AnyConnect实施和性能/扩展参考，用于COVID-19准备

目录

简介

随着世界各国正在与COVID-19全球大流行作战，越来越多的公司正在实施远程工作政策来防止疾病的传播。因此，对远程访问VPN(RAVPN)的需求增加，以便员工访问公司内部资源。本文提供配置指南的参考，用于在网络内快速设置RAVPN，或识别和解决性能或扩展相关问题。

实施

以下部分详细介绍AnyConnect远程访问配置和各种思科平台上的部署，以及证书安装指南，因为由于RAVPN的证书身份验证要求，证书部署是思科远程访问不可或缺的一部分。

许可

在设备上终止RAVPN连接需要许可证。ASA平台仅支持2个VPN对等点，无许可证。FTD不允许在未获得许可的情况下将AnyConnect配置部署到设备。由于COVID-19爆发，思科提供免费临时许可证，以帮助用户在其思科设备上实施RAVPN。有关此项的详细信息，请参阅：获取紧急COVID-19 AnyConnect许可证

AnyConnect初始配置快速入门指南

按照以下快速入门指南实施具有最常见配置的AnyConnect远程访问：

- 在 ASA 上使用拆分隧道功能配置 AnyConnect Secure Mobility Client
- FTD上的AnyConnect远程访问VPN配置
- FMC管理的FTD的初始AnyConnect配置（视频）

有关完整的产品配置指南，请参阅以下内容。

完整配置指南

ASA ：

- ASA ASDM配置
- ASA CLI 配置

FTD:

- 由FDM管理的FTD
- FTD由FMC管理

IOS/IOS-XE:

- 用于SSLVPN的IOS路由器
- 用于SSL VPN的IOS-XE路由器（仅CSR）
- 用于IKEv2 VPN的IOS/IOS-XE路由器

证书安装指南

- ASA
- FTD FDM
- FTD FMC
- IOS/IOS-XE

性能和扩展问题

随着RAVPN使用率的显着增加，AnyConnect用户可能会遇到性能问题。请参阅以下内容，确定如何确定这些问题以及解决这些问题的缓解策略。

问题症状和识别

高 CPU 利用率

CPU利用率直接影响VPN用户的性能。CPU利用率将随着设备处理的加密或解密流量的增加而增加

。当平台接近其可处理的最大VPN吞吐量时，设备可以体验到高CPU。需要确定CPU使用率较高是由于设备超订用还是由于其他问题。

要检查设备是否处于高CPU，建议运行以下命令：

show process cpu-usage non-zero

show cpu usage

示例输出：

```
asa# show processes cpu-usage non-zero
PC         Thread       5Sec     1Min     5Min   Process
0x00000000019da592   0x00007fffd808b040     0.0%     0.0%     0.5%   Logger
0x0000000000844596   0x00007fffd807bd60     0.0%     0.0%     0.1%   CP Processing
0x0000000000c0dc8c   0x00007fffd8074960     0.1%     0.1%     0.1%   ARP Thread
   -          -        43.8%    43.8%    40.3%   DATAPATH-0-2209
   -          -        43.9%    43.8%    40.3%   DATAPATH-1-2210

asa# show cpu usage
CPU utilization for 5 seconds = 88%; 1 minute: 88%; 5 minutes: 82%
```

在上例中，观察到DATAPATH-0和DATAPATH-1占CPU总利用率的87.7%。在这种情况下，ASA超订用，因此需要确定此症状是否是由于大量加密和解密流量造成的。然后，可以根据该平台产品手册中记录的VPN吞吐量值对其进行基准测试。

要计算每秒通过设备的VPN流量总量，可以在*Global Statistics* 部分(在*show crypto accelerator statistics* 命令中找到)中添加*Input bytes*和*Output bytes*。在ASA或FTD上，使用命令clear crypto accelerator statistics清*除show crypto accelerator statistics*的输出*结果*。等待一定时间，然后运行命令：*show crypto accelerator statistics*，如下所示：

```
asa# show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capability]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 2
   Max crypto throughput: 1000 Mbps
   Max crypto connections: 5000
[Global Statistics]
   Number of active accelerators: 2
   Number of non-operational accelerators: 0
   Input packets: 257353
   Input bytes: 271730225                          <----------------
   Output packets: 2740
   Output error packets: 0
   Output bytes: 57793                             <----------------
[…]
```

以特定间隔拍摄几个快照，获得可转换为每秒位数(bps)的平均吞吐量（以字节为单位）。 要达到此目的，公式是：

$$\frac{[InputBytes + OutputBytes] * 8}{1,000,000 * seconds} = Mbps$$

在上一个示例中，在***0秒时发***出clear crypto accelerator statistics命令。10秒后，发出***show crypto accelerator statistics***命令以获取10秒间隔内的总字节数。然后，这些值用于计算在10秒间隔内处理的217Mbps的bps。可能需要多个快照才能获得更准确的平均值。

请注意，所有加密/解密流量（HTTPS、SSL、IPsec、SSH等）的这些值都会增加。 我们可以使用此值确定平均VPN吞吐量，并将其与数据表进行比较。如果平台的平均吞吐量与数据表上显示的吞吐量大致相同，则加密和解密流量会超订用设备。

此外，由于计数器不会增加VPN流量，因此此方法无法用于确定Firepower 2100平台上的VPN吞吐量。正在CSCvt46830中跟踪此情况 。

最大VPN连接数

当达到最大VPN连接数时，用户可能会遇到无法连接的中断期。尽管激活AnyConnect Plus或Apex许可证可解锁VPN对等体的最大数量，但如果达到该最大数量，则不允许在设备上添加其他用户。

要检查设备上可用的VPN连接最大数量，请检查***show vpn-sessiondb***的输出：

```
asa# show vpn-sessiondb
----------------------------------------------------------------------------
VPN Session Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concur : Inactive
                            ------------------------------------------------
AnyConnect Client           :     10 :        218 :          11 :        0
  SSL/TLS/DTLS              :     10 :        218 :          11 :        0
Clientless VPN              :      0 :         73 :           4
  Browser                   :      0 :         73 :           4
----------------------------------------------------------------------------
Total Active and Inactive   :     10             Total Cumulative :    291
Device Total VPN Capacity   :    250
Device Load                 :     4%
----------------------------------------------------------------------------

----------------------------------------------------------------------------
Tunnels Summary
----------------------------------------------------------------------------
                             Active : Cumulative : Peak Concurrent
                            ------------------------------------------------
Clientless                  :      0 :         73 :               4
AnyConnect-Parent           :     10 :        218 :              11
SSL-Tunnel                  :     10 :         77 :              10
DTLS-Tunnel                 :     10 :         65 :              10
----------------------------------------------------------------------------
Totals                      :     30 :        433
----------------------------------------------------------------------------
```

要确定平台支持的用户总数，请查看位于下方的设备数据表。

如果VPN用户无法连接，并且您已验证设备未达到最大VPN用户数，请向TAC寻求其他帮助。

数据表参考

以下数据表突出显示了平台支持的最大VPN用户数和基于测试的最大VPN吞吐量。IKEv2和DTLS

AnyConnect的总（聚合）吞吐量应与每个部分中列出的IPsec VPN吞吐量相似。

- ASAv
- ASA 5500
- ASA 5585
- Firepower 1000
- Firepower 2100
- Firepower 4100
- Firepower 9300

潜在缓解

启用分割隧道

默认情况下，ASA和FTD上的组策略将实施隧道。这将通过VPN发送RA客户端生成的所有流量，以便头端进行处理。由于数据包加密和解密与CPU利用率直接相关，因此必须确保只有必要的流量由公司安全策略允许的VPN头端处理。考虑使用拆分隧道策略而不是全隧道来将VPN头端从不必要的负载中保存。

- ASA拆分隧道指南
- FTD(FMC)分割隧道指南

注意：Tunnel All实施公司范围的参数安全策略，而分割隧道依靠客户端设备来帮助保护用户的互联网流量。思科提供Umbrella等其他安全工具，以在使用拆分隧道策略时保护VPN用户。

实施VPN负载均衡（仅ASA）

VPN负载均衡是ASA平台支持的一项功能，允许两个或多个ASA共享VPN会话负载。如果两台设备都支持500个VPN对等体，通过在它们之间配置VPN负载均衡，设备将支持它们之间总共1000个VPN对等体。此功能可用于将同步VPN用户数量增加到单个设备可以处理的数量之外。有关VPN负载均衡（包括负载均衡算法）的详细信息，请访问：VPN负载均衡

配置优化

平台上启用的其他服务将增加设备的处理量和负载。例如，IPS、SSL解密、NAT等。考虑将设备配置为仅终止VPN会话的VPN集中器。

隧道协议选择

默认情况下，ASA上的组策略配置为尝试建立DTLS隧道。如果UDP 443流量在VPN头端和AnyConnect客户端之间被阻止，它将自动回退到TLS。建议使用DTLS或IKEv2来提高最大VPN吞吐量性能。由于协议开销较少，DTLS提供比TLS更好的性能。IKEv2还提供比TLS更好的吞吐量。此外，使用AES-GCM密码可能会略微提高性能。这些密码在TLS 1.2、DTLS 1.2和IKEv2中可用。

按隧道实施QoS（仅FTD）

可以实施QoS以限制在出站方向发送给AnyConnect用户的流量。这样，VPN头端就可以强制每个远程访问客户端获得其出口带宽的公平份额。有关此项的详细信息，请访问：FTD配置

实施加密引擎加速器偏差（仅ASA）

加密引擎加速器偏差用于重新分配加密核心，使一个加密协议优于另一个加密协议（SSL或IPsec）。 这的目的是优化AnyConnect吞吐量，如果大多数VPN隧道使用IPsec或SSL。实施此命令可能导致服务中断，因此需要维护窗口。此外，性能（AnyConnect吞吐量和CPU利用率）的提高可能因流量配置文件而异。如果VPN头端仅终止SSL会话或仅终止IPsec会话，则可考虑使用此命令进一步优化VPN头端。命令参考位于：命令参考

要查看当前加密核心分配，请运行命令***show crypto accelerator load-balance***。此命令不显示设备能够处理的加密利用率总量 — 它表示分配给每个核心的ssl或ipsec流量的比率。要查找设备的大致利用率，请参阅上述“**CPU利用率高**”部分，并将计算值与平台数据表中的值进行比较。

在主要终止远程访问SSLVPN的ASA平台上，建议使用crypto engine accelerator-bias ssl命令调整加密核心分配以***支持SSL***。

以下示例显示在ASA5555上使用crypto engine accelerator-bias ssl命令***进行核心分配，以***支持AnyConnect SSL客户端：

```
asa# sh run all crypto engine
crypto engine accelerator-bias ssl
asa# show crypto accelerator load-balance

[..]
                  Crypto SSL Load Balancing Stats:
                  ================================

Engine      Crypto Cores             SSL Sessions            Active Session
                                                             Distribution (%)
======     ==============      ============================   ================
  0        IPSEC 1, SSL 7      Total: 166714  Active:   205         100.0%
[..]
```

无论平台当前的加密利用率如何，活动会话分布始终为100%。

注意：加密核心再平衡在以下平台上可用：ASA 5585、5580、5545/5555、4110、4120、4140、4150、SM-24、SM-36、SM-44和ASASM。

常见问题

许可

问:为什么我不能下载AnyConnect软件？

A：您必须购买AnyConnect Plus或Apex许可证才能下载AnyConnect客户端。之后，您应该有权。如果您在购买AnyConnect Apex或Plus许可证后仍无权获得授权，请通过授权提交问题以解决此问题。

问:为什么在智能许可帐户中看到99999为AnyConnect许可证购买？

A：对于某些AnyConnect许可证（例如AnyConnect Plus永久许可证或非带状AnyConnect Plus或Apex许可证），应执行此操作。

问:什么因素决定了“使用中”的下降时间？

A：当注册使用AnyConnect许可证的设备时，该值会递减。例如，如果注册FMC，然后将AnyConnect Plus许可证添加到设备，则AnyConnect Plus许可证的“使用中”值将减少。此值不**会根据**当前用户会话递减。注册ASAv**设备**不会减去“使用中”计数。这是一个已知的表面问题。注册的设备数量不能超过已购买的授权用户数量。

问:什么因素决定了购买的价值？

A：购买值取决于随许可证购买的授权用户数量。例如，25个用户的AnyConnect Plus许可证将包含25个已购买计数。

问:如何启用强加密？

A：要启用强加密，在创建注册令牌时必须选中“允许使用此令牌注册的产品上的出口控制功能”复选框。

问:如何从PAK转换到智能许可？

A：应使用此许可打开案例。

问:如果我有“X”用户许可证，如果“X+1”或更多用户连接到设备，会发生什么情况？

A：借助Apex和Plus许可证，设备的完整VPN用户容量将解锁。只要设备未达到其最大vpn用户限制，设备将继续接受连接。设备上没有针对VPN用户会话的实施，它基于荣誉。如果需要增加设备的vpn会话使用，您有责任购买额外的授权用户许可证。要检查设备支持的最大用户数，请在Cisco网站上查看设备的数据表或运行***show vpn-sessiondb***并检查“设备总VPN容量”。对于ASA，您还可以运行***show version***或***show vpn-sessiondb license-summary***命令。

问:如何检查许可证是否已在我的设备上激活？

A：在FTD上，除非激活许可证，否则您将无法部署AnyConnect配置。在ASA上，您可以检查***show version***或***show vpn-sessiondb license-summary***，以检查允许的用户数。如果没有激活的许可证，最多将是2个用户。请注意，在ASA上，上述命令不会显示Plus/Apex许可证信息。正在使用增强请求CSCuw74731跟踪此项。

配置

问：我可以使用哪些ASA平台进行VPN负载均衡？能否在VPN负载平衡集群中使用不同的ASA硬件平台或不同的软件版本？

答：是,VPN负载平衡集群可以由不同的物理或虚拟ASA型号（包括ASAv）组成。但是，通常建议集群为同构。如果vpn负载平衡集群中使用不同的软件版本，则仅支持IPsec会话。有关详细信息，请参阅：VPN负载平衡的准则和限制。

问：如何配置分割隧道？您能否排除Office 365等特定类型的应用流量，使其不能通过拆分隧道配置

进行隧道传输？

A：有关各种使用案例的配置示例，请参阅思科社区文章AnyConnect Split Tunneling。您还可以结合使用分割隧道和动态分割隧道来实现基于应用的分割隧道。有关如何为Office 365和WebEx优化AnyConnect拆分隧道的示例，请参阅如何为Microsoft Office365和Cisco Webex连接优化Anyconnect。

问：当连接到带AnyConnect的ASA头端时，我看到错误“Untrusted certificate warning”。这为何发生？

A：这可能是因为头端使用自签名证书。要解决此问题，可从证书颁发机构购买SSL证书并将其安装在头端ASA上。有关详细的实施步骤，请参阅：配置ASA:SSL 数字证书安装和续约.

问：Cisco RAVPN头端是否支持通配符证书？

A：是，支持通配符和带DNS使用者备用名称(SAN)的证书。

问：单台设备能否同时使用负载均衡和故障切换？

A：VPN负载均衡支持主用/备用故障切换。如果主用设备发生故障，备用设备将立即接管，对VPN隧道没有影响。主用/主用故障转移配置不支持VPN负载均衡。

监控

问：我可以使用哪个SNMP MIB来监控ASA CPU的使用情况？

答：CISCO-PROCESS-MIB可用于监控ASA CPU的使用情况。有关受支持MIB的完整列表，请参阅：自适应安全设备MIB支持列表。另外，要获取特定ASA支持的SNMP MIB和OID的列表，可以发出以下命令：***show snmp-server oidlist。***

问：如何监控当前连接到VPN头端的用户数？

A：从CLI使用*show vpn-sessiondb*检查ASA或FTD或SNMP MIB上的当前用户数

CISCO-REMOTE-ACCESS-MONITOR-MIB。

故障排除

问：某些AnyConnect VPN用户似乎经常出现断开连接。如何排除此类问题：

A：有关VPN断开连接和其他常见AnyConnect问题的故障排除，请参阅：AnyConnect VPN客户端故障排除指南 — 常见问题。

问：当有一定数量的用户连接到VPN前端时，将无法再连接任何用户。许可证在设备上激活，***show vpn-sessiondb***显示设备可以处理更多用户。问题可能是什么？

A：检查这些用户的VPN本地地址池，确保连接的用户数量不超过可用地址的数量。您可以使用命令***show ip local pool [pool-name]进行验证***。旧平台上的另一个潜在原因是***vpn-sessiondb max-anyconnect-premium-or-essentials-limit***命令设置为低值。您可以使用命令show run all vpn-***sessiondb来验证这一点***。如果出现这种情况，可以增加该值或删除命令以防止此限制。

获取其他帮助

如需其他帮助，请联系TAC。需要有效的支持合同：思科全球支持联系方式

您也可以访问Cisco VPN社区。

此外，您还可以查看TAC安全展播客

参考

请在下面找到其他链接，这些链接可用于AnyConnect部署和一般处理COVOD-19相关问题。

- 思科安全解决方案应对远程员工人数的增加 — 思科社区
- AnyConnect订购指南
- AnyConnect许可常见问题
- 安全远程工作人员的AnyConnect VPN、ASA和FTD常见问题