AnyConnect实施和性能/比例缩放参考COVID-19准备的

目录

简介

因为国家(地区)环球作战COVID-19全局大流行病，越来越多的公司实现远程工作策略防止传播疾病。结果，有远程访问VPN的(RAVPN)不断增长的需求提供雇员存取对于内部公司资源。此条款为快速设置在网络内的RAVPN提供对配置指南的参考或识别并且论及性能或扩展相关问题。

实施

以下部分详细信息AnyConnect远程访问配置和部署在多种Cisco平台，以及认证安装指南，因为证书部署是必要组成部分对Cisco远程访问由于证书验证需求RAVPN的。

许可授权

许可证要求终止在设备的RAVPN连接。ASA平台只将支持2 VPN对等体，不用许可证。FTDs不会允许在设备将被部署的AnyConnect配置没有许可授权。由于COVID-19爆发， Cisco提供有实现的RAVPN自由的临时许可证协助用户在他们的Cisco设备。可以找到关于此的更多信息：获取紧急COVID-19 AnyConnect许可证

AnyConnect初始配置Quickstart指南

跟随这些quickstart指南实现与多数常见配置的AnyConnect远程访问：

- 配置AnyConnect有分割隧道的安全移动性客户端在ASA
- AnyConnect在FTD的远程访问VPN配置
- FMC管理的FTD的最初的AnyConnect配置(视频)

关于全双工产品配置指南，下面请参阅。

完全配置指南

ASA ：

- ASA ASDM配置
- ASA CLI配置

FTD ：

- FDM管理的FTD
- FMC管理的FTD

IOS/IOS-XE ：

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

认证安装指南

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

性能和扩展问题

对于显著增加的RAVPN使用情况， AnyConnect用户可能遇到性能问题。请参阅以下确定如何识别这些问题和缓解策略寻址他们。

问题症状和识别

高 CPU 利用率

CPU利用率直接地影响VPN用户的性能。CPU利用率将增加当设备处理的加密的或解密的流量。设

备能体验高CPU，当平台接近能处理的最大数量VPN吞吐量时。确定是必要的高CPU利用率是否归结于的设备订购过量或归结于另一议题。

要检查设备是否体验高CPU，被建议运行以下命令：

非零show process CPU使用情况

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%
```

在上述示例中，注意到DATAPATH-0和DATAPATH-1消耗87.7%总CPU利用率。在这种情况下，ASA是订购过量的并且是必要确定此症状是否是由于的很多已加密和解密的流量。这可能然后被基准点在该平台的数据表描述的VPN吞吐量值。

要计算VPN流量通过设备的总量每秒，我们能添加***输入字节，***并且***输出字节***在***全局统计信息***部分内在***显示加密加速器***查找***statistics命令***。在ASA或FTD，请清除输出***显示***与clear命令***加密加速器统计信息的加密加速器统计信息***。等待一定数量的时刻，然后运行命令：如以下所显示，***显示加密加速器统计信息***：

```
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                             <----------------
[…]
```

采取一些个快照在特定间隔并且获得在可以转换到比特/秒的字节的平均的吞吐量(位/秒)。要执行此的公式是：

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

在前一个示例中， ***statistics命令***一个***清楚的加密加速器***发出在时间0秒。10几秒后， ***statistics命令显示的加密加速器***发出获得在10秒的粒的总字节。这些值然后用于计算处理一10秒的粒217Mbps的位/秒。多个快照可能是需要的获得一更加准确的平均值。

注意这些值为所有已加密/解密的流量(HTTPS、SSL、IPsec、SSH等等)将增加。我们能使用此值确定平均值VPN吞吐量和比较它到数据表。如果平均的吞吐量近似是相同数量，因为什么在数据表被看到为平台，设备由已加密和解密的流量过度预定。

另外，因为计数器不为VPN流量，增加此方法不可能用于确定在火力的VPN吞吐量2100平台。这在CSCvt46830被跟踪 。

最大VPN连接

当点击VPN连接时最大，用户可能体验他们不能连接的期限中断。虽然激活AnyConnect加上或尖顶许可证取消锁定VPN对等体最大，如果该最大数量被到达另外的用户不会允许在设备上。

要检查最大数量VPN连接可用在设备，请检查输出***显示vpn-sessiondb*** ：

```
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
----------------------------------------------------------------------------
```

要确定总计支持平台支持的相当数量用户，检查数据表您的下面查找的设备。

如果VPN用户不能连接，并且验证设备不点击VPN用户最大，请寻找从TAC的其他帮助。

数据表参考

以下数据表选定VPN用户最大平台支持的和最大数量根据测试的VPN吞吐量。IKEv2和DTL AnyConnect预计有相似的总(聚集的)吞吐量作为在每个部分列出的IPSec VPN吞吐量。

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

潜在的缓和

启用分割隧道

默认情况下，在ASA的组策略和FTD将实现tunnelall。这将发送在头端将处理的VPN的RA客户端生成的所有流量。因为数据包加密和解密与CPU利用率直接地涉及，确保仅必要的流量由VPN头端处理如允许由公司的安全策略是重要的。考虑使用分割隧道策略而不是全通道保存从多余的负载的VPN头端。

- ASA分割隧道指南
- FTD (FMC)分割隧道指南

注意：建立隧道所有实现公司范围内参数安全策略，而分割隧道依靠客户端设备帮助保护用户的互联网数据流。当使用时， Cisco提供附加安全性工具类似伞为了保护VPN用户分割隧道策略。

实现VPN负载均衡(仅ASA)

是提供两个或多个ASA能力共享VPN会话负载支持VPN负载均衡ASA平台的功能。如果两设备支持500 VPN对等体，通过配置在他们之间的VPN负载均衡，设备将支持在他们之间的总共1000 VPN对等体。此功能可以用于增加相当数量在单个设备之外的同时VPN用户能处理。可以找到关于VPN负载均衡的更多信息包括负载均衡算法此处：VPN负载均衡

配置优化

在平台启用的其它服务在设备将增加相当数量处理并且装载。例如， IPS， SSL解密、NAT等等。考虑配置设备作为只终止VPN会话的VPN集中器。

隧道协议选择

默认情况下，在ASA的组策略配置尝试设立DTL通道。如果UDP 443流量阻塞在VPN头端和AnyConnect客户端之间，自动地fallback对TLS。推荐使用DTL或IKEv2增加最大VPN吞吐量性能。DTL提供比TLS改善性能由于较少协议开销。IKEv2提供比TLS也改善吞吐量。另外，使用AES-GCM密码器可能轻微改进性能。这些密码器是可用的在TLS 1.2， DTL 1.2和IKEv2。

每个通道QoS (仅FTD强制执行)

QoS可以实现限制流量总量发送对出站方向的AnyConnect用户。通过该执行， VPN头端能强制执行每个远程访问客户端获得出口带宽其公平份额。可以找到关于此的更多信息此处：FTD配置

实现Crypto engine accelerator偏心(仅ASA)

Crypto engine accelerator偏心用于再分配crypto核心支持在其他的一份加密协议(SSL或IPsec)。如果多数VPN通道使用IPsec或SSL，此的目的是AnyConnect吞吐量的优化。实现此命令能导致服务中断和，因此维护窗口要求。另外，性能(AnyConnect吞吐量和CPU利用率)改进可能根据数据流配置文件变化。如果VPN头端只终止仅SSL会话或IPSec会话，此命令可以为VPN头端的进一步优化考虑。可以找到命令参考此处：命令参考

要查看当前crypto磁心存储区分配，请运行show crypto命令***加速器负载均衡***。此命令不显示设备有能力在处理上-的总量crypto利用率指示分配ssl或IPSec数据流比与每个核心。要查找大约数量在设备的利用率在**高CPU利用率**参考上面部分并且比较计算值对在数据表的值平台的。

在主要终止远程访问SSLVPN的ASA平台上，推荐crypto磁心存储区分配调节支持SSL于crypto命令***引擎加速器偏心ssl***。

以下示例显示在ASA5555的磁心存储区分配以***加密引擎加速器偏心ssl***命令支持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%
[..]
```

不管平台的当前crypto利用率，激活的会话分配永远将是100%。

Note:重新平衡密码的核心是可用的在以下平台：ASA 5585， 5580， 5545/5555， 4110， 4120， 4140， 4150， SM-24、SM-36、SM-44和ASASM。

FAQ

许可授权

问：为什么不能下载AnyConnect软件？

A：您必须采购AnyConnect加上或尖顶许可证为了能下载AnyConnect客户端。在此以后，应该标题名为您。如果没有尽管采购AnyConnect尖顶或正许可证标题名为，请开有权利的一个Case调整此问题。

问：为什么为在聪明的许可授权的帐户的AnyConnect许可证看到采购的99999 ？

A：这预计与某些AnyConnect许可证，例如AnyConnect加上永久或非被结合的AnyConnect加上或尖顶许可证。

问：什么确定，当“在使用中的”减少量？

A：此值减少，每当一个设备使用AnyConnect许可证注册。例如，如果注册FMC然后添加AnyConnect加上许可证到设备， AnyConnect的在使用中的值加上许可证将减少。此值不减少基于当前用户会话。注册ASAv设备不减少“在使用中的”计数。这是已知表面问题。您比采购授权用户的数量不能注册更多设备。

问：什么确定采购的值？

A：采购价取决于授权用户数量采购与许可证。例如， 25用户AnyConnect加上许可证将有25采购的计数。

问：如何启用强加密？

A：当创建注册标记时，为了启用强加密，您必须检查方框“在产品的Allow出口已控制功能注册与此标记”。

问：如何从PAK转换到许可授权的聪明？

A：应该打开一个案件与许可授权此的。

问：如果我有一个“X”用户许可证，什么将发生，如果"X+1"或更多用户连接到设备？

A：使用尖顶和加上许可证，设备的全双工VPN用户产能取消锁定。只要设备不达到其最大VPN用户限制，设备将继续接受连接。没有在设备的实施VPN用户会话的，并且它是基于的荣誉称号。如果设备的VPN会话使用需要增加，是您的责任采购另外的授权用户许可证。要检查设备支持的最大用户数，检查数据表或宣传单页在Cisco网站或运行的设备请***显示vpn-sessiondb***和检查“设备总VPN产能”。对于ASA，您能也运行***show version***或***显示vpn-sessiondb许可证摘要***命令。

问：如何能检查许可证在我的设备激活？

A：在FTDs，除非许可证激活，您不能部署AnyConnect配置。在ASA，您能检查***show version***或***显示vpn-sessiondb许可证摘要***检查多少个用户允许。没有一个激活的许可证，最大数量将是2个用户。关于ASA的注意，上述的命令不会显示加上/尖顶许可证信息。这跟踪与增强请求CSCuw74731。

配置

问： 能使用什么ASA平台VPN负载均衡？能否使用不同的ASA硬件平台或不同的软件版本在VPN负载均衡集群？

A： VPN负载均衡集群能的是包括不同的物理或虚拟ASA型号，包括ASAv。然而，通常推荐为了集群能是同类的。若不同软件版本用于VPN负载均衡集群，然后支持仅IPSec会话。请参考的详细信息： 指南和限制VPN负载均衡的。

问： 如何配置分割隧道？并且能从被建立隧道排除某种应用流量，例如办公室365，在独立的隧道配置里？

A：请参阅Cisco公共条款AnyConnect分割隧道关于多种使用案件配置示例。您能也使用切分通道和动态分割隧道的组合达到应用程序基于分割隧道。关于关于怎样的一示例优化办公室365和

WebEx的AnyConnect分割隧道，请参阅如何优化Microsoft Office365和Cisco WebEx连接的Anyconnect。

问：当连接对ASA与AnyConnect时的头端我看到错误“不信任证书警告”。这为何发生？

A：因为头端使用一自签名证书，这是可能的。要修复此， SSL证书在头端ASA可以从采购认证机关和安装。关于详细的实施步骤，请参考： 配置 ASA：SSL数字证书安装和续订。

问：Cisco RAVPN头端支持通配符证书？

A：与DNS附属的替代名称(SAN)支持是通配符和证书。

问： 单个设备能否使用负载均衡和故障切换？

A：活动/等待故障切换支持与VPN负载均衡。如果活动装置出故障，暂挂设备将立即接管没有影响到VPN通道。VPN负载均衡不支持与一个主动/主动故障切换配置。

监控

问： 能使用哪SNMP MIB监控ASA CPU使用情况？

A： CISCO-PROCESS-MIB可以用于监控ASA CPU使用情况。对于支持的MIB完整列表，请参考： 可适应安全工具MIB支持列表。并且得到支持的SNMP MIB和OIDs的列表特定ASA的，一个人能发出以下命令：***显示snmp-server oidlist。***

问：如何监控用户数量当前连接对VPN头端？

A：使用***显示***从CLI的***vpn-sessiondb***检查用户当前数量ASA或FTD的或者SNMP MIB

CISCO-REMOTE-ACCESS-MONITOR-MIB。

排除故障

问：我们的一些AnyConnect VPN用户似乎体验常见断开。我如何排除故障这样问题：

A：对于排除故障VPN断开和其他普通的AnyConnect问题，请参考： AnyConnect VPN客户端故障排除指南-常见问题。

问：当一定数量的用户连接对VPN头端时，没有其他用户不能连接。许可证在设备激活并且***显示vpn-sessiondb***显示设备能处理更多用户。什么能是问题？

A：检查VPN本地地址池那些用户确保，编号用户连接不超过可用相当数量的地址。您能验证与show ip local pool命令***[pool-name]***。在更旧的平台的另一潜在原因是***vpn-sessiondb MAX anyconnect高级版或精华限制***命令设置为低值。您能验证此与show run命令***所有vpn-sessiondb***。如果这是实际情形，值可以增加或命令可以删除防止此限制。

获得另外的帮助

对于其他帮助，请与TAC联系。有效支持合同将要求：思科全球支持联系方式

您能也访问Cisco VPN公共此处。

另外，您能检查TAC安全显示播客

参考资料

请在另外的链路之下一般来说请找出对其他资源有用的为AnyConnect部署和COVOD-19相关问题处理。

- Cisco安全在远程工作者响应增加- Cisco公共
- AnyConnect订购指南
- AnyConnect许可授权FAQ
- AnyConnect VPN、ASA和FTD FAQ安全远程工作者的