

## 【专家问答】问题汇总\_思科保障远程办公安全

感谢大家参与本期“[思科保障远程办公安全](#)”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。以下为此次 Webex Meetings 在线答疑的部分问题及回复，以供大家参考：

### 问答专家：



**Divya Nair**

安全业务组技术市场工程师



**Jonny Noble**

领导 Cisco 云安全技术营销团队



**Aditya Ganjoo**

印度班加罗尔技术营销工程师

### 【问题一】

Q 你好，有没有针对 DNS 查询的故障排除指南？使用 Anyconnect VPN 连接时，解决本地 dns 总是很麻烦。谢谢

A 你好，您是否遇到通过 VPN tunnel 的本地 DNS 解析问题？

如果是，则可以检查组策略属性中的特定值。

如果您正在寻找最佳实践，则可以使用 Anyconnect 为 DNS 配置以下三个选项：

拆分 DNS-与域名匹配的 DNS 查询在 Cisco Adaptive Security Appliance (ASA) 上配置。它们通过 tunnel 移动（例如，移动到 ASA 上定义的 DNS 服务器），而其它的则不这样做。

Tunnel-all-DNS-仅允许到 ASA 定义的 DNS 服务器的 DNS 通信。此设置在组策略中配置。

标准 DNS-所有 DNS 查询都在 ASA 定义的 DNS 服务器中移动。在否定响应的情况下，DNS 查询也可能会转

到物理适配器上配置的 DNS 服务器。

您也可以查看以下链接，以更清楚地了解 Anyconnect 的 DNS 行为：

<https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/116016-technote-AnyConnect-00.html#anc1>

如果觉得帖子有帮助，请记得评分。

#### Q 你好，谢谢回复

“拆分 DNS-与域名匹配的 DNS 查询是在 Cisco 自适应安全设备 (ASA) 上配置的。它们通过隧道移动 (例如，移动到 ASA 上定义的 DNS 服务器)，而其他则没有。”

当您说“在 ASA 上定义的 DNS 服务器”时，表示在 ASA 防火墙或隧道或组策略中配置了 DNS 服务器

与域名匹配的 DNS 查询，您是说域名是在防火墙上还是在组策略中配置的？

如果我们拥有类似 test.local 和 test.com 这样的域名怎么办？

test.com (这是 test.local dns 同一服务器中的转发区域 (例如: 192.168.1.100))

test.com 也解析为私有 IP 地址

这是我当前的配置：

```
dns domain-lookup Inside
dns server-group DefaultDNS
name-server 192.168.1.100
domain-name test.local
```

谢谢！

#### A 你好，所有值都将在组策略下。您可以在组策略下添加多个值/域。

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/S/cmdref3/s16.html#pgfid-1597902>

#### Q 谢谢回复。

我已经尝试了所有 split-dns, standard, tunnel 所有 dns ... 仍然无法解决 (从服务器可访问 dns 服务器)。 我

正在使用 anyconnect 4.8 和 ASA 代码 9.2

请指教

**A** 您好, 您可以共享 show run group-policy <policy-name>的输出吗?

**Q** 你好, 这是我的 sh run 组策略:

1)

```
group-policy it-test internal
group-policy it-test attributes
dns-server value 192.168.1.100
vpn-idle-timeout 20
vpn-tunnel-protocol ikev1 ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value it-test-acl
default-domain value test.local
address-pools value it-test-pool
```

2 )

```
group-policy it-test2 internal
group-policy it-test2 attributes
wins-server none
dns-server value 192.168.1.100
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value it-test2-acl
default-domain value test.local
split-dns value test.local test.com
split-tunnel-all-dns disable
address-pools value it-test2-Pool
```

删除“ split-tunnel-all-dns disable”后也尝试了以下操作, 但没有帮助。

3 )

```
group-policy it-test2 internal
group-policy it-test2 attributes
wins-server none
dns-server value 192.168.1.100
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value it-test2-acl
default-domain value test.local
```

split-dns value test.local test.com  
split-tunnel-all-dns disable  
address-pools value it-test2-Pool

谢谢。

**A** 你好,

请禁用/删除通道所有拆分的 dns 配置, 并保留 split-dns 的值, 并确保 DNS 服务器 (IP) 是拆分通道 ACL 的一部分。

要确认 DNS 查找 (如果它们正在通过 Anyconnect), 可以使用 Wireshark, 在计算机上开始捕获并检查 DNS 请求发送到哪个适配器。

如果可能的话, 请共享测试计算机的 ipconfig / all 输出和捕获。

Regards

**Q** 请禁用/删除通道所有拆分的 dns 配置, 并保留 split-dns 的值, 并确保 DNS 服务器 (IP) 是拆分通道 ACL 的一部分。

--已禁用, 完整子网为 (192.168.1.0/24) 是拆分隧道 acl 的一部分

要确认 DNS 查找 (如果它们正在通过 Anyconnect), 可以使用 Wireshark, 在计算机上开始捕获并检查 DNS 请求发送到哪个适配器。

--是的, 通过 Anyconnect 链接

如果可能的话, 请共享测试计算机的 ipconfig / all 输出和捕获。

--请见附件

**A** 我可以看到请求到达 DNS 服务器, 但它返回服务器错误:

标准查询响应, 服务器故障

您说当您不使用 Anyconnect 时, 它可以正常工作。

如有可能, 请共享工作中的快照。

Q 谢谢回复。

我的意思是当我在 anyconnect 上时，它是工作的，如果我删除“ split-dns value test.com”，它将通过物理适配器和公共 ip 地址进入公共 dns (ISP)。

并且内部 dns 服务器在我们本地的局域网中工作（我可以很快共享数据包捕获）

您能告诉我为什么 anyconnect mac 地址显示为 00: 11: 22: 33: 44: 55

```
> Frame 7: 76 bytes on wire (608 bits), 76 bytes captured (608 bits)
  v Ethernet II, Src: Cisco_3c:7a:00 (00:05:9a:3c:7a:00), Dst: Cimsys_33:44:55 (00:11:22:33:44:55)
    > Destination: Cimsys_33:44:55 (00:11:22:33:44:55)
    > Source: Cisco_3c:7a:00 (00:05:9a:3c:7a:00)
      Type: IPv4 (0x0800)
    > Internet Protocol Version 4, Src: 172.16.228.5, Dst: 192.168.1.100
    > User Datagram Protocol, Src Port: 53259, Dst Port: 53
  v Domain Name System (query)
    Transaction ID: 0x4538
    > Flags: 0x0100 Standard query
    Questions: 1
```

A MAC 地址用于目标 IP，即您的下一跳。

AC 的 MAC 地址为 0-05-9A-3C-7A-00。

“ AnyConnect 驱动程序不会干扰本机 DNS 解析器。因此，将根据网络适配器的顺序执行 DNS 解析，其中在连接 VPN 时，AnyConnect 始终是首选适配器。此外，DNS 查询首先通过隧道发送，如果没有解析，解析器将尝试通过公共接口解析它。split-include 访问列表包括覆盖 Tunnel DNS 服务器的子网。要从 AnyConnect 4.2 开始，Tunnel DNS 服务器的主机路由将由 AnyConnect 客户端自动添加为“包含拆分的网络”（安全路由），因此“包含拆分的访问列表”不再需要显式添加隧道 DNS 服务器子网。”

我认为您的 case 是这样的情况。

Q 谢谢回复，

我已经从 acl 中删除了子网，但是出了同样的问题。

从 Wireshark 捕获分析中，DNS 查询是否响应错误？

当您说“ MAC 地址用于目标 IP，即您的下一跳”。

可能是 ASA 防火墙接口吗？

**A** 需要检查，我不认为它是 ASA 的 MAC 地址。 我寻找了 MAC 地址，似乎是基于 CIMSYS Inc 的设备。

## 【问题二】

**Q** 你好

在 cisco anyconnect 中，我们是否可以使用 FTD 防火墙阻止非 Windows 连接的计算机并仅允许域计算机连接到 anyconnect？

谢谢

**A** 你好，

您可以对 AnyConnect 用户使用计算机证书身份验证，以确保只有域计算机可以加入。

配置指南

[https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/firepower\\_threat\\_defense\\_remote\\_access\\_vpns.html#id\\_login\\_via\\_clientcert](https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/firepower_threat_defense_remote_access_vpns.html#id_login_via_clientcert)

**Q** 谢谢你的回复。

基本上，我想知道的是，我已经在执行 DLP 的域计算机，他们都不能从计算机上复制任何东西，以及所有计算机，例如，如果我的员工使用他们的个人计算机连接到公司网络，我如何能防止他们不复制任何东西，除了使用必需的应用程序工作等等，基本上，我不想让他们在连接到网络时从网络复制任何数据。

我怎样才能做到这一点？ 如何为加入域的计算机创建一个隧道组 (tunnel-group)，为非加入域的计算机创建另一个隧道组并执行策略？

谢谢。

**A** 是的，您需要创建其他连接配置文件并强制执行策略。

这可以通过不同的方式来完成，例如通过为用户提供组 URL，通过 Radius 属性或通过 ASA 上的组锁定功能。

Regards.

❓ 你能不能提供一个我可以参考的配置指南示例？

谢谢。

👉 请参考以下内容：

<https://community.cisco.com/t5/security-documents/steps-to-configure-group-lock-for-vpn-users-on-microsoft-radius/ta-p/3151643>

<https://community.cisco.com/t5/security-documents/asa-ssl-vpn-tunnel-group-group-url-and-group-alias-selection/ta-p/3111990>

❓ 这些链接配置了不同的组隧道组和组别名，但是我正在寻找对每个组策略实施 DLP 类型的策略，以使它们将无法通过 Anyconnect 隧道复制任何数据。

基本上，他们不应该通过 Anyconnect VPN 隧道复制任何数据，我如何在 Anyconnect VPN 上实施这种策略

👉 你好，如果我理解的对，您正在寻求对 BYOD 用户实施 DLP。在 FTD 上执行此操作的最佳方法是让 BYOD 用户连接到单独的连接配置文件/组策略。给此连接一个与域用户不同的地址池。然后，您可以在 FTD 访问策略上使用应用程序筛选器来阻止 BYOD VPN 池的文件传输协议。请记住，FTD 并不是真正的 DLP 应用程序，但是应用程序筛选器将帮助您完成所需的工作

[https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/rule\\_management\\_common\\_characteristics.html#id\\_16281](https://www.cisco.com/c/en/us/td/docs/security/firepower/650/configuration/guide/fpmc-config-guide-v65/rule_management_common_characteristics.html#id_16281)

希望以上对您有帮助

👉 除了 Divya 所说的之外，您还可以使用 Anyconnect 来执行按需脚本 (On-demand Scripts)：

[https://www.cisco.com/c/en/us/td/docs/security/vpn\\_client/anyconnect/anyconnect40/administration/guide/b\\_AnyConnect\\_Administrator\\_Guide\\_4-0/customize-localize-anyconnect.html#ID-1408-00000396](https://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect40/administration/guide/b_AnyConnect_Administrator_Guide_4-0/customize-localize-anyconnect.html#ID-1408-00000396)

Regards

**【问题三】**

Q 大家好，我有几个问题：

1.在使用 Firepower 威胁防御 (FTD) 设备作为前端时，当前不支持 webvpn 定制 (即 webvpn 主页) 和 AnyConnect 定制 (消息, 语言等)，我是否理解正确？ (由 FMC 管理或 FDM / CDO 管理)

2.基本 posture 检查 (例如我们可以使用 ASA 和 DAP / Hostscan 进行的检查) 目前尚不能单独使用 FTD (例如，我们必须参考 ISE 等外部解决方案) -对吗？

3.对于具有 ASA 的 DAP / Hostscan，它是否需要 AnyConnect Premium，在 ASAv 平台型号上支持吗？

A 1. 是对的。 FTD 不支持无客户端 WebVPN 和 AnyConnect 自定义。

2. 您需要在 FTD 上使用 ISE Posture 进行客户状态评估。

3. 带有 DAP 的 ASA 需要 Apex 许可证 (以前是 Premium 许可证)，并且在 ASAv 型号上受支持。

Q 一个后续问题-我们中的一些人试图使 DAP 在 ASAv 上运行并遇到问题。 请查看此贴：

<https://community.cisco.com/t5/vpn/asa-virtual-unable-to-activate-hostscan/td-p/4044100>

您可以在这里回答吗，还是我们应该开个 TAC Case ？

A 您好，请查看以下内容

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCvs84158/?rfs=iqvred>

A 也在您提到的帖子下面更新了。

Q 谢谢两位。

贴在这里方便其他用户查看：增加内存以将 ASAv 作为 ASAv10 (与 ASAv5) 模型一起运行，可以解决无法

添加主机扫描的问题，这是使用 DAP 所必需的。

#### 【问题四】

Q Cisco ASA 5508-X 在任何给定时间最多只能有 5 个会话。



我们已购买了 100 个用户的许可，我在文件中附加了我们正在运行的配置，如果有人能够帮助我们指出正确的方向，我们将不胜感激。

我们已将分配的带宽从 300 Mbps 提高到 1GB，以允许更多用户使用，但在任何给定时间我们仍然只能获得 5 个。

"show vpn-sessiondb summary" 命令结果

```
-----  
VPN Session Summary  
-----  
Active : Cumulative : Peak Concur : Inactive  
-----  
AnyConnect Client      :    2 :    321 :    7 :    1  
  SSL/TLS/DTLS         :    2 :    321 :    7 :    1  
Clientless VPN         :    0 :    20 :    3  
  Browser               :    0 :    20 :    3  
Site-to-Site VPN       :    2 :   1093 :    2  
  IKEv2 IPsec           :    2 :   1093 :    2  
-----  
Total Active and Inactive :    5          Total Cumulative :  1434  
Device Total VPN Capacity :   100  
Device Load                :    5%
```

"show vpn-sessiondb detail" 命令结果:

```
-----  
VPN Session Summary  
-----  
Active : Cumulative : Peak Concur : Inactive  
-----  
AnyConnect Client      :    2 :    321 :    7 :    1  
  SSL/TLS/DTLS         :    2 :    321 :    7 :    1  
Clientless VPN         :    0 :    20 :    3  
  Browser               :    0 :    20 :    3  
Site-to-Site VPN       :    2 :   1093 :    2  
  IKEv2 IPsec           :    2 :   1093 :    2  
-----  
Total Active and Inactive :    5          Total Cumulative :  1434  
Device Total VPN Capacity :   100  
Device Load                :    5%
```

-----  
Tunnels Summary

	Active	Cumulative	Peak Concurrent
IKEv2	2	1093	2
IPsecOverNatT	2	1094	2
Clientless	0	20	3
AnyConnect-Parent	3	321	7
SSL-Tunnel	2	325	6
DTLS-Tunnel	2	309	6
<b>Totals</b>	<b>11</b>	<b>3162</b>	

**A** 您好。

如果您看到的是 100 作为安装限制，是否可以使用 show vpn-session license-summary 的输出进行确认？

ASA 5506 上的输出示例如下（请参见红线）：

```
ASA5506-X(config)# sh vpn-sessiondb license-summary
```

```
-----
VPN Licenses and Configured Limits Summary
-----
```

```
Status : Capacity : Installed : Limit
-----
```

```
AnyConnect Premium : ENABLED : 50 : 50 : NONE
```

```
AnyConnect Essentials : DISABLED : 50 : 0 : NONE
```

```
Other VPN (Available by Default) : ENABLED : 10 : 10 : NONE
```

```
Shared License Server : DISABLED
```

```
Shared License Participant : DISABLED
```

```
AnyConnect for Mobile : ENABLED(Requires Premium or Essentials)
```

```
Advanced Endpoint Assessment : ENABLED(Requires Premium)
```

```
AnyConnect for Cisco VPN Phone : ENABLED
```

```
VPN-3DES-AES : ENABLED
```

```
VPN-DES : ENABLED
-----
```

第 6 个连接进入时，您是否看到任何系统日志？您可能需要增加日志记录以临时调试。我检查了您的配置，没有发现任何问题。

**Q** 我们的输出确认如下。

我们这里确实显示的是安装限制 100 个

**Result of the command: "show vpn-session license-summary"**

---

## VPN Licenses and Configured Limits Summary

---

	Status	Capacity	Installed	Limit
AnyConnect Premium	: ENABLED	: 100	: 100	: 100
AnyConnect Essentials	: DISABLED	: 100	: 0	: 100
Other VPN (Available by Default)	: ENABLED	: 100	: 100	: 100
Shared License Server	: DISABLED			
Shared License Participant	: DISABLED			
AnyConnect for Mobile	: ENABLED(Requires Premium or Essentials)			
Advanced Endpoint Assessment	: ENABLED(Requires Premium)			
AnyConnect for Cisco VPN Phone	: ENABLED			
VPN-3DES-AES	: ENABLED			
VPN-DES	: ENABLED			

---

---

## VPN Licenses Usage Summary

---

	All	Peak	Eff.	
	In Use	In Use	Limit	Usage
AnyConnect Premium	: 4	: 8	: 100	: 4%
Anyconnect Client	: 4	: 7	: 100	: 4%
Clientless VPN	: 0	: 3	: 100	: 0%
Other VPN	: 2	: 3	: 100	: 2%
L2TP Clients				
Site-to-Site VPN	: 2	: 2	: 100	: 2%

---

Result of the command: "show vpn-session license-summary"

---

---

## VPN Licenses and Configured Limits Summary

---

	Status	Capacity	Installed	Limit
AnyConnect Premium	: ENABLED	: 100	: 100	: 100
AnyConnect Essentials	: DISABLED	: 100	: 0	: 100
Other VPN (Available by Default)	: ENABLED	: 100	: 100	: 100
Shared License Server	: DISABLED			
Shared License Participant	: DISABLED			
AnyConnect for Mobile	: ENABLED(Requires Premium or Essentials)			
Advanced Endpoint Assessment	: ENABLED(Requires Premium)			
AnyConnect for Cisco VPN Phone	: ENABLED			
VPN-3DES-AES	: ENABLED			
VPN-DES	: ENABLED			

---

-----  
**VPN Licenses Usage Summary**  
-----

	All	Peak	Eff.	
	In Use	In Use	Limit	Usage
AnyConnect Premium	:	4	8	100 : 4%
Anyconnect Client	:	4	7	100 : 4%
Clientless VPN	:	0	3	100 : 0%
Other VPN	:	2	3	100 : 2%
L2TP Clients				
Site-to-Site VPN	:	2	2	100 : 2%

-----

**A** 请共享 show run vpn-sessiondb 的输出, 也可以共享看到此问题时的日志?

**Q** 您好,

以下是您要求的输出:

```
TBROG-FW-01# show run vpn-sessiondb
vpn-sessiondb max-other-vpn-limit 100
vpn-sessiondb max-anyconnect-premium-or-essentials-limit 100
TBROG-FW-01#
```

can you advise what logs you're wanting to see? I have below my latest successful attempt from external ip 71.195.58.236. any other attempts after our 6th connection i can no longer see any logs generated.

```
6|Mar 25 2020|08:10:05|722022|Group <GroupPolicy_VPN> User <USER> IP <71.195.58.236> UDP
SVC connection established without compression
5|Mar 25 2020|08:10:05|722033|Group <GroupPolicy_VPN> User <USER> IP <71.195.58.236> First
UDP SVC connection established for SVC session.
6|Mar 25 2020|08:10:05|725002|71.195.58.236|59949||Device completed SSL handshake with client
Outside:71.195.58.236/59949 to 50.234.X.XX/443 for DTLSv0.9 session
6|Mar 25 2020|08:10:05|725003|71.195.58.236|59949||SSL client Outside:71.195.58.236/59949 to
50.234.2.58/443 request to resume previous session
6|Mar 25 2020|08:10:05|725001|71.195.58.236|59949||Starting SSL handshake with client
Outside:71.195.58.236/59949 to 50.234.X.XX/443 for DTLS session
6|Mar 25 2020|08:10:05|725001|71.195.58.236|59949||Starting SSL handshake with client
Outside:71.195.58.236/59949 to 50.234.X.XX/443 for DTLS session
4|Mar 25 2020|08:10:01|722051|Group <GroupPolicy_VPN> User <USER> IP <71.195.58.236> IPv4
Address <192.168.99.150> IPv6 address <::> assigned to session
6|Mar 25 2020|08:10:01|722055|Group <GroupPolicy_VPN> User <USER> IP <71.195.58.236> Client
Type: Cisco AnyConnect VPN Agent for Windows 4.2.03013
6|Mar 25 2020|08:10:01|722022|Group <GroupPolicy_VPN> User <USER> IP <71.195.58.236> TCP
SVC connection established without compression
```

**A** 您可以给我们发送尝试连接第六个客户端时的以下信息吗：

调试 webvpn 255

调试 webvpn anyconnect 255

第六次连接失败后的 DART 捆绑包。

**Q** 我认为这超出了我的能力范围，或者我不熟悉如何生成和访问这些日志。

有没有我可以遵循的指南来获取此日志输出？

**A** 对于调试，您将需要登录到 ASA CLI 并在尝试进行第六次连接之前启用以下命令：

```
ASA5506-X# debug webvpn anyconnect 255
```

```
ASA5506-X# debug webvpn 255
```

DART 本质上是一种诊断模块，可用于将客户端日志整理到一个位置。以下链接逐步介绍了设置步骤

<https://community.cisco.com/t5/security-documents/how-to-collect-the-dart-bundle-for-anyconnect/tap/3156025>

但是，如果您更方便，那么开 TAC Case 可能会更好，以便工程师可以发起远程会话进行故障排除。

**A** 真奇怪。您能否提高日志记录级别进行调试，然后测试第 6 个连接？

另外，您是否使用其他用户名进行过测试？

我会要求进行其他调试，例如 debug webvpn anyconnect 255，然后对其进行测试，但我不确定防火墙上的资源使用情况。

## 【问题五】

**Q** 您好，我目前正在使用 AnyConnect 4.3.05017 (Windows 7) 连接到公司网络 (COVID-19 ...)，并且受到一个已知问题的困扰，而该问题显然没有解决办法：

当 AnyConnect 处于活动状态时，无法将其他路由安装到路由表中。但是，作为我工作的一部分，我需要访问

可通过虚拟网络适配器访问的 VirtualBox 虚拟机。每当我启动虚拟机时, AnyConnect 都会删除路由表条目。

这些是事件数据条目:

```
A routing table change notification has been received. Starting automatic correction of the routing table.
```

```
Routing table - fixed - deleted route
```

```
Destination Netmask Gateway IfAddr IfName IfIndex LL Metric
```

```
192.168.66.0 255.255.255.0 0.0.0.0 192.168.66.1 VirtualBox Host-Only Network 16 Y 1
```

```
Automatic correction of the routing table has been successful.
```

我知道保持对路由表的控制是一项安全功能, 但是在这种情况下 (以及 Internet 上的其他报告), 这使我无法完成分配的工作。该怎么办? 客户端或服务器端是否有可用于解决此错误行为的配置选项?

**A** 您是否尝试过使用“分割-排除隧道”功能(Split-Exclude Tunneling): 通过这种方法, 您告诉设备去指定那些您不打算通过隧道发送的流量?

**Q** 谢谢, 这可能会有所帮助!

显然, 在 ASA 中禁用了本地 LAN 访问, 因此我无法在客户端中启用它 (因为我只是开发人员, 而不是网络管理员)。但是我可以要求管理员根据以下链接里的信息来 enable 此功能 <https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/70847-local-lan-pix-asa.html>, 这很可能会使配置正常。

**A** 不客气, 如果还需要帮助, 请告诉我们。

## 【问题六】

**Q** 我们有两个相互连接的区域, 其中外部区域使用 AnyConnect 进行 Internet 访问。

我的 enclave 位于 ASA-5585-X 的后面, 我需要给极少数用户访问此 enclave 的权限。我的第一个念头是将一个 AnyConnect 会话嵌套在另一个会话中, 在一个隧道内创建一个隧道, 但似乎不起作用

如果我让外部 enclave 的管理员创建一个暴露防火墙外部接口的 NAT, 最终用户是否可以连接到其他 IP 地址

并绕过外部防火墙进行 VPN 会话？

概念布局

Internet====>> Outside firewall ====>> Outer enclave ====>>Inside firewall (my ASA) ====>> Inner enclave

我需要这个:

Internet =====>> VPN  
=====>>Innerenclave

但是不知道为什么有问题。请问有任何建议吗？

Thanks

**A** 您可以为用户创建静态 NAT，以访问内部防火墙背后的资源。

Internet=====>> VPN=====>>Inner enclave

或者，您可以在 VPN 策略上允许特定的 Inner enclave 子网，然后限制外部（少量用户），在 Inside FW 上配置入口 ACL。

假设 Anyconnect VPN 将在外部 FW 上终止，然后一切都将以明文形式进行。

希望以上有帮助。

**Q** 假定内部 enclave 内的子网信息已发布到外部 enclave 内，而事实并非如此。

我不能使用基于 IP 的限制，因为一些需要访问内部 enclave 的用户都在外部 enclave 内。

有什么方法可以使用 Windows 10 VPN 适配器连接到 ASA？

**A** 使用外部 VPN 终止所有连接并对外部和内部用户使用不同的隧道组/连接配置文件/组策略时是否存在问题？

我问的原因是因为使用 L2TP 客户端仍将是“隧道中的隧道”。(unnel-in-a-tunnel)

## 【问题七】

- 如果我们在远程访问 VPN 上使用无拆分隧道或全隧道 DNS 并将这些功能与 Umbrella 结合使用，则非托管端点遇到 https 站点的 Umbrella 阻止页面并出现证书错误的问题。鉴于 https 用于所有 Web 流量的 80% (或更多)，这已成为一个日益严重的问题。

对于受托管端点，这并不是什么大问题，因为我们可以按照 Umbrella 文档中的说明通过 GPO (或其他 EMM 软件) 将证书推送到本地证书存储中：

<https://docs.umbrella.com/deployment-umbrella/docs/install-cisco-umbrella-root-certificate>

对于非托管端点，告诉最终用户下载并信任 Umbrella 证书非常麻烦。我们可以采取任何最佳实践来避免这样做吗？

- ▲ 你好，对于不受管理的设备，最佳实践是将它们拆分为一个不同的网络 (或 Umbrella 仪表板中的标识)，并对它们应用单独的策略。

在该单独的策略中，您不应该启用智能代理 (不检查文件，因此也不要 HTTPS 解密)，并且通过仅将所有安全性强制措施保留在 DNS 层，就不会遇到这些问题。

虽然我了解到，在公司网络中进行这种流量分配比较容易 (例如，来宾流量或不受管理的设备通过单独的 VLAN 或单独的 SSID 进行传输)，但就您而言，这听起来像是您在指正在连接到的远程工作人员 VPN，这是托管和非托管设备的相同连接类型。

在这种情况下，您将需要在所有伞形策略中禁用文件检查，这些策略涵盖将要包含非托管设备的身份。

- 我估计就是这么回事儿，不过还是很感谢您的确认。

## 【问题八】



Q 我已经找到并被指出要逐步进行拆分,但是我不想拆分。谁能告诉我怎么样能够不需要一步一步地分割隧道?

A 您能详细说明一下要求吗?

您要禁用拆分隧道吗?如果是,则可以使用 TunnelAll 选项。

如果可能,请共享配置,用例是什么?

Q 如果使用“TunnelAll”,则该更改如何影响 NAT 语句?基本上,我一直用“分割隧道”(split tunnel)。当我更改为“TunnelAll”时,所有互联网访问都丢失了。

谢谢。

A 我估计这是一个 ASA。

您需要以下命令才能访问 Internet。

我们需要为 Anyconnect 用户提供流量。

```
same-security-traffic permit intra-interface  
object network obj-AnyconnectPool  
nat (outside,outside) dynamic interface
```

其中 obj-AnyconnectPool 是 Anyconnect 池网络

Q 是 head end ASA。

我已经有了允许内部接口通信 (the permit intra interface traffic)。

我可以尝试您建议的 NAT。很难想象这将如何允许流量进入内部,我将在一个小时内尝试。谢谢

A 我建议的 NAT 是为 Anyconnect 用户提供 Internet 访问权限,因为您提到他们一旦连接到 Anyconnect (使用 TunnelAll) 后就失去了 Internet 访问权限。

对于内部访问,您可以使用此 NAT 免除 Anyconnect 流量:

```
nat (inside,outside) source static any any destination static obj-Anyconnect obj-Anyconnect
```

● 通过隧道，他们都可以同时进入内部并被允许进入互联网，但是流量是否从 ASA 传到 ASA，而不是他们的家庭网络？

还有路由，您会添加一条路线(route)吗

建议在 ASA 中或向下游注入路由。

▲ 没错。

TunnelAll 意味着流量必须到达前端 (ASA)，然后从那里将流量路由到外部 (使用外部接口上的 Dynamic PAT)。

您将需要在下游设备上反向路由 (对于池)。

像这样:

```
ip route x.x.x.x mask <ASA inside interface IP>
```

● 我已经使用该 NAT 进行内部访问-如何允许通过头端 headend 设备将 AnyConnect 的 IP 池允许到 Internet ？

客户端连接到 AnyConnect-从 AnyConnect IP 池接收 IP 地址。

使用下面的 NAT，它们可以访问内部网络，但不能访问 INTERNET。 [我用内部对象组替换了“any”。]

```
nat (inside,outside) source static any any destination static obj-Anyconnect obj-Anyconnect
```

要使 AnyConnect IP 池也可以上网，究竟需要什么？ 因为此 NAT 不允许客户端访问 Internet ？？？

▲ 您好，以下指南涵盖您需要的所有步骤，

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/100918-asa-sslvpn-00.html>

您可以先看一下，如果仍有问题，请让我们知道。

▲ 我在之前的回帖里已经提到，您可以使用以下 NAT:

```
object network obj-AnyconnectPool  
nat (outside,outside) dynamic interface
```

Q 所以 AnyConnect IP pool 将有两个 NAT statements ?

A 是的, 一个用于内部网络访问, 一个用于 Internet 访问。

Q 我想说谢谢 您提供的最后一个链接正是我所需要的! 我仍然需要弄清楚后端路由, 但是非常高兴地说, 感谢您, AnyConnect 在 Tunnelall 配置中已经正常工作了。

A 非常高兴能够帮助到您

## 【问题九】

Q 请指导如何对任何 connec 用户应用 qos ?

在 ssp asa 设备上可以吗?

要求是给每个用户 1 Mb, 远程桌面用户抱怨性能

以及 sql 客户端用户 (从远程连接到 sql server 的桌面应用程序)。

使用 anyconnect 从远程连接用户时, 如何解决 sql server / database 断开连接的问题

谢谢

A 解密后, 您需要检查流量 (明文流量)。 Anyconnect 会像对待其他流量一样对待 SQL / DB 流量。 您还需要确保设备不会被 VPN 流量淹没。

请查看 ASA 数据表以获取有关 ASA 通过 VPN 服务提供的吞吐量的更多信息。

不幸的是, 在 ASA 上, 没有任何方法可以限制或限制每个 Anyconnect 会话的流量。

您可以将所有 AnyConnect 用户或远程访问 VPN 用户共同限制为一定的带宽。 下面是示例配置:

```
access-list 101 extended permit ip internal_Resource_IP internal_Resource_Mask anyconnect_IP_Pool  
anyconnect_Mask
```

```
class-map remote-access  
match access-list 101
```

```
policy-map outside-policy  
class remote-access  
police output 1000000 <-- this value is 1 Mb in bits
```

<https://www.cisco.com/c/en/us/td/docs/security/asa/asa98/configuration/firewall/asa-98-firewall-config/conns-qos.html#ID-2133-000002dd>

**A** 请检查此链接以获取 IP 配置和最佳做法:

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

如果还需要更多解答，您可以在以下论坛发帖提问

<https://community.cisco.com/t5/network-security/bd-p/discussions-network-security>