配置安全訪問的選項和VPN功能（中國）

目錄

問題

分析Cisco Secure Access中國部署的VPN功能的組織需要澄清加密支援和操作限制。具體來說，以下問題包括：部署在中國大陸的思科安全防火牆裝置是否正式支援IPsec VPN(IKEv1/IKEv2)、為什麼通常建議使用GRE隧道以及存在哪些先決條件或替代方案來實現安全通訊。此外，從AWS中國的虛擬檢查點防火牆遷移到FTD平台以與AWS Transit Gateway建立連線時，需要瞭解對GRE通道的支援。

環境

- 思科安全接入中國（雲交付的安全服務邊緣解決方案）
- 思科在中國大陸的安全防火牆部署
- FTD平台遷移方案
- AWS China Transit Gateway連線要求
- 僅支援GRE的虛擬檢查點防火牆環境

解析

思科安全訪問中國提供全面的VPN功能，以及特定的協定支援和配置選項：

IPsec VPN支援

思科安全訪問中國僅支援使用IKEv2協定的IPsec VPN。此部署模型不支援IKEv1。支援的IPsec引數和配置選項在官方Cisco Secure Access China文檔中記錄。

IPsec支援的主要特徵：

- 以獨佔方式支援IKEv2協定。
- 不需要特殊的韌體或加密映像。
- 雲交付的安全服務邊緣(SSE)解決方案。
- 標準IPsec引數配置可用。

高可用性選項

為了提高可靠性，思科安全接入中國網路隧道組支援具有高可用性功能的主集線器和輔助集線器配置。

原因

未發現具體原因。

相關內容

- Cisco Secure Access中國IPsec引數
- Cisco Secure Access中國GRE配置
- 支援的IPsec引數文檔
- 網路通道組高可用性
- VPN部署使用手冊
- 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）。