安全訪問基於客戶端的ZTA狀態配置和行為規範

目錄

問題

使用思科安全訪問客戶端型零信任訪問(ZTA)安全狀態功能進行網際網路訪問時，出現有關具體行為和配置功能的問題。具體關注事項包括：

- 作業系統狀態要求是否支援可配置的寬限期（最長365天），在此期間，即使裝置不符合要求的作業系統版本，裝置仍可使用ZTA模組訪問網際網路目標。
- 除了作業系統（如防火牆、系統密碼等）之外，安全狀態要求是否會導致在無法滿足時立即阻止目標訪問。
- 是否可以通過安全訪問GUI介面為安全狀態要求故障配置自定義警告消息或除阻止之外的操作（如監控）。

環境

- 具有零信任訪問(ZTNA)功能的思科安全訪問
- 基於客戶端的ZTA狀態實施
- Internet訪問使用案例場景
- 安全狀態要求，包括作業系統、防火牆和系統密碼條件

解析

下面幾節中介紹的有關安全訪問基於客戶端的ZTA狀態行為和配置功能的說明。

作業系統狀態寬限期

描述的作業系統狀態要求行為是正確的。配置作業系統狀態條件時，它支援可配置的寬限期（最多365天）。在此寬限期內，不滿足所需作業系統版本的裝置在升級到目標版本時，仍然可以使用ZTA模組訪問網際網路目標。

非作業系統狀態要求

對於作業系統以外的終端安全評估條件（例如防火牆、系統密碼和其他安全控制），當這些要求未滿足時，會立即阻止對目標的訪問。這些終端安全評估型別不支援作業系統要求的寬限期功能。

狀態故障操作和自定義消息

狀態要求失敗的操作通過訪問策略配置進行控制。

訪問策略支援多種操作型別，包括：

- 允許
- 封鎖
- 警告
- 隔離

可以通過Access Policy Security配置檔案設定配置安全評估失敗的自定義警告消息和通知頁面。通過管理通知頁面文檔和配置介面處理警告和通知頁面管理。

這意味著除阻止之外的其他操作（如通過「警告」操作進行監視）是可用的，並且可以進行配置，這與只可能存在阻止操作的初始評估相反。

原因

這些問題源於需要瞭解作業系統狀態要求和其他狀態型別之間的具體行為差異，以及澄清安全訪問GUI介面中無法立即顯現的狀態故障處理的可用配置選項。

相關內容

- 管理Secure Access通知頁面文檔
- 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）。