ASA 8.X:允许用户应用在重新建立L2L VPN隧道时运行

目录

简介

本文档提供有关持续IPSec隧道流功能以及如何在VPN隧道中断时保留TCP流的信息。

先决条件

要求

本文档的读者应该对VPN的工作原理有基本的了解。有关详细信息，请参阅以下文档：

- L2L VPN配置示例
- 带ASA的L2L VPN

使用的组件

本文档中的信息基于8.2版及更高版本的思科自适应安全设备(ASA)。

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。

规则

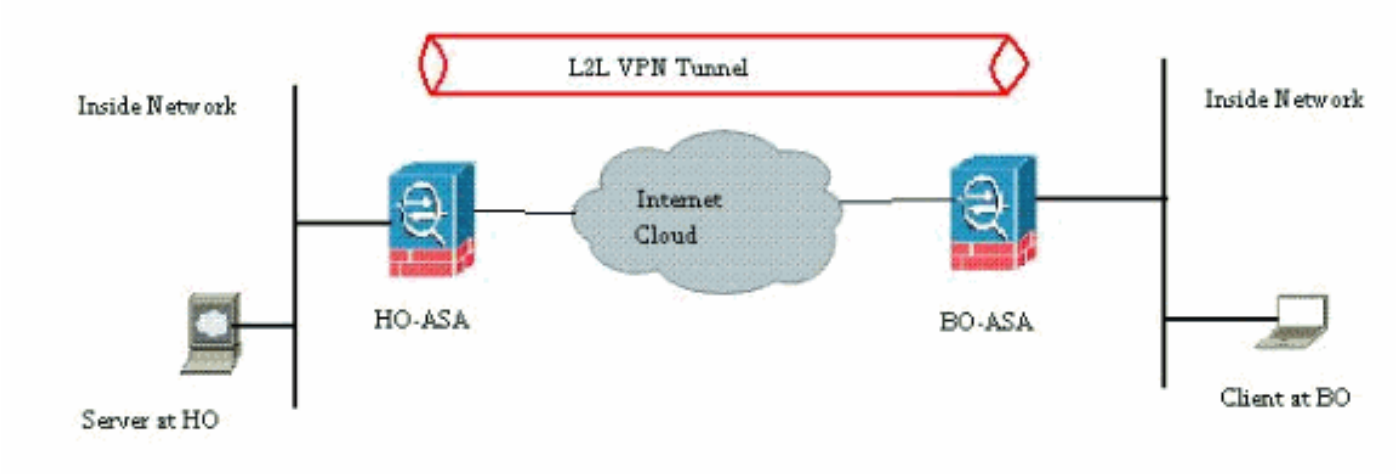
有关文档约定的更多信息，请参考 Cisco 技术提示约定。

配置

如网络图所示，分支机构(BO)通过站点到站点VPN连接到总部(HO)。假设分支机构的最终用户尝试从总部的服务器下载大文件。下载持续数小时。文件传输正常，直到VPN正常运行。但是，当VPN中断时，文件传输将挂起，用户必须在隧道建立后从头重新启动文件传输请求。

网络图

本文档使用以下网络设置：



此问题是由于ASA工作方式的内置功能。ASA 监控通过其中的每个连接，并依照应用检查功能在其状态表中维护一个条目。通过 VPN 的加密流量细节以安全关联 (SA) 数据库的形式进行维护。对于本文档的场景，它维护两个不同的流量。一个是VPN网关之间的加密流量，另一个是总部的服务器与分支机构最终用户之间的流量。当 VPN 终止时，删除此特殊 SA 的流量详细信息。但是，此 TCP 连接的 ASA 维护的状态表条目由于无活动而变得过时，进而妨碍下载。这意味着在用户应用终止时，ASA 将仍保留该特殊流量的 TCP 连接。但是，TCP 连接将丢失，并最终在 TCP 空闲计时器到期后超时。

通过引入被称为 Persistent IPSec Tunneled Flows 的功能解决了此问题。Cisco ASA中集成了新命令，以在VPN隧道重新协商时保留状态表信息。命令如下所示：

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

默认情况下禁用该命令。通过启用此功能，当L2L VPN从中断中恢复并重新建立隧道时，Cisco ASA将维护TCP状态表信息。

在此场景中，必须在隧道两端启用此命令。如果它是另一端的非思科设备，则在Cisco ASA上启用此命令应足够。如果在隧道已处于活动状态时启用该命令，则必须清除并重新建立隧道，此命令才能生效。有关清除和重新建立隧道的详细信息，请参阅清除安全关联。

此功能的兼容性详细信息

Cisco ASA软件版本8.0.4及更高版本中已引入此功能。仅以下类型的VPN支持此功能：

- LAN到LAN隧道
- 网络扩展模式(NEM)中的远程访问隧道

以下类型的VPN不支持此功能：

- 客户端模式下的IPSec远程访问隧道
- AnyConnect或SSL VPN隧道

以下平台上不存在此功能：

- 软件版本为6.0的Cisco PIX
- 思科VPN集中器
- Cisco IOS®平台

启用此功能不会在ASA的内部CPU处理上造成任何额外过载，因为它将保持设备在隧道开启时具有的相同TCP连接。

注意：此命令仅适用于TCP连接。它对UDP流量没有任何影响。UDP连接将根据配置的超时时间超时。

配置

注意：使用命令查找工具(仅限注册客户)可获取有关本节中使用的命令的详细信息。

本部分提供有关如何配置本文档所述功能的信息。

本文档使用以下配置：

- CiscoASA

以下是VPN隧道一端的Cisco ASA防火墙运行配置输出示例：

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
```

启用此功能

默认情况下，此功能被禁用。在ASA的CLI中使用以下命令可启用此功能：

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

可使用以下命令查看此信息：

```
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时，可通过以下路径启用此功能：

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

然后，选中当隧道丢弃网络扩展模式(NEM)时保留状态VPN流量。

验证

使用本部分可确认配置能否正常运行。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 show 命令。使用 OIT 可查看对 show 命令输出的分析。

- **show asp table vpn-context detail** — 显示加速安全路径的VPN上下文内容，这可能有助于您排除故障。以下是启用永久IPSec隧道流功能**时，show asp table vpn-context**命令的输出示例。请注意，它包含特定**的PRESERVE**标志。

```
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
```

故障排除

在本节中，为避免隧道摆动提供了一些解决方法。此外，还详细介绍了解决方法的优缺点。

将IKE生存期值设置为零

通过将IKE生存期值保持为零，可以使VPN隧道保持活动状态无限时间，但不能重新协商。有关SA的信息由VPN对等体保留，直到生命期到期。通过将值赋为零，可以使此IKE会话永久持续。通过这种方式，您可以避免在隧道重新加密期间出现间歇性流断开问题。这可以通过以下命令完成：

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

但是，这在降低VPN隧道的安全级别方面有一个特定缺点。在指定的时间间隔内重新输入IKE会话，每次都会根据修改的加密密钥为VPN隧道提供更高的安全性，并且任何入侵者都难以解码信息。

注意：禁用IKE生存期并不意味着隧道根本不重新生成密钥。但是，IPSec SA将在指定的时间间隔内重新生成密钥，因为该时间间隔不能设置为零。IPSec SA允许的最小生存期值为120秒，最大为214783647秒。有关此的详细信息，请参阅IPSec SA生存期。

隧道丢弃时的错误消息

当配置中未使用此功能时，当VPN隧道中断时，Cisco ASA返回此日志消息：

```
%ASA-6-302014TCP57983:XX.XX.XX.XX/80TCP10.0.0.100/11350:00:3653947
```

您可以看到，原因是隧**道已被拆除**。

注意：**必**须启用第6级日志记录才能查看此消息。

此功能与reclassify-vpn选项有何不同

当隧道退回时，将使用preserve-vpn-flow选项。这允许先前的TCP流保持打开状态，因此当隧道恢复时，可以使用相同的流。

当使用**sysopt connection reclassify-vpn**命令时，它会清除任何与隧道流量相关的先前流，并将流分类以通过隧道。当已创建与VPN无关的TCP流时，会使用reclassify-vpn选项。这会造成流量在VPN建立后不流经隧道的情况。有关此项的详细信息，请参阅sysopt reclassify-vpn。

相关信息

- 使用ASA的站点到站点VPN(L2L)
- Cisco ASA文档页面
- 技术支持和文档 - Cisco Systems