ASA 8.X：允许用户应用以L2L VPN通道的重建运行

目录

简介

本文提供关于不变IPSec隧道流功能的信息和如何保留在VPN通道的中断的TCP流。

先决条件

要求

本文读者应该有关于怎样的基本的了解VPN工作。有关详细信息，请参阅以下文档：

- 示例L2L VPN配置
- 与ASA的L2L VPN

使用的组件

本文档中的信息根据Cisco可适应安全工具(ASA)有版本8.2和以上的。

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

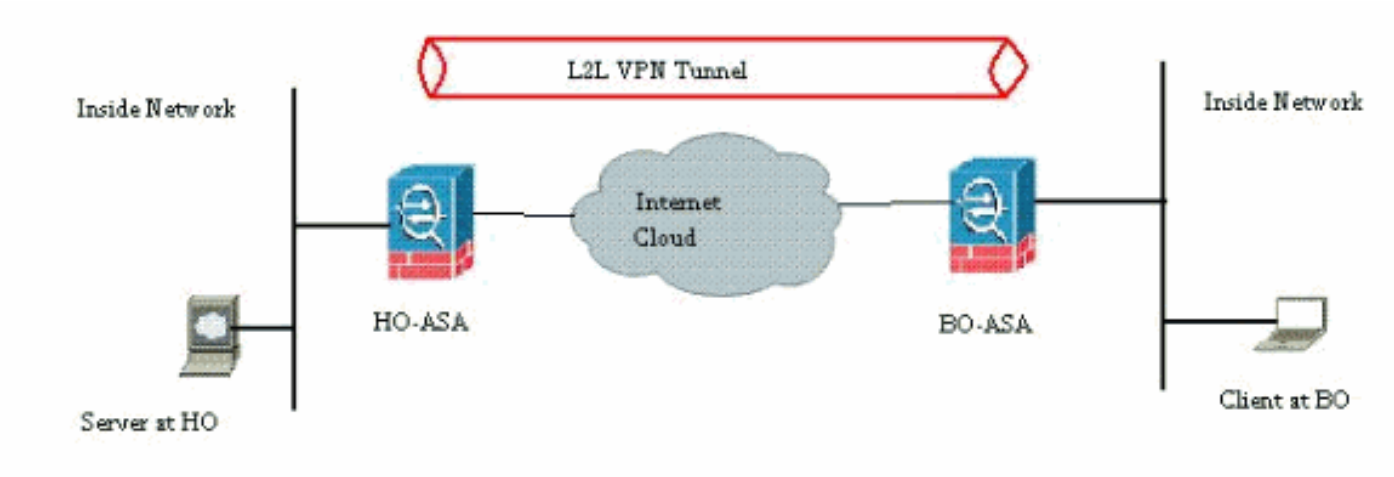
有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

如网络图所显示，分支机构(BO)连接到总部(HO)通过站点到站点VPN。在尝试的分支机构考虑一最终用户下载在总部从服务器的一个大文件位于的。下载持续几小时。文件传输良好工作，直到VPN良好工作。然而，当打乱时VPN，暂停文件传输，并且用户必须再重新发动文件传输请求从开始，在通道设立后。

网络图

本文档使用以下网络设置：



此问题出现由于关于怎样的内置的功能ASA工作。ASA监控在其状态表里穿过它并且根据应用检查功能维护一个条目的每连接。穿过VPN以安全关联(SA)数据库的形式的加密流量详细信息维护。对于本文的方案，它维护两不同的通信流。一个是VPN网关和其他之间的加密流量是在服务器在总部和最终用户之间的通信流在分支机构。当VPN终止时，此特定的SA流详细信息删除。然而，此TCP连接的ASA维护的状态条目变得过时由于没有活动，阻碍下载。这意味着ASA将保留该特定的流量的TCP连接，当用户应用终止时。然而，在TCP空闲计时器超时后， TCP连接将变为迷路者和最终超时。

介绍呼叫Persistent IPSec被建立隧道的流的功能解决了此问题。new命令集成到Cisco ASA保留状态表信息在VPN通道的重新协商。命令显示此处：

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

默认情况下禁用该命令。通过启用此，思科ASA将维护TCP状态表信息，当L2L VPN从中断恢复并且重新建立通道。

在此方案中，此命令在通道的两端必须启用。如果它是非Cisco设备在另一边，启用此on命令Cisco ASA应该足够了。如果命令启用，当通道已经是活跃的，必须清除和重新建立通道为了此命令能生效。欲了解更详细的信息在清洁和建立通道，参考结算安全关联。

此的兼容性详细信息功能

此功能在Cisco ASA软件版本8.0.4介绍及以后。这为VPN的这些类型仅支持：

- 对LAN通道的LAN
- 在网络扩展模式(NEM)的远程访问隧道

此功能不为VPN的这些类型支持：

- 在客户端模式的IPSec远程访问隧道
- AnyConnect或SSL VPN通道

此功能在这些平台不存在：

- 与软件版本6.0的Cisco PIX
- Cisco VPN集中器
- Cisco IOS平台

启用此功能不创建在ASA的内部CPU处理的任何另外的超载，因为保持设备有的同样TCP连接，当通道是UP时。

注意： 此命令为仅TCP连接是可适用的。它在UDP流量没有任何效果。UDP连接根据已配置的超时周期超时。

配置

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。

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

这是思科ASA防火墙的示例运行的配置输出在VPN通道的一端：

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，此功能禁用。这可以启用通过使用此at命令ASA的CLI ：

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

通过使用此命令，这可以查看：

```
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
```

当曾经ASDM时，此功能可以通过跟随此路径启用：

Configuration>远程访问VPN >网络(客户端)访问>Advanced > IPsec >System选项。

然后，*当通道为网络扩展模式(NEM)*选项时，*下降请检查保留有状态的VPN流*。

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。

- **显示asp表VPN上下文详细信息**—显示加速的安全路径的VPN上下文内容，也许帮助您排除故障问题。下列是从**显示asp表VPN上下文**命令的一输出示例:，当不变IPSec建立隧道功能启用的流时。注意它包含一特定**保留**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

在此部分，提交某些应急方案避免通道飘荡。应急方案的利弊也被选派。

调整IKE寿命值到零

您能做VPN通道坚持运行在无限的时间，但是不通过保持IKE寿命值重新协商，作为零。关于SA的信息由VPN对等体保留，直到寿命超时。通过赋予一个值作为零，您能做此IKE会话为时永久。在通道的密钥期间，通过此，您能避免断断续续流断开问题。这可以实行同此命令：

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

然而，这有一个特定缺点根据减弱VPN通道的安全等级。键变更在指定的时间时间间隔内的IKE会话每次提供更多安全给VPN通道根据已修改加密密钥，并且所有入侵者解码信息变得很难。

注意： 禁用IKE寿命不意味着通道根本不键变更。但是，因为那不可能调整到零， IPSec SA将键变更在指定的时间间隔。为IPSec允许的最低的寿命值SA是120秒，并且最大数量是214783647秒。关于此的更多信息，参考SA IPSec寿命。

错误消息，当通道下降

当此功能没有用于配置时，思科ASA返回此日志消息，当打乱时VPN通道：

```
%ASA-6-302014 outside:XX.XX.XX.XX/80TCP57983inside:10.0.0.100/11350:00:3653947
```

您能看到原因是**通道被切断了**。

注意： 必须启用级别6记录日志发现此消息。

此功能如何有所不同与重新列级VPN选项

保留VPN流选项，当通道重新启动时，使用。这允许一个上一个TCP流如此坚持开放，当通道恢复时，同一个流可以使用。

当使用时**sysopt连接重新列级VPN**命令，清除适合于对通道流量并且分类流通过通道的所有上一个流。重新列级VPN选项用于情况，当不是涉及的VPN的TCP流已经创建。这创建流量不在通道间流的情况，在VPN设立后。关于此的更多信息，参考sysopt重新列级VPN。

相关信息

- Site to Site VPN (L2L)与ASA
- 思科ASA文档页
- 技术支持和文档 - Cisco Systems