ASA 8.X:允許使用者應用程式在重新建立L2L VPN隧道時運行

目錄

簡介

本文檔提供有關持續IPSec隧道流功能以及如何在VPN隧道中斷時保留TCP流的資訊。

必要條件

需求

本文檔的讀者應該對VPN的工作方式有基本的瞭解。請參閱以下文件以瞭解更多資訊：

- L2L VPN配置示例
- 含ASA的L2L VPN

採用元件

本檔案中的資訊是根據版本8.2和更新版本的思科調適型安全裝置(ASA)。

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。

慣例

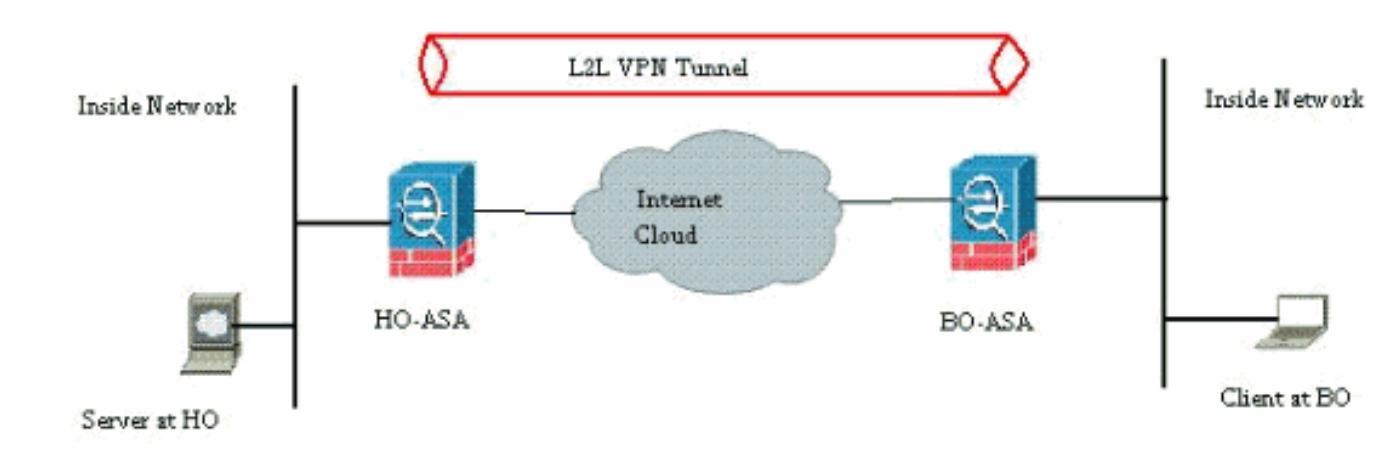
請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

如網路圖所示，分支機構(BO)通過站點到站點VPN連線到總部(HO)。假設分支機構的終端使用者嘗試從總部所在的伺服器下載大檔案。下載持續數小時。檔案傳輸工作正常，直到VPN工作正常。但是，當VPN中斷時，檔案傳輸掛起，使用者必須在建立隧道後從頭開始重新發起檔案傳輸請求。

網路圖表

本檔案會使用以下網路設定：



之所以會出現此問題，是因為ASA工作方式的內建功能。ASA監控通過它的每個連線，並根據應用檢查功能在其狀態表中維護一個條目。通過VPN的加密流量詳細資訊以安全關聯(SA)資料庫的形式維護。對於本文檔的情況，它維護兩個不同的流量。一個是VPN網關之間的加密流量，另一個是總部伺服器和分支機構終端使用者之間的流量。當VPN終止時，此特定SA的流詳細資訊將被刪除。但是，ASA為此TCP連線維護的狀態表項因沒有活動而失效，從而阻礙了下載。這意味著在使用者應用程式終止時，ASA仍會保留該特定流的TCP連線。但是，在TCP空閒計時器過期後，TCP連線將丟失，並最終超時。

通過引入名為持久IPSec隧道流的功能解決了此問題。在Cisco ASA中整合了一個新命令，用於在VPN隧道重新協商時保留狀態表資訊。命令如下所示：

```
sysopt connection preserve-vpn-flows
```

預設情況下，此命令處於禁用狀態。通過啟用此功能，Cisco ASA將在L2L VPN從中斷中恢復並重新建立隧道時維護TCP狀態表資訊。

在此案例中，此命令必須在通道的兩端啟用。如果另一端是非思科裝置，則在Cisco ASA上啟用此命令就足夠了。如果當隧道處於活動狀態時啟用該命令，則必須清除並重新建立隧道，此命令才能生效。有關清除和重新建立通道的更多詳細資訊，請參閱清除安全關聯。

此功能相容性詳細資訊

此功能已在Cisco ASA軟體8.0.4版及更高版本中引入。只有以下型別的VPN才支援此操作：

- LAN到LAN通道
- 網路擴充模式(NEM)下的遠端存取通道

以下型別的VPN不支援此功能：

- 客戶端模式下的IPSec遠端訪問隧道
- AnyConnect或SSL VPN隧道

以下平台上不存在此功能：

- Cisco PIX軟體版本6.0
- Cisco VPN集中器
- Cisco IOS®平台

啟用此功能不會對ASA的內部CPU處理造成任何額外過載，因為它將保持隧道啟動時裝置具有的TCP連線。

注意：此命令僅適用於TCP連線。它對UDP流量沒有任何影響。UDP連線將根據配置的超時時間超時。

組態

註：使用Command Lookup Tool(僅供已註冊客戶使用)可獲取本節中使用的命令的詳細資訊。

本節提供用於設定本文件中所述功能的資訊。

本檔案會使用以下設定：

- CiscoASA

以下是VPN隧道一端的Cisco ASA防火牆的運行配置輸出示例：

CiscoASA

```
ASA Version 8.2(1)
!
hostname CiscoASA
domain-name example.com
enable password <removed>
passwd <removed>
names
!
interface Ethernet0/0
 speed 100
 duplex full
 nameif outside
 security-level 0
 ip address 209.165.201.2 255.255.255.248
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.224.9.5 255.255.255.0
!
interface Ethernet0/2
 shutdown
```

```
 no nameif
 no security-level
 no ip address
!
!
interface Management0/0
 nameif management
 security-level 100
 ip address 10.224.14.10 255.255.255.0
!
boot system disk0:/asa822-k8.bin
ftp mode passive
 !---Output Suppressed ! access-list test extended
permit ip 10.224.228.0 255.255.255.128 any access-list
test extended permit ip 10.224.52.0 255.255.255.128 any
access-list 100 extended permit ip 10.224.228.0
255.255.255.128 any access-list 100 extended permit ip
10.224.52.0 255.255.255.128 any access-list
inside_access_out extended permit ip any 10.224.228.0
255.255.255.1 ! !---Output Suppressed global (outside) 1
interface nat (inside) 0 access-list test nat (inside) 1
10.224.10.0 255.255.255.0 ! !---Output Suppressed route
inside 10.0.0.0 255.0.0.0 10.224.9.1 1 route outside
0.0.0.0 255.255.255.255 209.165.201.1 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 sip-provisional-media 0:02:00
uauth 0:05:00 absolute timeout tcp-proxy-reassembly
0:01:00 dynamic-access-policy-record DfltAccessPolicy !
!---Output Suppressed http server idle-timeout 40 http
10.224.3.0 255.255.255.0 management http 0.0.0.0 0.0.0.0
inside ! snmp-server enable traps snmp authentication
linkup linkdown coldstart ! !--- To preserve and resume
stateful (TCP) tunneled IPsec LAN-to-LAN traffic within
the timeout period after the tunnel drops and recovers.
sysopt connection preserve-vpn-flows
service resetoutside
!
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256
esp-md5-hmac
crypto ipsec transform-set testSET esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 209.165.200.10
crypto map map1 5 set transform-set testSET
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 5
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto isakmp policy 10
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
!---Output Suppressed ! telnet timeout 5 ssh timeout 5
console timeout 0 threat-detection basic-threat threat-
detection statistics access-list ! !---Output Suppressed
! tunnel-group 209.165.200.10 type ipsec-l2l tunnel-
```

```
group 209.165.200.10 ipsec-attributes pre-shared-key *
!---Output Suppressed 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 prompt hostname
state Cryptochecksum:5c228e7131c169f913ac8198ecf8427e :
end
```

啟用此功能

預設情況下，此功能被禁用。可通過在ASA的CLI上使用以下命令啟用此功能：

```
CiscoASA(config)#sysopt connection preserve-vpn-flows
```

可以使用以下命令檢視此問題：

```
CiscoASA(config)#show run all sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
sysopt connection permit-vpn
sysopt connection reclassify-vpn
sysopt connection preserve-vpn-flows
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
no sysopt noproxyarp outside
```

使用ASDM時，可通過以下路徑啟用此功能：

Configuration > Remote Access VPN > Network(Client)Access > Advanced > IPsec > System Options。

然後，選中*Preserve stateful VPN flows when the tunnel drops for Network Extension Mode(NEM)*選項。

驗證

使用本節內容，確認您的組態是否正常運作。

輸出直譯器工具(僅供已註冊客戶使用)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

- **show asp table vpn-context detail** — 顯示加速安全路徑的VPN上下文內容，可幫助您對問題進行故障排除。以下是啟用持續IPSec隧道流功能時**show asp table vpn-context**命令的輸出示例。請注意，它包含特定**的PRESERVE**標誌。

```
CiscoASA(config)#show asp table vpn-context
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

```
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000,
gc=0
```

疑難排解

在本節中，提供了一些避免隧道擺動的解決方法。還詳細說明了解決方案的優缺點。

將IKE生存期值設定為零

您可以通過將IKE生存期值保持為零來使VPN隧道保持無止境的存活時間，但不能重新協商。有關SA的資訊由VPN對等體保留，直到生存期到期。通過將值指定為零，您可以使此IKE會話永久持續下去。通過此步驟，可以避免重新鍵入隧道期間出現間歇性流量斷開問題。可以使用以下命令來完成此操作：

```
CiscoASA(config)#crypto isakmp policy 50 lifetime 0
```

但是，這在損害VPN隧道的安全級別方面有一個特定的缺點。在指定的時間間隔內重新鍵入IKE會話可以為VPN隧道提供更高的安全性，因為每次都修改了加密金鑰，並且任何入侵者都難以解碼資訊。

注意：禁用IKE生存期並不意味著隧道完全不重新生成金鑰。但是，IPSec SA仍將在指定的時間間隔重新生成金鑰，因為不能將該時間間隔設定為零。IPSec SA允許的最小生存時間值為120秒，最大生存時間值為214783647秒。有關此問題的詳細資訊，請參閱IPSec SA生存期。

通道捨棄時的錯誤訊息

當配置中未使用此功能時，當VPN隧道中斷時，Cisco ASA會返回此日誌消息：

```
%ASA-6-302014:outside:XX.XX.XX.XX/80inside:10.0.0.100/1135 duration 0:00:36 bytesTCP57983,53947
```

您可以看到，原因是通**道已被拆除**。

注意：必須啟用6級日誌記錄才能看到此消息。

此功能與reclassify-vpn選項的不同之處

隧道退回時使用preserve-vpn-flow選項。這允許先前的TCP流量保持開啟狀態，因此當通道恢復時，可以使用相同的流量。

使用**sysopt connection reclassify-vpn**命令時，它會清除與隧道流量相關的任何先前流量，並對通過隧道的流量進行分類。如果已建立與VPN無關的TCP流，則會使用reclassify-vpn選項。這會造成建立VPN後流量不通過通道的情況。有關此問題的詳細資訊，請參閱sysopt reclassify-vpn。

相關資訊

- 使用ASA的站點到站點VPN(L2L)
- Cisco ASA文檔頁面
- 技術支援與文件 - Cisco Systems