisco ASA シリーズ 操作全般 CLI コンフィギュレーション ガイド、](#)リモートで ASDM かセキュア シェル（SSH）によって設定されるようにデバイスがする [9.2](#)。

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 ASA 5500-X 次世代 ファイアウォールバージョン 9.2(1)
- Adaptive Security Device Manager バージョン 7.1(6)
- Cisco AnyConnect セキュア モビリティ クライアント 3.1.05152

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

この設定も Cisco ASA セキュリティ アプライアンス モデル 5500 シリーズ バージョン 7.x および それ 以降と使用することができます。

背景説明

リモート アクセス VPN は、モバイル ユーザからの要求を処理し、組織のネットワークに安全に接続できるようにします。 モバイルユーザは Cisco AnyConnect セキュア モビリティ クライアント ソフトウェアを使用して信頼できる接続を設定できます。 Cisco AnyConnect セキュア モビリティ クライアントはこれらの要求を受け入れるために設定されるセントラルサイト デバイスへの接続を開始します。 この例では、ダイナミック暗号マップを使用するセントラルサイト デバイスは適応型セキュリティ アプライアンス（ASA）ソフトウェア ASA 5500-X シリーズです。

セキュリティ アプライアンス モデル アドレス管理では、プライベート ネットワークに直接接続されたように、トンネルによって接続し、プライベート ネットワークのリソースとクライアントをクライアント関数を可能にする IP アドレスを設定しなければなりません。

なお、クライアントに割り当てられる私用 IP アドレスをだけ取扱っています。 プライベート ネットワーク上のその他のリソースに割り当てられた IP アドレスは、VPN 管理ではなく、ネットワーク管理業務の一部に位置づけられます。 従って、IP アドレスがここで説明されているとき、Cisco はトンネルエンドポイントとしてクライアント関数を可能にするプライベート ネットワーク アドレス方式で利用可能 なそれらの IP アドレスを意味します。

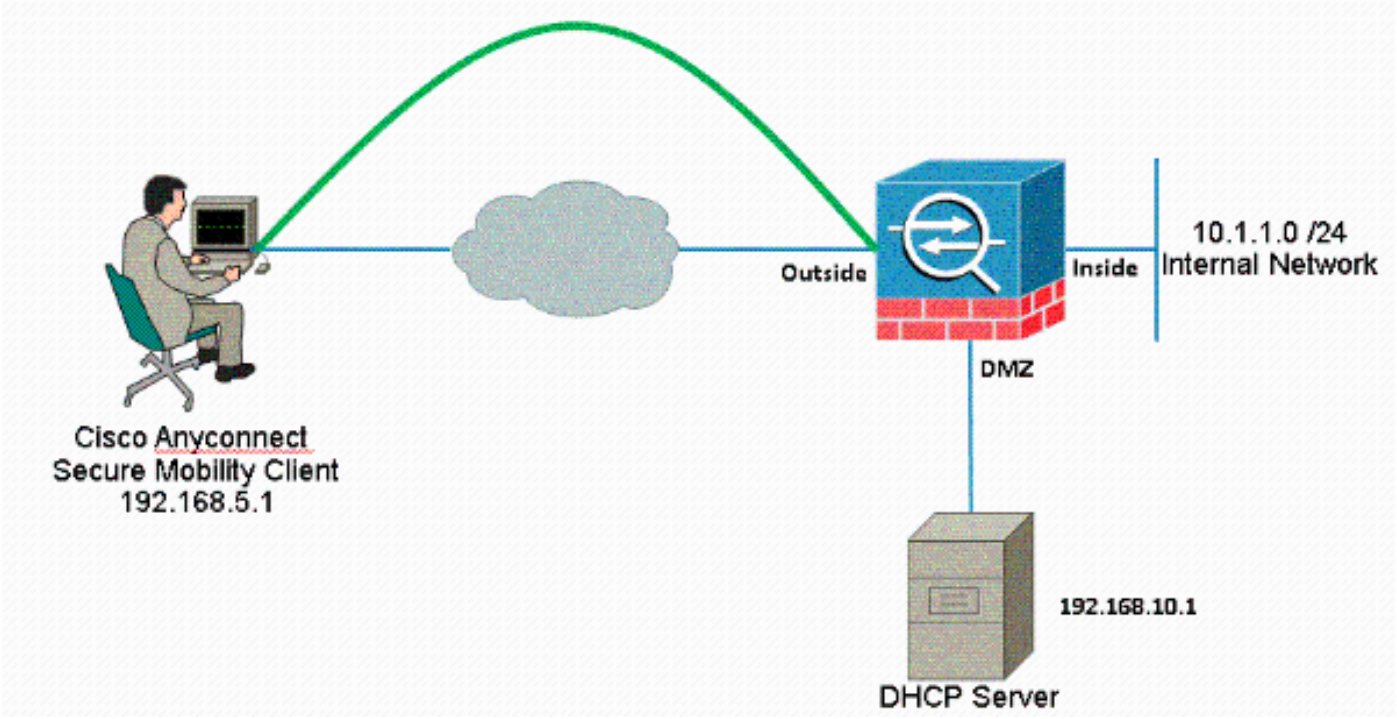
設定

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 RFC 1918 でのアドレスであり、ラボ環境で使用されたものです。

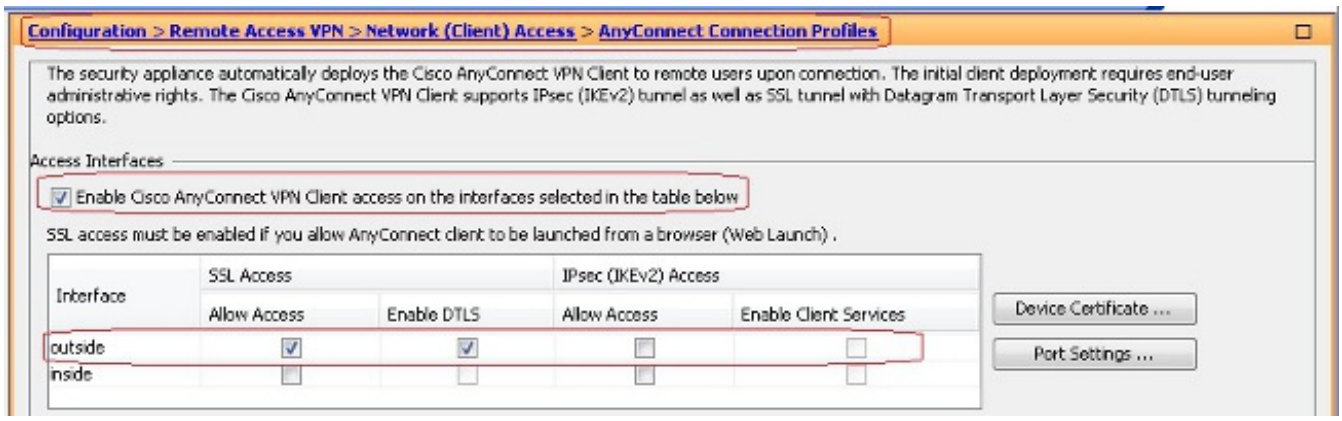
設定 Cisco AnyConnect セキュア モビリティ クライアント

ASDM の手順

リモート アクセス VPN を設定するには、次の手順を実行します。

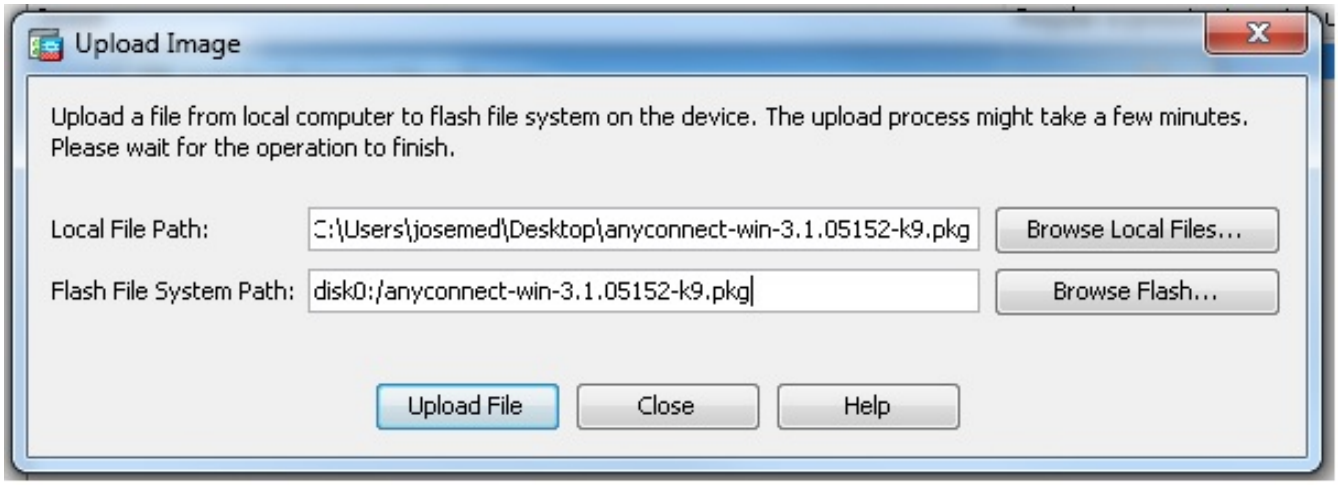
- WebVPN をイネーブルにします。

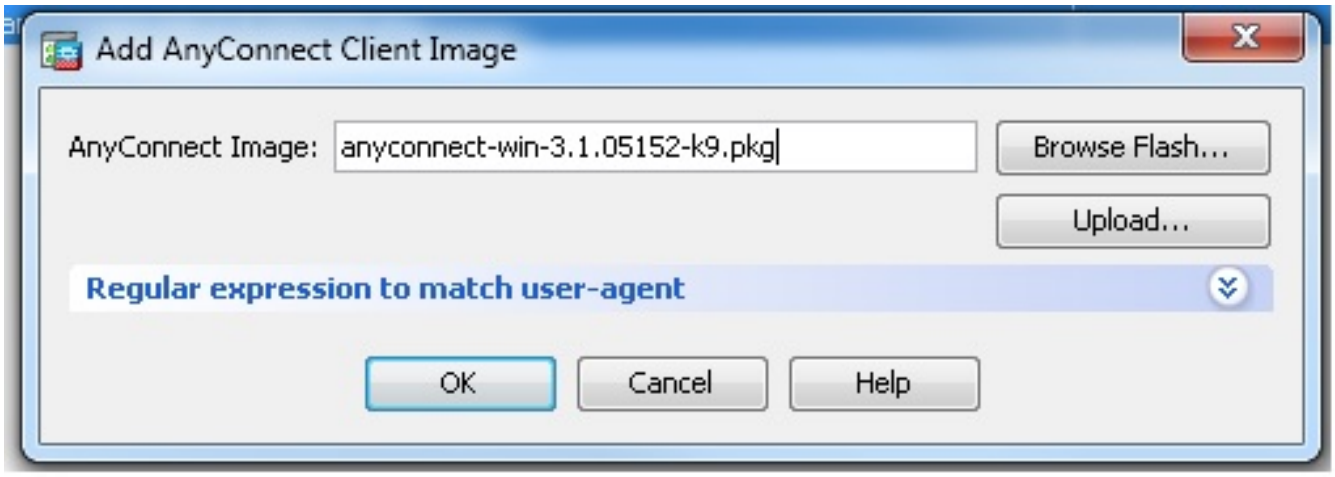
  [Configuration] > [Remote Access VPN] > [Network (Client) Access] > [SSL VPN Connection Profiles] を選択し、[Access Interfaces] の下で、外部インターフェイスに対して [Allow Acces] と [Enable DTLS] のチェックボックスをオンにします。 また、outside インターフェイスの SSL VPN を有効に するために**この表** チェックボックス**で選択されるインターフェイスのイネーブル Cisco AnyConnect VPN Client かレガシー SSL VPN クライアント アクセス**をチェックして下さい。



[Apply] をクリックします。

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Anyconnect Client Software] > [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。



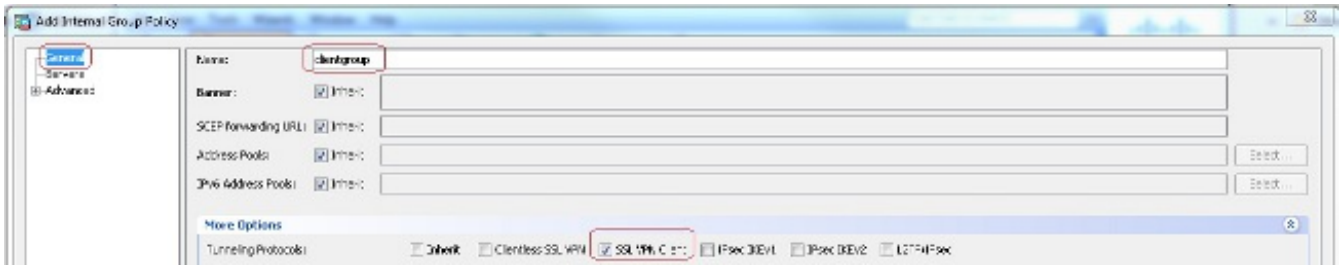


同等の CLI 設定：

```
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
```

- 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、トンネリング プロトコルとして SSL を有効に するために **SSL VPN クライアント** チェックボックスを選択して下さい。



サーバ タブの DHCP ネットワーク スコープを設定して下さい、ユーザ向けの DHCP スコープを自動的に割り当てられるために設定するために**オプションを**『More』 を選択 して下さい。

同等の CLI 設定：

```
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)#
```

- [Configuration] > [Remote Access VPN] > [AAA/Local Users] > [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。

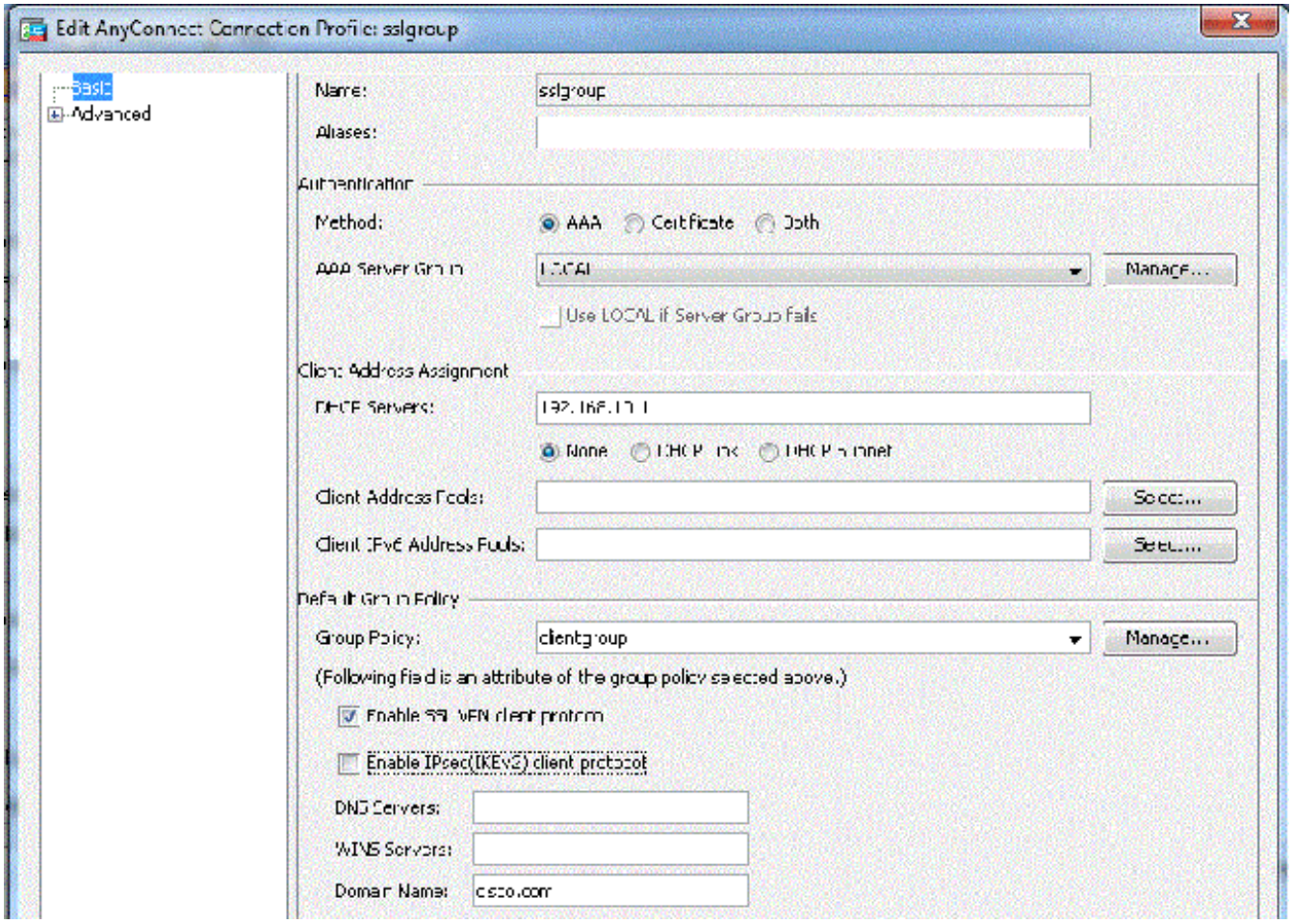
同等の CLI 設定：`ciscoasa(config)#`**`username ssluser1 password asdmASA`**

- トンネル グループを設定します。

[Configuration] > [Remote Access VPN] > [Network (Client) Access] > [Anyconnect 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。[DHCP Servers] 用のスペースに DHCP サーバの IP アドレスを指定します。[Default Group Policy] の下で、[Group Policy] 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。DHCP リンクか DHCP サブネットを設定して下さい。



[Advanced] > [Group Alias/Group URL] 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。

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)#dhcp-server 192.168.10.1
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
```

サブネット の 選択かリンク選択

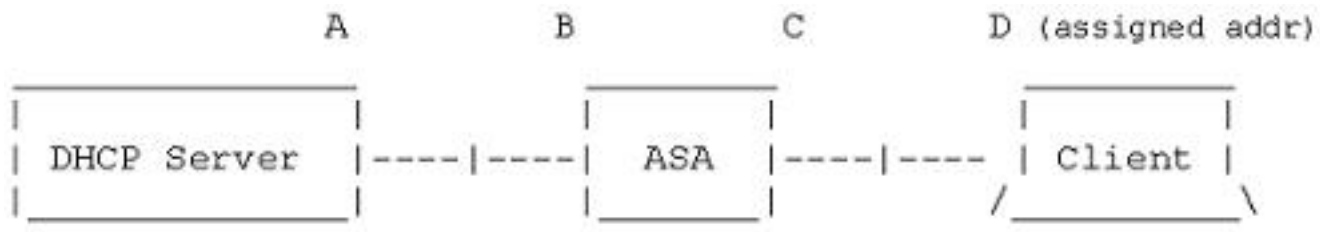
RFC 3011 および RFC 3527 のための DHCP プロキシ サポートは 8.0.5 および 8.2.2 で導入される機能であり、前方リリースでサポートされました。

- RFC 3011 は新しい DHCP オプションを、DHCP クライアントがアドレスを割り当てるためサブネットを規定 するようにするサブネット の 選択 オプション定義します。 このオプションは DHCPサーバがアドレスを選択するためサブネットを判別するのに使用する方式に優先します。
- RFC 3527 は新しい DHCP サブオプションを、DHCP クライアントが DHCPサーバが応答する必要があるアドレスを規定 するようにするリンク選択サブオプション定義します。

ASA の点では、これらの RFC はユーザが ASA にローカルではない、DHCPサーバはまだ ASA のインターフェイスに直接答えられます DHCPアドレス 割り当てのための dhcp ネットワーク ス

コープを規定 することを可能にし。 下記の図は新しい動作の説明を助ける必要があります。 これはネットワークのそのスコープのためのスタティック ルートを作成しないで使用に非ローカルなスコープを与えます。

RFC 3011 か RFC 3527 が有効に ならないとき、DHCP プロキシ交換はこれに類似したに検知します:



Message Exchange:

Discover: B -> A

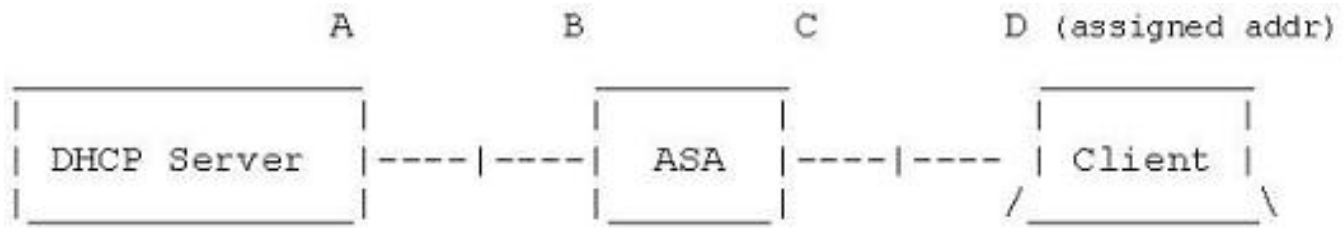
Offer: A -> dhcp-network-scope

Request: B -> A

Ack: A -> dhcp-network-scope

Release: B -> A

有効に なるこれらの RFC のどちらかによって交換はこれに代りに類似したに検知 し、VPN クライアントまだ正しいサブネットのアドレスは割り当てられます:



Message Exchange:

Discover: B -> A

Offer: A -> B

Request: B -> A

Ack: A -> B

Release: B -> A

CLI の使用で ASA を設定して下さい

後述のステップを実行して DHCP サーバを設定し、コマンドラインから VPN Client に IP アドレスを割り当てます。 Cisco ASA 5500 シリーズ各コマンドに関する詳細については適応性があるセキュリティ アプライアンス コマンド参照を参照して下さい使用される。

```
ASA#show run
ASA Version 9.2(1)
!

!--- Specify the hostname for the Security Appliance.

hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!


!--- Configure the outside and inside interfaces.

interface GigabitEthernet0/0
nameif inside
security-level 100
ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/1
nameif outside
security-level 0
ip address 192.168.1.1 255.255.255.0
!
interface GigabitEthernet0/2
nameif DMZ
security-level 50
ip address 192.168.10.2 255.255.255.0


!--- Output is suppressed.


passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/asa802-k8.bin
ftp mode passive

object network obj-10.1.1.0
subnet 10.1.1.0 255.255.255.0
object network obj-192.168.5.0
subnet 192.168.5.0 255.255.255.0

pager lines 24
logging enable
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu dmz 1500
no failover
icmp unreachable rate-limit 1 burst-size 1


!--- Specify the location of the ASDM image for ASA to fetch the image
for ASDM access.

asdm image disk0:/asdm-716.bin
no asdm history enable
arp timeout 14400
```

```
nat (inside,outside) source static obj-10.1.1.0 obj-10.1.1.0 destination static
obj-192.168.5.0 obj-192.168.5.0
!
object network obj-10.1.1.0
nat (inside,outside) dynamic interface
route outside 0.0.0.0 0.0.0.0 192.168.1.2 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
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
!
!--- Enable webvpn and specify an Anyconnect image

webvpn
enable outside
anyconnect image disk0:/anyconnect-win-3.1.05152-k9.pkg 1
anyconnect enable
tunnel-group-list enable


group-policy clientgroup internal
group-policy clientgroup attributes


!--- define the DHCP network scope in the group policy.This configuration is Optional
```

```
dhcp-network-scope 192.168.5.0


!--- In order to identify remote access users to the Security Appliance,
!--- you can also configure usernames and passwords on the device.

username ssluser1 password ffIRPGpDSOJh9YLq encrypted


!--- Create a new tunnel group and set the connection
!--- type to remote-access.

tunnel-group sslgroup type remote-access


!--- Define the DHCP server address to the tunnel group.

tunnel-group sslgroup general-attributes
default-group-policy clientgroup
dhcp-server 192.168.10.1

!--- If the use of RFC 3011 or RFC 3527 is required then the following command will
enable support for them

tunnel-group sslgroup general-attributes
dhcp-server subnet-selection (server ip) (3011)
hcp-server link-selection (server ip) (3527)

!--- Configure a group-alias for the tunnel-group

tunnel-group sslgroup webvpn-attributes
group-alias sslgroup_users enable

prompt hostname context
Cryptochecksum:e0725ca9ccc28af488ded9ee36b7822d
: end
ASA#
```