Best practices voor beveiligde web applicatie gebruiken

Inhoud

Inleiding
Achtergrondinformatie
Netwerkomgeving
ICMP
Firewalls
Unicast doorsturen van omgekeerde paden
IP-spoofing met WCCP
Configuratie van SWA-netwerk
Interfaces
Routing voor beheernetwerk
TALOS-telemetrie
DNS
Taakverdeling
Actieve verificatie
Passieve verificatie
Configuratie van services
Web proxy
HTTPS-proxy
Layer 4 Traffic Monitor (L4TM)
Beleidsconfiguratie
Complexiteit
Identificatieprofielen
Decryptie-beleid
Toegangsbeleid
Aangepaste en externe URL-categorieën
Monitoren en meldingen
CLI-monitoren
Vastlegging
Geavanceerde Web Security Rapportage (AWSR)
E-mailmeldingen
Beschikbaarheidsbewaking
SNMP-bewaking
Conclusie

Inleiding

Dit document beschrijft de beste praktijken voor hoe u de Cisco Secure Web Applicatie (SWA) kunt configureren.

Achtergrondinformatie

Deze handleiding is bedoeld als referentie voor best practice-configuratie en het richt zich op veel aspecten van een SWA-implementatie, omvat de ondersteunde netwerkomgeving, beleidsconfiguratie, bewaking en probleemoplossing. Hoewel de best practices die hier worden gedocumenteerd belangrijk zijn voor alle

beheerders, architecten en operatoren om te begrijpen, zijn het slechts richtlijnen en moeten ze als zodanig worden behandeld. Elk netwerk heeft zijn eigen specifieke vereisten en uitdagingen.

Als beveiligingsapparaat is de SWA op verschillende unieke manieren met het netwerk verbonden. Het is zowel een bron als een bestemming van webverkeer; het werkt tegelijkertijd als webserver en webclient. Het maakt minimaal gebruik van IP-adres op de server Spoofing en man-in-the-middle technieken om HTTPS-transacties te controleren. Het kan ook parodie client-IP-adressen, die een andere laag van complexiteit aan de implementatie toevoegen en extra vereisten aan de ondersteunende netwerkconfiguratie oplegt. In deze handleiding worden de meest voorkomende problemen met betrekking tot de verwante configuratie van netwerkapparaten besproken.

De beleidsconfiguratie van de SWA heeft niet alleen gevolgen voor de veiligheid, de doeltreffendheid en de handhaving, maar ook voor de prestaties van het apparaat. Deze handleiding gaat in op de manier waarop de complexiteit van een configuratie van invloed is op systeembronnen. Het definieert complexiteit in deze context en beschrijft hoe je die kunt minimaliseren in het beleidsontwerp. Er wordt ook aandacht besteed aan specifieke eigenschappen en hoe zij moeten worden gevormd om veiligheid, schaalbaarheid, en doeltreffendheid te verhogen.

In het gedeelte Monitoring and Alerting van dit document wordt uitgelegd hoe u het apparaat het effectiefst kunt bewaken. Bovendien wordt hier aandacht besteed aan de bewaking van de prestaties en beschikbaarheid en aan het gebruik van systeembronnen. Het biedt ook informatie die nuttig is bij het oplossen van basisproblemen.

Netwerkomgeving

ICMP

Path MTU Discovery, zoals gedefinieerd in RFC 1191, het mechanisme bepaalt de maximale grootte van een pakket langs willekeurige paden. In het geval van IPv4 kan een apparaat de Maximum Transmission Unit (MTU) van een pakket langs een pad bepalen door het Donâ€™t Fragment (DF)-bit in de IP-header van het pakket in te stellen. Als, bij één of andere verbinding langs de weg, een apparaat niet het pakket zonder fragment kan door:sturen het, **wordt** een **noodzakelijke Fragmentation van het Protocol van het Bericht van de Controle van Internet (ICMP) (Type 3, Code 4)** bericht teruggestuurd naar de bron. Vervolgens wordt een kleiner pakket opnieuw verzonden. Dit gaat door tot de MTU voor het volledige pad wordt ontdekt. IPv6 ondersteunt fragmentatie niet en gebruikt een ICMPv6-bericht Packet Too Big (Type 2) om aan te geven dat een pakket niet via een bepaalde link kan worden aangepast.

Omdat het proces van pakketfragmentatie ernstige gevolgen kan hebben voor de prestaties van een TCP-stroom, maakt de SWA gebruik van Path MTU Discovery. De genoemde ICMP-berichten moeten worden ingeschakeld in relevante netwerkapparaten om de SWA in staat te stellen de MTU voor het pad door het netwerk te bepalen. Dit gedrag kan worden uitgeschakeld in de SWA met de opdracht **Path** Discovery **Command Line Interface (CLI)**. Als u dit doet, daalt de standaard MTU naar 576 bytes (per RFC 879), wat een zware impact heeft op de prestaties. De beheerder moet de extra stap zetten van het handmatig configureren van de MTU in de SWA vanaf `etherconfig` CLI-opdracht.

In het geval van het **Web Cache Communication Protocol (WCCP)**, wordt webverkeer omgeleid naar de SWA van een ander netwerkapparaat langs het clientpad naar het internet. In dit geval worden andere protocollen, zoals ICMP, niet doorgestuurd naar de SWA. Er is een mogelijkheid dat de SWA een ICMP

Fragmentation Benodigd bericht van een router op het netwerk kon teweegbrengen, maar het bericht zou niet aan de SWA worden geleverd. Als dit een mogelijkheid is in het netwerk, moet Path MTU Discovery worden uitgeschakeld. Zoals vermeld, met deze configuratie, de extra stap van het handmatig instellen van de MTU op de SWA van `etherconfig` CLI-opdracht is vereist.

Firewalls

In een standaardconfiguratie, ontleedt de SWA niet het cliënt IP adres wanneer het proxying van een verbinding. Dit betekent dat al het uitgaande webverkeer afkomstig is van het SWA IP-adres. Het is noodzakelijk om ervoor te zorgen dat **NAT**-apparaten **(Network Address Translation)** een voldoende grote pool van externe adressen en poorten hebben om dit aan te passen. Het is een goed idee om specifiek adres voor dit doel te wijden.

Sommige firewalls maken gebruik **van** DoS-bescherming **(Denial-of-Service)** of andere beveiligingsfuncties die geactiveerd worden wanneer grote aantallen gelijktijdige verbindingen afkomstig zijn van één IP-adres van één client. Wanneer IP-spoofing van client niet is ingeschakeld, moet het IP-adres van de SWA worden uitgesloten van deze bescherming.

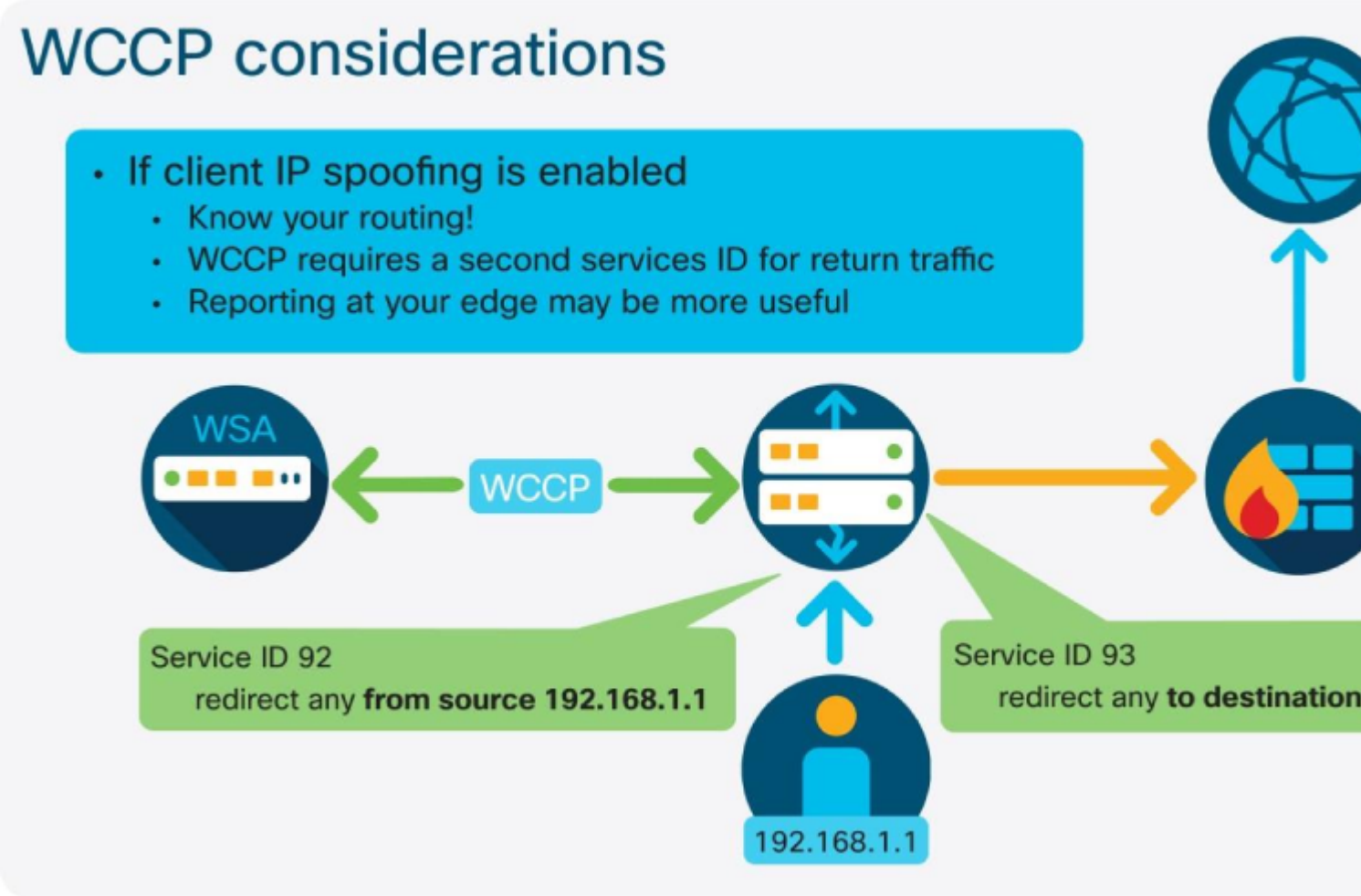
Unicast doorsturen van omgekeerde paden

De SWA spooft het IP-adres van de server wanneer er met een client wordt gecommuniceerd, en kan optioneel worden geconfigureerd om het IP-adres van de client te paraferen wanneer er met een upstream server wordt gecommuniceerd. Beschermingen zoals **Unicast Reverse Path Forwarding (uRPF)** kunnen op switches worden ingeschakeld om ervoor te zorgen dat een inkomend pakket overeenkomt met de verwachte ingangshaven. Deze bescherming controleert de broninterface van een pakket tegen de routeringstabel om ervoor te zorgen dat het op de verwachte poort is gearriveerd. De SWA moet in voorkomend geval van deze beschermingsmaatregelen worden vrijgesteld.

IP-spoofing met WCCP

Wanneer de functie IP-spoofing in de SWA is ingeschakeld, kunnen uitgaande verzoeken het apparaat gebruiken via het bronadres van het oorspronkelijke clientverzoek. Dit vereist extra configuratie van de verwante netwerkinfrastructuur om ervoor te zorgen dat de terugkeerpakketten aan de uitgaande interface van de SWA, in plaats van de cliënt worden geleid die het verzoek voortkwam.

Wanneer WCCP op een netwerkapparaat (router, switch of firewall) is geïmplementeerd, wordt een service-ID gedefinieerd die verkeer aanpast op basis van een **toegangscontrolelijst (ACL)**. De service-ID wordt vervolgens toegepast op een interface en gebruikt om verkeer aan te passen voor omleiding. Als IP-spoofing is ingeschakeld, moet een tweede service-ID worden gemaakt om ervoor te zorgen dat het retourverkeer ook naar de SWA wordt omgeleid.



Configuratie van SWA-netwerk

Interfaces

De SWA heeft vijf bruikbare netwerkinterfaces: M1, P1, P2, T1 en T2. Elk van deze moet zo mogelijk voor zijn specifieke doel worden aangewend. Het is nuttig om elke haven te gebruiken om eigen redenen. De M1-interface moet worden aangesloten op een speciaal beheernetwerk en split-routing moet worden ingeschakeld om de blootstelling van administratieve services te beperken. De P1 kan worden beperkt tot het verkeer van het cliëntverzoek, In tegenstelling, mag P2 geen expliciete volmachtsverzoeken goedkeuren. Dit vermindert de hoeveelheid verkeer op elke interface en staat betere segmentatie in het netwerkontwerp toe.

De T1- en T2-poorten zijn beschikbaar voor de functie **Layer 4 Traffic Monitor (L4TM)**. Deze functie bewaakt een gespiegelde Layer 2-poort en voegt de mogelijkheid toe om verkeer te blokkeren op basis van een geblokkeerde lijst met bekende kwaadaardige IP-adressen en domeinnamen. Het doet dit door de bron en de bestemming IP adressen van verkeer te bekijken en verzendt een TCP teruggesteld pakket, of het Onbereikbare bericht van de Haven als de geblokkeerde lijst wordt aangepast. Het verkeer dat met elk protocol wordt verstuurd, kan met deze functie worden geblokkeerd.

Zelfs als de L4TM-functie niet is ingeschakeld, kan Transparent omzeilen worden verbeterd wanneer de T1 en T2 poorten zijn aangesloten op een gespiegelde poort. In het geval van WCCP kent de SWA alleen het IP-adres van de bron en de bestemming van een inkomend pakket en moet hij beslissen of hij dit pakket als proxy zal gebruiken of dat hij het zal omzeilen op basis van die informatie. De SWA lost elke 30 minuten

alle items in de lijst met omzeilingsinstellingen op, ongeacht de **tijd** die de record **nodig heeft om te leven (TTL)**. Als de L4TM-functie is ingeschakeld, kan de SWA echter gesnoopte DNS-vragen gebruiken om deze records vaker bij te werken. Dit vermindert het risico van een vals negatief in een scenario waarin de klant een ander adres dan de SWA heeft opgelost.

Routing voor beheernetwerk

Als het specifieke beheernetwerk geen internettoegang heeft, kan elke service worden geconfigureerd om de tabel met gegevensrouting te gebruiken. Dit kan worden aangepast aan de netwerktopologie, maar in het algemeen wordt voorgesteld om het beheernetwerk voor alle systeemdiensten en het datanetwerk voor clientverkeer te gebruiken. Vanaf AsyncOS versie 11.0 zijn de services waarvoor routing kan worden ingesteld:

- Externe URL-feeds
- **Advanced Malware Protection (AMP)**, reputatie en analyse van bestanden
- Updates en upgrades
- DNS
- Actieve map

Voor extra uitgaande filtering van beheerverkeer kunnen statische adressen worden geconfigureerd voor gebruik in deze services:

- Externe URL-feeds:
  1. Aangepast is afhankelijk van waar ze worden gehost
  2. reputatie en analyse van AMP-bestanden
  3. cloud-sa.amp.cisco.com (Noord-Amerika)
  4. cloud-sa.eu.amp.cisco.com (Europa)
  5. cloud-sa.apjc.amp.cisco.com

- Bijwerken en upgrades:
  1. downloads-static.ironport.com
  2. updates-static.ironport.com

TALOS-telemetrie

De Cisco Talos-groep is bekend voor het identificeren van nieuwe en opkomende bedreigingen. Alle gegevens die naar Talos worden verzonden, worden geanonimiseerd en opgeslagen in Amerikaanse datacentra. Het deelnemen aan SensorBase verbetert de categorisering en identificatie van webbedreigingen en leidt tot een betere bescherming tegen de SWA, evenals andere Cisco-beveiligingsoplossingen.

DNS

De best practices voor de beveiliging van Domain Name Server (DNS) suggereren dat elk netwerk twee DNS-resolvers moet hosten: één voor gezaghebbende records vanuit een lokaal domein en één voor recursieve resolutie van internetdomeinen. Om dit aan te passen, laat de SWA DNS servers toe om voor specifieke domeinen worden gevormd. Als slechts één DNS server beschikbaar is voor zowel lokale als recursieve vragen, overweeg de extra lading het wanneer gebruikt voor alle vragen van de SWA toevoegt. De betere optie kan zijn om interne resolver voor lokale domeinen en de wortel Internet resolvers voor externe domeinen te gebruiken. Dit is afhankelijk van het risicoprofiel en de tolerantie van de beheerder.

Standaard heeft de SWA-cache een DNS-record gedurende minimaal 30 minuten, ongeacht de TTL van de record. Moderne websites die zwaar gebruik maken van **Content Delivery Networks (CDNâ€™s)** hebben lage TTL-records omdat hun IP-adressen vaak veranderen. Dit kan ertoe leiden dat een client één IP-adres voor een bepaalde server en de SWA een ander adres voor dezelfde server cachen. Om dit tegen te gaan, kan

de SWA standaard TTL worden verlaagd tot vijf minuten van deze CLI-opdrachten:

```
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.
...
```

Secundaire DNS-servers moeten worden geconfigureerd voor het geval dat de primaire server niet beschikbaar is. Als alle servers met dezelfde prioriteit zijn geconfigureerd, wordt de IP-server willekeurig gekozen. Afhankelijk van het aantal geconfigureerde servers varieert de time-out voor een bepaalde server. De tabel is de time-out voor een query voor maximaal zes DNS-servers:

Aantal DNS-servers	**Query-tijdelijke versie (achter elkaar)**
1	60
2	5, 45
3	10, 45
4	1, 3, 11, 45
5	1, 3, 11, 45, 1
6	1, 3, 11, 45, 1, 1

Er zijn ook geavanceerde DNS-opties die alleen via de CLI beschikbaar zijn. Deze opties zijn beschikbaar in CLI:

advancedproxyconfig > DNS uit. Selecteer een van deze opties:

- 0-altijd gebruik DNS antwoorden in volgorde
- 1-gebruik het client-geleverde adres dan DNS
- 2-beperkt DNS-gebruik
- 3-zeer beperkt DNS gebruik

Voor de opties 1 en 2 wordt DNS gebruikt als Web Reputation is ingeschakeld.

Voor opties 2 en 3, DNS wordt gebruikt voor expliciete volmachtsverzoeken, als er geen stroomopwaartse volmacht is of in het geval de gevormde stroomopwaartse volmacht ontbreekt.

Voor alle opties, DNS wordt gebruikt wanneer de IP van de Bestemming adressen in beleidslidmaatschap worden gebruikt.

Deze opties bepalen hoe de SWA beslist over het IP-adres waarmee verbinding moet worden gemaakt tijdens de evaluatie van een clientverzoek. Wanneer een verzoek wordt ontvangen, ziet de SWA een bestemmingsIP adres en een hostname. De SWA moet beslissen of het oorspronkelijke IP-adres van de bestemming voor de TCP-verbinding moet worden vertrouwd, of dat de eigen DNS-resolutie moet worden uitgevoerd en het opgeloste adres moet worden gebruikt. Standaard is "0 = Gebruik altijd DNS-antwoorden in volgorde," wat betekent dat de SWA niet vertrouwt op de client om het IP-adres te leveren.

- Optie 1: De SWA probeert het door de client geleverde IP-adres voor de verbinding, maar valt terug naar het opgeloste adres als dat mislukt. Het opgeloste adres wordt gebruikt voor beleidsevaluatie (webcategorie, webreputatie, enzovoort).
- Optie 2â€”De SWA gebruikt alleen het door de client opgegeven adres voor de verbinding en valt niet terug. Het opgeloste adres wordt gebruikt voor beleidsevaluatie (webcategorie, webreputatie, enzovoort).
- Optie 3â€”De SWA gebruikt alleen het door de client opgegeven adres voor de verbinding en valt niet terug. Het door de klant opgegeven IP-adres wordt gebruikt voor beleidsevaluatie (webcategorie, webreputatie, enzovoort).

De gekozen optie hangt af van hoeveel vertrouwen de beheerder in de cliënt moet plaatsen wanneer het bepalen van het opgeloste adres voor een bepaalde hostname. Als de client een stroomafwaartse proxy is, kies optie 3 om de extra latentie van onnodige DNS-lookups te voorkomen.

Taakverdeling

WCCP maakt een transparante verdeling van de verkeersbelasting mogelijk wanneer maximaal acht toestellen worden gebruikt. Het maakt het mogelijk om verkeersstromen te balanceren op basis van hash of masker, het kan worden gewogen als er een mix van apparaatmodellen in het netwerk, en apparaten kunnen worden toegevoegd en verwijderd uit de servicepool zonder downtime. Wanneer de behoefte groter is dan wat met acht SWA's kan worden behandeld, wordt aanbevolen een speciale lastverdeler te gebruiken.

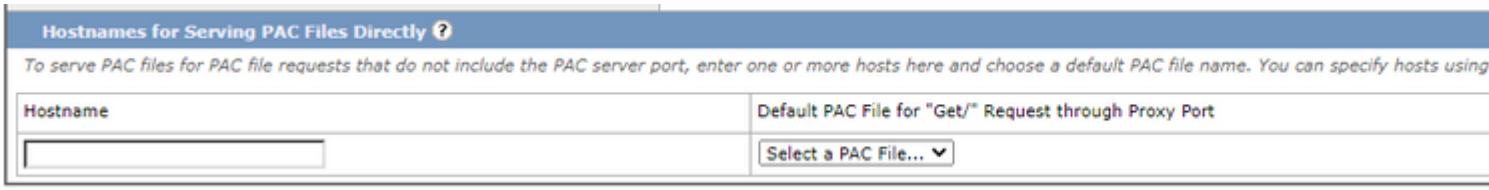
De specifieke best practices voor WCCP-configuratie variëren op basis van het gebruikte platform. Voor Cisco Catalyst ®-switches worden de beste praktijken gedocumenteerd in het witboek Cisco Catalyst Instant Access Solution.

WCCP heeft beperkingen bij gebruik in combinatie met een Cisco adaptieve security applicatie (ASA). IP-spoofing van clients wordt namelijk niet ondersteund en de clients en SWA moeten achter dezelfde interface staan. Om deze reden is het flexibeler om een Layer 4-switch of -router te gebruiken om verkeer om te leiden. WCCP-configuratie op het ASA-platform wordt beschreven in WCCP on ASA: Concepts, Limitations, and Configuration.

Voor expliciete implementaties, is een Proxy Automation (PAC) bestand de meest gebruikte methode, maar het heeft veel nadelen en veiligheidsimplicaties die buiten het bereik van dit document vallen. Als een PAC-bestand wordt geïmplementeerd, wordt voorgesteld om Group Policy Objects (GPO's) te gebruiken om de locatie te configureren in plaats van te vertrouwen op het Web Proxy AutoDiscovery Protocol (WPAD) dat een gemeenschappelijk doel is voor aanvallers en gemakkelijk kan worden geëxploiteerd als het verkeerd is geconfigureerd. De SWA kan meerdere PAC-bestanden hosten en hun verloop in het cache van de browser controleren.

Een PAC-bestand kan direct bij de SWA worden opgevraagd vanaf een configureerbaar TCP-poortnummer

(9001 standaard). Als een haven niet wordt gespecificeerd, kan het verzoek naar het volmachtsproces zelf worden verzonden alsof het een uitgaand Webverzoek was. In dit geval is het mogelijk om een specifiek PAC-bestand te ondersteunen op basis van de HTTP-hostheader die in het verzoek aanwezig is.



Kerberos moet anders worden geconfigureerd wanneer het wordt gebruikt in een omgeving met hoge beschikbaarheid. De SWA biedt ondersteuning voor keytab-bestanden, waardoor meerdere hostnamen kunnen worden gekoppeld aan een **Service Principle Name (SPN)**. Zie Een serviceaccount maken in Windows Active Directory voor Kerberos-verificatie in implementaties met hoge beschikbaarheid voor meer informatie.

Actieve verificatie

Kerberos is een veiliger en breder ondersteund verificatieprotocol dan **NT LAN Manager Security Support Provider (NTSP)**. Het besturingssysteem Apple OS X ondersteunt NTLMSSP niet, maar kan Kerberos gebruiken om te verifiëren of domeinnamen worden toegevoegd. Basis verificatie mag niet worden gebruikt, omdat het referenties verstuurt die niet zijn versleuteld in de HTTP-header en gemakkelijk kunnen worden gesnuifd door een aanvaller op het netwerk. Als er basisverificatie moet worden gebruikt, moet credentiële codering zijn ingeschakeld om ervoor te zorgen dat de referenties worden verzonden via een versleutelde tunnel.

Er moet meer dan één domeincontroller worden toegevoegd aan de configuratie om beschikbaarheid te garanderen, maar er is geen inherente taakverdeling van dit verkeer. De SWA stuurt een TCP SYN pakket naar alle geconfigureerde domeincontrollers en de eerste om te reageren wordt gebruikt voor verificatie.

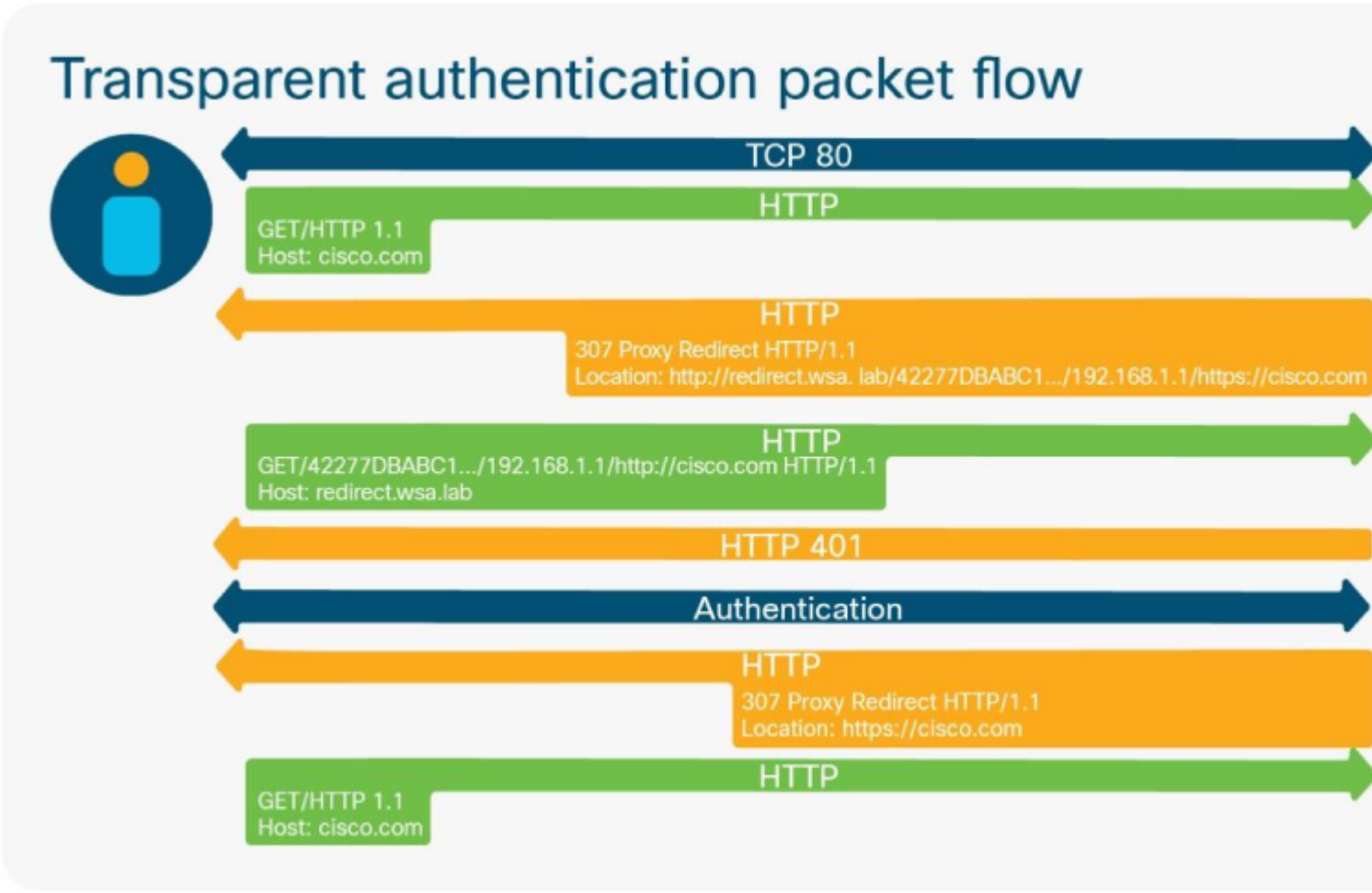
De "redirect hostname" die is geconfigureerd in de authenticatie instellingen pagina bepaalt waar een transparante client wordt verzonden om de authenticatie te voltooien. Om een Windows-client geïntegreerde verificatie te voltooien en **Single Sign-On (SSO)** te bereiken, moet de redirect hostname in de zone "Trusted Sites" in het bedieningspaneel "Internet-opties" staan. Het Kerberos-protocol vereist dat de **FQDN (FFull Qualified Domain Name)** wordt gebruikt om een resource te specificeren, wat betekent dat de naam "shortname" (of "NETBIOS") niet kan worden gebruikt als Kerberos het beoogde verificatiemechanisme is. De FQDN moet handmatig worden toegevoegd aan de "Trusted Sites" (bijvoorbeeld via het groepsbeleid). Bovendien moet de optie Automatisch inloggen met gebruikersnaam en wachtwoord worden ingesteld in het bedieningspaneel "Internet-opties".

Er zijn ook aanvullende instellingen nodig in Firefox voor de browser om de verificatie met netwerkproxy's te voltooien. Deze instellingen kunnen worden geconfigureerd in de pagina **About:config**. Voor Kerberos om met succes te voltooien, moet redirect hostname worden toegevoegd aan de optie **network.onderhandelate-auth.usted-uris**. Voor NTLMSSP, moet het aan de optie **network.automatic-ntlm-auth.usted-uris** worden toegevoegd.

Verificatieplaatsvervangers worden gebruikt om een geverifieerde gebruiker voor een ingestelde duur te onthouden nadat de verificatie is voltooid. IP-surrogaten moeten waar mogelijk worden gebruikt om het aantal actieve verificatiegebeurtenissen dat plaatsvindt te beperken. Actief authenticeren van een client is een resourcetaak, vooral wanneer Kerberos wordt gebruikt. De surrogaattijd is standaard 3600 seconden

(een uur) en kan worden verlaagd, maar de laagste aanbevolen waarde is 900 seconden (15 minuten).

Deze afbeelding laat zien hoe "redirect.WSA.lab" wordt gebruikt als de redirect hostnaam.



Passieve verificatie

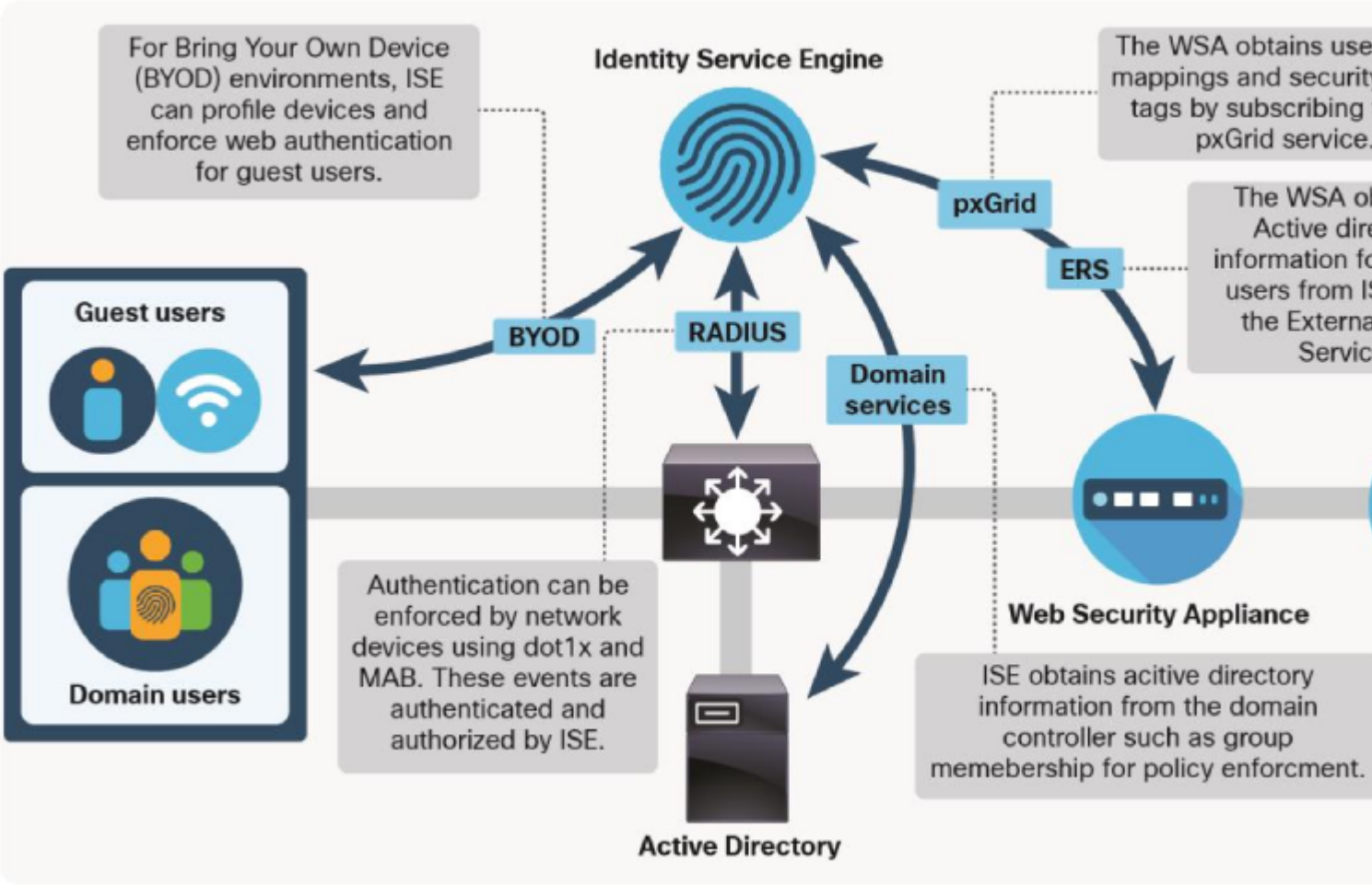
De SWA kan gebruik maken van andere Cisco security platforms om passief proxygebruikers te identificeren. Passieve gebruikersidentificatie maakt een directe verificatieuitdaging en elke Active Directory-communicatie uit de SWA overbodig, waardoor de latentie en het gebruik van bronnen op het apparaat worden beperkt. De momenteel beschikbare mechanismen voor passieve authenticatie zijn via **Context Directory Agent (CDA)**, de **Identity Services Engine (ISE)** en de **Identity Services Connector Passive Identity Connector (ISE-PIC)**.

ISE is een product met veel functies dat beheerders helpt hun verificatieservices te centraliseren en gebruik te maken van een uitgebreide set toegangscontroles voor netwerken. Wanneer ISE leert over een gebruikersverificatie-gebeurtenis (door Dot1x-verificatie of webverificatie omleiden), wordt een sessiedatabank ingevuld die informatie bevat over de gebruiker en het apparaat dat bij de verificatie betrokken is. De SWA maakt verbinding met ISE over het **Platform Exchange Grid (pxGrid)** en krijgt de gebruikersnaam, het IP-adres en de Security Group Tag (SGT) die aan een proxyverbinding zijn gekoppeld. Sinds AsyncOS versie 11.7, kan de SWA ook de **Externe Dienst van de Rust (ERS)** op ISE vragen om groepsinformatie te verkrijgen.

De voorgestelde versies zijn ISE 3.1 en SWA 14.0.2-X en hoger. Voor meer informatie over ISE

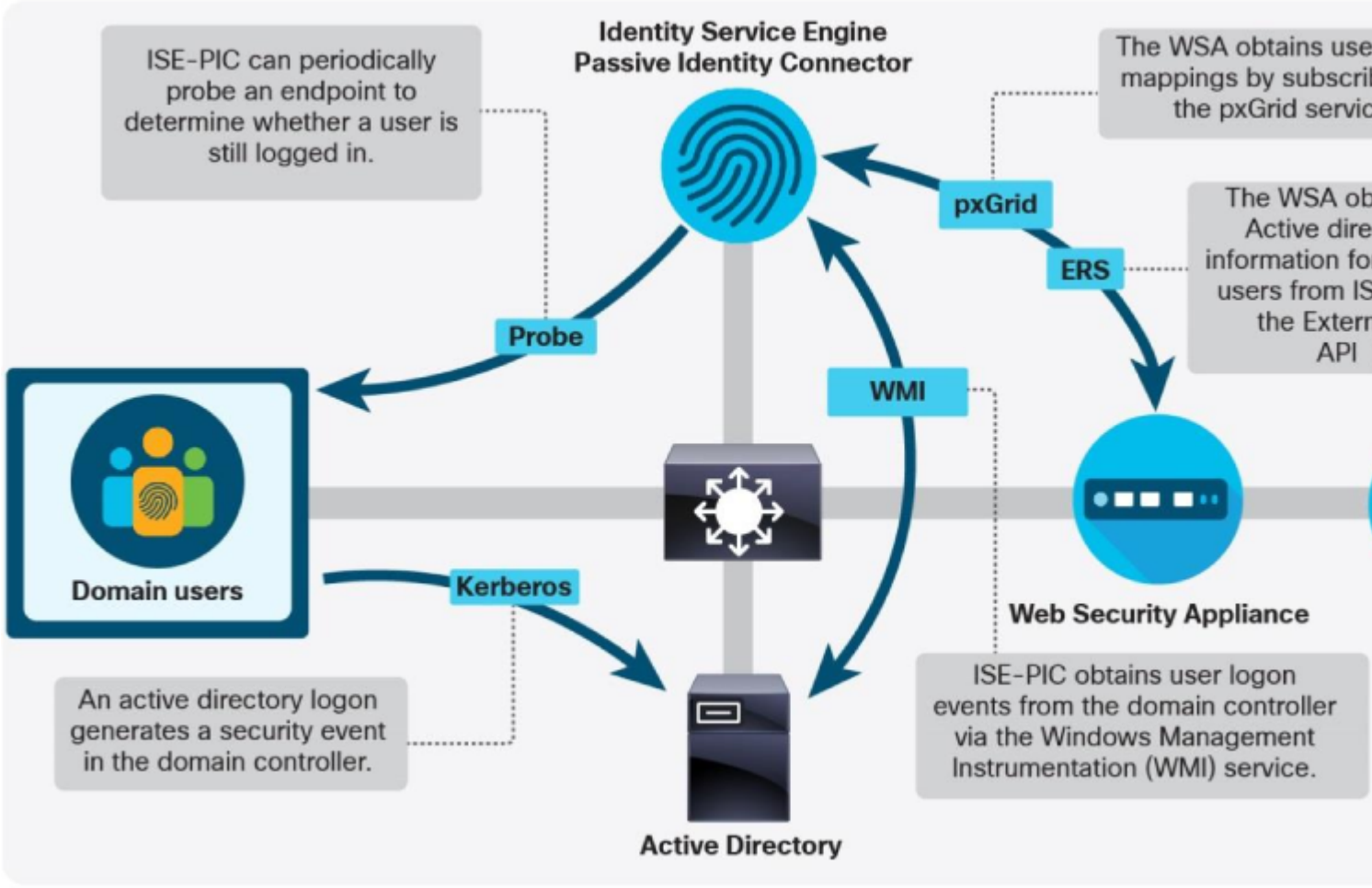
Compatibility Matrix voor SWA, zie ISE Compatibility Matrix for Secure Web Appliance .

Zie Eindgebruikershandleiding voor Web Security Appliance voor meer informatie over de volledige integratiestappen.



Cisco kondigt de end-of-life aan voor de Cisco Context Directory Agent (CDA)-software, zie Cisco Context Directory Agent (CDA).

Vanaf CDA patch 6, is compatibel met Microsoft Server 2016. Beheerders worden echter actief aangemoedigd om hun CDA-implementaties te migreren naar ISE-PIC. Beide oplossingen gebruiken WMI om zich te abonneren op het Windows Security Event Log om user-to-IP-toewijzingen (bekend als "sessies") te genereren. In het geval van CDA, de SWA vraagt deze kaarten met RADIUS. In het geval van ISE-PIC worden dezelfde pxGrid- en ERS-verbindingen gebruikt als bij de volledige ISE-inzet. ISE-PIC-functionaliteit is beschikbaar in een volledige ISE-installatie en in een standalone virtueel apparaat.

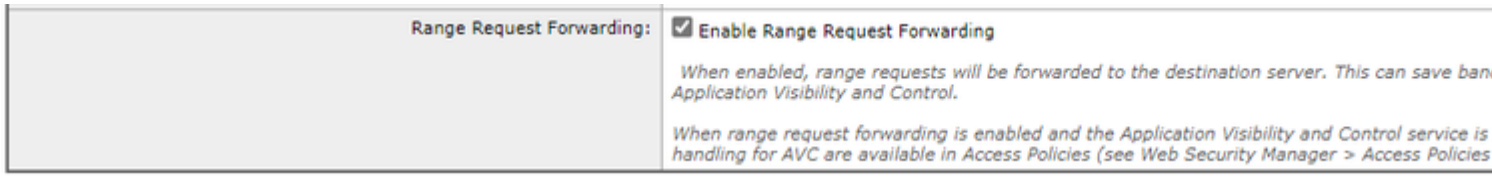


Configuratie van services

Web proxy

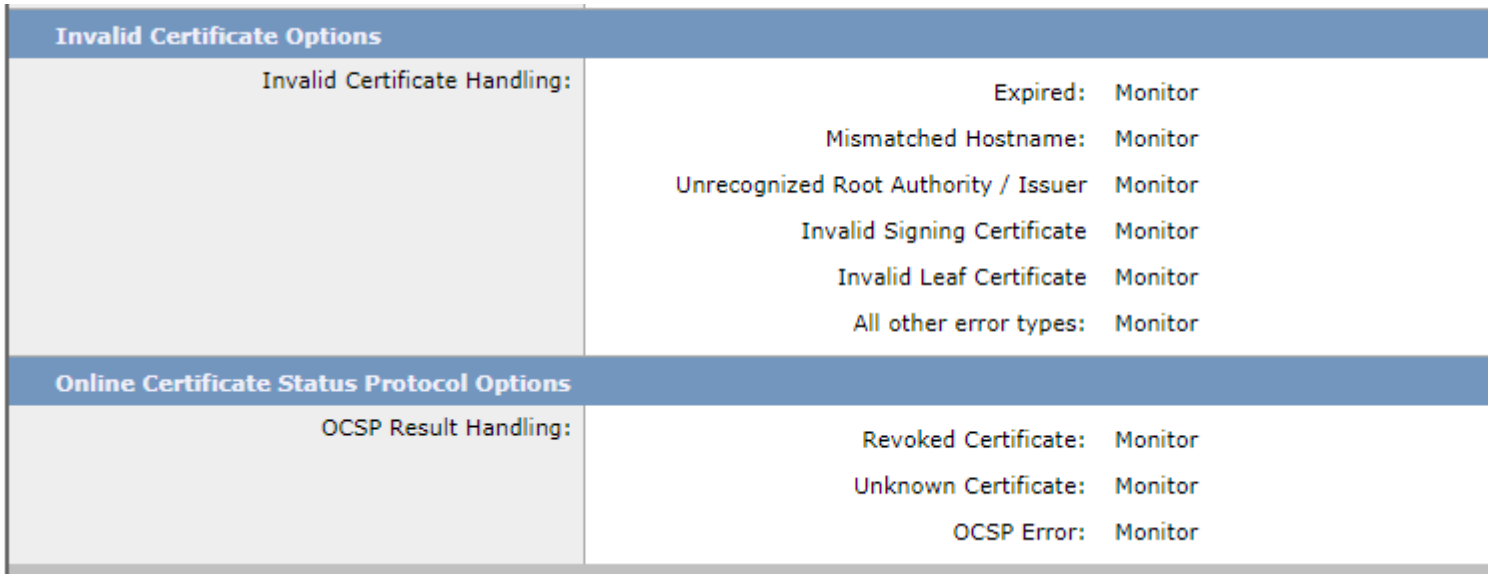
Caching moet in de configuratie van de webproxy zijn ingeschakeld om bandbreedte te besparen en de prestaties te verhogen. Dit wordt minder belangrijk naarmate het percentage HTTPS-verkeer toeneemt, omdat de SWA standaard geen cache HTTPS-transacties bevat. Als de proxy wordt geïmplementeerd om alleen expliciete clients te bedienen, moet de voorwaartse modus worden gespecificeerd om verkeer te weigeren dat niet specifiek voor de proxyservice is bestemd. Op deze manier wordt het oppervlak van de aanval van het apparaat verkleind en wordt een goed beveiligingsprincipe toegepast: schakel het uit als het niet nodig is.

De headers van het bereikverzoek worden gebruikt in HTTP verzoeken om het bytebereik van een bestand dat gedownload moet worden te specificeren. Het wordt algemeen gebruikt door besturingssysteem en applicatie update daemons om kleine delen van een bestand tegelijkertijd over te brengen. Standaard stript de SWA deze kopregels zodat het gehele bestand kan verkrijgen ten behoeve van het scannen van Antivirus (AV), de reputatie en analyse van bestanden en **Application Visibility Control (AVC)**. Als het doorsturen van headers voor bereikverzoeken wereldwijd in de proxy-instellingen wordt ingeschakeld, kunnen beheerders een afzonderlijk toegangsbeleid maken dat deze headers doorstuurt of ontdoet. Meer informatie over deze configuratie wordt uitgelegd in sectie **Toegangsbeleid**.



HTTPS-proxy

Volgens de best practices op beveiligingsgebied moeten er privésleutels worden gegenereerd op het apparaat waar deze worden gebruikt en nooit ergens anders worden vervoerd. De HTTPS-proxywizard maakt het maken van het sleutelpaar en het certificaat mogelijk dat wordt gebruikt voor de decryptie van **TLS-**verbindingen **(Transport Layer Security)**. Het **verzoek tot ondertekening van het certificaat (CSR)** kan dan worden gedownload en ondertekend door een in-house **certificaatautoriteit (CA)**. In een **Active Directory (AD)**-omgeving is dit de beste methode omdat een AD-geïntegreerde CA automatisch wordt vertrouwd door alle leden van het domein en geen extra stappen vereist om het certificaat te implementeren. Een beveiligingsfunctie van de HTTPS-proxy is het valideren van servercertificaten. De beste praktijken stellen voor dat de ongeldige certificaten vereisen dat de verbinding wordt gelaten vallen. Door Decrypt in te schakelen voor EUN kan de SWA een blokpagina presenteren waarin de reden voor het blok wordt uitgelegd. Als dit niet is ingeschakeld, resulteren alle HTTPS-sites die worden geblokkeerd, in een browserfout. Dit leidt tot meer helpdesktickets en de veronderstelling van de gebruiker dat er iets kapot is, in plaats van de wetenschap dat de SWA de verbinding heeft geblokkeerd. Alle ongeldige certificaatopties moeten op ten minste Decrypt worden ingesteld. Als u een van deze opties als monitor laat, kan u geen nuttige foutmeldingen vastleggen in het geval dat certificaatproblemen verhinderen dat een site wordt geladen.



Op dezelfde manier moeten **OCSP**-controles (**Online Certificate Services Protocol)** ingeschakeld worden en mag Monitor niet voor een optie worden gebruikt. Ingetrokken certificaten moeten worden verwijderd en alle andere moeten ten minste op Decrypt worden ingesteld om vastlegging van relevante foutmeldingen mogelijk te maken. **AIA chasing (AIA chasing)** is een middel waarmee een klant de ondertekenaar van het certificaat kan gamen, en een URL van waaruit extra certificaten kunnen worden gehaald. Bijvoorbeeld, als een certificaatketting die van een server wordt ontvangen onvolledig is (het mist een midden of wortelcertificaat), kan de SWA het AIA veld controleren en het gebruiken om de ontbrekende certificaten te halen en authenticiteit te verifiëren. Deze instelling is alleen beschikbaar in de CLI via deze opdrachten:

```
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]>
...
```

> **Opmerking**: deze instelling is standaard ingeschakeld en mag niet worden uitgeschakeld, omdat veel moderne servers op dit mechanisme vertrouwen om een volledige vertrouwensketen aan klanten te bieden.

Layer 4 Traffic Monitor (L4TM)

L4TM is een zeer effectieve manier om het bereik van de SWA uit te breiden met kwaadaardig verkeer dat niet de proxy, waaronder verkeer op alle TCP- en UDP-poorten. De T1- en T2-poorten zijn bedoeld om te worden aangesloten op een netwerktaper of op een switch monitorsessie, waarmee SWA al het verkeer van klanten passief kan controleren. Als er verkeer wordt gezien dat bestemd is voor een kwaadaardig IP-adres, kan de SWA TCP-sessies beëindigen door een RST te verzenden en het IP-adres van de server te spoofen. Voor UDP-verkeer kan er een onbereikbaar bericht op Port worden verstuurd. Bij het configureren van de monitorsessie is het het beste om verkeer dat bestemd is voor de beheerinterface van de SWA uit te sluiten om te voorkomen dat de functie de toegang tot het apparaat mogelijk verstoort.
Naast het controleren op kwaadaardig verkeer, de L4TM ook snoops DNS-vragen om de lijst met omzeilingsinstellingen bij te werken. Deze lijst wordt gebruikt in WCCP implementaties om bepaalde verzoeken terug te sturen naar de WCCP router voor directe routing naar de webserver. Pakketten die overeenkomen met de lijst met omzeilingsinstellingen worden niet door de proxy verwerkt. De lijst kan IP-adressen of servernamen bevatten. De SWA lost elke 30 minuten elke items in de lijst met omzeilinstellingen op, ongeacht de TTL van de record. Als de L4TM-functie is ingeschakeld, kan de SWA echter gesnoopte DNS-vragen gebruiken om deze records vaker bij te werken. Dit vermindert het risico van een vals negatief in een scenario waarin de klant een ander adres dan de SWA heeft opgelost.

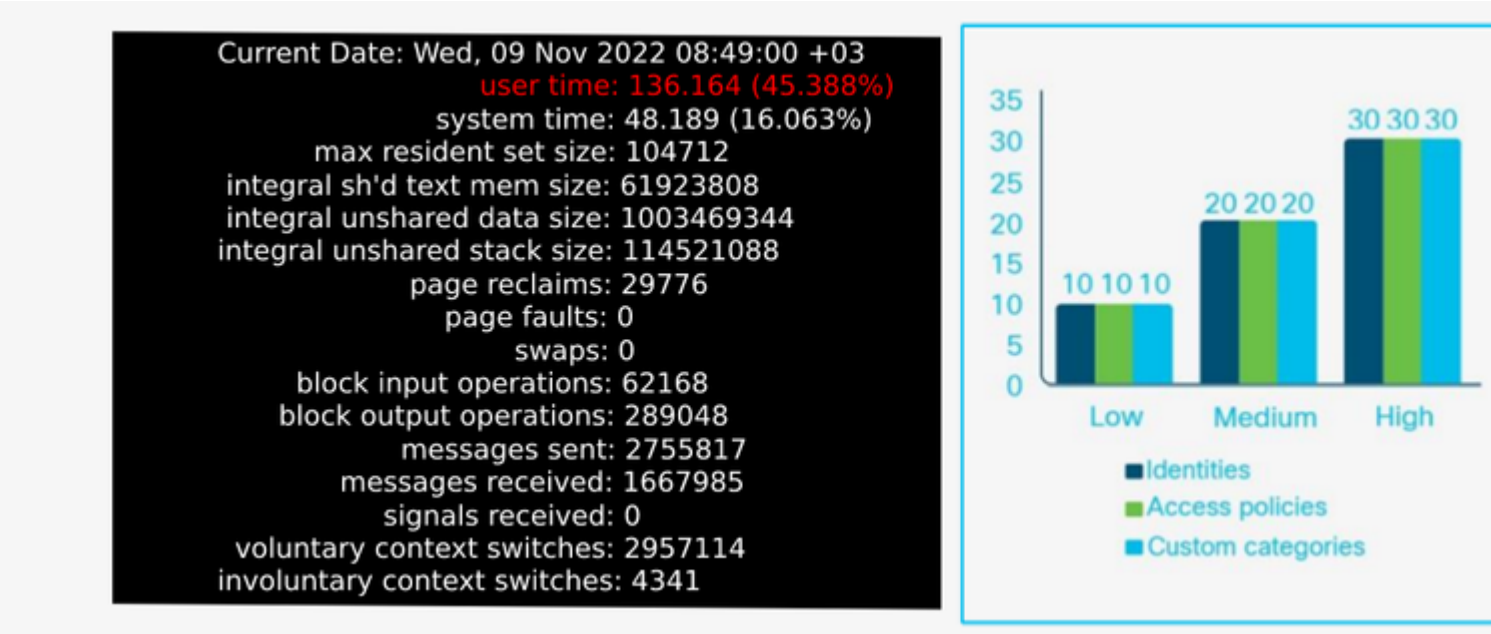
Beleidsconfiguratie

Correcte beleidsconfiguratie is van centraal belang voor de prestaties en schaalbaarheid van de SWA. Dit geldt niet alleen vanwege de effectiviteit van het beleid zelf in het beschermen van klanten en het afdwingen van bedrijfseisen. De manier waarop beleid wordt geconfigureerd heeft een directe invloed op het gebruik van hulpbronnen en de algehele gezondheid en prestaties van de SWA. Een te complexe of slecht ontworpen reeks beleidsregels kan instabiliteit en een langzame reactiesnelheid van het apparaat veroorzaken.

Complexiteit

Verschillende beleidselementen worden gebruikt bij de opbouw van het SWA-beleid. Het XML-bestand dat uit de configuratie wordt gegenereerd, wordt gebruikt om een aantal back-end configuratiebestanden en toegangsregels te maken. Hoe complexer de configuratie, hoe meer tijd het proxyproces moet besteden aan het evalueren van de verschillende regelsets voor elke transactie. Bij benchmarking en omvangbepaling van de SWA wordt een basisset van beleidselementen gecreëerd die drie niveaus van complexiteit van de

configuratie vertegenwoordigen. Tien identiteitsprofielen, decryptie beleid, en toegangsbeleid, samen met tien aangepaste categorieën die tien regex-vermeldingen, vijftig server IP-adressen, en 420 server hostnamen bevatten, wordt beschouwd als een Low Complexity configuratie. Het vermenigvuldigen van elk van deze cijfers met twee en drie resulteert in respectievelijk een configuratie met gemiddelde complexiteit en hoge complexiteit.
Wanneer een configuratie te complex wordt, omvatten de eerste symptomen gewoonlijk langzame reactie in de Webinterface en CLI. De gevolgen voor de gebruikers kunnen in eerste instantie niet groot zijn. Maar hoe complexer de configuratie is, hoe meer tijd het proxy proces moet besteden in de gebruikersmodus. Daarom kan het controleren van het percentage van de tijd die in deze modus wordt doorgebracht een handige manier zijn om een overmatig complexe configuratie te diagnosticeren als de oorzaak van een langzame SWA.
De CPU-tijd, in seconden, wordt elke vijf minuten ingelogd in het track_stats-log. Dit betekent dat het gebruikerstijdspercentage kan worden berekend als (gebruikerstijd + systeemtijd)/300. Aangezien de gebruikerstijd 270 nadert, besteedt het proces te veel CPU-cycli in gebruikersmodus, en dit is bijna altijd omdat de configuratie te complex is om efficiënt te worden geparseerd.

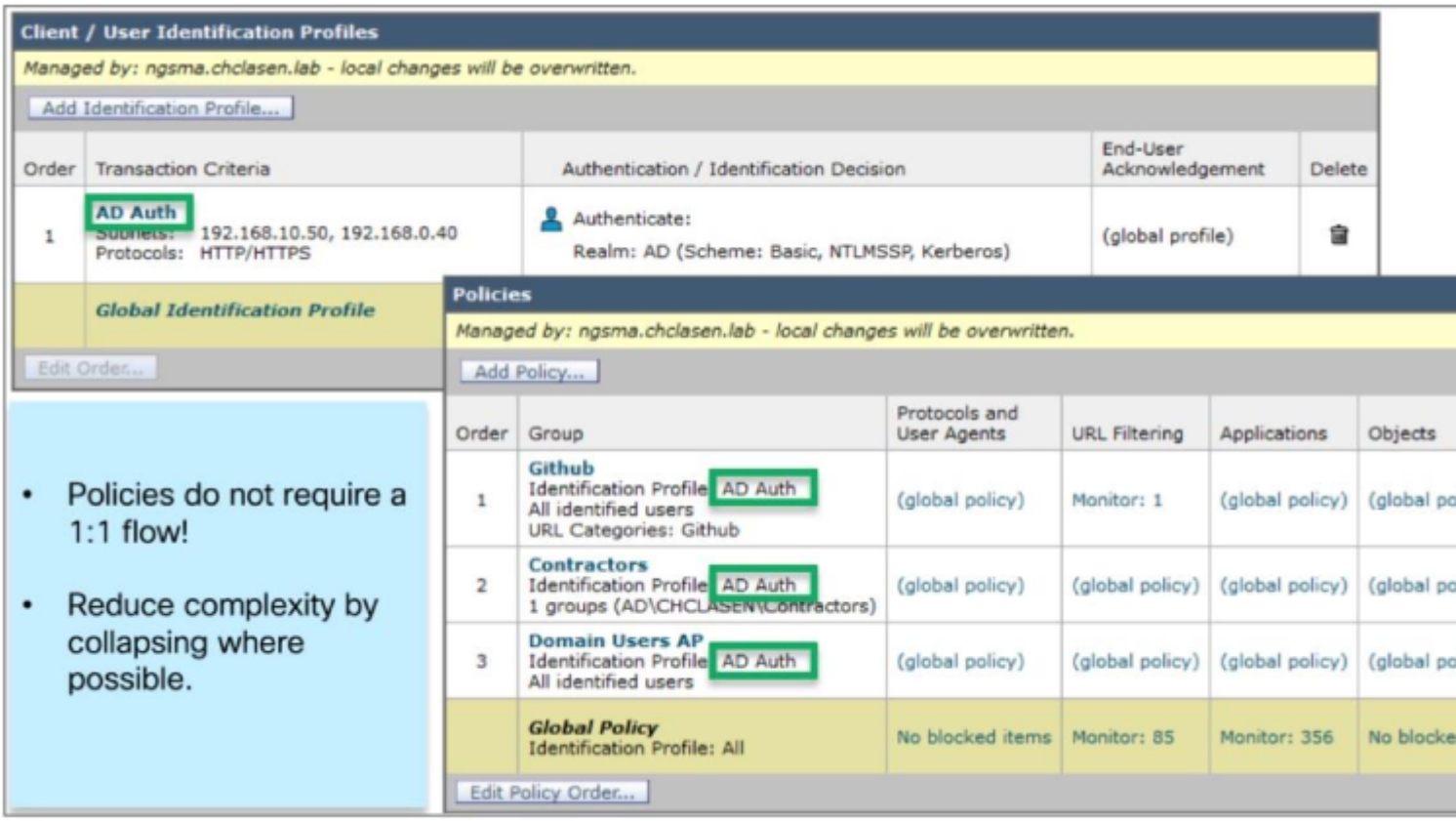


Identificatieprofielen

De Identificatie (ID) profielen zijn de eerste beleidselementen die worden beoordeeld wanneer een nieuw verzoek wordt ontvangen. Alle informatie die in de eerste sectie van het profiel van ID wordt gevormd wordt geëvalueerd met logische EN. Dit betekent dat alle criteria moeten overeenkomen voor het verzoek om het profiel te matchen. Bij het opstellen van een beleid mag het slechts zo specifiek zijn als absoluut noodzakelijk is. Profielen met afzonderlijke hostadressen zijn bijna nooit nodig en kunnen leiden tot uitdijende configuraties. Leveraging de gebruiker-agent string gevonden in de HTTP headers, aangepaste categorie lijst, of subnetnet is over het algemeen een betere strategie om de scope van een profiel te beperken.

Over het algemeen worden beleid dat verificatie vereist onderaan geconfigureerd en worden er bovenop uitzonderingen toegevoegd. Bij het bestellen van beleid dat geen authenticatie vereist, moet het meest gebruikte beleid zo dicht mogelijk bij de top liggen. Vertrouw niet op mislukte verificatie om de toegang te beperken. Als bekend is dat een client in het netwerk niet kan worden geverifieerd bij een proxy, moet deze worden vrijgesteld van verificatie en worden geblokkeerd in het toegangsbeleid. Clients die niet herhaaldelijk kunnen verifiëren sturen niet-geverifieerde aanvragen naar de SWA, die resources gebruiken en buitensporige CPU- en geheugengebruik kunnen veroorzaken.

Een veel voorkomend misverstand voor beheerders is dat er een uniek ID-profiel en een bijbehorende decryptie- en toegangsbeleid moet zijn. Dit is een inefficiënte strategie voor de beleidsvorming. Indien mogelijk moet het beleid "samengevouwen" worden, zodat één ID-profiel kan worden gekoppeld aan meerdere vormen van decryptie en toegangsbeleid. Dit is mogelijk omdat alle criteria in een bepaald beleid moeten overeenkomen om verkeer aan het beleid te kunnen aanpassen. Meer algemeen in het authenticatiebeleid en specifieker in het resulterende beleid maakt minder beleid als geheel mogelijk.



Decryptie-beleid

Net als bij het ID-profiel worden de criteria die in het decryptie-beleid zijn vastgesteld, ook als logische EN beoordeeld, met één belangrijke uitzondering wanneer informatie van de ISE wordt gebruikt. Hier is hoe beleidsaanpassing werkt, afhankelijk van welke elementen zijn geconfigureerd (AD-groep, gebruiker of SGT):

- AD-groepen en gebruikers - Geen wijziging in eerder gedrag; het beleid wordt aangepast als de gebruiker een lid van de groep is, OF de gebruiker wordt gespecificeerd in het beleid.
- SGT- en AD-groepen en gebruikersâ€”Het beleid wordt afgestemd als de gebruiker is gekoppeld aan de SGT EN lid is van de AD-groep, OF de gebruiker wordt gespecificeerd in het beleid.
- SGT en gebruiker-het beleid aangepast als de gebruiker met SGT wordt geassocieerd of de gebruiker in het beleid wordt gespecificeerd.

Van alle door de SWA verrichte diensten is de evaluatie van HTTPS-verkeer vanuit prestatieoogpunt het meest significant. Het percentage ontsleuteld verkeer heeft een directe invloed op de grootte van het apparaat. Een beheerder kan rekenen op ten minste 75% van het webverkeer als HTTPS.

Na de eerste installatie moet het percentage gedecrypteerd verkeer worden bepaald om er zeker van te zijn dat de verwachtingen voor de toekomstige groei nauwkeurig zijn ingesteld. Na de inzet moet dit aantal eens per kwartaal worden gecontroleerd. Het vinden van het percentage van HTTPS-verkeer dat door de SWA is gedecodeerd, is eenvoudig te doen met een kopie van de access_logs, zelfs zonder extra

logboekbeheersoftware. U kunt eenvoudige Bash- of PowerShell-opdrachten gebruiken om dit nummer te verkrijgen. Hier zijn de stappen die voor elke omgeving worden beschreven:

1. Vind het aantal totale HTTPS-verbindingen (zowel expliciet als transparant):

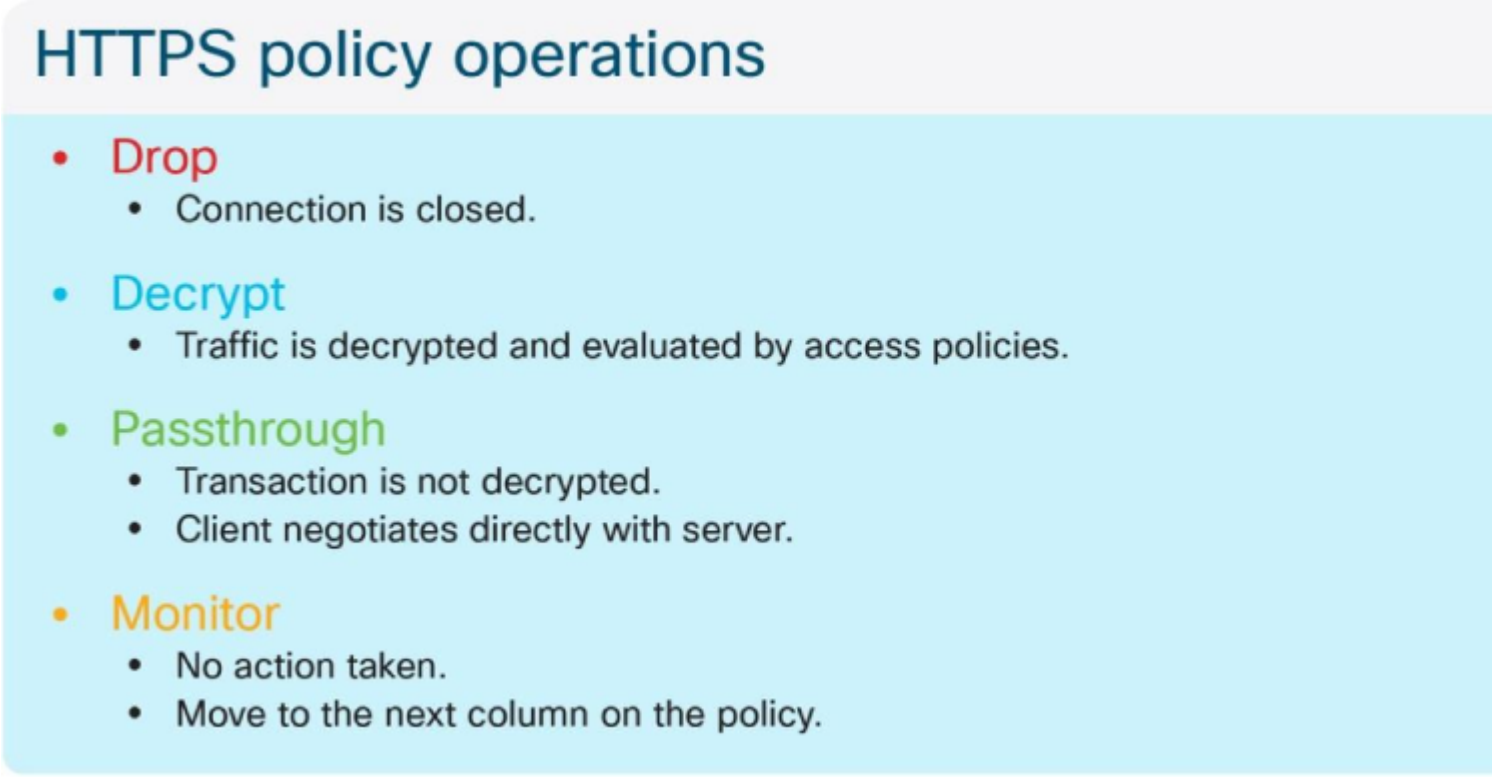
```
Bash:
grep -cE 'tunnel://|TCP_CONNECT' aclog.current

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

2. Vind het aantal gedecrypteerde HTTPS-verbindingen:

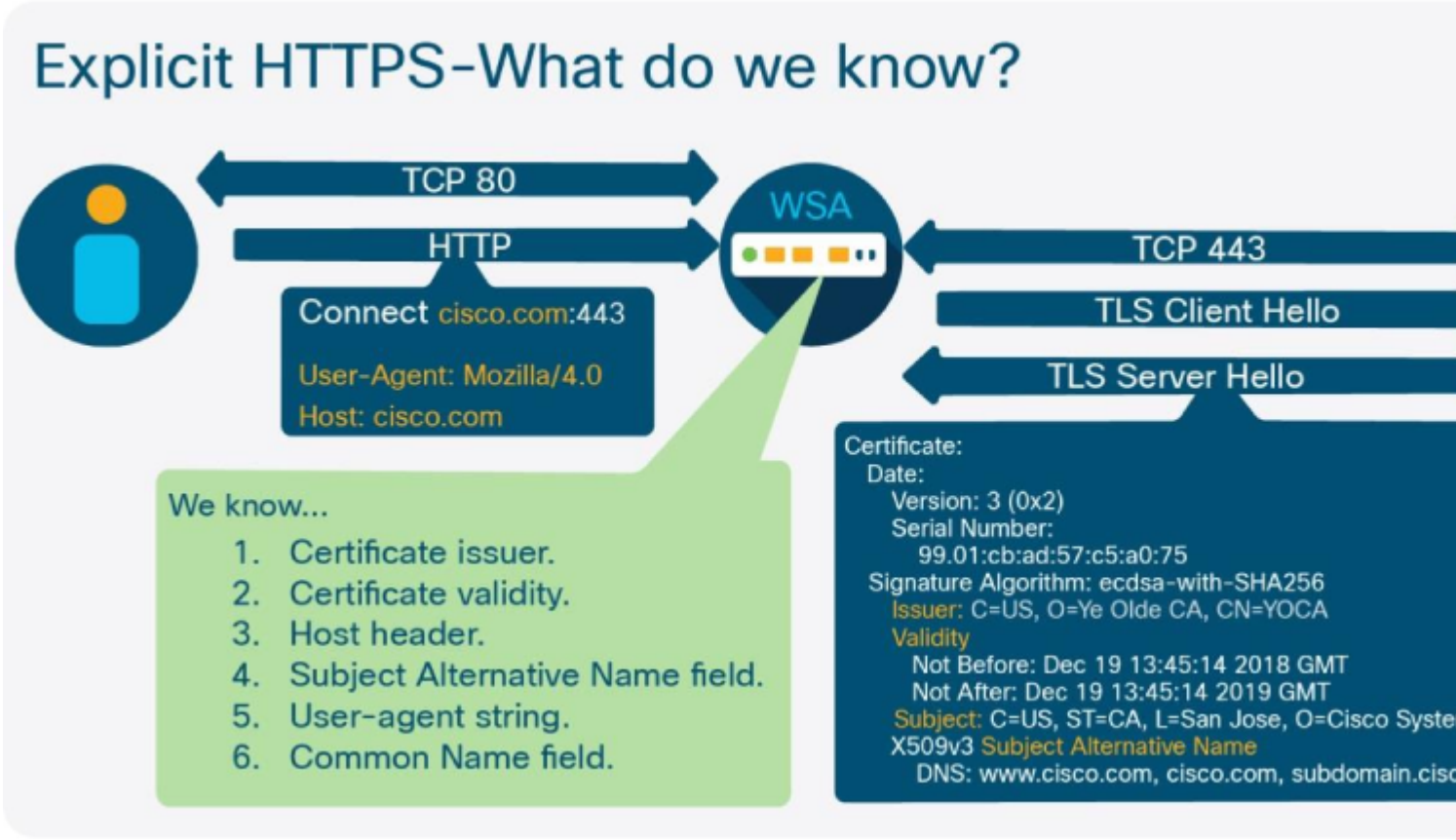
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECTâ€™| Select-String -Pattern â€
```

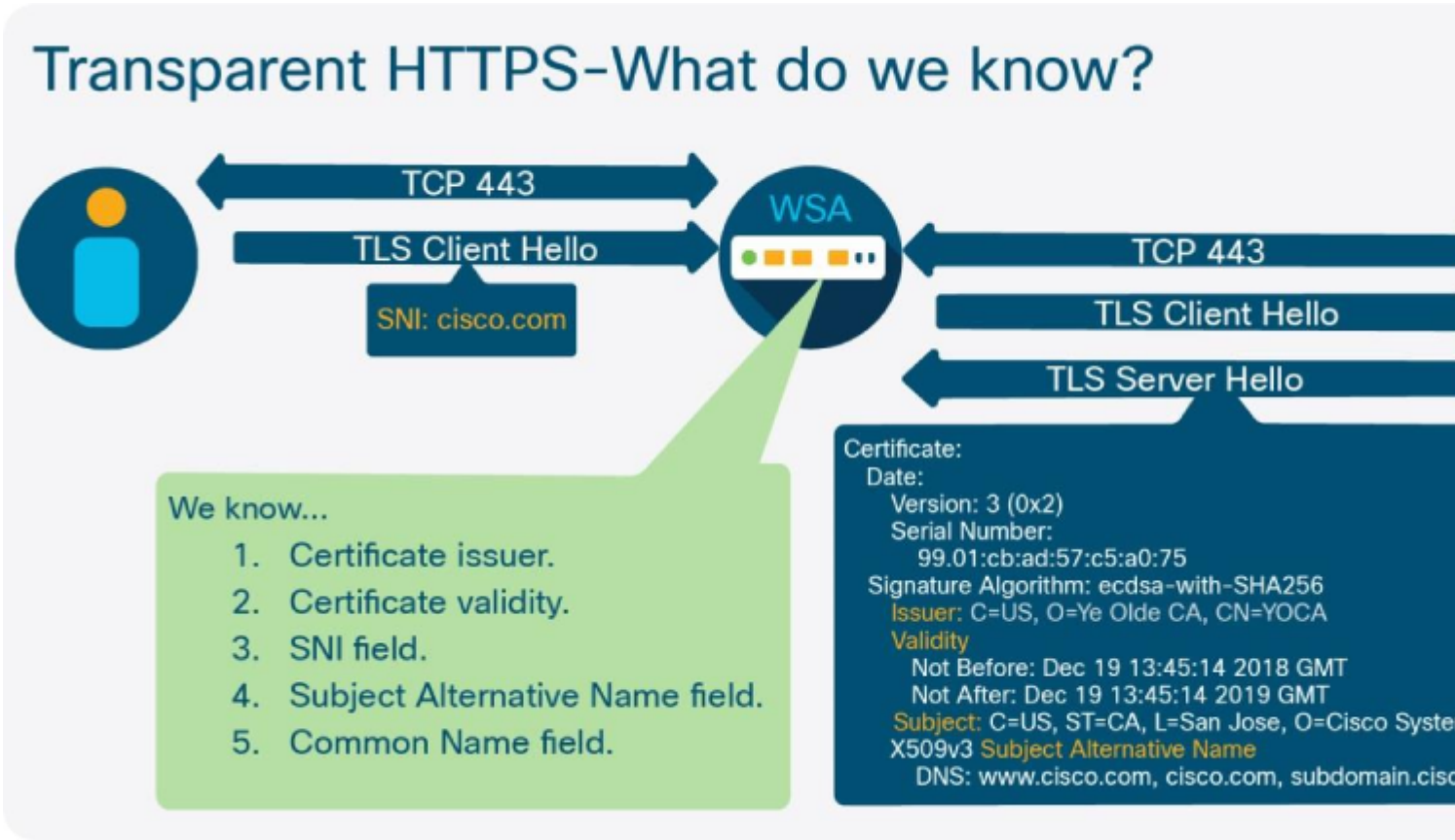
3. Verdeel de tweede waarde door de eerste waarde en vermenigvuldig met 100.

Bij het ontwerpen van decryptie beleid, is het belangrijk om te begrijpen hoe de diverse acties die in het beleid worden vermeld het apparaat veroorzaken om verbindingen te evalueren HTTPS. De passthrough-actie wordt gebruikt wanneer de client en server elk einde van hun TLS-sessie moeten kunnen afsluiten zonder dat de SWA elk pakket hoeft te decoderen. Zelfs als een site is ingesteld op passthrough, moet de SWA nog steeds worden verplicht om één TLS-handdruk met de server te voltooien. Dit komt doordat de SWA ervoor moet kiezen om een verbinding te blokkeren op basis van de geldigheid van het certificaat en een TLS-verbinding met de server moet starten om het certificaat te verkrijgen. Als het certificaat geldig is, sluit de SWA de verbinding en stelt de client in staat om de sessie rechtstreeks met de server uit te voeren.



Het enige geval waarin de SWA geen TLS-handdruk uitvoert, is wanneer de servernaam of het IP-adres aanwezig is in een aangepaste categorie, die is ingesteld op passthrough, en de servernaam beschikbaar is in een HTTP CONNECT of TLS-client Hello. In een expliciet scenario, de client levert de hostnaam van de server aan de proxy voorafgaand aan de TLS sessie initiatie (in de host header), dus dit veld wordt gecontroleerd aan de aangepaste categorie. In een transparante implementatie controleert de SWA het veld **Server Name Indication (SNI)** in het TLS Client Hello-bericht en evalueert het met de aangepaste categorie. Als de hostheader of SNI niet aanwezig is, moet de SWA de handdruk met de server voortzetten om de velden **Onderwerp Alternatieve Naam (SAN)** en **Gemeenschappelijke Naam (CN)** op het certificaat in die volgorde te controleren.
Wat dit gedrag betekent voor beleidsontwerp is dat het aantal TLS handdrukken kan worden verminderd door bekende en intern vertrouwde servers te bepalen en hen te plaatsen om door te gaan van de lijst van de douanecategorie, in plaats van te vertrouwen op de score van de Webcategorie en van de reputatie, die SWA nog vereisen om een TLS handdruk met de server te voltooien. Het is echter belangrijk op te merken dat dit ook controles van de geldigheid van certificaten onmogelijk maakt.





De snelheid waarmee nieuwe sites op internet verschijnen, is waarschijnlijk een aantal sites die niet gecategoriseerd zijn door de webreputatie- en categorisatiedatabanken die door de SWA worden gebruikt. Dit geeft niet aan dat de site noodzakelijkerwijs meer kans op kwaadaardige, en bovendien nog al deze sites worden onderworpen aan AV-scanning, AMP-bestandsreputatie en analyse, en elke object blokkering of scanning die is geconfigureerd. Om deze redenen wordt het niet aangeraden om niet-gecategoriseerde

plaatsen in de meeste omstandigheden te laten vallen. Het is het beste om ze te decoderen en scannen door de AV-motoren en te evalueren door AVC, AMP, toegangsbeleid, enzovoort. Er is meer informatie over ongecategoriseerde sites in de sectie **Toegangsbeleid**.

Toegangsbeleid

Net als bij het ID-profiel worden de criteria die in het decryptie-beleid zijn vastgesteld, ook als logisch EN met één belangrijke uitzondering beoordeeld wanneer informatie van de ISE wordt gebruikt. Het beleid-aanpassende gedrag wordt daarna verklaard, gebaseerd op welke elementen worden gevormd (de groep van de AD, gebruiker, of SGT):

- AD-groepen en gebruikers - Geen wijziging in eerder gedrag; het beleid wordt aangepast als de gebruiker een lid van de groep is, OF de gebruiker wordt gespecificeerd in het beleid.
- SGT- en AD-groepen en gebruikersâ€"Het beleid dat wordt afgestemd als de gebruiker is gekoppeld aan de SGT EN lid is van de AD-groep, OF de gebruiker is gespecificeerd in het beleid.
- SGT en gebruiker-het beleid aangepast als de gebruiker met SGT wordt geassocieerd OF de gebruiker in het beleid wordt gespecificeerd.

HTTP-verkeer wordt direct na verificatie geevalueerd met behulp van het toegangsbeleid. HTTPS-verkeer wordt geëvalueerd na te zijn geauthenticeerd en als de decrypt-actie wordt toegepast per het overeenkomende decryptie-beleid. Voor gedecrypteerde verzoeken, zijn er twee access_log vermeldingen. De eerste logingang toont de actie die op de aanvankelijke verbinding van TLS wordt toegepast (decrypt), en een tweede logboekingang toont de actie die door het toegangsbeleid op het gedecrypteerde HTTP-verzoek wordt toegepast.
Zoals uitgelegd in **Web Proxy** sectie bereik verzoek headers worden gebruikt om een specifieke byte bereik van een bestand aan te vragen en worden vaak gebruikt door OS en applicatie update services. De SWA, standaard, verwijderen deze kopregels van uitgaande verzoeken, omdat zonder het gehele bestand, het onmogelijk is om malware scannen uit te voeren of AVC-functies te gebruiken. Als veel hosts op het netwerk vaak om kleine byte bereiken vragen om updates op te halen, kan dit de SWA activeren om het gehele bestand meerdere malen tegelijk te downloaden. Dit kan snel de beschikbare internetbandbreedte uitputten en servicestoringen veroorzaken. De meest voorkomende oorzaken van dit storingsscenario zijn Microsoft Windows update en Adobe software update daemons.
Om dit te verzachten is de beste oplossing om dit verkeer helemaal rond de SWA te sturen. Dit is niet altijd haalbaar voor transparant geïmplementeerde omgevingen, en in deze gevallen is de volgende beste optie om specifiek toegangsbeleid voor het verkeer te maken en het doorsturen van een bereik-aanvraag op dat beleid mogelijk te maken. Er moet rekening mee worden gehouden dat AV-scanning en AVC niet mogelijk zijn voor deze verzoeken, en daarom moet het beleid zorgvuldig worden ontworpen om alleen het beoogde verkeer te sturen. Vaak, de beste manier om dit te bereiken is door de user-agent string in de request header aan te passen. De gebruiker-agent string voor gemeenschappelijke update daemons kan online gevonden worden, of de verzoeken kunnen door een beheerder worden opgenomen en onderzocht. De meeste updateservices, waaronder Microsoft Windows update en Adobe software updates, maken geen gebruik van HTTPS.
Zoals wordt beschreven in de sectie **Decryptie Beleid**, is het niet aan te raden om ongecategoriseerde sites te laten vallen in het decryptie beleid. Om dezelfde redenen wordt het niet aangeraden om deze te blokkeren in het toegangsbeleid. De Dynamic Content Analysis (DCA) engine kan de inhoud van een bepaalde site gebruiken, samen met andere heuristische gegevens naar gecategoriseerde sites die anders worden gemarkeerd door het zoeken naar URL-databases. Als u deze functie inschakelt, wordt het aantal niet-gecategoriseerde vonnissen in de SWA verminderd.
In de instellingen Objectscanning van een toegangsbeleid is er de mogelijkheid om verschillende soorten archiefbestanden te inspecteren. Als het netwerk regelmatig archiefbestanden downloadt als onderdeel van applicatieupdates, kan dit het CPU-gebruik aanzienlijk verhogen. Dit verkeer moet van tevoren worden geïdentificeerd en vrijgesteld als het de bedoeling is om alle archiefbestanden te inspecteren. De eerste plaats om mogelijke methodes te onderzoeken om dit verkeer te identificeren is het gebruiker-agent koord, aangezien dit kan helpen IP toegestane lijsten vermijden die omslachtig kunnen worden om te handhaven.

Aangepaste en externe URL-categorieën

De Aangepaste categorielijsten worden gebruikt om een server te identificeren op IP-adres of hostnaam. Het is mogelijk om reguliere expressies (regex) te gebruiken om patronen op te geven waarmee servernamen kunnen worden gekoppeld. Het is veel meer resource-intensief om een regex patroon te gebruiken om een servernaam aan te passen dan het is om een substring match te gebruiken, en dus moeten ze alleen worden gebruikt wanneer absoluut noodzakelijk. Een "." kan worden toegevoegd aan het begin van een domeinnaam om een subdomein te matchen zonder de noodzaak voor regex. Bijvoorbeeld, ".cisco.com" komt ook overeen met "www.cisco.com."
Zoals uitgelegd in de sectie **Complexiteit**, wordt de lage complexiteit gedefinieerd als tien aangepaste categorielijsten, de gemiddelde complexiteit als twintig, en de hoge complexiteit als dertig. Het wordt aanbevolen dit nummer onder twintig te houden, vooral als de lijsten regexpatronen gebruiken of een groot aantal vermeldingen bevatten. Verwijs naar de sectie **Toegangsbeleid** voor extra details over het aantal ingangen voor elk type.
Externe URL-feeds zijn veel flexibeler dan statische douanecategorielijsten en het gebruik ervan kan een directe invloed hebben op de beveiliging omdat ze de noodzaak voor een beheerder om ze handmatig te onderhouden, verwijderen. Omdat deze functie kan worden gebruikt om lijsten op te halen die niet worden onderhouden of gecontroleerd door de SWA-beheerder, werd de mogelijkheid om individuele uitzonderingen toe te voegen aan de gedownloade adressen toegevoegd in AsyncOS versie 11.8.
De Office365 API is vooral nuttig om beleidsbeslissingen te nemen over deze algemeen geïmplementeerde service en kan worden gebruikt voor individuele toepassingen (PowerPoint, Skype, Word, enzovoort). Microsoft adviseert proxies te omzeilen voor alle Office365 verkeer om de prestaties te optimaliseren. Microsoft documentatie stelt:
"Terwijl SSL Break en Inspect tot de grootste latentie leidt, kunnen andere diensten zoals volmachtsauthentificatie en reputatieschakeling slechte prestaties en een slechte gebruikerservaring veroorzaken. Bovendien hebben deze perimeternetwerkapparaten voldoende capaciteit nodig om alle netwerkverbindingsverzoeken te verwerken. We raden aan om uw proxy- of inspectieapparaten te omzeilen voor directe Office 365-netwerkverzoeken."https://learn.microsoft.com/en-us/microsoft-365/enterprise/managing-office-365-endpoints?view=o365-worldwide .

Het kan moeilijk zijn deze leidraad te gebruiken in een transparante proxyomgeving. Beginnend in AsyncOS versie 11.8, is het mogelijk om de dynamische categorielijst te gebruiken die van Office365 API wordt teruggewonnen om de lijst van omzeilingsinstellingen te bevolken. Deze lijst wordt gebruikt om transparant doorgestuurd verkeer terug naar het WCCP-apparaat te sturen voor directe routing.
Door alle Office365-verkeer te omzeilen, ontstaat een blinde vlek voor beheerders die enige basisbeveiligingscontroles en rapportage voor dit verkeer nodig hebben. Als Office365-verkeer niet wordt omzeild door de SWA, is het belangrijk om de specifieke technische uitdagingen te begrijpen die zich kunnen voordoen. Eén daarvan is het aantal verbindingen dat nodig is voor de toepassingen. De grootte moet op de juiste manier worden aangepast om de extra persistente TCP-verbindingen aan te kunnen die Office365-applicaties nodig hebben. Dit kan het totale aantal verbindingen verhogen met tussen tien en vijftien persistente TCP-sessies per gebruiker.
De decrypt en re-encrypt acties die door de volmacht HTTPS worden uitgevoerd introduceren een kleine hoeveelheid latentie aan de verbindingen. Office365-toepassingen kunnen zeer gevoelig zijn voor latentie en als andere factoren zoals langzame WAN-verbinding en ongelijke geografische locatie dit samenstellen, kan de gebruikerservaring lijden.
Sommige Office365-toepassingen maken gebruik van eigen TLS-parameters die voorkomen dat de HTTPS-proxy een handdruk met de toepassingsserver uitvoert. Dit is vereist om het certificaat te valideren of de hostnaam op te halen. Wanneer dit wordt gecombineerd met een toepassing zoals Skype voor Bedrijven die geen **Server Name Indication (SNI)**-veld verstuurt in het TLS Client Hello-bericht, wordt het noodzakelijk om dit verkeer volledig te omzeilen. AsyncOS 11.8 heeft de mogelijkheid geïntroduceerd om verkeer te omzeilen alleen gebaseerd op IP-adres van bestemming, zonder certificaatcontroles om dit scenario te adresseren.

Monitoren en meldingen

CLI-monitoren

De SWA CLI biedt opdrachten voor real-time bewaking van belangrijke processen. Het nuttigst zijn de bevelen die statistieken met betrekking tot het proxproces tonen. De opdracht **statusdetail** is een goede bron voor een samenvatting van het gebruik van bronnen en prestatiegegevens, omvat uptime, gebruikte bandbreedte, responslatentie, aantal verbindingen en meer. Hier is voorbeelduitvoer van deze opdracht:

```
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
```

De **snelheidsopdracht** toont real-time informatie over het percentage van de CPU dat wordt gebruikt door het proxproces, evenals het aantal aanvragen per seconde (RPS) en cachestatistieken. Deze opdracht blijft nieuwe uitvoer opvragen en weergeven tot deze wordt onderbroken. Dit is een voorbeeld van uitvoer van deze opdracht:

```
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
```

De opdracht **tcpservices** geeft informatie weer over de geselecteerde poorten voor procesluisteren. Er wordt ook een verklaring weergegeven voor elk proces en voor de adres- en poortcombinatie:

```
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
```

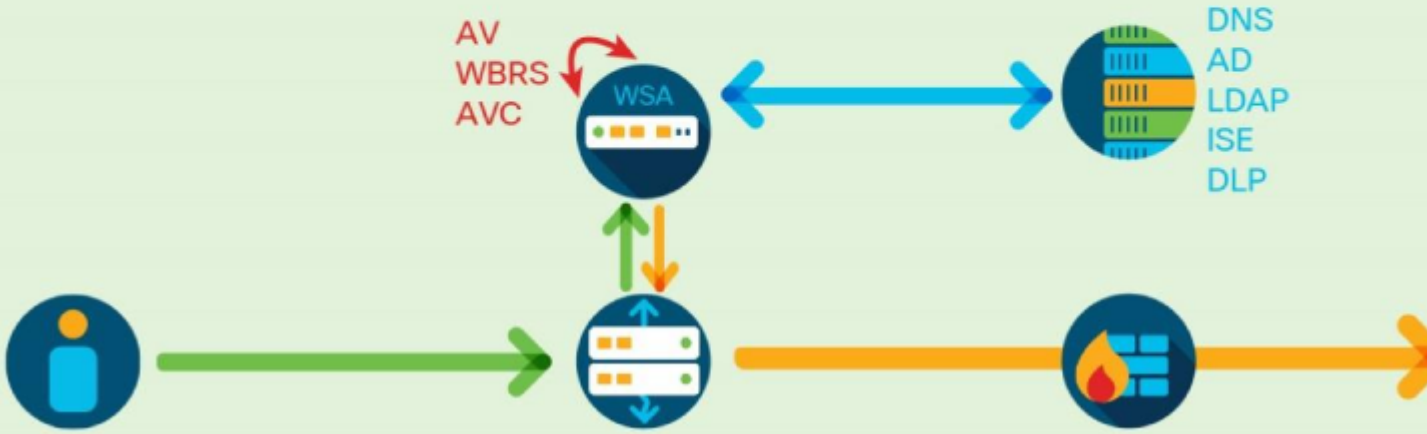
Vastlegging

Webverkeer is zeer dynamisch en gevarieerd. Nadat de implementatie van een proxy is voltooid, is het belangrijk om regelmatig de hoeveelheid en samenstelling van het verkeer dat via het apparaat wordt doorgegeven opnieuw te beoordelen. U moet het percentage gedecrypteerd verkeer op een regelmatige basis (eens per kwartaal) controleren om te verzekeren de grootte met de verwachtingen en de specificaties van de aanvankelijke installatie verenigbaar is. Dit kan worden gedaan met een logboekbeheerproduct zoals **Advanced Web Security Reporting (AWSR)** of met eenvoudige Bash- of PowerShell-opdrachten met de toegangslogboeken. Het aantal RPS moet ook regelmatig opnieuw worden beoordeeld om ervoor te zorgen dat het apparaat voldoende overhead heeft om rekening te houden met pieken in het verkeer en mogelijke failover in een configuratie met hoge beschikbaarheid en taakverdeling.

Het track_stats log wordt elke vijf minuten toegevoegd en bevat verschillende delen van output die direct gerelateerd zijn aan het prox proces en de objecten in het geheugen. Het nuttigst in prestatiescontrole zijn de secties die de gemiddelde latentie voor diverse verzoekprocessen tonen, DNS raadplegingstijd, AV de tijd van het motoraftasten, en veel nuttiger gebieden omvatten. Dit logbestand kan niet worden geconfigureerd vanuit de GUI of de CLI en is alleen toegankelijk via Secure Copy Protocol (SCP) of File Transfer Protocol (FTP). Dit is het belangrijkste logboek om te hebben wanneer de prestaties van het probleemoplossing zodat het vaak moet worden onderzocht.

Where can latency be introduced?

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

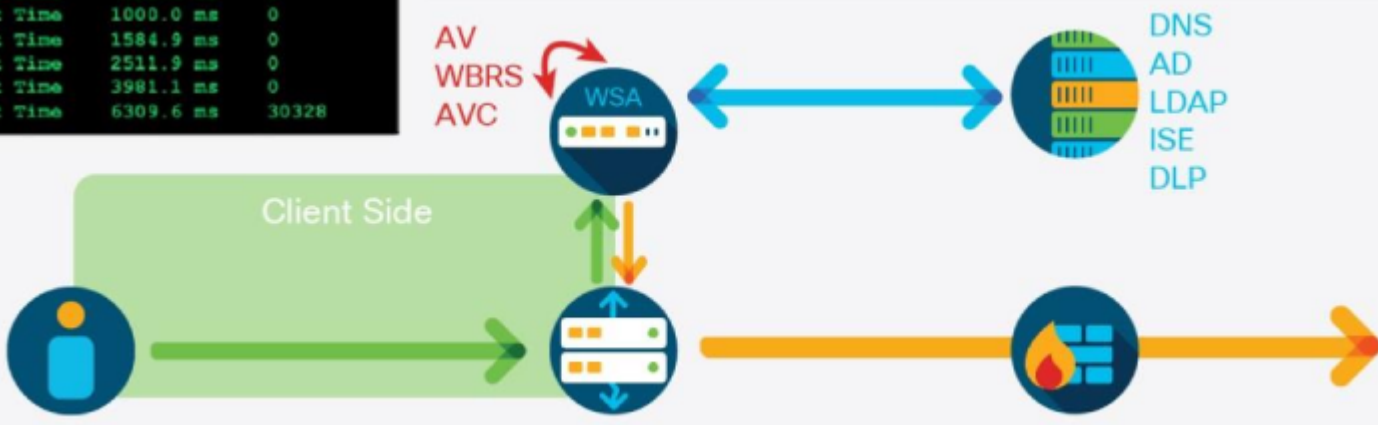


Client side latency

```
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 wa response.
- May indicate an upstream issues-keep investigating!
- Access logs can show this in custom field **% : 1>**

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

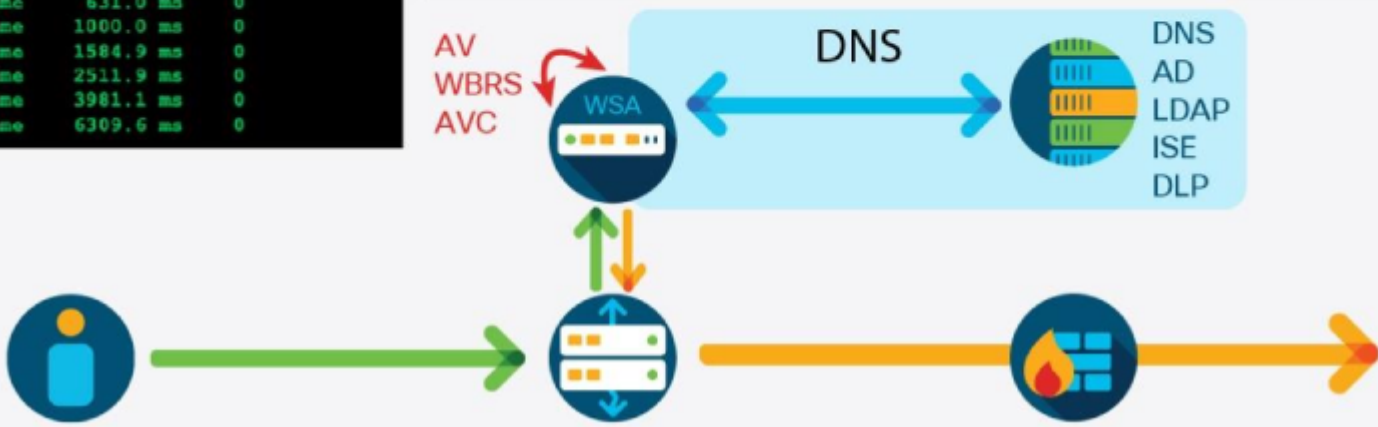


DNS latency

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

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

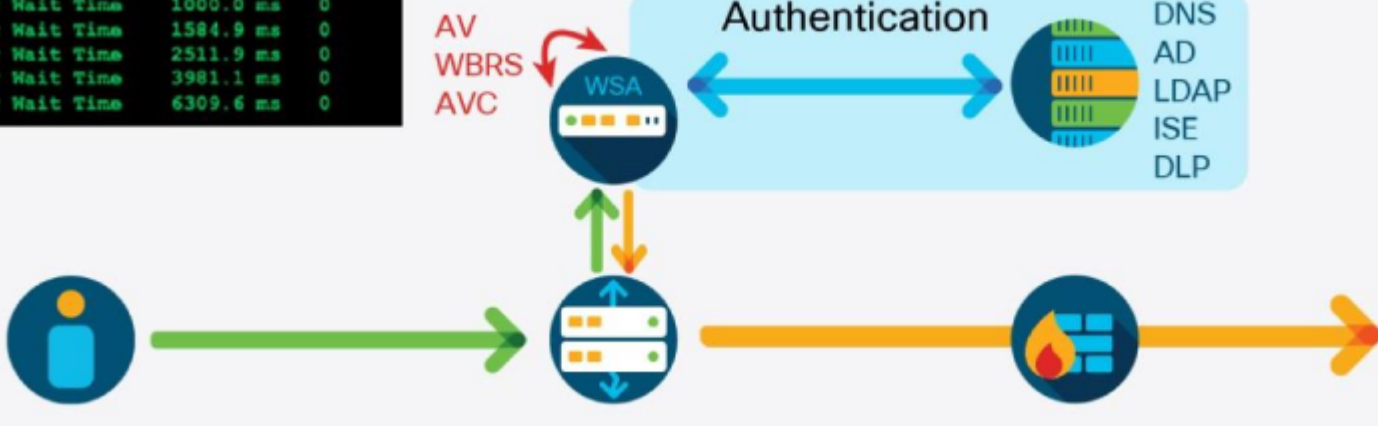


Authentication latency

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

%:<a	x-p2p-auth-wait-time	Wait-time to receive the respo Web Proxy authentication proc Web Proxy sent the request.

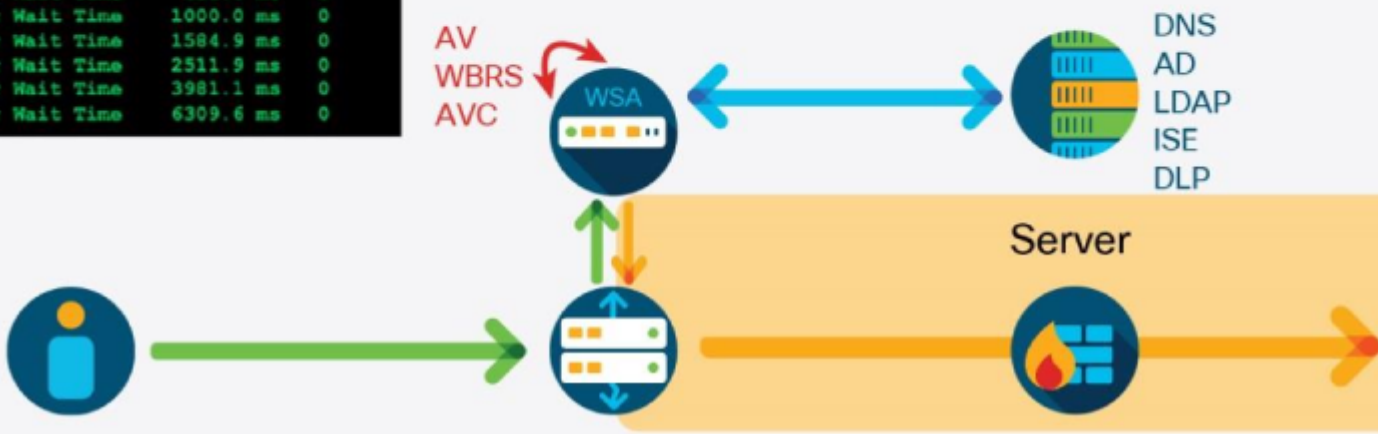


Server latency-wait time

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 byte of the server response.
- Calls for investigation of your upstream devices and WAN
- **access logs** can show this in custom field **% : >1**

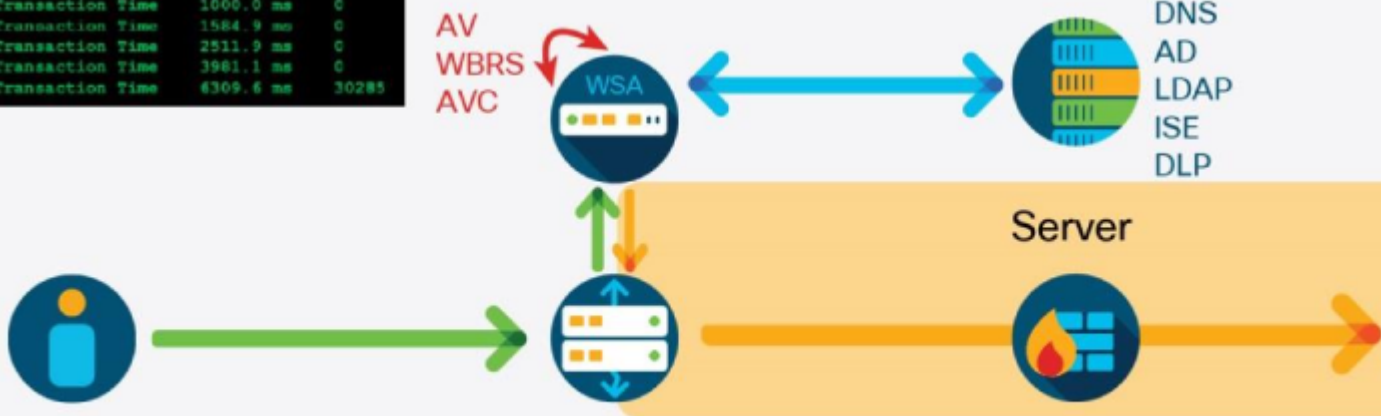
%:>1	x-s2p-first-byte-time	Wait-time for first response by

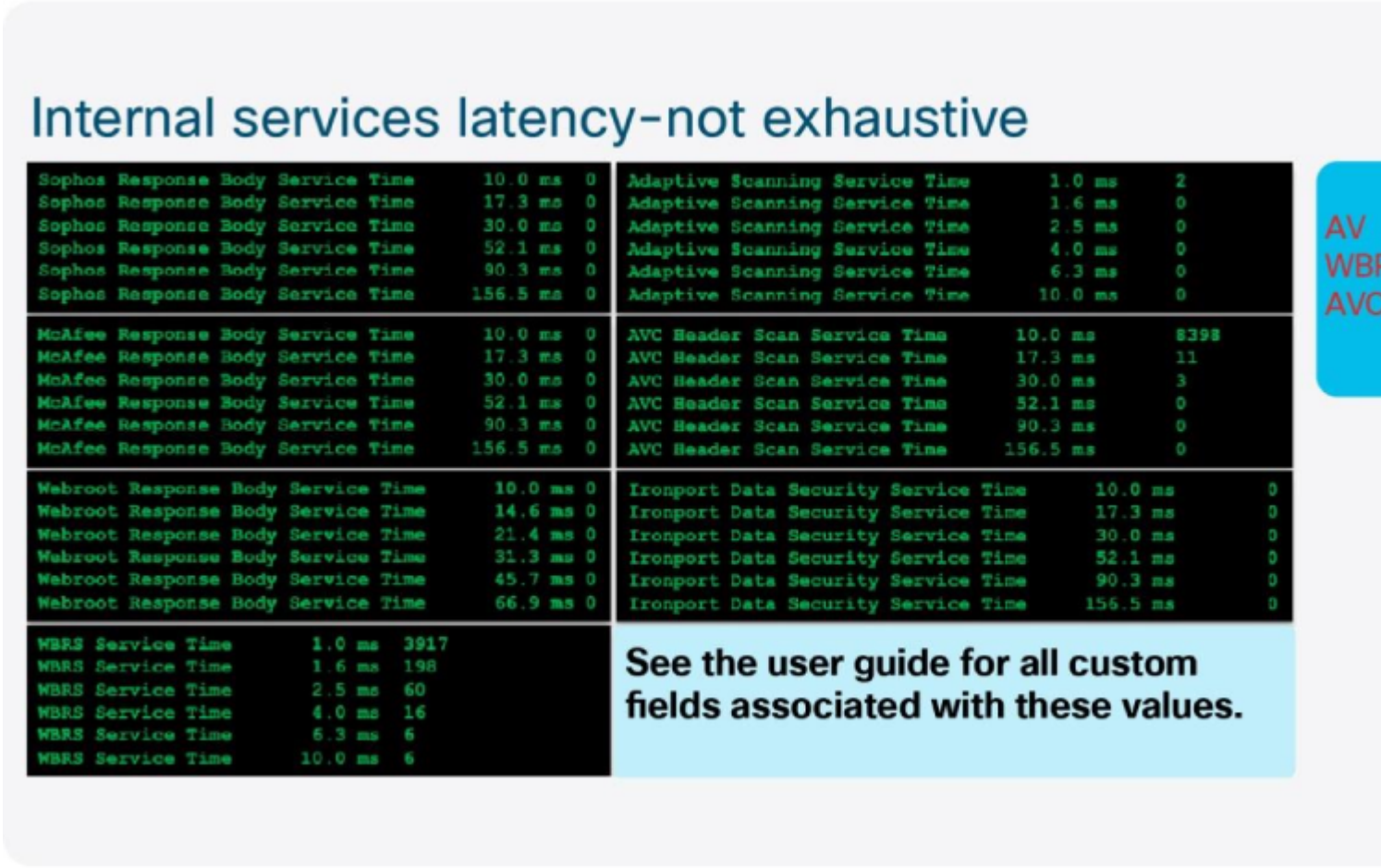


Server latency-transaction time

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	8097
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-s transaction to complete.
- Calls for investigation of your upstream devices and WAN
- No **access logs** custom field, but can be determined by a combinationof them.





Elke 60 seconden wordt er een aparte SHD-logregel geschreven die veel velden bevat die belangrijk zijn voor prestatiebewaking, waaronder latency, RPS en totale client-side en server-side verbindingen. Dit is een voorbeeld van een SHD-logregel:

```
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
```

Er kunnen extra aangepaste velden worden toegevoegd aan de access_logs die latency informatie voor individuele verzoeken aanduiden. Deze velden zijn onder andere serverrespons, DNS-resolutie en AV-scannerlatentie. De velden moeten aan het logbestand worden toegevoegd om waardevolle informatie te verzamelen die kan worden gebruikt voor probleemoplossing. Dit is de aanbevolen aangepaste veldstring voor gebruik:

```
[ 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,
```

De uit deze waarden afgeleide prestatiegegevens zijn als volgt:

Aangepast veld	**Beschrijving**
%:<a	Wacht tijd om de reactie van het proces van de Webvolmachtsauthentificatie te ontvangen, nadat de Volmacht van het Web het verzoek verzond.
%:<b	Wacht op tijd om aanvraagformulier naar server na header te schrijven.
%:<d	Wacht tijd om de reactie van het webproxy DNS proces te ontvangen, nadat de webproxy het verzoek heeft verzonden.
%:<h	Wacht met het schrijven van de header van de aanvraag naar de server na de eerste byte.

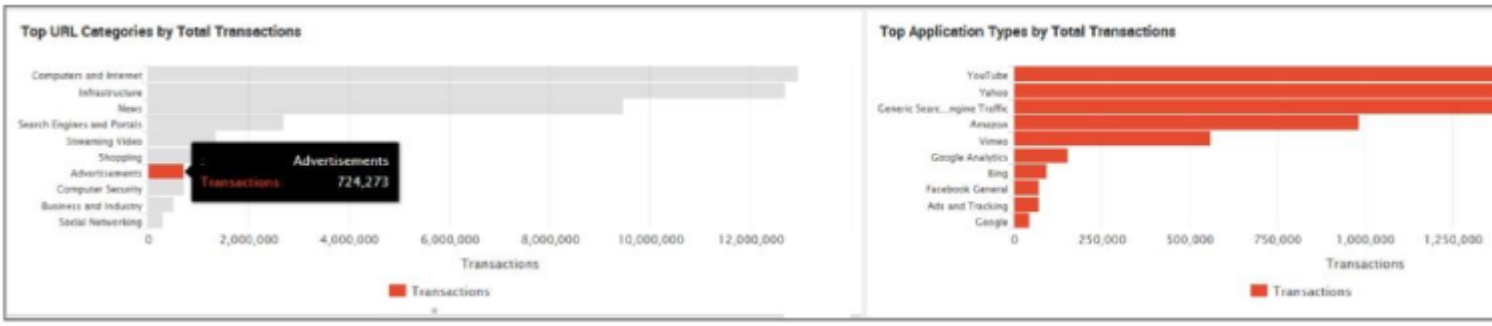
%:<r	Wacht tijd om de reactie van de web reputatie filters te ontvangen, nadat de web proxy het verzoek heeft verzonden.
%:<s	Wacht tijd om de uitspraak van het web proxy antispyware proces te ontvangen, nadat de web proxy het verzoek heeft verzonden.
%:>	Wacht op de eerste reactiebyte van de server.
%>a	Wacht tijd om de reactie van het web proxy authenticatie proces te ontvangen, omvat de tijd die nodig is voor de web proxy om het verzoek te verzenden.
%:>b	Wacht op volledige respons lichaam na ontvangen header.
%>c	Tijd die de webproxy nodig heeft om een reactie van het schijfcachegeheugen te lezen.
%>d	Wacht tijd om de reactie van het web proxy DNS proces te ontvangen, omvat de tijd die nodig is voor de web proxy om het verzoek te verzenden.
%>h	Wacht op de kop van de server na de eerste antwoordbyte.
%>r	Wacht tijd om het oordeel van de web reputatie filters te ontvangen, inclusief de tijd die nodig is voor de web proxy om het verzoek te verzenden.
%:>s	Wacht tijd om het vonnis van het web proxy antispyware proces te ontvangen, omvat de tijd die nodig is voor de web proxy om het verzoek te verzenden.
%:1<	Wacht tijd op eerste aanvraag byte van nieuwe client verbinding.
%:1>	Wacht tijd op de eerste byte die naar de client is geschreven.
%:b<	Wacht op de volledige cliëntgegevens.
%:b>	Wacht tijd op de volledige carrosserie geschreven naar client.
%:e>	Wacht tijd om de reactie van de AMP scanning engine te ontvangen, nadat web proxy het verzoek heeft verzonden.
%:e<	Wacht tijd om het vonnis van de AMP-scanengine te ontvangen, inclusief de tijd die de webproxy nodig heeft om het verzoek te verzenden.
%:h<	Wacht na de eerste byte op de volledige kop van de client.
%:h>	Wacht tijd op de volledige header die is geschreven naar client.
%:m<	Wacht tijd om het vonnis van de McAfee scanning engine te ontvangen, inclusief de tijd die de web proxy nodig heeft om het verzoek te verzenden.
%:m>	Wacht met het ontvangen van de reactie van de McAfee scanning engine, nadat de web proxy het verzoek heeft verzonden.
%f	Clientbronpoort.
%p	Webserverpoort.
%k	IP-adres voor gegevensbronnen (IP-adres van webserver).
%:w<	Wacht tijd om het vonnis van de Webroot scanengine te ontvangen, inclusief de tijd die de webproxy nodig heeft om het verzoek te verzenden.
%:w>	Wacht tijd om de reactie van de Webroot scanning engine te ontvangen, nadat de web proxy het verzoek heeft verzonden.

Het SWA-licentiemodel maakt hergebruik van licenties voor fysieke apparaten voor virtuele apparaten mogelijk. U kunt hiervan profiteren en test SWAv-toestellen implementeren voor gebruik in een

labomgeving. Nieuwe functies en configuraties kunnen op deze manier worden beproefd om stabiliteit en betrouwbaarheid te garanderen zonder dat de licentievoorwaarden worden geschonden.

Geavanceerde Web Security Rapportage (AWSR)

AWSR moet worden benut om optimaal gebruik te maken van de rapportage van gegevens van de SWA. Vooral in omgevingen waar veel SWA's worden ingezet, is deze oplossing vele malen schaalbaarder dan het gebruik van gecentraliseerde rapportage op een **security management applicatie (SMA)**, en biedt aangepaste rapportage-eigenschappen die een enorme hoeveelheid diepte en aanpassing aan de gegevens toevoegen. Rapporten kunnen worden gegroepeerd en aangepast om aan de behoeften van elke organisatie te voldoen. Cisco Advanced Services Group moet worden benut voor het vergroten van de omvang van AWSR.



E-mailmeldingen

Het ingebouwde alarmsysteem voor e-mail op de SWA kan het best worden gebruikt als alarmsysteem voor de basislijn. Het moet op de juiste manier worden aangepast om aan de behoeften van de beheerder te voldoen. Het kan namelijk zeer veel ruis veroorzaken als alle informatiegebeurtenissen zijn ingeschakeld. Het is belangrijker om de waarschuwingen te beperken en ze actief te controleren dan om alles te waarschuwen en ze als spam te negeren.

Waarschuwingsinstellingen	**Configuratie**
Van Adres aan gebruik wanneer het verzenden van alarm	Automatisch gegenereerd
Eerste aantal seconden wachten voor verzending van een dubbele waarschuwing	300 seconden
Maximum aantal seconden om te wachten voor verzending van een dubbele waarschuwing	360 seconden

Beschikbaarheidsbewaking

Er zijn twee methoden die kunnen worden gebruikt om de beschikbaarheid van een webproxy te bewaken. De eerste is **Layer 3 (L3)**-bewaking, die test of het IP-adres van het apparaat op het netwerk bereikbaar is. De eenvoudigste manier om dit te testen is door met regelmatige tussenpozen een **ICMP Echo (ping)**-verzoek naar het adres te sturen en te controleren op een antwoordpakket. De eigenschappen van het antwoord, zoals TTL, en latentie kunnen worden geparst om de gezondheid van de netwerklaag te bepalen.

Het is mogelijk dat een apparaat op pings kan reageren maar dat de volmachtsprocessen koel of intermitterend zijn. Daarom is het raadzaam om een **Layer 7 (L7)** monitor te gebruiken, die een expliciete proxy aanvraag naar het apparaat stuurt en verwacht een **200 OK** HTTP responscode. Dit test niet alleen de bereikbaarheid van de netwerkinterface, maar ook de reactiesnelheid van de proxy-diensten en de

levensvatbaarheid van upstream-diensten als er een externe bron wordt gevraagd. Dit type van controle neemt typisch de vorm van een expliciet HTTP-**HOOFD-**verzoek dat de proxy vraagt om verbinding te maken met een resource. De **HEAD** methode vraagt de headers die zouden worden teruggestuurd moet de client een **GET** request sturen, maar omvat alleen de response headers en geen data.

Als u een **L7** monitoring tool of script gebruikt, is het belangrijk om ervoor te zorgen dat het verkeer is vrijgesteld van authenticatie. Anders resulteert dit in regelmatige verificatiefouten en het gebruik van resources. Wanneer u een aangepaste user-agent string gebruikt in de monitoring tool, moet deze gebruikt worden om het verkeer te identificeren. Hoewel het verkeer is vrijgesteld van authenticatie, kan het nog steeds worden beperkt van onnodige internettoegang door het toegangsbeleid.

Wanneer u een of meer van deze methoden gebruikt, moet een beheerder een basislijn van acceptabele metriek rond de proxyrespons instellen en dat gebruiken om alarmdrempels op te bouwen. U moet tijd besteden aan het verzamelen van de antwoorden van dergelijke controles en voordat u besluit hoe u de drempels en de waarschuwing gaat configureren.

SNMP-bewaking

Het **Simple Network Management Protocol (SNMP)** is de belangrijkste methode om de status van het apparaat te bewaken. Het kan worden gebruikt om meldingen van het apparaat (vallen) te ontvangen of om verschillende **Object Identifiers (OIDâ€™s)** te peilen om informatie te verzamelen. Er zijn veel OID's beschikbaar op de SWA die alles bedekken, van hardware tot hulpbrongebruik tot individuele procesinformatie en statistische verzoeken.

Er is een aantal specifieke **Machine Information Base (MIB)** die om zowel hardware- als prestatiegerelateerde redenen moet worden bewaakt. De volledige lijst van MIB's is hier te vinden: https://www.cisco.com/web/ironport/tools/web/asyncosweb-mib.txt.

Dit is een lijst van te controleren aanbevolen MIB's en geen uitputtende lijst:

Hardware-OID	Name
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	ventilatoreenheid
1.3.6.1.4.1.15497.1.1.1.9.1.2	graden Celsius

Dit is OIDs-kaart rechtstreeks naar de uitvoer van de CLI-opdracht **voor statusdetails**:

OID	Name	Het veld Statusdetails
Systeembronnen		
1.3.6.1.4.1.15497.1.1.1.2.0	benutting per centimeter	CPU
1.3.6.1.4.1.15497.1.1.1.1.0	PerCentMemory-gebruik	RAM

Transacties per seconde		
1.3.6.1.4.1.15497.1.2.3.7.1.1.0	cacheThruputNow	Gemiddelde transacties per seconde in last minute.
1.3.6.1.4.1.15497.1.2.3.7.1.2.0	cachegeheugenDoorvoersnelheid1 uurPiek	Maximum aantal transacties per seconde in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.1.3.0	cacheDoorvoersnelheid1 uurGemiddeld	Gemiddelde transacties per seconde in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.1.8.0	cacheThruputLifePeak	Maximum aantal transacties per seconde sinds het opnieuw opstarten van proxy.
1.3.6.1.4.1.15497.1.2.3.7.1.9.0	cacheDoorvoersnelheidGemiddeld	Gemiddelde transacties per seconde sinds proxy opnieuw opstarten.
Bandbreedte		
1.3.6.1.4.1.15497.1.2.3.7.4.1.0	cacheBreedteTotalNow	Gemiddelde bandbreedte in de laatste minuut.
1.3.6.1.4.1.15497.1.2.3.7.4.2.0	cacheBreedteTotaal1 uurPiek	Maximale bandbreedte in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.4.3.0	cacheBreedteTotaal1kGemiddeld	Gemiddelde bandbreedte in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.4.8.0	cacheBreedteTotalLifePeak	Maximale bandbreedte sinds opnieuw opstarten van proxy.
1.3.6.1.4.1.15497.1.2.3.7.4.9.0	cacheBreedteTotaleLifeGemiddeld	Gemiddelde bandbreedte sinds proxy opnieuw opstarten.
Responstijd		
1.3.6.1.4.1.15497.1.2.3.7.9.1.0	cacheHitsNow	Gemiddelde cachesnelheid in last minute.
1.3.6.1.4.1.15497.1.2.3.7.9.2.0	cachegeheugenHits1hrPeak	Maximale cachesnelheid in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.9.3.0	cacheHits1hrGemiddeld	Gemiddelde cachesnelheid in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.9.8.0	cacheHitsLifePeak	Maximale cachesnelheid sinds opnieuw starten van proxy.
1.3.6.1.4.1.15497.1.2.3.7.9.9.0	cacheHitsLifeMean	Gemiddelde cache hit rate sinds proxy opnieuw opstarten.
Cache hit rate		
1.3.6.1.4.1.15497.1.2.3.7.5.1.0	cacheHitsNow	Gemiddelde cachesnelheid in last minute.
1.3.6.1.4.1.15497.1.2.3.7.5.2.0	cachegeheugenHits1hrPeak	Maximale cachesnelheid in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.5.3.0	cacheHits1hrGemiddeld	Gemiddelde cachesnelheid in afgelopen uur.
1.3.6.1.4.1.15497.1.2.3.7.5.8.0	cacheHitsLifePeak	Maximale cachesnelheid sinds opnieuw starten van proxy.

1.3.6.1.4.1.15497.1.2.3.7.5.9.0	cacheHitsLifeMean	Gemiddelde cache hit rate sinds proxy opnieuw opstarten.
Aansluitingen		
1.3.6.1.4.1.15497.1.2.3.2.7.0	cacheClientIdleConns	Inactiviteitsclient verbindingen.
1.3.6.1.4.1.15497.1.2.3.3.7.0	cacheServerIdleConns	Inactiviteitsserververbindingen.
1.3.6.1.4.1.15497.1.2.3.2.8.0	cacheClienttotaalConns	Totale aantal clientverbindingen.
1.3.6.1.4.1.15497.1.2.3.3.8.0	cacheServerTotalConns	Totale aantal serververbindingen.

Conclusie

In deze handleiding worden de belangrijkste aspecten van de configuratie, implementatie en bewaking van SWA beschreven. Als referentiegids heeft zij tot doel waardevolle informatie te verschaffen aan degenen die het meest effectieve gebruik van de SWA wilden garanderen. De best practices die hier worden beschreven zijn belangrijk voor de stabiliteit, schaalbaarheid en efficiëntie van het apparaat als een security tool. Het probeert ook te blijven als een relevante bron gaat vooruit en moet dus regelmatig worden bijgewerkt om veranderingen in netwerkomgevingen en productfunctiesets weer te geven.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.