ASA 8.X：路由SSL VPN流量通过被建立隧道的默认网关配置示例

目录

简介

本文描述如何配置可适应安全工具(ASA)通过被建立隧道的默认网关(TDG)路由SSL VPN流量。当您创建有被建立隧道的选项的时一个默认路由，从终止在不可能路由使用获知或静态路由的ASA的通道的所有流量发送到此路由。对于涌现从通道的流量，此路由改写所有其他配置的或了解的默认路由。

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

- 在版本8.x运行的ASA
- Cisco SSL VPN客户端(SVC) 1.x**注意：** 请从 Cisco 软件下载中下载 SSL VPN Client 程序包 (sslclient-win*.pkg)（仅限仅限注册用户）。将 SVC 复制到 ASA 上的闪存中。SVC需要下载到远程用户计算机为了建立与ASA的SSL VPN连接。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本8.x的Cisco 5500系列ASA

- 适用于 Windows 1.1.4.179 的 Cisco SSL VPN Client 版本
- 运行 Windows 2000 Professional 或 Windows XP 的 PC
- Cisco Adaptive Security Device Manager (ASDM)版本6.1(5)

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。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

SSL VPN 客户端 (SVC) 是一种 VPN 隧道技术，这种技术让远程用户可以利用 IPsec VPN 客户端的优势，而无需网络管理员在远程计算机上安装和配置 IPsec VPN 客户端。SVC 使用远程计算机上已经具有的 SSL 加密以及安全设备的 WebVPN 登录和身份验证。

在当前方案中，有连接对在ASA后的内部资源的SSL VPN客户端通过SSL VPN通道。独立的隧道没有启用。当SSL VPN客户端连接对ASA，所有数据将被建立隧道。除访问内部资源以外，主要标准是路由此通道流量通过默认被建立隧道的网关(DTG)。

您能与标准的默认路由一起定义通道流量的一个分开的默认路由。ASA接收的未加密的数据流，没有静态或获取的路由，通过标准的默认路由路由。ASA接收的加密流量，没有静态或获取的路由，将通过对通过被建立隧道的默认路由定义的DTG。

为了定义一个被建立隧道的默认路由，请使用此命令：

```
route <if_name> 0.0.0.0 0.0.0.0 <gateway_ip> tunneled
```

配置

本部分提供有关如何配置本文档所述功能的信息。

注意： 使用命令查找工具（仅限注册用户）可获取有关本部分所使用命令的详细信息。

网络图

本文档使用以下网络设置：

在本例中， SSL VPN客户端通过通道访问ASA的网络内部。为目的地含义的流量除网络内部之外通过TDG (192.168.100.20)也被以隧道传输，尽管没有配置的独立的隧道和路由。

在数据包路由对TDG后，在这种情况下是Router2，进行地址转换路由那些数据包向前到互联网。关于配置一个路由器的更多信息作为互联网网关，参考如何配置一个Cisco路由器在非思科有线调制解调器背后。

ASA配置使用ASDM 6.1(5)

本文采取基本配置，例如接口配置，适当地是完成和工作。

注意： 参考允许HTTPS访问ASDM关于如何允许ASDM将配置的ASA的信息。

注意： 除非更换端口号，否则无法在同一 ASA 接口上启用 WebVPN 和 ASDM。有关详细信息，请参阅在相同 ASA 接口上同时启用 Webvpn 和 ASDM。

通过使用SSL VPN向导，完成这些步骤为了配置SSL VPN。

1. 从向导菜单，请选择**SSL VPN向导**。
2. 点击**Cisco SSL VPN客户端**复选框，并且**其次**单击。
3. 在连接名名称字段输入一名称对于连接，然后选择由用户使用访问从SSL VPN接口下拉列表的SSL VPN的接口。
4. 单击 **Next**。
5. 选择认证模式，并且**其次**单击。(此示例使用本地认证。)
6. 除现有默认组策略之外，创建一项新的组策略。
7. 创建将分配到SSL VPN客户端PCs他们一次得到连接地址的新池。范围192.168.10.40-192.168.10.50的池是创建的名义上*newpool*。
8. 单击**浏览**为了选择和上载SSL VPN客户端镜像到ASA的闪存。
9. 点击**加载**为了设置文件路径从计算机的本地目录。
10. 单击**浏览本地文件**为了选择sslclient.pkg文件存在的目录。
11. 点击**上传文件**为了上传选定文件到ASA闪存。
12. 一旦文件上传对ASA闪存，请点击OK键完成该任务。
13. 现在它显示最新的anyconnect pkg文件上传对ASA闪存。单击 **Next**。
14. SSL VPN客户端配置的摘要显示。点击**芬通社**完成向导。

在ASDM显示的配置主要适合于对SSL VPN客户端向导配置。

在CLI中，您能观察某更多的配置。完整CLI配置如下所示，并且重要命令突出显示了。

ciscoasa

```
ciscoasa#show running-config : Saved : ASA Version
8.0(4) ! hostname ciscoasa enable password
8Ry2YjIyt7RRXU24 encrypted names ! interface Ethernet0/0
nameif outside security-level 0 ip address 209.165.201.2
255.255.255.224 ! interface Ethernet0/1 nameif inside
security-level 100 ip address 192.168.100.2
255.255.255.0 ! interface Ethernet0/2 nameif manage
security-level 0 ip address 10.1.1.1 255.255.255.0 !
interface Ethernet0/3 shutdown no nameif no security-
level no ip address ! interface Ethernet0/4 shutdown no
nameif no security-level no ip address ! interface
Ethernet0/5 shutdown no nameif no security-level no ip
address ! passwd 2KFQnbNIdI.2KYOU encrypted ftp mode
passive access-list nonat extended permit ip
192.168.100.0 255.255.255.0 192.168.10.0 255.255.255.0
access-list nonat extended permit ip 192.168.10.0
255.255.255.0 192.168.100.0 255.255.255.0 !--- ACL to
define the traffic to be exempted from NAT. no pager
logging enable logging asdm informational mtu outside
1500 mtu inside 1500 mtu manage 1500 !--- Creating IP
address block to be assigned for the VPN clients ip
local pool newpool 192.168.10.40-192.168.10.50 mask
255.255.255.0 no failover icmp unreachable rate-limit 1
burst-size 1 asdm image disk0:/asdm-615.bin no asdm
history enable arp timeout 14400 global (outside) 1
interface nat (inside) 0 access-list nonat !--- The
traffic permitted in "nonat" ACL is exempted from NAT.
nat (inside) 1 192.168.100.0 255.255.255.0 route outside
0.0.0.0 0.0.0.0 209.165.201.1 1 !--- Default route is
configured through "inside" interface for normal
```

```
traffic. route inside 0.0.0.0 0.0.0.0 192.168.100.20
tunneled !--- Tunneled Default route is configured
through "inside" interface for encrypted traffic !
timeout xlate 3:00:00 timeout conn 1:00:00 half-closed
0:10:00 udp 0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00
h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00
sip-disconnect 0:02:00 timeout uauth 0:05:00 absolute
dynamic-access-policy-record DfltAccessPolicy http
server enable !--- Configuring the ASA as HTTP server.
http 10.1.1.0 255.255.255.0 manage !--- Configuring the
network to be allowed for ASDM access. ! !--- Output is
suppressed ! telnet timeout 5 ssh timeout 5 console
timeout 0 threat-detection basic-threat threat-detection
statistics access-list ! class-map inspection_default
match default-inspection-traffic ! ! policy-map type
inspect dns preset_dns_map parameters message-length
maximum 512 policy-map global_policy class
inspection_default inspect dns preset_dns_map inspect
ftp inspect h323 h225 inspect h323 ras inspect netbios
inspect rsh inspect rtsp inspect skinny inspect esmtp
inspect sqlnet inspect sunrpc inspect tftp inspect sip
inspect xdmcp ! service-policy global_policy global ! !-
-- Output suppressed ! webvpn enable outside !--- Enable
WebVPN on the outside interface svc image
disk0:/sslclient-win-1.1.4.179.pkg 1 !--- Assign the
AnyConnect SSL VPN Client image to be used svc enable !-
-- Enable the ASA to download SVC images to remote
computers group-policy grppolicy internal !--- Create an
internal group policy "grppolicy" group-policy grppolicy
attributes VPN-tunnel-protocol svc !--- Specify SSL as a
permitted VPN tunneling protocol ! username cisco
password ffIRPGpDSOJh9YLq encrypted privilege 15 !---
Create a user account "cisco" tunnel-group Test type
remote-access !--- Create a tunnel group "Test" with
type as remote access tunnel-group Test general-
attributes address-pool newpool !--- Associate the
address pool vpnpool created default-group-policy
grppolicy !--- Associate the group policy "clientgroup"
created prompt hostname context
Cryptochecksum:1b247197c8ff70ee4432c13fb037854e : end
ciscoasa#
```

验证

在此部分给的命令可以用于验证此配置。

命令输出解释程序（仅限注册用户）(OIT) 支持某些 **show** 命令。使用 OIT 可查看对 show 命令输出的分析。

- **显示WebVPN svc** — —显示在ASA闪存存储的SVC镜像。
- **show vpn-sessiondb svc** — 显示有关当前 SSL 连接的信息。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- Cisco ASA 5500系列自适应安全设备支持
- 单臂路由器上用于公共 Internet 的 PIX/ASA 和 VPN 客户端配置示例
- 在 ASA 上用 ASDM 配置 SSL VPN Client (SVC) 的示例
- 技术支持和文档 - Cisco Systems