分割路由配置的安全访问目标地址

目录

问题

在集中星型网络架构中的Windows终端上部署具有思科安全客户端(CSC)的思科安全访问(CSA)时，组织最可能需要配置拆分路由，以允许分支站点流量通过本地分支互联网电路直接连接到CSA，而不是通过中心进行发夹连接。此配置需要了解建立CSA隧道时使用的所有Cisco目标地址，以便在网络设备（例如防御性防火墙）上定义路由例外（分支/分割路由）。

具体要求是在建立TLS/DTLS隧道时识别CSC使用的CSA终端的所有目标信息（IP地址或URL），从而正确配置绕过CSA流量的中心分支VPN隧道的路由策略。

环境

- 思科安全访问(CSA)部署
- Windows终端上的思科安全客户端(CSC)
- 带有防御防火墙的中心辐射型网络拓扑
- 与CSA的TLS/DTLS隧道连接

分辨率

要配置思科安全访问连接的拆分路由，必须在Fortigate设备上配置以下各节中描述的目标信息，以允许直接连接到CSA终端。

CSA目标域和端口

主域

```
*.vpn.sse.cisco.com
```

所需的端口和协议

- TCP/UDP 443:用于TLS/DTLS隧道建立
- UDP 500/4500:用于IPsec隧道建立
- TCP 80:用于VPN证书吊销检查

防御配置方法

在Fortigate设备上配置路由策略，以通过本地辐条Internet电路（而不是通过中心辐条VPN隧道）将发往CSA域(*.vpn.sse.cisco.com)和指定端口的流量定向到。这将启用下一代码片断中概述的流量。

所需的流量

```
Spoke Site → CSA Tunnel Connection → CSA-mediated Internet Communication
```

而不是通过中心站点的流量

```
Spoke Site → Hub Site → CSA Tunnel Connection → CSA-mediated Internet Communication
```

重要注意事项

CSA连接目标是在运行时动态确定的，这意味着特定IP地址不能预先用于静态路由配置。使用*.vpn.sse.cisco.com的基于域的方法提供了配置拆分路由策略的最可靠方法。

请参考官方Cisco Secure Access文档，了解最新的目标和端口要求，因为这些要求很可能使用新的软件版本进行更新。

原因

在集中星型网络拓扑中，默认情况下，来自分支站点的所有互联网绑定流量通常通过中心站点路由。当使用CSC实施CSA时，此默认路由行为会导致CSA隧道流量在到达CSA终端之前通过集线器站点形成发夹，从而可能导致延迟和带宽低效。CSA终端选择的动态性质需要基于域的路由策略，而不是基于静态IP的规则，以确保适当的拆分路由功能。

相关内容

- 思科安全访问文档 — 连接要求
- 思科安全访问文档 — 网络配置
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。