網路安全裝置設計手冊

目錄

[簡介](#)
[背景資訊](#)
[設計](#)
[網路](#)
[一般注意事項](#)
[負載平衡](#)
[防火牆](#)
[身份](#)
[訪問/解密/路由/出站惡意軟體策略](#)
[自訂URL類別](#)
[防惡意軟體和信譽](#)

簡介

本檔案介紹如何設計思科網路安全裝置(WSA)及相關元件以取得最佳效能。

背景資訊

當您為WSA設計解決方案時，需要仔細考慮，不僅要考慮裝置本身的配置，還要考慮相關的網路裝置及其功能。每個網路都是多個裝置的合作，如果其中一個裝置不能正確參與網路，使用者體驗可能會下降。

配置WSA時必須考慮兩個主要元件：硬體和軟體。硬體有兩種型別。第一個是硬體物理型別，如S170、S380和S680系列型號，以及其他壽命終止(EoL)型號，如S160、S360、S660、S370和S670系列型號。另一種硬體型別是虛擬的，例如S000v、S100v和S300v系列型號。在此硬體上運行的作業系統(OS)稱為*AsyncOS for Web*，其核心基於FreeBSD。

WSA提供代理服務，還可以掃描、檢查所有流量並將其分類(HTTP、HTTPS和檔案傳輸協定(FTP))。 所有這些協定都是在TCP之上運行的，並且嚴重依賴域名系統(DNS)來實現正常運行。因此，網路運行狀況對於裝置的正常運行及其與網路各部分（包括企業控制內部和外部部分）的通訊至關重要。

設計

使用本節中介紹的資訊來設計WSA和相關元件以獲得最佳效能。

網路

無錯誤、快速的網路對於WSA的正確運行至關重要。如果網路不穩定，使用者體驗可能會下降。網路問題通常是在網頁到達時間較長或無法訪問時檢測到的。最初的傾向是歸咎於裝置，但通常都是網路行為不當。因此，為確保網路為HTTP、HTTPS、FTP和DNS等高級應用協定提供最佳服務，應認真考慮和稽核。

一般注意事項

以下是您可以實作的一些一般注意事項，以確保最佳網路行為：

- 確保第2層(L2)網路穩定，生成樹操作正確，並且沒有頻繁的生成樹計算和拓撲更改。
- 使用的路由協定也應提供快速收斂性和穩定性。開放最短路徑優先(OSPF)快速計時器或增強型內部閘道路由通訊協定(EIGRP)是此類網路的良好選擇。
- 始終在WSA上至少使用兩個資料介面：一個面向終端使用者電腦，另一個用於出站操作（連線到上游代理或網際網路）。 這樣做是為了消除可能存在的資源限制，例如當耗盡TCP埠數量或網路緩衝區滿時（特別是內部和外部使用單個介面）。
- 將管理介面專門用於純管理流量，以提高安全性。為了通過GUI實現這一目的，請導航至**Network > Interfaces**，然後選中**Separate routing（M1埠僅限裝置管理服務）**覈取方塊。
- 使用快速DNS伺服器。任何通過WSA的事務至少需要一個DNS查詢（如果沒有在快取中）。DNS伺服器速度慢或行為不當會影響任何事務，並被視為延遲或緩慢的Internet連線。
- 使用單獨的路由表時，以下規則適用：

  所有介面都包含在預設的*Management*路由表中(M1、P1、P2)。

  資料路由表中只包含*數據*介面。

  附註：路由表的分離不是基於每個介面，而是基於服務。例如，WSA和Microsoft Active Directory(AD)域控制器之間的流量始終遵循管理路由表中指定的路由，並且可以在此表中配置指向P1/P2介面的路由。在資料路由表中不能包含使用管理介面的路由。

負載平衡

為確保最佳網路行為，您可以實施以下一些負載均衡注意事項：

- DNS輪替 — 這是將單個主機名用作代理，但是在DNS伺服器上有多個A記錄時使用的術語。每個客戶端都將此解析為不同的IP地址並使用不同的代理。一個限制是DNS記錄的更改會在重新啟動時反映在客戶端上（本地DNS快取），因此如果必須進行更改，其穩定性較低。但是，這對終端使用者是透明的。
- 代理地址控制(PAC)檔案 — 這些是代理自動指令碼檔案，用於根據瀏覽器中寫入的函式來確定應如何處理每個URL。它具有將同一URL總是直接轉送或轉送到同一代理的功能。
- 自動發現 — 這說明使用DNS/DHCP方法獲取PAC檔案（如前面的考慮中所述）。 通常，將前三個考慮事項合併到一個解決方案中。但是，這非常複雜，許多使用者代理（如Microsoft Office、Adobe Downloader、Javascripts和Flash）根本無法讀取PAC檔案。
- Web快取控制通訊協定(WCCP) — 此通訊協定（尤其是WCCP第2版）提供了一種強健且功能非常強大的方法，可在多個WSA之間建立負載平衡，並整合高可用性。

- 單獨的負載平衡裝置 — 思科建議您使用負載平衡器作為專用電腦。

防火牆

為確保最佳網路行為，您可以實施以下防火牆注意事項：

- 確保允許來自每個來源的整個網路中的網際網路控制訊息通訊協定(ICMP)。這一點非常重要，因為WSA取決於路徑最大轉換單元(MTU)探索機制(如RFC 1191所述)，該機制取決於ICMP回應請求(型別��和回應回覆（型別0）），並且需要ICMP無法到達分段（型別3，代碼4）。 如果使用**pathmtudiscovery** CLI指令在WSA上停用路徑MTU探索，則WSA會根據RFC 879使用預設MTU 576位元組。這會因為額外負荷增加和封包重組而影響效能。

- 確保網路內部沒有非對稱路由。雖然這在WSA上不是問題，但路徑上遇到的任何防火牆都會丟棄資料包，因為它沒有收到通訊的兩端。

- 使用防火牆時，將WSA IP地址從威脅中排除為常規終端電腦工作站非常重要。防火牆可能會阻止
- 由於連線過多（根據一般防火牆知識）而產生的WSA IP地址。

- 如果客戶設施裝置上的任何WSA IP地址都使用了網路地址轉換(NAT)，請確保每個WSA在NAT中使用單獨的外部全域性地址。如果對具有單個外部全域性地址的多個WSA使用NAT，可能會遇到以下問題：

  從所有WSA到外部世界的所有連線都使用單個外部全域性地址，並且防火牆很快耗盡資源。

  如果流向該單一目標的流量激增，則目標伺服器可能會阻止該流量，並切斷整個企業對此資源的訪問。這可能是公司雲端儲存、Office雲連線或每台電腦的防病毒軟體更新的寶貴資源。

身份

請記住，*邏輯AND原*則適用於標識的所有元件。例如，如果同時配置使用者代理和IP地址，則表示來自此IP地址的*用戶*代理。這並不意味著使用者代理或*此*IP地址。

使用同一身份對相同代理型別（或無代理）和/或使用者代理進行身份驗證。

對於支援代理身份驗證的已知瀏覽器/使用者代理（例如Internet Explorer、Mozilla Firefox和Google Chrome），確保每個需要身份驗證的身份包含使用者代理字串非常重要。有些應用程式需要訪問Internet，但不支援代理/WWW身份驗證。

標識自上而下與搜尋第一個匹配條目結尾的匹配項相匹配。因此，如果配置了*Identity 1*和*Identity 2*，並且事務與Identity 1匹配，則不會根據身份2對其進行檢查。

訪問/解密/路由/出站惡意軟體策略

這些策略針對不同型別的流量應用：

- 訪問策略應用於純HTTP或FTP連線。它們確定是接受還是丟棄該事務。

- 解密策略確定HTTPS事務是否應解密、丟棄或通過。如果事務被解密，則其連續部分可視為純

HTTP請求，並與訪問策略匹配。如果必須丟棄HTTPS請求，請將其放在解密策略中，而不是訪問策略中。否則，丟棄的事務先被解密，然後被丟棄，會消耗更多的CPU和記憶體。

- 路由策略確定事務允許通過WSA後的上游方向。如果存在上游代理，或者WSA處於*聯結器*模式並將流量傳送到雲網路安全塔，則此情況適用。

- 出站惡意軟體策略適用於從終端使用者到Web伺服器的HTTP或FTP上傳。這通常是HTTP Post請求。

對於每種型別的策略，必須記住邏輯或*原則適*用適用。如果您引用了多個身份，則事務應與配置的任何身份匹配。

要獲得更精細的控制，請使用以下策略。每個策略中錯誤配置的標識可能會產生問題，在這種情況下，使用策略中引用的多個標識更為有利。請記住，身份不會影響流量，它們只是識別策略中稍後匹配的流量型別。

通常，解密策略使用身份進行身份驗證。雖然這並非錯誤，有時也是必需的，但使用具有在解密策略中引用的身份驗證的身份意味著所有與解密策略匹配的事務都將被解密，以便進行身份驗證。解密操作可能遭捨棄或通過，但由於身份具有身份驗證，因此發生解密是為了稍後丟棄或通過流量。這是昂貴的，應該避免。

已觀察到包含30個或更多標識以及30個或更多訪問策略的某些配置，其中所有訪問策略包括所有標識。在這種情況下，如果所有訪問策略中均匹配了此多個身份，則無需使用這些身份。雖然這不會損害裝置操作，但會與故障排除嘗試產生混淆，而且效能方面成本很高。

自訂URL類別

使用自定義URL類別是WSA上功能強大的工具，通常會被誤解和誤用。例如，有些配置包含標識中所有匹配影片站點。WSA具有內建工具，可在影片站點更改URL時自動更新，這經常發生。因此，允許WSA自動管理URL類別，並將自定義URL類別用於尚未分類的特殊站點。

請務必小心正規表示式。如果使用特殊字元匹配(如圓點(.)和星號(*))，它們可能會被證明是非常廣泛的CPU和記憶體。WSA擴展任何正規表示式，使其與每個事務匹配。例如，下面是一個正規表示式：

```
example.*
```

此表達式將匹配包含單詞*example*的任何URL，而不僅是*example.com*域。避免在正規表示式中使用*dot*和*star*，並且僅將其用作最後的手段。

以下是可能會產生問題的正規表示式的另一個示例：

```
www.example.com
```

如果在「正規表示式」欄位中使用此示例，它不僅匹配*www.example.com*，而且還匹配*www.www3example2com.com*，因為此處的小點表示任*何字元*。如果希望僅匹配*www.example.com*，請轉義圓點：

```
www\.example\.com
```

在這種情況下，如果可以採用以下格式將其包括在自定義URL類別域中，則沒有理由使用「正規表示式」功能：

防惡意軟體和信譽

如果啟用了多個掃描引擎，請考慮同時啟用自適應掃描的選項。自適應掃描是WSA上的一個功能強大但很小的引擎，它預掃描每個請求，並確定掃描請求時應使用的綜合引擎。這稍微提高了WSA的效能。