如何使用思科網路安全裝置重新導向URL?

目錄

問題

如何使用思科網路安全裝置重新導向URL?

環境

運行任何AsyncOS版本的思科網路安全裝置(WSA)。

除了使用思科網路安全裝置監控和阻止到特定網站的流量外，您還可以使用它來將使用者重定向到其他網站。您可以將裝置配置為將最初發往URL或網站的流量重定向到使用自定義URL類別指定的位置。這允許您重定向裝置上的流量，而不是重定向目標伺服器。

對於HTTP流量

1. 建立自訂URL類別(**GUI > Web安全管理員 > 自訂URL類別**)，並包含您要重新導向的URL。

2. 在相關的訪問策略(**GUI > Web Security Manager > Access Policies > URL Categories**)中包含此新的自定義URL類別。

3. 在「自定義URL類別……」部分，選擇相關的「自定義URL」類別，選擇「設定」列下的**Include**，然後選擇相關自定義URL類別的**Redirect**選項。

4. 選擇Redirect選項後，Custom URL Category名稱下將顯示一個文本框。在此文本框中，輸入要重新定向請求的URL。

對於HTTPS流量

預設情況下，無法像HTTP URLs那樣重新導向HTTPS URL。若要重新導向HTTPS URL，必須首先對其進行解密(**GUI > Web Security Manager > Decryption Policy**)。 HTTPS URL解密後，將接受訪問策略。然後，可以在「訪問策略」下重定向HTTPS URL。

1. 建立自定義URL類別(**GUI > Web Security Manager > Custom URL Category**)，並包含您要重定向的URL。

2. 在相關的訪問策略(GUI > Web Security Manager > Access Policies > URL Categories)和解密策略(GUI > Web Security Manager > Decryption Policy > **URL Categories**)中包含此新的自定義URL類別。

3. 在Decryption Policy中，為包含的自定義URL類別選擇**Decrypt**選項。

4. 在Access Policy中，為包含的自定義URL類別選擇**Redirect**選項。

5. 選擇Redirect選項後，Custom URL Category名稱下將顯示一個文本框。在此文本框中，輸入您希望請求重定向到的URL。