

Best Practices für sichere Web-Appliances

Inhalt

[Einleitung](#)

[Hintergrundinformationen](#)

[Netzwerkumgebung](#)

[ICMP](#)

[Firewalls](#)

[Unicast Reverse Path Forwarding](#)

[IP-Spoofing mit WCCP](#)

[SWA-Netzwerkkonfiguration](#)

[Schnittstellen](#)

[Management-Netzwerkrouting](#)

[TALOS-Telemetrie](#)

[DNS](#)

[Lastenausgleich](#)

[Aktive Authentifizierung](#)

[Passive Authentifizierung](#)

[Servicekonfiguration](#)

[Webproxy](#)

[HTTPS-Proxy](#)

[Layer-4-Datenverkehrsüberwachung \(L4TM\)](#)

[Richtlinienkonfiguration](#)

[Komplexität](#)

[Identifikationsprofile](#)

[Entschlüsselungsrichtlinien](#)

[Zugriffsrichtlinien](#)

[Benutzerdefinierte und externe URL-Kategorien](#)

[Monitore und Warnmeldungen](#)

[CLI-Monitore](#)

[Protokollieren](#)

[Advanced Web Security Reporting \(AWSR\)](#)

[E-Mail-Benachrichtigung](#)

[Verfügbarkeitsüberwachung](#)

[SNMP-Überwachung](#)

[Schlussfolgerung](#)

Einleitung

In diesem Dokument werden die Best Practices für die Konfiguration der Cisco Secure Web Appliance (SWA) beschrieben.

Hintergrundinformationen

Dieser Leitfaden soll als Referenz für die Konfiguration anhand von Best Practices dienen. Er behandelt viele Aspekte einer SWA-Bereitstellung, einschließlich der unterstützten Netzwerkumgebung, der Richtlinienkonfiguration, der Überwachung und der Fehlerbehebung. Die hier dokumentierten Best Practices sind zwar für alle Administratoren, Architekten und Betreiber wichtig zu verstehen, stellen jedoch nur Richtlinien dar und müssen entsprechend behandelt werden. Jedes Netzwerk hat seine eigenen

spezifischen Anforderungen und Herausforderungen.

Als Sicherheitsgerät kommuniziert der SWA auf verschiedene Weise mit dem Netzwerk. Er ist Quelle und Ziel von Web-Datenverkehr und fungiert gleichzeitig als Webserver und Web-Client. Dabei werden mindestens serverseitige Techniken wie IP-Adressen-Spoofing und Man-in-the-Middle-Techniken verwendet, um HTTPS-Transaktionen zu überprüfen. Darüber hinaus können Client-IP-Adressen getäuscht werden, wodurch die Bereitstellung noch komplexer wird und zusätzliche Anforderungen an die Netzwerkkonfiguration gestellt werden. In diesem Handbuch werden die häufigsten Probleme im Zusammenhang mit der Konfiguration der Netzwerkgeräte behandelt.

Die Konfiguration der SWA-Richtlinien wirkt sich nicht nur auf die Effektivität der Absicherung und Durchsetzung der Richtlinien aus, sondern auch auf die Leistung der Appliance. In diesem Leitfaden wird erläutert, wie sich die Komplexität einer Konfiguration auf die Systemressourcen auswirkt. Sie definiert Komplexität in diesem Kontext und beschreibt, wie sie im Richtlinienentwurf minimiert werden kann. Bestimmte Funktionen und ihre Konfiguration sind ebenfalls wichtig, um Sicherheit, Skalierbarkeit und Effizienz zu erhöhen.

Im Abschnitt Überwachung und Warnmeldungen dieses Dokuments werden die effektivsten Methoden zur Überwachung der Appliance erläutert. Außerdem werden die Überwachung von Leistung und Verfügbarkeit sowie die Nutzung von Systemressourcen behandelt. Darüber hinaus enthält es nützliche Informationen zur grundlegenden Fehlerbehebung.

Netzwerkumgebung

ICMP

Path MTU Discovery (MTU-Pfaderkennung), wie in [RFC 1191](#) definiert, legt den Mechanismus die maximale Größe eines Pakets entlang beliebiger Pfade fest. Im Fall von IPv4 kann ein Gerät die Maximum Transmission Unit (MTU) eines Pakets auf einem Pfad bestimmen, indem es das Donâ€™t Fragment (DF)-Bit im IP-Header des Pakets festlegt. Wenn ein Gerät an einem Link entlang des Pfads das Paket nicht ohne Fragmentierung weiterleiten kann, wird eine **ICMP-Fragmentierung (Internet Control Message Protocol) erforderlich (Typ 3, Code 4)** Nachricht an die Quelle zurückgesendet. Der Client sendet dann ein kleineres Paket erneut. Dieser Vorgang wird fortgesetzt, bis die MTU für den vollständigen Pfad erkannt wird. IPv6 unterstützt keine Fragmentierung und verwendet eine ICMPv6-Nachricht vom Typ "Packet Too Big" (Zu große Pakete, Typ 2), um anzuzeigen, dass ein Paket nicht über eine bestimmte Verbindung passt.

Da der Prozess der Paketfragmentierung die Leistung eines TCP-Datenflusses erheblich beeinträchtigen kann, verwendet die SWA die MTU-Pfaderkennung. Die genannten ICMP-Meldungen müssen in den entsprechenden Netzwerkgeräten aktiviert werden, damit die SWA die MTU für ihren Pfad durch das Netzwerk bestimmen kann. Dieses Verhalten kann in der SWA mithilfe des Befehls `pathmtudiscovery` **Command-Line Interface (CLI) deaktiviert** werden. Dadurch sinkt die Standard-MTU auf 576 Byte (gemäß RFC 879), was die Leistung erheblich beeinträchtigt. Der Administrator muss zusätzlich die MTU in der SWA manuell konfigurieren von `etherconfig` CLI-Befehl.

Im Fall des **Web Cache Communication Protocol (WCCP)** wird der Web-Datenverkehr von einem anderen Netzwerkgerät entlang des Client-Pfads zum Internet an die SWA umgeleitet. In diesem Fall werden andere Protokolle, z. B. ICMP, nicht an die SWA umgeleitet. Es besteht die Möglichkeit, dass der SWA eine Meldung auslösen könnte, dass ein Router im Netzwerk eine ICMP-Fragmentierung benötigt, die

Meldung jedoch nicht an den SWA gesendet wird. Wenn dies im Netzwerk möglich ist, muss die MTU-Pfaderkennung deaktiviert werden. Wie bereits erwähnt, ist bei dieser Konfiguration der zusätzliche Schritt zum manuellen Einstellen der MTU auf dem SWA von `etherconfig` CLI-Befehl ist erforderlich.

Firewalls

In einer Standardkonfiguration macht der SWA beim Proxying einer Verbindung keinen Spoofing-Vorgang für die Client-IP-Adresse durch. Das bedeutet, dass der gesamte ausgehende Internetdatenverkehr von der SWA-IP-Adresse stammt. Es muss sichergestellt werden, dass **NAT-Geräte (Network Address Translation)** über einen ausreichenden Pool an externen Adressen und Ports verfügen, um dies zu ermöglichen. Es ist eine gute Idee, diesem Zweck eine bestimmte Adresse zu widmen.

Einige Firewalls verwenden **Denial-of-Service (DoS)**-Schutz oder andere Sicherheitsfunktionen, die ausgelöst werden, wenn eine große Anzahl gleichzeitiger Verbindungen von einer einzigen Client-IP-Adresse ausgeht. Wenn Client-IP-Spoofing nicht aktiviert ist, muss die SWA-IP-Adresse von diesen Schutzmaßnahmen ausgeschlossen werden.

Unicast Reverse Path Forwarding

Die SWA spiegelt die Server-IP-Adresse bei der Kommunikation mit einem Client wider und kann optional so konfiguriert werden, dass sie bei der Kommunikation mit einem Upstream-Server gespiegelt wird. Schutzfunktionen wie **Unicast Reverse Path Forwarding (uRPF)** können auf Switches aktiviert werden, um sicherzustellen, dass ein eingehendes Paket mit dem erwarteten Eingangsport übereinstimmt. Bei diesen Schutzmaßnahmen wird die Quellschnittstelle eines Pakets anhand der Routing-Tabelle überprüft, um sicherzustellen, dass es am erwarteten Port angekommen ist. Die SWA müssen gegebenenfalls von diesen Schutzmaßnahmen ausgenommen werden.

IP-Spoofing mit WCCP

Wenn die IP-Spoofing-Funktion im SWA aktiviert ist, behalten ausgehende Anfragen die Appliance bei und verwenden die Quelladresse der ursprünglichen Client-Anfrage. Dies erfordert eine zusätzliche Konfiguration der zugehörigen Netzwerkinfrastruktur, um sicherzustellen, dass Rückgabepakete an die ausgehende SWA-Schnittstelle und nicht an den Client, von dem die Anforderung stammt, weitergeleitet werden.

Wenn WCCP auf einem Netzwerkgerät (Router, Switch oder Firewall) implementiert ist, wird eine Dienst-ID definiert, die den Datenverkehr anhand einer **Zugriffskontrollliste (ACL)** vergleicht. Die Service-ID wird dann auf eine Schnittstelle angewendet und zur Zuordnung des Datenverkehrs für die Umleitung verwendet. Wenn IP-Spoofing aktiviert ist, muss eine zweite Dienst-ID erstellt werden, um sicherzustellen, dass auch der zurückkehrende Datenverkehr an die SWA umgeleitet wird.

30 Minuten alle Einträge in der Umgehungseinstellungsliste auf, unabhängig von der **Time to Live (TTL)** des Datensatzes. Wenn die L4TM-Funktion jedoch aktiviert ist, kann der SWA Snooped-DNS-Abfragen verwenden, um diese Datensätze häufiger zu aktualisieren. Dadurch wird das Risiko eines Fehlalarms in einem Szenario reduziert, in dem der Client eine andere Adresse als den SWA aufgelöst hat.

Management-Netzwerkrouting

Wenn das dedizierte Managementnetzwerk nicht über einen Internetzugang verfügt, kann für jeden Dienst die Verwendung der Datenweiterleitungstabelle konfiguriert werden. Dieser kann an die Netzwerktopologie angepasst werden. Im Allgemeinen wird jedoch empfohlen, das Managementnetzwerk für alle Systemdienste und das Datennetzwerk für den Client-Datenverkehr zu verwenden. Ab AsyncOS Version 11.0 kann das Routing für folgende Dienste festgelegt werden:

- Externe URL-Feeds
- **Advanced Malware Protection (AMP)**-Dateireputation und -analyse
- Updates und Upgrades
- DNS
- Active Directory

Für eine zusätzliche Ausgangsfilterung des Verwaltungsdatenverkehrs können statische Adressen für die Verwendung in den folgenden Services konfiguriert werden:

- Externe URL-Feeds:
 1. Benutzerdefiniert hängt davon ab, wo sie gehostet werden
 2. Reputation und Analyse von AMP-Dateien
 3. cloud-sa.amp.cisco.com (Nordamerika)
 4. cloud-sa.eu.amp.cisco.com (Europa)
 5. cloud-sa.apjc.amp.cisco.com (Asien/Pazifik)
- Updates und Upgrades:
 1. downloads-static.ironport.com
 2. updates-static.ironport.com

TALOS-Telemetrie

Die Cisco Talos-Gruppe ist dafür bekannt, neue Bedrohungen zu identifizieren. Alle an Talos übermittelten Daten werden anonymisiert und in US-amerikanischen Rechenzentren gespeichert. Die Teilnahme an SensorBase verbessert die Kategorisierung und Identifizierung von Web-Bedrohungen und führt zu einem besseren Schutz vor den SWAs und anderen Cisco Sicherheitslösungen.

DNS

Nach den Best Practices für die DNS-Sicherheit muss jedes Netzwerk zwei DNS-Resolver hosten: einen für autoritative Datensätze innerhalb einer lokalen Domäne und einen für die rekursive Auflösung von Internet-Domänen. Um dies zu ermöglichen, lassen die SWAs DNS-Server für bestimmte Domänen konfigurieren. Wenn nur ein DNS-Server für lokale und rekursive Abfragen verfügbar ist, sollten Sie die zusätzliche Last berücksichtigen, die er bei Verwendung für alle SWA-Abfragen hinzufügt. Die bessere Option besteht darin, den internen Resolver für lokale Domänen und den Root-Internet-Resolver für externe Domänen zu verwenden. Dies hängt vom Risikoprofil und der Toleranz des Administrators ab.

Standardmäßig speichern die SWA einen DNS-Eintrag mindestens 30 Minuten im Cache, unabhängig vom TTL des Eintrags. Moderne Websites, die **Content Delivery Networks (CDNs)** intensiv nutzen, verfügen über niedrige TTL-Werte, da sich ihre IP-Adressen häufig ändern. Dies kann dazu führen, dass ein Client eine IP-Adresse für einen bestimmten Server zwischenspeichert und der SWA eine andere Adresse für

denselben Server zwischenspeichert. Um dem entgegenzuwirken, kann die Standard-TTL für SWA von den folgenden CLI-Befehlen auf fünf Minuten herabgesetzt werden:

```
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.
...
```

Falls der primäre DNS-Server nicht verfügbar ist, müssen sekundäre DNS-Server konfiguriert werden. Wenn alle Server mit derselben Priorität konfiguriert sind, wird die Server-IP nach dem Zufallsprinzip ausgewählt. Abhängig von der Anzahl der konfigurierten Server ist die Zeitüberschreitung für einen bestimmten Server unterschiedlich. Die Tabelle gibt das Timeout für eine Abfrage für bis zu sechs DNS-Server an:

Anzahl der DNS-Server	Abfragetimeout (in der Sequenz)
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

Darüber hinaus gibt es erweiterte DNS-Optionen, die nur über die CLI verfügbar sind. Die folgenden Optionen stehen in der CLI zur Verfügung:

advancedproxyconfig > DNS aus. Wählen Sie eine der folgenden Optionen aus:

- 0 - DNS-Antworten immer in der richtigen Reihenfolge verwenden
- 1 - Verwenden Sie die vom Client angegebene Adresse und dann DNS
- 2 - Eingeschränkte DNS-Nutzung
- 3 - Sehr begrenzte DNS-Nutzung

Bei den Optionen 1 und 2 wird DNS verwendet, wenn die Webreputation aktiviert ist.

Bei den Optionen 2 und 3 wird DNS für explizite Proxyanforderungen verwendet, wenn kein

Upstreamproxy vorhanden ist oder der konfigurierte Upstreamproxy fehlschlägt.

Bei allen Optionen wird DNS verwendet, wenn Ziel-IP-Adressen in der Richtlinienmitgliedschaft verwendet werden.

Diese Optionen steuern, wie der SWA bei der Auswertung einer Client-Anforderung die IP-Adresse festlegt, mit der eine Verbindung hergestellt werden soll. Wenn eine Anforderung eingeht, sieht der SWA eine Ziel-IP-Adresse und einen Hostnamen. Der SWA muss entscheiden, ob er der ursprünglichen Ziel-IP-Adresse für die TCP-Verbindung vertrauen oder ob er eine eigene DNS-Auflösung durchführen und die aufgelöste Adresse verwenden möchte. Der Standardwert ist "0 = DNS-Antworten immer in der richtigen Reihenfolge verwenden". Dies bedeutet, dass der SWA dem Client nicht vertraut, um die IP-Adresse anzugeben.

- Option 1 - Der SWA versucht die vom Client bereitgestellte IP-Adresse für die Verbindung, greift jedoch auf die aufgelöste Adresse zurück, wenn dies fehlschlägt. Die aufgelöste Adresse wird für die Richtlinienbewertung verwendet (Webkategorie, Webreputation usw.).
- Option 2 - Der SWA verwendet nur die vom Client bereitgestellte Adresse für die Verbindung und greift nicht zurück. Die aufgelöste Adresse wird für die Richtlinienbewertung (Webkategorie, Webreputation usw.) verwendet.
- Option 3 - Der SWA verwendet nur die vom Client bereitgestellte Adresse für die Verbindung und greift nicht zurück. Die vom Client bereitgestellte IP-Adresse wird für die Richtlinienbewertung verwendet (Webkategorie, Webreputation usw.).

Die gewählte Option hängt davon ab, wie viel Vertrauen der Administrator dem Client anvertrauen muss, wenn er die aufgelöste Adresse für einen bestimmten Hostnamen ermittelt. Wenn es sich bei dem Client um einen Downstream-Proxy handelt, wählen Sie Option 3 aus, um die zusätzliche Latenz unnötiger DNS-Abfragen zu vermeiden.

Lastenausgleich

WCCP ermöglicht ein transparentes Load Balancing des Datenverkehrs, wenn bis zu acht Appliances verwendet werden. Sie ermöglicht die Verteilung von Datenverkehrsflüssen auf der Basis von Hash oder Maske. Sie kann gewichtet werden, wenn verschiedene Appliance-Modelle im Netzwerk vorhanden sind, und Geräte können ohne Ausfallzeiten zum Service-Pool hinzugefügt oder daraus entfernt werden. Sobald der Bedarf die Kapazitäten von acht SWAs übersteigt, wird die Verwendung eines dedizierten Load Balancers empfohlen.

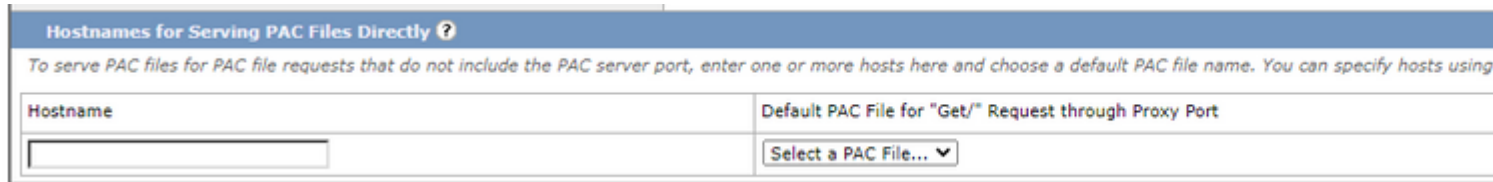
Die spezifischen Best Practices für die WCCP-Konfiguration unterscheiden sich je nach verwendeter Plattform. Die Best Practices für Cisco Catalyst® Switches sind im [Cisco Catalyst Instant Access Solution Whitepaper](#) dokumentiert.

Bei Verwendung von WCCP mit einer Cisco Adaptive Security Appliance (ASA) gelten Einschränkungen. Client-IP-Spoofing wird nicht unterstützt, und die Clients und SWA müssen sich hinter derselben Schnittstelle befinden. Aus diesem Grund ist die Verwendung eines Layer-4-Switches oder -Routers zur Umleitung des Datenverkehrs flexibler. Die WCCP-Konfiguration auf der ASA-Plattform wird unter [WCCP auf ASA](#) beschrieben: [Konzepte, Einschränkungen und Konfiguration](#).

Bei expliziten Bereitstellungen stellt eine Proxy Autoconfiguration (PAC)-Datei die am häufigsten bereitgestellte Methode dar. Sie hat jedoch zahlreiche Nachteile und Sicherheitsauswirkungen, die über den Rahmen dieses Dokuments hinausgehen. Wenn eine PAC-Datei bereitgestellt wird, wird empfohlen, den Speicherort mithilfe von Gruppenrichtlinienobjekten (Group Policy Objects, GPOs) zu konfigurieren, anstatt sich auf das Webproxy Autoermittlungsprotokoll (WPAD) zu verlassen, das ein häufiges Ziel für Angreifer ist und bei falscher Konfiguration leicht ausgenutzt werden kann. Der SWA kann mehrere PAC-Dateien

hosten und deren Ablauf im Browser-Cache steuern.

Eine PAC-Datei kann direkt vom SWA über eine konfigurierbare TCP-Portnummer angefordert werden (standardmäßig 9001). Wenn kein Port angegeben ist, kann die Anforderung an den Proxy-Prozess selbst gesendet werden, als handele es sich um eine ausgehende Webanforderung. In diesem Fall ist es möglich, eine bestimmte PAC-Datei basierend auf dem HTTP-Host-Header in der Anfrage bereitzustellen.



Kerberos muss bei Verwendung in einer Umgebung mit hoher Verfügbarkeit anders konfiguriert werden. Der SWA bietet Unterstützung für Keytab-Dateien, sodass mehrere Hostnamen mit einem **Service Principle Name (SPN)** verknüpft **werden können**. Weitere Informationen finden Sie unter [Erstellen eines Dienstkontos in Windows Active Directory für die Kerberos-Authentifizierung in Hochverfügbarkeitsbereitstellungen](#) .

Aktive Authentifizierung

Kerberos ist ein sichereres und weit verbreitetes Authentifizierungsprotokoll als **NT LAN Manager Security Support Provider (NTLMSSP)**. Das Apple OS X-Betriebssystem unterstützt NTLMSSP nicht, kann sich jedoch mithilfe von Kerberos authentifizieren, wenn die Domäne hinzugefügt wird. Die Standardauthentifizierung darf nicht verwendet werden, da sie Anmeldeinformationen unverschlüsselt im HTTP-Header sendet und von einem Angreifer im Netzwerk leicht gesniffen werden kann. Wenn die Standardauthentifizierung verwendet werden muss, muss die Verschlüsselung der Anmeldeinformationen aktiviert werden, um sicherzustellen, dass die Anmeldeinformationen über einen verschlüsselten Tunnel gesendet werden.

Der Konfiguration muss mehr als ein Domain Controller hinzugefügt werden, um die Verfügbarkeit sicherzustellen. Ein Load Balancing dieses Datenverkehrs ist jedoch nicht erforderlich. Die SWA senden ein TCP-SYN-Paket an alle konfigurierten Domänencontroller, und der erste, der antwortet, wird für die Authentifizierung verwendet.

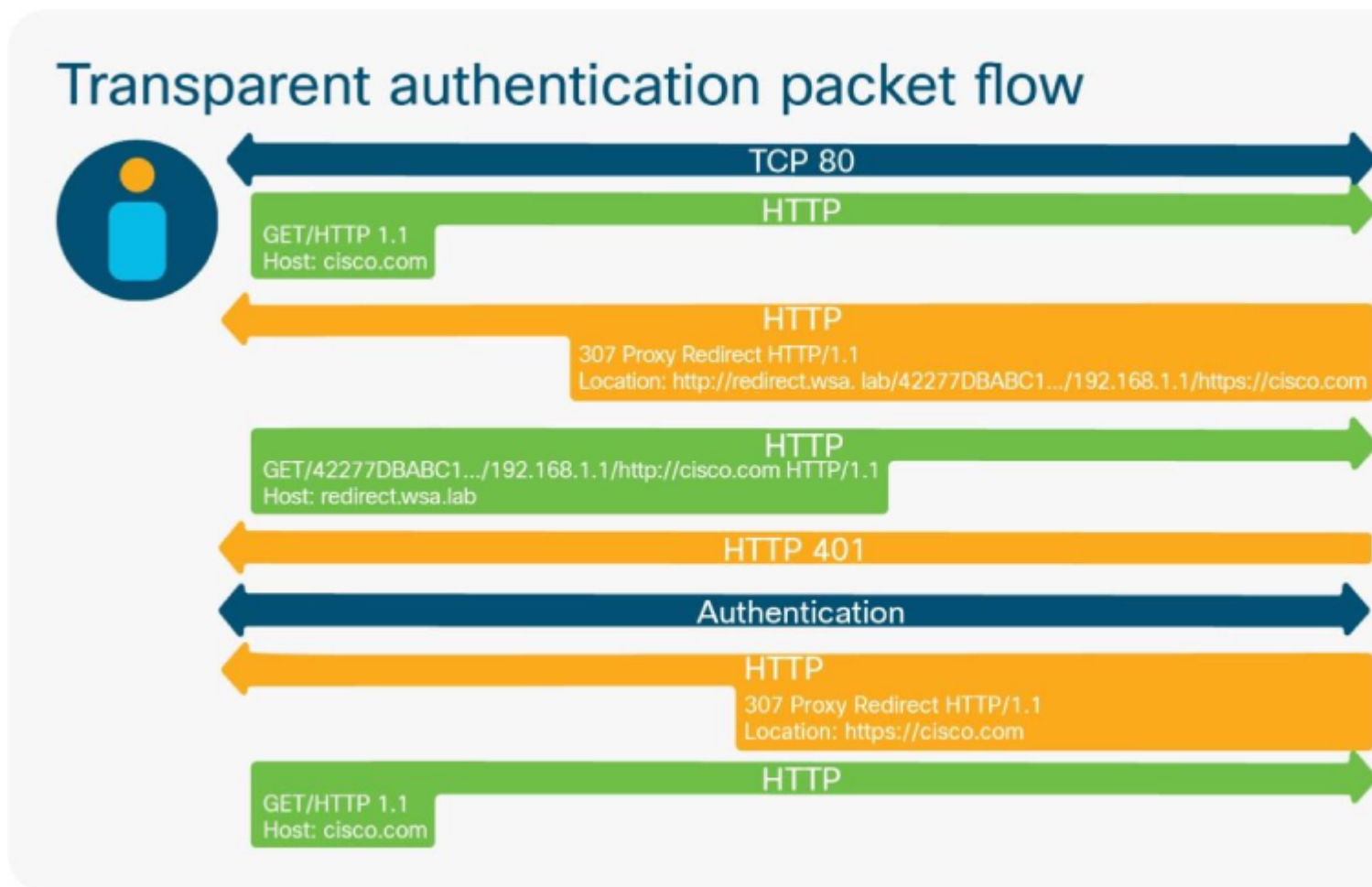
Der "Redirect Hostname", der auf der Seite für die Authentifizierungseinstellungen konfiguriert wird, bestimmt, wohin ein transparenter Client gesendet wird, um die Authentifizierung abzuschließen. Damit ein Windows-Client die integrierte Authentifizierung abschließen und eine **einmalige Anmeldung (Single Sign-On, SSO)** durchführen kann, muss sich der Umleitungs-Hostname in der Zone "Trusted Sites" (Vertrauenswürdige Sites) im Bedienfeld "Internetoptionen" befinden. Das Kerberos-Protokoll erfordert, dass der **vollqualifizierte Domänenname (FQDN)** zum Angeben einer Ressource verwendet wird, was bedeutet, dass der "Kurzname" (oder "NETBIOS"-Name) nicht verwendet werden kann, wenn Kerberos der beabsichtigte Authentifizierungsmechanismus ist. Der FQDN muss den "vertrauenswürdigen Sites" manuell hinzugefügt werden (z. B. über die Gruppenrichtlinie). Zusätzlich muss die automatische Anmeldung mit Benutzername und Passwort in der Systemsteuerung "Internetoptionen" eingestellt werden.

Zusätzliche Einstellungen sind in Firefox erforderlich, damit der Browser die Authentifizierung mit Netzwerkproxys abschließen kann. Diese Einstellungen können auf der Seite **about:config** konfiguriert werden. Damit Kerberos erfolgreich abgeschlossen werden kann, muss der Umleitungshostname der Option **network.negotiation-auth.trusted-uris** hinzugefügt werden. Für NTLMSSP muss sie der Option

`network.automatic-ntlm-auth.trusted-uris` hinzugefügt werden.

Authentifizierungs-Surrogate werden verwendet, um sich einen authentifizierten Benutzer für einen festgelegten Zeitraum nach Abschluss der Authentifizierung zu merken. Es müssen, wann immer möglich, IP-Surrogate verwendet werden, um die Anzahl der aktiven Authentifizierungsereignisse zu begrenzen. Die aktive Authentifizierung eines Clients ist eine ressourcenintensive Aufgabe, insbesondere bei Verwendung von Kerberos. Das Surrogat-Timeout beträgt standardmäßig 3.600 Sekunden (eine Stunde) und kann gesenkt werden, der niedrigste empfohlene Wert beträgt jedoch 900 Sekunden (15 Minuten).

Dieses Bild zeigt, wie "redirect.WSA.lab" als Umleitungshostname verwendet wird.



Passive Authentifizierung

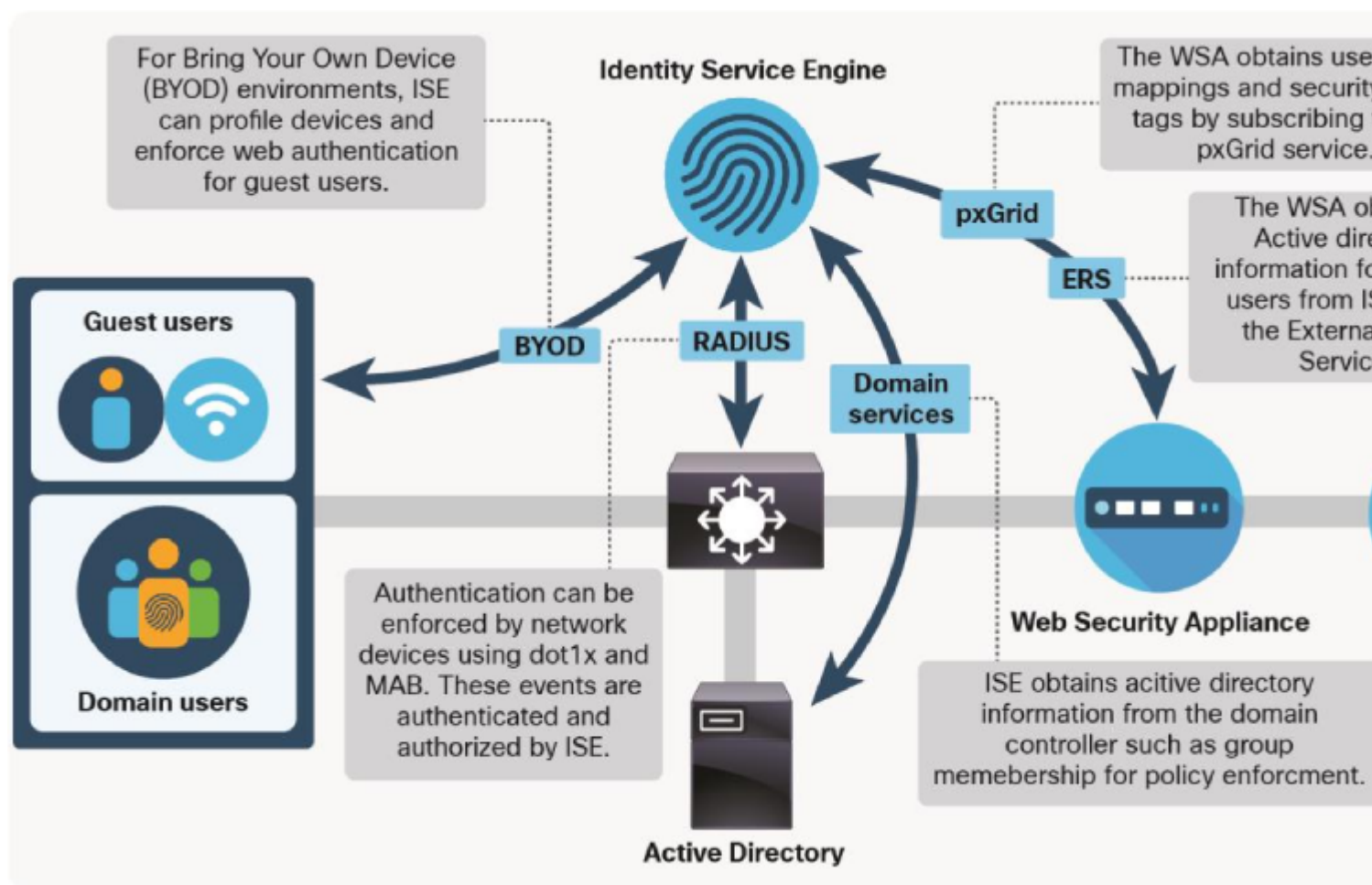
Die SWA können andere Cisco Sicherheitsplattformen nutzen, um Proxy-Benutzer passiv zu identifizieren. Die passive Benutzeridentifizierung macht direkte Authentifizierungsprobleme und jegliche Active Directory-Kommunikation aus dem SWA überflüssig, wodurch wiederum die Latenz und die Ressourcennutzung auf der Appliance reduziert werden. Die derzeit verfügbaren Mechanismen für die passive Authentifizierung werden über den **Context Directory Agent (CDA)**, die **Identity Services Engine (ISE)** und den **Identity Services Connector Passive Identity Connector (ISE-PIC)** bereitgestellt.

ISE ist ein funktionsstarkes Produkt, mit dem Administratoren ihre Authentifizierungsservices zentralisieren und eine umfassende Netzwerkzugriffskontrolle nutzen können. Wenn die ISE von einem Benutzerauthentifizierungsereignis erfährt (entweder über die Point1x-Authentifizierung oder die Web-

Authentifizierungsumleitung), füllt sie eine Sitzungsdatenbank mit Informationen über den Benutzer und das Gerät auf, der bzw. das an der Authentifizierung beteiligt ist. Der SWA stellt über das **Platform Exchange Grid (pxGrid)** eine Verbindung zur ISE her und bezieht den Benutzernamen, die IP-Adresse und das Security Group Tag (SGT), das mit einer Proxy-Verbindung verknüpft ist. Seit AsyncOS-Version 11.7 kann der SWA auch den **External Restful Service (ERS)** auf der ISE abfragen, um Gruppeninformationen abzurufen.

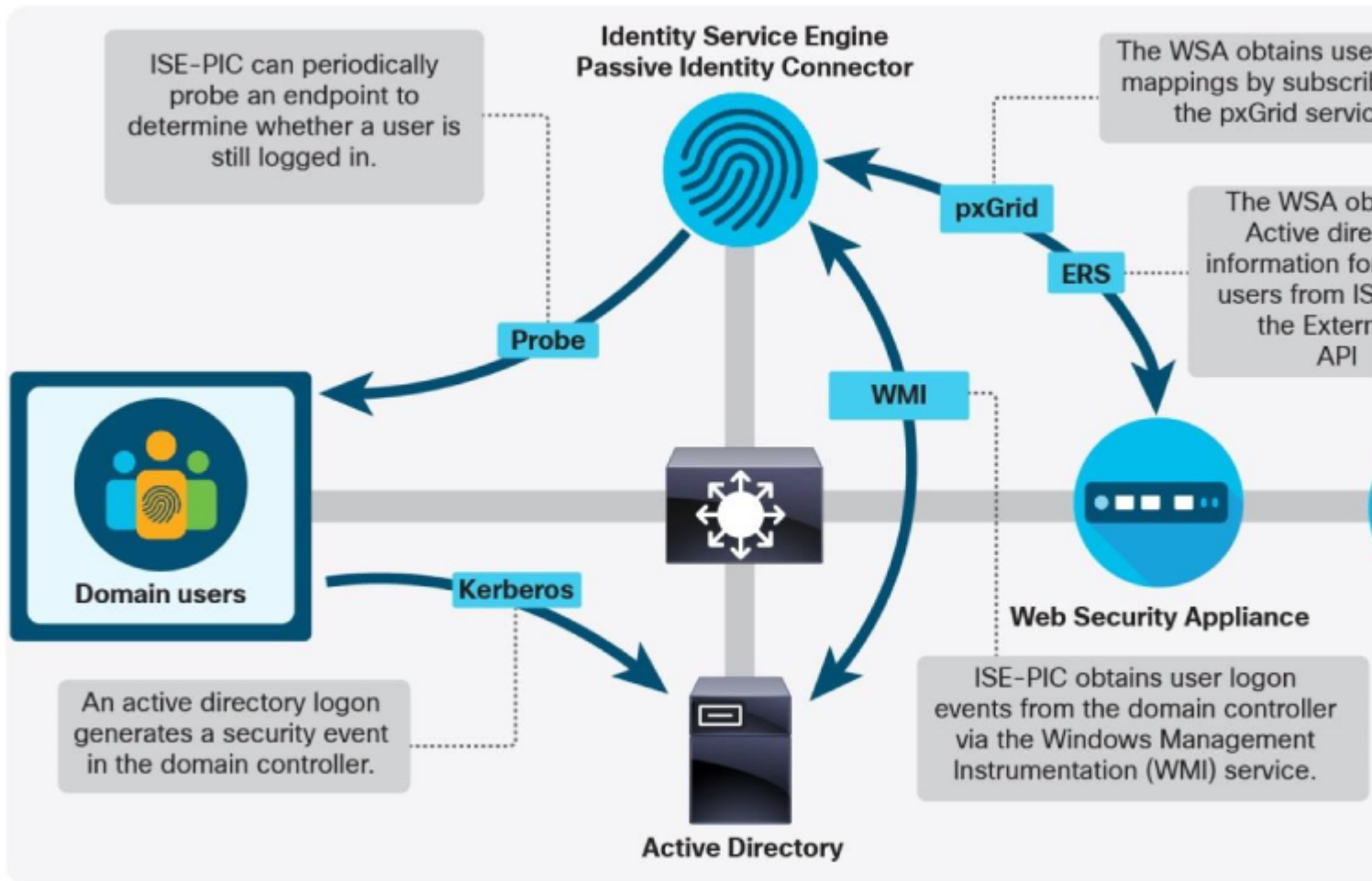
Die empfohlenen Versionen sind ISE 3.1 und SWA 14.0.2-X und höher. Weitere Informationen zur ISE-Kompatibilitätstmatrix für SWA finden Sie unter [ISE-Kompatibilitätstmatrix für die sichere Web-Appliance](#).

Weitere Informationen zu den Schritten der vollständigen Integration finden Sie im [Benutzerhandbuch für die Web Security Appliance](#).



Cisco kündigt das Ende des Lebenszyklus der Cisco Context Directory Agent (CDA)-Software an (siehe [Cisco Context Directory Agent \(CDA\)](#)).

Ab CDA Patch 6 ist kompatibel mit Microsoft Server 2016. Administratoren werden jedoch aktiv aufgefordert, ihre CDA-Bereitstellungen auf ISE-PIC zu migrieren. Beide Lösungen verwenden WMI zum Abonnieren des Windows-Sicherheitsereignisprotokolls, um Benutzer-zu-IP-Zuordnungen (Sitzungen) zu generieren. Im Falle von CDA fragt die SWA diese Zuordnungen mit RADIUS ab. Im Fall von ISE-PIC werden die gleichen pxGrid- und ERS-Verbindungen wie bei der vollständigen ISE-Bereitstellung verwendet. Die ISE-PIC-Funktion ist sowohl in einer vollständigen ISE-Installation als auch in einer eigenständigen virtuellen Appliance verfügbar.



Servicekonfiguration

Webproxy

Das Caching muss in der Webproxy-Konfiguration aktiviert werden, um Bandbreite zu sparen und die Leistung zu steigern. Dies wird umso wichtiger, als der Anteil des HTTPS-Datenverkehrs zunimmt, da die SWA HTTPS-Transaktionen nicht standardmäßig zwischenspeichern. Wenn der Proxy nur für explizite Clients bereitgestellt wird, muss der Weiterleitungsmodus angegeben werden, um Datenverkehr abzulehnen, der nicht speziell für den Proxydienst bestimmt ist. Auf diese Weise wird die Angriffsfläche der Appliance reduziert und ein gutes Sicherheitsprinzip angewandt: Deaktivieren Sie sie, wenn sie nicht benötigt wird.

Bereichsanforderungs-Header werden in HTTP-Anforderungen verwendet, um den Bytebereich einer herunterzuladenden Datei anzugeben. Es wird häufig von Daemons für Betriebssystem- und Anwendungsaktualisierungen verwendet, um kleine Teile einer Datei gleichzeitig zu übertragen. Standardmäßig werden diese Header vom SWA entfernt, sodass die gesamte Datei für Antivirus-Scans (AV), Dateireputation und -analysen sowie AVC (**Application Visibility Control**) abgerufen werden kann. Wenn die globale Weiterleitung von Bereichsanforderungs-Headern in den Proxyeinstellungen aktiviert ist, können Administratoren individuelle Zugriffsrichtlinien erstellen, die diese Header weiterleiten oder entfernen. Weitere Informationen zu dieser Konfiguration finden Sie im Abschnitt **Zugriffsrichtlinien**.

<p>Range Request Forwarding:</p>	<p><input checked="" type="checkbox"/> Enable Range Request Forwarding</p> <p><i>When enabled, range requests will be forwarded to the destination server. This can save bandwidth and improve performance for Application Visibility and Control.</i></p> <p><i>When range request forwarding is enabled and the Application Visibility and Control service is handling for AVC are available in Access Policies (see Web Security Manager > Access Policies)</i></p>
----------------------------------	---

HTTPS-Proxy

Empfohlene Sicherheitsverfahren legen nahe, dass private Schlüssel auf der Appliance generiert und niemals woanders hin transportiert werden müssen. Der HTTPS-Proxy-Assistent ermöglicht die Erstellung des Schlüsselpaars und des Zertifikats für die Entschlüsselung von **TLS-Verbindungen (Transport Layer Security)**. Die **Zertifikatsanforderung (Certificate Signing Request, CSR)** kann dann heruntergeladen und von einer internen **Zertifizierungsstelle (Certificate Authority, CA) signiert werden**. In einer **Active Directory (AD)**-Umgebung ist dies die beste Methode, da eine AD-integrierte Zertifizierungsstelle automatisch von allen Mitgliedern der Domäne als vertrauenswürdig angesehen wird und keine zusätzlichen Schritte zur Bereitstellung des Zertifikats erforderlich sind.

Eine Sicherheitsfunktion des HTTPS-Proxys ist die Validierung von Serverzertifikaten. Best Practices legen nahe, dass ungültige Zertifikate erfordern, dass die Verbindung getrennt wird. Wenn Sie Entschlüsseln für EUN aktivieren, kann der SWA eine Blockseite mit der Begründung für den Block anzeigen. Wenn diese Option nicht aktiviert ist, führen blockierte HTTPS-Sites zu einem Browserfehler. Dies führte zu einer Erhöhung der Helpdesk-Tickets und der Annahme des Benutzers, dass etwas defekt ist, anstatt zu wissen, dass der SWA die Verbindung blockiert hat. Alle ungültigen Zertifikatoptionen müssen mindestens auf Entschlüsseln festgelegt sein. Wenn Sie eine dieser Optionen als Monitor belassen, können keine nützlichen Fehlermeldungen protokolliert werden, wenn Zertifikatprobleme das Laden einer Website verhindern.

Invalid Certificate Options	
Invalid Certificate Handling:	Expired: Monitor
	Mismatched Hostname: Monitor
	Unrecognized Root Authority / Issuer: Monitor
	Invalid Signing Certificate: Monitor
	Invalid Leaf Certificate: Monitor
	All other error types: Monitor
Online Certificate Status Protocol Options	
OCSP Result Handling:	Revoked Certificate: Monitor
	Unknown Certificate: Monitor
	OCSP Error: Monitor

Ebenso müssen **OCSP-Prüfungen (Online Certificate Services Protocol)** aktiviert bleiben, und Monitor darf für keine der Optionen verwendet werden. Zurückgezogene Zertifikate müssen gelöscht werden, und alle anderen Zertifikate müssen mindestens auf Entschlüsseln festgelegt sein, damit relevante Fehlermeldungen protokolliert werden können. **Authority Information Access Chasing (AIA-Verfolgung)** ist ein Mittel, mit dem ein Client den Unterzeichner des Zertifikats und eine URL, von der zusätzliche Zertifikate abgerufen werden können, heraussuchen kann. Wenn beispielsweise eine Zertifikatskette, die von einem Server empfangen wird, unvollständig ist (es fehlt ein Zwischen- oder Stammzertifikat), kann der SWA das AIA-Feld überprüfen und es verwenden, um die fehlenden Zertifikate abzurufen und die Authentizität zu überprüfen. Diese Einstellung ist in der CLI nur über die folgenden Befehle verfügbar:

```
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]>

...

Hinweis: Diese Einstellung ist standardmäßig aktiviert und darf nicht deaktiviert werden, da viele moderne Server auf diesen Mechanismus angewiesen sind, um eine vollständige Vertrauenskette für Clients bereitzustellen.

Layer-4-Datenverkehrsüberwachung (L4TM)

Mit L4TM kann die Reichweite des SWA auf schädlichen Datenverkehr ausgedehnt werden, der nicht über den Proxy läuft. Dies gilt auch für Datenverkehr an allen TCP- und UDP-Ports. Die T1- und T2-Ports sind für den Anschluss an eine Netzwerkschnittstelle oder eine Switch-Überwachungssitzung vorgesehen, sodass der gesamte Datenverkehr von den Clients passiv vom SWA überwacht werden kann. Wenn Datenverkehr für eine schädliche IP-Adresse erkannt wird, kann der SWA TCP-Sitzungen beenden, indem er eine RST sendet, während er die Server-IP-Adresse manipuliert. Für UDP-Datenverkehr kann eine Nachricht "Port Unreachable" (Port nicht erreichbar) gesendet werden. Bei der Konfiguration der Überwachungssitzung ist es am besten, Datenverkehr, der für die Verwaltungsschnittstelle des SWA bestimmt ist, auszuschließen, um zu verhindern, dass die Funktion den Zugriff auf das Gerät potenziell beeinträchtigt.

Neben der Überwachung auf schädlichen Datenverkehr durchsucht L4TM auch DNS-Abfragen, um die Liste der Umgehungseinstellungen zu aktualisieren. Diese Liste wird in WCCP-Bereitstellungen verwendet, um bestimmte Anforderungen für das direkte Routing zum Webserver an den WCCP-Router zurückzugeben. Pakete, die mit der Liste der Umgehungseinstellungen übereinstimmen, werden vom Proxy nicht verarbeitet. Die Liste kann IP-Adressen oder Servernamen enthalten. Der SWA löst alle 30 Minuten alle Einträge in der Umgehungseinstellungsliste auf, unabhängig von der TTL des Datensatzes. Wenn die L4TM-Funktion jedoch aktiviert ist, kann der SWA Snooped-DNS-Abfragen verwenden, um diese Datensätze häufiger zu aktualisieren. Dadurch wird das Risiko eines Fehlalarms in einem Szenario reduziert, in dem der Client eine andere Adresse als den SWA aufgelöst hat.

Richtlinienkonfiguration

Eine korrekte Richtlinienkonfiguration ist für die Leistung und Skalierbarkeit der SWA von zentraler Bedeutung. Dies liegt nicht nur an der Effektivität der Richtlinien selbst beim Schutz von Kunden und bei der Durchsetzung von Unternehmensanforderungen. Die Art und Weise, wie Richtlinien konfiguriert werden, hat direkte Auswirkungen auf die Ressourcennutzung und den allgemeinen Status und die Leistung der SWA. Ein übermäßig komplexer oder schlecht konzipierter Richtlinienatz kann Instabilität und eine langsame Reaktionsfähigkeit der Appliance verursachen.

Komplexität

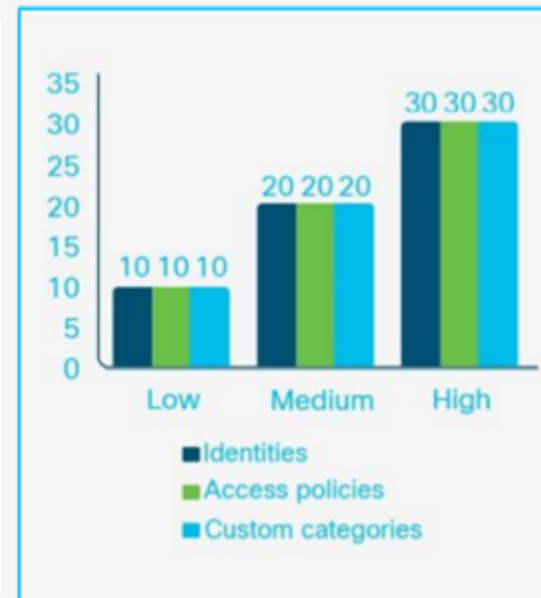
Verschiedene politische Elemente werden bei der Erstellung von SWA-Policen verwendet. Die aus der

Konfiguration generierte XML-Datei wird zum Erstellen einer Reihe von Back-End-Konfigurationsdateien und Zugriffsregeln verwendet. Je komplexer die Konfiguration, desto mehr Zeit muss der Proxy-Prozess für die Auswertung der verschiedenen Regelsätze für jede Transaktion aufwenden. Beim Benchmarking und der Bedarfsbestimmung der SWA werden grundlegende Richtlinienelemente erstellt, die drei Komplexitätsstufen der Konfiguration repräsentieren. Zehn Identitätsprofile, Entschlüsselungsrichtlinien und Zugriffsrichtlinien sowie zehn benutzerdefinierte Kategorien mit zehn regulären Einträgen, fünfzig Server-IP-Adressen und 420 Server-Hostnamen werden als Konfiguration mit geringer Komplexität betrachtet. Die Multiplikation dieser Zahlen mit zwei bzw. drei ergibt eine Konfiguration mit mittlerer Komplexität bzw. hoher Komplexität.

Wenn eine Konfiguration zu komplex wird, gehören zu den ersten Symptomen in der Regel eine langsame Reaktion in der Webschnittstelle und der CLI. Zunächst kann es keine nennenswerten Auswirkungen auf die Benutzer geben. Je komplexer die Konfiguration ist, desto mehr Zeit muss der Proxy-Prozess im Benutzermodus verbringen. Aus diesem Grund kann die Überprüfung des prozentualen Zeitaufwands in diesem Modus eine nützliche Methode sein, um eine übermäßig komplexe Konfiguration als Ursache für eine langsame SWA zu diagnostizieren.

Die CPU-Zeit in Sekunden wird im track_stats-Protokoll alle fünf Minuten protokolliert. Das bedeutet, dass der Nutzerzeitprozentsatz als $(\text{Nutzerzeit} + \text{Systemzeit})/300$ berechnet werden kann. Wenn die Benutzerzeit auf 270 heranrückt, verbringt der Prozess zu viele CPU-Zyklen im Benutzermodus, und das fast immer, weil die Konfiguration zu komplex ist, um effizient analysiert zu werden.

```
Current Date: Wed, 09 Nov 2022 08:49:00 +03
user time: 136.164 (45.388%)
system time: 48.189 (16.063%)
max resident set size: 104712
integral sh'd text mem size: 61923808
integral unshared data size: 1003469344
integral unshared stack size: 114521088
page reclaims: 29776
page faults: 0
swaps: 0
block input operations: 62168
block output operations: 289048
messages sent: 2755817
messages received: 1667985
signals received: 0
voluntary context switches: 2957114
involuntary context switches: 4341
```



Identifikationsprofile

Die Identifizierungsprofile (ID) sind die ersten Richtlinienelemente, die beim Empfang einer neuen Anforderung ausgewertet werden. Alle im ersten Abschnitt des ID-Profiles konfigurierten Informationen werden mit einem logischen AND ausgewertet. Das bedeutet, dass alle Kriterien übereinstimmen müssen, damit die Anfrage dem Profil entspricht. Bei der Erstellung einer Richtlinie darf diese nur so konkret wie unbedingt erforderlich sein. Profile, die einzelne Host-Adressen enthalten, sind fast nie erforderlich und können zu umfangreichen Konfigurationen führen. Die Nutzung der in den HTTP-Headern, der benutzerdefinierten Kategorieliste oder dem Subnetz enthaltenen User-Agent-Zeichenfolge ist im Allgemeinen eine bessere Strategie, um den Umfang eines Profils einzuschränken.

Im Allgemeinen werden Richtlinien, die eine Authentifizierung erfordern, am unteren Rand konfiguriert, und Ausnahmen am oberen Rand. Bei der Bestellung von Richtlinien, die keine Authentifizierung erfordern, müssen die am häufigsten verwendeten Richtlinien so nah wie möglich am Anfang sein. Verlassen Sie sich nicht auf eine fehlgeschlagene Authentifizierung, um den Zugriff einzuschränken. Wenn ein Client im

Netzwerk bekanntermaßen nicht in der Lage ist, sich bei einem Proxy zu authentifizieren, muss er von der Authentifizierung ausgenommen und in den Zugriffsrichtlinien blockiert werden. Clients, die sich nicht wiederholt authentifizieren können, senden nicht authentifizierte Anfragen an die SWA, die Ressourcen nutzen und eine übermäßige CPU- und Speichernutzung verursachen können.

Administratoren sind häufig der Ansicht, dass sie ein eindeutiges ID-Profil sowie eine entsprechende Entschlüsselungsrichtlinie und Zugriffsrichtlinie verwenden müssen. Dies ist eine ineffiziente Strategie für die Richtlinienkonfiguration. Richtlinien müssen nach Möglichkeit "zusammengefasst" werden, damit ein einzelnes ID-Profil mit mehreren Entschlüsselungs- und Zugriffsrichtlinien verknüpft werden kann. Dies ist möglich, da alle Kriterien in einer bestimmten Richtlinie übereinstimmen müssen, damit der Datenverkehr mit der Richtlinie übereinstimmt. Da die Authentifizierungsrichtlinie und die daraus resultierenden Richtlinien allgemeinerer Natur sind, sind insgesamt weniger Richtlinien möglich.

- Policies do not require a 1:1 flow!
- Reduce complexity by collapsing where possible.

Client / User Identification Profiles

Managed by: ngsma.chclasen.lab - local changes will be overwritten.

Add Identification Profile...

Order	Transaction Criteria	Authentication / Identification Decision	End-User Acknowledgement	Delete
1	AD Auth <small>Subnets: 192.168.10.50, 192.168.0.40 Protocols: HTTP/HTTPS</small>	<small>Authenticate:</small> Realm: AD (Scheme: Basic, NTLMSSP, Kerberos)	(global profile)	🗑️

Policies

Managed by: ngsma.chclasen.lab - local changes will be overwritten.

Add Policy...

Order	Group	Protocols and User Agents	URL Filtering	Applications	Objects
1	Github <small>Identification Profile: AD Auth All identified users URL Categories: Github</small>	(global policy)	Monitor: 1	(global policy)	(global po
2	Contractors <small>Identification Profile: AD Auth 1 groups (AD\CHCLASEN\Contractors)</small>	(global policy)	(global policy)	(global policy)	(global po
3	Domain Users AP <small>Identification Profile: AD Auth All identified users</small>	(global policy)	(global policy)	(global policy)	(global po
Global Policy <small>Identification Profile: All</small>		No blocked items	Monitor: 85	Monitor: 356	No blocke

Edit Policy Order...

Entschlüsselungsrichtlinien

Wie beim ID-Profil werden auch die in der Entschlüsselungsrichtlinie festgelegten Kriterien als logisches UND ausgewertet, mit einer wichtigen Ausnahme, wenn Informationen von der ISE verwendet werden. Die Richtlinienanpassung erfolgt je nach konfigurierten Elementen (AD-Gruppe, Benutzer oder SGT) wie folgt:

- AD groups and users (AD-Gruppen und -Benutzer): Keine Änderung des vorherigen Verhaltens; die Richtlinie wird zugeordnet, wenn der Benutzer Mitglied einer Gruppe ist ODER wenn der Benutzer in der Richtlinie angegeben ist.
- SGT- und AD-Gruppen und Benutzer - Die Richtlinie wird zugeordnet, wenn der Benutzer dem SGT zugeordnet ist UND Mitglied der AD-Gruppe ist ODER wenn der Benutzer in der Richtlinie angegeben ist.
- SGT and users (SGT und Benutzer): Die Richtlinie wurde zugeordnet, wenn der Benutzer dem SGT zugeordnet ist oder der Benutzer in der Richtlinie angegeben ist.

Von allen von der SWA ausgeführten Services ist die Auswertung des HTTPS-Verkehrs aus Leistungssicht am wichtigsten. Der Anteil des entschlüsselten Datenverkehrs hat direkte Auswirkungen auf die Größe der

Appliance. Ein Administrator kann sich darauf verlassen, dass mindestens 75 % des Webdatenverkehrs über HTTPS erfolgen wird.

Nach der Erstinstallation muss der Prozentsatz des entschlüsselten Datenverkehrs bestimmt werden, um sicherzustellen, dass die Erwartungen für ein zukünftiges Wachstum richtig festgelegt werden. Nach der Bereitstellung muss diese Nummer einmal pro Quartal überprüft werden. Der prozentuale Anteil des HTTPS-Datenverkehrs, der vom SWA entschlüsselt wird, ist mit einer Kopie von access_logs leicht zu ermitteln, selbst ohne zusätzliche Protokollverwaltungssoftware. Diese Nummer kann mit einfachen Bash- oder PowerShell-Befehlen abgerufen werden. Im Folgenden werden die einzelnen Schritte für die jeweilige Umgebung beschrieben:

1. Ermitteln Sie die Anzahl der HTTPS-Verbindungen insgesamt (explizit und transparent):

Bash:
grep -cE 'tunnel://|TCP_CONNECT' aclog.current

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT').length

2. Die Anzahl der entschlüsselten HTTPS-Verbindungen ermitteln:

Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT' | Select-String -Pattern 'DECRYPT').length

3. Den zweiten Wert durch den ersten Wert teilen und mit 100 multiplizieren.

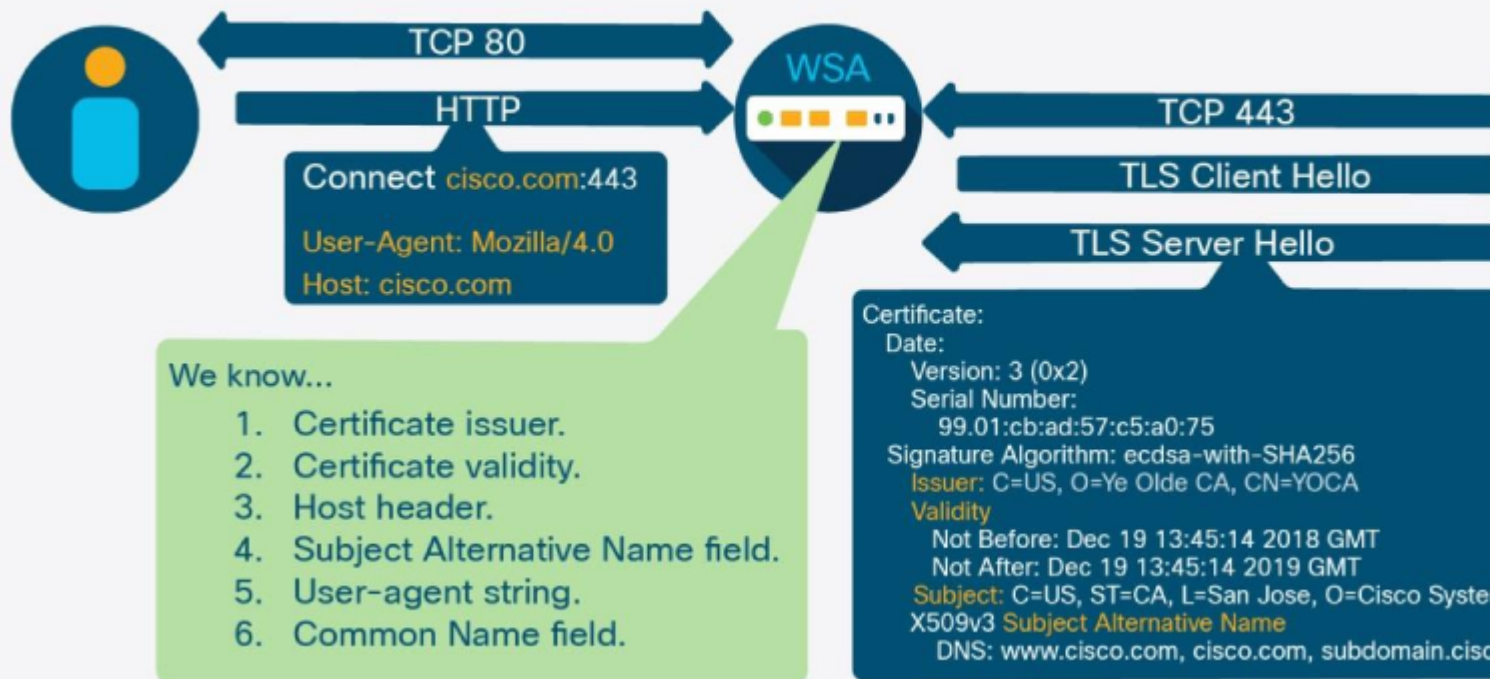
Beim Entwerfen von Entschlüsselungsrichtlinien ist es wichtig zu verstehen, wie die verschiedenen in der Richtlinie aufgeführten Aktionen dazu führen, dass die Appliance HTTPS-Verbindungen auswertet. Die Passthrough-Aktion wird verwendet, wenn der Client und der Server jedes Ende ihrer TLS-Sitzung beenden dürfen müssen, ohne dass der SWA jedes Paket entschlüsselt. Selbst wenn ein Standort auf "Passthrough" gesetzt ist, muss der SWA einen TLS-Handshake mit dem Server durchführen. Der Grund hierfür ist, dass der SWA eine Verbindung basierend auf der Zertifikatsgültigkeit blockieren und eine TLS-Verbindung mit dem Server initiieren muss, um das Zertifikat zu erhalten. Wenn das Zertifikat gültig ist, schließt der SWA die Verbindung und ermöglicht dem Client, die Sitzung direkt mit dem Server einzurichten.

HTTPS policy operations

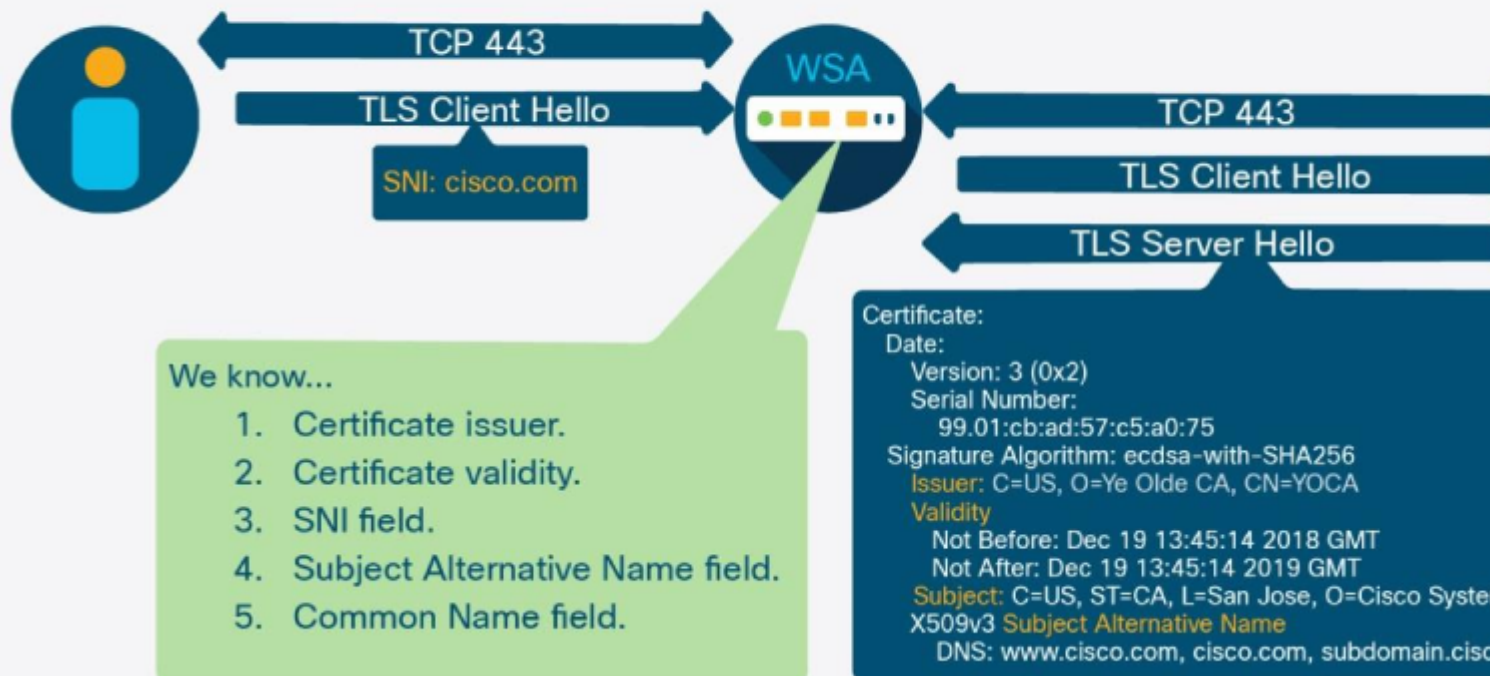
- **Drop**
 - Connection is closed.
- **Decrypt**
 - Traffic is decrypted and evaluated by access policies.
- **Passthrough**
 - Transaction is not decrypted.
 - Client negotiates directly with server.
- **Monitor**
 - No action taken.
 - Move to the next column on the policy.

Der einzige Fall, in dem der SWA keinen TLS-Handshake ausführt, ist, wenn der Servername oder die IP-Adresse in einer benutzerdefinierten Kategorie vorhanden ist, die auf "Passthrough" gesetzt ist, und der Servername entweder in einem HTTP CONNECT- oder einem TLS Client Hello verfügbar ist. In einem expliziten Szenario gibt der Client dem Proxy den Hostnamen des Servers vor der TLS-Sitzungsiniiierung (im Host-Header) an, sodass dieses Feld mit der benutzerdefinierten Kategorie abgeglichen wird. Bei einer transparenten Bereitstellung überprüft der SWA das Feld **Servernamen-Angabe (SNI)** in der TLS-Client-Hello-Nachricht und vergleicht es mit der benutzerdefinierten Kategorie. Wenn der Host-Header oder SNI nicht vorhanden ist, muss der SWA den Handshake mit dem Server fortsetzen, um die Felder **Subject Alternative Name (SAN)** und **Common Name (CN)** im Zertifikat in dieser Reihenfolge zu überprüfen. Dieses Verhalten bedeutet für das Richtliniendesign, dass die Anzahl der TLS-Handshakes reduziert werden kann, indem bekannte und intern vertrauenswürdige Server ermittelt und auf Passthrough aus einer benutzerdefinierten Kategorieliste festgelegt werden, anstatt sich auf die Webkategorie und Reputationsbewertung zu verlassen, bei denen der SWA weiterhin einen TLS-Handshake mit dem Server durchführen muss. Es ist jedoch wichtig zu beachten, dass dadurch auch Prüfungen der Gültigkeit von Zertifikaten verhindert werden.

Explicit HTTPS-What do we know?



Transparent HTTPS-What do we know?



Die Geschwindigkeit, mit der neue Websites im Web erscheinen, ist es wahrscheinlich eine Reihe von Websites nicht kategorisiert durch die Web-Reputation und Kategorisierungs-Datenbanken von der SWA verwendet gefunden. Dies bedeutet nicht, dass die Website ist notwendigerweise eher schädlich, und zusätzlich alle diese Websites immer noch unterworfen AV-Scanning, AMP-Dateireputation und Analyse, und jedes Objekt blockieren oder Scannen, die konfiguriert ist. Aus diesen Gründen wird in den meisten

Fällen nicht empfohlen, nicht kategorisierte Websites zu löschen. Es ist am besten, sie so einzustellen, dass sie von den AV-Engines entschlüsselt und gescannt und von AVC, AMP, Zugriffsrichtlinien usw. ausgewertet werden. Weitere Informationen zu nicht kategorisierten Sites finden Sie im Abschnitt **Zugriffsrichtlinien**.

Zugriffsrichtlinien

Wie beim ID-Profil werden auch die in der Entschlüsselungsrichtlinie festgelegten Kriterien als logisches UND bewertet, mit einer wichtigen Ausnahme, wenn Informationen von der ISE verwendet werden. Das Verhalten für die Richtlinienzuordnung wird als Nächstes anhand der konfigurierten Elemente (AD-Gruppe, Benutzer oder SGT) erläutert:

- AD groups and users (AD-Gruppen und -Benutzer): Keine Änderung des vorherigen Verhaltens; Übereinstimmung der Richtlinie, wenn der Benutzer Mitglied einer Gruppe ist ODER der Benutzer in der Richtlinie angegeben ist.
- SGT- und AD-Gruppen und -Benutzer - Die Richtlinie wurde zugeordnet, wenn der Benutzer dem SGT zugeordnet ist UND Mitglied der AD-Gruppe ist ODER wenn der Benutzer in der Richtlinie angegeben ist.
- SGT and users (SGT und Benutzer): Die Richtlinie wurde zugeordnet, wenn der Benutzer mit dem SGT verknüpft ist ODER der Benutzer in der Richtlinie angegeben ist.

Der HTTP-Datenverkehr wird unmittelbar nach der Authentifizierung anhand der Zugriffsrichtlinien ausgewertet. Der HTTPS-Datenverkehr wird nach der Authentifizierung ausgewertet, und es wird geprüft, ob die Entschlüsselungsaktion gemäß der entsprechenden Entschlüsselungsrichtlinie angewendet wird. Für entschlüsselte Anforderungen gibt es zwei access_log -Einträge. Der erste Protokolleintrag zeigt die Aktion an, die auf die anfängliche TLS-Verbindung angewendet wurde (Entschlüsselung), und ein zweiter Protokolleintrag zeigt die Aktion an, die von der Zugriffsrichtlinie auf die entschlüsselte HTTP-Anfrage angewendet wurde.

Wie im **Webproxy**-Abschnitt erläutert, werden Bereichsanforderungs-Header verwendet, um einen bestimmten Bytebereich einer Datei anzufordern. Sie werden häufig von Aktualisierungsdiensten für Betriebssysteme und Anwendungen verwendet. Die SWA entfernen diese Header standardmäßig von ausgehenden Anfragen, da es ohne die gesamte Datei nicht möglich ist, Malware-Scans durchzuführen oder AVC-Funktionen zu nutzen. Wenn viele Hosts im Netzwerk häufig kleine Bytebereiche anfordern, um Updates abzurufen, kann dies dazu führen, dass die SWA die gesamte Datei mehrere Male gleichzeitig herunterladen. Dadurch kann die verfügbare Internetbandbreite schnell erschöpft und es zu Serviceausfällen kommen. Die häufigsten Ursachen für dieses Fehlerszenario sind Microsoft Windows Update- und Adobe Software Update-Daemons.

Die beste Lösung zur Vermeidung dieses Problems besteht darin, diesen Datenverkehr vollständig durch die SWA zu steuern. Dies ist in transparent bereitgestellten Umgebungen nicht immer umsetzbar. In diesen Fällen besteht die nächstbeste Option darin, dedizierte Zugriffsrichtlinien für den Datenverkehr zu erstellen und die Weiterleitung von Bereichsanfragen in diesen Richtlinien zu aktivieren. Es muss beachtet werden, dass AV-Scanning und AVC für diese Anforderungen nicht möglich sind. Daher müssen die Richtlinien sorgfältig darauf ausgelegt werden, nur den beabsichtigten Datenverkehr zu berücksichtigen. Häufig lässt sich dies am besten erreichen, indem die im Anforderungsheader gefundene User-Agent-Zeichenfolge abgeglichen wird. Die Benutzer-Agent-Zeichenfolge für allgemeine Update-Daemons kann online gefunden werden, oder die Anforderungen können von einem Administrator erfasst und geprüft werden. Die meisten Aktualisierungsdienste, darunter Microsoft Windows Update und Adobe Software-Updates, verwenden kein HTTPS.

Wie im Abschnitt zu **Entschlüsselungsrichtlinien** beschrieben, wird nicht empfohlen, nicht kategorisierte Websites in den Entschlüsselungsrichtlinien zu löschen. Aus den gleichen Gründen wird nicht empfohlen, sie in den Zugriffsrichtlinien zu blockieren. Die Dynamic Content Analysis (DCA)-Engine kann den Inhalt einer bestimmten Site zusammen mit anderen heuristischen Daten für kategorisierte Sites verwenden, die andernfalls durch URL-Datenbanksuchvorgänge als nicht kategorisiert gekennzeichnet würden. Durch die Aktivierung dieser Funktion wird die Anzahl nicht kategorisierter Urteile im SWA reduziert.

In den Einstellungen für das Objektscannen einer Zugriffsrichtlinie besteht die Möglichkeit, verschiedene Arten von Archivdateien zu überprüfen. Wenn das Netzwerk regelmäßig Archivdateien als Teil von Anwendungs-Updates herunterlädt, kann dies die CPU-Auslastung deutlich erhöhen. Dieser Datenverkehr muss vorab identifiziert und freigestellt werden, wenn alle Archivdateien überprüft werden sollen. Der erste Ort, an dem mögliche Methoden zur Identifizierung dieses Datenverkehrs untersucht werden sollten, ist die Zeichenfolge "user-agent", da diese dazu beitragen kann, Listen mit zulässigen IP-Adressen zu vermeiden, deren Verwaltung mühsam werden kann.

Benutzerdefinierte und externe URL-Kategorien

Die benutzerdefinierten Kategorielisten werden verwendet, um einen Server nach IP-Adresse oder Hostnamen zu identifizieren. Sie können reguläre Ausdrücke (regex) verwenden, um Muster anzugeben, nach denen Servernamen zugeordnet werden können. Es ist viel ressourcenintensiver, ein reguläres Muster zu verwenden, um mit einem Servernamen zu übereinstimmen, als eine Teilzeichenfolgenübereinstimmung zu verwenden. Daher müssen sie nur verwendet werden, wenn dies absolut notwendig ist. Ein "." kann am Anfang eines Domännennamens hinzugefügt werden, um einer Subdomäne ohne regulären Ausdruck zu entsprechen. Beispiel: ".cisco.com" entspricht auch "www.cisco.com".

Wie im Abschnitt zur **Komplexität** erläutert, wird eine geringe Komplexität als zehn benutzerdefinierte Kategorielisten definiert, mittlere Komplexität als zwanzig und hohe Komplexität als dreißig. Es wird empfohlen, diese Zahl unter zwanzig zu halten, insbesondere wenn die Listen reguläre Muster verwenden oder eine große Anzahl von Einträgen enthalten. Im Abschnitt **Zugriffsrichtlinien** finden Sie weitere Informationen zur Anzahl der Einträge für jeden Typ.

Externe URL-Feeds sind wesentlich flexibler als statische benutzerdefinierte Kategorielisten, und ihre Nutzung kann sich direkt auf die Sicherheit auswirken, da sie die manuelle Verwaltung durch einen Administrator überflüssig machen. Da mit dieser Funktion Listen abgerufen werden können, die nicht vom SWA-Administrator verwaltet oder gesteuert werden, wurde die Möglichkeit zum Hinzufügen einzelner Ausnahmen zu den heruntergeladenen Adressen in AsyncOS, Version 11.8, hinzugefügt.

Die Office365-API ist besonders nützlich, um Richtlinienentscheidungen für diesen häufig bereitgestellten Dienst zu treffen, und kann für einzelne Anwendungen (PowerPoint, Skype, Word usw.) genutzt werden. Microsoft empfiehlt zur Leistungsoptimierung, Proxys für den gesamten Office365-Datenverkehr zu umgehen. In der Microsoft-Dokumentation heißt es:

"Während SSL Break and Inspect die größte Latenz verursacht, können andere Services wie Proxy-Authentifizierung und Reputationsprüfung zu Leistungseinbußen und einem schlechten Anwendererlebnis führen. Darüber hinaus benötigen diese Perimeter-Netzwerkgeräte genügend Kapazität, um alle Netzwerkverbindungsanforderungen zu verarbeiten. Wir empfehlen, Ihre Proxy- oder Prüfgeräte für direkte Office 365-Netzwerkanforderungen zu umgehen."<https://learn.microsoft.com/en-us/microsoft-365/enterprise/managing-office-365-endpoints?view=o365-worldwide> .

In einer transparenten Proxy-Umgebung kann die Verwendung dieses Leitfadens schwierig sein. Ab AsyncOS Version 11.8 ist es möglich, die dynamische Kategorielliste aus der Office365-API zum Ausfüllen der Umgehungseinstellungsliste zu verwenden. Diese Liste wird verwendet, um transparent umgeleiteten Datenverkehr zum direkten Routing zurück an das WCCP-Gerät zu senden.

Durch das Umgehen des gesamten Office365-Datenverkehrs wird ein toter Winkel für Administratoren geschaffen, die grundlegende Sicherheitskontrollen und Berichterstellung für diesen Datenverkehr benötigen. Wenn der Office365-Datenverkehr nicht von der SWA umgangen wird, ist es wichtig, die spezifischen technischen Herausforderungen zu kennen, die auftreten können. Eine davon ist die Anzahl der Verbindungen, die von den Anwendungen benötigt werden. Die Dimensionierung muss entsprechend angepasst werden, um die zusätzlichen persistenten TCP-Verbindungen zu ermöglichen, die von Office365-Anwendungen benötigt werden. Dadurch kann die Gesamtzahl der Verbindungen um 10 bis 15 persistente TCP-Sitzungen pro Benutzer erhöht werden.

Die vom HTTPS-Proxy ausgeführten Entschlüsselungs- und Wiederverschlüsselungsaktionen führen zu einer geringen Latenz der Verbindungen. Office 365-Anwendungen können sehr latenzanfällig sein. Wenn andere Faktoren wie eine langsame WAN-Verbindung und unterschiedliche geografische Standorte dies

verschlimmern, kann dies die Benutzerfreundlichkeit beeinträchtigen.

Einige Office365-Anwendungen verwenden proprietäre TLS-Parameter, die verhindern, dass der HTTPS-Proxy einen Handshake mit dem Anwendungsserver abschließt. Dies ist erforderlich, um das Zertifikat zu validieren oder den Hostnamen abzurufen. Wenn dies mit einer Anwendung wie Skype for Business kombiniert wird, die kein **SNI-Feld (Server Name Indication)** in ihrer TLS Client Hello-Nachricht sendet, muss dieser Datenverkehr vollständig umgangen werden. AsyncOS 11.8 bietet die Möglichkeit, Datenverkehr nur auf Basis der Ziel-IP-Adresse zu umgehen, ohne dass in diesem Szenario Zertifikatprüfungen durchgeführt werden müssen.

Monitore und Warnmeldungen

CLI-Monitore

Die SWA-CLI stellt Befehle für die Echtzeitüberwachung wichtiger Prozesse bereit. Am nützlichsten sind die Befehle, die Statistiken zum Proxy-Prozess anzeigen. Der Befehl **status detail** ist eine gute Quelle für eine Zusammenfassung der Ressourcennutzung und Leistungsmetriken, einschließlich Betriebszeit, genutzte Bandbreite, Reaktionslatenz, Anzahl der Verbindungen usw. Hier ist ein Beispiel für die Ausgabe dieses Befehls:

```
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
```

Der Befehl **rate** zeigt Echtzeitinformationen über den Prozentsatz der vom Proxyprozess verwendeten CPU sowie die Anzahl der Anforderungen pro Sekunde (RPS) und Cache-Statistiken an. Mit diesem Befehl wird die Abfrage fortgesetzt und die neue Ausgabe angezeigt, bis sie unterbrochen wird. Dies ist ein Beispiel für die Ausgabe dieses Befehls:

```
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

Der Befehl **tcpsservices** zeigt Informationen zu ausgewählten Prozess-Listening-Ports an. Außerdem wird eine Erläuterung der einzelnen Prozesse sowie der Kombination aus Adresse und Port angezeigt:

```
SWA_CLI> tcpsservices
```

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

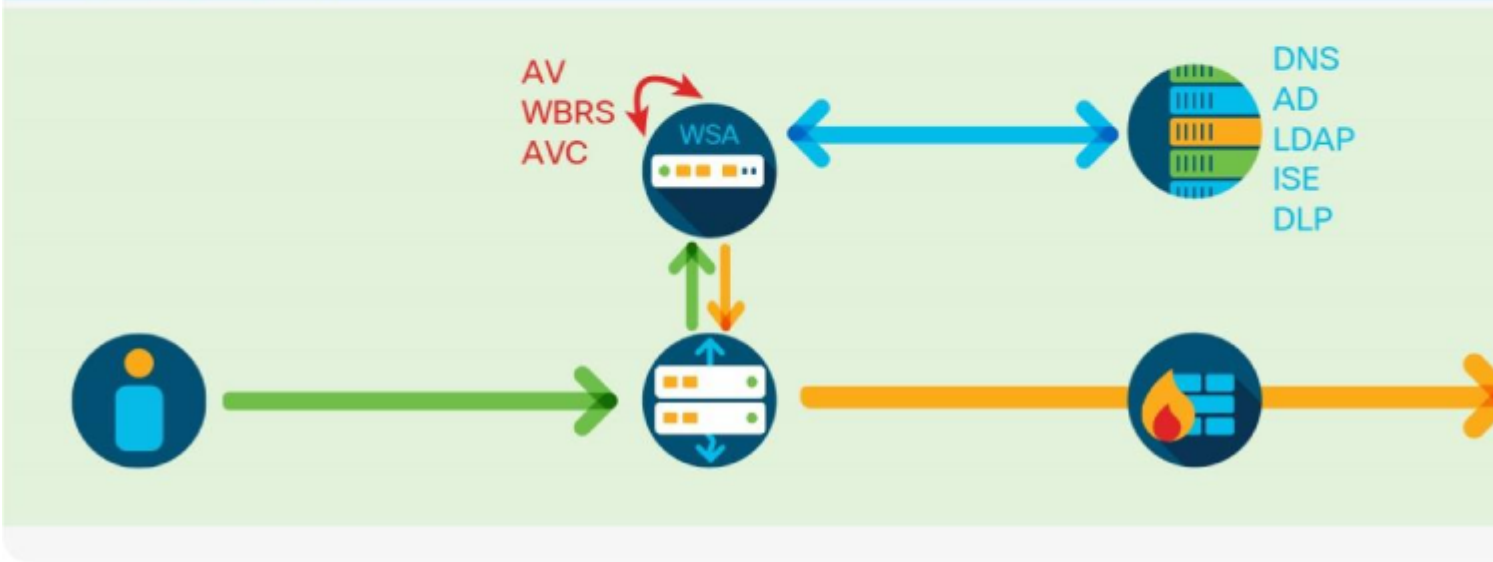
Protokollieren

Der Web-Datenverkehr ist äußerst dynamisch und vielfältig. Nachdem die Proxy-Bereitstellung abgeschlossen ist, müssen Menge und Zusammensetzung des Datenverkehrs, der durch die Appliance geleitet wird, regelmäßig überprüft werden. Sie müssen den Anteil des entschlüsselten Datenverkehrs regelmäßig (einmal pro Quartal) überprüfen, um sicherzustellen, dass die Größe den Erwartungen und Spezifikationen der Erstinstallation entspricht. Dies kann mit einem Protokollverwaltungsprodukt wie **Advanced Web Security Reporting (AWSR)** oder mit einfachen Bash- oder PowerShell-Befehlen mit den Zugriffsprotokollen erfolgen. Die Anzahl der RPS muss regelmäßig überprüft werden, um sicherzustellen, dass die Appliance genügend Overhead aufweist, um Datenverkehrsspitzen und ein mögliches Failover in einer hochverfügbaren Konfiguration mit Lastausgleich zu berücksichtigen.

Das track_stats-Protokoll wird alle fünf Minuten angehängt und enthält mehrere Abschnitte der Ausgabe, die direkt mit dem Proxy-Prozess und seinen Objekten im Speicher in Zusammenhang stehen. Besonders nützlich bei der Leistungsüberwachung sind die Abschnitte, die die durchschnittliche Latenz für verschiedene Anforderungsprozesse anzeigen, einschließlich der DNS-Suchzeit, der AV-Engine-Scanzeit und vieler weiterer nützlicher Felder. Dieses Protokoll kann nicht über die GUI oder die CLI konfiguriert werden und ist nur über Secure Copy Protocol (SCP) oder File Transfer Protocol (FTP) zugänglich. Dies ist das wichtigste Protokoll bei der Fehlerbehebung. Daher muss es regelmäßig abgefragt werden.

Where can latency be introduced?

- Client Side
- External Services
- Internal Services
- Server Side

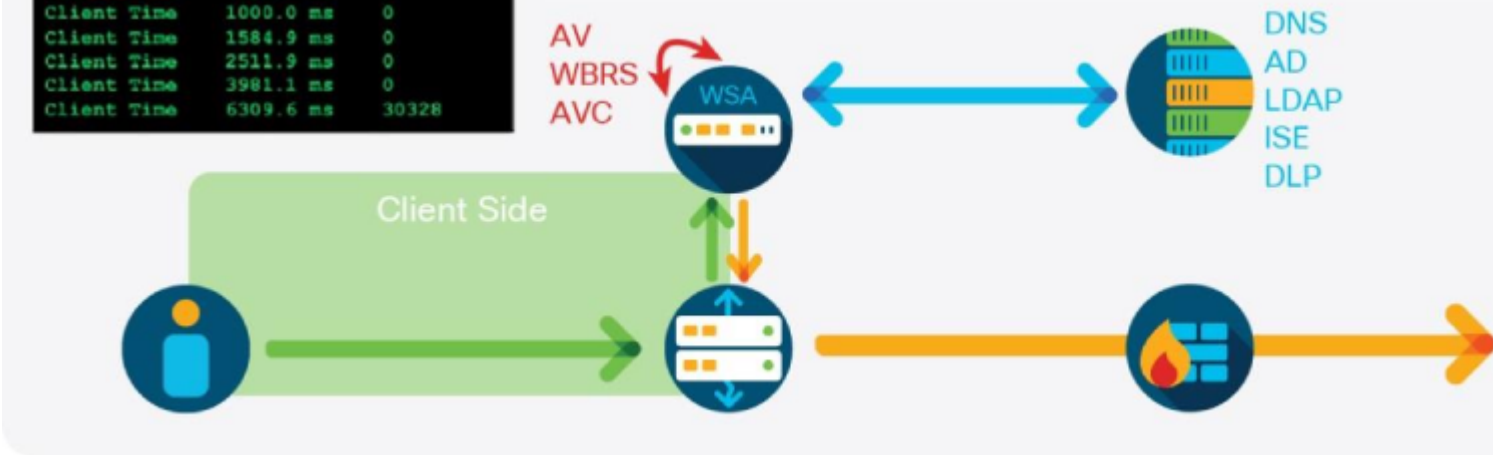


Client side latency

Client Time	1.0 ms	15575
Client Time	1.6 ms	185
Client Time	2.5 ms	855
Client Time	4.0 ms	573
Client Time	6.3 ms	180
Client Time	10.0 ms	264
Client Time	15.8 ms	580
Client Time	25.1 ms	924
Client Time	39.8 ms	1330
Client Time	63.1 ms	4936
Client Time	100.0 ms	5278
Client Time	158.5 ms	10
Client Time	251.2 ms	13
Client Time	398.1 ms	0
Client Time	631.0 ms	0
Client Time	1000.0 ms	0
Client Time	1584.9 ms	0
Client Time	2511.9 ms	0
Client Time	3981.1 ms	0
Client Time	6309.6 ms	30328

- **“Client Time”** in **track_stats** log.
- The amount of time in milliseconds that the client was waiting for a response.
- May indicate an upstream issues-keep investigating!
- Access logs can show this in custom field `%:1>`

<code>%:1></code>	<code>x-p2c-first-byte-time</code>	Wait-time for first byte written
----------------------	------------------------------------	----------------------------------



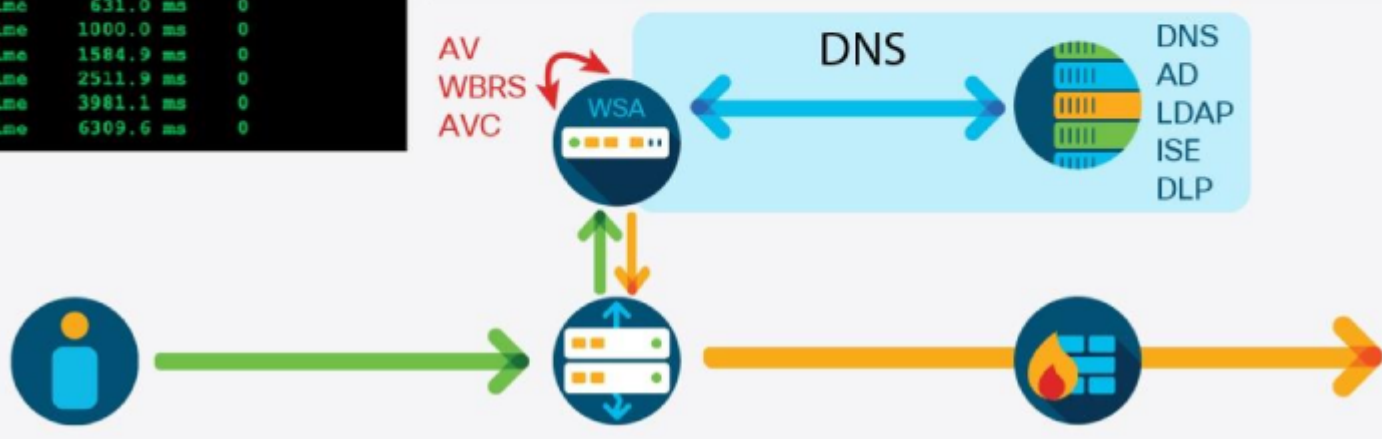
DNS latency

```

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 response.
- Calls for investigation for your DNS resolvers (or path to them)
- **access logs** can show this in custom field `% :>d`

<code>%:>d</code>	<code>x-p2p-dns-svc-time</code>	Time taken by the Web Proxy to receive the request and send a DNS result to the Web Proxy
----------------------	---------------------------------	---



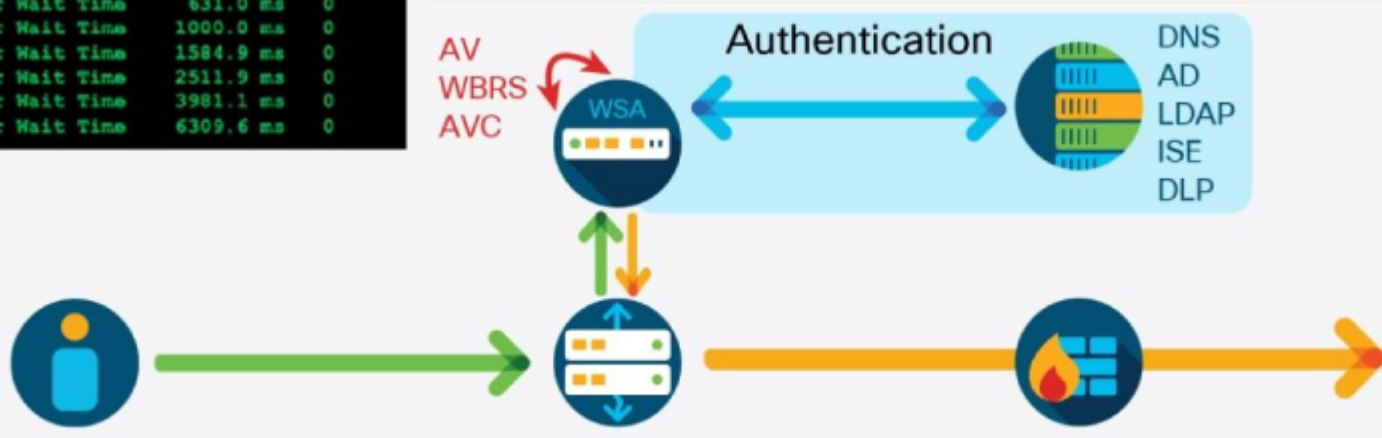
Authentication latency

```

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 Service Wait Time.”
- Use the first to get pure auth time without the request time
- **access logs** can show this in custom field `% :>a`

<code>%:>a</code>	<code>x-p2p-auth-wait-time</code>	Wait-time to receive the response from the Web Proxy authentication process and 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.
- **access logs** can show this in custom field % : >1

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



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-transaction to complete.
- Calls for investigation of your upstream devices and WAN.
- No **access logs** custom field, but can be determined by a combination of them.



Internal services latency-not exhaustive

Sophos Response Body Service Time	10.0 ms	0	Adaptive Scanning Service Time	1.0 ms	2
Sophos Response Body Service Time	17.3 ms	0	Adaptive Scanning Service Time	1.6 ms	0
Sophos Response Body Service Time	30.0 ms	0	Adaptive Scanning Service Time	2.5 ms	0
Sophos Response Body Service Time	52.1 ms	0	Adaptive Scanning Service Time	4.0 ms	0
Sophos Response Body Service Time	90.3 ms	0	Adaptive Scanning Service Time	6.3 ms	0
Sophos Response Body Service Time	156.5 ms	0	Adaptive Scanning Service Time	10.0 ms	0
McAfee Response Body Service Time	10.0 ms	0	AVC Header Scan Service Time	10.0 ms	8398
McAfee Response Body Service Time	17.3 ms	0	AVC Header Scan Service Time	17.3 ms	11
McAfee Response Body Service Time	30.0 ms	0	AVC Header Scan Service Time	30.0 ms	3
McAfee Response Body Service Time	52.1 ms	0	AVC Header Scan Service Time	52.1 ms	0
McAfee Response Body Service Time	90.3 ms	0	AVC Header Scan Service Time	90.3 ms	0
McAfee Response Body Service Time	156.5 ms	0	AVC Header Scan Service Time	156.5 ms	0
Webroot Response Body Service Time	10.0 ms	0	Ironport Data Security Service Time	10.0 ms	0
Webroot Response Body Service Time	14.6 ms	0	Ironport Data Security Service Time	17.3 ms	0
Webroot Response Body Service Time	21.4 ms	0	Ironport Data Security Service Time	30.0 ms	0
Webroot Response Body Service Time	31.3 ms	0	Ironport Data Security Service Time	52.1 ms	0
Webroot Response Body Service Time	45.7 ms	0	Ironport Data Security Service Time	90.3 ms	0
Webroot Response Body Service Time	66.9 ms	0	Ironport Data Security Service Time	156.5 ms	0
WBRB Service Time	1.0 ms	3917	See the user guide for all custom fields associated with these values.		
WBRB Service Time	1.6 ms	198			
WBRB Service Time	2.5 ms	60			
WBRB Service Time	4.0 ms	16			
WBRB Service Time	6.3 ms	6			
WBRB Service Time	10.0 ms	6			

Eine einzelne SHD-Protokollzeile wird alle 60 Sekunden geschrieben und enthält viele Felder, die für die Leistungsüberwachung wichtig sind, z. B. Latenz, RPS und die Gesamtanzahl der Client- und Serververbindungen. Dies ist ein Beispiel für eine SHD-Protokollzeile:

```
Fri Nov 11 14:16:42 2022 Info: Status: CPULd 2.4 DskUtil 45.7 RAMUtil 6.7 Reqs 62 Band 11383 Latency 619
Fri Nov 11 14:17:42 2022 Info: Status: CPULd 2.6 DskUtil 45.7 RAMUtil 6.7 Reqs 55 Band 10532 Latency 774
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 791
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 1403
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
```

Den access_logs können weitere benutzerdefinierte Felder hinzugefügt werden, die Latenzinformationen für einzelne Anforderungen angeben. Zu diesen Feldern gehören Serverantwort, DNS-Auflösung und AV-Scanner-Latenz. Die Felder müssen dem Protokoll hinzugefügt werden, um nützliche Informationen für die Fehlerbehebung zu sammeln. Dies ist die empfohlene benutzerdefinierte Feldzeichenfolge für die Verwendung:

```
[ 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<, F

a; DNS response = %:

d, WBRs response = %:

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

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

Die aus diesen Werten abgeleiteten Leistungsinformationen sind wie folgt:

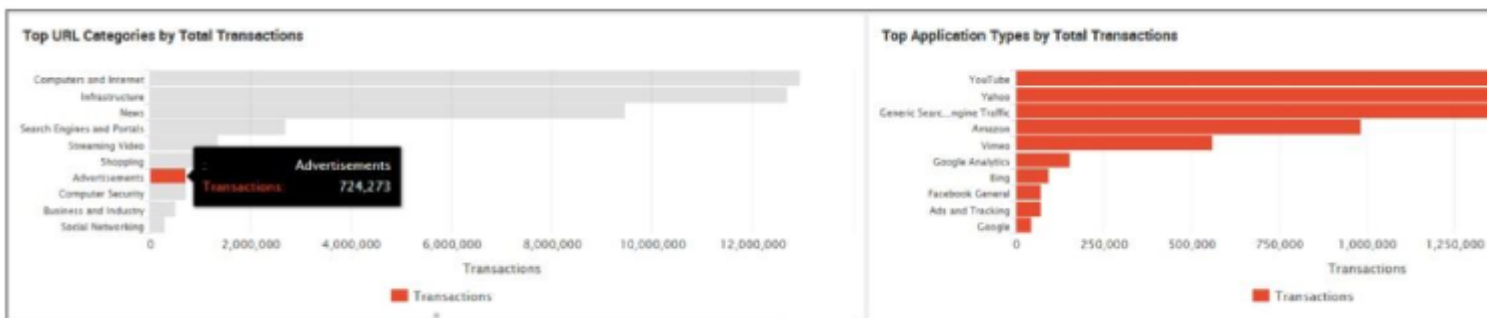
Benutzerdefiniertes Feld	Beschreibung
%:<a	Warten Sie, bis die Antwort vom Webproxy-Authentifizierungsprozess empfangen wird, nachdem der Webproxy die Anforderung gesendet hat.
%:<b	Wartezeit, bis der Anforderungstext nach dem Header auf den Server geschrieben wird.
%:<d	Warten Sie, bis die Antwort vom Webproxy-DNS-Prozess empfangen wird, nachdem der Webproxy die Anforderung gesendet hat.
%:<h	Wartezeit, bis der Anforderungsheader nach dem ersten Byte auf den Server

	geschrieben wird.
%:<r	Die Wartezeit bis zum Empfang der Antwort von den Web-Reputationsfiltern, nachdem der Web-Proxy die Anforderung gesendet hat.
%:<s	Warten Sie, bis das Urteil vom Anti-Spyware-Prozess des Webproxys eingegangen ist, nachdem der Webproxy die Anforderung gesendet hat.
%:>	Wartezeit auf das erste Antwortbyte vom Server.
%:>a	Die Wartezeit bis zum Empfang der Antwort vom Webproxy-Authentifizierungsprozess, einschließlich der Zeit, die der Webproxy benötigt, um die Anforderung zu senden.
%:>b	Wartezeit auf vollständigen Antworttext nach Empfang des Headers.
%:>c	Die Zeit, die der Webproxy benötigt, um eine Antwort aus dem Festplatten-Cache zu lesen.
%:>d	Die Wartezeit, bis die Antwort vom DNS-Prozess des Webproxys empfangen wird. Dies schließt die Zeit ein, die der Webproxy benötigt, um die Anforderung zu senden.
%:>h	Wartezeit für den Server-Header nach dem ersten Antwortbyte.
%:>r	Die Wartezeit, bis das Urteil der Web-Reputationsfiltereingeht, beinhaltet die Zeit, die der Web-Proxy benötigt, um die Anforderung zu senden.
%:>s	Wartezeit bis zum Empfang des Urteils vom Antispyware-Prozess des Webproxys, einschließlich der Zeit, die der Webproxy benötigt, um die Anforderung zu senden.
%:l<	Wartezeit für das erste Anforderungsbyte einer neuen Clientverbindung.
%:l>	Wartezeit für das erste auf den Client geschriebene Byte.
%:b<	Wartezeit auf vollständigen Clienttext.
%:b>	Wartezeit für den vollständigen Text, der auf den Client geschrieben wurde.
%:e>	Wartezeit bis zum Empfang der Antwort vom AMP-Scanmodul, nachdem der Webproxy die Anforderung gesendet hat.
%:e<	Wartezeit bis zum Empfang des Urteils von der AMP-Scan-Engine, einschließlich der Zeit, die der Webproxy benötigt, um die Anforderung zu senden.
%:h<	Wartezeit für vollständigen Client-Header nach dem ersten Byte.
%:h>	Wartezeit für den vollständigen, auf den Client geschriebenen Header.
%:m<	Die Wartezeit bis zum Empfang des Urteils vom McAfee-Scan-Modul, einschließlich der Zeit, die der Web-Proxy benötigt, um die Anforderung zu senden.
%:m>	Warten Sie, bis die Antwort vom McAfee-Scan-Modul empfangen wird, nachdem der Web-Proxy die Anfrage gesendet hat.
%F	Client-Quellport.
%p	Webserver-Port.
%k	IP-Adresse der Datenquelle (Webserver-IP-Adresse).
%:w<	Die Wartezeit bis zum Empfang des Urteils vom Webroot-Scanmodul, einschließlich der Zeit, die der Webproxy benötigt, um die Anforderung zu senden.
%:w>	Warten Sie, bis die Antwort vom Webroot-Scanmodul empfangen wird, nachdem der Webproxy die Anforderung gesendet hat.

Das SWA-Lizenzmodell ermöglicht die Wiederverwendung von Lizenzen für physische Appliances für virtuelle Appliances. Sie können diese nutzen und Test-SWA-v-Appliances zur Verwendung in Laborumgebungen bereitstellen. Neue Funktionen und Konfigurationen können auf diese Weise gesteuert werden, um Stabilität und Zuverlässigkeit ohne gleichzeitige Verletzung von Lizenzbedingungen zu gewährleisten.

Advanced Web Security Reporting (AWSR)

AWSR muss genutzt werden, um die Berichtsdaten aus den SWAs optimal zu nutzen. Insbesondere in Umgebungen, in denen viele SWAs bereitgestellt werden, ist diese Lösung um ein Vielfaches skalierbarer als die Verwendung von zentralisiertem Reporting auf einer **Security Management Appliance (SMA)** und bietet benutzerdefinierte Reporting-Attribute, die den Daten eine enorme Tiefe und Anpassung verleihen. Die Berichte können gruppiert und an die Anforderungen jedes Unternehmens angepasst werden. Die Cisco Advanced Services-Gruppe muss bei der Bedarfsbestimmung für AWSR verwendet werden.



E-Mail-Benachrichtigung

Das integrierte E-Mail-Warnsystem der SWA lässt sich am besten als Basis-Warnsystem einsetzen. Es muss entsprechend den Anforderungen des Administrators angepasst werden, da es sehr laut sein kann, wenn alle Informationsereignisse aktiviert sind. Es ist wichtiger, die Warnmeldungen einzuschränken und aktiv zu überwachen, als bei allen Vorgängen Warnmeldungen auszugeben und sie als Spam zu ignorieren.

Warnmeldungseinstellungen	Konfiguration
Von Adresse, die beim Senden von Warnungen verwendet wird	Automatisch generiert
Anfängliche Wartezeit in Sekunden bis zum Senden einer doppelten Warnung	300 Sekunden
Maximale Dauer in Sekunden, die gewartet wird, bevor ein Alert-Doppel gesendet wird	3600 Sekunden

Verfügbarkeitsüberwachung

Es gibt zwei Methoden zur Überwachung der Verfügbarkeit eines Webproxys. Die erste ist die **Layer-3-Überwachung (L3)**, die prüft, ob die IP-Adresse der Appliance im Netzwerk erreichbar ist. Der einfachste Weg, dies zu testen, besteht darin, eine **ICMP-Echo-(Ping)-Anfrage** in regelmäßigen Abständen an die Adresse zu senden und nach einem Antwortpaket zu suchen. Die Attribute der Antwort, z. B. TTL, und die Latenz können analysiert werden, um den Zustand der Netzwerkschicht zu bestimmen.

Es ist möglich, dass ein Gerät auf Pings reagiert, die Proxy-Prozesse jedoch nicht oder nur zeitweilig. Aus diesem Grund ist es ratsam, einen **Layer-7-Monitor (L7)** zu verwenden, der eine explizite Proxy-Anforderung an die Appliance sendet und einen **200 OK-HTTP-Antwortcode** erwartet. Dabei wird nicht nur

die Erreichbarkeit der Netzwerkschnittstelle getestet, sondern auch die Reaktionsfähigkeit der Proxydienste und die Funktionsfähigkeit der Upstream-Dienste, falls eine externe Ressource angefordert wird. Diese Art der Überwachung erfolgt in der Regel in Form einer expliziten **HTTP-HEAD**-Anforderung, die den Proxy auffordert, eine Verbindung mit einer Ressource herzustellen. Die **HEAD**-Methode fordert die Header an, die zurückgegeben werden, damit der Client eine **GET**-Anforderung senden muss, enthält jedoch nur die Antwortheader und keine Daten.

Wenn Sie ein **L7**-Überwachungstool oder -skript verwenden, müssen Sie sicherstellen, dass der Datenverkehr von der Authentifizierung ausgenommen ist. Andernfalls kann es zu regelmäßigen Authentifizierungsfehlern und zur Auslastung von Ressourcen kommen. Wenn Sie eine benutzerdefinierte Benutzer-Agent-Zeichenfolge im Überwachungstool verwenden, muss dieser zur Identifizierung des Datenverkehrs verwendet werden. Auch wenn der Datenverkehr von der Authentifizierung ausgenommen ist, kann er durch die Zugriffsrichtlinien dennoch vor unnötigem Internetzugriff eingeschränkt werden.

Wenn Sie eine oder mehrere dieser Methoden verwenden, muss ein Administrator eine Baseline akzeptabler Metriken für die Proxyantwort erstellen und diese zum Erstellen von Warnmeldungsschwellenwerten verwenden. Sie müssen Zeit aufwenden, um die Antworten dieser Prüfungen zu sammeln, und bevor Sie entscheiden, wie Sie die Schwellenwerte und die Warnmeldung konfigurieren.

SNMP-Überwachung

Das **Simple Network Management Protocol (SNMP)** ist die wichtigste Methode zur Überwachung des Systemzustands der Appliance. Sie kann verwendet werden, um Warnungen von der Appliance zu empfangen (Traps) oder um verschiedene **Objektkennungen (OIDs) abzufragen**, um Informationen zu sammeln. Die SWAs enthalten zahlreiche OIDs, die sämtliche Aspekte abdecken, von der Hardware- über die Ressourcennutzung bis hin zu individuellen Prozessinformationen und Anforderungsstatistiken.

Es gibt eine Reihe spezifischer **Machine Information Base (MIB)**, die aus Hardware- und leistungsbezogenen Gründen überwacht werden müssen. Die vollständige Liste der MIBs finden Sie hier: <https://www.cisco.com/web/ironport/tools/web/asyncosweb-mib.txt>.

Es handelt sich hierbei um eine Liste der zu überwachenden empfohlenen MIBs, nicht jedoch um eine vollständige Liste:

Hardware-OID	Name
1.3.6.1.4.1.15497.1.1.1.18.1.3	RAID-ID
1.3.6.1.4.1.15497.1.1.1.18.1.2	RAID-Status
1.3.6.1.4.1.15497.1.1.1.18.1.4	raidLetzterFehler
1.3.6.1.4.1.15497.1.1.1.10	Lüfertabelle
1.3.6.1.4.1.15497.1.1.1.9.1.2	Grad Celsius

Dies sind OIDs, die direkt der Ausgabe des CLI-Befehls **status detail** zugeordnet werden:

OID	Name	Statusdetailfeld
Systemressourcen		

1.3.6.1.4.1.15497.1.1.1.2.0	proCentCPU-Auslastung	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	perCentSpeicherauslastung	RAM
Transaktionen pro Sekunde		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	CacheDurchsatzJetzt	Durchschnittliche Transaktionen pro Sekunde in letzter Minute.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	CacheDurchsatz1StdPeak	Maximale Anzahl von Transaktionen pro Sekunde in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	CacheDurchsatz1StdMittel	Durchschnittliche Transaktionen pro Sekunde in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	CacheDurchsatzLifePeak	Maximale Anzahl von Transaktionen pro Sekunde seit dem Neustart des Proxys.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	CacheDurchsatzLebensmittel	Durchschnittliche Transaktionen pro Sekunde seit dem Neustart des Proxys.
Bandbreite		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBreiteGesamtJetzt	Durchschnittliche Bandbreite in letzter Minute.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	CacheBwidthTotal1StdPeak	Maximale Bandbreite in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	CacheBreiteInsgesamt1StdMittel	Durchschnittliche Bandbreite in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	CacheBwidthTotalLifePeak	Maximale Bandbreite seit dem Neustart des Proxys.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	ZwischenspeicherGesamtlebensdauerMittel	Durchschnittliche Bandbreite seit dem Neustart des Proxys.
Reaktionszeit		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	CacheTrefferJetzt	Durchschnittliche Cache-Trefferrate in

		letzter Minute.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	CacheTreffer1StdPeak	Maximale Cache-Trefferrate in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	CacheHits1StdMean	Durchschnittliche Cache-Trefferrate in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	ZwischenspeicherTrefferLebensspitze	Die maximale Cache-Trefferrate seit dem Neustart des Proxys.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	ZwischenspeicherTrefferLebensmittel	Durchschnittliche Cache-Trefferrate seit Proxy-Neustart.
Cache-Trefferrate		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	CacheTrefferJetzt	Durchschnittliche Cache-Trefferrate in letzter Minute.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	CacheTreffer1StdPeak	Maximale Cache-Trefferrate in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	CacheHits1StdMean	Durchschnittliche Cache-Trefferrate in der letzten Stunde.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	ZwischenspeicherTrefferLebensspitze	Die maximale Cache-Trefferrate seit dem Neustart des Proxys.
1.3.6.1.4.1.15497.1.2.3.7.5.9.0	ZwischenspeicherTrefferLebensmittel	Durchschnittliche Cache-Trefferrate seit Proxy-Neustart.
Verbindungen		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	Inaktive Clientverbindungen.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleVerbindungen	Inaktive Serververbindungen
1.3.6.1.4.1.15497.1.2.3.2.8.0	CacheClientGesamtVerbindungen	Clientverbindungen gesamt
1.3.6.1.4.1.15497.1.2.3.3.8.0	CacheServerInsgesamtVerbindungen	Serververbindungen gesamt

Schlussfolgerung

In diesem Leitfaden werden die wichtigsten Aspekte der SWA-Konfiguration, -Bereitstellung und -Überwachung beschrieben. Als Referenz dient die Bereitstellung wertvoller Informationen für alle, die eine möglichst effektive Nutzung der SWA sicherstellen möchten. Die hier beschriebenen Best Practices sind wichtig für die Stabilität, Skalierbarkeit und Effizienz des Geräts als Sicherheitstool. Darüber hinaus soll die

Lösung auch in Zukunft eine relevante Ressource bleiben und muss daher regelmäßig aktualisiert werden, um Veränderungen bei Netzwerkumgebungen und Produktmerkmalen Rechnung zu tragen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.