使用安全Web裝置最佳實踐

目錄

簡介

本文檔介紹如何配置Cisco Secure Web Appliance (SWA)的最佳做法。

背景資訊

本指南旨在作為最佳實踐配置的參考，它涉及SWA部署的許多方面，包括支援的網路環境、策略配置、監控和故障排除。雖然此處記錄的最佳實踐對於所有管理員、架構師和操作員都很重要，但是它們只是指導原則，因此必須這樣對待。每個網路都有自己特定的要求和挑戰。

作為安全裝置，SWA以幾種獨特的方式與網路互動。它既是網路流量的源也是目標。它與Web伺服器和Web客戶端同時運行。它至少使用伺服器端IP地址欺騙和中間人技術來檢查HTTPS事務。它還可以欺騙客戶端IP地址，這會增加部署的複雜性，並對支援的網路配置提出額外的要求。本指南介紹了與網路裝置配置相關的最常見問題。

SWA策略配置不僅會影響安全效力和實施，還會影響裝置的效能。本指南說明配置的複雜性如何影響系統資源。它定義了此環境中的複雜性，並描述如何在策略設計中將其最小化。此外，還關注特定功能以及如何配置它們以提高安全性、可擴充性和有效性。

本文檔的「監控和警報」部分介紹了監控裝置的最有效方法；還介紹了效能和可用性的監控以及系統資源使用情況。它還提供了對基本故障排除有用的資訊。

網路環境

ICMP

路徑MTU發現(如RFC 1191中所定義)，此機制確定沿任意路徑的資料包的最大大小。在IPv4的情況下，裝置可以在封包的IP標頭中設定不分段(DF)位元，藉此判斷路徑上任何封包的最大傳輸單位(MTU)。如果沿著路徑的某個連結上的裝置無法在不對封包進行分段的情況下將其轉送，則會將需要網際網路控制訊息通訊協定(ICMP)分段（型別3，代碼4）訊息傳送回來源。然後使用者端重新傳送較小的封包。此作業會一直持續，直到找到完整路徑的MTU。IPv6不支援分段，並且使用Packet Too Big (Type 2) ICMPv6消息表示無法通過給定鏈路容納資料包。

由於資料包分段的過程可能對TCP流的效能產生嚴重影響，因此SWA使用路徑MTU發現。必須在相關網路裝置中啟用上述ICMP消息，以允許SWA確定其在網路中路徑的MTU。可使用 pathmtudiscovery 命令列介面(CLI)命令在SWA中停用此行為。這樣做會使預設MTU降至576位元組（根據RFC 879），嚴重影響效能。管理員必須採取額外步驟，以便從etherconfig CLI命令在SWA中手動配置MTU。

在採用Web快取通訊協定(WCCP)的情況下，Web流量會從另一個網路裝置沿著使用者端路徑重新導向至SWA，進而到達網際網路。在這種情況下，其他協定（例如ICMP）不會重定向到SWA。SWA可能會觸發來自網路上路由器的ICMP需要分段消息，但此消息不會傳送到SWA。如果網路中可能發生這種情況，則必須停用路徑MTU發現。如前所述，對於此配置，需要使用etherconfig CLI命令在SWA上手動設定MTU的附加步驟。

防火牆

在預設配置中，代理連線時，SWA不會欺騙客戶端IP地址。這意味著所有出站Web流量都來自SWA IP地址。必須確保網路地址轉換(NAT)裝置具有足夠大的外部地址和埠池來滿足此要求。為此，最好指定一個特定的地址。

某些防火牆採用拒絕服務(DoS)保護或其他安全功能，可在大量同時連線源自單個客戶端IP地址時觸發。如果未啟用客戶端IP欺騙，則必須將SWA IP地址從這些保護中排除。

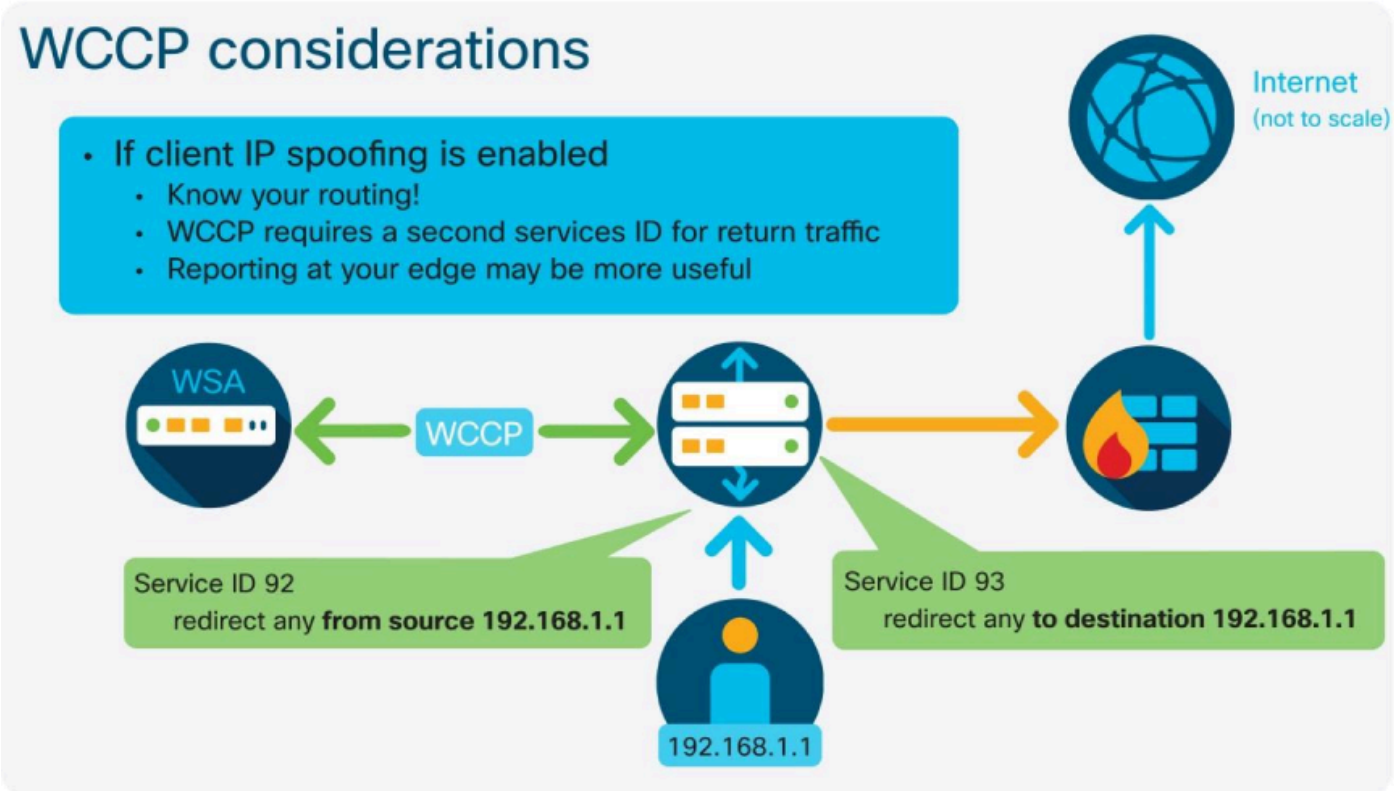
單點傳送反向路徑轉送

SWA在與客戶端通訊時欺騙伺服器IP地址，並且可選地被配置為在與上游伺服器通訊時欺騙客戶端IP地址。可在交換器上啟用單點傳送反向路徑轉送(uRPF)等保護，以確保傳入封包符合預期的輸入連線埠。這些保護根據路由表檢查資料包的源介面，以確保它到達預期埠。有必要酌情豁免《全部門會計準則》不受這些保護。

使用WCCP進行IP欺騙

在SWA中啟用IP欺騙功能時，出站請求會使用原始客戶端請求的源地址。這需要對相關網路基礎設施進行額外的配置，以確保返回的資料包被路由到SWA出站介面，而不是傳送請求的客戶端。

在網路裝置（路由器、交換機或防火牆）上實施WCCP時，會定義一個服務ID，該服務ID根據訪問控制清單(ACL)匹配流量。然後，服務ID將應用到介面，並用於匹配重定向流量。如果啟用了IP欺騙，必須建立第二個服務ID，以確保返回流量也重定向到SWA。



SWA網路配置

介面

SWA有五個可用的網路介面：M1、P1、P2、T1和T2。在可能的情況下，必須針對其特定目的使用其中每一項。由於各自的原因使用每個埠是有益的。M1介面必須連線到專用管理網路，並且必須啟用分割路由以限制管理服務的接觸。P1可以限制為客戶端請求流量，相反，P2不允許接受顯式代理請求。這可以減少每個介面上的流量並在網路設計中實現更好的分段。

T1和T2連線埠適用於第4層流量監控(L4TM)功能。此功能可監控映象的第2層埠，並根據已阻止的已知惡意IP地址和域名清單增加阻止流量的功能。它透過檢視流量的源和目標IP地址來執行此操作，並傳送TCP重置資料包或埠不可達消息（如果阻止的清單匹配）。使用此功能可以阻止透過任何協定傳送的流量。

即使未啟用L4TM功能，當T1和T2埠連線到映象埠時，透明旁路功能也可以增強。對於WCCP，SWA只知道傳入資料包的源和目標IP地址，必須根據此資訊決定代理或繞過它。無論記錄的生存時間(TTL)為何，SWA每30分鐘解析一次旁路設定清單中的任何條目。但是，如果啟用L4TM功能，SWA可以使用監聽的DNS查詢更頻繁地更新這些記錄。這降低了客戶端解析與SWA不同的地址時出現假負值的風險。

管理網路路由

如果專用管理網路無法訪問Internet，則可以將每項服務配置為使用資料路由表。這可以量身訂做以符合網路拓撲，但一般而言，建議對所有系統服務使用管理網路，對使用者端流量使用資料網路。自AsyncOS版本11.0起，可以設定路由的服務包括：

- 外部URL源
- 進階惡意軟體防護(AMP)檔案信譽和分析
- 更新和升級
- DNS
- Active directory

對於管理流量的其他出口過濾，可以配置靜態地址以用於以下服務：

- 外部URL源：
  1.自定義取決於託管位置
  2. AMP檔案信譽和分析
  3. cloud-sa.amp.cisco.com（北美）
  4. cloud-sa.eu.amp.cisco.com（歐洲）
  5. cloud-sa.apjc.amp.cisco.com（亞太地區）

- 更新和升級：
  1. downloads-static.ironport.com
  2. updates-static.ironport.com

TALOS遙測

Cisco Talos團隊以發現新威脅和新興威脅著稱。傳送到Talos的所有資料均被匿名並儲存在美國資料中心。參與SensorBase可以增強網路威脅的分類和辨識，從而更好地保護SWA和其他思科安全解決方案。

DNS

域名伺服器(DNS)安全最佳實踐表明，每個網路必須託管兩個DNS解析器：一個用於本地域內的權威記錄，另一個用於網際網路域的遞迴解析。為了適應這一點，SWA允許為特定域配置DNS伺服器。如果只有一個DNS伺服器可用於本地查詢和遞迴查詢，請考慮它用於所有SWA查詢時增加的額外負載。更好的選項是本地域使用內部解析器，外部域使用根網際網路解析器。這取決於管理員的風險設定檔和允差。

預設情況下，無論記錄的TTL如何，SWA都會快取DNS記錄至少30分鐘。現代網站大量使用內容交付網路(CDN)，其IP地址經常變化，因此TTL記錄較低。這可能導致客戶端為給定伺服器快取一個IP地址，而SWA為同一伺服器快取另一個地址。要對此進行反駁，SWA預設TTL可透過以下CLI命令降低到五分鐘：

```
SWA_CLI> dnsconfig
...
Choose the operation you want to perform:
- NEW - Add a new server.
- EDIT - Edit a server.
- DELETE - Remove a server.
- SETUP - Configure general settings.
- SEARCH - Configure DNS domain search list.
[]> SETUP
...
Enter the minimum TTL in seconds for DNS cache.
...
```

必須配置輔助DNS伺服器，以防主伺服器不可用。如果所有伺服器都配置了相同的優先順序，則會隨機選擇伺服器IP。根據配置的伺服器數量，給定伺服器的超時可能會有所不同。此表格是最多六台DNS伺服器的查詢逾時：

DNS伺服器數量	查詢超時（按順序）
1	60
2	5、45
3	5、10、45
4	1、3、11、45
5	1、3、11、45、1
6	1、3、11、45、1、1

此外，也只有透過CLI才能使用高級DNS選項。使用advancedproxyconfig > DNS命令可在CLI中使用這些選項。

選取下列選項之一：

- 0 -始終使用DNS答案以
- 1 -使用客戶端提供的地址，然後使用DNS
- 2 -有限的DNS使用
- 3 - DNS使用非常有限

對於選項1和2，如果啟用了Web信譽，則使用DNS。

對於選項2和3，如果沒有上游代理或在配置的上游代理發生故障的情況下，DNS用於顯式代理請求。

對於所有選項，在策略成員身份中使用目標IP地址時使用DNS。

這些選項控制SWA在評估客戶端請求時如何決定要連線的IP地址。收到請求後，SWA會看到目標IP地址和主機名。SWA必須決定是信任用於TCP連線的原始目標IP地址，還是執行自己的DNS解析並使用解析地址。預設值為「0 =始終按順序使用DNS答案」，這意味著SWA不信任客戶端提供IP地址。

- 選項1 - SWA嘗試客戶端提供的IP地址進行連線，但如果失敗，則返回解析地址。解析的地址用於策略評估(Web類別、Web信譽等)。
- 選項2 - SWA僅使用客戶端提供的地址進行連線，不回退。解析的地址用於策略評估（Web類別、Web信譽等）。
- 選項3 - SWA僅使用客戶端提供的地址進行連線，不回退。客戶端提供的IP地址用於策略評估（Web類別、Web信譽等）。

選擇的選項取決於管理員在確定給定主機名的解析地址時必須給予客戶端多少信任。如果客戶端是下行代理，請選擇選項3以避免不必要的DNS查詢增加延遲。

負載平衡

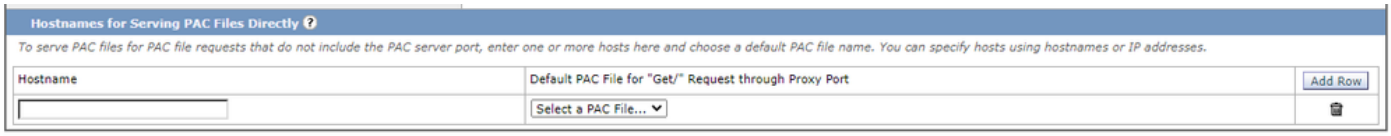
WCCP允許在最多使用八台裝置時執行透明流量負載均衡。它允許根據雜湊或掩碼平衡流量，可在網路中混合使用裝置型號的情況下進行加權，並且可在不停機的情況下向服務池增加和刪除裝置。一旦需求超過八個SWA所能處理的範圍，建議使用專用的負載均衡器。

WCCP配置的具體最佳實踐因使用的平台而異。對於Cisco Catalyst®交換機，最佳實踐記錄在Cisco Catalyst即時接入解決方案白皮書中。

WCCP在與Cisco Adaptive Security Appliance (ASA)一起使用時存在限制。也就是說，不支援客戶端IP欺騙。此外，客戶端和SWA必須位於同一介面之後。因此，使用第4層交換器或路由器來重新導向流量會更為靈活。有關ASA平台上的WCCP配置，請參閱ASA上的WCCP：概念、限制和配置。

對於顯式部署，代理自動配置(PAC)檔案是部署最廣泛的方法，但它有許多缺點和安全影響超出了本文檔的範圍。如果部署了PAC檔案，建議使用組策略對象(GPO)配置位置，而不是依賴Web代理自動發現協定(WPAD)，WPAD是攻擊者的常見目標，如果配置錯誤，很容易被攻擊。SWA可以託管多個PAC檔案，並控制它們在瀏覽器快取中的到期時間。

PAC檔案可以直接從SWA從可配置的TCP埠號（預設情況下為9001）請求。如果未指定連線埠，則可將要求傳送至代理程式本身，就如同它是傳出Web要求一樣。在這種情況下，可以根據請求中存在的HTTP主機報頭為特定PAC檔案提供服務。



在高可用性環境中使用時，Kerberos的配置必須不同。SWA提供對keytab檔案的支援，從而允許多個主機名與服務主體名稱(SPN)關聯。有關詳細資訊，請參閱在Windows Active Directory中建立服務帳戶，用於高可用性部署中的Kerberos身份驗證。

主動驗證

Kerberos比NT LAN Manager安全支援提供者(NTLMSSP)更安全，而且比NT LAN Manager安全支援提供者(NTLMSSP)支援更廣泛。Apple OS X作業系統不支援NTLMSSP，但可以在域加入時使用Kerberos進行身份驗證。不能使用基本身份驗證，因為它傳送未加密的憑據到HTTP報頭，並且很容易被網路上的攻擊者嗅探。如果必須使用基本身份驗證，則必須啟用憑據加密以確保透過加密隧道傳送憑據。

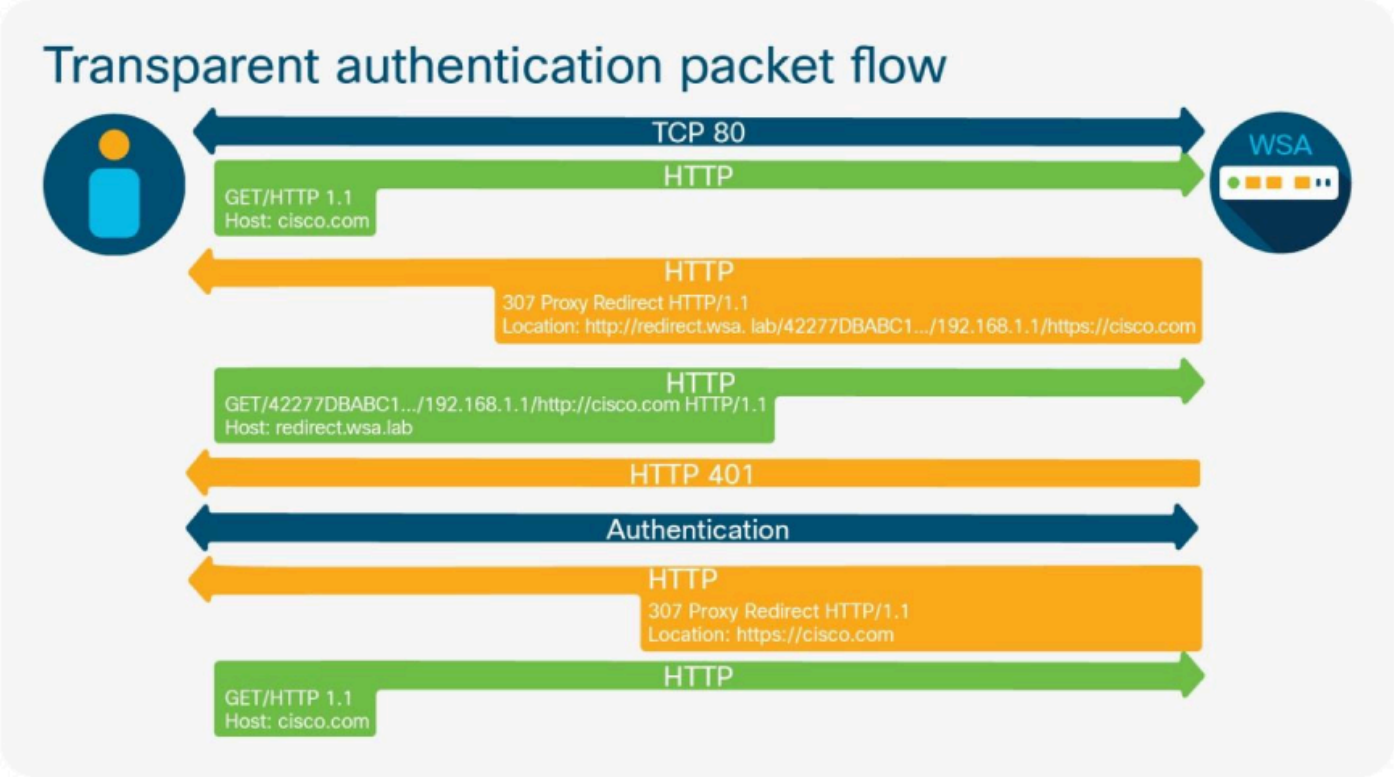
必須將多個域控制器增加到配置以確保可用性，但是此流量沒有固有的負載平衡。SWA將TCP SYN資料包傳送到所有已配置的域控制器，第一個作出響應的域控制器用於身份驗證。

在身份驗證設定頁面中配置的重定向主機名確定傳送透明客戶端的位置以完成身份驗證。要使Windows客戶端完成整合身份驗證並實現單一登入(SSO)，重定向主機名必須位於Internet選項控制台中的受信任站點區域。Kerberos通訊協定要求使用完整網域名稱(FQDN)來指定資源，這表示如果Kerberos是預期的驗證機制，就無法使用「簡短名稱」（或「NETBIOS」名稱）。需要將FQDN手動增加到受信任的站點（例如，透過組策略）。此外，必須在Internet選項控制台中設定「使用使用者名稱和密碼自動登入」。

Firefox中還需要其他設定，瀏覽器才能完成網路代理的身份驗證。這些設定可在about：config頁中進行配置。要成功完成Kerberos，必須將重定向主機名增加到network.negotiate-auth.trusted-uris選項。對於NTLMSSP，必須將其增加到network.automatic-ntlm-auth.trusted-uris選項。

身份驗證代理用於在身份驗證完成之後的一段時間內記住經過身份驗證的使用者。必須儘可能使用IP代理來限制發生的活動身份驗證事件的數量。主動驗證使用者端是一項需要大量資源的作業，尤其是使用Kerberos時。預設情況下，替代超時為3600秒（1小時），可以減少，但建議的最低值為900秒（15分鐘）。

此影像顯示如何使用「redirect.WSA.lab」作為重新導向主機名稱：



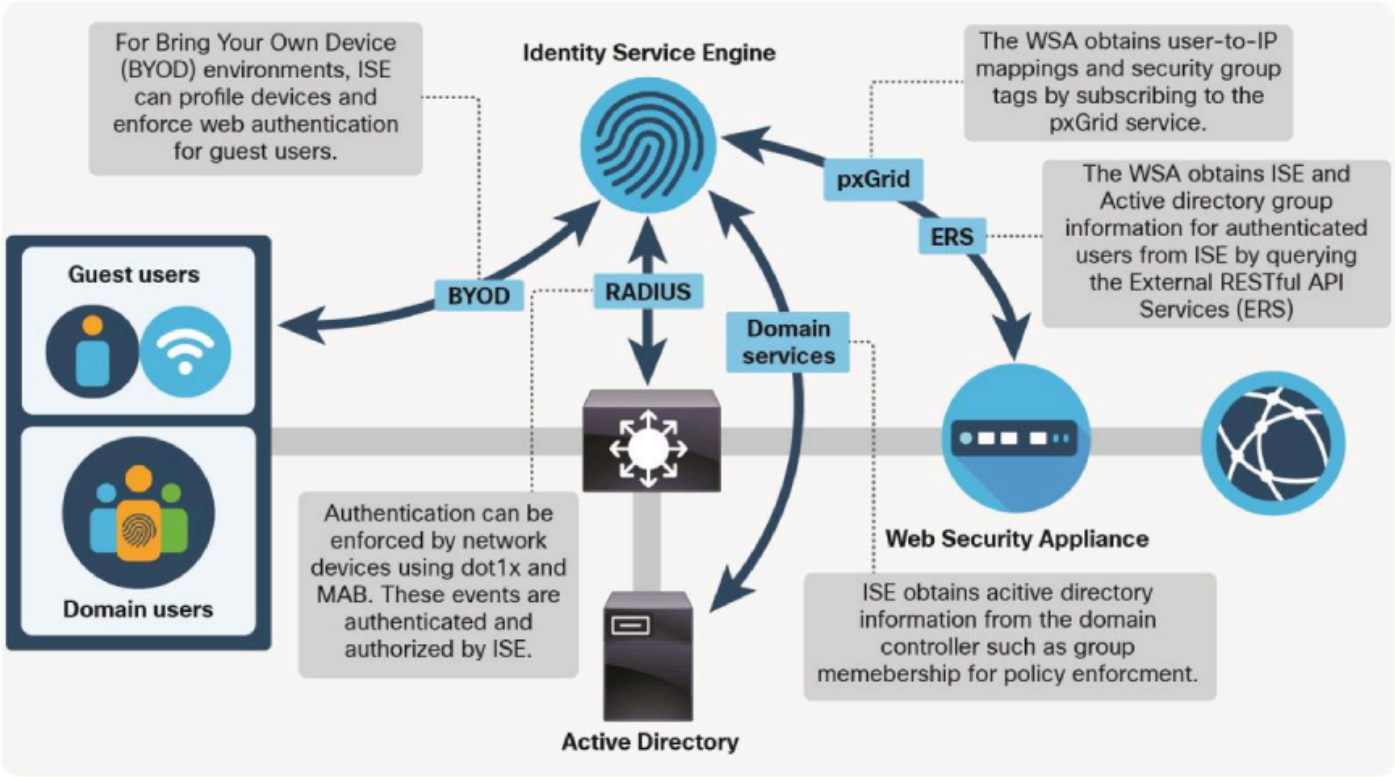
被動驗證

SWA可以利用其他思科安全平台被動辨識代理使用者。被動使用者辨識消除了直接身份驗證質詢和來自SWA的任何Active Directory通訊的需要，從而減少了裝置上的延遲和資源使用。當前可用的被動身份驗證機制是透過上下文目錄代理(CDA)、身份服務引擎(ISE)和身份服務聯結器被動身份聯結器(ISE-PIC)。

ISE是一個功能豐富的產品，可幫助管理員集中其身份驗證服務並利用廣泛的網路訪問控制集。當ISE獲知使用者身份驗證事件（透過Dot1x身份驗證或Web身份驗證重定向）時，它會填充會話資料庫，其中包含有關身份驗證所涉及的使用者和裝置的資訊。SWA透過平台交換網格(pxGrid)連線到ISE，並獲取與代理連線關聯的使用者名稱、IP地址和安全組標籤(SGT)。從AsyncOS版本11.7開始，SWA還可以查詢ISE上的外部Restful服務(ERS)以獲取組資訊。

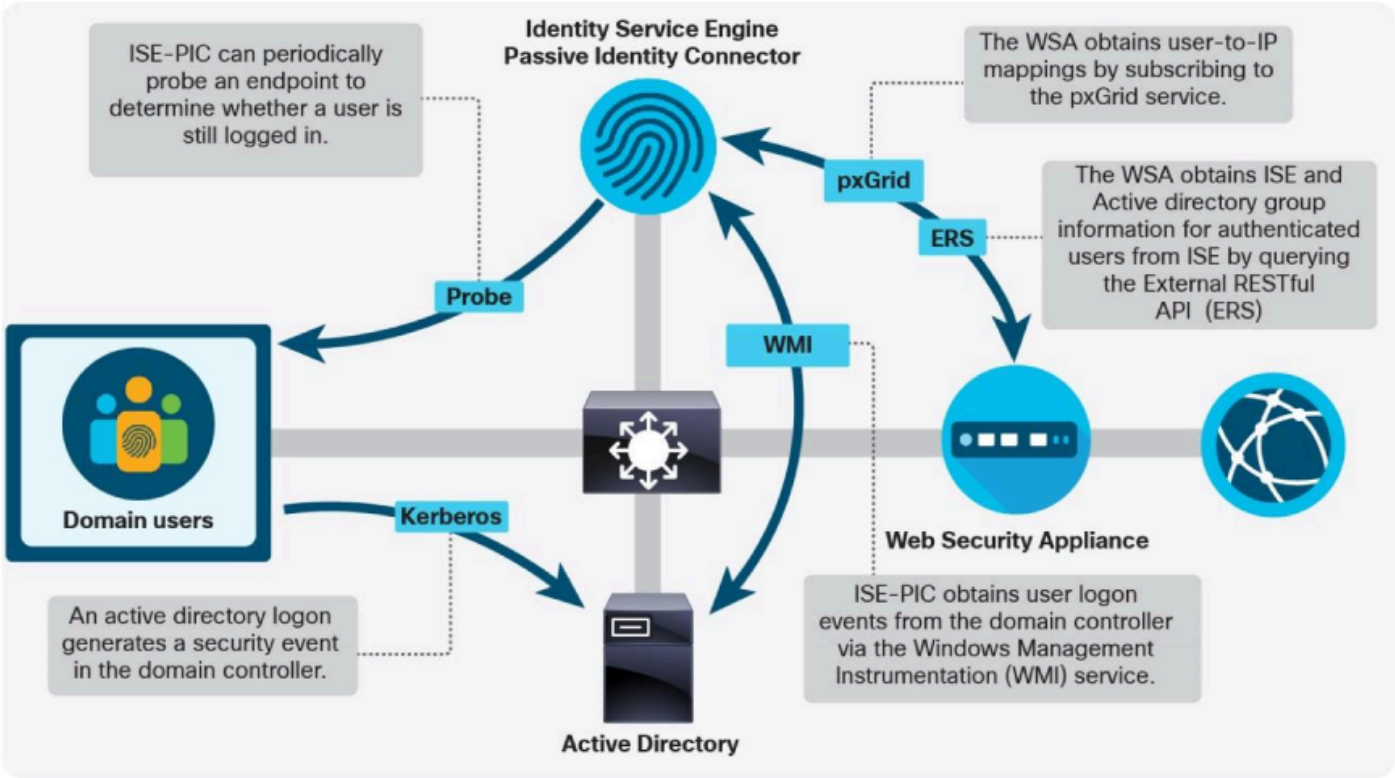
建議版本為ISE 3.1和SWA 14.0.2-X及更高版本，有關SWA的ISE相容性清單的詳細資訊，請參閱安全Web裝置的ISE相容性清單。

有關完全整合步驟的詳細資訊，請參閱網路安全裝置最終使用手冊。



思科宣佈Cisco Context Directory Agent (CDA)軟體的壽命終止，請參閱Cisco Context Directory Agent (CDA)。

自CDA修補6起，與Microsoft Server 2016相容。但是，我們積極鼓勵管理員將其CDA部署遷移到ISE-PIC。兩種解決方案都使用WMI訂閱Windows安全事件日誌，以生成使用者到IP的對映（稱為「會話」）。對於CDA，SWA使用RADIUS查詢這些對映。對於ISE-PIC，在完整ISE部署中使用相同的pxGrid和ERS連線。ISE-PIC功能在完整ISE安裝中以及在獨立虛擬裝置中可用。

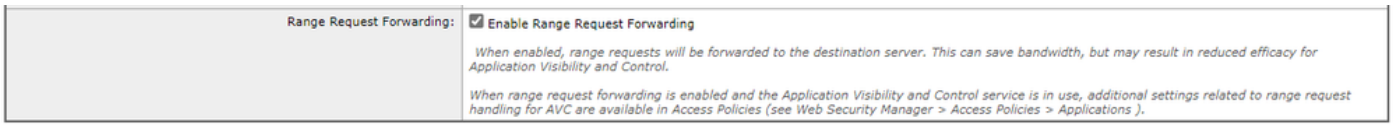


服務配置

Web代理

必須在Web代理配置中啟用快取，以便節省頻寬並提高效能。隨著HTTPS流量的百分比增加，這一點變得不再那麼重要，因為SWA預設情況下不會快取HTTPS事務。如果將代理部署為僅為顯式客戶端提供服務，則必須指定轉發模式以拒絕並非專門用於代理服務的任何流量。透過這種方式，裝置攻擊面得以減少，並實施了良好的安全原則：如果不需要則將其關閉。

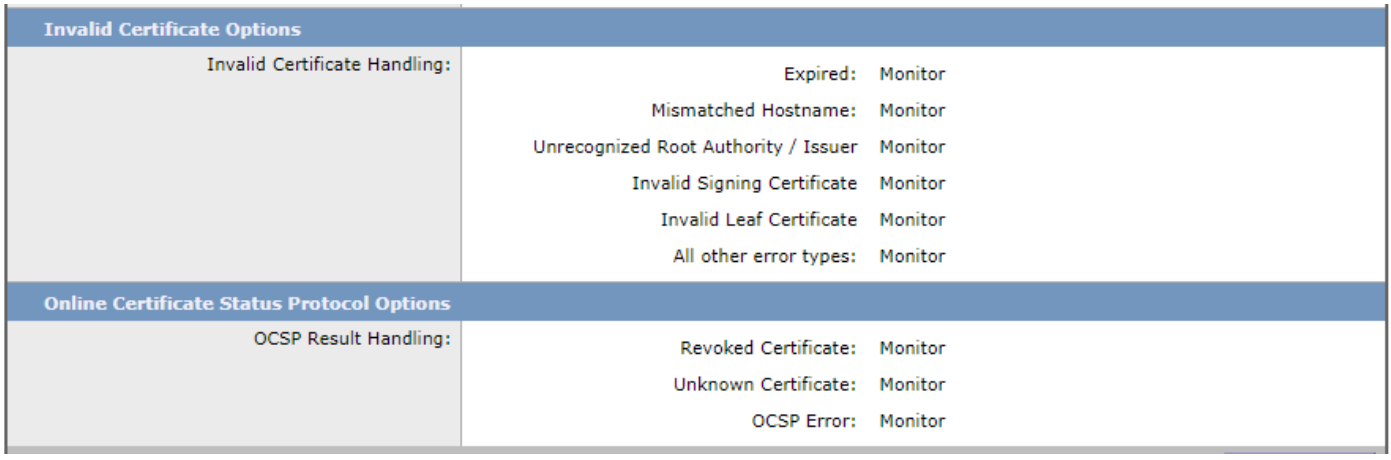
範圍要求標頭用於HTTP要求中，以指定要下載之檔案的位元組範圍。它通常由作業系統和應用程式更新守護程式使用，以便一次傳輸檔案的小部分。預設情況下，SWA會刪除這些標頭，以便獲取整個檔案，用於防病毒(AV)掃描、檔案信譽和分析以及應用可視性控制(AVC)。透過在代理設定中全局啟用範圍請求報頭的轉發，管理員可以建立轉發或刪除這些報頭的單獨訪問策略。有關此配置的詳細資訊，請參閱訪問策略部分。



HTTPS代理

安全最佳實踐建議，私鑰必須在使用它們的裝置上生成，並且不得傳輸到其他地方。HTTPS代理嚮導允許建立金鑰對和用於解密傳輸層安全(TLS)連線的證書。然後憑證簽署請求(CSR)可以下載並由內部憑證授權單位(CA)簽署。在Active Directory (AD)環境中，這是最佳方法，因為AD整合的CA自動受域所有成員的信任，並且不需要其他步驟來部署證書。

HTTPS代理的一個安全功能是驗證伺服器證書。最佳實踐建議無效證書要求斷開連線。啟用Decrypt for EUN可讓SWA顯示說明區塊原因的區塊頁面。如果沒有啟用此功能，任何被阻止的HTTPS站點都會導致瀏覽器錯誤。這導致了幫助台票證的增加，並且使用者認為有東西壞了，而不是知道SWA阻止了連線。所有無效的憑證選項都必須至少設定為「解密」。如果保留這些選項中的任何選項為監視器，則無法在證書問題阻止載入站點時記錄有用的錯誤消息。



同樣地，線上證書服務協定(OCSP)檢查必須保持啟用狀態，並且不能對任何選項使用監控。必須丟棄吊銷的證書，並且所有其他證書必須至少設定為「解密」，以允許記錄相關錯誤消息。Authority

Information Access Tracking (AIA Tracking)是客戶端收集證書簽名者和URL的方法，從中可以獲取其他證書。例如，如果從伺服器接收的證書鏈不完整（缺少中間或根證書），SWA可以檢查AIA欄位並使用該欄位來獲取缺少的證書並驗證真實性。此設定只能透過下列指令在CLI中使用：

```
SWA_CLI> advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
- CONTENT-ENCODING - Block content-encoding types
- SCANNERS - Scanner related parameters
[]> HTTPS
...
Do you want to enable automatic discovery and download of missing Intermediate Certificates?
[Y]>
...
```

注意：此設定預設處於啟用狀態，不能停用，因為許多現代伺服器依賴此機製為客戶端提供完全信任鏈。

第4層流量監控器(L4TM)

L4TM是擴展SWA的覆蓋範圍，使之包括不透過代理的惡意流量，以及所有TCP和UDP埠上的流量的一種非常有效的方法。T1和T2埠用於連線到網路分路器或交換機監控會話。這允許SWA被動地監控來自客戶端的所有流量。如果發現發往惡意IP地址的流量，SWA可以在欺騙伺服器IP地址的同時傳送RST來終止TCP會話。對於UDP流量，它可以傳送Port Unreachable消息。配置監控會話時，最好排除任何發往SWA管理介面的流量，以防止該功能可能干擾對裝置的訪問。

除了監控惡意流量之外，L4TM還會監聽DNS查詢，以更新繞過設定清單。此清單用於WCCP部署，用於將某些請求返回到WCCP路由器以直接路由到Web伺服器。與旁路設定清單匹配的資料包不會由代理處理。此清單可包含IP位址或伺服器名稱。無論記錄的TTL如何，SWA每30分鐘解析一次旁路設定清單中的任何條目。但是，如果啟用L4TM功能，SWA可以使用監聽的DNS查詢更頻繁地更新這些記錄。這降低了客戶端解析與SWA不同的地址時出現假負值的風險。

策略配置

正確的策略配置對於SWA的效能和可擴充性至關重要。這不僅是因為策略本身在保護客戶和執行公

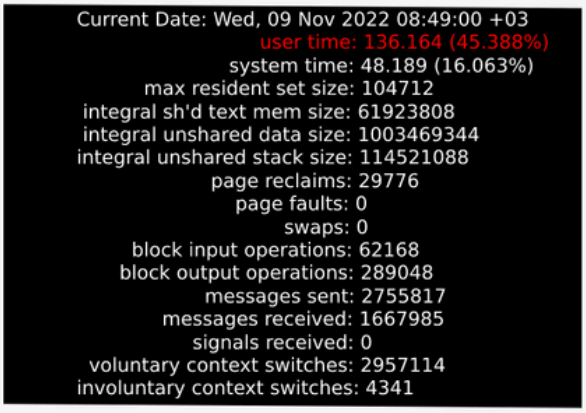
司要求方面的有效性，還因為配置的策略對資源使用量以及SWA的整體運行狀況和效能有直接影響。一組過於複雜或設計不當的策略可能導致裝置不穩定和響應速度緩慢。

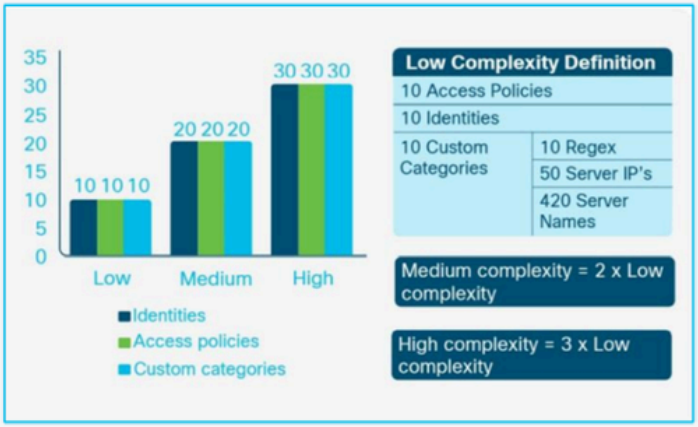
複雜性

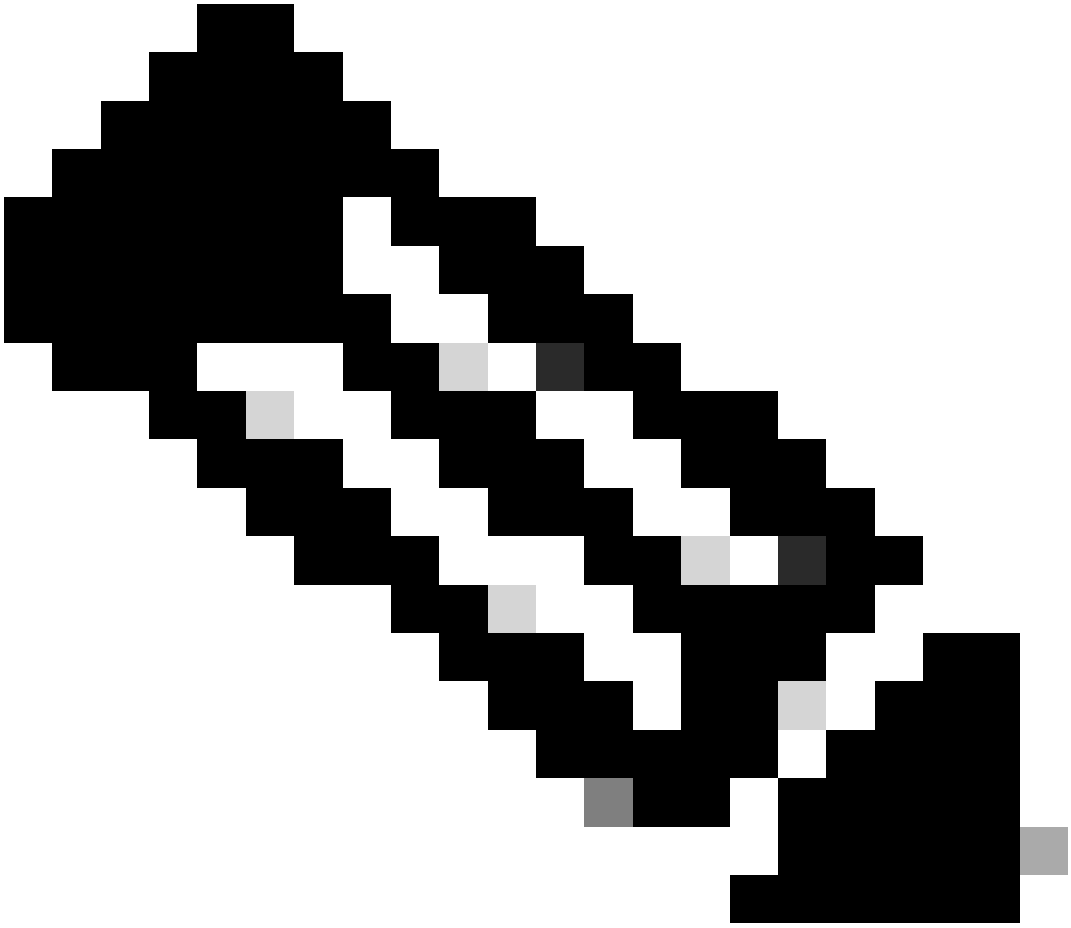
在制訂全部門辦法政策時使用了各種政策要素。從配置生成的XML檔案用於建立多個後端配置檔案和訪問規則。配置越複雜，Proxy進程需要花費更多時間來評估每個事務的各種規則集。在對SWA進行基準測試和調整其規模時，會建立一組基本策略元素，這些元素代表配置複雜性的三個層級。十個身份配置檔案、解密策略和訪問策略，以及十個包含10個正規表示式條目、50個伺服器IP地址和420個伺服器主機名的自定義類別，被視為低複雜性配置。將每個數字乘以2和3分別得到中等複雜度和高度複雜度的配置。

當配置變得過於複雜時，最初的症狀通常包括Web介面和CLI響應緩慢。一開始不會對使用者造成重大影響。但配置越複雜，代理進程必須在使用者模式下花費的時間就越多。因此，檢查在此模式中花費的時間百分比是一種有用的方法，可以將過於複雜的配置診斷為SWA緩慢的原因。

每五分鐘在track_stats日誌中記錄一次CPU時間（以秒為單位）。這表示使用者時間百分比可以計算為（使用者時間+系統時間）/300。當使用者時間接近270時，該進程在使用者模式下花費了太多的CPU週期，這幾乎總是因為配置太複雜，無法有效地進行分析。







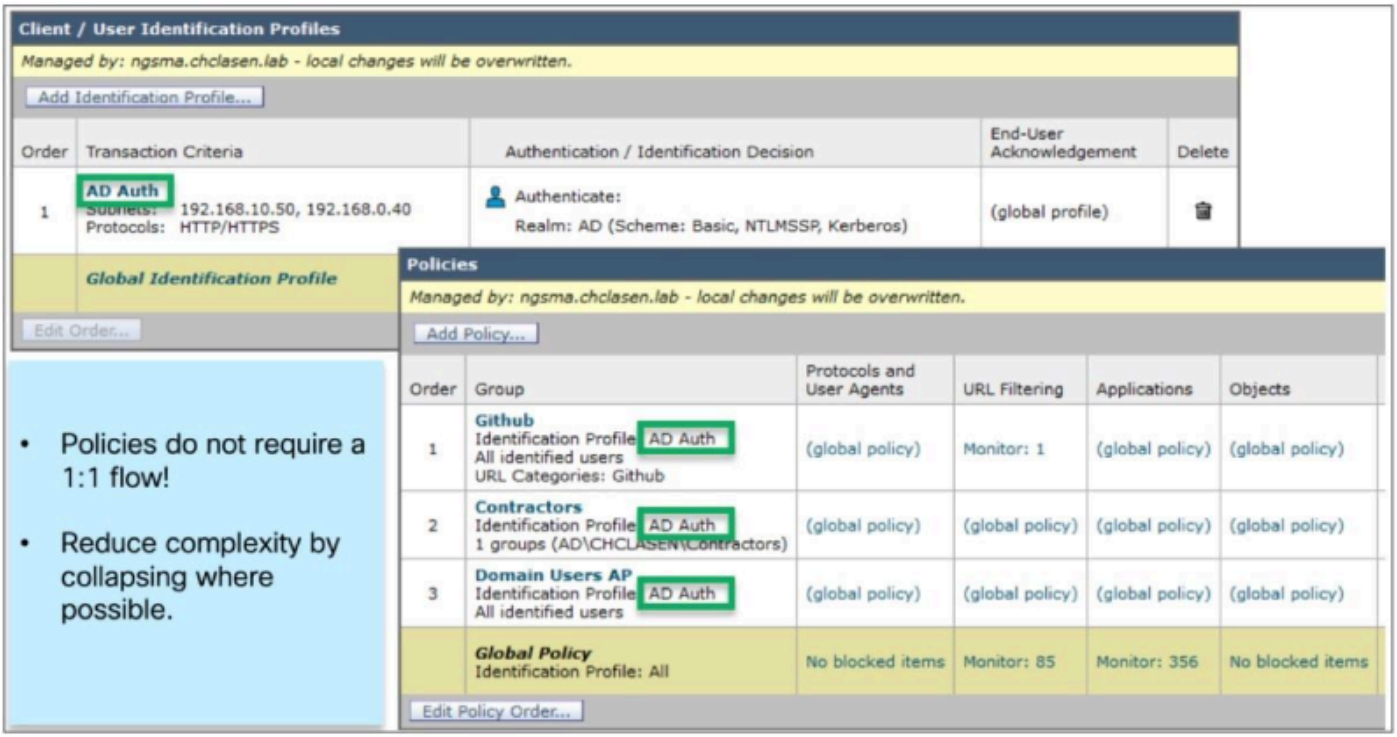
註：到目前為止，SWA的最大限制是60,000個併發客戶端連線和60,000個併發伺服器連線。

標識配置檔案

標識(ID)配置檔案是在收到新請求時評估的第一個策略元素。在ID設定檔的第一部分中設定的所有資訊都會以邏輯AND進行評估。這意味著所有條件必須匹配，請求才能與配置檔案匹配。建立策略時，策略必須嚴格到絕對必要。包含單個主機地址的配置檔案幾乎從來都不是必需的，並且可能導致配置蔓延。使用HTTP標頭、自定義類別清單或子網中的使用者代理字串通常是限制配置檔案範圍的更好策略。

通常，需要身份驗證的策略配置在底部，並在頂部增加異常。在訂購不需要身份驗證的策略時，最常用的策略必須儘可能最接近頂部。不要依賴失敗的身份驗證來限制訪問。如果已知網路上的使用者端無法向代理主機進行驗證，則必須在存取原則中免除驗證並封鎖該使用者端。無法重複進行身份驗證的客戶端將未經身份驗證的請求傳送到SWA，SWA使用資源並可能導致CPU和記憶體利用率過高。

對於管理員來說，一個常見的誤解是必須有一個唯一的ID配置檔案以及相應的解密策略和訪問策略。對於策略配置而言，這種策略效率很低。如有可能，策略必須是「摺疊的」，以便單個ID配置檔案可以與多個解密和訪問策略相關聯。這是可能的，因為給定策略中的所有條件必須匹配，流量才能與策略匹配。在身份驗證策略中越普遍，在生成的策略中越具體，則整個策略的數量越少。



解密策略

與ID配置檔案一樣，解密策略中設定的條件也被評估為邏輯AND，但使用ISE的資訊時有一個重要例外。下面是策略匹配的工作方式，具體取決於配置的元素（AD組、使用者或SGT）：

- AD組和使用者-不更改以前的行為；如果使用者是組的成員，或者已在策略中指定使用者，則此策略匹配。
- SGT和AD組及使用者-如果使用者與SGT相關聯且是AD組的成員，或者已在策略中指定使用者，則匹配策略。
- SGT和使用者-如果使用者與SGT相關聯或在策略中指定了使用者，則匹配策略。

在SWA執行的所有服務中，從效能角度而言，對HTTPS流量的評估最為重要。解密流量的百分比對裝置的大小有直接影響。管理員可以依靠至少75%的Web流量進行HTTPS。

在初始安裝之後，必須確定解密流量的百分比，以確保準確設定未來成長的預期。部署後，必須每季度檢查一次此編號。使用access_logs副本可以輕鬆查詢SWA解密的HTTPS流量百分比，即使沒有額外的日誌管理軟體也是如此。可以使用簡單的Bash或PowerShell命令來獲取此數字。以下是針對每個環境描述的步驟：

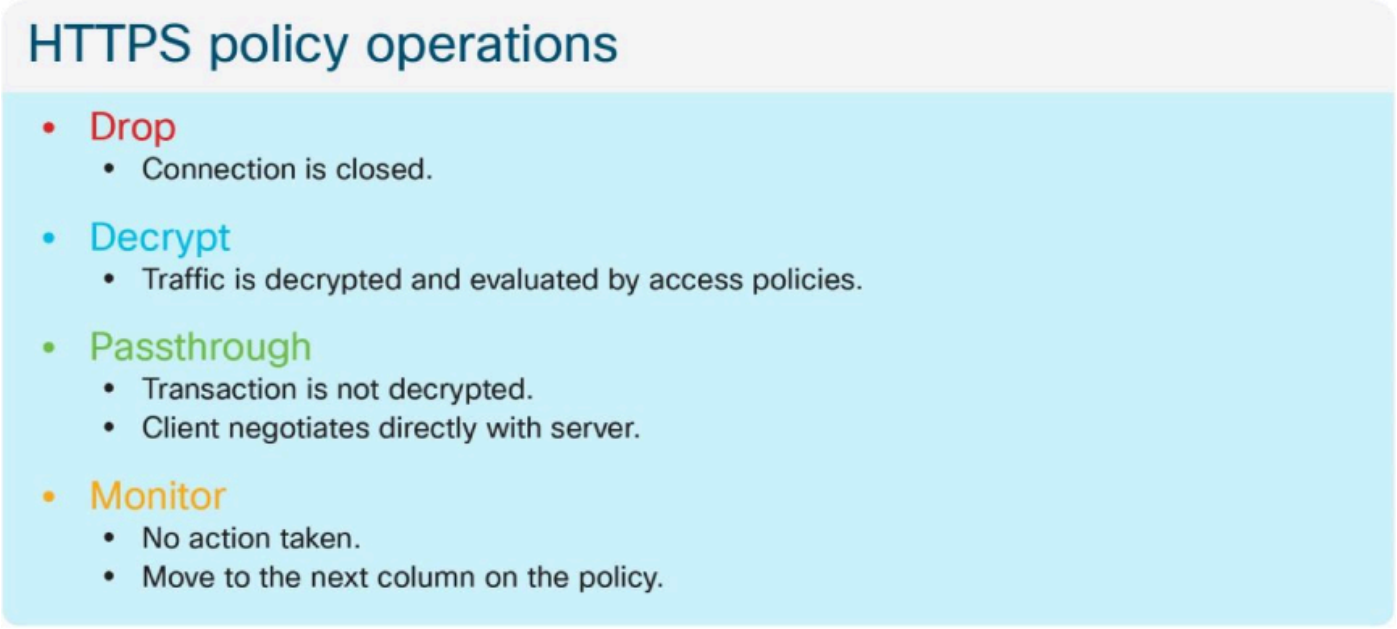
1. Linux命令：

```
cat aclog.current | grep -Ev "\/407|\/401" | awk 'BEGIN { total=0; decrypt=0; ssl=0;} {total++; if($0 ~
```

2. Powershell命令：

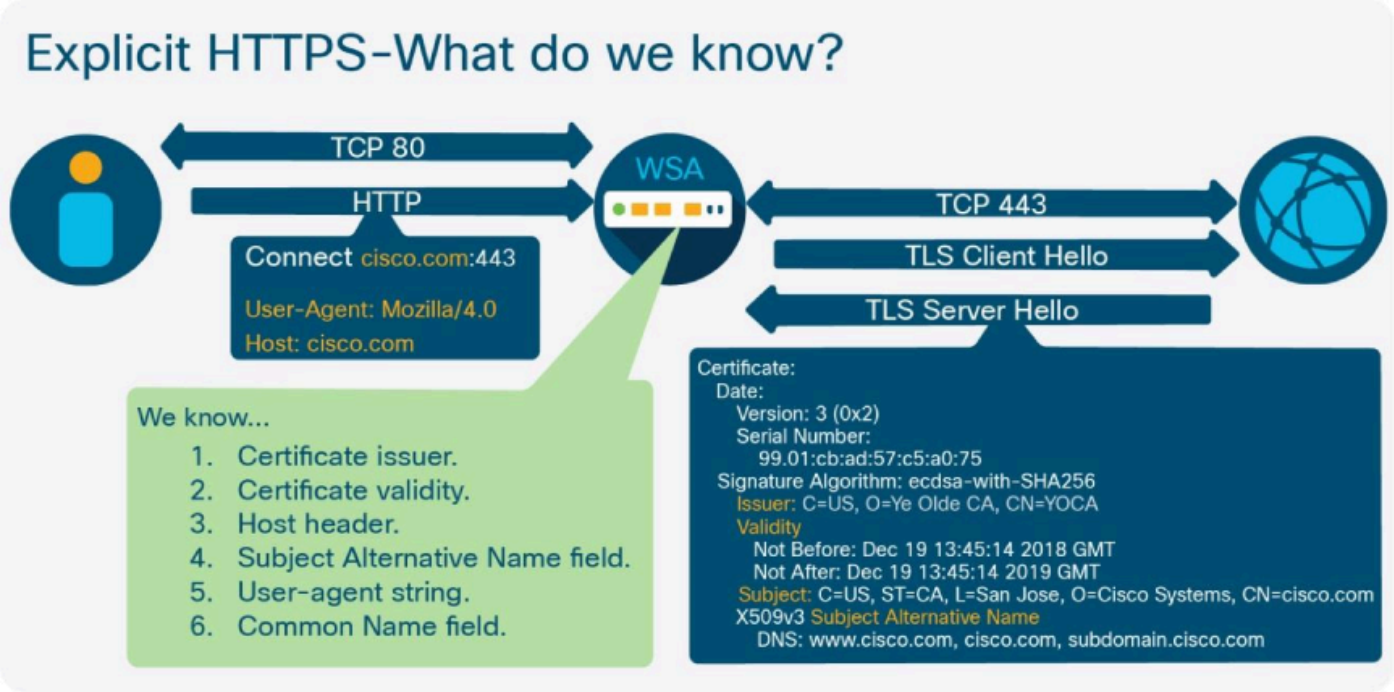
```
$lines = Get-Content -Path "aclog.current" | Where-Object { $_ -notmatch "/407|/401" }; $total = 0; $de
```

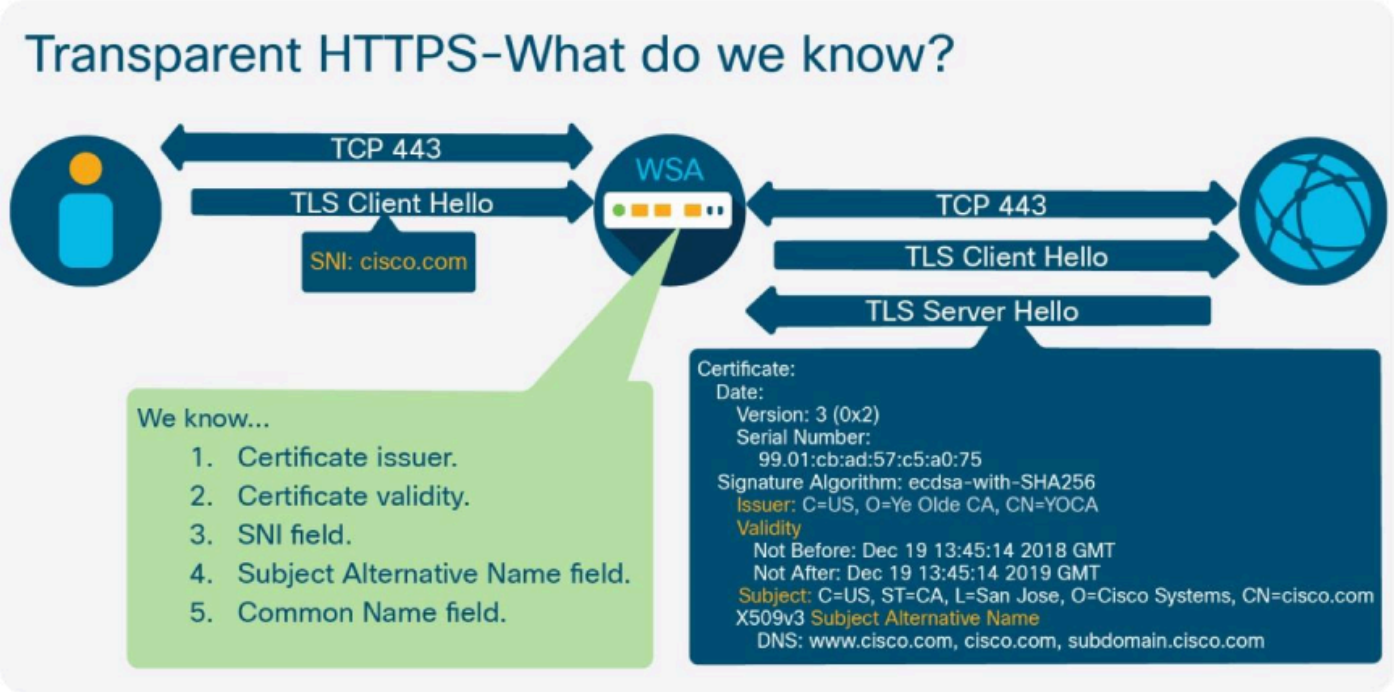
設計解密策略時，必須瞭解策略中列出的各種操作如何導致裝置評估HTTPS連線。當必須允許客戶端和伺服器終止其TLS會話的每一端，而沒有SWA解密每個資料包時，會使用直通操作。即使站點設定為直通，仍必須要求SWA完成與伺服器的一次TLS握手。這是因為SWA必須根據證書有效性選擇阻止連線，並且必須啟動與伺服器的TLS連線以獲取證書。如果證書有效，SWA將關閉連線，並允許客戶端繼續直接與伺服器建立會話。



SWA不執行任何TLS握手的唯一情況是，伺服器名稱或IP地址存在於自定義類別中（設定為直通），並且伺服器名稱在HTTP CONNECT或TLS客戶端Hello中可用。在顯式場景中，客戶端在TLS會話初始化之前（在主機標頭中）向代理提供伺服器的主機名，因此將根據自定義類別檢查此欄位。在透明部署中，SWA檢查TLS客戶端Hello消息中的伺服器名稱指示(SNI)欄位，並根據自定義類別對其進行評估。如果主機報頭或SNI不存在，SWA必須繼續與伺服器握手，以便按順序檢查證書上的主題備用名稱(SAN)和公用名稱(CN)欄位。

此行為對策略設計的意義是，透過確定公認和內部信任的伺服器並將其設定為從自定義類別清單傳遞，而不是依賴網路類別和信譽得分（這仍需要SWA完成與伺服器的TLS握手），可以減少TLS握手的數量。但是，必須注意的是，這也會阻止證書有效性檢查。





鑑於新網站在網上出現的速度，可能會發現一些網站未按照全部門辦法使用的Web信譽和分類資料庫進行分類。這並不表示該站點一定更可能是惡意站點，此外，所有這些站點仍會受到AV掃描、AMP檔案信譽和分析，以及任何已配置的對象阻止或掃描。出於這些原因，建議不要在多數情況下丟棄未分類站點。最好將它們設定為由AV引擎解密和掃描，並由AVC、AMP、訪問策略等進行評估。訪問策略部分提供了有關未分類站點的詳細資訊。

訪問策略

與ID配置檔案一樣，解密策略中設定的條件也被評估為邏輯AND，當使用ISE的資訊時，有一個重要例外。接下來會根據配置的元素（AD組、使用者或SGT）解釋策略匹配行為：

- AD組和使用者-不更改以前的行為；如果使用者是組的成員，或者已在策略中指定使用者，則

此策略匹配。
- SGT和AD組及使用者-如果使用者與SGT相關聯且是AD組的成員，或者已在策略中指定使用者，則匹配策略。
- SGT和使用者-如果使用者與SGT關聯，或者已在策略中指定使用者，則匹配策略。

在經過身份驗證後，將立即根據訪問策略評估HTTP流量。在驗證之後，以及是否根據匹配的解密策略應用了解密操作，將評估HTTPS流量。對於解密的請求，有兩個access_log條目。第一個日誌條目顯示應用於初始TLS連線（解密）的操作，第二個日誌條目顯示訪問策略應用於已解密HTTP請求的操作。

如Web代理部分所說明的，範圍請求報頭用於請求檔案的特定位元組範圍，並且通常由作業系統和應用程式更新服務使用。預設情況下，SWA從出站請求中刪除這些報頭，因為如果沒有整個檔案，將無法執行惡意軟體掃描或使用AVC功能。如果網路中的許多主機經常請求小位元組範圍來檢索更新，則可能會觸發SWA同時下載整個檔案多次。這會快速耗儘可用的Internet頻寬並導致服務中斷。此失敗情況的最常見原因是Microsoft Windows更新和Adobe軟體更新守護程式。

要緩解這種情況，最佳解決方案是將此流量完全控制在SWA周圍。這對於透明部署的環境並非總是可行，在這些情況下，下一個最佳選項是為流量建立專用訪問策略，並在這些策略上啟用範圍請求報頭轉發。必須考慮這些請求無法進行AV掃描和AVC，因此必須仔細設計策略以僅針對預期流量。通常，實現這一點的最佳方式是匹配請求報頭中的使用者代理字串。常見更新守護程式的使用者-代理字串可以線上找到，或者可以由管理員捕獲並檢查請求。大多數更新服務（包括Microsoft Windows和Adobe軟體更新）不使用HTTPS。

如解密策略部分中所述，不建議刪除解密策略中未經分類的站點。出於同樣的原因，建議不要在訪問策略中阻止它們。動態內容分析(DCA)引擎可以使用給定站點的內容，以及其他啟發式資料來分類站點，否則這些站點將被URL資料庫查詢標籤為未分類。啟用此功能可減少SWA中未分類裁決的數量。

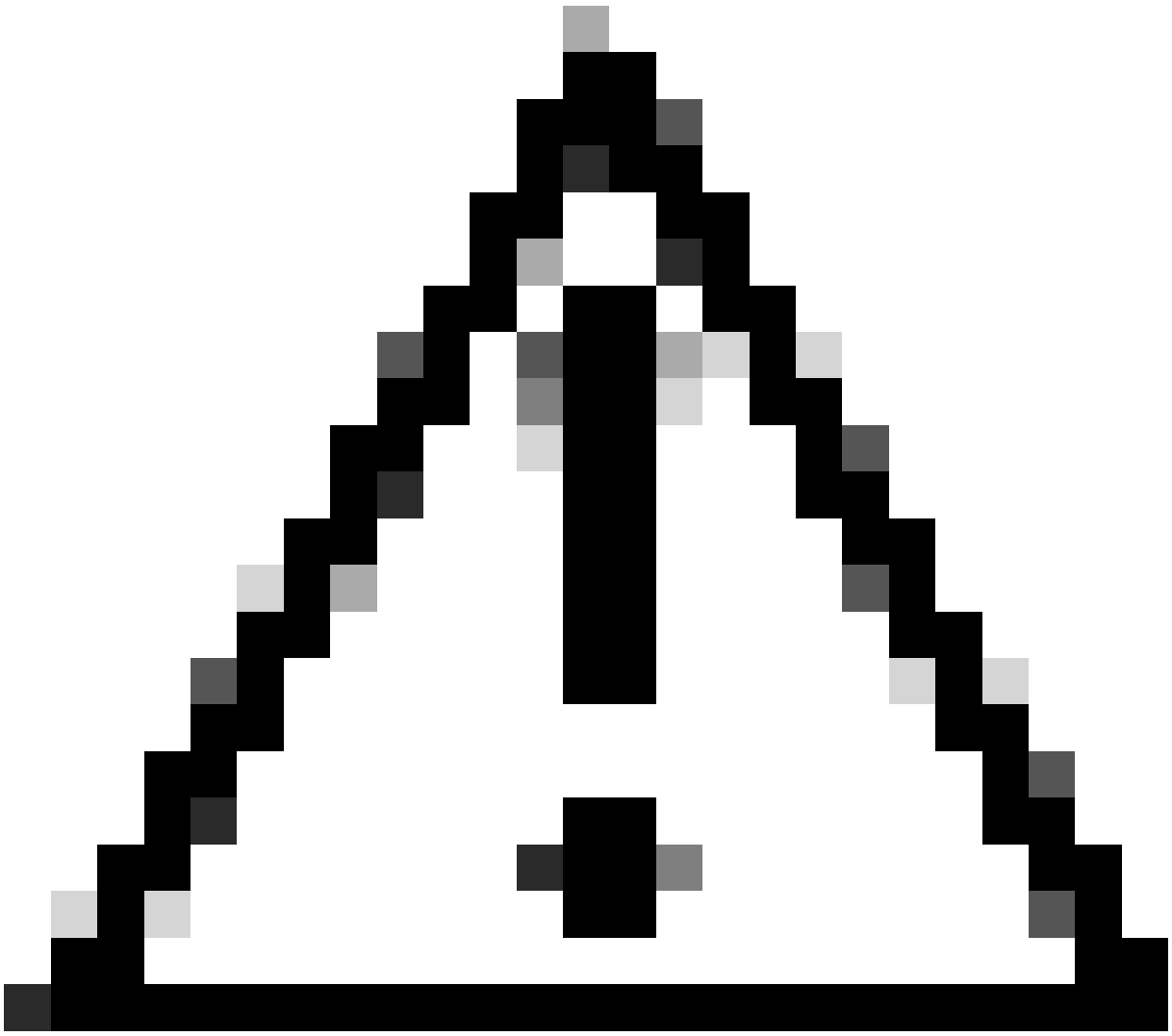
訪問策略的「對象掃描」設定提供了檢查多種型別的存檔檔案的功能。如果網路定期下載存檔檔案作為應用程式更新的一部分，則啟用存檔檔案檢查會顯著增加CPU使用率。如果要檢查所有存檔檔案，必須提前辨識並免除此流量。首先研究確定此流量的可能方法的是使用者代理字串，因為這樣有助於避免可能變得繁瑣維護的IP允許清單。

自定義和外部URL類別

Custom類別清單用於透過IP地址或主機名標識伺服器。可以使用正規表示式(regex)指定伺服器名稱匹配的模式。使用regex模式匹配伺服器名稱比使用子字串匹配要耗費大量資源，因此必須僅在絕對必要時使用它們。可在域名的開頭增加「。」以匹配子域，而無需正規表示式。例如，「.cisco.com」也與「www.cisco.com」匹配。
如複雜性部分所說明的，低複雜性定義為十個自定義類別清單，中等複雜性定義為二十個，而高複雜性定義為三十個。建議將此數字保持在20以下，特別是當清單使用regex模式或包含大量條目時。有關每種型別的條目數的更多詳細資訊，請參閱訪問策略部分。

外部URL源比靜態自定義類別清單靈活得多，利用它們可能會對安全產生直接影響，因為它們不再需要管理員手動維護它們。由於此功能可用於檢索不由SWA管理員維護或控制的清單，因此在AsyncOS 11.8版中增加了將單個例外增加到下載地址的能力。

Office365 API對於針對此常見部署服務做出策略決策特別有用，可用於單個應用程式（PowerPoint、Skype、Word等）。Microsoft建議略過所有Office365流量的代理程式，以最佳化效能。Microsoft文檔說明：



注意：「雖然SSL中斷和檢查導致延遲時間最長，但代理身份驗證和信譽查詢等其他服務可能導致效能不佳和使用者體驗不佳。此外，這些外圍網路裝置需要足夠的容量來處理所有網路連線請求。我們建議略過您的代理或檢查裝置來進行直接Office 365網路要求。」- https://learn.microsoft.com/en-us/microsoft-365/enterprise/managing-office-365-endpoints?view=o365-worldwide

---

在透明的代理環境中使用本指南可能會很困難。從AsyncOS版本11.8開始，可以使用從Office365 API檢索的動態類別清單填充旁路設定清單。此清單用於將透明重新導向的流量傳送回WCCP裝置

以進行直接路由。

略過所有Office365流量，會為需要一些基本安全控制及報告此流量的管理員建立盲點。如果SWA未繞過Office365流量，瞭解可能出現的具體技術挑戰就非常重要。其中之一是應用程式所需的連線數。大小必須適當調整，以適應Office365應用程式所需的額外持續TCP連線。這可以使每個使用者的總連線計數增加10到15個持續TCP會話。

HTTPS代理執行的解密和重新加密操作會為連線帶來少量延遲。Office365應用程式對延遲非常敏感，如果廣域網連線緩慢和地理位置分散等其他因素加劇了這一情況，使用者體驗可能會受到影響。

有些Office365應用程式使用專有的TLS引數，會阻止HTTPS代理與應用程式伺服器完成交握。這是驗證證書或檢索主機名所必需的。當它與某個應用程式（例如Skype for Business）結合使用時，該應用程式在其TLS客戶端Hello消息中不傳送伺服器名稱指示(SNI)欄位，則有必要完全繞過此流量。AsyncOS 11.8引入了僅基於目標IP地址繞過流量的功能，無需進行證書檢查即可解決此問題。

監視和警報

CLI監視器

SWA CLI提供用於即時監控重要進程的命令。最有用的命令是顯示與prox進程相關的統計資訊的命令。status detail命令是資源使用和效能度量（包括正常運行時間、使用的頻寬、響應延遲、連線數等）摘要的良好來源。以下是此命令的示例輸出：

```
SWA_CLI>  status detail

Status as of:                  Fri Nov 11 14:06:52 2022 +03
Up since:                      Fri Apr 08 10:15:00 2022 +03 (217d 3h 51m 52s)
System Resource Utilization:
  CPU                                3.3%
  RAM                                6.2%
  Reporting/Logging Disk            45.6%
Transactions per Second:
  Average in last minute               55
  Maximum in last hour                201
  Average in last hour                 65
  Maximum since proxy restart       1031
  Average since proxy restart          51
Bandwidth (Mbps):
  Average in last minute            4.676
  Maximum in last hour            327.258
  Average in last hour             10.845
  Maximum since proxy restart    1581.297
  Average since proxy restart      11.167
Response Time (ms):
  Average in last minute               635
  Maximum in last hour              376209
  Average in last hour                 605
  Maximum since proxy restart      2602943
  Average since proxy restart          701
```

```
Cache Hit Rate:
  Average in last minute                    0
  Maximum in last hour                      2
  Average in last hour                      0
  Maximum since proxy restart              15
  Average since proxy restart               0
Connections:
  Idle client connections                 186
  Idle server connections                 184
  Total client connections               3499
  Total server connections               3632
SSLJobs:
  In queue Avg in last minute               4
  Average in last minute                45214
  SSLInfo Average in last min              94
Network Events:
  Average in last minute                  0.0
  Maximum in last minute                   35
  Network events in last min           124502
```

rate命令顯示有關prox進程使用的CPU百分比的即時資訊，以及每秒請求數(RPS)和快取統計資訊。此命令會持續輪詢並顯示新輸出，直到中斷為止。以下是此命令的輸出示例：

```
SWA_CLI>  rate

Press Ctrl-C to stop.
  %proxy  reqs                          client    server    %bw  disk  disk
     CPU  /sec   hits blocks misses     kb/sec    kb/sec  saved   wrs   rds
  5.00    51      1    147    370       2283      2268    0.6    48    37
  4.00    36      0    128    237      21695     21687    0.0    47    38
  4.00    48      2    179    307       8168      8154    0.2    65    33
  5.00    53      0    161    372       2894      2880    0.5    48    32
  6.00    52      0    198    328      15110     15100    0.1    63    33
  6.00    77      0    415    363       4695      4684    0.2    48    34
  7.00    85      1    417    433       5270      5251    0.4    49    35
  7.00    67      1    443    228       2242      2232    0.5    85    44
```

tcpservices命令顯示有關所選進程監聽埠的資訊。系統還會顯示每個進程以及地址和埠組合的解釋：

```
SWA_CLI> tcpservices

System Processes (Note: All processes may not always be present)
  ftpd.main    - The FTP daemon
  ginetd       - The INET daemon
  interface    - The interface controller for inter-process communication
  ipfw         - The IP firewall
  slapd        - The Standalone LDAP daemon
  sntpd        - The SNTP daemon
  sshd         - The SSH daemon
  syslogd      - The system logging daemon
  winbindd     - The Samba Name Service Switch daemon
```

```
Feature Processes
  coeuslogd    - Main WSA controller
  gui          - GUI process
  hermes       - Mail server for sending alerts, etc.
  java         - Processes for storing and querying Web Tracking data
  musd         - AnyConnect Secure Mobility server
  pacd         - PAC file hosting daemon
  prox         - WSA proxy
  trafmon      - L4 Traffic Monitor
  uds          - User Discovery System (Transparent Auth)
  wccpd        - WCCP daemon

COMMAND      USER         TYPE NODE   NAME
connector    root         IPv4 TCP    127.0.0.1:8823
java         root         IPv6 TCP    [::127.0.0.1]:18081
hybridd      root         IPv4 TCP    127.0.0.1:8833
gui          root         IPv4 TCP    172.16.40.80:8443
ginetd       root         IPv4 TCP    172.16.40.80:ssh
nginx        root         IPv6 TCP    *:4431
nginx        root         IPv4 TCP    127.0.0.1:8843
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
nginx        nobody       IPv6 TCP    *:4431
nginx        nobody       IPv4 TCP    127.0.0.1:8843
api_serve    root         IPv4 TCP    172.16.40.80:6080
api_serve    root         IPv4 TCP    127.0.0.1:60001
api_serve    root         IPv4 TCP    172.16.40.80:6443
chimera      root         IPv4 TCP    127.0.0.1:6380
nectar       root         IPv4 TCP    127.0.0.1:6382
redis-ser    root         IPv4 TCP    127.0.0.1:6383
redis-ser    root         IPv4 TCP    127.0.0.1:6379
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25255
```

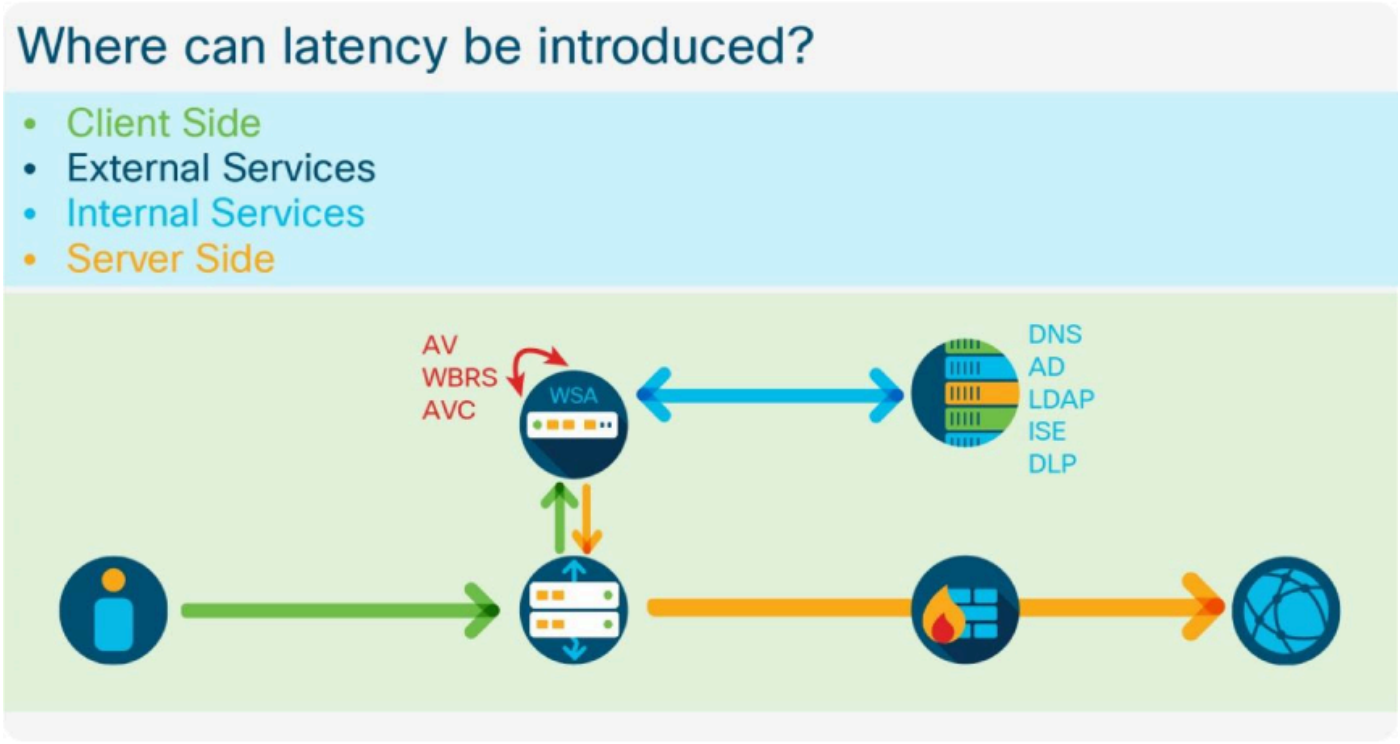
```
prox         root         IPv4 TCP    127.0.0.1:socks
prox         root         IPv6 TCP    [::1]:socks
prox         root         IPv4 TCP    172.16.11.69:socks
prox         root         IPv4 TCP    172.16.11.68:socks
prox         root         IPv4 TCP    172.16.11.252:socks
prox         root         IPv4 TCP    127.0.0.1:ftp-proxy
prox         root         IPv6 TCP    [::1]:ftp-proxy
prox         root         IPv4 TCP    172.16.11.69:ftp-proxy
prox         root         IPv4 TCP    172.16.11.68:ftp-proxy
prox         root         IPv4 TCP    172.16.11.252:ftp-proxy
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.16.11.69:https
prox         root         IPv4 TCP    172.16.11.68:https
prox         root         IPv4 TCP    172.16.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25256
prox         root         IPv4 TCP    127.0.0.1:http
prox         root         IPv6 TCP    [::1]:http
prox         root         IPv4 TCP    172.16.11.69:http
prox         root         IPv4 TCP    172.16.11.68:http
prox         root         IPv4 TCP    172.16.11.252:http
prox         root         IPv4 TCP    127.0.0.1:3128
prox         root         IPv6 TCP    [::1]:3128
prox         root         IPv4 TCP    172.16.11.69:3128
prox         root         IPv4 TCP    172.16.11.68:3128
prox         root         IPv4 TCP    172.16.11.252:3128
prox         root         IPv4 TCP    127.0.0.1:https
prox         root         IPv6 TCP    [::1]:https
prox         root         IPv4 TCP    172.21.11.69:https
prox         root         IPv4 TCP    172.21.11.68:https
prox         root         IPv4 TCP    172.21.11.252:https
prox         root         IPv4 TCP    127.0.0.1:25257
smart_age    root         IPv6 TCP    [::127.0.0.1]:65501
smart_age    root         IPv6 TCP    [::127.0.0.1]:28073
interface    root         IPv4 TCP    127.0.0.1:domain
stunnel      root         IPv4 TCP    127.0.0.1:32137
```

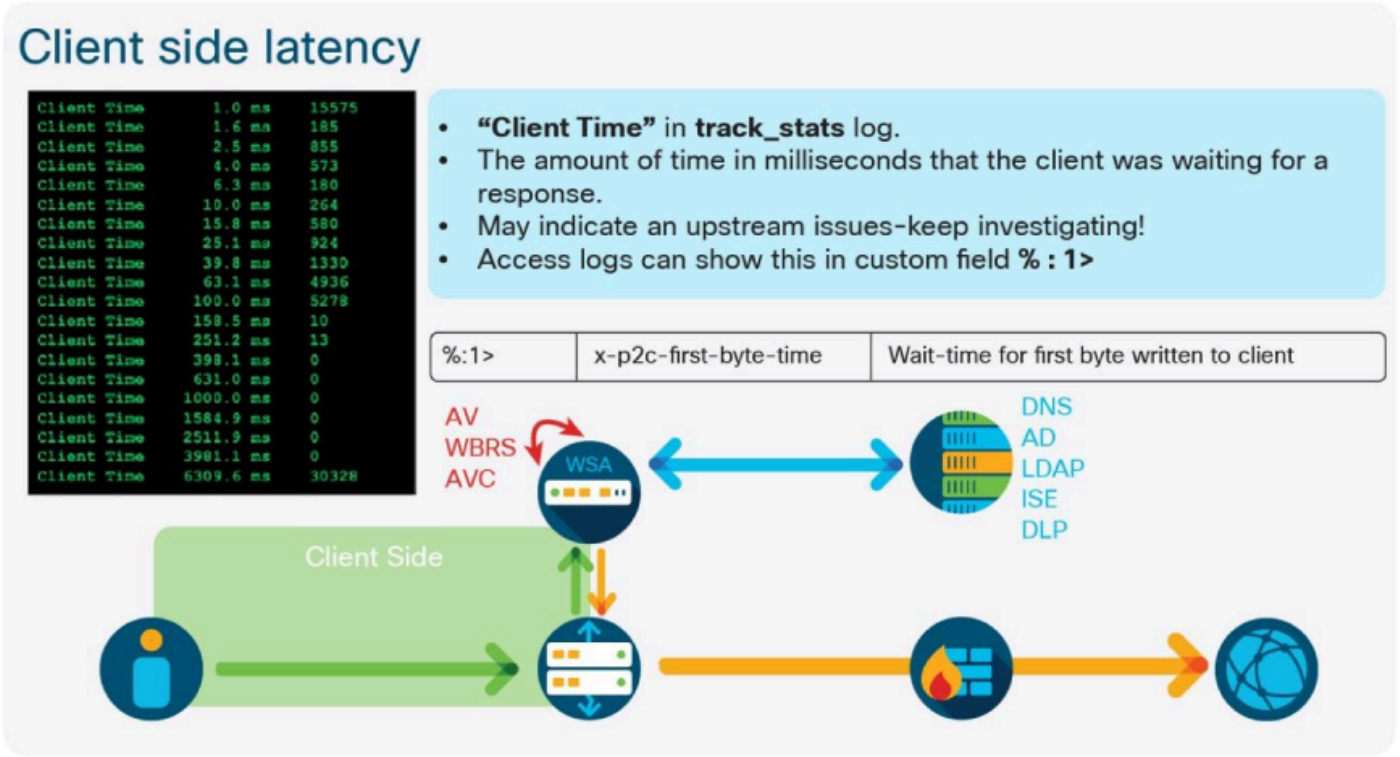
記錄

Web流量具有高度動態性和多樣性。代理部署完成後，定期重新評估透過裝置的資料流的數量和構成非常重要。您必須定期檢查解密流量的百分比（每季度一次），以確保大小與初始安裝的預期和規格一致。這可以使用日誌管理產品(例如高級網路安全報告(AWSR))或具有訪問日誌的簡單Bash或PowerShell命令來完成。還必須定期重新評估RPS的數量，以確保裝置有足夠的開銷來應對高可用性、負載平衡配置中的流量高峰和可能的故障切換。

每五分鐘會附加一次track_stats日誌，該日誌包含幾個輸出部分，這些輸出直接與prox進程及其記

憶體中的對象相關。在效能監控中最有用的部分是顯示各種請求進程的平均延遲，包括DNS查詢時間、AV引擎掃描時間和許多更有用的欄位。此日誌不能從GUI或CLI配置，只能透過安全複製協定(SCP)或檔案傳輸協定(FTP)訪問。這是排除效能故障時最重要的日誌，因此必須頻繁輪詢。



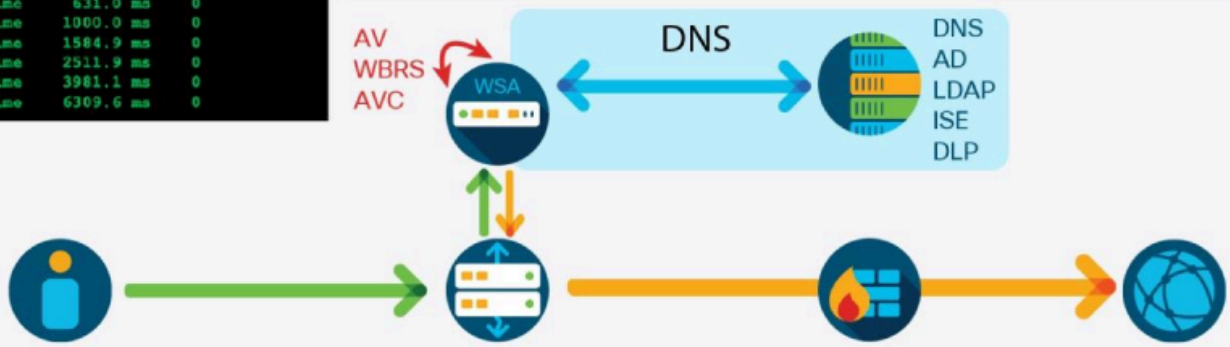


DNS latency

```
DNS Time       1.0 ms    51
DNS Time       1.6 ms    347
DNS Time       2.5 ms    152
DNS Time       4.0 ms    71
DNS Time       6.3 ms    98
DNS Time      10.0 ms    7
DNS Time      15.8 ms    11
DNS Time      25.1 ms    13
DNS Time      39.8 ms    2
DNS Time      63.1 ms    3
DNS Time     100.0 ms    7
DNS Time     158.5 ms    16
DNS Time     251.2 ms    4
DNS Time     398.1 ms    1
DNS Time     631.0 ms    0
DNS Time    1000.0 ms    0
DNS Time    1584.9 ms    0
DNS Time    2511.9 ms    0
DNS Time    3981.1 ms    0
DNS Time    6309.6 ms    0
```

- The amount of time in milliseconds that the WSA waited for a DNS response.
- Calls for investigation for your DNS resolvers (or path to them).
- **access logs** can show this in custom field **% : >d**

%:>d	x-p2p-dns-svc-time	Time taken by the Web Proxy DNS Process to send a DNS result to ehe Web proxy.

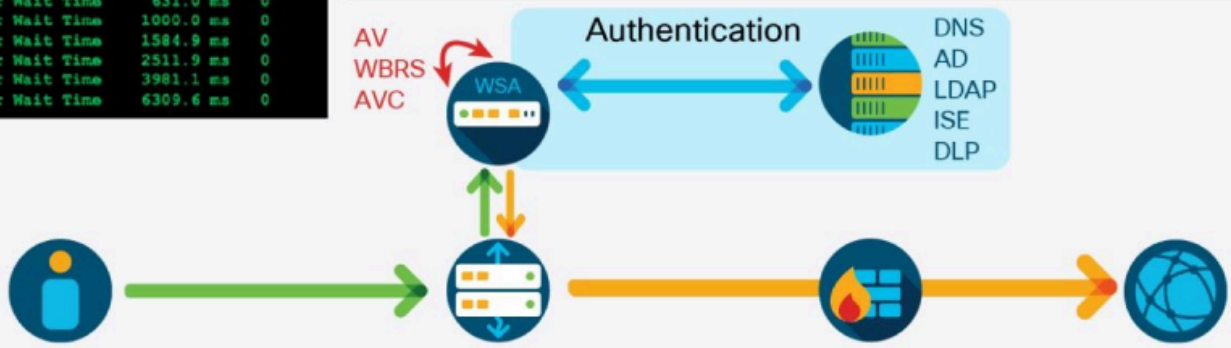


Authentication latency

```
Server Wait Time       1.0 ms    0
Server Wait Time       1.6 ms    0
Server Wait Time       2.5 ms    0
Server Wait Time       4.0 ms    0
Server Wait Time       6.3 ms    0
Server Wait Time      10.0 ms    0
Server Wait Time      15.8 ms    0
Server Wait Time      25.1 ms    0
Server Wait Time      39.8 ms    0
Server Wait Time      63.1 ms    0
Server Wait Time     100.0 ms    0
Server Wait Time     158.5 ms    1
Server Wait Time     251.2 ms    1
Server Wait Time     398.1 ms    0
Server Wait Time     631.0 ms    0
Server Wait Time    1000.0 ms    0
Server Wait Time    1584.9 ms    0
Server Wait Time    2511.9 ms    0
Server Wait Time    3981.1 ms    0
Server Wait Time    6309.6 ms    0
```

- There are two metrics: **“Auth Helper Wait Time”** and **“Auth Helper Service Wait Time.”**
- Use the first to get pure auth time without the request time added.
- **access logs** can show this in custom field **% : >a**

%:<a	x-p2p-auth-wait-time	Wait-time to receive the response from the Web Proxy authentication process, after the Web Proxy sent the request.

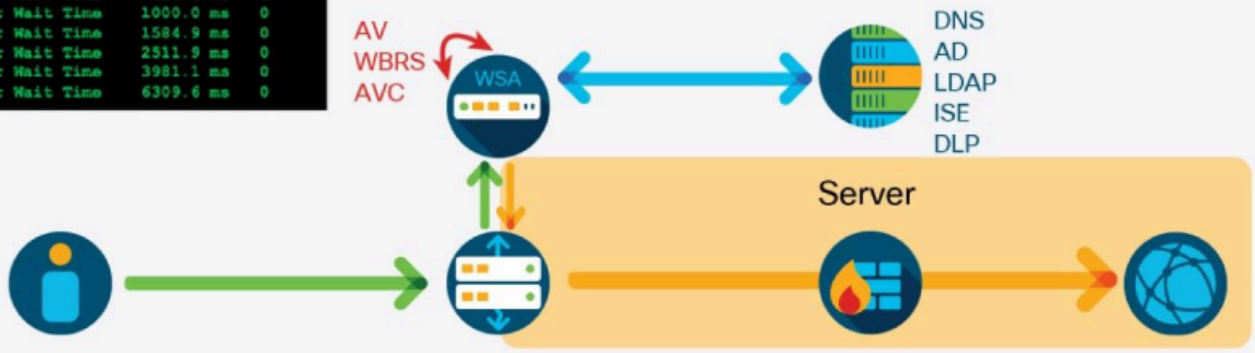


Server latency-wait time

```
Server Wait Time        1.0 ms    0
Server Wait Time        1.6 ms    0
Server Wait Time        2.5 ms    0
Server Wait Time        4.0 ms    0
Server Wait Time        6.3 ms    0
Server Wait Time       10.0 ms    0
Server Wait Time       15.8 ms    0
Server Wait Time       25.1 ms    0
Server Wait Time       39.8 ms    0
Server Wait Time       63.1 ms    0
Server Wait Time      100.0 ms    0
Server Wait Time      158.5 ms    1
Server Wait Time      251.2 ms    1
Server Wait Time      398.1 ms    0
Server Wait Time      631.0 ms    0
Server Wait Time     1000.0 ms    0
Server Wait Time     1584.9 ms    0
Server Wait Time     2511.9 ms    0
Server Wait Time     3981.1 ms    0
Server Wait Time     6309.6 ms    0
```

- The amount of time in milliseconds that the WSA waited for the first byte of the server response.
- Calls for investigation of your upstream devices and WAN connection.
- **access logs** can show this in custom field **% : >1**

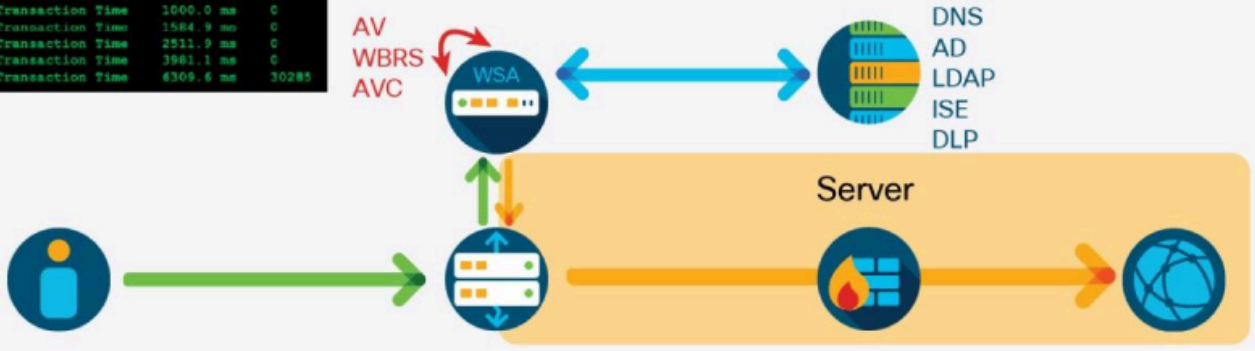
%:>1	x-s2p-first-byte-time	Wait-time for first response byte from server

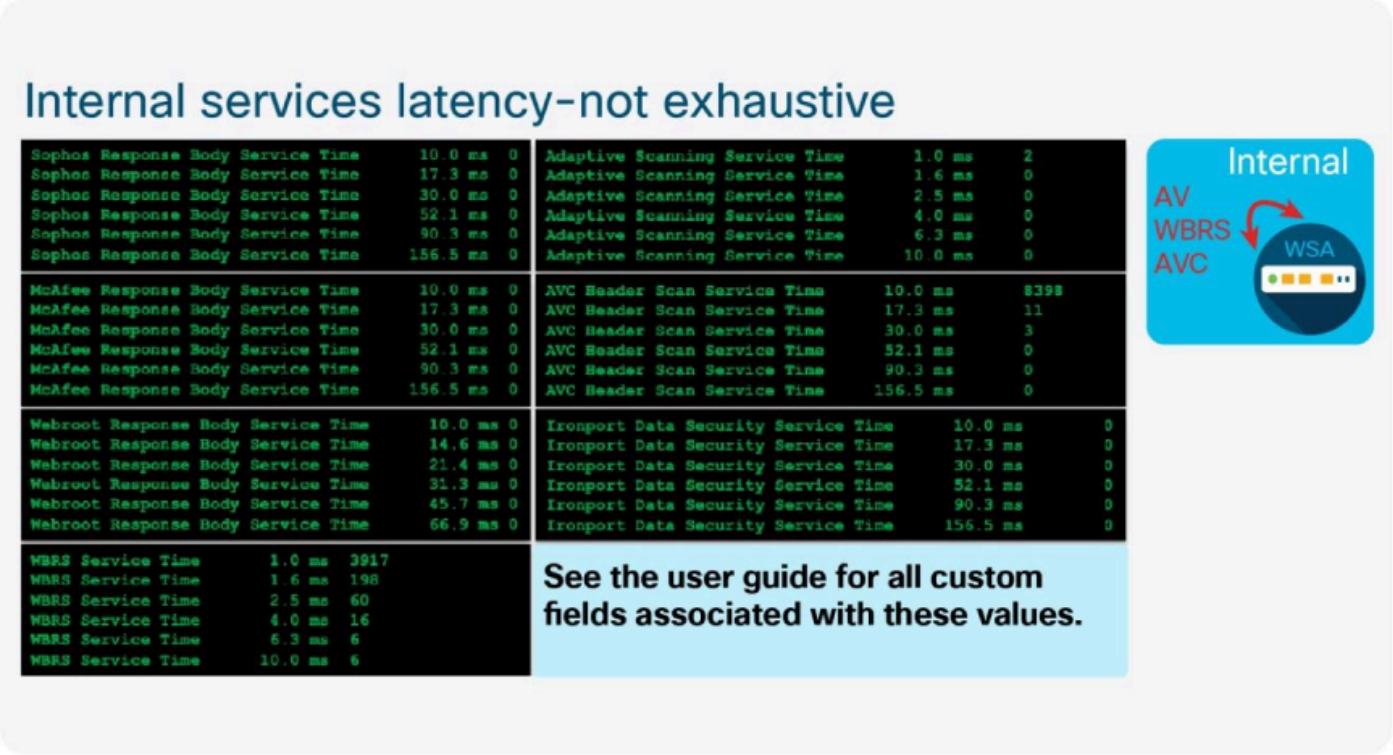


Server latency-transaction time

```
Server Transaction Time        1.0 ms    1422
Server Transaction Time        1.6 ms    858
Server Transaction Time        2.5 ms    1035
Server Transaction Time        4.0 ms    1106
Server Transaction Time        6.3 ms    758
Server Transaction Time       10.0 ms    810
Server Transaction Time       15.8 ms    288
Server Transaction Time       25.1 ms    45
Server Transaction Time       39.8 ms    73
Server Transaction Time       63.1 ms    4221
Server Transaction Time      100.0 ms    8897
Server Transaction Time      158.5 ms    5
Server Transaction Time      251.2 ms    0
Server Transaction Time      398.1 ms    2
Server Transaction Time      631.0 ms    0
Server Transaction Time     1000.0 ms    0
Server Transaction Time     1584.9 ms    0
Server Transaction Time     2511.9 ms    0
Server Transaction Time     3981.1 ms    0
Server Transaction Time     6309.6 ms    30285
```

- The amount of time in milliseconds for the entire server-side transaction to complete.
- Calls for investigation of your upstream devices and WAN connection.
- No **access logs** custom field, but can be determined by a combinationof them.





每隔60秒就會寫入一條SHD日誌行，其中包含許多對效能監控很重要的欄位，包括延遲、RPS以及客戶端和伺服器端的總連線。以下是SHD日誌行的示例：

```
Fri Nov 11 14:16:42 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 62 Band 11383 Latency 61
Fri Nov 11 14:17:42 2022 Info: Status: CPULd 2.6 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 10532 Latency 77
Fri Nov 11 14:18:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.6 Reqs 48 Band 7285 Latency 579
Fri Nov 11 14:19:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.6 Reqs 52 Band 34294 Latency 79
Fri Nov 11 14:20:43 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 8696 Latency 691
Fri Nov 11 14:21:43 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 49 Band 7064 Latency 140
Fri Nov 11 14:22:43 2022 Info: Status: CPULd 1.9 DskUtil 45.7 RAMUtil 6.8 Reqs 41 Band 5444 Latency 788
Fri Nov 11 14:23:43 2022 Info: Status: CPULd 2.2 DskUtil 45.7 RAMUtil 6.8 Reqs 48 Band 6793 Latency 820
Fri Nov 11 14:24:44 2022 Info: Status: CPULd 2.3 DskUtil 45.7 RAMUtil 6.7 Reqs 44 Band 8735 Latency 673
Fri Nov 11 14:25:44 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 53 Band 8338 Latency 731
```

其他自訂欄位可以新增至access_logs，代表個別要求的延遲資訊。這些欄位包括伺服器響應、DNS解析和AV掃描器延遲。這些欄位必須增加到日誌中，以收集用於故障排除的重要資訊。建議使用以下自訂欄位字串：

```
[ Request Details: ID = %I, User Agent = %u, AD Group Memberships = ( %m ) %g ] [ Tx Wait Times (in ms)
```

```
, Response Header = %:h>, Client Body = %:b> ] [ Rx Wait Times (in ms): 1st request byte = %:1<,
```

```
a; DNS response = %:

 d, WBRS response = %:

  r, AVC response = %:A>, AVC total = %:A<, DCA response = %:C>, DCA total = %:C<, McAfee respon

   s, AMP response = %:e>, AMP total = %:e<; Latency = %x; %L ][Client Port = %F, Server IP = %k
```

從這些值衍生的效能資訊如下：

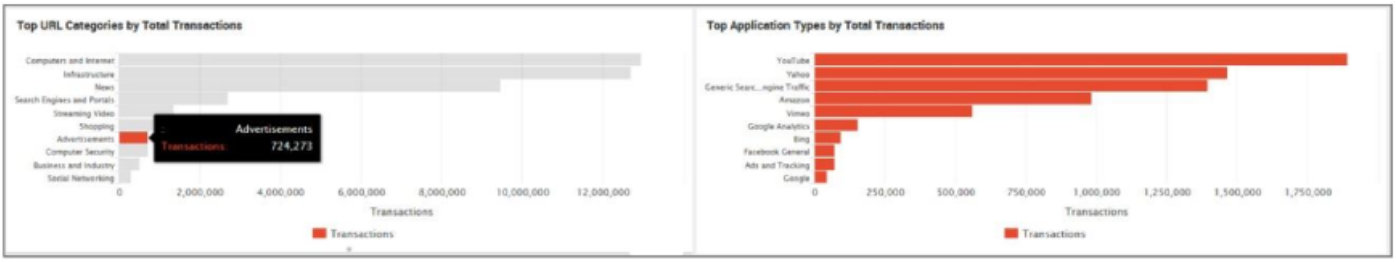
自定義欄位	說明
%：<a	在Web代理傳送請求後，從Web代理身份驗證過程接收響應的等待時間。
%：<b	在標頭之後將要求主體寫入伺服器的等待時間。
%：<d	在Web代理傳送請求後，從Web代理DNS進程接收響應的等待時間。
%：<h	第一個位元組之後將要求標頭寫入伺服器的等待時間。
%：<r	Web代理傳送請求後，從Web信譽過濾器接收響應的等待時間。
%：<s	在Web代理傳送請求後，從Web代理反間諜軟體進程接收判定結果的等待時間。
%：>	伺服器第一個回應位元組的等待時間。
%：>a	從Web代理身份驗證過程接收響應的等待時間，包括Web代理傳送請求所需的時間。

%：>b	收到標頭後等待完整回應主體的時間。
%：>c	Web代理從磁碟快取讀取響應所需的時間。
%：>d	從Web代理DNS進程接收響應的等待時間，包括Web代理傳送請求所需的時間。
%：>h	第一個回應位元組之後的伺服器標頭等待時間。
%：>r	從Web信譽過濾器接收裁決的等待時間，包括Web代理傳送請求所需的時間。
%：>s	從Web代理反間諜軟體進程接收判定結果的等待時間，包括Web代理傳送請求所需的時間。
%：1<	等待新客戶端連線的第一個請求位元組的時間。
%：1>	第一個位元組寫入客戶端的等待時間。
%：b<	等待完整的客戶端正文的時間。
%：b>	將完整主體寫入客戶端的等待時間。
%：e>	Web代理傳送請求後，從AMP掃描引擎接收響應的等待時間。
%：e<	從AMP掃描引擎接收判定結果的等待時間，包括Web代理傳送請求所需的時間。
%：h<	第一個位元組後等待完成客戶端報頭的時間。
%：h>	將完整標頭寫入使用者端的等待時間。
%：m<	從McAfee掃描引擎接收判定結果的等待時間，包括Web代理傳送請求所需的時間。
%：m>	在Web代理傳送請求後，從McAfee掃描引擎接收響應的等待時間。
%F	客戶端源埠。
%p	Web伺服器埠。
%k	資料來源IP地址（Web伺服器IP地址）。
%：w<	從Webroot掃描引擎接收判定結果的等待時間，包括Web代理傳送請求所需的時間。
%：w>	Web代理傳送請求後，從Webroot掃描引擎接收響應的等待時間。

SWA許可模式允許對虛擬裝置重複使用物理裝置許可證。您可以利用此優勢並部署測試SWAv裝置以便在實驗室環境中使用。新功能和配置可透過這種方式進行試用，以確保穩定性和可靠性，同時不會違反許可條款。

進階網路安全報告(AWSR)

必須利用AWSR來充分利用全部門辦法的報告資料。特別是在部署了許多SWA的環境中，此解決方案的可擴充性比在安全管理裝置(SMA)上使用集中報告要高許多倍，並且提供自定義報告屬性，為資料增加了大量的深度和定製性。報告可以分組和定製，以滿足任何組織的需求。必須利用Cisco Advanced Services組確定AWSR的大小。



電子郵件警示

SWA上的內建電子郵件警報系統最好用作基本警報系統。必須適在地修改它以滿足管理員的需要，因為如果所有資訊事件都啟用，它可能會非常嘈雜。限制警報並主動監控它們比對所有警報都發出警報並將其視為垃圾郵件更重要。

警示設定	組態
傳送警報時使用的發件人地址	自動產生
傳送重複警報之前等待的初始秒數	300秒
傳送重複警示前等待的最大秒數	3600秒

可用性監控

有兩種方法可用於監控Web代理的可用性。

1. 第一種是第3層(L3)監控，測試裝置IP地址在網路上是否可以訪問。測試此情況的最簡單方法是定期向地址傳送ICMP響應(ping)請求並檢查應答資料包。可以分析回覆的屬性（如TTL和延遲）以確定網路層的運行狀況。
2. 裝置可以響應ping，但Proxy進程可能無響應或間歇性中斷。因此，建議使用第7層(L7)監控器，該監控器向裝置傳送顯式代理請求，並需要200 OK HTTP響應代碼。這不僅測試網路介面的可達性，而且測試代理服務的響應性以及如果請求外部資源時上游服務的可行性。此監控型別通常採用請求代理連線到資源的顯式HTTP HEAD請求的形式。HEAD方法請求客戶端傳送GET請求時返回的報頭，但僅包括響應報頭而不包括資料。
    - 如果使用L7監控工具或指令碼，請確保流量免於身份驗證，這一點非常重要。否則，將導致常規身份驗證失敗和資源消耗。在監控工具中使用自定義使用者代理字串時，必須使用該字串來辨識流量。即使流量免於身份驗證，仍可透過訪問策略限制其不必要地訪問Internet。

當您使用其中一種或多種方法時，管理員必須建立代理響應周圍可接受度量的基線，並使用該基線來構建警報閾值。在決定如何配置閾值和警報之前，您必須專門花時間收集這些檢查的響應。

SNMP監控

簡單網路管理協定(SNMP)是監控裝置運行狀況的主要方法。它可用於接收來自裝置的警報（陷阱）或輪詢各種對象識別符號(OID)以收集資訊。SWA上有許多OID涵蓋從硬體到資源使用到單個流程資訊和請求統計的所有內容。

由於硬體和效能相關的原因，有許多特定電腦資訊庫(MIB)必須受到監控。MIB完整清單請見：https://www.cisco.com/web/ironport/tools/web/asyncosweb-mib.txt。

這是建議監控的MIB清單，而不是詳盡的清單：

硬體OID	名稱
1.3.6.1.4.1.15497.1.1.1.18.1.3	raidID
1.3.6.1.4.1.15497.1.1.1.18.1.2	raidStatus
1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLastError
1.3.6.1.4.1.15497.1.1.1.10	fanTable
1.3.6.1.4.1.15497.1.1.1.9.1.2	攝氏度

這是OID直接對映到status detail CLI命令的輸出：

OID	名稱	狀態詳細資訊欄位
系統資源		
1.3.6.1.4.1.15497.1.1.1.2.0	百分比	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	百分比記憶體利用率	RAM
每秒交易數		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruNow	最後一分鐘內的平均每秒交易數。
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cacheThru1hrPeak	過去一小時內每秒交易數目上限。
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheThru1hrMean	過去一小時內每秒的平均作業事件。
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruLifePeak	代理重新啟動後每秒的最大事務數。
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheThruLifeMean	代理重新啟動後每秒的平均事務數。
頻寬		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBwidthTotalnow	過去一分鐘內的平均頻寬。
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBwidthTotal1hrPeak	過去一小時內的最大頻寬。
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBwidthTotal1hrMean	過去一小時的平均頻寬。
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBwidthTotalLifePeak	代理重新啟動後的最大頻寬。
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBwidthTotalLifeMean	代理重新啟動後的平均頻寬。
回應時間		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	快取命中	過去一分鐘內的平均快取命中率。
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cacheHits1hrPeak	過去一小時內快取命中率上限。
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrMean	過去一小時的平均快取命中率。

1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	代理重新啟動後的最大快取命中率。
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	代理重新啟動後的平均快取記憶體命中率。
快取命中率		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	快取命中	過去一分鐘內的平均快取命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cacheHits1hrPeak	過去一小時內快取命中率上限。
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrMean	過去一小時的平均快取命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	代理重新啟動後的最大快取命中率。
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	代理重新啟動後的平均快取記憶體命中率。
連線		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	空閒客戶端連線。
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleConns	空閒伺服器連線。
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClientTotalConns	使用者端連線總數。
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotalConns	伺服器連線總數。

結論

本指南旨在說明SWA配置、部署和監控的最重要方面。作為參考指南，其目標是為那些希望確保最有效地使用全部門辦法的人提供有價值的資訊。此處介紹的最佳實踐對於裝置作為安全工具的穩定性、可擴充性和有效性非常重要。它還尋求隨著相關資源的不斷發展而繼續保留，因此必須經常更新以反映網路環境和產品功能集的變化。

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）。