Problemen met de latentie van een beveiligd webapparaat oplossen

Inhoud

Inleiding

In dit document worden de stappen beschreven voor het oplossen van problemen bij het gebruik van High Latency, High Disk en High CPU in Cisco Secure Web Appliance (SWA).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco SWA-beheer
- Proxy-implementatiemethoden (expliciet en transparant)
- SWA Command Line Interface (CLI)-opdrachten

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Wanneer u contact opneemt met de technische ondersteuning van Cisco, wordt u gevraagd om details te verstrekken over de uitgaande en inkomende netwerkactiviteit van SWA, die kan worden gecontroleerd door een pakketopname uit te voeren om verkeer te verzamelen voor debugging- of verificatiedoeleinden.

Frequente oorzaken van hoge latentie bij SWA

Over het algemeen zijn er drie hoofdcategorieën voor de hoge latentie in SWA:

1. Ontoereikende omvang van SWA of overbelaste middelen
2. Complexe configuraties
3. Netwerkgerelateerde latentieproblemen

Een van de meest voorkomende oorzaken van hoge latentie in SWA is onvoldoende dimensionering van de oplossing. De juiste omvang is van cruciaal belang om ervoor te zorgen dat het SWA-systeem over voldoende middelen beschikt om de huidige en verwachte werklasten aan te kunnen. Als het systeem ondermaats is, kan het moeite hebben om verzoeken efficiënt te verwerken, wat leidt tot vertragingen in de activiteiten en verminderde prestaties. Factoren zoals het aantal gebruikers, het volume van de decodering en specifieke scanvereisten moeten tijdens de implementatie zorgvuldig worden geëvalueerd om beperkte middelen te voorkomen. Als de SWA-capaciteit niet wordt afgestemd op de behoeften van de organisatie, kan dit leiden tot aanhoudende latentie en een slechtere gebruikerservaring.

Complexe configuraties kunnen de prestaties verlagen en latentie op de SWA veroorzaken, vooral bij hoge belasting, omdat elk verzoek onder verschillende omstandigheden moet worden verwerkt.

Netwerkgerelateerde latentie kan het gevolg zijn van de SWA zelf, services van derden zoals Active Directory, DLP, DNS of netwerkvertragingen tussen de client-, SWA- en upstreamservers.

Het analyseren van de verzoeken die naar de SWA worden verzonden, inclusief het identificeren van de topgebruikers en de meest gebruikte URL's, kan helpen om mogelijk wangedrag te ontdekken en de hoofdoorzaken van latentie aan te wijzen. Deze informatie is van onschatbare waarde voor het diagnosticeren van prestatieproblemen, het beheren van het bandbreedteverbruik en het garanderen van een passend gebruik van het systeem.

Tools voor probleemoplossing met SWA-latentie

Systeemstatus

Gebruik deze stappen om het huidige verbruik van bronnen in SWA te controleren:

Stap 1. Toegang tot de grafische gebruikersinterface (GUI) van SWA.

Stap 2. Navigeer naar Rapportage > Systeeminformatie > Systeemstatus.

Stap 3. Controleer deze kritieke statistieken om de systeemprestaties te beoordelen:

- CPU-gebruik (%): geeft de huidige CPU-belasting aan
- RAM-gebruik (%): geeft het geheugengebruik weer
- Rapportage/logboekgebruik (%): toont het percentage schijfruimte dat wordt gebruikt voor rapportage en logboekregistratie
- Uptime van het systeem: geeft de totale tijd weer dat het systeem is uitgevoerd zonder opnieuw op te starten

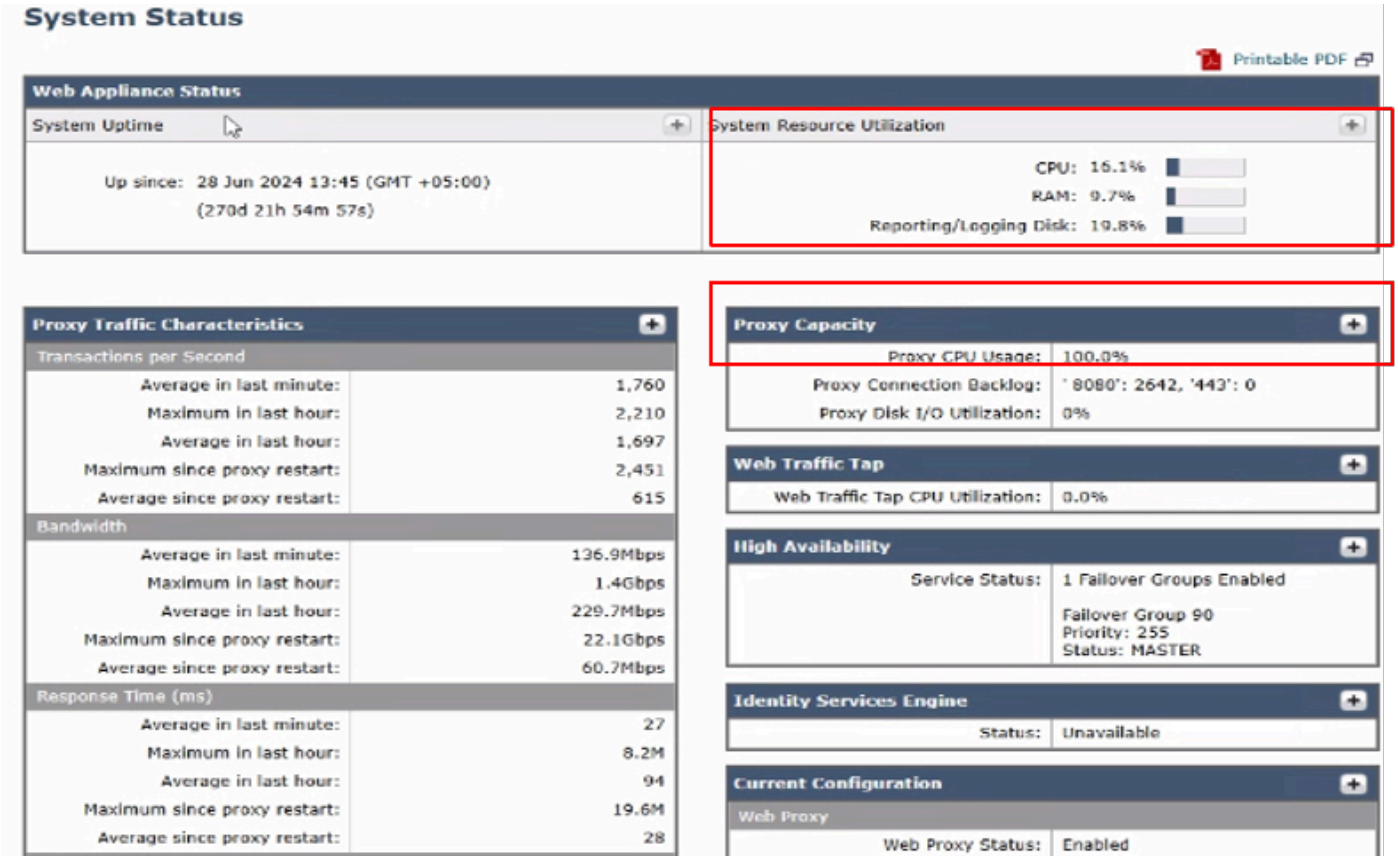


Image — Systeemstatus

Deze pagina geeft een overzicht van de huidige status van RAM, CPU en schijfgebruik. Als u het gebruik van bronnen in de loop van de tijd wilt bekijken vanuit de SWA-GUI, gaat u naar Rapportage en kiest u Systeemcapaciteit.

systeemcapaciteit

De pagina Systeemcapaciteit in de SWA biedt een uitgebreid overzicht van het gebruik van bronnen en prestatiestatistieken over een bepaald tijdsbereik. Deze pagina biedt gedetailleerde grafieken om het gedrag van het systeem te monitoren en te analyseren, optimale prestaties te garanderen en potentiële knelpunten te identificeren.

Beschikbare grafieken en statistieken op de pagina Systeemcapaciteit zijn:

1. Algemeen CPU-gebruik: geeft het totale CPU-gebruik weer, waardoor een overzicht op hoog niveau van de systeemprestaties wordt gegeven.
2. CPU-gebruik per functie: verdeelt CPU-gebruik op basis van specifieke functies, waaronder:

- webproxy
- Logboekregistratie
- verslaggeving
- McAfee
- Sophos
- Webroot
- Aanvaardbaar gebruik en reputatie

3. Responstijd/latentie (milliseconden): houdt responstijden bij om vertragingen in de verwerking van verzoeken te identificeren.

4. Transacties per seconde: toont het aantal transacties dat per seconde door de SWA wordt afgehandeld.

5. Uitgeschakelde verbindingen: bewaakt het aantal uitgaande verbindingen dat wordt aangelegd.

6. Bandbreedte uit (bytes): meet de hoeveelheid uitgaande bandbreedte die wordt gebruikt.

7. Proxybuffergeheugen (%): geeft het percentage geheugen weer dat door het proxyproces wordt gebruikt.

Controleer de statistieken op tekenen van een hoog bronnengebruik in dit dashboard.

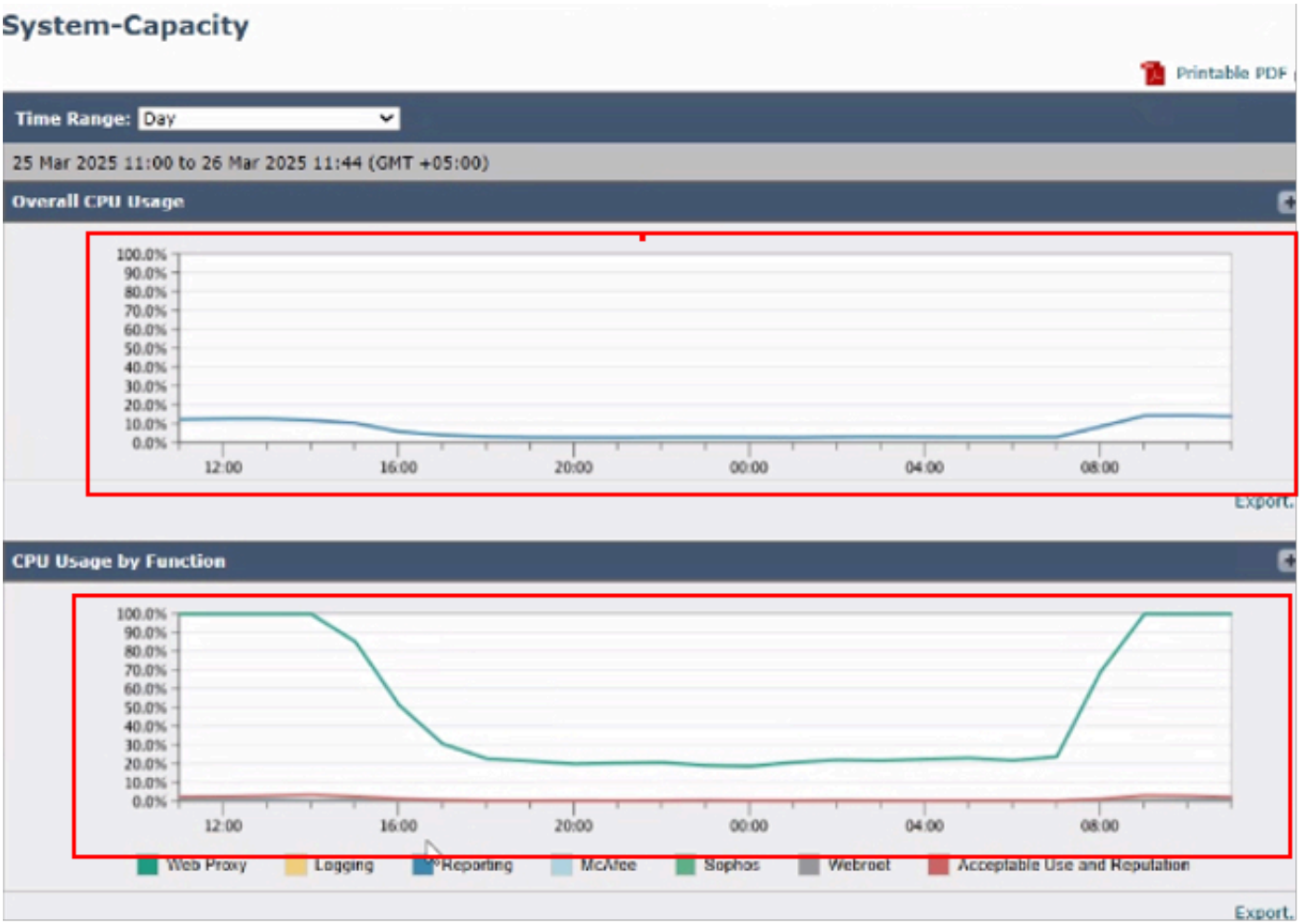
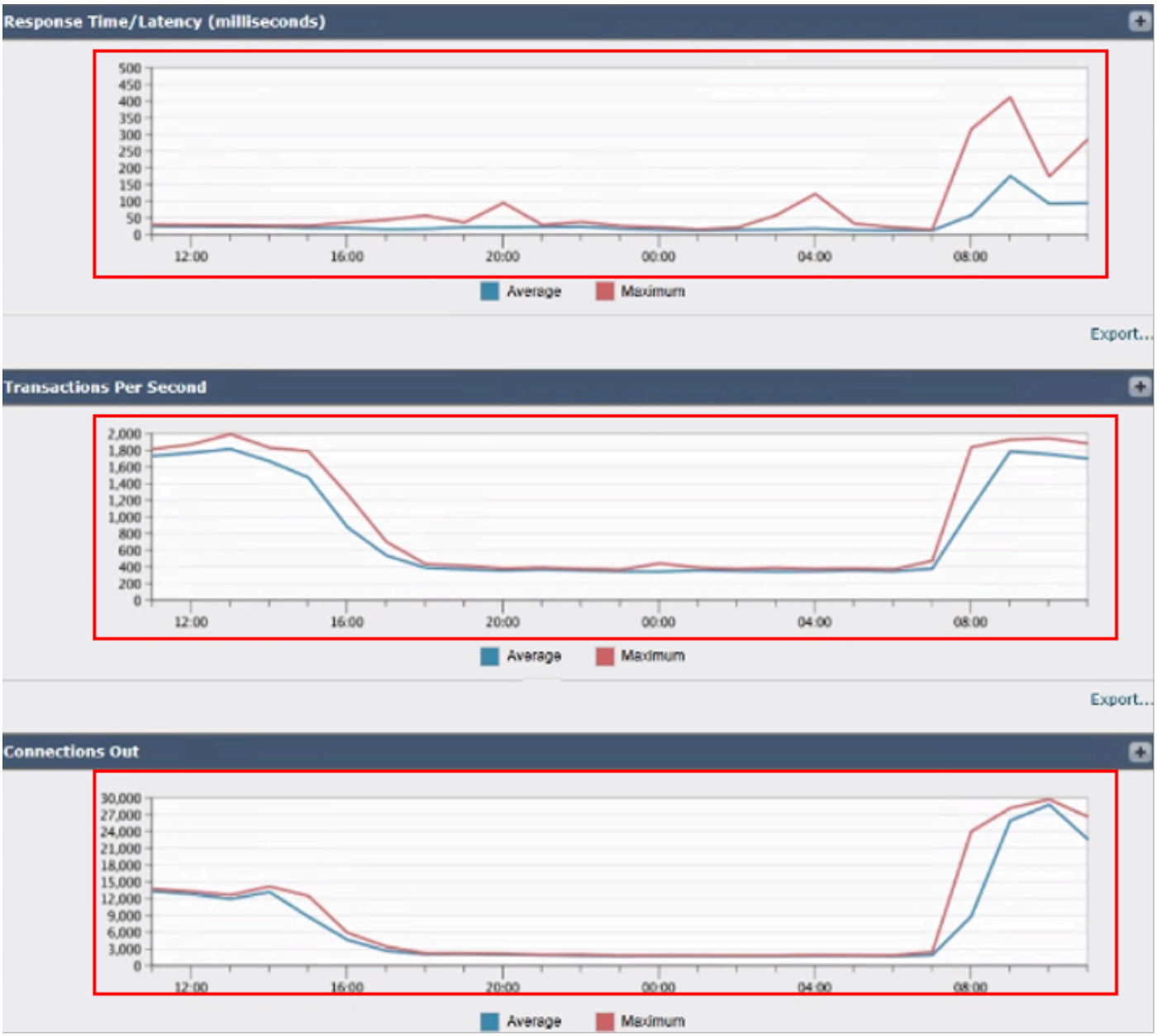


Image- Systeemcapaciteit



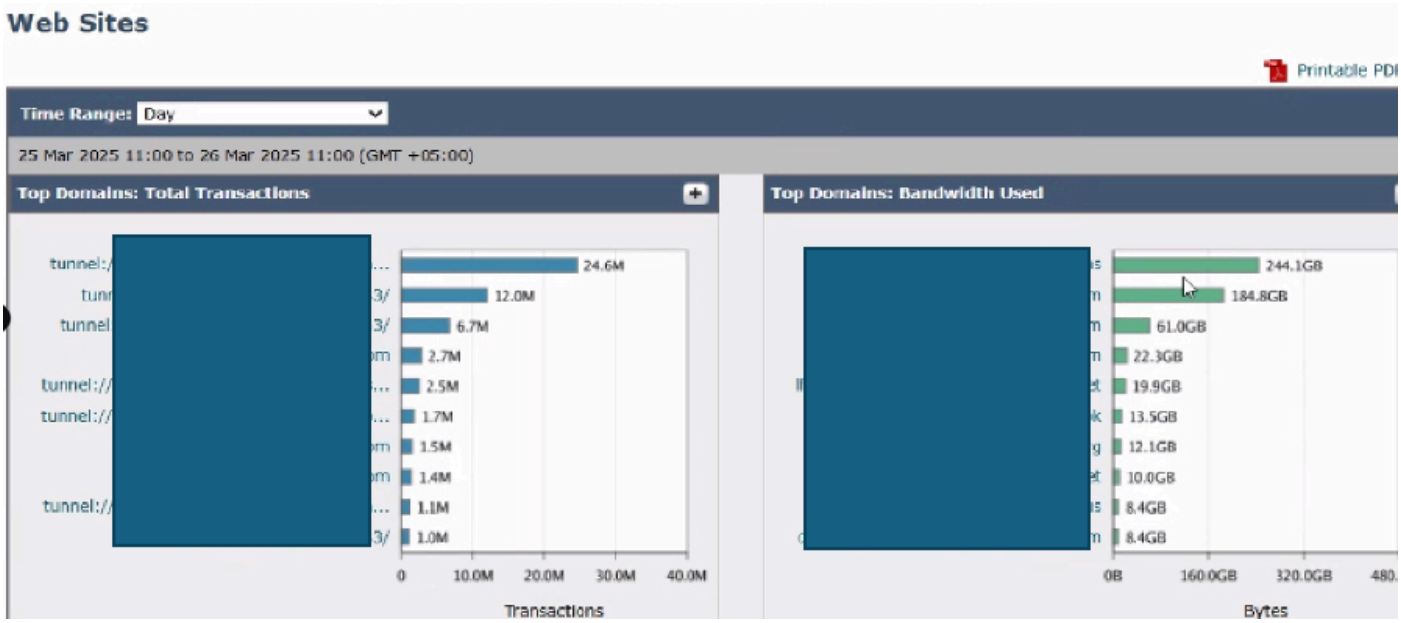
Afbeelding: SWA-transacties per seconde en verbindingen uit

Afbeelding - SWA-geheugengebruik

Analyseer topbestemmingen

Om topbestemmingen te analyseren, navigeert u naar de SWA GUI, navigeert u naar Rapportage en selecteert u Websites. Bekijk de lijst met de beste HTTP / HTTPS-websites en identificeer domeinen met veel verkeer of vaak gebruikte domeinen.

Overweeg op basis van uw bevindingen generieke URL's te omzeilen of vrij te stellen, zoals Microsoft Updates, Adobe, Office365 en online vergaderplatforms. Deze aanpak helpt het verkeer op de SWA te verminderen, wat leidt tot lagere latentie en een lagere belasting van de proxyverwerking.



Afbeelding - Dashboard van SWA-topwebsites

Domains Matched

Items Displayed 10

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
[redacted]	0B	23514:57	0	24.6M	24.6M
	0B	1909:50	0	12.0M	12.0M
	0B	26710:03	0	6.7M	6.7M
	3.0MB	4941:17	2,798	2.7M	2.7M
	0B	10029:17	0	2.5M	2.5M
	0B	2579:58	0	1.7M	1.7M
	4.2GB	5981:18	1.5M	0	1.5M
	184.8GB	2125:54	1.4M	1,806	1.4M
	0B	2062:27	0	1.1M	1.1M
	0B	1354:09	0	1.0M	1.0M
Totals (all available data):	741.1GB	111839:46	6.7M	64.8M	71.5M

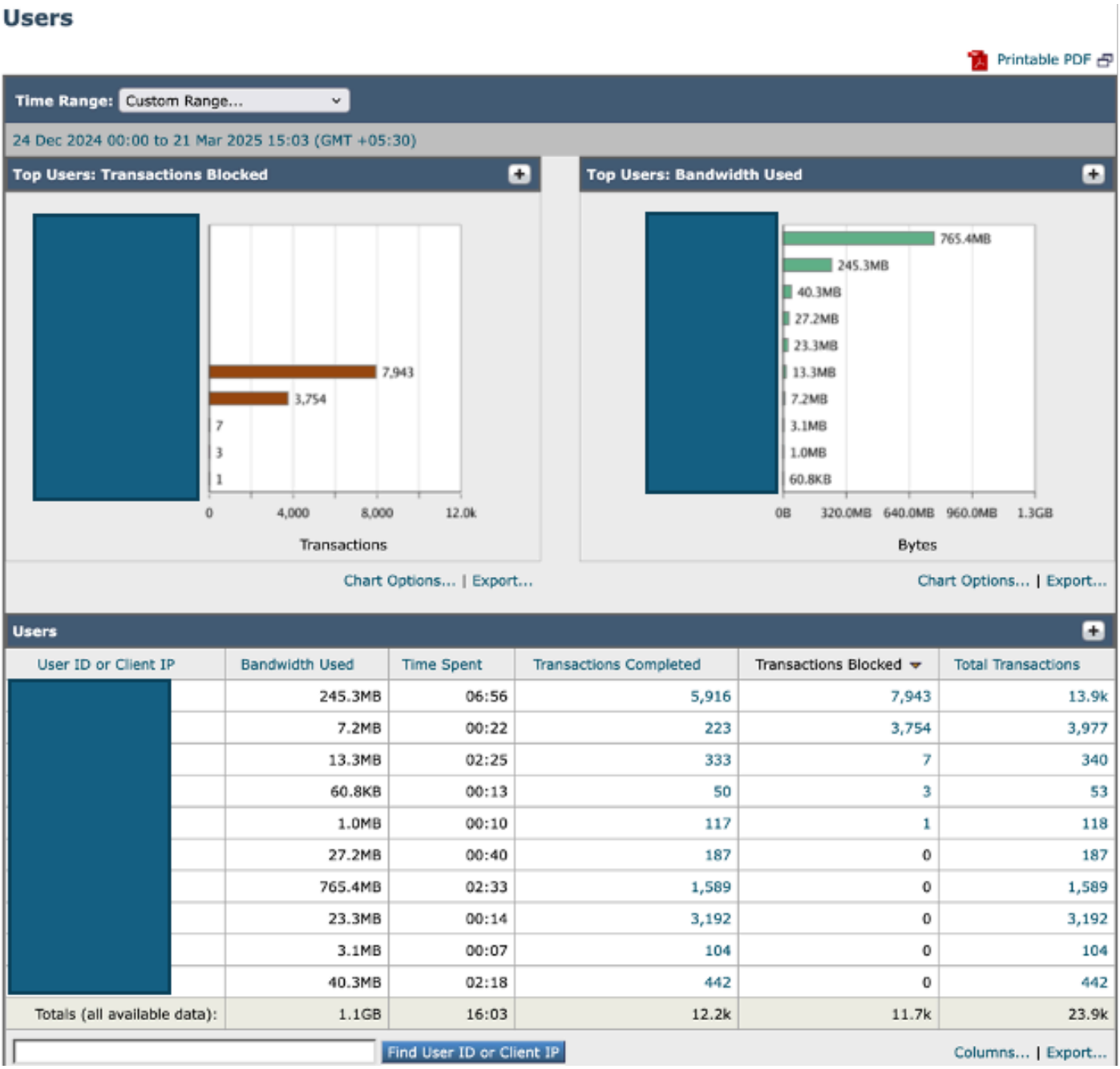
Afbeelding - Dashboard SWA-topdomeinen

Analyseer topgebruikers

Om potentiële bronnen van overmatig verkeer te identificeren, navigeert u naar de SWA GUI van Rapportage en kiest u Gebruikers.

Controleer de lijst om te bepalen welke gebruikers het hoogste aantal transacties genereren voor de SWA. Controleer bovendien of gebruikersmachines het grootste aantal transacties naar de SWA genereren en de maximale bandbreedte verbruiken.

Deze analyse kan helpen bij het identificeren van gebruikers of apparaten die verantwoordelijk zijn voor aanzienlijke verkeersbelastingen, waardoor gerichte acties mogelijk zijn om de algehele systeembelasting te verminderen.



Dashboard voor topgebruikers van Image-SWA

SHD-logboeken

Door de SHD_log te bekijken, kunt u enkele prestatiestatistieken analyseren, zoals het aantal sessies van gebruikers naar SWA (CliConn), het aantal sessies van SWA naar internet (SrvConn), de gemiddelde verzoeken per seconde (Reqs) enzovoort.

Raadpleeg voor meer informatie over het SHD-logboek de link Problemen met beveiligde webtoestelprestaties met SHD-logboeken oplossen,

Enkele belangrijke parameters die in de SHD-logs moeten worden beoordeeld, zijn:

- ClientConns: aantal actieve clientverbindingen

- ServerConns: aantal actieve serververbindingen
- ProxLd: Gemiddelde Proxy-procesbelasting
- CPULD: Gemiddelde totale CPU-belasting
- RAMUTIL: RAM-GEBRUIK
- Latentie: gemiddelde servicetijd in één minuut
- DiskUtil: Schijfgebruik en I/O-prestaties

Net als in dit voorbeeld leidt het hebben van ongeveer 1.600 verzoeken per seconde tot een hoge proxyprocesbelasting.

```
Wed Mar 26 11:09:30 2025 Info: Status: CPULd 16.3 DskUtil 19.9 RAMUtil 9.3 Reqs 1661 Band 152966 Latenc
Wed Mar 26 11:10:31 2025 Info: Status: CPULd 13.6 DskUtil 19.9 RAMUtil 9.5 Reqs 1699 Band 107048 Latenc
Wed Mar 26 11:11:31 2025 Info: Status: CPULd 15.0 DskUtil 19.9 RAMUtil 9.5 Reqs 1669 Band 178803 Latenc
Wed Mar 26 11:12:31 2025 Info: Status: CPULd 17.6 DskUtil 19.9 RAMUtil 9.2 Reqs 1785 Band 143721 Latenc
```

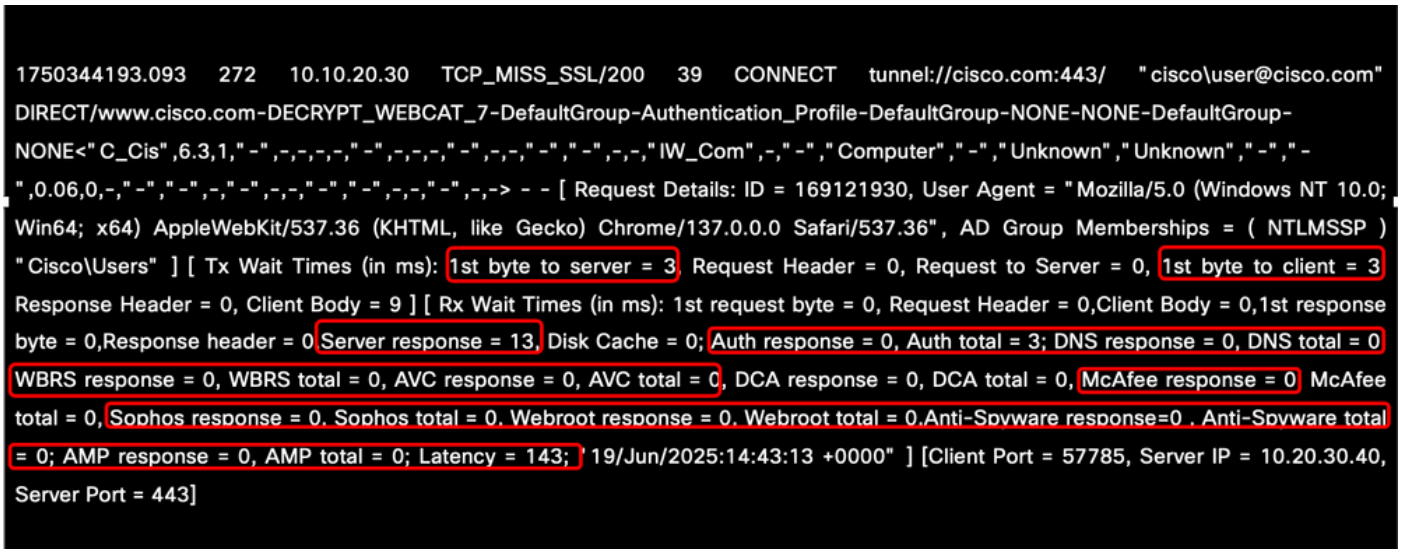
Toegang tot logboeken gebruiken om problemen met latentie op te lossen

Wanneer zich latentieproblemen voordoen met verkeer dat wordt benaderd via een SWA, kunnen Access Logs dienen als een waardevol hulpmiddel voor het identificeren van de waarschijnlijke hoofdoorzaak. Om het oplossen van problemen te verbeteren, kunt u de bestaande instellingen voor het toegangslogboek wijzigen of een nieuw toegangslogboek maken. Door het opnemen van Prestatieparameters in het Aangepaste Veld, kunt u dieper inzicht krijgen in factoren die bijdragen aan latentie, waardoor effectievere analyse en resolutie mogelijk wordt.

Raadpleeg voor meer informatie over de prestatieparameters en de configuratiestappen de koppeling: Prestatieparameter configureren in toegangslogboeken

Hier is de gedetailleerde handleiding voor het verzamelen van logs in de SWA: Access Secure Web Appliance Logs

Latentiebronnen kunnen worden geanalyseerd door belangrijke parameters te onderzoeken die helpen bepalen of er vertragingen optreden tussen de client en de SWA, binnen interne SWA-processen of tussen de SWA en de webserver. Belangrijke indicatoren waarmee rekening moet worden gehouden, zijn netwerkgebaseerde services zoals DNS-resolutie, verificatietijd en responstijden van server of client. Bovendien moeten vertragingen veroorzaakt door scanengines zoals AMP, Sophos en AVC worden geëvalueerd om hun impact op de algehele latentie te identificeren.



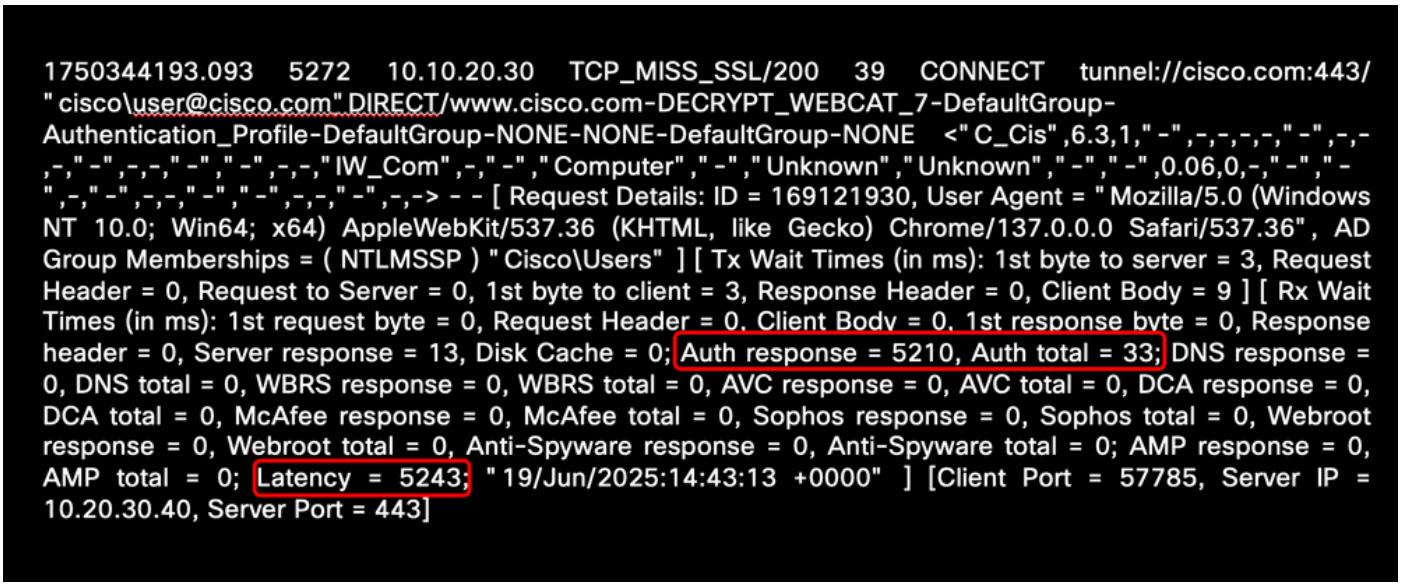
Afbeelding - Prestatieparameters in het AccessLog

Hoge verificatietijd

Als de verificatieresponstijd hoog is, is deze informatie vereist voor TAC om problemen met de verificatielatentie beter en sneller op te lossen:

- Huidige SWA-configuratie
- Verificatielogs in foutopsporings- of traceringsmodus
- Pakketopnames van
    - Clientmachine.
    - SWA (Met filter om het clientverkeer en het SWA-verkeer naar alle actieve mappen die zijn geconfigureerd in de instellingen van het domein, vast te leggen.)
- Zorg ervoor dat Accesslogs zowel aangepast veld %m als %g heeft om het verificatiemechanisme en de groepen te identificeren
- HAR-bestand van de client tijdens het reproduceren van het probleem
- De uitvoer van de opdracht testauthconfig vanuit de CLI

Dit voorbeeld toont de hoge latentietijd met betrekking tot verificatie:



Afbeelding - Voorbeeld van hoge latentie-verificatie

Hoge DNS-tijd

Als de DNS-responstijd hoog is, is deze informatie vereist voor TAC om problemen met DNS-latentie op te lossen:

- Huidige SWA-configuratie
- Systeemlogboeken in overtrekmodus
- IP-adres DNS-servers
- Pakketopnames van
  - Clientmachine
  - SWA (Filteren met het IP-adres van DNS-servers.)
- Zorg ervoor dat de accesslogs zowel %:<d als %:>d in het aangepaste veld hebben
- HAR-bestand van de client tijdens het reproduceren van het probleem

Als u meer wilt weten over de DNS-configuratie en het oplossen van problemen, raadpleegt u de link Problemen oplossen Secure Web Appliance DNS Service

Dit voorbeeld toont de hoge latentietijd met betrekking tot de DNS-naamresolutie:

```
1750344193.093   4472   10.10.20.30   TCP_MISS_SSL/200   39   CONNECT   tunnel://cisco.com:443/
" cisco\user@cisco.com" DIRECT/www.cisco.com-DECRYPT_WEBCAT_7-DefaultGroup-
Authentication_Profile-DefaultGroup-NONE-NONE-DefaultGroup-NONE   <" C_Cis" ,6.3,1," -" ,-,-,-,-," -" ,-,-
,-," -" ,-,-," -" ," -" ,-,-," IW_Com" ,-," -" ," Computer" ," -" ," Unknown" ," Unknown" ," -" ," -" ,0.06,0,-," -" ," -
" ,-," -" ,-,-," -" ," -" ,-,-," -" ,-,-> - - [ Request Details: ID = 169121930, User Agent = " Mozilla/5.0 (Windows
NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36" , AD
Group Memberships = ( NTLMSSP ) " Cisco\Users" ] [ Tx Wait Times (in ms): 1st byte to server = 3, Request
Header = 0, Request to Server = 0, 1st byte to client = 3, Response Header = 0, Client Body = 9 ] [ Rx Wait
Times (in ms): 1st request byte = 0, Request Header = 0, Client Body = 0, 1st response byte = 0, Response
header = 0, Server response = 13, Disk Cache = 0; Auth response = 0, Auth total = 3; DNS response = 4320,
DNS total = 65, WBRS response = 0, WBRS total = 0, AVC response = 0, AVC total = 0, DCA response = 0,
DCA total = 0, McAfee response = 0, McAfee total = 0, Sophos response = 0, Sophos total = 0, Webroot
response = 0, Webroot total = 0, Anti-Spyware response = 0, Anti-Spyware total = 0; AMP response = 0,
AMP total = 0; Latency = 4353; " 19/Jun/2025:14:43:13 +0000" ] [Client Port = 57785, Server IP =
10.20.30.40, Server Port = 443]
```

Afbeelding - Voorbeeld van hoge DNS-resolutie latentie

Hoge scanmotortijd

Als de responstijd hoog is voor Web Reputation Score (WBRS), Application and Visibility Control (AVC) en Malware Scanning-engines, is deze informatie vereist voor TAC om problemen met de hoge responstijd van de scanengine op te lossen:

- Huidige SWA-configuratie.
- Afhankelijk van de engine met een hoge responstijd kunt u het logniveau wijzigen in foutopsporing.

Dit voorbeeld toont de hoge latentietijd gerelateerd aan Sophos Engine:

```
1750344193.093   4500   10.10.20.30   TCP_MISS_SSL/200   39   CONNECT   tunnel://cisco.com:443/
" cisco\user@cisco.com"DIRECT/www.cisco.com-DECRYPT_WEBCAT_7-DefaultGroup-Authentication_Profile-
DefaultGroup-NONE-NONE-DefaultGroup-NONE   <" C_Cis" ,6.3,1," -" ,-,-,-,-," -" ,-,-,-," -" ,-,-,-," -" ," -" ,-,-
," IW_Com" ,-," -" ," Computer" ," -" ," Unknown" ," Unknown" ," -" ," -" ,0.06,0,-," -" ," -" ,-," -" ,-,-,-," -" ," -" ,-,-
," -" ,-,-> - - [ Request Details: ID = 169121930, User Agent = " Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36" , AD Group Memberships = (
NTLMSSP ) " Cisco\Users" ] [ Tx Wait Times (in ms): 1st byte to server = 3, Request Header = 0, Request to
Server = 0, 1st byte to client = 3, Response Header = 0, Client Body = 9 ] [ Rx Wait Times (in ms): 1st request
byte = 0, Request Header = 0, Client Body = 0, 1st response byte = 0, Response header = 0, Server response =
13, Disk Cache = 0; Auth response = 0, Auth total = 0; DNS response = 0, DNS total = 0, WBRS response = 0,
WBRS total = 0, AVC response = 0, AVC total = 0, DCA response = 0, DCA total = 0, McAfee response = 0,
McAfee total = 0, Sophos response = 4376, Sophos total = 145, Webroot response = 0, Webroot total = 0,
Anti-Spyware response = 0, Anti-Spyware total = 0; AMP response = 0, AMP total = 0; Latency = 4409;
" 19/Jun/2025:14:43:13 +0000" ] [Client Port = 57785, Server IP = 10.20.30.40, Server Port = 443]
```

Afbeelding - Malware-scanengine met hoge latentie

Als de scanengines een hoge respons laten zien, kunt u de scanservice vanuit de CLI opnieuw starten met de volgende stappen voor onmiddellijk herstel:

Stap 1. Typ diagnostische gegevens en druk op Enter (Dit is een verborgen opdracht en u moet de exacte opdracht typen.)

Stap 2. Kies SERVICES.

Stap 3. Als u de WBRS-service opnieuw wilt starten, kiest u WBRS en gaat u verder met stap 6.

Stap 4. Kies OPNIEUW STARTEN.

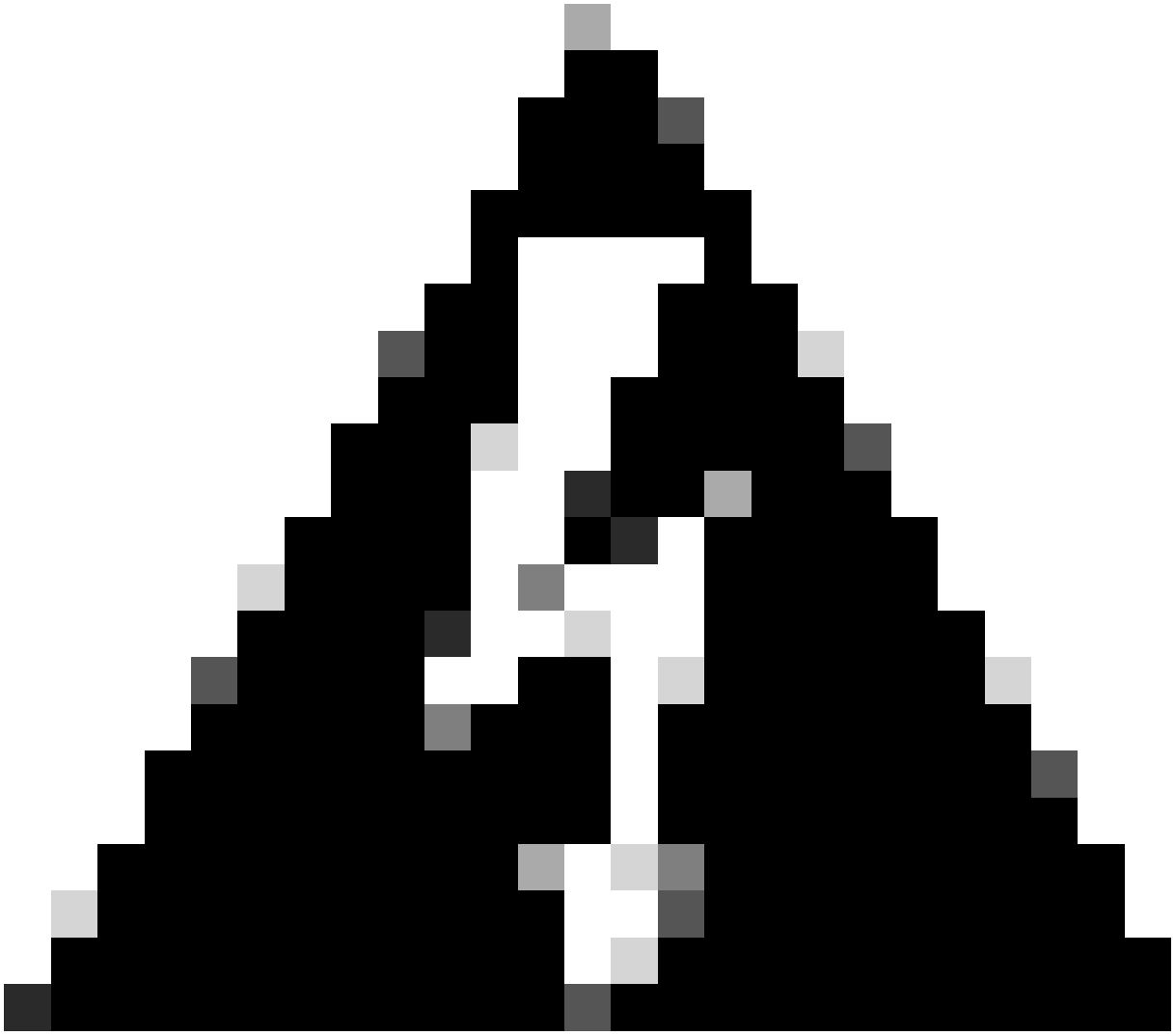
Stap 5. Druk op Enter om de wizard af te sluiten.

Stap 6. In het geval dat u van plan bent om een Malware scanning engine opnieuw te starten, kies ANTIVIRUS.

Stap 7. Selecteer uw scanners.

Stap 8. Kies OPNIEUW STARTEN.

Stap 9. Druk op Enter om de wizard af te sluiten.



Waarschuwing: het opnieuw opstarten van de interne services veroorzaakt onderbreking van de service. Aanbevolen wordt om dit uit te voeren in de uren buiten de productie of met voorzichtigheid.

Best practices bij het aansluiten van pakketafvang

Tijdens het vastleggen van pakketten moet u deze informatie verzamelen en delen met Cisco TAC.

- IP-adres van de client.
- De URL waar je toegang toe probeert te krijgen.
- Het IP-adres voor die URL is opgelost vanaf de client-pc en vanaf de SWA.
- Gebruikerservaring (zoals pagina die niet is geladen of gedeeltelijk is geladen en als er foutmeldingen zijn, maak dan een schermafbeelding).
- Tijdstempel van de test.
- Sluit alle andere browsers en apps op het clientsysteem. Toegang tot de website,

logboeken vastleggen in Kladblok voor één poging tot succes/mislukking en delen met Cisco Support.

Zie Koppeling Packet Capture configureren op Content Security Appliance voor gedetailleerde informatie over het vastleggen van pakketten in SWA

Configuratiecomplexiteit

Een andere veel voorkomende oorzaak van hoge latentie en slechte prestaties is de complexiteit van de configuratie. Dit gebeurt wanneer de SWA is geconfigureerd met een buitensporig aantal voorwaarden, profielen en beleidsregels. Een dergelijke complexiteit kan de responstijden aanzienlijk verhogen en het proxy-proces zwaar belasten. Dit probleem heeft de neiging om meer uitgesproken tijdens de piekuren, wanneer het verkeer op zijn hoogst.

Hier zijn enkele tips om de configuratie te optimaliseren:

1. Beperk HTTPS-decodering: decodeer alleen het verkeer dat essentieel is voor uw beveiligingsbeleid. Verminder waar mogelijk de verwerkingsoverhead met behoud van de beveiliging.
2. Prioriteren van beleid voor efficiëntie: regel het meest gebruikte beleid bovenaan de lijst met beleidsregels. Dit zorgt voor een snellere verwerking door eerst het meest veeleisende verkeer aan te pakken.
3. Gestroomlijnd beleidsontwerp: vereenvoudig het beleid door het aantal beleidsregels zoveel mogelijk te beperken. Dit vermindert onnodige verwerking en verbetert de algehele systeemprestaties.
4. Anti-malware- en antivirusscanning optimaliseren: controleer scanconfiguraties voor anti-malware- en antivirusprocessen. Deze kunnen CPU-intensief zijn, dus het nauwkeurig afstemmen ervan kan het verbruik van bronnen aanzienlijk verlagen zonder de beveiliging in gevaar te brengen.
5. Gebruik lichtgewicht reguliere expressies: vermijd complexe of resource-zware reguliere expressies. Zorg ervoor dat tekens zoals stippen (.) en sterren (*) op de juiste manier zijn ontsnapt om de verwerkingsbelasting te verminderen en inefficiënties te voorkomen.

Ga voor gedetailleerde informatie over best practices voor SWA naar Best practices voor veilige webapparaten gebruiken

CLI-opdrachten

Versie

Gebruik de opdracht version om de toewijzing van hardware (voor virtuele SWA) en de RAID-status (voor fysieke SWA) te controleren. Hardwareconfiguratie controleren: zorg ervoor dat het aantal CPU-kernen, het geheugen en de harde schijven worden toegewezen zoals verwacht. In virtuele modellen wordt de RAID-status weergegeven als Onbekend. Als de RAID-status is gedegradeerd of mislukt in het fysieke toestel, neemt u contact op met Cisco TAC om de schijfstatus van de back-end te bekijken.

Hier is een voorbeeld van het toewijzen van meer CPU aan de SWA die kan leiden tot wangedrag:

```
SWA Lab> version
Current Version
===============
Product: Cisco S100V Secure Web Appliance
Model: S100V
BIOS: 6.00
CPUs: 3 expected, 4 allocated
Memory: 8192 MB expected, 8192 MB allocated
Hard disk: 200 GB, or 250 GB expected; 200 GB allocated
RAID: NA
RAID Status: Optimal
```

DisplayAlerts

Gebruik de opdracht displayalerts om SWA-netwerkgerelateerde waarschuwingsberichten te controleren die de hoofdoorzaak kunnen aangeven.

In dit voorbeeld reageerde de DNS-server op IP-adres 10.10.10.10 niet en kan het bericht "De service Bestandsreputatie is niet bereikbaar" wijzen op een probleem met de netwerkconnectiviteit.

```
SWA LAB> displayalerts
Date and Time Stamp           Description
--------------------------------------------------------------------------------
26 Mar 2025 11:20:07 +0500 The File Reputation service is not reachable.
26 Mar 2025 11:20:07 +0500 Critical: Reached maximum failures querying DNS server 10.10.10.10
26 Mar 2025 11:20:07 +0500 Critical: Reached maximum failures querying DNS server 10.10.10.10
26 Mar 2025 10:16:18 +0500 Warning: Communication with the File Reputation service has been established
```

process_status

Gebruik de opdracht process_status om het proces- en geheugengebruik van interne SWA-services te bekijken.

Als het Prox-proces, het belangrijkste proces voor het verwerken van verkeersproxy's, gedurende enkele minuten consequent meer dan 100% wordt gebruikt, duidt dit op een aanhoudende hoge belasting van het proces. Af en toe korte pieken in CPU-gebruik op de Prox of andere processen zijn echter normaal en verwacht.

<#root>

```
SWA LAB> process_status
USER     PID
```

%CPU

%MEM

VSZ RSS TT STAT STARTED TIME

COMMAND

root 11 2805.4 0.0 0 512 - RNL 28Jun24 11863204:12.63 idle
root 71189

102.0

19.5

6670700 6478032 - R 23Feb25 18076:32.80

prox

root 91880 99.0 0.6 369564 214832 - R 28Jun24 58854:51.78 counterd
root 91267 76.0 0.9 379804 292324 - R 28Jun24 59371:01.26 counterd
root 12 25.9 0.0 0 1600 - WL 28Jun24 30899:57.88 intr
root 46955 25.0 0.2 91260 59336 - S 23Jan25 7547:02.96 wbnpd
root 95056 23.0 11.2 5369332 3710348 - I 28Jun24 31719:23.99 java
root 93190 12.0 1.4 3118384 456088 - S 01:15 29:57.05 beakerd
root 64579 11.0 0.2 101336 71204 - S 6Aug24 12074:55.55 coeuslogd

statusdetail

De opdracht Statusdetails geeft een realtime samenvatting van het gebruik van systeembronnen, de statistieken van het netwerkverkeer en de verbindingsstatistieken, die de algehele status en prestaties van de SWA weergeven. Het weerspiegelt de weergave Systeemstatus in de GUI voor snelle bewaking en probleemoplossing.

<#root>

SWA LAB> Status detail

Status as of: Wed Mar 26 11:51:27 2025 PKT

Up since: Fri Jun 28 13:45:43 2024 PKT (270d 22h 5m 43s)

System Resource Utilization:

CPU 16.0%

RAM 10.3%

Reporting/Logging Disk 19.8%

```
Transactions per Second:
  Average in last minute                1745
  Maximum in last hour                  2210
  Average in last hour                  1708
  Maximum since proxy restart           2451
  Average since proxy restart            615
Bandwidth (Mbps):
  Average in last minute              149.699
  Maximum in last hour               1356.387
  Average in last hour                229.634
  Maximum since proxy restart       22075.244
  Average since proxy restart          60.689
Response Time (ms):
  Average in last minute                  99
  Maximum in last hour                 8194128
  Average in last hour                    87
  Maximum since proxy restart          19608632
  Average since proxy restart             28
Cache Hit Rate:
  Average in last minute                   3
  Maximum in last hour                     6
  Average in last hour                     2
  Maximum since proxy restart             89
  Average since proxy restart              2
Connections:
  Idle client connections               3481
  Idle server connections                754


Total client connections              21866


  Total server connections             19049


SSLJobs:
  In queue Avg in last minute              0
  Average in last minute                12050
  SSLInfo Average in last min              0
Network Events:
  Average in last minute                16.0
  Maximum in last minute                 171
  Network events in last min          151918
```

Ipcheck

De opdracht ipcheck geeft gedetailleerde systeeminformatie weer voor de Secure Web Appliance, inclusief hardwarespecificaties, schijfgebruik, netwerkinterfaces, geïnstalleerde softwaresleutels en versiegegevens, en biedt een uitgebreide momentopname van de huidige status van het toestel.

<#root>

```
SWA LAB > ipcheck
  Ipcheck Rev           1
  Date                  Fri Mar 21 16:34:56 2025
```

```
Model                 S100V
Platform              vmware (VMware Virtual Platform)
Secure Web Appliance Version  Version: 15.2.1-011
Build Date            2024-10-03
Install Date          2025-02-13 17:49:24
Burn-in Date          Unknown
BIOS Version          6.00
RAID Version          NA
RAID Status           Unknown
RAID Type             NA
RAID Chunk            Unknown
BMC Version           NA
Disk 0                200GB VMware Virtual disk 1.0 at mpt0 bus 0 scbus2 target 0 lun 0
Disk Total            200GB

Root                  4GB 64%


Nextroot              4GB 65%


Var                   400MB 38%


Log                   130GB 24%


DB                    2GB 0%


Swap                  8GB
Proxy Cache           50GB
RAM Total             8192M
```

snelheid

De opdracht rate drukt elke 10 seconden de verbindingssnelheden en het aantal verzoeken per seconde af.

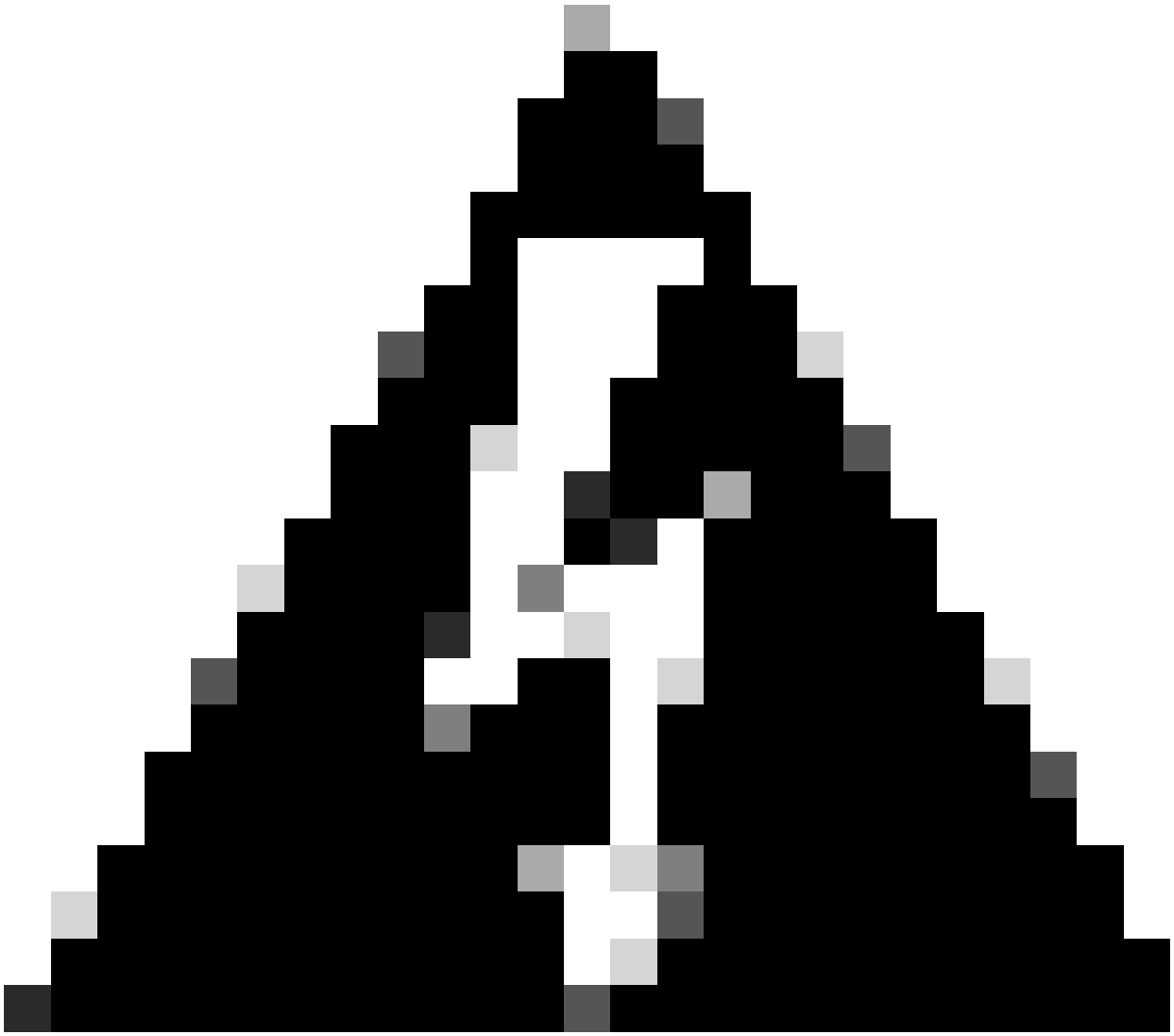
<#root>

```
SWA LAB> 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


100.00  1800     17  16352   1626    178551    178551    0.0  2366   0


100.00  1813     18  16453   1659    226301    224952    0.6  3008   0
```

```
99.00  1799      10  16338   1645    206234    206234    0.0  3430   1
```

Logboeken verzamelen voor hoge latentie

Het hangt af van het gedeelte dat u een hoge responstijd van Access Logs of een hoge procesbelasting van SHD-logs ziet, voor verdere probleemoplossing kunt u het bijbehorende logboekabonnement het beste wijzigen in Debug.



Waarschuwing: als u het logniveau instelt op foutopsporing of tracering, kan dit leiden tot een hoger bronnengebruik en kan het gebeuren dat logbestanden snel roteren of overschrijven.

toegangslogveld	SHD-logveld	corresponderend logboekabonnement

Auth response, Auth totaal	--	authlogs
DNS-respons, DNS totaal	--	system_logs
WBRS-respons, WBRS totaal	WBRS_WucLd	Neem contact op met Cisco TAC
AVC-respons, AVC totaal	--	AVC_logs
McAfee-reactie, McAfee-totaal	McAfeeLd	mcafee_logs
Sophos reactie, Sophos totaal	SophosLd	sophos_logs
Webroot-respons, Webroot-totaal	WebrootLd	weblogs
AMP-respons, AMP totaal	AMPLd	amp_logs

Gerelateerde informatie

Problemen met de prestaties van veilige webapparaten oplossen met SHD-logboeken

Toegang tot beveiligde logbestanden van webapparaten

Packet Capture configureren op Content Security Appliance

Best practices voor veilige webapparaten gebruiken

Prestatieparameter configureren in toegangslogboeken

Problemen oplossen Ongebruikelijke procestoestanden in SWA

Bepaal de decoderingssnelheid in SWA

Problemen oplossen met de DNS-service van een beveiligd webapparaat

Toegang tot beveiligde logbestanden van webapparaten

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.