常规 VPN 参数

虚拟专用网络的 ASA 实施包含不能简单归类的有用功能。本章将介绍其中一些功能。

准则和限制

本节包括此功能的准则和限制。

情景模式准则

同时支持单情景和多情景模式。在相应版本的《ASA 常规操作 CLI 配置指南》中，有关在多情景模式下不支持内容的列表以及提供这些版本中新增内容细分信息的新功能，请参阅多情景模式准则。

防火墙模式准则

仅在路由防火墙模式下受支持。不支持透明模式。

网络地址转换 (NAT)

有关 NAT 配置的准则和信息，请参阅《*Cisco Secure Firewall ASA* 系列防火墙 *CLI* 配置指南》的适用于 *VPN* 的 *NAT* 部分。

配置 IPsec 以绕过 ACL

如要在不检查源和目标接口的 ACL 的情况下允许来自 IPsec 隧道的所有数据包，请在全局配置模式下输入 **sysopt connection permit-vpn** 命令。

如果使用位于 ASA 之后单独的 VPN 集中器并且想要最大限度提高 ASA 性能，则可能需要绕过用于 IPsec 流量的接口 ACL。通常，需要使用 **access-list** 命令创建允许 IPsec 数据包的 ACL，并将其应用于源接口。使用 ACL 可以指定想要允许其通过 ASA 的确切流量。

以下示例在不检查 ACL 的情况下允许 IPsec 流量通过 ASA：

```
hostname(config)# sysopt connection permit-vpn
```

注释 配置了 **no sysopt connection permit-vpn** 时，尽管在外部接口上有访问组（调用 **deny ip any any** ACL），系统仍会允许来自客户端的解密直通流量。

如果尝试使用 **no sysopt permit-vpn** 命令结合外部接口上的访问控制列表 (ACL) 来控制通过站点间或远程访问 VPN 对受保护网络进行的访问，则无法成功进行控制。

sysopt connection permit-vpn 将在为需要关注的流量启用了加密映射的接口上绕过 ACL（入口和出口），连同所有其他接口的出口 (out) ACL 一起，但不包括入口 (in) ACL。

在这种情况下，启用管理访问内部接口时，系统不应用ACL，用户仍然可以使用SSH连接到ASA。流向内部网络中主机的流量会被 ACL 正确地阻止，但流向内部接口的解密直通流量不会被阻止。

ssh 和 **http** 命令具有比 ACL 更高的优先级。如要拒绝从 VPN 会话流向设备的 SSH、Telnet 或 ICMP 流量，应使用 **ssh**、**telnet** 和 **icmp** 命令。

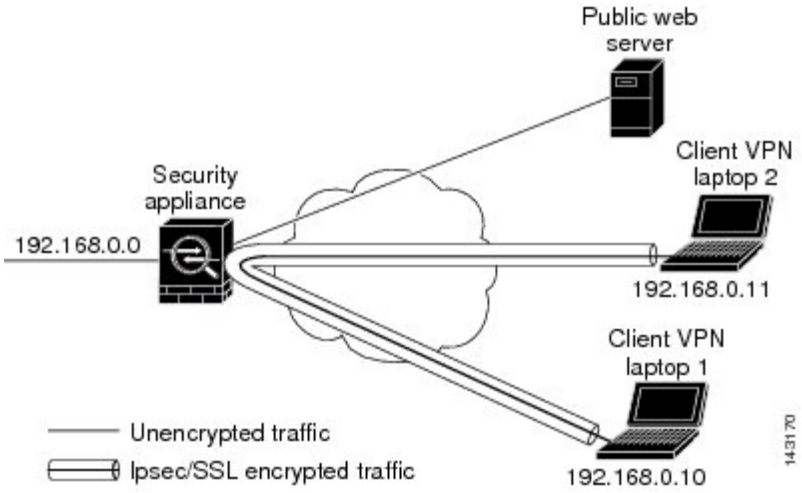
允许接口内流量 (Hairpinning)

ASA 提供一项功能，允许受 IPsec 保护的流量出入同一个接口，从而使得 VPN 客户端可以向其他 VPN 用户发送这些流量。该功能也称为“hairpinning”，可以将其视为通过 VPN 集线器 (ASA) 连接的 VPN 分支（客户端）。

Hairpinning还可以将传入VPN流量通过与未加密流量相同的接口重新向外传出去。例如，对于没有分割隧道但需要同时访问 VPN 和浏览 Web 的 VPN 客户端来说，此功能非常有用。

下图显示了 VPN 客户端 1 发送安全 IPsec 流量至 VPN 客户端 2，同时还将未加密流量发送至公共 Web 服务器。

图 *1:* 使用 ***Hairpinning*** 的接口内功能的 ***VPN*** 客户端



要配置此功能，请在全局配置模式下使用 **same-security-traffic** 命令及其 intra-interface 参数。

该命令的语法为 same-security-traffic permit {*inter-interface* | *intra-interface*}。

以下示例显示如何启用接口内流量：

```
hostname(config)# same-security-traffic permit intra-interface
hostname(config)#
```

注释 如果使用 **same-security-traffic** 命令和 **inter-interface** 参数，则可允许安全级别相同的接口之间进行通信。该功能不是特定于 IPsec 连接的功能。有关详细信息，请参阅本指南的“配置接口参数”一章。

要使用 hairpinning，必须按照接口内流量的 NAT 注意事项中所述，对 ASA 接口应用适当的 NAT 规则。

接口内流量的 NAT 注意事项

要使 ASA 能够通过该接口退送未加密的流量，必须为该接口启用 NAT，以便公用可路由地址替换专用 IP 地址（除非已在本地 IP 地址池中使用公用 IP 地址）。以下示例对来自客户端 IP 池的流量应用接口 PAT 规则：

```
hostname(config)# ip local pool clientpool 192.168.0.10-192.168.0.100
hostname(config)# object network vpn_nat
hostname(config-network-object)# subnet 192.168.0.0 255.255.255.0
hostname(config-network-object)# nat (outside,outside) interface
```

然而，当 ASA 通过同一接口退送加密的 VPN 流量时，NAT 是可选的。无论是否使用 NAT，VPN 到 VPN Hairpinning 均可正常工作。要对所有传出流量应用 NAT，请仅实施以上命令。要使 VPN 到 VPN 流量豁免 NAT，请添加为 VPN 到 VPN 流量实施 NAT 豁免的命令（添加到以上示例命令中），例如：

```
hostname(config)# nat (outside,outside) source static vpn_nat vpn_nat destination static
vpn_nat vpn_nat
```

有关 NAT 规则的详细信息，请参阅本指南的“应用 NAT”一章。

设置最大活动 IPsec 或 SSL VPN 会话数

要将 VPN 会话数限制为低于 ASA 允许的值，请在全局配置模式下输入 **vpn-sessiondb** 命令：

vpn-sessiondb {**max-anyconnect-premium-or-essentials-limit** <number> | **max-other-vpn-limit** <number>}

max-anyconnect-premium-or-essentials-limit 关键字指定 Secure Client 的最大会话数，从 1 到许可证允许的最大会话数。

注释 正确的许可期限、级别和用户计数不再使用这些命令来确定。请参阅Secure Client订购指南：http://www.cisco.com/c/dam/en/us/products/collateral/security/anyconnect-og.pdf

max-other-vpn-limit 关键字用于指定除 Secure Client会话之外的其他 VPN 的最大会话数，范围为从 1 到许可证允许的最大会话数。这包括思科 VPN 客户端 (IPsec IKEv1) 和 LAN 间 VPN 会话。

该限制会影响计算得出的 VPN 负载均衡的负载百分比。

以下示例显示如何设置值为 450 的最大 Anyconnect VPN 会话数限制：

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 450
hostname(config)#
```

使用客户端更新确保达到可接受的 IPsec 客户端修订级别

注释 本节中的信息仅适用于 IPsec 连接。

客户端更新功能使得处于中央位置的管理员能够自动通知 VPN 客户端用户更新 VPN 客户端软件。

远程用户可能正在使用已过时的 VPN 软件或硬件客户端版本。您可以随时使用**client-update** 命令来启用更新客户端修订版本的功能；指定更新适用的客户端类型和修订版本号；提供可以从中获得更新的 URL 或 IP 地址；对于 Windows 客户端，可以选择性地通知用户应更新其 VPN 客户端版本。对于 Windows 客户端，您可以为用户提供一种完成该更新的机制。该命令仅适用于 IPsec 远程访问隧道组类型。

要执行客户端更新，请在常规配置模式或 tunnel-group ipsec-attributes 配置模式下输入 **client-update** 命令。如果客户端已经在运行修订号列表中包含的软件版本，则无需更新其软件。如果客户端未运行列表中包含的软件版本，则应进行更新。以下程序说明如何执行客户端更新：

过程

步骤 1 在全局配置模式下，输入此命令以启用客户端更新：

```
hostname(config)# client-update enable
hostname(config)#
```

步骤 2 在全局配置模式下，指定要对所有特定类型客户端应用的客户端更新参数。也就是说，指定客户端类型、可从中获取更新映像的 URL 或 IP 地址，以及该客户端的可接受的修订版本号。最多可以指定四个修订版本号，以逗号分隔。

如果用户的客户端修订版本号与某个指定的修订版本号匹配，则不需要更新客户端。该命令用于为整个 ASA 中所有指定类型的客户端指定客户端更新值。

使用以下语法：

```
hostname(config)# client-update type type url url-string rev-nums rev-numbers
hostname(config)#
```

可用的客户端类型为 **win9X**（包括 Windows 95、Windows 98 和 Windows ME 平台）、**winnt**（包括 Windows NT 4.0、Windows 2000 和 Windows XP 平台）、**windows**（包括所有基于 Windows 的平台）。

如果客户端已经在运行修订号列表中包含的软件版本，则无需更新其软件。如果客户端未运行列表中包含的软件版本，则应进行更新。最多可以指定这些客户端更新条目中的三个条目。关键字**windows** 涵盖了所有允许的 Windows 平台。如果指定了 **windows**，则不要指定单个 Windows 客户端类型。

注释
对于所有的 Windows 客户端，必须使用协议 http:// 或 https:// 作为 URL 的前缀。

以下示例为远程访问隧道组配置客户端更新参数。该示例指定了修订版本号 4.6.1 以及用于检索更新的 URL https://support/updates。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.6.1
hostname(config)#
```

或者，也可以只为单个隧道组配置客户端更新，而不是为特定类型的所有客户端配置更新。（请参阅步骤 3。）

注释
在 URL 末尾包含应用的名称可以让浏览器自动启动该应用；例如：
https://support/updates/vpnclient.exe。

步骤 3 为特定的 ipsec-ra 隧道组定义一组客户端更新参数。

在 tunnel-group ipsec-attributes 模式下，指定隧道组名称及其类型、可从中获取更新映像的 URL 或 IP 地址，以及修订版本号。如果用户的客户端修订版本号与某个指定的修订版本号匹配，则不需要更新客户端。例如，对于 Windows 客户端，请输入此命令：

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

步骤 4 （可选） 向安装过时 Windows 客户端的活动用户发送通知，指出其客户端需要更新。对于这些用户，系统将显示一个弹出窗口，让他们可以启动浏览器，并从您在URL中指定的站点下载经新的软件。此消息中唯一可配置的部分是 URL。（请参阅步骤 2 或 3。）非活动用户将在下次登录时收到通知消息。您可以向所有隧道组上的所有活动客户端发送此通知，也可以将其发送到特定隧道组上的客户端。例如，要通知所有隧道组上的所有活动客户端，则在特权 EXEC 模式下输入以下命令：

```
hostname# client-update all
hostname#
```

如果用户的客户端修订版本号与某个指定的修订版本号匹配，则不需要更新客户端，并且不会向该用户发送通知消息。

下一步做什么

注释 如果指定客户端更新类型为 **windows**（指定所有基于 Windows 的平台），然后要对同一实体输入 **win9x** 或 **winnt** 的客户端更新类型，必须先使用此命令的 **no** 形式删除 windows 客户端类型，然后使用新的客户端更新命令指定新客户端类型。

对公共 IP 连接实施 NAT 分配的 IP

在极少数情况下，您可能要在内部网络上使用 VPN 对等体的实际 IP 地址，而非已分配的本地 IP 地址。通常在使用 VPN 的情况下，对等体会获得分配的本地 IP 地址以访问内部网络。但是，在有些情况下，例如当内部服务器和网络安全基于对等体的真实 IP 地址时，可能就需要将本地 IP 地址重新转换为对等体的真实公共地址。

ASA 引入了一种方法，可以将 VPN 客户端在内部/受保护网络中分配的 IP 地址转换为其公共（源）IP 地址。该功能支持以下场景：内部网络中的目标服务器/服务和网络安全策略要求使用 VPN 客户端的公共/源 IP 而非其在内部企业网络中分配的 IP 进行通信。

可以在每个隧道组一个接口的基础上启用此功能。当VPN会话已建立或断开连接时，动态添加或删除对象 NAT 规则。

因为路由问题，除非您知道您需要此功能，否则我们不建议使用此功能。

- 仅支持旧版 (IKEv1) 和 Secure Client。
- 流向公共 IP 地址的返回流量必须路由回 ASA，以便应用 NAT 策略和 VPN 策略。
- 仅支持 IPv4 的已分配地址和公共地址。
- 不支持 NAT/PAT 设备之后的多个对等体。
- 不支持负载均衡（因为路由问题）。
- 不支持漫游。

过程

步骤 1 在全局配置模式下，输入 **tunnel general**。

步骤 2 使用此语法来启用地址转换：

```
hostname(config-tunnel-general)# nat-assigned-to-public-ip interface
```

此命令动态安装将已分配 IP 地址转换为源的公共 IP 地址的 NAT 策略。*interface* 用于确定要应用 NAT 的接口。

步骤 3 使用此语法来禁用地址转换：

```
hostname(config-tunnel-general)# no nat-assigned-to-public-ip
```

显示 VPN NAT 策略

地址转换使用基础对象 NAT 机制；因此，VPN NAT 策略会如同手动配置的对象 NAT 策略一样显示。此示例将 95.1.226.4 用作分配的 IP，将 75.1.224.21 用作对等体的公共 IP：

```
hostname# show nat
Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
    translate_hits = 315, untranslate_hits = 315

prompt# show nat detail

Auto NAT Policies (Section 2)
1 (outside) to (inside) source static _vpn_nat_95.1.226.4 75.1.224.21
    translate_hits = 315, untranslate_hits = 315
    Source - Origin: 95.1.226.4/32, Translated: 75.1.224.21/32
```

Outside 是 Secure Client连接至的接口，而 *inside* 是特定于新隧道组的接口。

注释 因为 VPN NAT 策略是动态的且不会添加到配置中，所以在 show run 对象和 show run nat 报告中，VPN NAT 对象和 NAT 策略会隐藏。

配置 VPN 会话限制

您可以运行的 IPsec 和 SSL VPN 会话数量与您的平台和 ASA 许可证支持的数量相同。要查看 ASA 的许可信息（包括最大会话数），请在全局配置模式下输入 **show version** 命令，并查找许可部分。以下示例显示该命令和该命令输出中的许可信息；为明确期间，其中还编入了其他输出内容。

```
hostname(config)# show version
...
Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 500            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 100            perpetual
Carrier                           : Enabled        perpetual
AnyConnect Premium Peers          : 5000           perpetual
AnyConnect Essentials             : 5000           perpetual
Other VPN Peers                   : 5000           perpetual
Total VPN Peers                   : 5000           perpetual
AnyConnect for Mobile             : Enabled        perpetual
AnyConnect for Cisco VPN Phone    : Enabled        perpetual
Advanced Endpoint Assessment      : Enabled        perpetual
Shared License                    : Disabled       perpetual
Total TLS Proxy Sessions          : 3000           perpetual
Botnet Traffic Filter             : Disabled       perpetual
IPS Module                        : Disabled       perpetual
Cluster                           : Enabled        perpetual
Cluster Members                   : 2              perpetual

This platform has an ASA5555 VPN Premium license.
```

显示许可证资源分配

使用以下命令显示资源分配：

```
asa2(config)# sh resource allocation
Resource       Total    % of Avail
Conns[rate]    100(U)      0.00%
Inspects[rate] unlimited
Syslogs[rate]  unlimited
Conns          unlimited
Hosts          unlimited
IPsec          unlimited
Mac-addresses  unlimited
ASDM           10          5.00%
SSH            10          10.00%
Telnet         10          10.0%
```

```
Xlates          unlimited
AnyConnect      1000        10%
AnyConnectBurst 200         2%
OtherVPN        2000        20%
OtherVPNBurst   1000        10%
```

显示许可证资源使用情况

使用以下命令显示资源使用情况：

注释 还可以使用 **sh resource usage system controller all 0** 命令显示系统级别使用情况，其限制为平台限制。

```
ASA(config-ca-trustpoint)# sh resource usage
Resource        Current  Peak  Limit  Denied  Context
Conns           1        16    280000 0       System
Hosts           2        10    N/A    0       System
AnyConnect      2        25    1000   0       cust1
AnyConnectBurst 0        0     200    0       cust1
OtherVPN        1        1     2000   0       cust2
OtherVPNBurst   0        0     1000   0       cust2
```

限制 VPN 会话

要将 AnyConnect VPN 会话（IPsec/IKEv2 或 SSL）数限制为低于 ASA 允许的值，可以在全局配置模式下使用 **vpn-sessiondb** max-anyconnect-premium-or-essentials-limit 命令。要删除会话限制，请使用此命令的 **no** 版本。

如果 ASA 许可证允许 500 个 SSL VPN 会话，而您想要将 AnyConnect VPN 会话数限制为 250 个，请输入以下命令：

```
hostname(config)# vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

要删除会话限制，请使用此命令的 **no** 版本：

```
hostname(config)# no vpn-sessiondb max-anyconnect-premium-or-essentials-limit 250
hostname(config)#
```

协商时使用身份证书

ASA 在与Secure Client协商 IKEv2 隧道时需要使用身份证书。对于 ikev2 远程访问信任点配置，请使用以下命令

```
crypto ikev2 remote-access trustpoint <name> [line<number>]
```

使用此命令可以让 Secure Client支持最终用户的组选择。可以同时配置两个信任点：两个 RSA、两个 ECDSA 或各一个。ASA 扫描已配置的信任点列表并选择客户端支持的第一个信任点。如果首选 ECDSA，则应先配置 ECDSA 信任点，再配置 RSA 信任点。

行号选项指定您想要插入信任点的行号。通常，此选项用于在不删除和重新添加另一行的情况下，在顶部插入信任点。如果未指定行，ASA 将在列表末尾添加信任点。

如果尝试添加已存在的信任点，将收到一条错误消息。如果使用 *no crypto ikev2 remote-access trustpoint* 命令而不指定要删除哪个信任点名称，则会删除所有信任点配置。

配置加密核心池

可以在对称多处理 (SMP) 平台上更改加密核心的分配，以提高 Secure Client TLS/DTLS 流量的吞吐量。这些更改可以加速 SSL VPN 数据路径，并在 Secure Client、智能隧道和端口转发方面提供客户可见的性能提升。以下步骤说明如何在单情景或多情景模式下配置加密核心池。

过程

指定如何分配密码加速器处理器：

crypto engine accelerator-bias

- **balanced** - 平均分配加密硬件资源（Admin/SSL 和 IPsec 核心）。
- **ipsec** - 将加密硬件资源优先分配给 IPsec（包括 SRTP 加密语音流量）。
- **ssl** - 将加密硬件资源优先分配给 Admin/SSL。当您支持基于 SSL 的 Secure Client 远程访问 VPN 会话时，请使用此偏差。

示例：

```
hostname(config)# crypto engine accelerator-bias ssl
```

配置动态分割隧道

通过动态拆分隧道，您可以在建立隧道后基于主机 DNS 域名动态调配拆分排除隧道。通过创建自定义属性并将其添加到组策略，可配置动态分割隧道。

开始之前

要使用此功能，必须具备 AnyConnect 版本 4.5（或更高版本）。有关进一步说明，请参阅关于动态分割隧道。

过程

步骤 1 在 WebVPN 上下文中可使用以下命令定义自定义属性：`anyconnect-custom-attr dynamic-split-exclude-domains description dynamic split exclude domains`

步骤 2 定义客户端需要访问的VPN隧道外的每个云/Web服务的自定义属性名称。例如，添加Google_domains以表示有关 Google Web 服务的 DNS 域名的列表。属性值包含要从 VPN 隧道中排除的域名列表，且必须为逗号分隔值(CSV)格式，如下所示：`anyconnect-custom-data dynamic-split-exclude-domains webex.com, webexconnect.com, tags.tiqcdn.com`

步骤 3 使用以下命令将之前定义的自定义属性附加到特定策略组中，该命令在组策略属性上下文中执行：`anyconnect-custom dynamic-split-exclude-domains value webex_service_domains`

下一步做什么

如果已配置拆分包含隧道，则仅当至少一个 DNS 响应 IP 地址是拆分包含网络的一部分时，才会实施动态拆分排除。如果在任何 DNS 响应 IP 地址与任何拆分包含网络之间没有重叠，则实施动态拆分排除不是必需的，因为匹配所有 DNS 响应 IP 地址的流量已从隧道中排除。

配置管理 VPN 隧道

管理 VPN 隧道可确保客户端系统在开启时连接到企业网络，这不仅限于最终用户建立了 VPN 连接的情况。您可以对办公室外的终端（尤其是用户很少通过VPN连接到办公网络的设备）执行补丁管理。需要企业网络连接的终端操作系统登录脚本也可以得益于此功能。

管理VPN隧道是为了向最终用户提供透明性；因此在默认情况下，用户应用发起的网络流量不会受到影响，而是会被定向到管理 VPN 隧道外部。

如果用户抱怨登录缓慢，可能表示管理隧道配置不当。有关管理 VPN 隧道的其他要求、不兼容问题、限制和故障排除，请参阅《Cisco Secure 客户端 安全移动客户端管理指南》。

开始之前

需要 AnyConnect 版本 4.7（或更高版本）。

过程

步骤 1 将已上传的配置文件 (profileMgmt) 添加到映射到管理隧道连接所用隧道组的组策略 (MgmtTunGrpPolicy)：

要指示配置文件是 AnyConnect 管理 VPN 配置文件，请在 **anyconnect profiles** 命令中包含 **type vpn-mgmt**。常规 AnyConnect VPN 配置文件的类型为 user。

```
group-policy MgmtTunGrpPolicy attributes
```

```
  webvpn
     anyconnect profiles value profileMgmt type vpn-mgmt
```

步骤 2 要通过用户隧道连接部署管理 VPN 配置文件，请将上传的配置文件 *(profileMgmt)* 添加到映射到用户隧道连接所用隧道组的组策略 *(DfltGrpPolicy)*：

```
group-policy DfltGrpPolicy attributes
  webvpn
     anyconnect profiles value profileMgmt type vpn-mgmt
```

查看活动 VPN 会话

以下主题介绍如何查看 VPN 会话信息。

按 IP 地址类型查看活动 Secure Client 会话

要使用命令行界面查看活动的 Secure Client 会话，请在特权 EXEC 模式下输入 **show vpn-sessiondb anyconnect filter p-ipversion** 或 **show vpn-sessiondb anyconnect filter a-ipversion** 命令。

- 显示按终端的公共 IPv4 或 IPv6 地址过滤的活动 Secure Client 会话。公共地址是由企业分配给终端的地址。

  show vpn-sessiondb anyconnect filter p-ipversion {v4 | v6}

- 显示按终端的已分配 IPv4 或 IPv6 地址过滤的活动 Secure Client 会话。已分配地址是由 ASA 分配给 Secure Client的地址。

  show vpn-sessiondb anyconnect filter a-ipversion {v4 | v6}

示例 Output from show vpn-sessiondb anyconnect filter p-ipversion [v4 | v6] command

```
hostname(config)# show vpn-sessiondb anyconnect filter p-ipversion v4

Session Type: AnyConnect

Username     : user1                  Index        : 40
Assigned IP  : 192.168.17.10          Public IP    : 198.51.100.1
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx     : 10570                  Bytes Rx     : 8085
Group Policy : GroupPolicy_SSLACCLIENT
Tunnel Group : SSLACCLIENT
Login Time   : 15:17:12 UTC Mon Oct 22 2012
Duration     : 0h:00m:09s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Output from show vpn-sessiondb anyconnect filter a-ipversion [v4 | v6] command

```
hostname(config)# show vpn-sessiondb anyconnect filter a-ipversion v6

Session Type: AnyConnect

Username     : user1                  Index        : 45
Assigned IP  : 192.168.17.10
Public IP    : 2001:DB8:8:1:90eb:3fe5:9eea:fb29
Assigned IPv6: 2001:DB8:9:1::24
Protocol     : AnyConnect-Parent SSL-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)RC4
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1
Bytes Tx     : 10662                  Bytes Rx     : 17248
Group Policy : GroupPolicy_SSL_IPv6   Tunnel Group : SSL_IPv6
Login Time   : 17:42:42 UTC Mon Oct 22 2012
Duration     : 0h:00m:33s
Inactivity   : 0h:00m:00s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

按 IP 地址类型查看活动的 LAN 到 LAN VPN 会话

要使用命令行界面查看活动的无客户端 SSL VPN 会话，请在特权 EXEC 模式下输入 **show vpn-sessiondb l2l filter ipversion** 命令。

该命令显示按连接的公共 IPv4 或 IPv6 地址过滤的活动 LAN 到 LAN VPN 会话。

公共地址是由企业分配给终端的地址。

show vpn-sessiondb l2l filter ipversion {v4 | v6}

关于 ISE 策略实施

思科身份服务引擎 (ISE) 是一个安全策略管理和控制平台。可自动化并简化有线连接、无线连接和 VPN 连接的接入控制和安全合规性管理。思科 ISE 主要用于与思科 TrustSec 结合提供安全接入和访客接入、支持自带设备 (BYOD) 计划和执行使用策略。

ISE 授权变更 (CoA) 功能提供一种机制，以在建立身份验证、授权和记帐 (AAA) 会话后更改其属性。当 AAA 中的用户或用户组的策略发生更改时，可以将 CoA 数据包从 ISE 直接发送到 ASA，以重新初始化身份验证并应用新策略。不需要内联安全状态实施点 (IPEP) 即可为与 ASA 设备建立的每个 VPN 会话应用访问控制列表 (ACL)。

在以下 VPN 客户端上支持 ISE 策略实施：

- IPSec
- Secure Client
- L2TP/IPSec

注释 系统支持某些策略元素，例如动态 ACL (dACL) 和安全组标记 (SGT)，而不支持诸如 VLAN 分配和 IP 地址分配之类的策略元素。

系统流程如下：

1. 最终用户请求 VPN 连接。
2. ASA 向 ISE 对用户进行身份验证，并且接收提供有限网络访问的用户 ACL。
3. 系统向 ISE 发送记帐启动消息以注册会话。
4. 直接在 NAC 代理和 ISE 之间进行安全状态评估。此过程对 ASA 透明。
5. ISE 通过 CoA“policy push”向 ASA 发送策略更新。这样可以识别提供更多网络访问权限的新用户 ACL。

注释 在连接的生存期内，可能会通过后续 CoA 更新进行对于 ASA 而言透明的其他策略评估。

这种流模型与使用 RADIUS CoA 的大多数场景不同。对于有线/无线 802.1x 身份验证，RADIUS CoA 不包含任何属性。它只会触发第二次身份验证，而在第二次身份验证中会附加所有属性，如 DACL。对于 ASA VPN 终端安全评估，没有第二次身份验证。所有属性都会在 RADIUS CoA 中返回。VPN 会话处于活动状态，无法更改大部分 VPN 用户设置。CoA 激活后可更改的唯一设置是重定向 URL、重定向 ACL 和安全组标记 (SGT)。

为 ISE 策略实施配置 RADIUS 服务器组

要启用 ISE 策略评估和实施，请针对 ISE 服务器配置 RADIUS AAA 服务器组并将服务器添加到该组。为 VPN 配置隧道组时，可以为该组中的 AAA 服务指定此服务器组。

过程

步骤 1 创建 RADIUS AAA 服务器组。

aaa-server *group_name* **protocol radius**

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)#
```

步骤 2 为 AAA 服务器组启用 RADIUS 动态授权 (CoA) 服务。

dynamic-authorization [**port** *number*]

可以选择是否指定端口。默认值为 1700，范围为 1024 至 65535。

当您在 VPN 隧道中使用服务器组时，RADIUS 服务器组将注册接收 CoA 通知，并且 ASA 会侦听用于从 ISE 获取 CoA 策略更新的端口

```
hostname(config-aaa-server-group)# dynamic-authorization
```

步骤 3 如果您不想将 ISE 用于授权，则请为 RADIUS 服务器组启用仅授权模式。

authorize-only

这表示当此服务器组用于授权时，RADIUS 访问请求消息将会构建为“仅授权”请求，而不是为 AAA 服务器定义的已配置的密码方法。如果您使用 **radius-common-pw** 命令为 RADIUS 服务器配置公用密码，则它将被忽略。

例如，如果您想将证书用于身份验证而不是此服务器组，则应使用仅授权模式。您仍可将此服务器组用于授权和在 VPN 隧道中记帐。

```
hostname(config-aaa-server-group)# authorize-only
```

步骤 4 启用 RADIUS 临时记帐更新消息的定期生成。

interim-accounting-update [**periodic** [*hours*]]

ISE 将基于其从 NAS 设备（如 ASA）收到的记帐记录，保留一个活动会话的目录。不过，如果 ISE 为期 5 天没有接收到该会话仍处于活动状态的任何指示（记帐消息或终端安全评估事务处理），则它将删除从其数据库中删除该会话记录。为了确保长期VPN连接不被删除，请将该组配置为针对所有活动会话向 ISE 发送定期临时记帐更新消息。

- **periodic**[*hours*] 允许为每个被配置为向有关服务器组发送审计记录的 VPN 会话定期生成和传输审计记录。可以选择包括发送这些更新的间隔（以小时为单位）。默认值为 24 小时，范围为 1 至 120。
- （无参数。）如果使用不带 **periodic** 关键字的此命令，则 ASA 仅会在将 VPN 隧道连接添加到无客户端VPN会话时发送临时审计更新消息。发生此情况时，将生成记帐更新，以便将新分配的 IP 地址通知给 RADIUS 服务器。

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

步骤 5 （可选。）将可下载 ACL 与来自 RADIUS 数据包的思科 AV 对中收到的 ACL 进行合并。

merge-dacl {**before-avpair** | **after-avpair**}

此选项仅适用于 VPN 连接。对于 VPN 用户，ACL 的形式可以是思科 AV 对 ACL、可下载 ACL 和在 ASA 上配置的 ACL。此选项确定可下载 ACL 和 AV 对 ACL 是否会合并，并且不适用于在 ASA 上配置的任何 ACL。

默认设置为 **no merge dacl**，此值指定可下载 ACL 将不与思科 AV 对 ACL 合并。如果同时收到 AV 对和可下载 ACL，则优先使用 AV 对。

before-avpair 选项指定可下载 ACL 条目应放置在思科 AV 对条目之前。

after-avpair 选项指定可下载 ACL 条目应放置在思科 AV 对条目之后。

```
hostname(config)# aaa-server servergroup1 protocol radius
hostname(config-aaa-server-group)# merge-dacl before-avpair
```

步骤 6 （可选。）指定在尝试下一服务器前，向组中的 RADIUS 服务器发送的最大请求数。

max-failed-attempts *number*

范围为 1 至 5。默认值为 3。

如果您使用本地数据库（仅用于管理访问）配置了回退方法，并且组中的所有服务器都无法响应，则会将该组视为无响应，并将尝试回退方法。该服务器组会在10分钟（默认值）内保持标记为无响应，以确保该时段内其他AAA请求不会尝试联系该服务器组，而是立即使用回退方法。要更改默认的无响应期间，请参阅下一步中的 **reactivation-mode** 命令。

如果没有回退方法，则 ASA 将继续重试该组中的服务器。

```
hostname(config-aaa-server-group)# max-failed-attempts 2
```

步骤 7 （可选。）指定用于重新激活组中的故障服务器的方法（重新激活策略）。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

其中：

- **depletion** [**deadtime** *minutes*] 仅在组中的所有服务器都处于非活动状态后才重新激活故障服务器。这是默认重新激活模式。可以指定从禁用组内最后一个服务器到随后重新启用所有服务器所经过的时长（0 到 1440 分钟之间）。默认值为 10 分钟。
- **timed** 在 30 秒钟的停机时间后重新激活出现故障的服务器。

```
hostname(config-aaa-server-group)# reactivation-mode deadtime 20
```

步骤 8 （可选。）向组中的所有服务器发送记帐消息。

accounting-mode simultaneous

如要恢复仅向活动服务器发送消息的默认设置，请输入 **accounting-mode single** 命令。

```
hostname(config-aaa-server-group)# accounting-mode simultaneous
```

步骤 9 将 ISE RADIUS 服务器添加至该组。

aaa-server *group_name* [(*interface_name*)] **host** {*server_ip* | *name*} [*key*]

其中：

- *group_name* 是 RADIUS 服务器组的名称。
- (*interface_name*) 是可以通过其访问服务器的接口的名称。默认值为 （内部）。需要使用圆括号。
- **host** {*server_ip* | *name*} 是 ISE RADIUS 服务器的 IP 地址或主机名。

- *key* 是用于加密连接的可选密钥。进入 aaa-server-host 模式后，您可以更轻松地在 **key** 命令中输入此密钥。如果不配置密钥，则不对连接加密（明文）。该密钥是一个区分大小写的字母数字字符串，最多 127 个字符，其值与 RADIUS 服务器上的密钥相同。

可以向该组添加多个服务器。

```
hostname(config)# aaa-server servergroup1 (inside) host 10.1.1.3
hostname(config-aaa-server-host)# key sharedsecret
hostname(config-aaa-server-host)# exit
```

ISE 策略实施的示例配置

使用密码针对 ISE 动态身份验证配置 VPN 隧道

以下示例显示如何为动态授权 (CoA) 更新和每小时定期记帐配置 ISE 服务器组。其中包括使用 ISE 配置密码身份验证的隧道组配置。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

针对 ISE 仅授权配置 VPN 隧道

以下示例显示如何使用ISE为本地证书验证和授权配置隧道组。包括服务器组配置中的仅授权命令，因为不会将服务器组用于身份验证。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

故障排除策略实施

以下命令可用于调试。

如要跟踪 CoA 活动，请输入以下命令：

```
debug radius dynamic-authorization
```

如要跟踪重定向 URL 功能，请输入以下命令：

```
debug aaa url-redirect
```

如要查看 URL 重定向功能对应的 NP 分类规则，请输入以下命令：

```
show asp table classify domain url-redirect
```

配置高级 SSL 设置

ASA 使用安全套接字层 (SSL) 协议和传输层安全 (TLS) 为 ASDM、无客户端 SSL VPN、VPN 和基于浏览器的会话提供安全消息传输支持。ASA 支持用于基于 SSL 的 VPN 和管理连接的 SSLv3、TLSv1、TLv1.1 TLSv1.2 以及 TLSv1.3 协议。此外，DTLS 还被用于 Cisco Secure 客户端的 AnyConnect VPN 模块连接。

支持以下密码（如下表所述）：

密码	TLSv1.1/DTLSV1	TLSV1.2/DTLSV1.2	TLSv1.3
TLS_AES_128_GCM_SHA256	否	否	是
TLS_CHACHA20_POLY1305_SHA256	否	否	是
AES256-GCM-SHA384	否	否	是
AES128-GCM-SHA256	否	是	否
AES128-SHA	是	是	否
AES128-SHA256	否	是	否
AES256-GCM-SHA384	否	是	否
AES256-SHA	是	是	否
AES256-SHA256	否	是	否
DERS-CBC-SHA	否	否	否
DES-CBC-SHA	是	是	否
DHE-RSA-AES128-GCM-SHA256	否	是	否

密码	TLSv1.1/DTLSV1	TLSV1.2/DTLSV1.2	TLSv13
DHE-RSA-AES128-SHA	是	是	否
DHE-RSA-AES128-SHA256	否	是	否
DHE-RSA-AES256-GCM-SHA384	否	l	否
DHE-RSA-AES256-SHA	是	是	否
ECDHE-ECDSA-AES128-GCM-SHA256	否	是	否
ECDHE-ECDSA-AES128-SHA256	否	是	否
ECDHE-ECDSA-AES256-GCM-SHA384	否	是	否
ECDHE-ECDSA-AES256-SHA384	否	是	否
ECDHE-RSA-AES128-GCM-SHA256	是	是	否
ECDHE-RSA-AES128-SHA256	否	是	否
ECDHE-RSA-AES256-GCM-SHA384	否	是	否
ECDHE-RSA-AES256-SHA384	否	是	否
NULL-SHA	否	否	否
RC4-MD5	否	否	否
RC4-SHA	否	否	否

注释 对于版本 9.4(1)，所有 SSLv3 关键字都已从 ASA 配置中删除，而且 SSLv3 支持也已从 ASA 中删除。如果您启用了 SSLv3，带 SSLv3 选项的命令将出现引导时间错误。ASA 随后将恢复为默认使用 TLSv1。

Citrix Mobile Receiver 可能不支持 TLS 1.1/1.2 协议；有关兼容性，请参阅 https://www.citrix.com/content/dam/citrix/en_us/documents/products-solutions/citrix-receiver-feature-matrix.pdf

要指定 ASA 协商 SSL/TLS 和 DTLS 连接的最低协议版本，请执行以下步骤：

过程

步骤 1 设置 ASA 将协商连接的最低协议版本。

ssl server-version ［**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**］ ［**dtlsv1** | **dtlsv1.2**］

其中：

- **tlsv1**- 输入此关键字则接受 SSLv2 ClientHello 消息并协商 TLSv1（或更高版本）
- **tlsv1.1**- 输入此关键字则接受 SSLv2 ClientHello 消息并协商 TLSv1.1（或更高版本）
- **tlsv1.2**- 输入此关键字则接受 SSLv2 ClientHello 消息并协商 TLSv1.2（或更高版本）
- **tlsv1.3** - 输入此关键字则接受 SSLv2 ClientHello 消息并协商 TLSv1.3（或更高版本）
- **dtlsv1**- 输入此关键字则接受 DTLSv1 ClientHello 消息并协商 DTLSv1（或更高版本）
- **dtlsv1.2**- 输入此关键字则接受 DTLSv1.2 ClientHello 消息并协商 DTLSv1.2（或更高版本）

注释
DTLS 的配置和使用仅适用于思科 Secure Client 远程访问连接。

请使用与 DTLS 版本相等或更高版本的 TLS，确保 TLS 会话与 DTLS 会话同样安全或更安全。鉴于此点，tlsv1.2 是选择 dtls1.2 时唯一可接受的 TLS 版本；而任何 TLS 版本均可与 dtls1 配合使用，因为其版本均等于或高于 DTLS 1.0。

示例：

示例：

```
hostname(config)# ssl server-version tlsv1.1

hostname(config)# ssl server-version tlsv1.2 dtlsv1.2
```

步骤 2 指定 ASA 作为服务器时使用的 SSL/TLS 协议的最高版本。

ssl server-max-version [**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**]

如果服务器最高版本配置为 TLSV1.2，则无法将 TLSV1.3 配置为服务器版本。

步骤 3 指定 ASA 用作客户端时所使用的 SSL/TLS 协议版本。

ssl client-version [**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**]

其中：

- **tlsv1** - 输入此关键字以指定 ASA 可以传输 TLSv1 客户端 Hello 消息并协商 TLSv1（或更高版本）。
- **tlsv1.1** - 输入此关键字以指定 ASA 可以传输 TLSv1.1 客户端 Hello 消息并协商 TLSv1.1（或更高版本）。
- **tlsv1.2** - 输入此关键字以指定 ASA 可以传输 TLSv1.2 客户端 Hello 消息并协商 TLSv1.2（或更高版本）。
- **tlsv1.3** - 输入此关键字以指定 ASA 可以传输 TLSv1.3 客户端 Hello 消息并协商 TLSv1.3（或更高版本）。

DTLS 不可用于 SSL 客户端角色。

示例：

示例：

```
hostname(config)# ssl client-version tlsv1
```

步骤 4 指定 ASA 作为客户端时使用的 SSL/TLS 协议的最高版本。

ssl client-max-version ［**tlsv1** | **tlsv1.1** | **tlsv1.2** | **tlsv1.3**］

如果客户端最高版本配置为 TLSV1.2，则无法将 TLSV1.3 配置为客户端版本。

步骤 5 指定 SSL、DTLS 和 TLS 协议的加密算法。

ssl cipher *version* ［ *level* | **custom** *string*］

其中：

- *version* 参数指定 SSL、DTLS 或 TLS 协议版本。支持的版本包括：
  - default - 用于出站连接的密码集。
  - dtlsv1 - 用于 DTLSv1 入站连接的密码。
  - dtlsv1.2 - 用于 DTLSv1.2 入站连接的密码。
  - tlsv1 - 用于 TLSv1 入站连接的密码。
  - tlsv1.1 - 用于 TLSv1.1 入站连接的密码。
  - tlsv1.2 - 用于 TLSv1.2 入站连接的密码。
  - tlsv1.3 - 用于 TLSv1.3 入站连接的密码。
- *level* 参数指定密码的强度并表示已配置的最低级别密码。有效值（按强度的升序排列）如下：
  - all - 包括所有密码。
  - low - 包括除 NULL-SHA 以外的所有密码。
  - medium（这是所有协议版本的默认值）- 包括所有密码（NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA 和 DES-CBC3-SHA 除外）。
  - fips - 包括所有符合 FIPS 的密码（NULL-SHA、DES-CBC-SHA、RC4-MD5、RC4-SHA 和 DES-CBC3-SHA 除外）。
  - high（仅适用于 TLSv1.2 和 TLSv1.3）- 仅包括 TLSv1.2 使用 SHA-2 密码的 AES-256。所有 TLSv1.3 密码的强度都很高。
- 通过指定 **custom** *string* 选项，您可以使用 OpenSSL 密码定义字符串对密码套件进行全面控制。有关详细信息，请参阅 https://www.openssl.org/docs/apps/ciphers.html。

推荐设置为 **medium**。使用 **high** 可能会限制连接。如果仅配置了几个密码，使用 custom 可能会限制功能。限制默认自定义值会限制出站连接，包括集群。

ASA 指定了支持的密码的优先级顺序。有关更多信息，请参阅命令参考。

此命令取代了从版本 9.3(2) 开始弃用的 ssl encryption 命令。

步骤 6 允许一个接口上有多个信任点。

ssl trust-point *name* [[**interface** *vpnlb-ip*] | [**domain** *domain-name*]

```
hostname(config)# ssl trust-point www-cert domain www.example.com
```

name 参数指定信任点的名称。**interface** 参数指定在其上配置信任点的接口的名称。vpnlb-ip 关键字仅适用于接口，并将此信任点与该接口上的 VPN 负载均衡集群 IP 地址关联。**domain***domain-name* 关键字-参数对指定与访问该接口所用的特定域名相关联的信任点。

最多可为每个接口配置 16 个信任点。

如果不指定接口或域，则此命令将为所有未配置信任点的接口创建回退信任点。

如果输入 **ssl trustpoint ?** 命令，则会显示可用的已配置信任点。如果输入 **ssl trust-point** *name***?** 命令（例如，**ssl trust-point mysslcert ?**），则会显示信任点 SSL 证书关联的可用已配置接口。

使用此命令时请遵守以下准则：

- trustpoint 的值必须是 **crypto ca trustpoint name** 命令中配置的 CA 信任点的名称。
- interface 的值必须是之前配置的接口的 nameif 名称。
- 删除信任点也会删除引用该信任点的任何 **ssl trust-point** 条目。
- 您可以为每个接口指定一个 ssl trust-point 条目，还可以指定一个不指定接口的条目。
- 可以将同一信任点重复用于多个条目。
- 一个配置了 domain 关键字的信任点可应用于多个接口（取决于连接方式）。
- 每个 *domain-name* 值只能有一个 **ssl trust-point**。
- 如果在输入此命令后显示以下错误：

  ```
  error:0B080074:x509 certificate routines:X509_check_private_key:key values
  mismatch@x509_cmp.c:339
  ```

  表示用户已配置新证书来替换先前配置的证书。无需任何操作。

- 证书按以下顺序选择：
  - 如果连接与 **domain** 关键字的值匹配，则首选该证书。（**ssl trust-point***name***domain***domain-name* 命令）
  - 如果与负载均衡地址建立连接，则选择 vpnlb-ip 证书。（**ssl trust-point** *name* **interface** *vpnlb-ip* 命令）
  - 为接口配置的证书。（**ssl trust-point** *name* interface 命令）
  - 未与接口关联的默认证书。(**ssl trust-point** *name*)
  - ASA 的自签名、自生成证书。

步骤 7 指定将与 TLS 所使用的 DHE-RSA 密码一起使用的 DH 群。

```
ssl dh-group [group14 | group15]

hostname(config)# ssl dh-group group14
```

group14 和 15 关键字配置 DH 群 14（2048 位模数，224 位素数阶子组）。

组 14 与 Java 7 不兼容。所有群均与 Java 8 兼容。组 14 符合 FIPS。默认值为 ssl dh-group group14。

步骤 8 指定将与 TLS 所使用的 ECDHE-ECDSA 密码一起使用的群。

```
ssl ecdh-group [group19 | group20 | group21]

hostname(config)# ssl ecdh-group group20
```

group19 关键字配置群 19（256 位 EC）。group20 关键字配置群 20（384 位 EC）。group21 关键字配置群 21（521 位 EC）。

默认值为 ssl ecdh-group group19。

注释
ECDSA 和 DHE 密码具有最高优先级。

下一步做什么

您可以使用以下命令来查看 TLS/DTLS 配置：

- 如果不是默认的 TLS/DTLS 版本，则输入**show run ssl** 。
- 如果是默认的 TLS/DTLS 版本，则输入**show run ssl all** 。

持续 IPsec 隧道流量

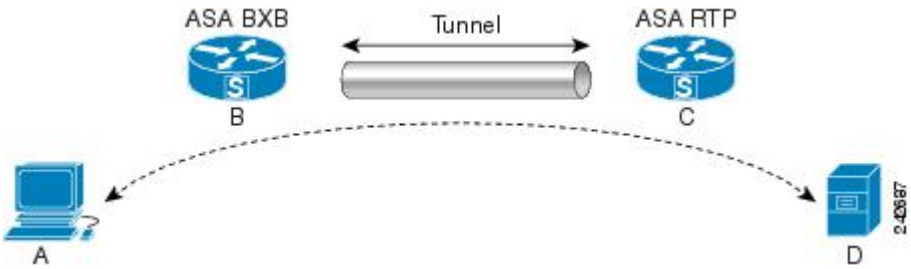
在运行版本低于 8.0.4 版的 ASA 软件的网络中，IPSec 隧道丢弃时，通过该隧道的现有 IPsec LAN 间或远程访问 TCP 流量会被丢弃。如果该隧道恢复，这些流量会按需重建。从资源管理和安全性角度来看，此策略非常不错。然而，对于用户，尤其是从 PIX 迁移至纯 ASA 环境的用户，以及无法轻松重启的旧版 TCP 应用，或者在包含常会频繁丢弃隧道的网关的网络中，在有些情况下，这一行为会带来问题。（有关详细信息，请参阅 CSCsj40681 和 CSCsi47630。）

持续 IPsec 隧道流量功能可以解决这一问题。启用此功能时，ASA 会保留和恢复状态 (TCP) 隧道流量。隧道丢弃时，所有其他流量都会被丢弃，并且必须在新隧道出现时重建。

注释　该功能支持在网络扩展模式下运行的 IPsec LAN 间隧道和 IPsec 远程访问隧道。它不支持 IPSec 或 AnyConnect/SSL VPN 远程访问隧道。

以下示例显示持续 IPsec 隧道流量功能的工作方式。

图 2: 网络场景



在此示例中，BXB 和 RTP 网络通过一对安全设备，经由安全的 LAN 间隧道进行连接。BXB 网络中的 PC 正经由安全隧道，通过 RTP 网络中的服务器执行 FTP 传输。在此场景中，假设在 PC 登录至服务器并开始传输后，出于某些原因，隧道丢弃。尽管隧道会因为数据仍在尝试流动而重建，FTP 传输却不会完成。用户必须终止传输，并通过重新登录至服务器来重新开始传输。然而，如果启用了持续 IPsec 隧道，一旦隧道在超时间隔内被重建，数据会继续成功流过新的隧道，因为安全设备会保留该流量的历史记录（状态信息）。

场景

以下各节说明隧道丢弃和隧道恢复时的数据流量状况，首先说明禁用持续 IPsec 隧道流量功能时的情况，然后说明启用该功能时的情况。有关这两种情况下的网络图解，请参阅上图。在此图中：

- 流量 B-C 定义隧道并承载加密 ESP 数据。
- 流量 A-D 是用于 FTP 传输的 TCP 连接并通过由流量 B-C 定义的隧道。此流量还包括防火墙用于检查 TCP/FTP 流量的状态信息。该状态信息至关重要，在传输过程中，防火墙会不断更新该状态信息。

注释 为简单起见，每个方向上的反向流量已被忽略。

已禁用持续 IPsec 隧道流量

LAN 到 LAN 隧道丢弃时，流量 A-D 和流量 B-C 以及属于它们的所有状态信息都会被删除。随后，隧道被重建，流量 B-C 被重建，并且能够继续承载隧道数据。但是 TCP/FTP 流量 A-D 出现故障。因为描述 FTP 传输中到目前为止的流量状况的状态信息已被删除，状态防火墙阻止未送达的 FTP 数据，并拒绝创建流量 A-D。已丢失此流量的历史记录的状况会一直存在，防火墙将 FTP 传输视为离群的 TCP 数据包，并将其丢弃。此为默认行为。

已启用持续 IPsec 隧道流量

在启用持续 IPsec 隧道流量功能的情况下，一旦隧道在超时时段内被重建，数据会继续成功流过，因为 ASA 仍然可以访问流量 A-D 中的状态信息。

在启用该功能的情况下，ASA 会单独对待该流量。这意味着，流量 B-C 定义的隧道被丢弃时，流量 A-D 不会被删除。ASA 保留和恢复状态 (TCP) 隧道流量。所有其他流量都被丢弃，并且必须在新隧

道上重建。这不会削弱隧道流量的安全策略，因为在隧道发生故障时，ASA 会丢弃流量 A-D 上抵达的所有数据包。

未丢弃隧道 TCP 流量，因此其依靠 TCP 超时进行清除。但是，如果为特定隧道流量禁用了超时，则该流量会保留在系统中，直到手动或通过其他方法（例如，通过来自对等体的 TCP RST）清除为止。

使用 CLI 配置持续 IPsec 隧道流量

配置示例

持续 IPsec 隧道流量故障排除

对持续 IPsec 隧道流量存在的问题进行故障排除时，**show asp table** 和 **show conn** 命令都十分有用。

持续 IPsec 隧道流量功能是否已启用？

要查看特定隧道是否已启用此功能，请使用 **show asp table** 命令查看与该隧道关联的 VPN 情景。show asp table vpn-context 命令对隧道丢弃后维持状态流量的每个情景显示“+PRESERVE”标志，如以下示例所示（为方便辨认，添加了粗体效果）：

```
hostname(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

------------------------------------------------------------------------------

hostname(config)# show asp table vpn-context detail

VPN CTX  = 0x0005FF54

Peer IP  = ASA_Private
Pointer  = 0x6DE62DA0
State    = UP
Flags    = DECR+ESP+PRESERVE
SA       = 0x001659BF
SPI      = 0xB326496C
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN CTX  = 0x0005B234

Peer IP  = ASA_Private
Pointer  = 0x6DE635E0
State    = UP
Flags    = ENCR+ESP+PRESERVE
SA       = 0x0017988D
SPI      = 0x9AA50F43
Group    = 0
```

```
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
hostname(config)#
Configuration and Restrictions
This configuration option is subject to the same CLI configuration restrictions as other
sysopt VPN CLI.
```

定位孤立流量

如果 LAN 间/网络扩展模式隧道丢弃，并且没有在超时之前恢复，则可能存在许多孤立隧道流量。这些流量不会因为隧道发生故障而被拆解，但是试图从中流过的所有数据都会被丢弃。要查看这些流量，请使用 **show conn** 命令，如以下示例所示（出于强调和显示用户输入的目的，添加了粗体效果）：

```
asa2(config)# show conn detail
9 in use, 14 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,
       E - outside back connection, F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media, n - GUP
       O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       X - inspected by service module
```

以下示例显示存在孤立流量时 **show conn** 命令的示例输出，孤立流量以 **V** 标志表示：

```
hostname# show conn
16 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:21 idle 0:00:00 bytes 1048 flags UOVB
TCP out 192.168.110.251:21137 in 192.168.150.252:21 idle bytes 1048 flags UIOB
```

要将报告内容限定为具有孤立流量的连接，请将 **vpn_orphan** 选项添加至 **show conn state** 命令，如以下示例所示：

```
hostname# show conn state vpn_orphan
14 in use, 19 most used
TCP out 192.168.110.251:7393 in 192.168.150.252:5013 idle 0:00:00 bytes 2841019 flags UOVB
```

使用加密存档进行故障排除

关于加密存档

加密问题难以分类。而加密存档可帮助您解决这些问题。加密存档包含有关加密请求的加密会话信息、对等体信息、发送加密请求的组件以及超时的加密会话信息。ASA 不会保存会话的密钥和初始化向量 (IV)。对于 SSL 和 IPsec，您还可以查看以下信息：

- 对于 SSL：会话 SSL 版本、源、目的 IP 地址和端口。
- 对于 IPsec：IPsec 安全关联信息。

一个环可以容纳 2000 个加密命令条目。ASA 会在其中一个环中推送 crypto 命令，并在完成加密请求后提取结果。加密存档文件现在包含超时加密请求的环和条目索引。环及其条目索引有助于对有问题的加密命令进行故障排除。

加密存档有两种格式：文本文件和二进制文件。您可以使用 **debug menu ctm 103** 命令来解码二进制文件。

例如：

```
ASA# debug menu ctm 103 crypto_eng0_arch_4.bin
[Nitrox V Archive Header v1.0 Info]
ASA Image Version: PIX (9.20) #0: Tue Mar 29 16:20:30 GMT 2022
...
SE SSL microcode: CNN5x-MC-SE-SSL-0011
AE microcode: CNN5x-MC-AE-MAIN-0002
Crypto Engine 0
Crash type: SE Ring Timeout
...
Core Soft Resets: 11
...
Timeout Ring (SE): 12
Timeout Entry: 642
SE TIMEOUT:
Core SE 6 Touts: 2
Core SE 8 Touts: 2
Core SE 12 Touts: 4
Core SE 32 Touts: 2
Core SE 37 Touts: 1
.....
[Timeout Session Info]
Active: TRUE
Sync: FALSE
Callback: TRUE
Saved Callback: FALSE
Commands in progress: 1
Engine : hardware
Device : n5 (Nitrox V)
Session : ssl
Priority: normal
NP VPN context handle : 0x00000000
Flag : 0
vcid : 0
Block size : 2050
async cb ring index: 0
tls offload rsa: FALSE
```

```
Session context:
SSL Version : dtls1.2
SSL Context Type : handshake
Encryption Mode : gcm
Auth Algorithm : null
Hash Algorithm : none
Key Size : 32
SSL V : dtls1.2
Source IP : 82.1.2.2
Source Port : 51915
Dest IP : 82.29.155.32
Dest Port : 443
```

在上例中，突出显示的信息显示了超时环、崩溃时间（超时条目）和 SSL 会话信息。

加密存档支持的设备

以下配备 Nitrox V 加密加速器的设备可支持加密存档：

- Cisco Firepower 3105、3110、3120、3130、3140
- Cisco Firepower 4112、4115、4125、4145
- Cisco Firepower 9300 SM-40、SM-48 和 SM-56

使用 SSL 计数器

您可以使用 SSL 计数器来查看 SSL 隧道信息和日志。有关围绕连接建立的状态机转换、其他状态和详细信息可用于帮助进行调试。

debug ssl state 命令提供以下信息：

- 具有关联 IP、端口和协议的远程设备和接口。
- 用于 SSL 连接建立错误的调试。
- 用于验证解密数据填充长度的调试。

使用 **show counters** 命令来查看 SSL 计数器。从版本 9.20.1 开始，有更多的 SSL 计数器可用于调试，例如：

- CNT_SSL_NP_CP_EVENT_NULL
- CNT_SSL_NP_CP_EVENT_ENQUEUE_ERR
- CNT_SSL_NP_CP_EVENT_RELEASE
- CNT_SSL_NP_SNP_FLOW_HNDSHK_FAIL
- CNT_SSL_NP_HDL_LOCK_RELEASE
- CNT_SSL_NP_VERIFY_PADDING
- CNT_SSL_NP_MAX_PAD_LEN_EXCEEDED

- CNT_SSL_NP_NO_CIPHERS_COMPATIBLE
- CNT_SSL_NP_CIPHER_LIC_NOT_GOOD

如何删除停滞的 ASP 表条目

在版本 9.19.1 及更早版本中，如果存在卡住的 ASP 加密规则，则您必须重新启动设备。在版本 9.20.1 及更高版本中，您可以使用 **debug menu asp 100 <encrypt_rule_id>** 命令从 ASP 表中删除停滞的加密规则，而无需重新启动设备。使用 **show asp table classify domain encrypt** 命令查找 *encrypt_rule_id*。

准则

- 由于调试输出在 CPU 进程中享有高优先级，因此可导致系统不可用。我们建议您仅在与思科 TAC 的故障排除会话期间使用此 debug 命令。
- 不会验证检查规则是否停滞。如果系统尝试删除的规则之前已使用此命令删除，则设备将会崩溃。
- 命令 ID 参数必须与 ASP 表中的实际 ID 完全匹配。

示例

在下面的示例中，当流量达到停滞规则 **0x7f039846aaaa** 时，流量会被丢弃，而不是达到良好规则 **0x7f039846bbbb**。您可以从命中计数中识别停滞的规则。停滞规则的命中计数为 9999，而良好规则的命中计数为 0。

1. 使用 **show asp table classify domain encrypt** 命令来查看 ASP 规则。

```
ASAv(config)# show asp table classify domain encrypt
...
out id=0x7f039846aaaa, priority=70, domain=encrypt, deny=false
hits=9999, user_data=0xaaaa, cs_id=0x7f03941866e0, reverse, flags=0x0, protocol=0
src ip/id=1.0.0.0, mask=255.0.0.0, port=0, tag=any
dst ip/id=2.0.0.0, mask=255.0.0.0, port=0, tag=any
src nsg_id=none, dst nsg_id=none
dscp=0x0, input_ifc=any, output_ifc=outside
out id=0x7f039846bbbb, priority=70, domain=encrypt, deny=false //this is a good rule
hits=0, user_data=0xbbbb, cs_id=0x7f03941866e0, reverse, flags=0x0, protocol=0
src ip/id=1.0.0.0, mask=255.0.0.0, port=0, tag=any
dst ip/id=2.0.0.0, mask=255.0.0.0, port=0, tag=any
src nsg_id=none, dst nsg_id=none
dscp=0x0, input_ifc=any, output_ifc=outside
...
```

2. 使用 **debug menu asp 100 <encrypt_rule_id>** 命令从 ASP 表中删除停滞的加密规则

```
ASAv(config)# debug menu asp 100 id=0x7f039846aaaa
Encrypt rule 0x7f0398469510 was successfully deleted.
```

3. 使用 **show asp table classify domain encrypt** 命令来验证 ASA 是否已删除停滞的 ASP 规则。

```
ASAv(config)# show asp table classify domain encrypt
...
out id=0x7f039846bbbb, priority=70, domain=encrypt, deny=false //now this rule has hits
hits=10, user_data=0xbbbb, cs_id=0x7f03941866e0, reverse, flags=0x0, protocol=0
```

```
src ip/id=1.0.0.0, mask=255.0.0.0, port=0, tag=any
dst ip/id=2.0.0.0, mask=255.0.0.0, port=0, tag=any
src nsg_id=none, dst nsg_id=none
dscp=0x0, input_ifc=any, output_ifc=outside
```

从 ASA 清除 WebVPN 配置

使用 **no webvpn** 和 **clear configure webvpn** 命令时，不会删除默认 WebVPN 配置。会保留 **http_in** 和 **http_out** 计数器以整理压缩统计信息。

要从 ASA 中清除 WebVPN 配置，请执行以下操作之一：

- 启动后使用 **no compression all** 命令禁用压缩统计信息。
- 使用 **clear compression all** 命令清除压缩统计信息计数器。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。