分割路由配置的安全訪問目標地址

目錄

問題

在中心輻射型網路架構中的Windows端點上部署思科安全訪問(CSA)和思科安全客戶端(CSC)時，組織最可能需要配置分割路由，以允許分支站點流量通過本地分支網際網路電路直接連線到CSA，而不是通過中心進行迴轉傳輸。此配置要求瞭解建立CSA隧道時使用的所有Cisco目的地址，以便可以在網路裝置（如防禦性防火牆）上定義路由例外（分支/分割路由）。

具體要求是在建立TLS/DTLS隧道時，確定CSC使用的CSA終端的所有目標資訊（IP地址或URL），從而正確配置繞過CSA流量的中心分支VPN隧道的路由策略。

環境

- 思科安全存取(CSA)部署
- Windows終端上的思科安全使用者端(CSC)
- 具有防禦性防火牆的集中型網路拓撲
- TLS/DTLS隧道連線到CSA

解析

要為思科安全訪問連線配置拆分路由，必須在防禦裝置上配置下一節中描述的目的地資訊，以允許直接連線到CSA終端。

CSA目標域和埠

主域

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

所需的埠和協定

- TCP/UDP 443:用於TLS/DTLS隧道建立
- UDP 500/4500:用於IPsec隧道建立
- TCP 80:用於VPN證書吊銷檢查

防禦配置方法

在Fortigate裝置上配置路由策略，以通過本地輻條Internet電路（而不是通過中心輻條VPN隧道）將目的地為CSA域(*.vpn.sse.cisco.com)和指定埠的流量定向到CSA域。這將啟用下一代碼片斷中概述的流量。

所需的流量

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

而不是通過中心站點的流量

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

重要注意事項

CSA連線目標是在運行時動態確定的，這意味著特定IP地址不能預先用於靜態路由配置。使用*.vpn.sse.cisco.com的基於域的方法提供了配置拆分路由策略的最可靠方法。

請參考官方Cisco Secure Access文檔，瞭解最新的目的地和埠要求，因為這些要求很可能使用新軟體版本進行更新。

原因

在中心輻射型網路拓撲中，預設情況下，來自輻射型站點的所有網際網路通訊通常都通過中心站點路由。當使用CSC實施CSA時，此預設路由行為會導致CSA隧道流量在到達CSA端點之前通過集線器站點進行迂迴，從而可能導致延遲和頻寬低效。CSA端點選擇的動態性質要求基於域的路由策略，而不是基於靜態IP的規則，以確保正確的拆分路由功能。

相關內容

- 思科安全存取檔案 — 連線要求
- 思科安全存取檔案 — 網路組態
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。