

【专家问答】问题汇总_配置、故障排除和最佳实践:

ASA 和 FTD 上的 AnyConnect 远程访问 VPN

感谢大家参与本期“[配置、故障排除和最佳实践: ASA 和 FTD 上的 AnyConnect 远程访问 VPN](#)”专家问答活动, 此次活动收到许多思科用户的提问, 同时也十分感谢我们的专家热心参与和解答。以下为本期在线答疑的部分问题及回复, 以供大家参考:

问答专家:



Dinesh Moudgil

思科安全团队High Touch Technical Support (HTTS) 工程师

6年以上经验, 专注于思科下一代防火墙, 入侵防御系统, 身份管理和访问控制 (AAA) 和VPN。他拥有CCNP, CCDP和CCIE # 58881认证, 以及多个供应商认证, 例如ACE, PCNSE和VCP。



Pulkit Saxena

思科安全团队High Touch Technical Support (HTTS) 工程师

7年行业经验, 具有多种防火墙, 不同的VPN解决方案, AAA和下一代IPS的实践经验, 多种培训课程讲师。Pulkit拥有Cisco和Juniper (CCIE Security和JNCIA) 等多家供应商的认证。



Jason Grudier

北卡罗来纳州罗利市VPN TAC团队的技术负责人

六年Cisco VPN团队工作经验, 之前是LabCorp的网络工程师。主要负责所有思科平台上的AnyConnect故障排除和配置, 以及DMVPN, GETVPN, Radius, LDAP和证书身份验证。



Gustavo Medina

Systems Sales Engineer, ENT 销售团队

10多年安全和企业网络方面的经验。他专注于不同的任务, 从技术升级和合作伙伴adoption到修订Cisco认证评估。Gustavo在安全方面拥有CCNA, CCNP CCSI和CCIE (# 51487) 证书。

【问题一】

❏ 请问用户互联网电脑使用 VPN 时候, 如何确保用户的电脑的威胁不影响到服务端

▲ 我们可以执行一些登录前检查, 以确保客户端计算机受信任并可以连接。

可能的选项是 posturing, DAP, CSD 主机扫描。 查看以下帮助链接:

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-firewalls/200238-ASA-VPN-posture-with-CSD-DAP-and-AnyCon.html>

<https://community.cisco.com/t5/security-documents/how-to-configure-posture-with-anyconnect-compliance->

[module-and/ta-p/3647768](https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_module-and/ta-p/3647768)

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/configure-posture.html

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/asdm78/vpn/asdm-78-vpn-config/vpn-asdm-dap.html>

一旦用户根据上述检查确认连接成功并符合要求，我们理想地认为它是受信任的用户。此外，我们只能允许相关流量进入 ASA 或使用 split tunnel 选项通过隧道传输的所有流量：

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100936-asa8x-split-tunnel-anyconnect-config.html>

除此之外，如果用户发送过多的流量或连接后连接不完整，则将根据问题进行特定的故障排除。但是，您提到的主要问题可以通过我提到的登录前检查来解决。

A 您好，除了 Pulkit 提到的那些以外，一些公司使用 Always-On 来阻止计算机不在受信任的网络上时访问 Internet 资源，除非 VPN 会话处于活动状态。在这种情况下强制将 VPN 始终打开会保护计算机免受安全威胁。

对于不强制执行永远在线的公司，除了已经提到的 posture 检查和 DUO 之类的 2FA（以确保仅授权人员使用 VPN），我们还必须为远程用户增加额外的保护，因为威胁参与者正在利用这种“无保护的远程工作者”增加的情形、发起不同的运动。您可以阅读我们的 TALOS 博客以获取更多信息：

<https://blog.talosintelligence.com/2020/03/covid-19-pandemic-threats.html>

通过 Cisco Umbrella 即使用户没有在 DNS 层连接到 VPN，也可以保护用户免受恶意 Internet 目的地的攻击。

由于它是从云中交付的，因此，Umbrella 可以在几分钟之内轻松保护所有地方的用户。

另外，我们的最后一道防线是 Cisco Advanced Malware Protection (AMP) for Endpoints。这一技术可以防止入侵并在入口点阻止恶意软件，并在高级威胁逃避防御前沿时检测，遏制和补救高级威胁。

【问题二】

Q 现在 firepower 看产品手册，ssl vpn 的吞吐量看哪个参考值？TIs？

A 请确认您要查找 SSL VPN 吞吐量详细信息的硬件以及所参考的文档。

【问题三】

● 您好，您能否确认我们应使用哪种方法来生成 csr，并将其上传到 FTD 防火墙以进行 Anyconnect 用户身份验证。

Objects>PKI>Cert Enrollment or using Open SSL?

谢谢。

▲ 我相信您正在寻找根据 SSL 握手强制执行的服务器身份验证，因此当 anyconnect 用户连接时，FTD 需要出示其证书，最终客户端将根据其受信任的 CA 列表进行检查。

这是一个可以帮助您进行配置链接：

<https://www.cisco.com/c/en/us/support/docs/network-management/remote-access/212424-anyconnect-remote-access-vpn-configurati.html>

为了回答您的问题，我们可以选择任何一种方法，在 FTD 上生成 CSR，或使用开放 SSL，对于第二种方法，一旦准备好，我们就可以导入完整的 PKCS12。

现在，如果您正在寻找使用证书的用户身份验证，FTD 仅需要在其数据库中具有 CA 证书，而无需用户证书。

希望这会有所帮助。

● 就我而言，我正在寻找域用户的证书身份验证，从个人设备连接的任何人都不应获得 VPN 访问权限。只有公司机器应该能够连接到 VPN

如果我只是将内部 CA 服务器的 ROOT CA 证书导入到 FTD 中，则必须在客户端安装哪个证书？有没有为用户创建证书时必须使用的任何特定证书的模板？

谢谢

▲ 那么您的要求是同时使用正确的证书进行客户端身份验证。您只需要在 FTD 上拥有客户端的根 CA 证书即可。

客户端需要在进行 SSL 协商时将其 ID 证书提供给 FTD，并且 FTD 应该具有相同的 CA 证书。

● 我们的网络中没有实现针对端点的 AMP，但是如果我仍然想将 AMP 与 anyconnect VPN 一起使用，我应该拥有哪些许可证，现在我们有 AnyConnect apex 许可证，并使用 FTD 实现了 AnyConnect，并且一切正常

想知道有什么“带有 AMP 的 Anyconnect”的选择？

▲ AMP4E 基于您要保护的端点数量。除了 Anyconnect 许可证，您还需要 AMP4E 许可证。对于部署，您可以使用 AnyConnect AMP 启动器，该启动器用作为端点部署高级恶意软件保护（AMP）的介质。它将 AMP for Endpoints 软件从企业内部托管的服务器推送到端点的子集，并将 AMP 服务安装到其现有用户群。

这是订购指南。

<https://www.cisco.com/c/dam/en/us/products/collateral/security/fireamp-endpoints/guide-c07-740737.pdf>

AMP4E 最近已添加到我们的 COVID-19 保证远程工作安全的 offer 中，您可以在这里阅读：

<https://blogs.cisco.com/security/expanding-free-security-offers-into-customers-endpoints>

有了这一新功能，现有客户可以超出其设备限制两倍，以支持增加远程工作人员。要利用此优惠，他们只需在其他设备上安装 AMP for Endpoints 连接器，就无需采取其他措施。与我们的 AnyConnect, Umbrella 和 Duo 优惠一样，此优惠有效期至 2020 年 7 月 1 日

● 大家好，我有另一个问题

就我而言，我们将 cisco FTD 作为外围防火墙

我们要创建 anyconnect 远程访问 VPN

但是我们不想使用外部接口 IP 终止我们的 anyconnect VPN，当我们获得 Internet 连接时，我们获得了 / 28 子网，我们有一个免费的公共 IP 地址，我想使用它来终止 VPN。

您能否指导我如何使用 Cisco FTD 达到此要求

▲ 您当然可以这样做，您将使用新 IP 设置第二个接口并像往常一样配置 anyconnect。只要该 IP 地址可以从客户端访问，并且 ISP 将流量转发到 FTD 设备，它就应该可以正常工作。

● 由于我有一个互联网连接，如果我设置第二个接口并配置 IP 地址，我应该在哪里连接另一端？

我不能再将一个接口连接到 provider，对吗？

我不了解您的解决方案，能否请您更具体些，让我知道我该怎么做

▲ Jason 在其较早的回复中的意思是，您可以配置另一个接口，您可以在其中使用 / 28 子网并在其上终止 RA-VPN。正如您提到的，您不想在现有外部链接上配置 RA-VPN 一样，这很容易理解。

现在，关于路由和连接性，逻辑保持不变，我们需要将新接口连接到上行链路，最终用户可以通过该接口实现连接性/可达性。

希望这可以说明。

【问题四】

● 各位专家，感谢主持这次问答环节，我现在列出一些想到的问题，感谢解答：

1. 您能描述将 ISE posture profile 集成到 FTD 中的过程吗？我对 ASA 熟悉，但是尚未尝试使用 FTD（通过 FMC 管理）

2. 在 FTD 中启用 sysopt 连接许可-vpn 的利弊是什么？两种情况下推荐的最佳做法是什么？（我知道没有 sysopt 连接许可-vpn，则所有访问都需要通过 ACP 进行调节）

3. FTD 和 ASA 一样支持 CoA 吗？与 ISE posture 特别相关的问题

4. 在 FMC 中是否内置了 Anyconnect 配置文件编辑器？如果不是首选？Anyconnect 独立编辑器还是 ISE 配置文件编辑器？

5. 您可以提供一个示例来自动完成通过 FMC 管理的 FTD 的配置推送吗？当前，我们在 ASA 中有一些带有参数的脚本，并且我们对配置进行了标准化，但是在 FTD 中，因为除了 Flexconfig 例外之外没有其他选项可以

访问 CLI，所以我认为使用 API 对象调用是必要的，只是我想有一个初始示例

6. (这更多是关于 FTD / FMC 的一般性问题) 为了快速解决 ASA 中的访问问题，我们使用 ASDM 快速了解正在处理的流量，在 FMC 中，我知道因为某些原因连接事件无法提供相同级别的信息：一个是连接事件的延迟，以及多位故障排除工程师在 FMC 上的负载，如果我没记错的话，连接事件也来自 snort 处理后端，因此接口 ACL 拒绝通过 syslog，因此连接事件可能无法提供所需的信息水平：什么是在 ACL 接口放置和 DPI 放置之间快速分析 ACP 规则的访问日志的最佳实践？

真的谢谢大家。

PS: 为了不混淆，您可以参考答案以及问题编号。

A 您好，以下是对您问题的回复：

1.这是您可以参考的文档，了解 FTD 上 ISE posture 所需的流程和配置步骤

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-access.html>

2. 当我们不想通过访问控制策略检查 VPN 通信时，建议使用为解密的通信选择“绕过访问控制策略”的选项。因此，流量将仅被转发到目的地，而无需 FTD 的任何深入检查。是否启用此功能，取决于您的安全要求以及对远程访问 VPN 用户的信任级别。如果您不信任来自远程访问 VPN 用户的流量，建议对它们产生的流量进行深度检查。

作为记录，默认情况下在 FTD 上禁用此命令，而在 ASA 上默认启用。

请注意，从 AAA 服务器下载的 VPN 过滤器 ACL 和授权 ACL 仍适用于 VPN 流量。

取消选中“针对解密流量的绕过访问控制策略 (sysopt permit-vpn)”的用例是，是否要允许 Anyconnect 用户流量的掉头操作，使其能够通过 FTD 访问 Internet 或访问内部资源。禁用此功能后，将执行 ACP 检查，您可以利用 URL 过滤等功能来限制 Anyconnect 用户启动的流量。

3.是的，从 6.3.0 版本开始，FTD 确实支持 RADIUS CoA，并且较新版本完全支持。

4.您可以使用 AnyConnect 配置文件编辑器创建 AnyConnect 客户端配置文件。该编辑器是基于 GUI 的配置工具，可作为 AnyConnect 软件包的一部分使用。它是您在 Firepower 管理中心之外运行的独立程序。

有关 AnyConnect 配置文件编辑器的详细信息，请参阅：

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/anyconnect-profile-editor.html

5.您可以利用 API Explorer，因为它为 REST API 提供了有限的接口，并提供了 REST API 功能的视图。

https://<management_center_IP_or_name>:<https_port>/api/api-explorer

Ref:

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/api/REST/Firepower_Management_Center_REST_API_Quick_Start_Guide_623/About_the_API_Explorer.html#concept_oq2_fg1_ccb

以下是一些链接，可帮助您开始使用 FMC API 编程 Firepower

<https://blogs.cisco.com/security/how-to-get-started-on-programming-firepower-using-fmc-apis>

https://www.cisco.com/c/en/us/td/docs/security/firepower/623/api/REST/Firepower_Management_Center_REST_API_Quick_Start_Guide_623/Objects_in_the_REST_API.html#concept_xh5_lt3_bcb

以下是一些非思科链接可能会有所帮助：

<https://www.youtube.com/watch?v=a2DNeRxnnkA>

<https://www.youtube.com/watch?v=iTfmLk3kwdg>

6. TAC 主要使用 CLI 和 FMC GUI 一起对与 ACP 规则有关的问题进行故障排除。

您可以在 LINA CLI 上使用数据包捕获选项，类似于在传统 ASA 上使用的数据包捕获选项。

要么

您可以使用 FTD clish 下的“系统支持防火墙引擎调试”来确认是否根据正确的访问控制规则对流量进行了评估。

这是供您参考的文档：<https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw/212474-working-with-firepower-threat-defense-f.html#anc13>

【问题五】

- 首先，感谢组织这个活动，我个人是间接地收集了很多信息，并且我确实将这一讨论加入了书签，我相信它很长一段时间将成为我的十大书签之一：)

问题：

我们将 SBL (登录前启动) 模块用于远程工作者，因为所有这些工作者都是从本地继承的，而 Windows 中的工作站均没有缓存的凭据。

一切工作正常，但是即使代理在任何连接中都具有配置文件，他们也可以在 Windows 登录屏幕上选择它们，但最终他们在 AnyConnect 中都具有配置文件的通用 FQDN 和配置文件名称。

这给我们的用户造成了一些混乱，如果他们出于任何原因必须重新连接，配置文件名称以及 FQDN 已经列出，但我还没有找到防止这种情况的方法。

是否可以阻止 FQDN 在 anyconnect 中被列出，可能只有配置文件名称 (profile name) ？

A 谢谢你的支持。

您可以共享您看到配置文件名称和 FQDN 的屏幕快照吗？

A 听起来您可能已在 preferences.xml 文件中启用了缓存。 但是请确保，如果转到 ProgramData / cisco / cisco 安全移动客户端/配置文件并打开已配置的 profilename.xml 文件，请发送用以开头的 bottom portion。 请修改那部分内容，因为这适合在所有地方公开 public。 如果主机地址和主机名相同，则它们会相应地对其进行修改以保持相同。

```
secret.cisco.com
secret.cisco.com
Would become
blah.blah.com
blah.blah.com
```

因此，我们知道它是相同的值。 如果不同，则只需将它们随机修改即可。

还有一个字段，允许用户在此框中输入。

```
true
```

如果将其设置为 false，则用户将无法修改 xml 配置文件填充的内容。

如果启用了缓存，并且他们在 FQDN 中输入用户名，而不是从 xml 概要文件中选择 HostName，则当他们下次连接时，它将显示最后的连接和 HostName。

在此文件夹中，您会看到一个 preferences.xml 文件夹，您可以在其中禁用缓存

C:\Users\%AppData%\Local\Cisco\Cisco AnyConnect Secure Mobility Client

最后，个人档案文件夹中是否有多个 profile.xml 文件？如果您这样做，它将在用户的 anyconnect 登录框中填充多个条目。

🔍 感谢两位专家。 以下根据您的要求为您提供的更多信息：

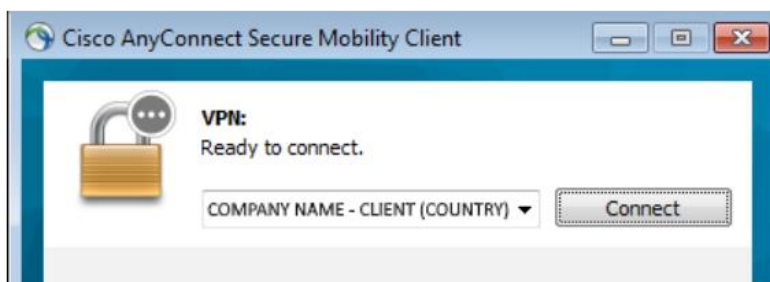
这是样本 XML 配置文件的底部：

```
<ServerList>
    <HostEntry>
        <HostName>COMPANY NAME - CLIENT (COUNTRY)</HostName>
        <HostAddress>https://vpn.company.com</HostAddress>
        <UserGroup>emea_client</UserGroup>
    </HostEntry>
</ServerList>
```

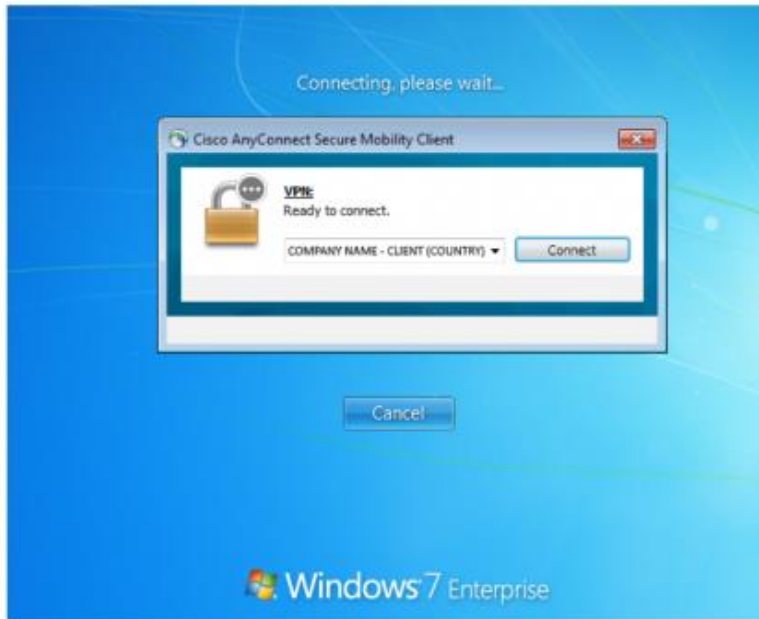
我们的主机名（显示为配置文件名称）与主机地址不同。

用户体验如下：

- 当用户已经在 Windows 中登录并选择配置文件名称并连接时，一切将按预期进行



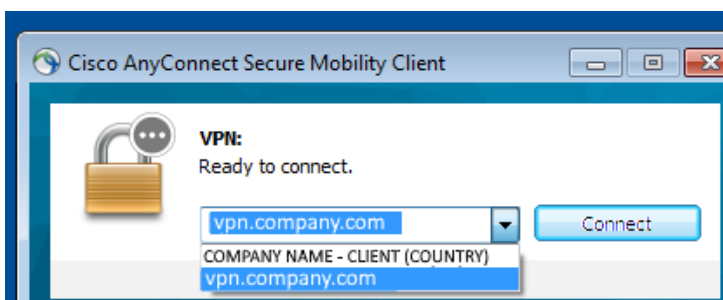
- 当改用 SBL 时, 远程工作人员将首先通过 SBL 屏幕进行连接, 选择配置文件, 但是在登录 Windows 时, 他们看到的是 FQDN, 而不再是所选的配置文件。



直到现在, 即使存在这种视觉故障, 但用户仍可以连接到应有的位置。

如果用户以某种方式断开连接并需要在登录 Windows 时重新连接, 则会出现问题, 在这种情况下, 代理将看到常规的配置文件名称以及正确指向我们的防火墙但不包含配置文件完整 URL 的 FQDN。因此它显然不允许任何连接。

在这种情况下, 视觉故障可能是一个问题, 因为如果人们需要选择配置文件名称或在配置文件列表中未正确显示的 FQDN, 就会感到困惑:)



我希望这能为您提供有关我们的设置以及正在发生的一切所需的所有信息。

PS: 所有这些屏幕截图均已从我们的内部信息中清除, 但取自我自己进行的实时测试。

A 看起来好像是因为以下 bug:

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvp53403>

您可以针对该问题跟踪该 bug。

Q 谢谢, 这似乎正是我们所发生的情况。

您知道是否存在没有此问题的 anyconnect 版本吗?

到目前为止,

version 4.7.04056 受影响

version 4.8.03036 受影响

A 目前, 该漏洞处于分配状态, 并且计划在以后的版本中对其进行修复。

Q 再次问好,

首先抱歉, 这是一个与 Cisco ISE 有交叉引用的问题。

如果我们需要根据来源国限制远程访问用户, 我知道以下几点:

Firepower 具有地理定位提要 (Geolocation feed), 并且可以基于它们创建 ACP 规则, 但不能用于终止在防火墙处终止的流量 (就像 RA VPN 一样)

用作 RADIUS 后端身份验证的 Cisco ISE 可以在身份验证/授权规则中使用 Tunnel-Client-Endpoint 属性, 该属性将提供连接客户端使用的公共 IP

据我所知, 思科 ISE 没有任何地理位置数据 feed

基于这些考虑,我正在考虑稍后导出 Firepower 地理位置 IP 列表,并通过 REST API 将条件对象构建到 Cisco ISE 中,然后如果 Tunnel-Client-Endpoint 落入允许访问的特定国家/地区对象,则进行匹配。

现在我的问题如下:

是否可以通过 REST API 从 FMC 导出地理位置 IP 数据?

是否可以通过某种方式在 ISE 中创建条件,使 IP 位于对象中列出的子网之中? (我相信没有办法)

ISE 或 Firepower 上的路线图中是否具有此类功能?

谢谢!

- A** 1. 您可以从 FMC 上以下目录“ / var / sf / geodb”中的文件“ ipv4_country_code_map”和“ ipv6_country_code_map”中获取映射信息。

```
root@fmcv66:/var/sf/geodb# cat ipv4_country_code_map
and
root@fmcv66:/var/sf/geodb# cat ipv6_country_code_map
```

这将产生带有 IP 和相关国家代码的输出。有关国家/地区代码的更多信息,请访问

https://en.wikipedia.org/wiki/List_of_ISO_3166_country_codes

如果您想从 FMC 知道国家/地区代码,则可以以 root 用户身份在 FMC 上运行以下 perl 命令:

```
root@fmcv66:/var/sf/geodb# perl -MFlyLoader -e 'my $t="country_code_continent_code_map";my
@c=("country_name","country_code");my $n=0;my $s=""x20;foreach my $row
(@{SF::SFDBI::connect()->selectall_arrayref("SELECT ".join(", ", @c)." from $t WHERE
country_code=242"))){print "$s ".++$n.". $s\n";my $i=0; foreach (@{$row}){printf "%9s: %s\n",@c[$i++],$_}'
```

```
***** 1. *****
```

```
country_name: fiji
```

```
country_code: 242
```

```
root@fmcv66:/var/sf/geodb#
```

我们还可以用以下 API 来检索地理位置对象:

GET geolocation

Request Type: GET

Description: Retrieves the geolocation object associated with the specified ID. If no ID is specified, retrieves list of all geolocation objects.

URL: /api/fmc_config/v1/domain/{domain_UUID}/object/geolocations

URL for GET by ID: /api/fmc_config/v1/domain/{domain_UUID}/object/geolocations/{object_UUID}

对于第 2 和第 3 个问题，我决不是 ISE 方面的专家，但它通常根据诸如属性或身份组而不是列表之类的条件进行检查。暂时不支持此功能，但是如果信息有任何更改，我将更新该这个回复贴。

👉 感谢您的支持，我会随时关注您的更新。

这可能解决了一个大问题，目前我已经看到第三方身份验证提供程序基于地理位置返回失败条件，但是在当前状态下，并非每个远程访问解决方案都可以针对此类提供程序进行身份验证，因此对 Firepower 或 ISE 的最好是开箱即用。(it would be good to have it out of the box for either Firepower or ISE)

👉 请注意，如果您使用 Duo MFA（基于 FTD 的远程访问 VPN 支持）并且有 Access 或 Beyond 计划，则可以基于用户地理位置来实施 Duo 策略。例如，您可以禁止您所在国家/地区的所有访问。您还可以使其更细化-例如，一般在禁止出差或居住在国外的特定用户的情况下做出这样的禁止。

👉 如果将 DUO 代理与 ISE 一起使用，或者将其与直接从 FTD 进行 SAML 身份验证的 DUO 一起使用，该方法是否可行？

👉 大家好，

ISE 本身不提供此类服务，但是您可以与 MDM 集成（Meraki Systems Manager 可以使用）以提供此服务。

从 FTD 本身，您可以配置控制平面 ACL 来阻止不需要的 blocks。您可以通过 @Dinesh Moudgil 指出的方式

从 FMC 获取此信息，从 cisco.com 上的 geo 软件包本身，从第三方资源或使用 ANSIBLE（我更倾向于这个）：

<https://developer.cisco.com/site/ftd-ansible/#!/country/country>

绝对是@Marvin Rhoads 所指的选项，使用 DUO 是我的首选方法。 您可以使用 DUO 代理来做到这一点，如
此处所述：

<https://duo.com/docs/ciscoise-radius>

<https://duo.com/docs/cisco#cisco-ise-using-radius>

但这对于 SAML 也是可行的，虽然没有得到充分的记录，但此视频说明了所有这些内容：

<https://youtu.be/W6bE2GTU0ls>

📍 感谢各位专家的建议。

@Marvin Rhoads: 一旦获得一些空闲时间 (!)，我将立即探索 DUO 选项，并最终使其与我们使用的另一个
MFA provider 同时工作，您知道地理定位是否可以使用免费许可证进行测试吗？

@Gustavo Medina @Dinesh Moudgil: 我喜欢建议的所有选项，对我而言最即时的现在看起来像是在具有
地理位置的 FTD 中使用控制平面 ACL，我对此选项有疑问：

1. 据我所知，control-plane ACL 可以通过 flexconfig 使用，并且过去存在一些问题，我想这些问题已经解
决，思科是否支持这种配置？

2. 如果是 FTD 中的 control-plane ACL，是否可以直接使用 SI 中的地理位置对象，还是必须创建和更新
“LINA”对象才能与 Flexconfig 一起使用？

3. 在这种情况下，我可以仅将此 ACL 应用于一个隧道组吗？据我所知，这将适用于该防火墙的所有入站远程
访问，所以这意味着我们将限制连接到该防火墙的任何人？

4. 如果问题 3 的答案是“是”（禁止所有连接用户使用 FW），那么 FTD 6.6 的 VRF-lite 新功能是否派上用场并
创建多个接口，并将

control-plane

ACL 附加到特定的“受限外部”

"restricted outside"

？

在写这些问题时，我开始觉得 control-plane ACL 在身份验证级别上的可扩展性不如地理位置，但我希望您对此表示赞同。

A 请确保使用此修复程序运行版本

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvn78593>

2. 将需要使用 LINA 对象。

3. 这是一般规则。每个隧道组不特定。

4. 应该可以，我已经测试过将策略应用于特定的 VRF，是可以的，但是我没有测试这种特殊的控制平面场景。

如果它不起作用，那么我们将需要提交 Bug。多实例

Multi-instance

也应该起作用。

我确实更喜欢对基于地理的规则使用 DUO，因为它更易于管理，但绝对不是唯一的选择。另一个选择是分开功能，并在 FTD 后面为 RA VPN 连接提供专用的 ASA，在其中您可以对此即时访问流量应用基于地理位置的规则。

A DUO 免费试用将为您提供有限的功能：

<https://duo.com/trial>

如果您与经销商联系，那是一个更好的选择。他们可以为启用所有功能的合格客户安排 Duo Proof of Value。

Q 我相信我遇到了一个非常奇怪的 Bug：

我正在 KVM 中的 FTDv 上测试远程访问部署，奇怪的是部署持续失败，并且很长时间才给出报错：由于配置错误导致部署失败...

现在来看 bash 中的 FTD：

```
tail -f / ngfw / var / log / messages
```

我注意到 anyconnect 软件包的副本有所进展，但是一旦达到 70%-72%，它就会停止并且不会继续进行部署

```
Apr 13 01:57:36 FTD-1 SF-IMS[9624]: [9624] sftunnel:control_services [INFO] FSTREAM_STATUS: Sending back task status 'Processing'
```

```
Apr 13 01:57:37 FTD-1 SF-IMS[9624]: [9624] sftunnel:stream_file [INFO] task_id=6
```

```
Apr 13 01:57:37 FTD-1 SF-IMS[9624]: [9624] sftunnel:stream_file [INFO] peer=a1f1e77e-44e0-11e9-a967-39f0b3b399ab
```

```
Apr 13 01:57:37 FTD-1 SF-IMS[9624]: [9624] sftunnel:stream_file [INFO] ELASTIC_FSTREAM status: curr_read=32385024, curr_write=32385024, total_bytes=46197839, stream_id_src=0, stream_id_dest=6, seq_id_src=4518, seq_id_dest=4518, state =Processing, started:2020 04 13 01:51:55 UTC, expires:2020 04 13 01:58:38 UTC
```

```
Apr 13 01:57:37 FTD-1 SF-IMS[9624]: [9624] sftunnel:stream_file [INFO] ELASTIC_FSTREAM status:: File copy 70 % completed, 32385024 bytes of file copied out of 46197839
```

我很惊讶，因为我有足够的带宽，并且复制非常快，直到停止为止，而我们正在谈论的文件少于 50 MB，而不是 500 MB。

有没有一种方法可以像使用 FTD 更新程序包一样手动复制 bash 中的 anyconnect 程序包？

我注意到 Anyconnect 软件包的复制路径位于此文件夹中：

```
/ngfw/var/cisco/deploy/pkg/var/cisco/packages/lina/domain/AnyConnect Image/111/
```

所以我只是通过 wget 从那里下载了软件包，然后再次启动了策略推送，确实花了一些时间，但是副本始终为 0%，然后继续处理其余的策略，感谢上帝：)

有机会手动上传这些软件包会更容易吗？我认为可以通过 REST api 使用 FDM，但不能使用 FMC 受管设备吗？

PS: 是否为此提交了 Bug？

A 在共享该片段之前，您是否看到 cgroups 进程终止了该进程？

当某个进程消耗的内存超过了规定的内存时，cgroups 进程将检测到这种情况并终止该进程。当进程终止时，依赖于该进程的功能可能会失败。

您为 FMCv 分配了多少内存？

这些是要求:

https://www.cisco.com/c/en/us/td/docs/security/firepower/quick_start/fmcfv/fpmc-virtual/fpmc-virtual-vmware.html#id_82840

- 我正在使用物理 FMC2500，版本 6.5.0.4。我觉得容量不该成问题。

我共享的日志来自在 KVM 中虚拟化的 FTD。

FTD 具有 4 个 vCPU 和 8GB RAM，目前服务器仅在运行此 VM，作为测试 FTD 映像。

FTD 的版本是 6.5.0（尚未安装修补程序）。

关于 cgroups，说实话我没有注意到，但是我将尝试再次上传另一个图像，所以我希望有类似的行为。

cgroup 会将日志消息放入 FMC 或 FTD 吗？任何特定的日志文件或常规消息？

- 我们有一个物理 FMC2500，我正在评估在 VMware ESX 中使用 FTDv 的选项。

我知道使用 ASA v 需要购买吞吐量许可证，FTDv 是否有类似要求？

据我所知，在我们的案例中，最低要求是

- 部署 FTDv 映像
- VMware ESX 中的硬件要求以启动映像
- FMC 上的可用性（因为它是硬件 FMC2500，所以不需要其他许可证）
- 我们的智能帐户中可用的 Anyconnect 许可证，用于连接的用户数

考虑到我们已经有的 ESX 硬件，FMC 和我们将要购买的 anyconnect 许可证，没有多余的额外费用，对吗？

万一我们应该，那么添加

- IPS 和安全智能/地理位置威胁许可证
- 通过传输中的 AMP 进行分析的恶意软件
- 网址过滤条件下的网址

提前致谢!

A 要回答您的问题，没有像 ASA 中所需的 FTDv 吞吐量许可证这样的要求。

是的，您提到的所有步骤都足以在虚拟环境中设置 FTDv。

另外，如果您需要其他功能，例如购买了特定许可证的许可证，则可以安装它们。

【问题六】

Q 我想附加一个脚本，该脚本将更新通过 VPN 连接的计算机的 DNS 条目。

(这将使远程连接更容易，以便为用户提供远程帮助)。

我想将此脚本添加到在 FTD 上创建的 Annyconnect 组（我们不使用 ASDM，而只是在 ASA 5xxx 系列上使用 Firepower instance）。

我找不到任何有关将 FTD 上的脚本添加到 AnyConnect 配置文件的文档。

能告诉我是否可能吗？

Q 嗨 Piotr，我觉得您的问题很有趣，所以我也想加入到讨论中来

我们目前正在防火墙上使用地址池，因为它们比通过内部 DHCP 服务器分配 IP 效率更高，但是缺点是 DNS 服务器的主机名到 IP 映射可能不正确，因为它仅在 Active Directory 上中继登录映射。

现在我正在考虑从内部服务器使用 DHCP，因为我们使用的是 Active Directory 集成的 DHCP，它还应该更

新特定主机的 A 记录, 我只是担心除非 DHCP 租约很短, 否则这可能无效(假设是 30 分钟, 每 15 分钟更新一次), 那么我的意思是 2 件事

A) DHCP 服务器成为单点故障, 或至少对基础结构至关重要 (由于租期短)

B) 大多数用户同时连接, 这意味着短的 DHCP 租约将或多或少地在同一时间产生相当多的流量 (例如, 并发连接的 1000 个用户平均每 15 分钟同时产生 500 (!) 个 dhcp 更新, 对 30 分钟的 DHCP lease!)

所以我想问一下, 问题:

1) 是否可以使用地址池但更新 DNS 服务器?

2) 是否可以将防火墙内部 DHCP 服务器用于远程访问 lease, 如果可以, 则使用 lease 信息更新 DNS 服务器?

3) 为 500-1000 个 (或更多) 平均并发用户使用 DHCP 服务器并保持较短的 DHCP 租用期是否合理且可持续?

如果是, 那将减轻 Piotr 看到的问题, 以及如何最好地解决这一问题?

A 到目前为止, 由于连接脚本不支持任何自定义, 因此在连接到由 FMC 或 FDM 管理的 FTD 设备的 AnyConnect 上不支持登录脚本。

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/firepower_threat_defense_remote_access_vpns.html

连接到 FTD 安全网关时, 不支持以下 AnyConnect 功能:

安全移动性, 网络访问管理以及所有其他核心 VPN 功能和 VPN 客户端配置文件以外的其他 AnyConnect 模块及其配置文件。

Posture

变体, 例如 Hostscan 和 Endpoint 姿

Posture

评估, 以及基于客户端

Posture

的任何动态访问策略。

AnyConnect 自定义和本地化支持。FTD 设备不会配置或部署这些“为这些功能配置 AnyConnect 所需的”文件。

A hi, 各位,

如@jgrudier 所述, 我们尚不支持自定义。这是 6.8 的路线图, 但是不支持将脚本推送到客户端。如果您修改 XML 配置文件, 并将其与 OnConnect 脚本一起推到客户端, 则它将起作用。您可以按照 AC 管理指南对功能进行一般性了解:

https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect48/administration/guide/b_AnyConnect_Administrator_Guide_4-8/customize-localize-anyconnect.html#ID-1408-00000396

@ giovanni.augusto, 关于 DHCP 的 DNS 更新, 它的工作方式是 ASA / FTD 通过 DHCP 传递主机名 (不是 FQDN, [这是 FQDN 的 ENH](#)), 其他一切取决于 DHCP 服务器, 以及它如何与 DDNS 环境通信。

可以做的是使 Windows 客户端直接与 DDNS 服务器通信以进行注册。

【问题七】

- 我想问一下如何允许用户通过 Skype 进行业务交流, 或者在 ASA 上通过 cisco jabber Anyconnect 远程访问 VPN 进行语音交流, 下面建议从安全性角度考虑是否可以做到安全? 以及如何通过我们的 SIEM 解决方案监控内部通信?

输入 same-security-traffic 命令以使 FW 成为 HUB。而且, 您需要为 nat (外部, 外部) 配置一个 nat 规则, 以使池地址空间能够相互访问。

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

Please note that this command allows traffic to enter and exit the same interface, which is disabled by default for security.

```
nat(outside,outside) source static "address pool obj" "address pool obj" dest static "address pool obj" "address pool obj" no-proxy-arp – route-lookup
```

And be place towards the top of your nat rules.

- ▲ 这是在 ASA 上设置发夹以允许 AnyConnect 客户端与其他 AnyConnect 客户端通信的唯一方法。我不会认为这是一个巨大的安全威胁，但这完全取决于您公司的需求，只有您才能做出这些决定。

从命令参考: <https://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/S/cmdref3/s1.html>

same-security-traffic intra-interface 命令允许流量进入和退出同一接口，通常不允许这样做。此功能对于进入接口但随后路由到同一接口的 VPN 流量可能很有用。在这种情况下，VPN 流量可能未加密，或者可能已为另一个 VPN 连接重新加密。例如，如果您有一个集线器和分支 VPN 网络，而 ASA 是集线器，而远程 VPN 网络是一个分支，则要使一个分支与另一个分支进行通信，流量必须先进入 ASA，然后再传到另一个分支。

same-security-traffic intra-interface 命令所允许的所有流量仍受防火墙规则的约束。注意不要造成不对称的路由情况，该情况可能导致回程流量无法穿越 ASA。

您正在尝试通过 SIEM 解决方案 监控的是什么？

- ▲ 几点评论:

- 您提到的“nat (outside , outside) for the pool address space to reach each other”仅在 Stick 上已经存在用于公共 Internet 的 NAT 时才需要。如果使用拆分隧道，则不需要这样做。
<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html#anc10>
- 如果使用拆分隧道，则不需要手动 NAT 即可进行双向通信，除非存在影响该流量配置的 NAT 规则。但是，Anyconnect VPN 池必须包含在拆分隧道 ACL 中。
<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html#anc14>
- 从安全角度考虑，同一个安全流量的内部接口应该不是大问题，因为流量仍将遵循 FW 规则，但是您当然总是希望为 DUO, Umbrella 和/或 AMP4E 类似的远程用户提供额外的保护。

- 您绝对可以像处理其他流量一样，在 SIEM 上监视这些通信。为了更好地了解您的远程用户在做什么，您可以使用 Stealthwatch Enterprise 或 Stealthwatch Cloud，如以下视频所示：
<https://cs.co/SWC-RemoteMonitoring>
<https://cs.co/SWE-RemoteMonitoring>

*我们甚至可以通过 Tetration 达到工作负载/应用粒度 (workload/app granularity)，但这是另外的话题了：)

【问题八】

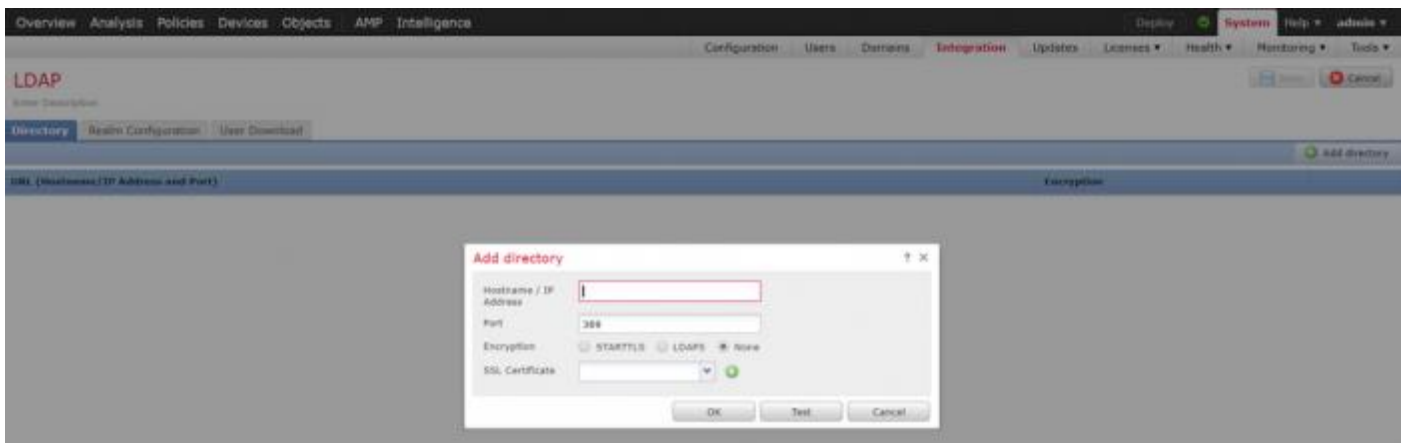
- 我通过 FMC 在 FTD 上使用领域配置远程 VPN。当我尝试与 AnyConnect 连接时，出现错误“登录错误”。

以下是 ldap 255 和 webvpn anyconnect 127 的调试输出：

```
ldap_client_server_add: Add server:0.0.0.0, group=4
ldap_client_server_unlock: Free server:0.0.0.0, group=4
[12] Session Start
[12] New request Session, context 0x00002b5de5d453b0, reqType = Authentication
[12] Fiber started
[12] Failed to convert ip address 0.0.0.0
[12] Fiber exit Tx=0 bytes Rx=0 bytes, status=-3
[12] Session End
```

感谢您的帮助

- ▲ 设置领域时，您是否在此处使用 FQDN 或 IP 地址：

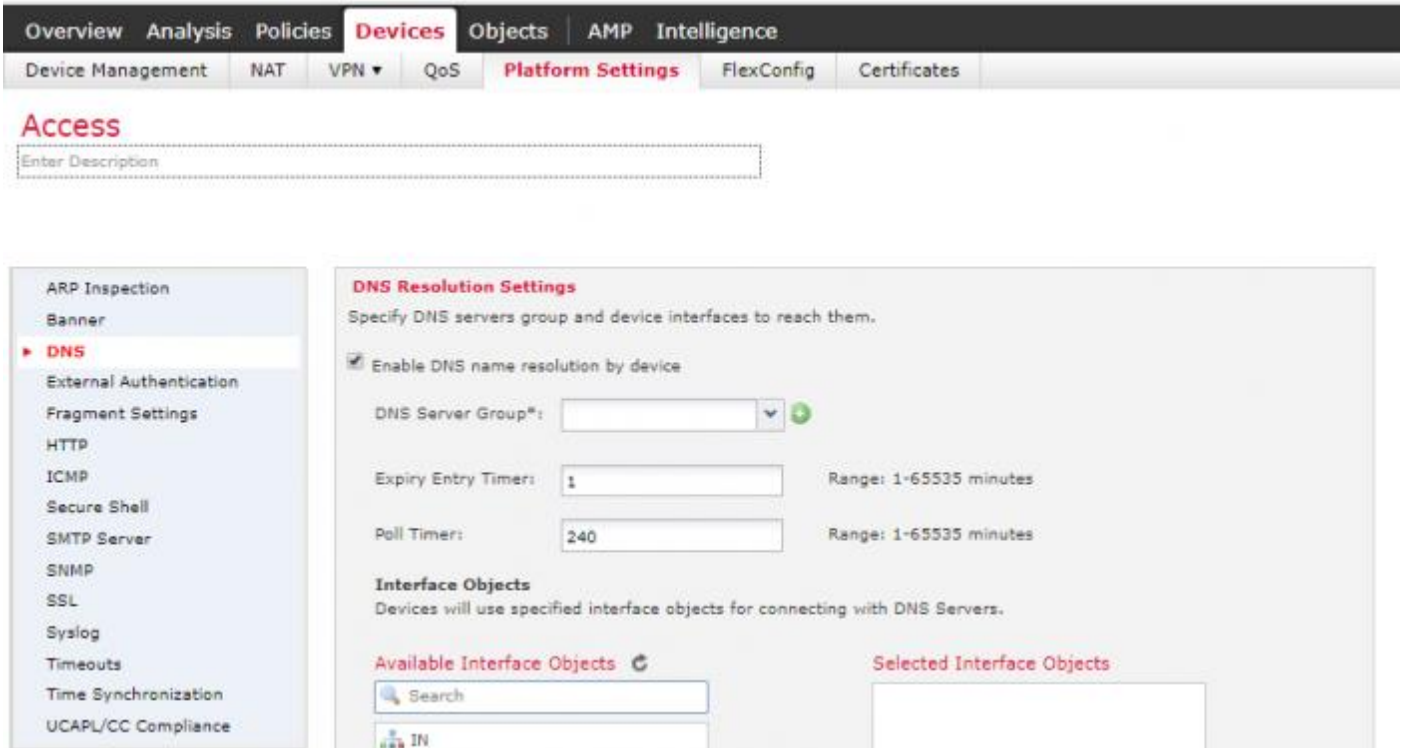


- 您好，jgrudier，感谢回复。

我使用 LDAP。 如果我没记错的话，我只能用 LDAP 配置 FQDN。

A 对的。 我认为在 FTD 上未正确设置 DNS 可能存在问题。

您是否在这里设置了 DNS:



Q 多谢，是我的错。不过现在，我遇到新的报错：

```
[19] Session Start
```

```
[19] New request Session, context 0x00002b5de5d453b0, reqType = Authentication
```

```
[19] Fiber started
```

```
[19] Creating LDAP context with uri=ldaps://172.25.YY.XX:636
```

```
[19] Connect to LDAP server: ldaps://172.25.YY.XX:636, status = Failed
```

```
[19] Unable to read rootDSE. Can't contact LDAP server.
```

```
[19] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
```

```
[19] Session End
```

```
ldap_client_server_add: Add server:172.25.YY.XX, group=4
```

```
ldap_client_server_unlock: Free server:172.25.YY.XX, group=4
```

```
#telnet 172.25.YY.XX 636
```

```
Trying172.25.YY.XX...
```

```
Connected to172.25.YY.XX.
```

```
Escape character is '^'].
```

这是 debug 和 ldaps config 的输出：

```
[27] Session Start
[27] New request Session, context 0x00002b5de5d453b0, reqType = Authentication
[27] Fiber started
[27] Creating LDAP context with uri=ldaps://172.25.XX.YY:636
[27] Connect to LDAP server: ldaps://172.25.XX.YY:636, status = Failed
[27] Unable to read rootDSE. Can't contact LDAP server.
[27] Fiber exit Tx=0 bytes Rx=0 bytes, status=-2
[27] Session End
ldap_client_server_add: Add server:172.25.XX.YY, group=4
ldap_client_server_unlock: Free server:172.25.XX.YY, group=4
telnet 172.25.XX.YY 636
Trying 172.25.XX.YY...
Connected to 172.25.XX.YY.
Escape character is '^]'.
^C
```

```
aaa-server srv protocol ldap
max-failed-attempts 4
realm-id 3
aaa-server srv-dc host srv-dc
server-port 636
ldap-base-dn DC=name,DC=local
ldap-group-base-dn DC=name,DC=local
ldap-scope subtree
ldap-naming-attribute samaccountname
ldap-login-password *****
ldap-login-dn user@name.local
ldap-over-ssl enable
server-type microsoft
```

A 作为测试，如果您转回 LDAP 而不是 LDAPS，是否成功？您是否已将证书验证为有效证书，并且 LDAP 服务器已接受该证书？

Q 我从来没有使用过 ldap。现在从 ASA 迁移到 FTD。在 ASA 上，ldaps 效果很好。

在系统/集成/领域中，状态为 i.O。我可以看到用户组

FirePower 管理中心具有根 CA 证书。我应该在 FTD 上安装证书吗？

A FTD 设备是否具有来自 LDAP 服务器的根 CA 证书和子 CA 证书作为受信任的 CA？

Q FTD 设备仅具有自签名证书。根 CA 证书仅具有 FirePower 管理中心。我试图在设备/证书中添加根 CA，但看不到证书。

A 我认为您最好开一个 TAC Case, 这时我需要开始研究证书和其他特定配置。

Q 感谢您的回复, 我昨天开 Case 了, 目前还没有解决。

A 我将与您的工程师一起探讨此案。

关于证书安装问题。请在大约 5 分钟后开始观看此处的视频。我完成了在 FTD 上安装证书所需的步骤。我认为问题可能出在您最初安装的 CA 而不是最终签署您的身份证书的 CA。

<https://community.cisco.com/t5/security-videos/initial-anyconnect-configuration-for-ftd-managed-by-fmc/ba-p/4057295>

【问题九】

Q 大家好, 希望有人能提供一些帮助的信息。

我有一个在 context mode 下运行的 ASA 5585-SSP-10, 版本 9.8 (2)。

我们有一个客户想要配置动态拆分隧道。但是, 我们无法完成配置, 如以下部分所示:

Remote Access VPN > Network (Client) Access > Group Policies > [policy name] > Advanced > AnyConnect Client

我们需要将客户属性分配给该组策略, 但是自定义属性选项在 ASDM (7.8 (2)) 上不可用。

我阅读了以下文章, 说需要最低 AC 4.5 和最低 ASA 9.0, 我们的 AC 为 4.7。

因此, 不确定在 context mode 下运行 5585 时是否有特定的东西会对此产生影响? 有没有人见过这个?

<https://community.cisco.com/t5/security-documents/anyconnect-split-tunneling-local-lan-access-split-tunneling/ta-p/4050866#toc-hId-744656474>

A 这是被支持的, 不应丢失。应该在最新的 ASDM 中可用。

如果您现在无法升级, 则也可以通过 CLI 进行配置:

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/vpn/asa-98-vpn-config/vpn-params.html>

❓ 因此，我们需要升级到最新的 ASDM 吗？如果我没记错的话，那是 7.13？

从 CLI，我似乎也没有动态拆分选项：

我唯一的选择是在所附图像上。

❗ 7.14.1 是最新版本：<https://software.cisco.com/download/home/283123066/type/280775064/release/7.14.1>

从您附加的图像中，您可以看到第二个选项：“anyconnect-custom”

但是首先，您需要在 webvpn 下配置属性，请参阅以下 3 个步骤：

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/vpn/asa-98-vpn-config/vpn-params.html>

【问题十】

❓ 单个 SSL VPN 客户端是否有预期的最大吞吐量？我有几位客户越来越多地使用他们以前使用较少的 SSL VPN（终止于 ASA 和 FTD 前端），并且有几位客户报告说，尽管前端配置合理，但性能却很差。

例如，一个客户端具有 Firepower 2110，具有 800 Mbps 的 Internet 带宽和光利用率。内部客户端的 Speedtest.net 报告速度接近 800 Mbps。但是一个 SSL VPN 客户端（具有完整的隧道）只能达到 30-40 Mbps。当该客户端不在 VPN（家庭网络，有线连接）上时，它们报告接近其 ISP 发布的下载速率（200 Mbps）。

我意识到在复杂的系统中有许多变量在起作用。但我正在寻找“最佳情况”的实验室编号，可以作为预期的最大实验室编号。我想我们可以使用 iPerf 或相关工具来做类似的事情。

❗ 你好，Marvin，以下是一些关键点：

1. 请使用 AnyConnect 4.7.x 或更高版本，因为我们解决了一些缓冲区和硬件加速问题，

2.使用 DTLS v1.2 或 IKEv2, 因为它们将带来更高的性能。 *不要*仅将 TLS 用作传输协议, 因为这会导致性能降低/较差。

注意: DTLS 1.2 支持在 ASA 版本 9.10.x 及更高版本中引入。 先前的 ASA 版本不支持 DTLS 1.2。 因此, 为了避免 [Bug CSCvp07143](#) = DTLS 1.2 and AnyConnect oMTU, 需要以下最低版本的 ASA:

- 9.10(1)22 or higher - latest 9.10.x version recommended

- 9.10(2)1 or higher - latest 9.12.x version recommended

3.根据使用的前端硬件和/或客户特定的 ASA / FPR 环境, 应审查和/或修改有关“加密引擎加速器偏向”(crypto engine accelerator-bias)的配置 (如果适用)。 考虑到正在使用 DTLSv1.2 或 IKEv2 的主要传输协议, 请应用最适合客户环境/配置的适当偏差设置。 在您的特定情况下, 使用 2100 时不需要这样做, 但可以使用下表作为以后的参考:

Platform	FTD Default	FTD User Configurable	ASA Default	ASA User Configurable	Other Variations
FPR9300 SM24,SM36,SM48	Balanced	Through Flex-Config, but marginal improvement	Balanced	Available	SSL/IPSEC
FPR41x0	Balanced	Through Flex-Config, but marginal improvement	Balanced	Available	SSL/IPSEC
FPR1000, FPR2100, FRP41x5, FPR9300 SM40, SM44, SM56	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable
ASA 5545-X & 5555-X	IPSec	Available	IPSec	Available	Balanced/SSL
ASA5506,5508,5516,5525-X	Not Applicable	Not Applicable	Not Applicable	Not Applicable	Not Applicable

4. Cipher Suite: 理想情况下, AES-GCM 将提供最佳性能结果。

5.组策略上的 MTU 配置: 理想情况下, 越高越好, 不要超过 1406。 建议值是 1406 (最低“开始”于 1406, 仅根据客户环境而降低)

6.必须在 ASA /组策略上配置/启用 AnyConnect TunnelOptimizations 自定义属性:

```
webvpn          anyconnect-custom-attr TunnelOptimizationsEnabled description Tunnel Optimizations
Enabled
```

```
anyconnect-custom-data TunnelOptimizationsEnabled False false
anyconnect-custom-data TunnelOptimizationsEnabled True true

group-policy <Group Policy Name> attributes
  anyconnect-custom TunnelOptimizationsEnabled value True
```

综上所述，在我的实验室设置中，我已经能够从单个客户端获得 200Mbps 的带宽。

👤 感谢 Gustavo Medina， 很有帮助。

1. 您提到的 Bug 错误已链接到内部 CDETS 网站，但我公开看到了该错误

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvp07143>

2. 我认为 FTD SSL VPN 客户端不支持 DTLS 1.2，直到我们升级到 FTD 6.6 (昨天才发布)。我确实看到有问题的 ASA 上使用的是 9.12 (3.9) 和 AnyConnect 4.8.03036。因此，客户端因此与 DTLS 1.2 隧道连接，我们看到它们的性能有所提高。

3. 是否通过 FMC 上的 Flexconfig 支持与托管的 FTD 设备一起使用的 AnyConnect 隧道优化？

👤 正确。6.6 引入了允许配置 DTLS v1.2 协议的功能

FDM-仅 REST API

FMC GUI 配置支持

*不支持不受硬件加密芯片支持的平台 (表示 5508 和 5516)

是的，您可以将 Flexconfig 用于这些自定义属性。类似于此处的动态拆分记录方式。

https://www.cisco.com/c/en/us/td/docs/security/firepower/config_examples/advanced-anyconnect-ftd-fmc/advanced-anyconnect-vpn-ftd-fmc.html#Cisco_Task_in_List_GUI.dita_8ea84895-b580-4900-9d4f-99a9c5557d3c

👤 谢谢-“ TunnelOptimizationsEnabled”大大提高了 ASA 上 SSL VPN 客户端的速度。

我还能够通过 FlexConfig 部署到 FTD 6.4.0.8 设备。但这似乎并没有帮助提高速度-我怀疑我们正在达到 DTLS 1.0 施加的部分上限。

除了最近的 TAC 文章建议我们使用它之外，我找不到关于此设置的太多文档：

<https://www.cisco.com/c/en/us/td/docs/security/asa/misc/anyconnect-faq/anyconnect-faq.html>

还有其他我漏掉的原始资料吗？

顺便说一下，此 ENH 错误应在 Firepower 6.6 版本中标记为已修复：

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvr51516>

A 我将记录一个 DOC 错误，以将其包含在配置指南，命令参考和 Anyconnect 管理指南中。

默认情况下，Anyconnect 4.9 将启用它。

我还将致力于将 CSCvr51516 移至正确的状态。

【问题十一】

Q 有与 RA VPN 相关的 Cisco ASA 版本的任何推荐吗？

A 在 CCO 上发布了某些推荐的 ASA OS 版本。您可以导航到以下链接，以查看 5585-X 防火墙的建议发行版

<https://software.cisco.com/download/home/283123066/type/280775065/release/9.8.4%20Interim>

A 当前的开发建议：

- 9.8 (4.latest) 适用于需要寿命的保守 CU。
- 需要特征速度的客户为 9.12 (2.latest)。

这些是 cisco.com 上当前已加星标的版本。推荐的发布基于遥测 (telemetry)，因此我们需要一些时间来部署最新版本。一旦我们从实际安装和正在运行的安装中收集了反馈，我们就会根据事实 (客户发现的缺陷，TAC 案例，升级等) 做出明智的决策。

【问题十二】

Q 大家好，感谢安排这个专家问答活动，很多有用的信息。

有时我们仍然无法为新用户分发任何连接的配置文件，以解决 12 秒身份验证超时问题。这是一个问题，因为我们的用户仍然可以选择将电话或回复短信用作其两因素“two-factor”验证方法。另外，我们关闭了无客户端 SSL，但允许用户通过此门户从防火墙登录并下载最新的客户端。

我的问题是，即使我们关闭了无客户端 VPN，我仍可以以某种方式将默认的 VPN 配置文件附加到此客户端下载中吗？

A 没有实用的方法可以通过无客户端连接将 xml 文件与下载内容一起推送出。如果用户由于超时而出现连接问题，则推送出此 xml 配置文件的最佳方法是，如果可以的话，使用 GPO 推送出该 xml 配置文件。另外，您可以只创建一个单独的隧道组，该隧道组仅具有用户/通过登录名 (user/pass login)，用户可以用来下载修改后的配置文件。然后，可以在修改超时后将它们映射到正确的隧道组和组策略。

A 一旦您的用户下载 Anyconnect 客户端，他们第一次连接时便会下载配置文件。像您这样的部署有不同的选择：

- 拥有基本的连接配置文件，而无需两步验证，也无法访问内部。这仅供用户下载配置文件。
- 使用 GPO 或类似方法将配置文件分发给您的用户到正确的位置（用户已经安装了客户端）。
- 使用 pre-deployment 选项并使用您自己的配置文件构建您的自定义 .MSI 程序包，然后分发该程序包，以使用户安装后即可使用该配置文件。

【问题十三】

Q 是否可以通过 FMC 在 FTD 上配置 Web VPN SSL ？

A 由 FMC 或 FDM 管理的 FTD 设备上没有无客户端 VPN 的选项。唯一的选择是门户，它将允许您下载客户端。

【问题十四】

Q 您好，请问下对于 FirePower 的 FTD 版本来说，是否已经不支持 l2tp over ipsec vpn 的功能呢？有的时候，客户的一些安全需求，导致客户电脑没有权限安装 anyconnect 的客户端，但是他们又需要通过外网访问，在 Firepower 上是否有功能代替呢？

A 目前，我们不支持 FTD 上基于 IPSEC 的 L2TP。

备用选项是使用 anyconnect。让我检查一下即将发布的版本中是否有任何添加 L2TP 的计划，我将进行更新。

更新如下：

我也与产品团队核实过，目前在即将发布的 firepower 版本中，我们也没有添加 L2TP 的路线图。

因此，anyconnect 客户端是必经之路。

【问题十五】

Q AnyConnect 远程访问 VPN 可以部署在 ASA 上吗？有相关的 configuration guid 吗？

A 您好，是的，ASA 支持远程访问 VPN。参考链接：

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa99/asav/quick-start/asav-quick/asav-config.html#97965>

配置与任何其他 ASA 平台相同，但请确保您具有适当的 VPN 许可证来部署 Anyconnect VPN。

配置示例：

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100936-asa8x-split-tunnel-anyconnect-config.html>

Smart licensing on ASA:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa910/configuration/general/asa-910-general-config/intro-license-smart.html#task_03242D29B58D4DB9B95F4F844973CE2E

【问题十六】

Q 如何将数据包跟踪器 (packet-tracer) 与 RA VPN vpn 过滤器一起使用。

假设 10.10.10.10 是 vpn 地址 & 内部地址是 192.168.10.3 什么是 packet-tracer 的语法

外部的 packet-tracer 输入会导致外部接口访问列表匹配吗？

A 在 9.9 (1) 之后，我们将解密选项添加到 Packet-tracer 中，还可以模拟通过 VPN 隧道的数据包。模拟的“解密”数据包将与现有的 VPN 隧道匹配，并将应用关联的隧道策略。

对于您的示例，语法为：

```
packet-tracer input outside tcp 10.10.10.10 5050 192.168.10.3 decrypted
```

运行上述命令时，应建立隧道，否则将收到警告。

Q 有与 RA VPN 相关的 Cisco ASA 版本的任何推荐吗？

A 在 CCO 上发布了某些推荐的 ASA OS 版本。您可以导航到以下链接，以查看 5585-X 防火墙的建议发行版。
<https://software.cisco.com/download/home/283123066/type/280775065/release/9.8.4%20Interim>

A 当前的开发建议：

9.8 (4.latest) 适用于需要更长使用寿命的保守 CU。

9.12 (2.latest) 适用于需要使用速度的客户

这些是 cisco.com 上当前已加星标的版本。推荐的发布基于 telemetry，因此我们需要一些时间来部署最新版本。一旦我们从实际安装和正在运行的安装中收集了反馈，我们就会根据事实（客户发现的缺陷，TAC 案例，升级等）做出明智的决策。

【问题十七】

Q 您好专家们,

我们最近在印度的两个位置购买了 Cisco FTD 2110 和 1010, FMC 位于 limerick, 三个都与站点到站点 VPN 连接。 远程访问正在使用 radius serve 在 limerick 中工作。 当我们尝试通过在 Limrick 中对 Radius 服务器进行身份验证来通过远程访问连接印度位置时, 它说身份验证失败。 故障排除时可以看到, 我们可以从印度本地计算机 ping radius serve , 但无法从 FTd 1010 到达。

期待解决方案, 谢谢

A 我需要您阐明通过站点到站点的所有三个连接的确切含义。 与 FMC 一样, 您可以在管理中心设备中为其他两个 FTD 进行站点到站点的配置。 这是我的理解, 如果您还有其他意思, 请告诉我。

现在, 当您说远程访问在 Limerick 中可以正常工作时, 这意味着远程访问 FMC 本身可以正常工作。

当您尝试访问印度位置时, 我相信您的意思是 anyconnect 连接而不是设备访问, 并且 anyconnect 连接失败, 错误为“身份验证失败”。

首先, 请验证在有问题的 FTD 上是否正确配置了 aaa 服务器, 然后我们可以通过以下命令从 CLI 中进行检查:

针对特定用户“test aaa server”, 以查看我们是否可以从 FTD 正常访问 AAA 服务器

Q 我的 FMC, Radius 服务器位于 Limerick。 一架 FTD 2110 位于钦奈, 一架 FTD 1010 位于班加罗尔。 所有 3 个都与站点互连到 Site VPN, 并且我只能通过本地 IP (Limerick IP 地址) 访问 FMC。

当我检查时, 尝试从 bangalore FTD CLI 连接 AAA 身份验证。

```
firepower# test aaa-server authentication BSB_RadiusServer host 192.168.0.198
Username: Gururajan.s
Password: *****
INFO: Attempting Authentication test to IP address (192.168.0.198) (timeout: 32
ERROR: Authentication Server not responding: No response from server
```

但是从班加罗尔本地 PC, 我可以通过 ping 到达 Radius 服务器 192.168.0.198, 但是当我从 FTD CLI 尝试时, 它无法连接.

FTD 无法到达 AAA 服务器 (Limerick), 因为它通过站点连接到站点 VPN, 而我无法从班加罗尔进行连接。

A Hello, @Gururajansrinivasan32898

FTD 将进行路由查找以到达 Radius 服务器, 结果将是可以通过配置 L2L VPN 的外部接口访问。VPN 很可能只定义了 Limerick, Chennai 和 Bangalore 的子网, 因此, 当 RA 客户端连接到 Chennai 和 Bangalore 时, 那些 FTD 将尝试到达 Radius 服务器, 以从其外部 IP 来获取流量。

您需要做的是在

VPN interesting traffic

中包含 Chennai 和 Bangalore 的外部 IP。在 Limerick 上, 确保从 Radius 服务器到 Chennai 和 Bangalore IP

的 NAT

exemption

到位。

A Hi @Gururajansrinivasan32898, 像 Gustavo 指出的那样, 我们需要修改 VPN 的相关流量, 其中包括 Chennai 和 Bangalore 的外部接口 IP。

这是因为这些 FTD 背后的本地用户能够访问 AAA 服务器, 因为这是相关 VPN traffic 的一部分。

【问题十八】

Q 大家好。

首先, 非常感谢您这样做。你们好棒 :)。

我有几个问题。我们运行 FTD 2140 (运行 FTD 映像并连接到 FMC) 生成了 csr。我是在 FTD 上做的。

```
openssl genrsa -out FTD1.key 2048
openssl req -new -key FTD1.key -out FTD1.csr
```

以上这些命令输出已提交给我们的公共 CA。而且我有一个 root.ca, identity ca 和.pem 文件。现在如何在 FTD 中使用身份证书？

当我发出此命令时，我得到错误提示

```
openssl pkcs12 -export -out FTD1.pfx -inkey FTD1.key -in FTD1.cer -certfile Root.cer
```

A 我进行了快速测试，以下命令在 FTD 上对我有用

```
openssl pkcs12 -export -out FTD1.pfx -inkey FTD1.key -in FTD1.cer
```

请注意，我使用了 CA 签署的 ID 证书的“Base 64 encoded”格式。

您能否确认尝试创建.pfx 证书时遇到什么错误以及 ID 证书的格式是什么？

Q 我收到了这个报错，我也不知道哪里错了。

```
FTD1:~$ openssl pkcs12 -export -out FTD1.pfx -inkey FTD1.key -in FTD1.cer -certfile Root.cer  
No certificate matches private key
```

我重新看了一下：

```
-FTD1:~$ cat FTD1.crt  
-----BEGIN CERTIFICATE-----  
MIIFJjCCAaw4CCQCdyDsSbw5UITANBgkqhkiG9w0BAQsFADBVMQswCQYDVQQGEwJH
```

```
FTD1:~$ cat FTD1.key  
-----BEGIN RSA PRIVATE KEY-----  
MIIEowIBAAKCAQEA1v91avgdvjcer+kznBdjRUGmXbqkwINZI+sV5rMK52OgSUET
```

```
FTD1:~$ cat FTD1.csr  
-----BEGIN CERTIFICATE REQUEST-----  
MIICuzCCAaMCAQAwdjELMAkGA1UEBhMCR0lxEzARBgNVBAgMCkxhbmNhc2hpcmUx
```

A 似乎您在命令中使用的私钥与您要导入的证书没有关联。

您能否检查命令中是否调用了正确的文件？

您不一定需要在 FTD 上生成此类 CSR。它可以在任何其他支持 OpenSSL 的设备上生成。

我做了一个包含 CA 证书的测试，该测试也适用于 FTD:

```
openssl pkcs12-导出-out FTD2.pfx -inkey FTD1.key -in FTD1.cer -certfile CA.cer
```

可能不同的变量是我使用的是.cer 扩展名和 Base 64 编码

🕒 您能否推荐一些链接来了解这一点。

说到 openssl 我是新手，我正在学习。

🔴 以下链接有助您理解 OpenSSL 和它的使用:

<https://www.digialocean.com/community/tutorials/openssl-essentials-working-with-ssl-certificates-private-keys-and-csrs>

https://wiki.openssl.org/index.php/Command_Line_Uilities

<https://www.freecodecamp.org/news/openssl-command-cheatsheet-b441be1e8c4a/>

<https://www.sslshopper.com/article-most-common-openssl-commands.html>

【问题十九】

🕒 大家好,

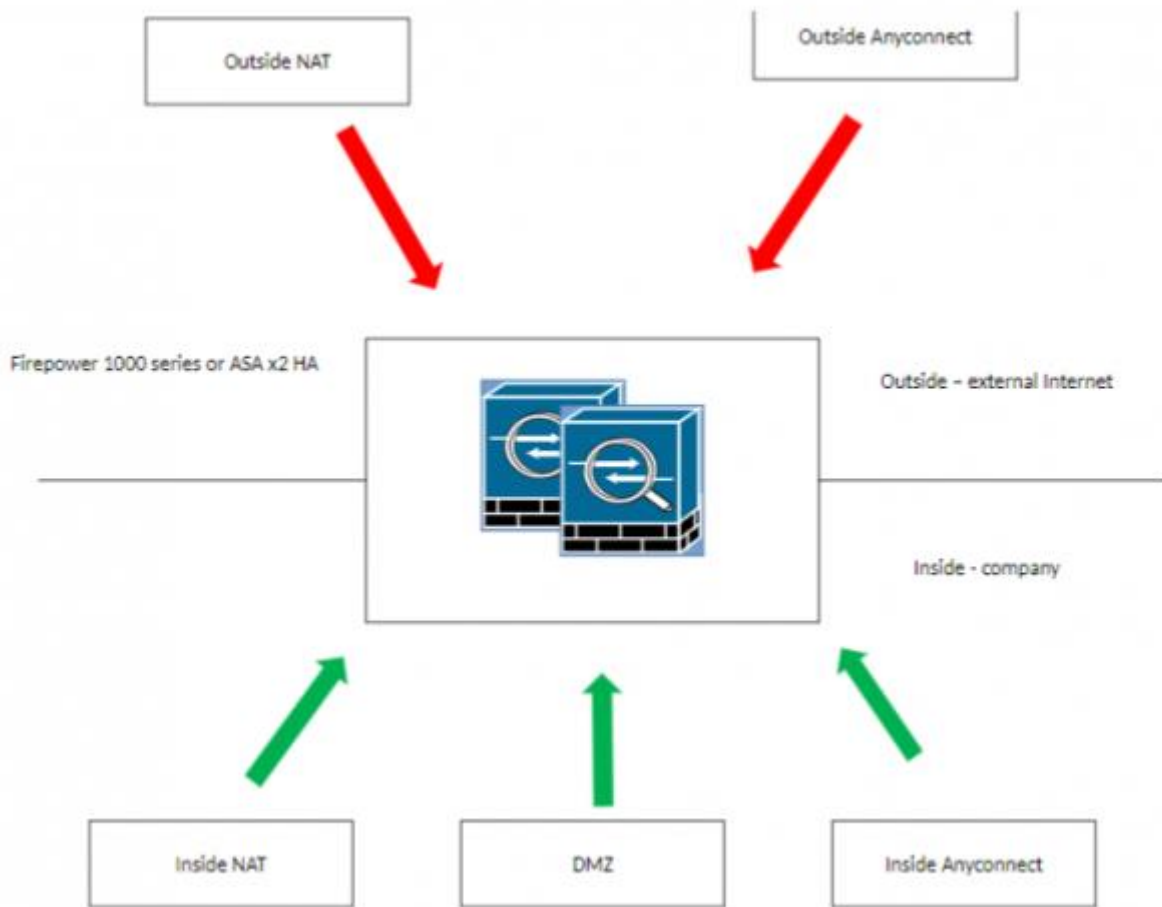
我在有关网络安全性的主题中问了这个问题，但是我将在这里重复。

我最近与一位同事讨论了下一个计划的可能实施方案。 HA 中有两个设备，例如两个 asa 5508-x 或两个 firepower1140。是否可以在与 NAT 和 DMZ 以及在同一对设备上配置的 anyconnect 的网络上实现？

如果是，在这种情况下正确的方法是配置两个外部接口，一个用于 NAT (例如， outside_nat)，第二个用于 anyconnect 的外部接口 (例如， outside_anyconnect)，或者为同一接口配置所有内容 (例如， 外部) ...

如果考虑第一种方法，则在 HA 中配置两个设备，配置端口通道，并将其分为 5 个 subs-outside_nat, inside_nat, DMZ, outside_anyconnect 和 inside_anyconnect。但是在这种情况下，问题出在外部接口上

有两条路由—是否可以在 asa 或 firepower 上配置两条默认路由？



A 您好，绝对有可能。最常见的情况是使用单个接口处理所有事务，对于具有双 ISP 冗余功能的客户，辅助接口不会传递任何流量，如果主链路断开，则辅助接口将接管并处理所有流量。

但是，我们确实有 CU 不想让辅助双 ISP 处于空闲状态，因此它们平衡了流量。正如您在 ASA 上所提到的，我们不能使用同一度量标准来使用多个路由。很久以前，实现此目标的唯一方法是使用 NAT 技巧，但是由于我们在 9.4.1 中引入了 PBR，因此非常容易实现。

特别是在 Anyconnect 的情况下，我们还有 CU 可以按您的意愿进行操作。具有专用接口，这不是 Anyconnect 用户的默认接口，这样他们就不会占用主链路带宽。它的工作原理是，您只需添加具有较高度量的辅助默认路由，然后在该辅助接口上配置 Anyconnect。当 Anyconnect 连接到达该接口时，ASA 或 FTD 将能够使用该辅助路由进行答复，因为它是即装即用的连接。

建立 Anyconnect 连接后，将使用正确的下一跳安装该连接的主机路由。

注意事项：

- 运行以下修复的代码
https://bst.cloudapps.cisco.com/bugsearch/bug/CSCun65747/?reffering_site=dumpcr
- 确保在该接口上未配置 RPF。

*虽然不确定图中的 anyconnect-inside 接口的用例是什么。如果您想扩展我可以提供帮助。

【问题二十】

❓ 进入生产网络之前，ASA 的最佳或理想配置是什么？

👉 在将设备投入生产之前，可能需要检查很多事情，并且这取决于多种因素，从防火墙的防护到最佳实践。

我建议您检查以下链接，然后让我们知道您是否有任何特定的查询：

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/200150-Cisco-Guide-to-Harden-Cisco-ASA-Firewall.html>
https://tools.cisco.com/security/center/resources/firewall_best_practices

【问题二十一】

❓ 非 Cisco 用户可以在登录时向非 VPN 用户交付非 Cisco 软件吗？我正在寻找一种将 Azure MFA 客户端交付给最终用户的方法。如果无法交付该软件，则是否有一种方法可以显示一条消息，要求用户不进行操作？

👉 无法从第三方交付任何东西。它只能推送任何连接模块，自定义项和 xml 配置文件。您可以修改登录标语以告诉他们下载文件，但那不需要用户交互。此外，您可以创建一个登录脚本，该脚本将在用户连接时启动，因此，如果您可以创建一个可以运行并下载程序的脚本，则可以从 ASA 而不是由 FMC 或 FDM 管理的 FTD 进行操作。

【问题二十二】

Q 我们已经配置并正在测试客户端.xml，其中已启用 FIPS 合规性，并且看起来工作正常。然后，有人问“您怎么知道它正在工作？”除了每次审计员希望查看.xml 之外，我还有其他地方可以验证是否符合 FIPS 法规吗？

A 您可以检查客户端 UI 的 VPN 统计信息。有一个 FIPS 部分。

【问题二十三】

Q 设置了 AnyConnect，并且我想为防恶意软件配置 DAP，以防病毒。

我正在通过 ASDM 进行配置。

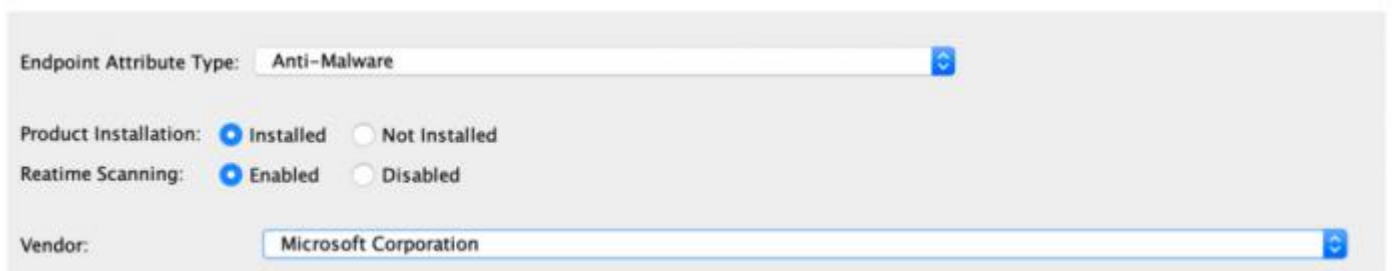
我的问题有没有一种方法可以添加防病毒列表，而不是一次添加一个列表？

允许客户使用 BYOD 的客户端防病毒软件太多了，手动添加所有内容将既耗时又效率低下？

先谢过了。请指教。

A 有两种方法可以解决此问题。

1.您可以根据 Vendor 执行检查，而不是对每个 AV 进行检查。



Endpoint Attribute Type: Anti-Malware

Product Installation: Installed Not Installed

Reatime Scanning: Enabled Disabled

Vendor: Microsoft Corporation

2.为避免在 ASDM 上添加属性，可以运行命令“ debug menu dap 1”和“ debug menu dap 2” [这些是用于 DAP 配置的 show 命令]，然后复制输出，在文本编辑器中对其进行修改。 根据要求填写所有必需的 AV，然后在 ASA 上载 dap.xml。

【问题二十四】

● 我在 Windows 和 Mac 上使用配置文件的 FTD 和 AnyConnect 4.8.02042 遇到问题。我使用独立的概要文件编辑器进行了一些更改，并将其移动到 ProgramData 中的“概要文件”文件夹中。诸如 HostEntry 和 AllowManualHostInput 之类的东西正在被识别和应用。但是，对 AuthenticationTimeout 和 EnableScripting 的更改却没有。

进行每次更改后，我将退出 AnyConnect 客户端并重新启动服务，为了更好地执行操作，我还重新启动了计算机。我可以从事件查看器中看到正在应用哪些设置。

使用默认首选项。如果预期使用本地配置文件，则某些设置（例如证书匹配）可能无法按预期运行。验证所选主机是否在配置文件的“服务器列表”部分中，并且已在安全网关上配置了该配置文件。

由于没有文件下载到“个人档案”文件夹，因此 FTD 似乎没有应用了个人档案。我还通过带有 XSD 文件的验证器传递了 XML 文件。

▲ 您是否还将其上传到 FTD 设备，然后将其应用于用户连接的组策略？

● 我没有，我认为 FTD 设备没有配置文件，因为用户连接后它没有下载任何文件到客户端。

▲ 我假设您只是想为本地用户创建个人资料？这实际上不是受支持的配置设计，但是如果您希望特定参数在连接到 VPN 头端时生效，那么您还需要在 xml 配置文件中创建服务器列表、主机名、主机地址部分。这些参数会将配置文件的其余部分链接到头端连接，而不是使用默认的组策略。最好将其应用于 FTD 设备，并在客户端连接时将其推出客户端。

● 我的个人资料确实包含我要连接的服务器的 serverlist 和 hostentry 部分。我一直遵循此评论 (<https://community.cisco.com/t5/vpn/community-ask-me-anything-configuration-troubleshooting-and-best/m-p/4063991/highlight/true#M271759>) “修改 XML 配置文件，并将其与您的 OnConnect 脚本一起推送到客户端，将其正确定位”。

我们将使用 GPO / MEMCM 组合将文件推送到客户端。

- A** 您仍然需要 xml 配置文件中的主机名/主机地址，因此客户端在连接时就知道要使用该 xml 配置文件，否则，它将仅使用默认配置文件，并且您修改的任何字段都不会生效。

【问题二十五】

- Q** cisco anyconnect vpn on asa ， 想要做 posture , asa 和 ISE 都需要什么许可证

- A** 因此，我们要配置 anyconnect ISE posture。

两个主要的许可要求是：

ISE 上的 BASE 和 APEX 许可证，对于已使用的每个会话基本许可证，必须已经存在 BASE 和 APEX 许可证。

根据您的要求，取决于用户数量，ASA 上的 AnyConnect 用户许可证。

以下链接提供了有关 ISE 许可证的信息：

https://www.cisco.com/c/en/us/td/docs/security/ise/2-1/admin_guide/b_ise_admin_guide_21/b_ise_admin_guide_20_chapter_0110.html#id_24976

一些有助于对配置和流程有基本了解的好文档：

<https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/117693-configure-ASA-00.html>

<https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/215236-ise-posture-over-anyconnect-remote-access.html>