ASA上具有ASDM的SSL VPN客戶端(SVC)配置示例

目錄

簡介

安全通訊端層(SSL)虛擬私人網路(VPN)技術可讓您使用以下其中一種方法，從任何位置安全地連線到公司內部網路：

- 無客戶端SSL VPN (WebVPN) -提供一個遠端客戶端，它要求透過啟用了SSL的Web瀏覽器才能訪問公司區域網(LAN)上的HTTP或HTTPS Web伺服器。此外，無客戶端SSL VPN透過通用

網際網路檔案系統(CIFS)協定為Windows檔案瀏覽提供訪問許可權。Outlook Web Access (OWA)是HTTP訪問的示例。

請參閱ASA上的無客戶端SSL VPN (WebVPN)配置示例詳細瞭解無客戶端SSL VPN。

- 瘦客戶端SSL VPN（埠轉發）— 提供一個遠端客戶端，它下載基於Java的小程式，並允許以安全方式訪問使用靜態埠號的傳輸控制協定(TCP)應用程式。郵局協定(POP3)、簡單郵件傳輸協定(SMTP)、Internet郵件訪問協定(IMAP)、安全外殼(ssh)和Telnet都是安全訪問的示例。由於本地電腦上的檔案發生更改，因此使用者必須具有本地管理許可權才能使用此方法。此SSL VPN方法不適用於使用動態埠分配的應用程式，例如某些檔案傳輸協定(FTP)應用程式。

  請參閱在ASA上用ASDM配置瘦客戶端SSL VPN (WebVPN)的示例以詳細瞭解瘦客戶端SSL VPN。

  注意：不支援使用者資料包協定(UDP)。

- SSL VPN客戶端（隧道模式）-下載一個小型客戶端到遠端工作站，並允許以完全安全方式訪問公司內部網路中的資源。您可以將SSL VPN客戶端(SVC)永久下載到遠端工作站，也可以在安全會話關閉後刪除該客戶端。

本文檔介紹如何使用自適應安全裝置管理器(ASDM)在自適應安全裝置(ASA)上配置SVC。結果部分中列出了此配置所產生的命令列。

必要條件

需求

在嘗試此配置之前，請確保滿足以下要求：

- SVC從思科自適應安全裝置軟體版本7.1及更高版本開始支援
- 所有遠端工作站的本地管理許可權
- 遠端工作站上的Java和ActiveX控制元件
- 埠443在連線路徑上的任何位置都不會被阻塞

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科調適型安全裝置軟體版本7.2(1)
- 思科調適型安全裝置管理員5.2(1)
- 思科調適型安全裝置5510系列
- Microsoft Windows XP Professional SP 2

本文檔中的資訊是在實驗室環境中開發的。本文檔中使用的所有裝置都已重置為其預設配置。如果您的網路運作中，請確保您已瞭解任何指令可能造成的影響。此配置中使用的所有IP地址都是從實驗環境中的RFC 1918地址中選擇的；這些IP地址在Internet上不可路由，僅供測試使用。

網路圖表

本檔案使用本節所述的網路組態。

遠端使用者使用啟用了SSL的Web瀏覽器連線到ASA的IP地址。身份驗證成功後，SVC將下載到客戶端電腦，使用者可以使用加密的安全會話來完全訪問公司網路上所有允許的資源。

預配置任務

開始之前，請完成以下任務：

- 要使ASDM可配置ASA，請參閱允許ASDM進行HTTPS訪問。

  要訪問ASDM應用程式，請從管理站使用啟用了SSL的Web瀏覽器並輸入ASA裝置的IP地址。例如：https://inside_ip_address，其中inside_ip_address是ASA的地址。載入ASDM後，可以開始配置SVC。

- 從Cisco軟體下載(僅供註冊客戶使用)網站將SSL VPN客戶端軟體套件(sslclient-win*.pkg)下載到您從中訪問ASDM應用程式的管理工作站的本地硬碟上。

除非更改埠號，否則WebVPN和ASDM無法在同一ASA介面上啟用。如果您希望這兩種技術使用同一裝置上的同一埠（埠443），則可以在內部介面上啟用ASDM，並在外部介面上啟用WebVPN。

慣例

如需檔案慣例的詳細資訊，請參閱思科技術提示慣例。

在ASA上配置SSL VPN客戶端

要在ASA上配置SSL VPN客戶端，請完成以下步驟：

1. 在ASA上啟用WebVPN訪問
2. 在ASA上安裝並啟用SSL VPN客戶端
3. 在客戶端上啟用SVC安裝
4. 啟用重新生成金鑰引數

步驟 1.在ASA上啟用WebVPN訪問

要在ASA上啟用WebVPN訪問，請完成以下步驟：

1. 在ASDM應用程式中，按一下Configuration，然後按一下VPN。

2. 展開WebVPN，然後選擇WebVPN Access。

3. 選擇要為其啟用WebVPN的介面，然後按一下Enable。

步驟 2.在ASA上安裝並啟用SSL VPN客戶端

要在ASA上安裝並啟用SSL VPN客戶端，請完成以下步驟：

1. 按一下Configuration，然後按一下VPN。

2. 在導航窗格中，展開WebVPN，然後選擇SSL VPN Client。

3. 按一下Add。

   系統將顯示Add SSL VPN Client Image對話方塊。

4. 按一下Upload按鈕。

   系統將顯示Upload Image對話方塊。

5. 按一下Browse Local Files按鈕在本地電腦上查詢檔案，或按一下Browse Flash按鈕在快閃記憶體檔案系統上查詢檔案。

6. 找到要上傳的客戶端映像檔案，然後按一下OK。

7. 按一下Upload File，然後按一下Close。

8. 客戶端映像載入到快閃記憶體後，選中Enable SSL VPN Client覈取方塊，然後按一下Apply。

   注意：如果收到錯誤消息，請驗證是否已啟用WebVPN訪問。在導航窗格中，展開WebVPN，然後選擇WebVPN Access。選擇要為其配置訪問的介面，然後按一下Enable。

9. 按一下Save，然後按一下Yes接受更改。

步驟 3.在客戶端上啟用SVC安裝

要在客戶端上啟用SVC安裝，請完成以下步驟：

1. 在導航窗格中，展開IP Address Management，然後選擇IP Pools。

2. 按一下Add，在Name、Starting IP Address、Ending IP Address和Subnet Mask欄位中輸入值。您在「起始IP地址」和「終止IP地址」欄位輸入的IP地址必須來自內部網路的子網。

3. 按一下OK，然後按一下Apply。

4. 按一下Save，然後按一下Yes接受更改。

5. 在導航窗格中，展開IP Address Management，然後選擇Assignment。

6. 選中Use internal address pools覈取方塊，然後取消選中Use authentication server和Use DHCP覈取方塊。

7. 按一下「Apply」。
8. 按一下Save，然後按一下Yes接受更改。
9. 在導航窗格中，展開General，然後選擇Tunnel Group。
10. 選擇要管理的隧道組，然後按一下Edit。
11. 按一下Client Address Assignment頁籤，然後從Available Pools清單中選擇新建立的IP地址池。
12. 按一下Add，然後按一下OK。
13. 在ASDM應用程式窗口中，按一下Apply。
14. 按一下Save，然後按一下Yes接受更改。

步驟 4.啟用重新生成鍵引數

若要啟用重新生成金鑰引數，請執行下列操作：

1. 在導航窗格中，展開General，然後選擇Group Policy。
2. 選擇要向此客戶端組應用的策略，然後按一下Edit。
3. 在General頁籤下，取消選中Tunneling Protocols Inherit覈取方塊，然後選中WebVPN覈取方塊。
4. 按一下WebVPN頁籤，按一下SSL VPN Client頁籤，然後選擇以下這些選項：
    a. 對於Use SSL VPN Client選項，取消選中Inherit覈取方塊，然後按一下Optional單選按鈕。

    此選項允許遠端客戶端選擇是否下載SVC。Always選擇確保在每個SSL VPN連線期間將SVC下載到遠端工作站。

    b. 對於Keep Installer on Client System選項，取消選中Inherit覈取方塊，然後按一下Yes單選按鈕。

    此操作允許SVC軟體保留在客戶端電腦上；因此，每次建立連線時，ASA都不需要將SVC軟體下載到客戶端。對於經常訪問公司網路的遠端使用者來說，此選項是一個不錯的選擇。

    c. 對於Renegotiation Interval選項，取消選中Inherit框，取消選中Unlimited覈取方塊，然後輸入重新生成金鑰之前經過的分鐘數。

    透過對金鑰的有效時間長度設定限制來增強安全性。

    d. 對於Renegotiation Method選項，取消選中Inherit覈取方塊，然後按一下SSL單選按鈕。重新交涉可以使用目前的SSL通道或專門為重新交涉建立的新通道。

您的SSL VPN客戶端屬性應配置如下圖所示：

5. 按一下OK，然後按一下Apply。

6. 按一下Save，然後按一下Yes接受更改。

結果

ASDM建立以下命令列配置：

ciscoasa

```
<#root>

ciscoasa(config)#

show run

ASA Version 7.2(1)
!
hostname ciscoasa
domain-name cisco.com
enable password 9jNfZuG3TC5tCVH0 encrypted
names
dns-guard
!
interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.22.1.160 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.1 255.255.255.0
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive
dns server-group DefaultDNS
 domain-name cisco.com
no pager
logging enable
logging asdm informational
mtu outside 1500
mtu inside 1500
mtu DMZ1 1500
mtu Mgt 1500
ip local pool CorporateNet 10.2.2.50-10.2.2.60 mask 255.255.255.0
icmp permit any outside
asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
global (outside) 1 interface
nat (inside) 1 0 0
route outside 0.0.0.0 0.0.0.0 172.22.1.1 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
!

!--- Group Policy Statements

group-policy GroupPolicy1 internal
group-policy GroupPolicy1 attributes
 vpn-tunnel-protocol IPSec l2tp-ipsec webvpn

!--- Enable the SVC for WebVPN

 webvpn
  svc enable
  svc keep-installer installed
  svc rekey time 30
  svc rekey method ssl
!
username cisco password 53QNetqK.Kqqfshe encrypted privilege 15
!
http server enable
http 10.2.2.0 255.255.255.0 inside
!
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart

!--- Tunnel Group and Group Policy using the defaults here

tunnel-group DefaultWEBVPNGroup general-attributes
 address-pool CorporateNet
 default-group-policy GroupPolicy1
!
no vpn-addr-assign aaa
no vpn-addr-assign dhcp
!
telnet timeout 5
ssh 172.22.1.0 255.255.255.0 outside
ssh timeout 5
console timeout 0
!
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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
```

```
!
service-policy global_policy global

!--- Enable webvpn and the select the SVC client

webvpn
 enable outside
 svc image disk0:/sslclient-win-1.1.1.164.pkg 1
 svc enable

!--- Provide list for access to resources

 url-list ServerList "E-Commerce Server1" http://10.2.2.2 1
 url-list ServerList "BrowseServer" cifs://10.2.2.2 2
 tunnel-group-list enable

prompt hostname context
Cryptochecksum:80a1890a95580dca11e3aee200173f5f
: end
```

自定義配置

在ASA上配置SSL VPN Client中介紹的過程對於組策略(GroupPolicy1)和隧道組(DefaultWebVPNGroup)都使用ASA預設名稱，如下圖所示：

此過程描述如何建立您自己的自定義組策略和隧道組，並根據組織的安全策略將它們連線在一起。

若要自訂組態，請完成以下步驟：

1. 建立自定義組策略
2. 建立自定義隧道組
3. 建立使用者並將該使用者增加到自定義組策略中

步驟 1.建立自定義組策略

要建立自定義組策略，請完成以下步驟：

1. 按一下Configuration，然後按一下VPN。
2. 展開General，然後選擇Group Policy。
3. 按一下Add，然後選擇Internal Group Policy。
4. 在Name欄位中，輸入組策略的名稱。

   在本示例中，組策略名稱已更改為SalesGroupPolicy。
5. 在General頁籤下，取消選中Tunneling Protocols Inherit覈取方塊，然後選中WebVPN覈取方塊。

6. 按一下WebVPN頁籤，然後按一下SSL VPN Client頁籤。

   在此對話方塊中，還可以選擇SSL VPN客戶端的行為。

7. 按一下OK，然後按一下Apply。

8. 按一下Save，然後按一下Yes接受更改。

步驟 2.建立自定義隧道組

要建立自定義隧道組，請完成以下步驟：

1. 按一下Configuration按鈕，然後按一下VPN。

2. 展開General，然後選擇Tunnel Group。

3. 按一下Add，然後選擇WebVPN Access。

4. 在Name欄位中，輸入隧道組的名稱。

   在本示例中，隧道組名稱已更改為SalesForceGroup。

5. 按一下Group Policy下拉箭頭，然後選擇新建立的組策略。

   您的群組原則與通道群組現已連結。

6. 按一下Client Address Assignment頁籤，然後輸入DHCP Server資訊，或從本地建立的IP池進行選擇。

7. 按一下OK，然後按一下Apply。

8. 按一下Save，然後按一下Yes接受更改。

步驟 3.建立使用者並將該使用者增加到自定義組策略中

要建立使用者並將該使用者增加到自定義組策略中，請完成以下步驟：

1. 按一下Configuration，然後按一下VPN。

2. 展開General，然後選擇Users。

3. 按一下Add，然後輸入使用者名稱和口令資訊。

4. 按一下VPN Policy頁籤。確保新建立的組策略顯示在Group Policy欄位中。

   此使用者繼承新組策略的所有特性。

5. 按一下OK，然後按一下Apply。

6. 按一下Save，然後按一下Yes接受更改。

驗證

使用本節內容，確認您的組態是否正常運作。

驗證

SSL VPN客戶端的身份驗證使用以下方法之一完成：

- Cisco Secure ACS伺服器(Radius)
- NT域
- Active Directory
- 一次性密碼
- 數位憑證
- 智慧卡
- 本地AAA身份驗證

本文檔使用在ASA裝置上建立的本地帳戶。

注意：如果自適應安全裝置具有多個共用同一CA的信任點，則只能使用其中一個共用CA的信任點來驗證使用者證書。

組態

要用遠端客戶端連線到ASA，請在啟用了SSL的Web瀏覽器的地址欄位中輸入https://ASA_outside_address。ASA_outside_address是ASA的外部IP地址。如果配置成功，則顯示Cisco Systems SSL VPN Client窗口。

注意：只有當您從ASA接受證書並且SSL VPN客戶端已下載到遠端工作站後，才會顯示Cisco Systems SSL VPN Client窗口。如果視窗沒有出現，請確定它並未最小化。

命令

有若干show命令與WebVPN關聯。您可以在命令列介面(CLI)執行這些命令以顯示統計資訊和其他資訊。有關show命令的詳細資訊，請參閱驗證WebVPN配置。

注意：輸出直譯器工具(僅限註冊客戶)(OIT)支援某些show命令。使用OIT檢視對show命令輸出的分析。

疑難排解

使用本節內容，對組態進行疑難排解。

SVC錯誤

問題

在身份驗證期間，您可能會收到以下錯誤消息：

```
"The SSl VPN connection to the remote peer was disrupted
and could not be automatically re-estabilished. A new connection requires
re-authentication and must be restarted manually. Close all sensitive networked
applications."
```

解決方案

如果PC上正在運行防火牆服務，可能會中斷身份驗證。停止服務並重新連線客戶端。

SVC是否與ASA建立了安全會話？

要確保SSL VPN客戶端已與ASA建立安全會話，請執行以下操作：

1. 按一下Monitoring。
2. 展開VPN Statistics，然後選擇Sessions。
3. 從Filter By下拉選單中，選擇SSL VPN Client，然後按一下Filter按鈕。

   您的配置應出現在會話清單中。

是否成功建立和終止安全會話？

您可以檢視即時記錄，以確保工作階段順利建立和終止。若要檢視階段作業記錄：

1. 點選監控，然後點選日誌記錄。
2. 選擇Real-time Log Viewer或Log Buffer，然後按一下View。

   注意：要僅顯示來自特定地址的會話，請按地址過濾。

檢查WebVPN配置檔案中的IP池

```
%ASA-3-722020: Group group User user-name IP IP_address  No address
available for SVC connection
```

沒有可用地址分配給SVC連線。因此，請在配置檔案中分配IP池地址。

如果您建立新的連線設定檔，請設定別名或group-url以存取此連線設定檔。如果沒有，所有SSL嘗

試都將命中未繫結IP池的預設WebVPN連線配置檔案。將此設定設定為使用預設連線配置檔案，並在其上放置IP池。

秘訣

- 使用分配給遠端客戶端的IP地址池確保路由正常工作。此IP地址池應來自LAN上的子網。您還可以使用DHCP伺服器或身份驗證伺服器來分配IP地址。
- ASA將建立預設隧道組(DefaultWebVPNGroup)和預設組策略(GroupPolicy1)。如果建立新的組和策略，請確保根據網路的安全策略應用值。
- 如果要允許透過CIFS瀏覽Windows檔案，請在Configuration > VPN > WebVPN > Servers and URLs下輸入WINS (NBNS)伺服器。此技術使用CIFS選項。

命令

有若干debug命令與WebVPN關聯。有關這些命令的詳細資訊，請參閱使用WebVPN Debug命令。

注意：使用debug命令可能會對Cisco裝置造成負面影響。使用 debug 命令之前，請先參閱有關偵錯命令的重要資訊。

相關資訊

- ASA上的無客戶端SSL VPN (WebVPN)配置示例
- 在ASA上使用ASDM配置瘦客戶端SSL VPN (WebVPN)的示例
- 使用ASDM和NTLMv1的WebVPN和單一登入的ASA配置示例
- Cisco ASA 5500系列調適型安全裝置
- 技術支援與文件 - Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。