使用DHCP進行地址分配的ASA的Anyconnect客戶端

目錄

簡介

本文檔介紹如何配置Cisco 5500-X系列自適應安全裝置(ASA)，以使DHCP伺服器使用自適應安全裝置管理器(ASDM)或CLI為所有Anyconnect客戶端提供客戶端IP地址。

必要條件

需求

本文檔假定ASA已完全正常運行並配置為允許Cisco ASDM或CLI進行配置更改。

> **註**:請參閱第1冊：Cisco ASA Series General Operations CLI Configuration Guide， 9.2，允許通過ASDM或Secure Shell(SSH)遠端配置裝置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Cisco ASA 5500-X新世代防火牆版本9.2(1)
- 調適型安全裝置管理器版本7.1(6)
- Cisco Anyconnect安全行動化使用者端3.1.05152

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置還可以與Cisco ASA安全裝置5500系列版本7.x及更高版本配合使用。

背景資訊

遠端訪問VPN滿足移動工作人員安全地連線到組織網路的要求。移動使用者可以使用Cisco Anyconnect安全移動客戶端軟體設定安全連線。Cisco Anyconnect安全移動客戶端啟動與配置為接受這些請求的中央站點裝置的連線。在本示例中，中心站點裝置是使用動態加密對映的ASA 5500-X系列自適應安全裝置。

在安全裝置地址管理中，您必須配置IP地址，通過隧道將客戶端與專用網路上的資源連線起來，並讓客戶端像直接連線到專用網路一樣工作。

此外，您僅處理分配給客戶端的私有IP地址。分配給專用網路上其他資源的IP地址是網路管理職責的一部分，而不是VPN管理的一部分。因此，此處討論IP地址時，Cisco是指私有網路編址方案中允許客戶端用作隧道端點的IP地址。

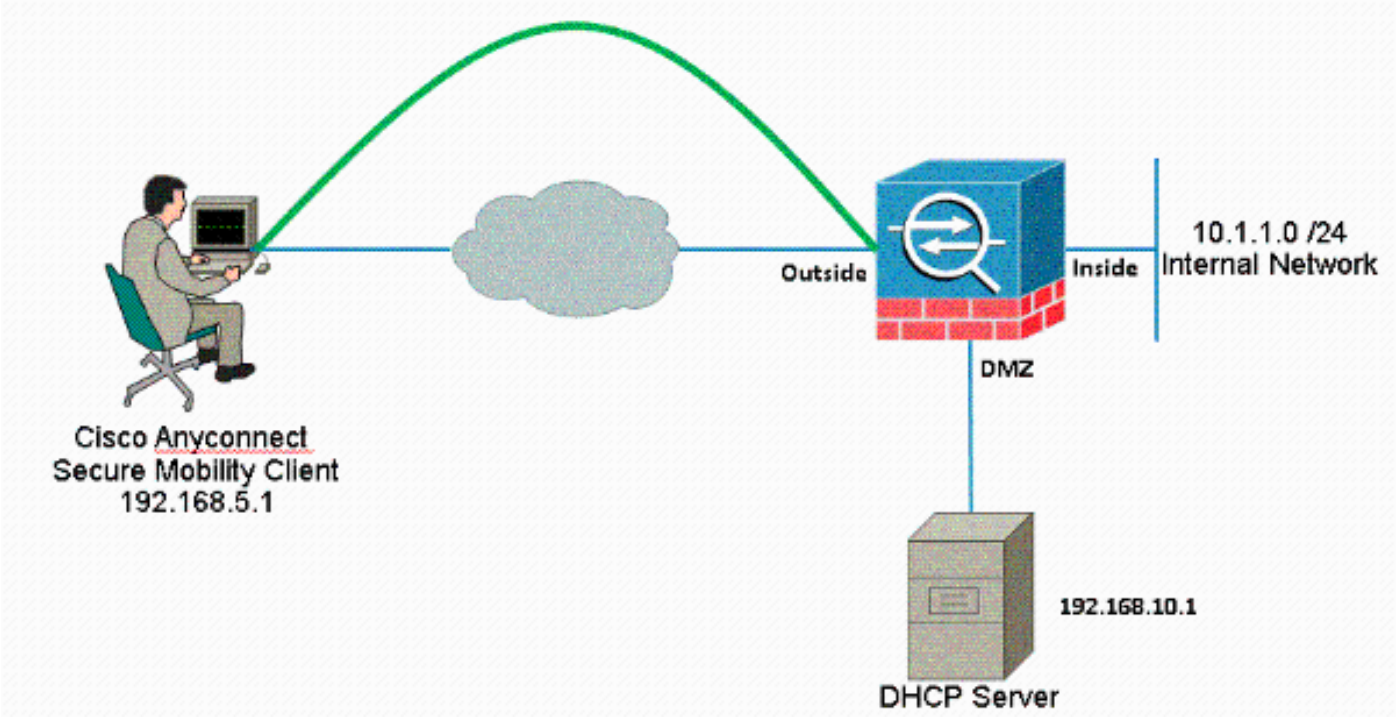
設定

本節提供用於設定本文件中所述功能的資訊。

> **註**：使用命令查詢工具(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



注意:此配置中使用的IP編址方案在Internet上不能合法路由。它們是在實驗室環境中使用的RFC 1918地址。

配置Cisco Anyconnect安全移動客戶端

ASDM過程

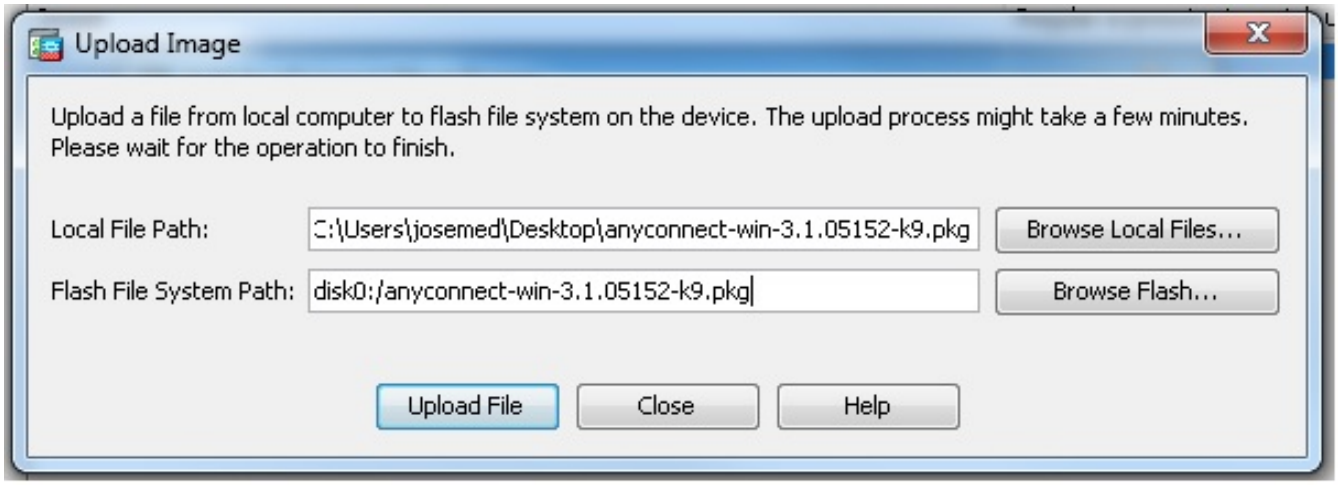
完成以下步驟以配置遠端訪問VPN:

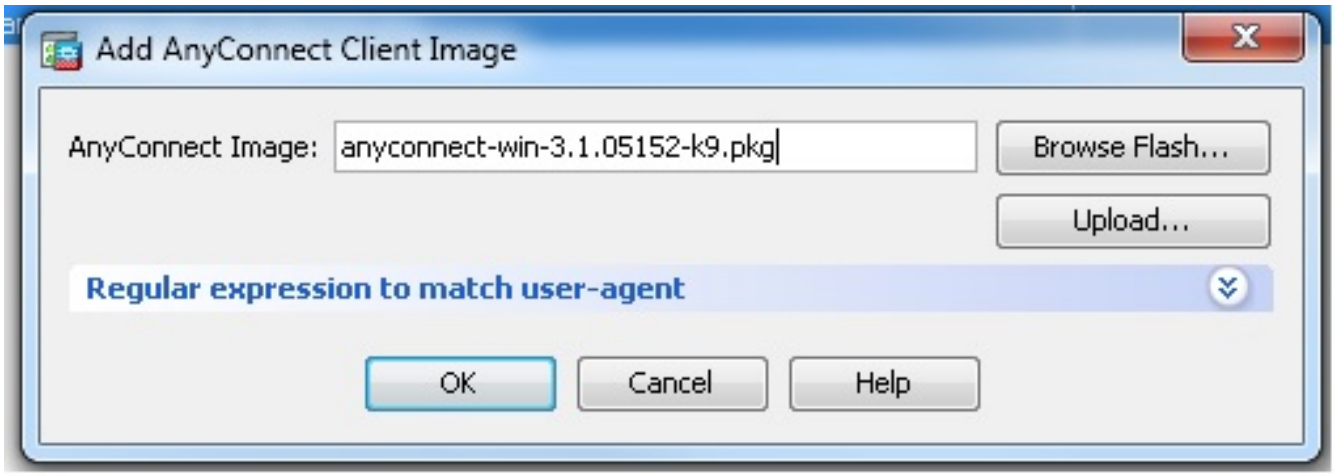
- 啟用WebVPN。

  選擇**Configuration > Remote Access VPN > Network(Client)Access > SSL VPN Connection Profiles**，並在**Access Interfaces**下按一下外部介面的**Allow Access**和**Enable DTLS**覈取方塊。此外，選中**Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interface selected in this table**覈取方塊，以在外部介面上啟用SSL VPN。

按一下「Apply」。

選擇**Configuration > Remote Access VPN > Network(Client)Access > Anyconnect Client Software > Add**，以便從ASA的快閃記憶體中新增Cisco AnyConnect VPN客戶端映像，如下所示。





等效的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
```

- 配置組策略。

選擇**Configuration > Remote Access VPN > Network(Client)Access > Group Policies**，以建立內部組策略**客戶端組**。在**General**頁籤下，選中**SSL VPN Client**覈取方塊以啟用SSL作為隧道協定。

在**Servers**頁籤中配置DHCP Network-Scope，選擇**More Options**以便為要自動分配的使用者配置DHCP範圍。

等效的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)#
```

- 選擇**Configuration > Remote Access VPN > AAA/Local Users > Local Users > Add**以建立新的使用者帳戶**ssluser1**。按一下**OK**，然後按一下**Apply**。

等效的CLI配置：

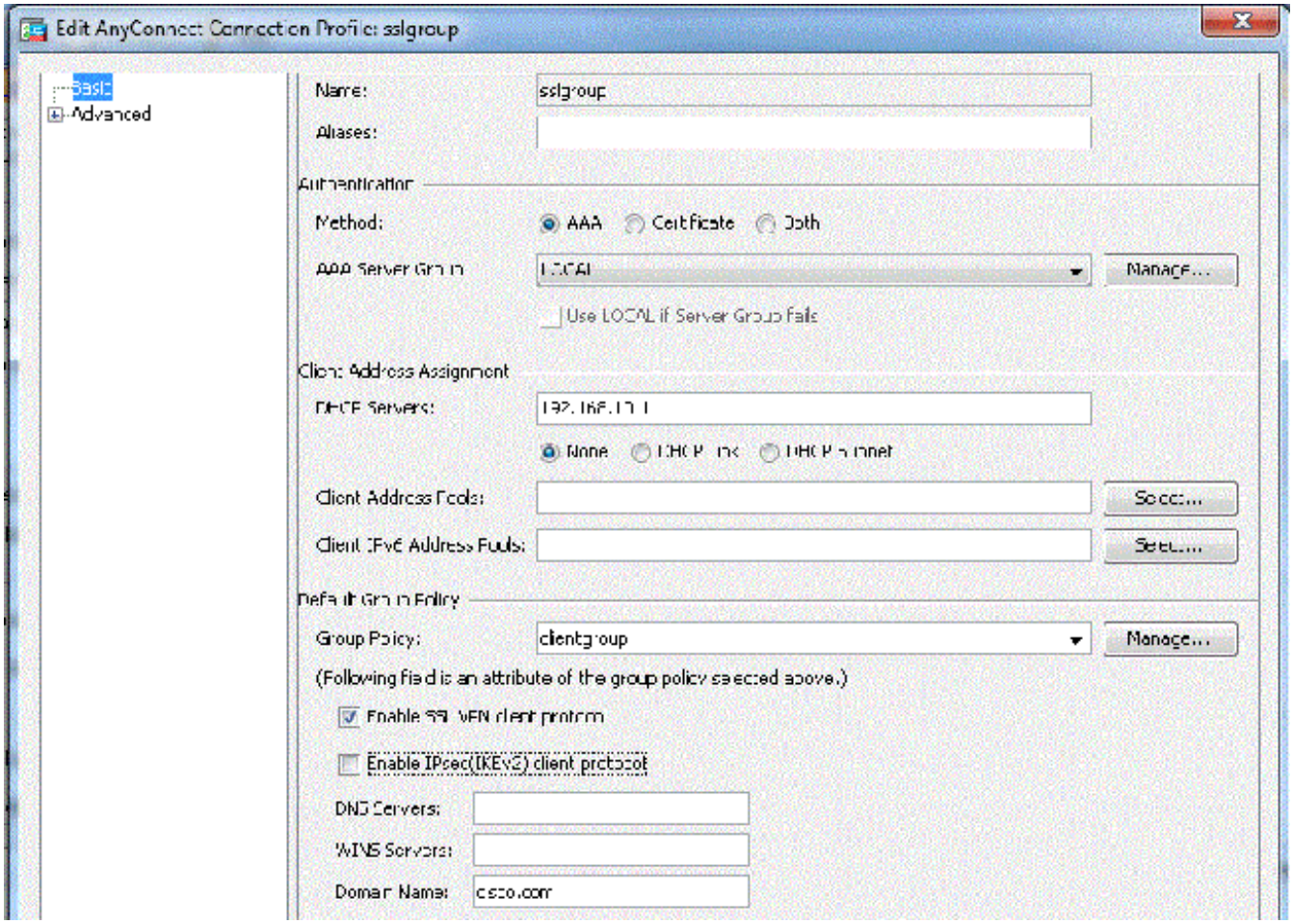
```
ciscoasa(config)#username ssluser1 password asdmASA
```

- 配置隧道組。

選擇**Configuration > Remote Access VPN > Network(Client)Access > Anyconnect Connection Profiles > Add**以建立新的隧道組**sslgroup**。

在**Basic**索引標籤中，您可以執行以下配置清單：

將隧道組命名為**sslgroup**。在為DHCP伺服器提供的空間中提供DHCP伺服器**IP地址**。在Default Group Policy下，從Group Policy下拉選單中選擇group policy **clientgroup**。配置DHCP鏈路或DHCP子網。



在**Advanced > Group Alias/Group URL**頁籤下，將組別名指定為**sslgroup_users**，然後按一下**OK**。

等效的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
```

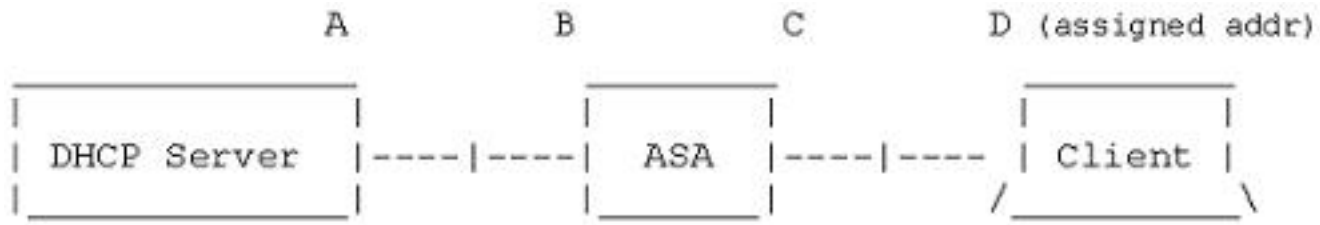
子網選擇或鏈路選擇

適用於RFC 3011和RFC 3527的DHCP代理支援是8.0.5和8.2.2中引入的一項功能，並在後續版本中支援。

- RFC 3011定義了一個新的DHCP選項，子網選擇選項，它允許DHCP客戶端指定要分配地址的子網。此選項優先於DHCP伺服器用於確定要選擇地址的子網的方法。
- RFC 3527定義了一個新的DHCP子選項，即鏈路選擇子選項，允許DHCP客戶端指定DHCP伺服器應響應的地址。

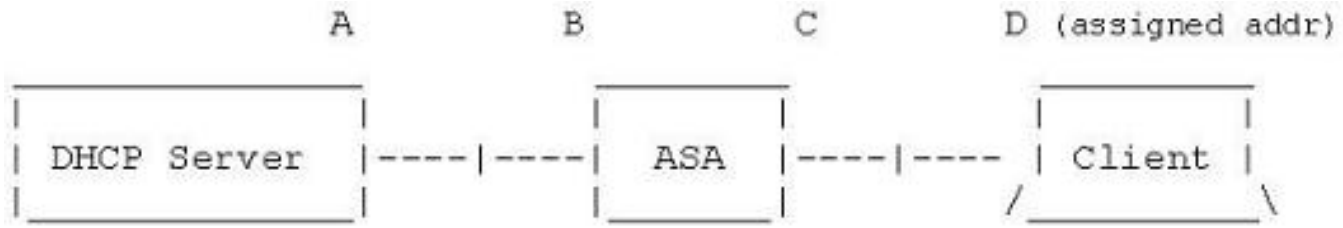
在ASA方面，這些RFC允許使用者為ASA本地的DHCP地址分配指定dhcp-network-scope，並且DHCP伺服器仍能夠直接回復到ASA的介面。下面的圖表應有助於說明新的行為。這將允許使用非本地作用域，而無需為其網路中的該作用域建立靜態路由。

未啟用RFC 3011或RFC 3527時，DHCP代理交換如下所示：




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

     Offer:    A -> dhcp-network-scope

     Request:  B -> A

     Ack:      A -> dhcp-network-scope

     Release:  B -> A
```

啟用其中一個RFC後，交換看起來與此相似，並且VPN客戶端仍然被分配了正確子網中的地址：




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

     Offer:    A -> B

     Request:  B -> A

     Ack:      A -> B

     Release:  B -> A
```

使用CLI配置ASA

完成這些步驟，以便配置DHCP伺服器從命令列向VPN客戶端提供IP地址。有關使用的每個命令的詳細資訊，請參閱Cisco ASA 5500系列自適應安全裝置 — 命令參考。

```
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#
```