ASA的Anyconnect客户端与使用地址分配的DHCP

目录

简介

本文描述如何配置Cisco 5500-X系列可适应安全工具(ASA)做DHCP服务器提供客户端IP地址给所有Anyconnect客户端以使用可适应安全设备管理器(ASDM)或CLI。

先决条件

要求

本文档假设 ASA 处于完全运行状态，并配置为允许 Cisco ASDM 或 CLI 进行配置更改。

> **注意**： 参考的书1 ：思科ASA系列一般操作CLI配置指南，允许设备的9.2远程配置由ASDM或安全壳SSH。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco ASA 5500-X下一代防火墙版本9.2(1)
- 可适应安全设备管理器版本7.1(6)
- Cisco AnyConnect安全移动客户端3.1.05152

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

相关产品

此配置可能也与Cisco ASA安全工具5500系列版本7.x和以上一起使用。

背景信息

远程访问 VPN 满足了移动工作者的安全连接组织网络的需要。使用Cisco AnyConnect安全移动客户端软件，移动用户能设置安全连接。Cisco AnyConnect安全移动客户端首次对中心站点已配置设备的连接接受这些请求。在本例中，中心站点设备是使用动态加密映射的ASA 5500-X系列可适应安全工具。

在安全工具地址管理方面，您必须配置通过通道联络有一种资源的一个客户端在私有网络，并且让客户端作用的IP地址，好象直接地连接对私有网络。

此外，您仅交易与分配到客户端的专用IP地址。分配给您的专用网络上其他资源的 IP 地址属于您的网络管理职责的一部分，不在 VPN 管理的范围内。所以，当IP地址讨论在这儿时，思科含义那些IP地址可用在让客户端功能作为隧道终点的您的私有网络编址方案。

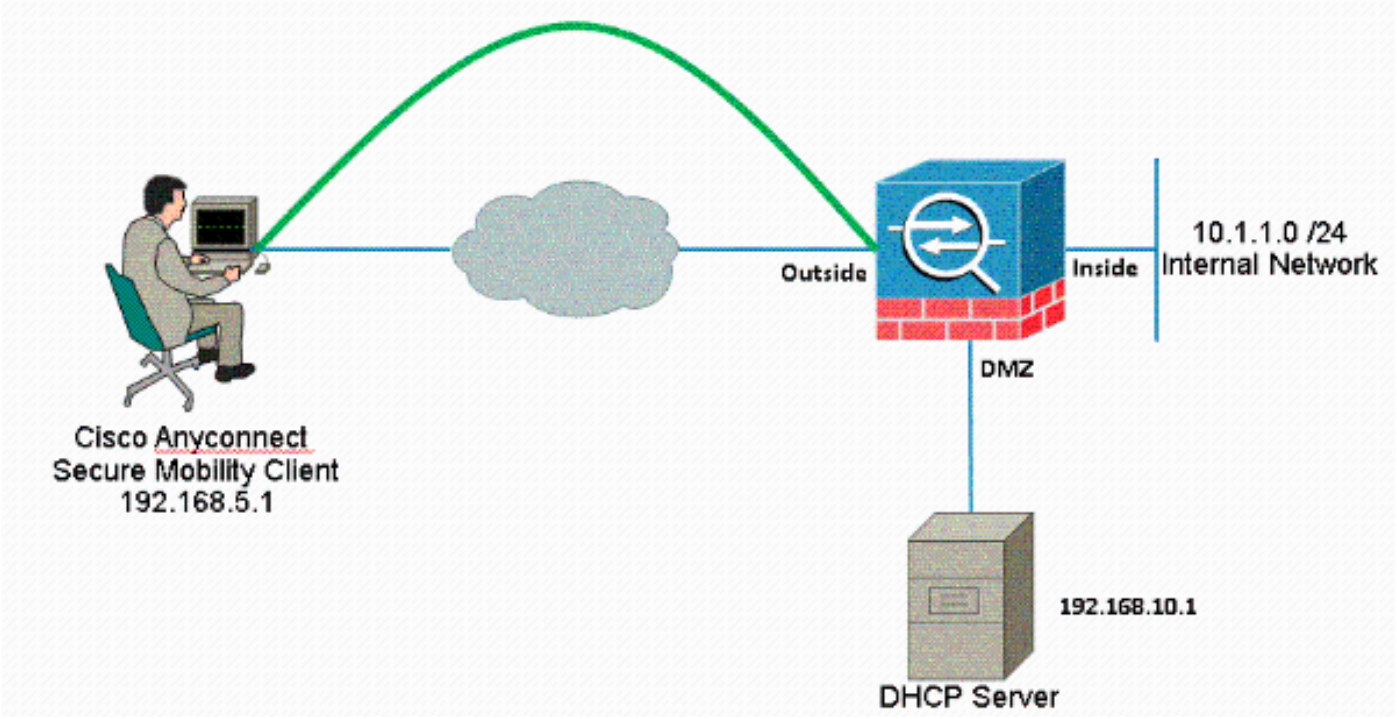
配置

本部分提供有关如何配置本文档所述功能的信息。

> **注意**： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：



注意： 此配置中使用的 IP 编址方案在 Internet 上不可合法路由。这些地址是在实验室环境中使用的 RFC 1918 地址。

配置Cisco AnyConnect安全移动客户端

ASDM 步骤

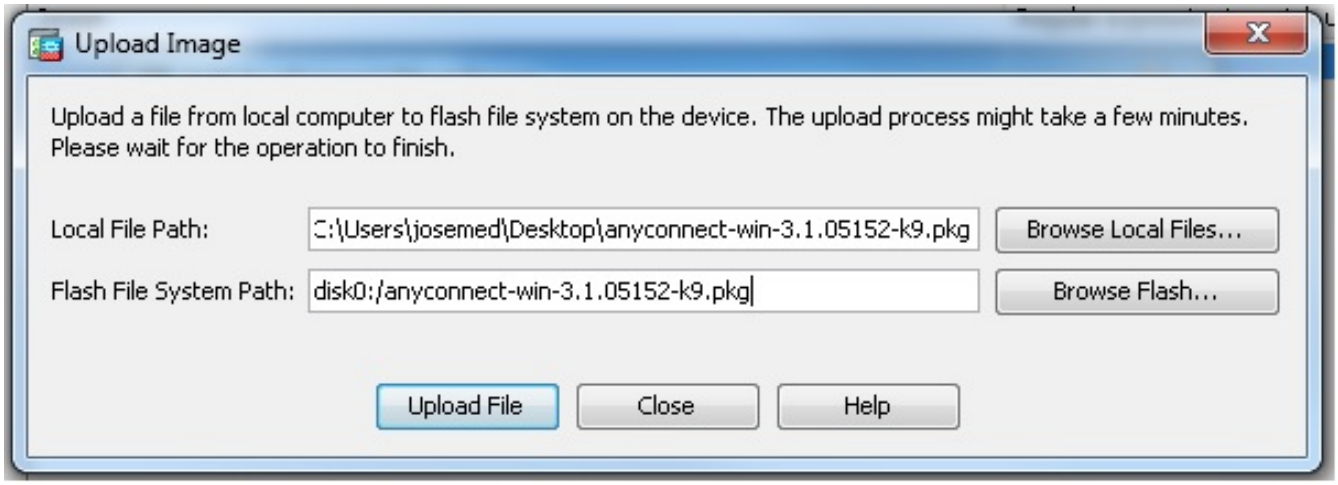
执行下列步骤以配置远程访问 VPN：

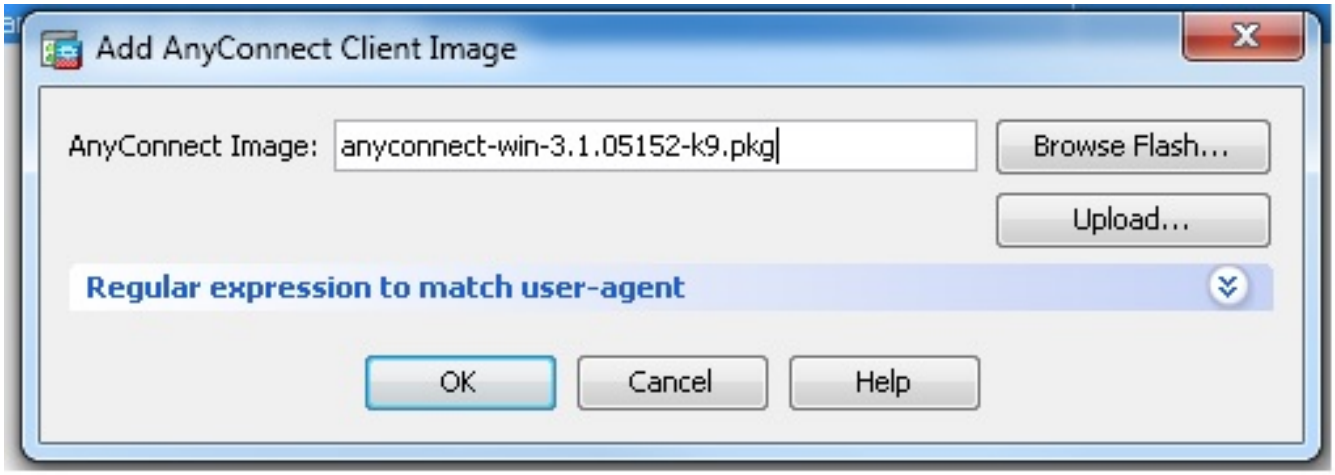
- 启用 Webvpn。

  选择 **Configuration > Remote Access VPN > Network (Client) Access > SSL VPN Connection Profiles**，然后在 Access Interfaces 下选中外部接口的 Allow Access 和 Enable DTLS 复选框。并且，请检查**在此表**复选框**选择的接口的Enable (event) Cisco AnyConnect VPN客户或传统SSL VPN客户端访问**为了启用在外部接口的SSL VPN。

单击 **Apply**。

选择**Configuration>远程访问VPN >网络(客户端)访问> Anyconnect客户端软件>Add**为了从ASA闪存添加Cisco AnyConnect VPN客户镜像如显示。



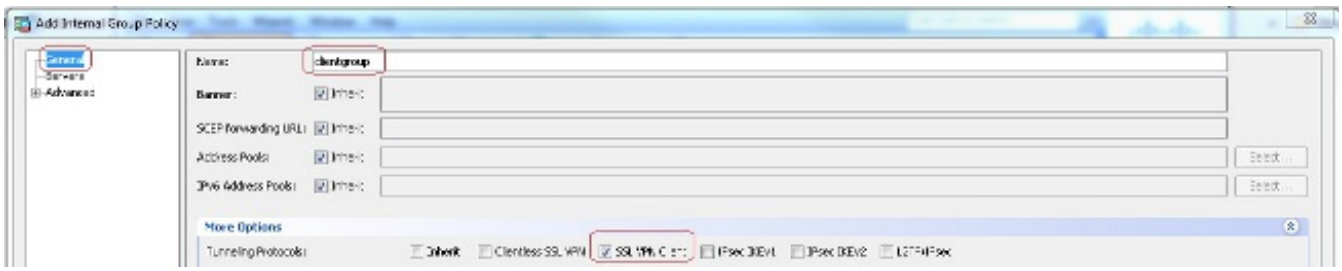


等效 CLI 配置：

```
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
```

- 配置组策略。

选择 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies** 以创建内部组策略 clientgroup。在**常规选项卡下**，请选择**SSL VPN客户端**复选框为了启用SSL作为隧道协议。



配置在**服务器**选项卡的DHCP网络范围，选择**更多选项**为了配置用户的DHCP范围能将自动地分

配。

等效 CLI 配置：

```
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)#
```

- 选择**Configuration>远程访问VPN > AAA/Local用户>本地用户>Add**为了创建新用户帐户**ssluser1**。单击 **OK**，然后单击 Apply。

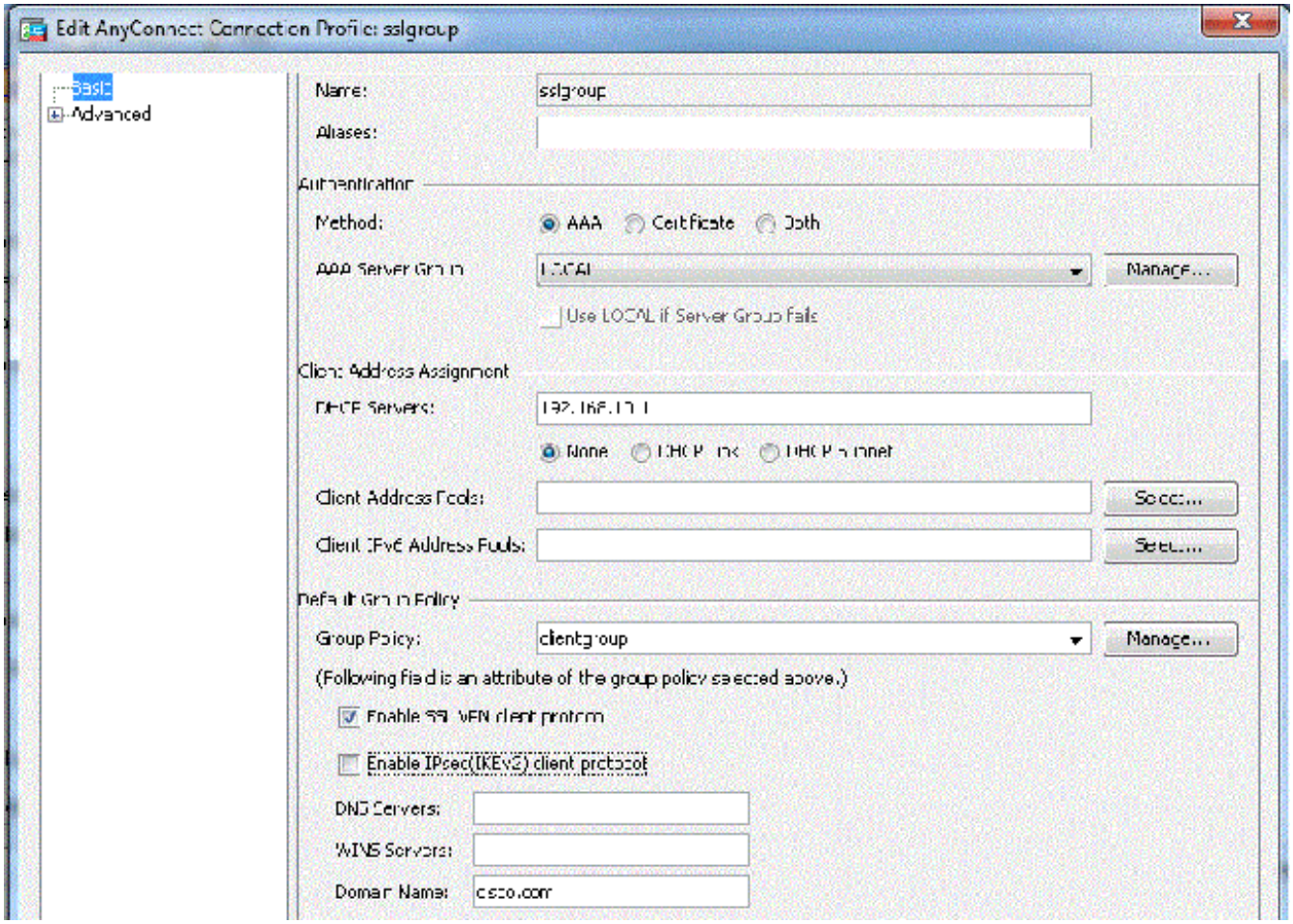
等效 CLI 配置：`ciscoasa(config)#`**`username ssluser1 password asdmASA`**

- 配置隧道组。

选择**Configuration>远程访问VPN >网络(客户端)访问> Anyconnect连接配置文件>Add**为了创建新通道组**sslgroup**。

在 **Basic** 选项卡中，您可以执行如下列出的配置：

将隧道组命名为 **sslgroup**。在为 **DHCP Servers** 提供的空白处，输入 DHCP 服务器 IP 地址。根据默认组策略，请从组策略下拉列表选择组策略**clientgroup**。配置DHCP林克或DHCP子网。



在**先进下>组别名/组URL**选项卡，指定组别名作为**sslgroup_users**并且点击OK键。

等效 CLI 配置：

```
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
```

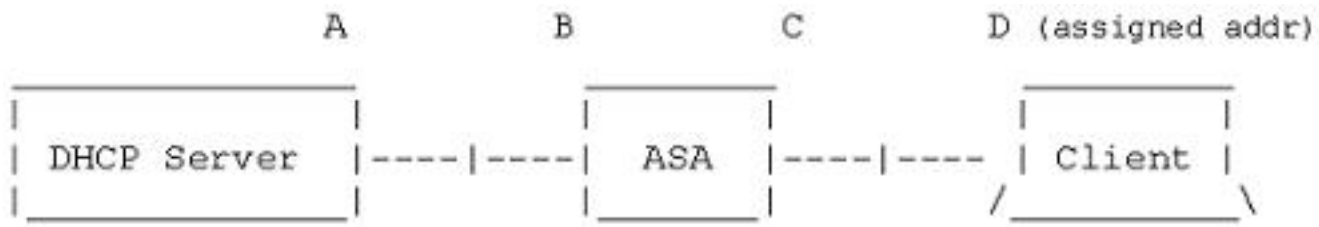
子网选择或林克选择

RFC 3011和RFC 3527的DHCP代理支持是在8.0.5和8.2.2介绍的功能，并且向前的版本支持。

- RFC 3011定义了一新的DHCP选项，子网选择选项，允许DHCP客户端指定子网分配地址。此选项优先于DHCP服务器使用确定子网选择地址的方法。
- RFC 3527定义了一个新的DHCP子选项，链路选择子选项，允许DHCP客户端指定地址DHCP服务器应该响应。

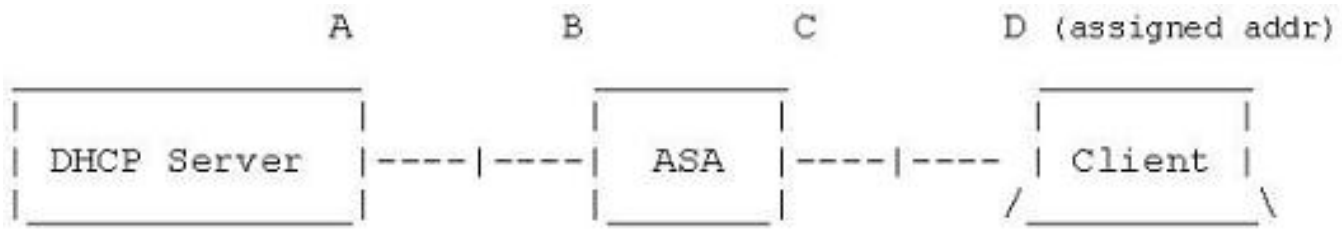
根据ASA，这些RFC将允许用户指定不是本地对ASA的DHCP地址分配的一个DHCP网络范围，并且DHCP服务器能应答直接地到ASA的接口。下图所示应该帮助说明新的行为。这将提供使用非本地的范围，而不必创建该范围的静态路由在他们的网络。

当RFC 3011或RFC 3527没有启用时， DHCP代理交换看起来类似于此：




```
Message Exchange:
     Discover: B -> A

     Offer:    A -> dhcp-network-scope

     Request:  B -> A

     Ack:      A -> dhcp-network-scope

     Release:  B -> A
```

使用启用的这些RFC之一，交换看起来类似于此，并且VPN客户端仍然分配在正确子网的一个地址：




```
Message Exchange:
     Discover: B -> A

     Offer:    A -> B

     Request:  B -> A

     Ack:      A -> B

     Release:  B -> A
```

配置与使用的ASA CLI

完成以下步骤，以便通过命令行配置 DHCP 服务器向 VPN 客户端提供 IP 地址。参考Cisco ASA 5500系列可适应安全命令参考关于使用的每命令的更多信息。

```
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#
```