驗證Cisco安全訪問中的IPS解密

目錄

問題

通過安全客戶端使用Cisco Secure Access with RAVPN(Remote Access VPN)時，組織需要驗證IPS（入侵防禦系統）解密和檢查是否針對到特定網站的流量正確執行。主要難題是確認TLS解密和檢查進程是否通過標準管理UI日誌以外的其他方法（如「活動搜尋」）正常工作。具體驗證要求包括確定客戶端證書檢查或調試/報告機制，這些機制可支援測試驗證並提供管理介面以外IPS操作的附加確認。

環境

- 具備RAVPN功能的思科安全訪問(CSA)
- 適用於遠端存取VPN連線的Cisco安全使用者端
- 已啟用IPS解密和檢測功能
- 需要解密以進行安全檢查的TLS/SSL流量
- 從RAVPN客戶端到外部網站的Web流量

解析

有兩種方法可以驗證IPS解密和檢查是否在Cisco安全訪問中的遠端訪問VPN流量中正常工作：

方法1:管理UI活動搜尋（主要方法）

思科安全訪問管理介面中的活動搜尋功能提供了最可靠的方法來確認IPS解密和檢查操作。此介面顯示詳細日誌和分析顯示安全服務對流量進行解密和檢查的時間。

要訪問「活動搜尋」，請執行以下操作：

導航到Cisco Secure Access管理控制面板並找到Activity Search功能，以檢視特定使用者會話和目標網站的流量檢測日誌和解密狀態。

要啟用解密日誌，可以在全域性設定上啟用此設定：

控制面板 — >安全 — >訪問策略 — >規則預設值和全域性設定 — >全域性設定 — >解密記錄。

方法2:客戶端證書驗證

作為額外的驗證方法，您可以執行客戶端證書檢查以確認正在發生流量解密。

當Cisco Secure Access成功解密並檢查TLS流量時，它會向客戶端顯示自己的證書，而不是原始網站證書。

通過證書檢查驗證解密：

1.檢查網站證書
在瀏覽器中開啟證書詳細資訊，並檢視頒發者和有效期。

如果憑證是由思科安全存取根CA核發，有效期約為10天，則表示入侵防禦系統在防火牆層級進行解密。

如果證書有效性大約為5天，則表示基於安全Web網關的解密。

2.驗證證書頒發者（DC命名）

此客戶端證書驗證方法與主要活動搜尋方法一起用作補充確認技術，從而進一步確保IPS解密過程按預期運行。

入侵防禦系統不解密：

如果 — ，將進行入侵防禦系統的解密

·它在全域性設定下啟用，且

·至少為其中一個訪問策略規則啟用了入侵防禦系統（我相信，即使禁用了規則，此條件仍然適用）

要繞過入侵防禦系統解密的域

使用系統提供的不解密清單並在系統提供的不解密清單中新增域。

或

在「思科安全訪問的全域性設定」下利用基於源的解密 —

注意：如果在安全訪問的網路隧道配置上沒有配置出站NAT，則此操作將起作用。

原因

需要多種驗證方法是因為需要在企業環境中驗證安全策略實施。雖然管理UI日誌提供了全面的可視性，但客戶端驗證方法提供了額外的確認點，這些確認點對於合規性測試、故障排除以及驗證場景非常有用，在這些場景中，直接訪問管理介面可能受到限制，或者全面測試過程需要多個驗證點。

相關內容

- 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）。