在AnyConnect和漫游客户端的OpenDNS之间的Interop

目录

简介

本文描述某些当前限制，并且做AnyConnect和OpenDNS的可用的应急方案漫游客户端。 Cisco用户在安全和加密的通信的AnyConnect VPN客户端取决于对他们的公司网络。同样地，漫游客户端的OpenDNS给用户能力在OpenDNS公共服务器帮助下安全地使用DNS服务。这两个客户端添加在终端的富有的一套安全功能，并且兼容彼此他们是重要的。

先决条件

漫游客户端的AnyConnect和OpenDNS的运行知识。

与ASA或IOS/IOS-XE数据转发器配置(隧道群/组政策)的熟悉AnyConnect的VPN。

要求

Cisco 建议您了解以下主题：

- ASA或IOS/IOS-XE头端
- 运行AnyConnect VPN客户端和OpenDNS的终端漫游客户端

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ASA头端运行版本9.4
- Windows 7
- AnyConnect客户端4.2.00096
- 漫游客户端2.0.154的OpenDNS

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

OpenDNS在将来开发AnyConnect插件与思科AnyConnect团队是可用的。当日期未设置时，此集成将允许漫游的客户端工作与AnyConnect客户端，不用寻址的应急方案。这也将使AnyConnect是漫游的客户端的一个交付机制。

功能

AnyConnect DNS处理

VPN头端可以配置用夫妇不同的方式处理从AnyConnect客户端的流量。

1. 全通道配置(通道所有) ：这强制从终端的所有流量在加密的VPN通道间发送，并且流量从未留下在明文的公共接口接口器
2. 分割隧道配置：

   a. 已分解包括隧道：流量仅被注定了对特定子网或在VPN头端定义的主机在通道间发送，其他流量在明文的通道的外部发送

   b. 已分解排除隧道：流量仅被注定了对特定子网或在VPN头端定义的主机从加密被屏蔽并且离开在明文的公共接口，其他流量在通道间加密和只发送

这些配置中的每一根据在终端的操作系统确定DNS解析如何处理由AnyConnect客户端。有在行为上的一个变化在AnyConnect的DNS处理机制Windows的，在版本4.2在CSCuf07885的修正以后。

Windows 7+

通道所有配置(和分割隧道用启用的通道所有DNS)

前AnyConnect 4.2 ：

对根据组政策配置的DNS服务器的仅DNS请求(通道DNS服务器)允许。AnyConnect驱动程序回答与'没有这样命名'答复的其他请求。结果，使用通道DNS服务器， DNS解析可能只执行。

AnyConnect 4.2 +

只要他们起源于VPN适配器和在通道间，发送对所有DNS服务器的DNS请求允许。其他请求响应与'没有这样命名'答复，并且DNS解析可能通过VPN通道只执行

在CSCuf07885修正之前， AC限制目标DNS服务器，然而以CSCuf07885的修正，限制哪些网络适配器可以启动DNS请求。

已分解包括配置(禁用的通道所有DNS和split-dns)

AnyConnect驱动程序不干涉本地DNS解析程序。所以， DNS解析执行根据大约网络适配器，并且AnyConnect总是首选的适配器，当VPN连接时。因此DNS查询通过通道首先将被发送，并且，如果没获得解决，解析程序将尝试通过公共接口解决它。已分解包括access-list将必须包括包括通道DNS服务器的子网。开始与AnyConnect 4.2，通道DNS服务器的主机路由由AnyConnect客户端自动地添加和已分解包括网络(请保护路由)，并且已分解包括access-list不再要求通道DNS服务器子网的明确新增内容。

已分解排除配置(禁用的通道所有DNS和split-dns)

AnyConnect驱动程序不干涉本地DNS解析程序。所以， DNS解析执行根据大约网络适配器，并且AnyConnect总是首选的适配器，当VPN连接时。因此DNS查询通过通道首先将被发送，并且，如果没获得解决，解析程序将尝试通过公共接口解决它。已分解排除access-list不应该包括包括通道DNS服务器的子网。开始与AnyConnect 4.2，通道DNS服务器的主机路由由将防止在已分解排除的误配置access-list的AnyConnect客户端自动地添加和已分解包括网络(请保护路由)，并且。

Split-dns (禁用的通道所有DNS，已分解包括已配置的)

前AnyConnect 4.2

匹配split-dns域的DNS请求允许建立隧道DNS服务器，但是没有允许到其他DNS服务器。如果查询被发送到其他DNS服务器，要防止这样内部DNS查询泄漏通道， AnyConnect驱动程序回应'没有这样名称'。split-dns域可以只所以是解决的通过通道DNS服务器。

不匹配DNS的请求split-dns域允许到其他DNS服务器，但是没有允许建立隧道DNS服务器。如果非split-dns域的一查询通过通道，尝试在这种情况下， AnyConnect驱动程序回应'没有这样名

称'。那么非split-dns域可以只是解决的通过公共DNS服务器通道的外部。

AnyConnect 4.2 +

只要他们起源于VPN适配器，匹配split-dns域的DNS请求允许到所有DNS服务器。如果查询由公共接口产生， AnyConnect驱动程序回应'没有这样名称'强制解析程序总是使用通道名字解析。split-dns域可以只所以是解决的通过通道。

只要他们起源于物理适配器，不匹配DNS的请求split-dns域允许到所有DNS服务器。如果查询由VPN适配器产生， AnyConnect回应'没有这样名称'强制解析程序通过公共接口始终尝试名字解析。那么非split-dns域可以只是解决的通过公共接口。

Mac OS X

通道所有配置(和分割隧道用启用的通道所有DNS)

当AnyConnect连接时，只有通道DNS服务器在系统DNS配置并且DNS请求维护能只发送到通道DNS服务器。

已分解包括配置(禁用的通道所有DNS和split-dns)

AnyConnect不干涉本地DNS解析程序。通道DNS服务器配置作为首选的解析程序，优先于公共DNS服务器，因而保证初始DNS要求名字解析在通道发送。因为DNS设置是全局在Mac OS X，使用公共DNS服务器通道的外部如提供在CSCtf20226上DNS查询是不可能的。开始与AnyConnect 4.2，通道DNS服务器的主机路由由AnyConnect客户端自动地添加和已分解包括网络(请保护路由)，并且已分解包括access-list不再要求通道DNS服务器子网的明确新增内容。

已分解排除配置(禁用的通道所有DNS和split-dns)

AnyConnect不干涉本地DNS解析程序。通道DNS服务器配置作为首选的解析程序，优先于公共DNS服务器，因而保证初始DNS要求名字解析在通道发送。因为DNS设置是全局在Mac OS X，使用公共DNS服务器通道的外部如提供在CSCtf20226上DNS查询是不可能的。开始与AnyConnect 4.2，通道DNS服务器的主机路由由AnyConnect客户端自动地添加和已分解包括网络(请保护路由)，并且已分解包括access-list不再要求通道DNS服务器子网的明确新增内容。

Split-dns (禁用的通道所有DNS，已分解包括已配置的)

如果split-dns为两IP协议(IPv4和IPv6)启用或为一份协议只启用，并且没有为另一份协议配置的地址池：
真的split-dns，类似于Windows，被强制执行。真的split-dns意味着匹配split-dns域的请求通过通道只是解决的，他们没有漏到DNS服务器通道的外部。

如果split-dns为一份协议只启用，并且客户端地址为另一份协议分配，只有"分割隧道的DNS fallback"被强制执行。这意味着AC只允许匹配split-dns域的DNS请求通过通道(其他请求由与"拒绝的"答复的AC应答强制故障切换到公共DNS服务器)，但是不能通过公共适配器强制执行匹配split-

dns域的请求无危险没有发送。

Linux

通道所有配置(和分割隧道用启用的通道所有DNS)

当AnyConnect连接时，只有通道DNS服务器在系统DNS配置并且DNS请求维护能只发送到通道DNS服务器。

已分解包括配置(禁用的通道所有DNS和split-dns)

AnyConnect不干涉本地DNS解析程序。通道DNS服务器配置作为首选的解析程序，优先于公共DNS服务器，因而保证初始DNS要求名字解析在通道发送。

已分解排除配置(禁用的通道所有DNS和split-dns)

AnyConnect不干涉本地DNS解析程序。通道DNS服务器配置作为首选的解析程序，优先于公共DNS服务器，因而保证初始DNS要求名字解析在通道发送。

Split-dns (禁用的通道所有DNS，已分解包括已配置的)

如果split-dns启用，只有“分割隧道的DNS fallback”被强制执行。这意味着AC只允许匹配split-dns域的DNS请求通过通道(其他请求由与“拒绝的”答复的AC应答强制故障切换到公共DNS服务器)，但是不能通过公共适配器强制执行匹配split-dns域的请求无危险没有发送。

漫游客户端的OpenDNS

漫游的客户端是管理在终端的DNS服务的软件块，并且使用OpenDNS公共DNS服务器巩固和加密DNS流量。

理论上来讲，客户端应该在一已保护和已加密状态。然而，如果客户端无法建立一个TLS会话用OpenDNS公共解析程序服务器(208.67.222.222)，它尝试发送DNS流量未加密在UDP端口53到208.67.222.222。漫游的客户端完全使用IP地址208.67.222.222 OpenDNS的公共的解析程序(有一些其他例如208.67.220.220， 208.67.222.220和208.67.220.222)。漫游的客户端一次安装，树立127.0.0.1 (localhost)作为本地DNS服务器并且改写当前单个接口的DNS设置。当前DNS设置在本地resolv.conf文件存储(在Windows)在漫游客户端配置文件夹内。OpenDNS将备份通过AnyConnect适配器了解的那些DNS服务器。例如，如果192.168.92.2是在公共适配器的DNS服务器，OpenDNS在以下位置将创建resolv.conf ：

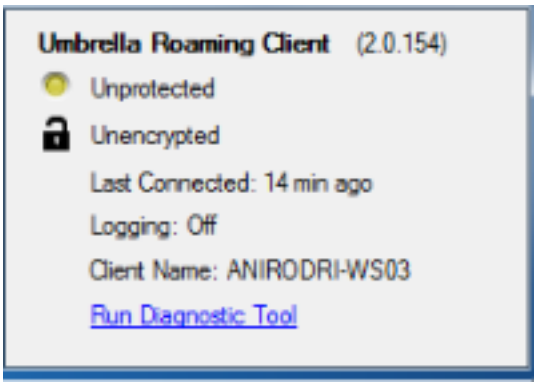
C:\ProgramData\OpenDNS\ERC\Resolver1-LocalAreaConnection-resolv.conf
nameserver 192.168.92.2

漫游的客户端将加密每数据包设置为OpenDNS;然而，它不启动也不使用加密隧道对208.67.222.222。 漫游的客户端有将打开non-DNS目的一个IPSec连接能阻塞IP地址的一个可选IP层执行功能。这在一活动AnyConnect连接面前将自动地禁用。它也绑定到127.0.0.1:53收到在计算机本地生成的查询。当终端需要解析名称时，本地查询处理对127.0.0.1由于覆盖，漫游的客户端的基础dnscrypt代理进程然后寄他们给在已加密信道的OpenDNS公共服务器。

如果DNS没有允许流到127.0.0.1:53，则漫游的客户端不能作用，并且下列将发生。 如果客户端无法到达公共DNS服务器或127.0.0.1:53限制地址，将过渡到一FAIL开放状态并且恢复在本地适配器的DNS设置。在背景，如果安全连接被重建，它继续发送探测器到208.67.222.222，并且能过渡到激活模式。

限制

查看两个客户端的高层次功能，是明显的漫游的客户端需要有能力更改本地DNS设置和绑定到127.0.0.1:53转送在安全信道间的查询。当VPN连接时， AnyConnect不干涉本地DNS解析程序的唯一的配置是已分解包括和已分解排除(当已分解通道所有DNS禁用)。所以，当漫游的客户端也是在使用中的时，当前推荐使用那些配置之一。漫游的客户端将留在一无保护/未加密状态是否使用通道所有配置，如镜像所显示，或者已分解通道所有DNS启用。



解决方法

如果目的是保护漫游的客户端之间的通信，并且OpenDNS服务器使用VPN建立隧道，则虚拟在VPN头端已分解排除access-list可以使用。这将是最接近的事对全通道配置。如果没有这样需求，则请已分解包括能使用access-list不包括OpenDNS公共服务器的地方，或者已分解排除能使用access-list包括OpenDNS公共服务器的地方。

另外，当曾经漫游的客户端，不可能使用时split-dns模式，因为这将导致本地DNS解决方法损耗。已分解通道所有DNS应该也依然是已禁用;然而，部分地支持它并且应该允许漫游的客户端变为已加密POST故障切换。

配置

通道OpenDNS流量

此示例在已分解排除使用一个假的IP地址access-list。使用此配置，与208.67.222.222的所有通信在VPN通道间发生，并且漫游的客户端在一已加密和已保护状态经营。

```
ciscoasa# sh run access-li split
access-list split standard permit host 2.2.2.2

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

从VPN通道排除OpenDNS流量

此示例在已分解排除使用OpenDNS解析程序地址access-list。使用此配置，与208.67.222.222的所有通信VPN通道的外部发生，并且漫游的客户端在一已加密和已保护状态经营。

```
ciscoasa# sh run access-li split
access-list split standard permit host 208.67.222.222

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy excludespecified
 split-tunnel-network-list value split
 default-domain value cisco.com
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#
```

此示例显示一内部192.168.1.0/24子网的一已分解包括配置。使用此配置，因为对208.67.222.222的流量没有通过通道，发送漫游的客户端在一已加密和已保护状态将经营。

```
ciscoasa# sh run access-li split
access-list split standard permit 192.168.1.0 255.255.255.0

ciscoasa# sh run group-policy
group-policy GroupPolicy-OpenDNS internal
group-policy GroupPolicy-OpenDNS attributes
 wins-server none
 dns-server value 1.1.1.1
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com
```

```
 address-pools value acpool
 webvpn
 anyconnect profiles value AnyConnect type user
ciscoasa#

Note: Split-tunnel-all-dns must be disabled in all of the  scenarios
```

验证

当VPN连接时，如此镜像所显示，漫游的客户端应该显示已保护和已加密：