

Probleemoplossing voor beveiligde web applicatie DNS-service

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[DNS-concept](#)

[DNS-service in proxyimplementaties](#)

[DNS-instellingen configureren](#)

[Best practices](#)

[DNS in GUI configureren](#)

[DNS vanuit CLI configureren](#)

[CLI DNS-opdrachten](#)

[Handmatig opnemen maken](#)

[terugvloed](#)

[advanced proxyconfig](#)

[DNS-cache](#)

[De DNS-cache wissen uit GUI](#)

Inleiding

Dit document beschrijft de configuratie van Domain Name Service (DNS) en hoe u problemen kunt oplossen in Secure Web Appliance (SWA), voorheen bekend als WSA.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Geïnstalleerde fysieke of virtuele beveiligde web applicatie (SWA)
- Licentie geactiveerd of geïnstalleerd
- Secure Shell-client (SSH)
- De setup-wizard is voltooid

- Administratieve toegang tot de SWA

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.

DNS-concept

DNS is het systeem in het internet dat de namen van objecten (meestal hostnamen) in IP-adres (Internet Protocol) of andere waarden van resourcerecord in kaart brengt.

De naamruimte van het internet is verdeeld in domeinen, en de verantwoordelijkheid voor het beheer van namen binnen elk domein is gedelegeerd, doorgaans naar systemen binnen elk domein.

De domeinnaamruimte is onderverdeeld in gebieden die zones worden genoemd die delegatiepunten in de DNS-boom zijn.

Een zone bevat alle domeinen vanaf een bepaald punt naar beneden, behalve die waarvoor andere zones gezaghebbend zijn.

Een zone heeft meestal een gezaghebbende naamserver, vaak meer dan één.

In een organisatie, kunt u vele naamserver hebben, maar de cliënten van Internet kunnen slechts die vragen die de servers van de wortelnaam kennen.

De andere naamserver beantwoorden alleen interne vragen.

DNS is gebaseerd op een client/server-model. In dit model slaan naamserver gegevens op over een deel van de DNS-database en leveren deze aan clients die de naamserver doorzoeken in het netwerk.

Naamserver zijn programma's die op een fysieke host worden uitgevoerd en zonegegevens opslaan. Als beheerder voor een domein stelt u een naamserver in met de database van alle Resource Records (RR's) die de hosts in uw zone of zones beschrijven

DNS-service in proxyimplementaties

In de expliciete implementatie: De proxy voert DNS-vragen uit

In de Transparent Implementatie: DNS-vragen lopen op de client.

DNS-instellingen configureren

U kunt DNS configureren vanuit zowel Graphical User Interface (GUI) als Command Line Interface (CLI).

AsyncOS voor Web kan gebruik maken van de Internet root DNS servers of uw eigen DNS servers. Als SWA Internet root servers gebruikt, kunt u alternatieve servers opgeven voor specifieke domeinen.

Aangezien een alternatieve DNS-server van toepassing is op één domein, moet deze betrouwbaar zijn (definitieve DNS-records leveren) voor dat domein.

AsyncOS ondersteunt gesplitste DNS waar interne servers zijn geconfigureerd voor specifieke domeinen en externe of root-DNS servers zijn geconfigureerd voor andere domeinen.

Als SWA gebruik maakt van een DNS-server, kunnen we ook uitzonderingsdomeinen en bijbehorende DNS-server opgeven.

Best practices

De beste praktijken van de veiligheid stellen voor dat elk netwerk twee DNS resolvers moet ontvangen: voor gebiedende verslagen van binnen een lokaal domein, en voor recursieve resolutie van de domeinen van Internet.

Om dit aan te passen, laat de SWA DNS servers toe om voor specifieke domeinen worden gevormd.

In het geval van één DNS server beschikbaar voor zowel lokale als recursieve vragen, overweeg de extra lading dit zou toevoegen als het voor alle vragen van SWA wordt gebruikt.

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.

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 time-out voor een query wordt in deze tabel gegeven 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

Ga voor meer informatie naar: [Richtlijnen voor beste praktijken van Cisco Web Security Appliance - Cisco](#)

DNS in GUI configureren

Gebruik de volgende stappen om DNS vanuit GUI te configureren:

Stap 1. Netwerk kiezen in het bovenste menu

Stap 2. Kies DNS

Network

System

Interfaces

Transparent Redirection

Routes

DNS

High Availability

Internal SMTP Relay

Upstream Proxy


External DLP Servers


Web Traffic Tap

Certificate Management

Cloud Services Settings


Alternatieve DNS-servers negeren (optioneel): Autoritatieve DNS-servers voor domeinen

 Opmerking: AsyncOS voldoet niet aan de versiepreferenties voor transparante FTP-verzoeken.

 Opmerking: in de modus Cloud Connector ondersteunt Cisco Web Security Applicatie alleen IPv4

Gebruik de Internet Root DNS-servers. Kies voor het gebruik van de Internet root DNS servers voor het zoeken van domeinnamen wanneer het apparaat geen toegang heeft tot DNS servers in uw netwerk.

Internet Root DNS-servers lost geen lokale hostnamen op.

 Opmerking: als u uw apparaat nodig hebt om lokale hostnamen op te lossen, gebruikt u een lokale DNS-server of voegt u de juiste statische items toe aan de lokale DNS vanaf de Command Line Interface (CLI).

Domain Search List: een DNS-domeinzoeklijst die wordt gebruikt wanneer een aanvraag wordt verzonden naar een naakte hostnaam (zonder punt ". ").


De opgegeven domeinen worden beurtelings geprobeerd, in de opgegeven volgorde (links naar rechts), om te zien of een DNS-match voor de hostnaam plus domein kan worden gevonden.

Routing Table for DNS Traffic: Specificeert de interface van de DNS-serviceroute voor het verkeer.

Wacht voordat u de omgekeerde DNS-looks uittikt: de wachttijd in seconden voor niet-responsieve omgekeerde DNS-lookups.

De secundaire DNS-servers ontvangen vragen over de hostnaam wanneer de primaire DNS-servers deze fouten teruggeven:

- Geen fout, geen antwoordsectie ontvangen
 - Server kan verzoek niet voltooien, geen antwoordsectie
 - Naamfout, geen antwoordsectie ontvangen
 - Functie niet geïmplementeerd
 - Server geweigerd om Query te beantwoorden
-

 Opmerking: AsyncOS evalueert transacties op basis van beleid voordat het externe afhankelijkheden evalueert om onnodige externe communicatie van het apparaat te vermijden. Als een transactie bijvoorbeeld wordt geblokkeerd op basis van een beleid dat niet-gecategoriseerde URL's blokkeert, dan zal de transactie niet mislukken op basis van

 een DNS-fout.

Prioriteit: een waarde van 0 heeft de hoogste prioriteit. Een willekeurige IP wordt geselecteerd als beide dezelfde prioriteit hebben.

DNS vanuit CLI configureren

U kunt dnsconfig van CLI gebruiken om DNS instellingen te configureren.

Stap 1. Type dnsconfig in CLI:

```
SWA_CLI> dnsconfig
```

```
Currently using the local DNS cache servers:
```

1. Priority: 0 10.1.1.1
2. Priority: 1 10.2.2.2
3. Priority: 2 10.3.3.3

```
Currently using the following Secondary DNS cache servers :
```

1. Priority: 0 10.10.10.10

```
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.

```
[>
```

Stap 2. Als u een nieuwe DNS-server aan de lijst wilt toevoegen, typt u NEW en drukt u op ENTER.

Stap 3. Kies tussen Primaire DNS nameservers of Secundaire DNS nameservers, waaraan u een nieuwe nameserver wilt toevoegen.

```
[> NEW
```

```
Do you want to make changes in the Primary DNS nameserver list or secondary DNS nameserver list?
```

1. Make changes to the primary DNS nameserver
2. Make changes to the secondary DNS nameserver

```
[> 1
```

Stap 4. Kies voor het toevoegen van een nieuwe naamserver of een alternatieve domeinserver (voorwaardelijke doorsturen van domeinnaam)

```
Do you want to add a new local DNS cache server or an alternate domain server?
```

1. Add a new local DNS cache server.
 2. Add a new alternate domain server.
- [> 1

Stap 5. Het IP-adres van de nieuwe naamserver opgeven

Stap 6. Geef de prioriteit op voor de nieuwe naamserver.

Please enter the IP address of your DNS server.
Separate multiple IPs with commas.
[> 10.4.4.4

Please enter the priority for 10.4.4.4.
A value of 0 has the highest priority.
The IP will be chosen at random if they have the same priority.

[0]> 4

Currently using the local DNS cache servers:

1. Priority: 0 10.1.1.1
2. Priority: 1 10.2.2.2
3. Priority: 2 10.3.3.3
4. Priority: 4 10.4.4.4

Currently using the following Secondary DNS cache servers :

1. Priority: 0 10.10.10.10

Stap 7. Druk op ENTER om de wizard te verlaten.

Stap 8. Type commit om de wijzigingen op te slaan.

Opmerking: Als u naamservern wilt bewerken of verwijderen, kunt u kiezen voor BEWERKEN en VERWIJDEREN uit dnsconfig.

Van de optie van de OPSTELLING kunt u de DNS cachetijd en offline DNS opsporingsinstellingen vormen:

```
SWA_CLI> dnsconfig
```

```
....
```

```
[>] setup
```

```
Do you want the Gateway to use the Internet's root DNS servers or would you like it to use your own DNS
```

```
1. Use Internet root DNS servers
```

```
2. Use own DNS cache servers
```

```
[2]> 2
```

```
Enter the number of seconds to wait before timing out reverse DNS lookups.
```

```
[20]>
```

```
Enter the minimum TTL in seconds for DNS cache.
```

```
[1800]>
```

Do you want to enable Secure DNS? [N]> N

Warning: Ensure that you configure the DNS server with DNSSEC because there is no backward compatibility. Failing to do so can result in invalid response with an unresolved hostname.

You must use FQDN with the hostname for the local and private domains.

Enter the number of failed attempts before considering a local DNS server offline.
[100]>

Enter the interval in seconds for polling an offline local DNS server.
[5]>

Minimale TTL in seconden voor DNS-cache: deze optie is om de minimale seconden te configureren die SWA heeft gecached een record. voor meer informatie bezoek DNS cache sectie in dit document.

Voer het aantal mislukte pogingen in voordat u een lokale DNS-server offline overweegt: Als DNS-server niet reageert op DNS-vragen, begint de teller.

Wanneer deze gedefinieerde waarde wordt bereikt, wordt die naamserver beschouwd als Offline DNS-server en SWA vermijdt om de DNS-query naar die naamserver te verzenden voor een vooraf gedefinieerde tijdsduur (Volgende optie).

Wanneer DNS server is gemarkeerd zo offline, kunt u deze foutmelding zien:

```
30 Jun 2023 07:37:03 +0200    Reached maximum failures querying DNS server 10.1.1.1
```

Geef het interval in seconden op voor het opiniepeilen van een offline lokale DNS-server: wanneer een DNS-server als offline is gemarkeerd, na dit tijdsinterval (in seconden), begint SWA DNS-query naar die server te sturen en de teller voor die DNS-server is mislukt antwoordresets naar nul.

CLI DNS-opdrachten

Handmatig opnemen maken

Om een handleiding "Een record" te maken kunt u het Hosts-bestand niet gebruiken of bewerken. U kunt localhost verborgen opdracht gebruiken van dnsconfig in CLI.

Opmerking: U moet wijzigingen doorvoeren nadat u deze configuraties hebt gewijzigd.

dnsconfig

Currently using the local DNS cache servers:

1. Priority: 0 10.1.1.1
2. Priority: 0 10.2.2.2

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.

[> localhosts

Local IP to Host mappings:

Choose the operation you want to perform:

- NEW - Add new local IP to host mapping.
- DELETE - Delete an existing mapping.

```
[ ]> new
```

Enter the IP address of the host you are adding.

```
[ ]> 10.20.30.40
```

Enter the canonical host name and any additional aliases (separate values with spaces)

```
[ ]> ManualHostEntry.cisco.com
```

terugvloed

dnsflush verwijdert alle gecacheerde DNS-records uit DNS-cachetabel:

```
SWA_CLI> dnsflush
```

```
Are you sure you want to clear out the DNS cache? [N]> Y
```

advanced proxyconfig

```
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

```
[ ]> DNS
```

Enter values for the DNS options:

Enter the URL format for the HTTP 307 redirection on DNS lookup failure.

```
[%P://www.%H.com/%u]>
```

Would you like the proxy to issue a HTTP 307 redirection on DNS lookup failure?

```
[Y]>
```

Would you like proxy not to automatically failover to DNS results when upstream proxy (peer) is unresponsive?

```
[N]>
```

Select one of the following options:

0 = Always use DNS answers in order

1 = Use client-supplied address then DNS

2 = Limited DNS usage
3 = Very limited DNS usage

For options 1 and 2, DNS will be used if Web Reputation is enabled.
For options 2 and 3, DNS will be used for explicit proxy requests, if there is no upstream proxy or in the event the configured upstream proxy fails.

For all options, DNS will be used when Destination IP Addresses are used in policy membership.

Find web server by:
[0]>

De HTTP 307 (Temporary Redirect) statuscode geeft aan dat de doelbron tijdelijk onder een ander Uniform Resource Identifier (URI) verblijft en dat de gebruikersagent DE aanvraagmethode NIET MAG wijzigen als hij een automatische omleiding naar die URI uitvoert. Aangezien de omleiding in de loop van de tijd kan veranderen, moet de client de oorspronkelijke effectieve request URI blijven gebruiken.

Meer details over: [Wat is de HTTP 307 tijdelijke omleiding status code - Kinsta](#)

Deze opties bepalen hoe SWA beslist over het IP-adres om verbinding te maken, wanneer een clientverzoek in transparante proxyimplementatie wordt geëvalueerd. Wanneer een verzoek wordt ontvangen, WSA een bestemmingsIP adres en een hostname zien. SWA moet beslissen of zij het oorspronkelijke IP-adres van de bestemming voor de TCP-verbinding vertrouwt of dat zij haar eigen DNS-resolutie doet en het opgeloste adres gebruikt. Standaard is "0 = Gebruik altijd DNS antwoorden in volgorde," wat betekent dat SWA niet vertrouwt op de client om het IP-adres te leveren.

Optie 1: 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 2: 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 3: SWA gebruikt alleen het door de client opgegeven adres voor de verbinding en valt niet terug. Het door de klant geleverde 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 opgeloste adres voor een bepaalde hostname bepaalt. Als client een downstream proxy is, kies optie 3 om de extra latentie van onnodige DNS-lookups te voorkomen.


DNS-cache

Om de efficiëntie en prestaties te verhogen, slaat Cisco SWA DNS-vermeldingen op voor domeinen waarmee u onlangs verbinding hebt gemaakt. Het DNS cache staat SWA toe om excessieve DNS-lookups van dezelfde domeinen te voorkomen. De DNS cache-ingangen

verlopen vanwege de TTL (Time to Live) van de record.

Wanneer de TTL van de record in DNS server groter is dan SWA dnsconfig cache TTL tijd, dan dns cache gebruik de TTL van de DNS server.

Wanneer de TTL van de record in DNS server minder is dan SWA dnsconfig cache TTL tijd, dan dns cache gebruik de TTL van WSA dnsconfig instelling.

 Waarschuwing: SWA heeft twee DNS cache, de ene is ontworpen voor Proxy-proces en de andere wordt gebruikt voor Interne proces.

Standaard heeft de SWA DNS-records voor minimaal 30 minuten gecachet, ongeacht het opnametl. Moderne websites die zwaar gebruik maken van Content Delivery Networks (CDN) zouden lage TTL-records hebben omdat hun IP-adressen vaak veranderen.

Dit kan resulteren in een client cache één IP-adres voor een bepaalde server en SWA cachet een ander adres voor dezelfde server. Om dit tegen te gaan, kan SWA standaard TTL worden verlaagd tot vijf minuten van de sectie SETUP in dsnconfig CLI commando.

Als bijvoorbeeld de "minimum TTL in seconden for DNS cache" in DNS-configuratie is ingesteld op 10 minuten en een record TTL heeft van 5 minuten, is de TTL voor de gecachede record verhoogd naar 10 minuten.

Aan de andere kant, als de TTL voor de opname is ingesteld op 15 minuten, slaat SWA de record 15 minuten in zijn cache op.

Soms is het echter nodig om het DNS-cache van vermeldingen te verwijderen. Corrupte of verlopen DNS-cacheingangen kunnen soms problemen veroorzaken met levering aan een externe host of hosts.

Dit probleem doet zich doorgaans voor nadat het apparaat offline is geweest in verband met een netwerkverplaatsing of een andere omstandigheid.

De DNS-cache wissen uit GUI

Stap 1. Netwerk kiezen in het bovenste menu

Stap 2. Kies DNS

Stap 3. Kies Clear DNS Cache

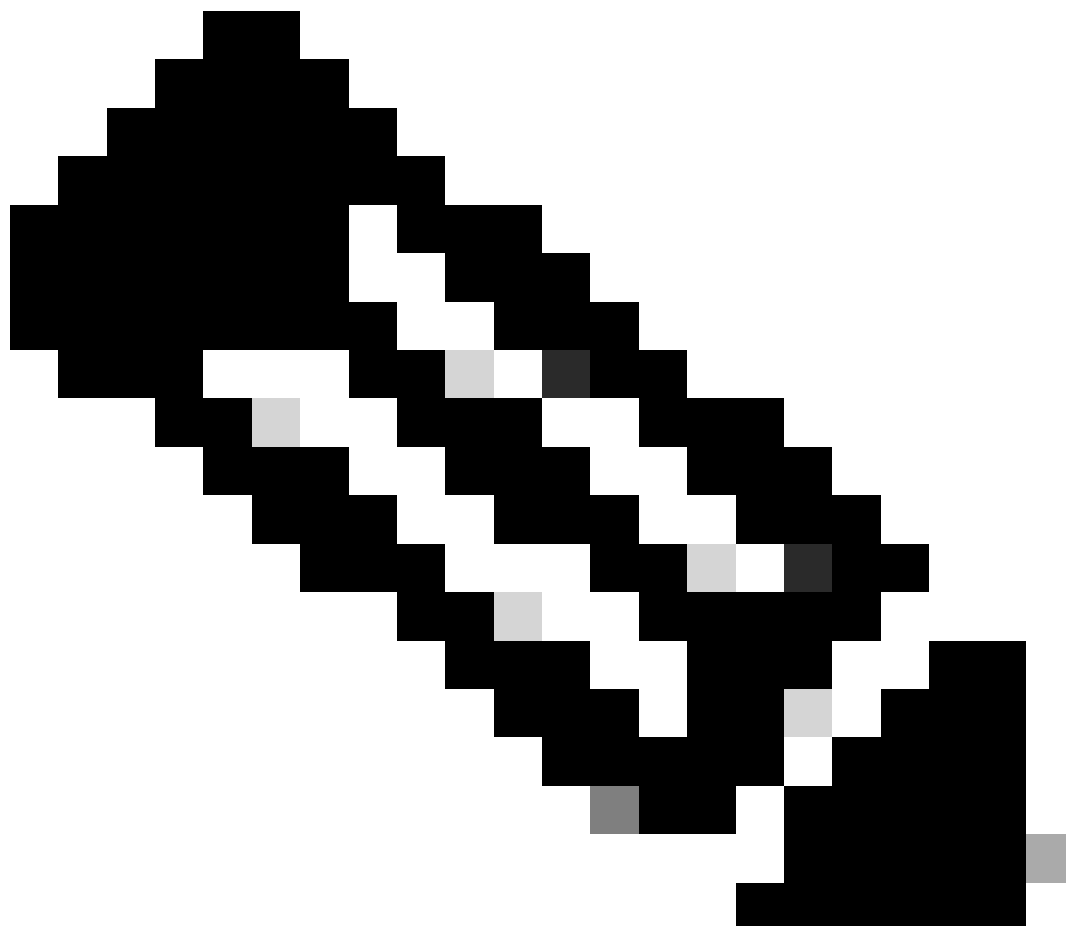
 Waarschuwing: deze opdracht kan een tijdelijke prestatievermindering veroorzaken terwijl de cache opnieuw wordt gevuld

De DNS-cache wissen uit CLI

Het DNS-cache in Cisco WAAS kan worden gewist door de opdracht dnsflushing uit de CLI.

DNS-cachegeheugen bekijken

Er is geen optie om cached DNS record in SWA van CLI of GUI te bekijken.



Opmerking: U kunt DNS-cache niet opvragen via nslookup.


Probleemoplossing voor DNS

DNS-logbestanden bekijken

Sommige logtypen die betrekking hebben op de webproxycomponent zijn niet ingeschakeld. Het belangrijkste logtype van de Webvolmacht, genoemd de "Logboeken Standaard van de Volmacht," wordt toegelaten door gebrek en vangt basisinformatie over alle modules van de Volmacht van het Web.

Elke Web Proxy module heeft ook een eigen logtype dat u handmatig kunt inschakelen zoals vereist.

Systeemlogbestanden, records, DNS, fouten en commit-activiteit. die standaard is ingeschakeld

 Tip: Als u het logniveau voor systeemlogbestanden wijzigt in DEBUG, kunt u de DNS-vragen en antwoorden zien. U kunt het logniveau wijzigen van GUI en CLI.

Logniveau van systeemlogbestanden wijzigen via GUI

Stap 1. Kies Systeembeheerders in het bovenste menu

Stap 2. Logabonnementen kiezen

Stap 3. Systeemlogbestanden kiezen

Stap 4. Kies DEBUG in het gedeelte Logniveau

Stap 5. Verzenden

Stap 6. Wijzigingen vastleggen

Edit DNS

DNS Server Settings																			
Primary DNS Servers:	<input checked="" type="radio"/> Use these DNS Servers <table border="1"><thead><tr><th>Priority ?</th><th>Server IP Address</th><th></th></tr></thead><tbody><tr><td><input type="text" value="0"/></td><td><input type="text" value="10.1.1.1"/></td><td></td></tr><tr><td><input type="text" value="1"/></td><td><input type="text" value="10.2.2.2"/></td><td></td></tr><tr><td><input type="text" value="2"/></td><td><input type="text" value="10.3.3.3"/></td><td></td></tr></tbody></table> <p>Alternate DNS servers Overrides (Optional): Add Row</p> <table border="1"><thead><tr><th>Domain(s)</th><th>DNS Server IP Address(es)</th><th></th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td><td></td></tr></tbody></table> <p><i>i.e., example.com, example2.com</i> <i>i.e., 10.0.0.3 or 2001:420:80:1::5</i></p>	Priority ?	Server IP Address		<input type="text" value="0"/>	<input type="text" value="10.1.1.1"/>		<input type="text" value="1"/>	<input type="text" value="10.2.2.2"/>		<input type="text" value="2"/>	<input type="text" value="10.3.3.3"/>		Domain(s)	DNS Server IP Address(es)		<input type="text"/>	<input type="text"/>	
Priority ?	Server IP Address																		
<input type="text" value="0"/>	<input type="text" value="10.1.1.1"/>																		
<input type="text" value="1"/>	<input type="text" value="10.2.2.2"/>																		
<input type="text" value="2"/>	<input type="text" value="10.3.3.3"/>																		
Domain(s)	DNS Server IP Address(es)																		
<input type="text"/>	<input type="text"/>																		
	<input type="radio"/> Use the Internet's Root DNS Servers <p>Alternate DNS servers Overrides (Optional): Add Row</p> <table border="1"><thead><tr><th>Domain</th><th>DNS Server IP Address</th><th></th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td><td></td></tr></tbody></table> <p>DNS Server FQDN <input type="text"/></p> <p><i>i.e., dns.example.com</i></p>	Domain	DNS Server IP Address		<input type="text"/>	<input type="text"/>													
Domain	DNS Server IP Address																		
<input type="text"/>	<input type="text"/>																		
Secondary DNS Servers:	<table border="1"><thead><tr><th>Priority ?</th><th>Server IP Address</th><th></th></tr></thead><tbody><tr><td><input type="text" value="0"/></td><td><input type="text" value="10.10.10.10"/></td><td></td></tr></tbody></table> <p>Add Row</p>	Priority ?	Server IP Address		<input type="text" value="0"/>	<input type="text" value="10.10.10.10"/>													
Priority ?	Server IP Address																		
<input type="text" value="0"/>	<input type="text" value="10.10.10.10"/>																		
Routing Table for DNS Traffic:	Management																		
IP Address Version Preference:	<input checked="" type="radio"/> Prefer IPv4 <input type="radio"/> Prefer IPv6 <input type="radio"/> Use IPv4 only <p><i>This preference applies when DNS results provide both IPv4 and IPv6 address for host. When selecting Prefer IPv4 or Prefer IPv6, ensure that the appliance network settings are configured appropriately to support IPv6.</i></p>																		
Secure DNS:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <p><i>SECURE DNS protects DNS data. It uses the DNSSEC protocol to strengthen the authentication in the DNS using digital signatures. If DNSSEC is enabled, fallback of DNSSEC query to DNS query will not occur. Supported DNSSEC Algorithms: DSA, DSA_NSEC3, ED448, ED25519, ECDSAP256SHA256, ECDSAP384SHA384, RSASHA1, RSASHA1_NSEC3, RSASHA256, RSASHA512.</i></p>																		
Wait Before Timing out Reverse DNS Lookups:	<input type="text" value="2"/> seconds																		
Domain Search List: ?	<input type="text"/> <p><i>Separate multiple entries with commas. Maximum allowed characters 2048.</i></p>																		

Cancel Submit

Afbeelding - Systeemlogbestanden wijzigen, niveau van logbestanden

Logniveau van systeemlogbestanden wijzigen van CLI

Stap 1. Inloggen op CLI

Stap 2. Type logconfiguratie

Stap 3. Kies BEWERKEN

Stap 4. Voer het nummer in dat aan System_Logs is gekoppeld

Stap 5. Druk op ENTER totdat u het logniveau bereikt

Stap 6. Kies nummer 4 wat voor Debug is

Stap 7. Druk op ENTER totdat u de wizard verlaat

Stap 8. Om wijzigingen op te slaan, typt commit.

```
SWA_CLI> logconfig


Currently configured logs:
...
42. "system_logs" Type: "System Logs" Retrieval: FTP Poll
...

Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- HOSTKEYCONFIG - Configure SSH host keys.
- AUDITLOGCONFIG - Adjust settings for audit logging.
[ ]> EDIT

Enter the number of the log you wish to edit:
[ ]> 42 <--- in this example the System_logs is number 42

Please enter the name for the log:
[system_logs]>

Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 4
....
SWA_CLI> commit
```

 Tip: Als u eenmaal problemen hebt opgelost, zorg er dan voor dat u het logniveau weer terugzet naar Informatie, anders zou er een grote belasting op de schijf Invoer / Uitvoer (I/O) en het logbestand zou worden ingevuld om snel.

raadpleging

Gebruik de opdracht nslookup om de reactie van de naamresolutie in SWA voor verschillende FQDN's te zien.

In dit voorbeeld, in de eerste poging om de naam van de TTL op te lossen wordt ingesteld op 30 minuten.

Bij de tweede poging, zien we dat de TTL minder dan 30 minuten is, wat aangeeft dat deze opname uit het cache is opgelost.

```
SWA_CLI> nslookup
```

```
Please enter the host or IP address to resolve.
```

```
[> cisco.com
```

```
Choose the query type:
```

1. A the host's IP address
2. AAAA the host's IPv6 address
3. CNAME the canonical name for an alias
4. MX the mail exchanger
5. NS the name server for the named zone
6. PTR the hostname if the query is an Internet address,

```
otherwise the pointer to other information
```

7. SOA the domain's "start-of-authority" information
8. TXT the text information

```
[1]> 1
```

```
A=10.20.3.15 TTL=30m
```

```
TSWA_CLI> nslookup
```

```
Please enter the host or IP address to resolve.
```

```
[> cisco.com
```

```
Choose the query type:
```

1. A the host's IP address
2. AAAA the host's IPv6 address
3. CNAME the canonical name for an alias
4. MX the mail exchanger
5. NS the name server for the named zone
6. PTR the hostname if the query is an Internet address,

```
otherwise the pointer to other information
```

7. SOA the domain's "start-of-authority" information
8. TXT the text information

```
[1]> 1
```

```
A=10.20.3.15 TTL=28m 49s
```

graven

dig is een andere nuttige opdracht om de DNS-records te bevragen. Met graven kunt u de broninterface of de DNS server specificeren waarin wij willen vragen:

In dit voorbeeld, hier is de vraag voor A-Record van server 10.1.1.1

```
dig @10.1.1.1 www.cisco.com A
```

```
; <<>> DiG 9.16.8 <<>> @10.1.1.1 www.cisco.com A
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58012
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1
```

```
;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 2cbc212c0877096701000000623db99b050bda7f896790e3 (good)
;; QUESTION SECTION:
;www.cisco.com.                IN      A

;; ANSWER SECTION:
www.cisco.com.                3600    IN      CNAME   origin-www.cisco.com.
www.cisco.com.                5       IN      A       10.20.3.15

;; Query time: 115 msec
;; SERVER: 10.1.1.1#53(10.1.1.1)
;; WHEN: Fri Mar 25 12:46:19 GMT 2022
;; MSG SIZE rcvd: 111
```

Het gebruik van graven:

```
dig [-s <source IP>] [-t] [-x <IP Address>] [@<IP address>] hostname [qtype]
```

Query a DNS server.

@<IP address> - Query the DNS server at this IP address

hostname - Record that you want to look up.

qtype - Query type: A, PTR, CNAME, MX, SOA, NS, TXT

options:

-s IP Address

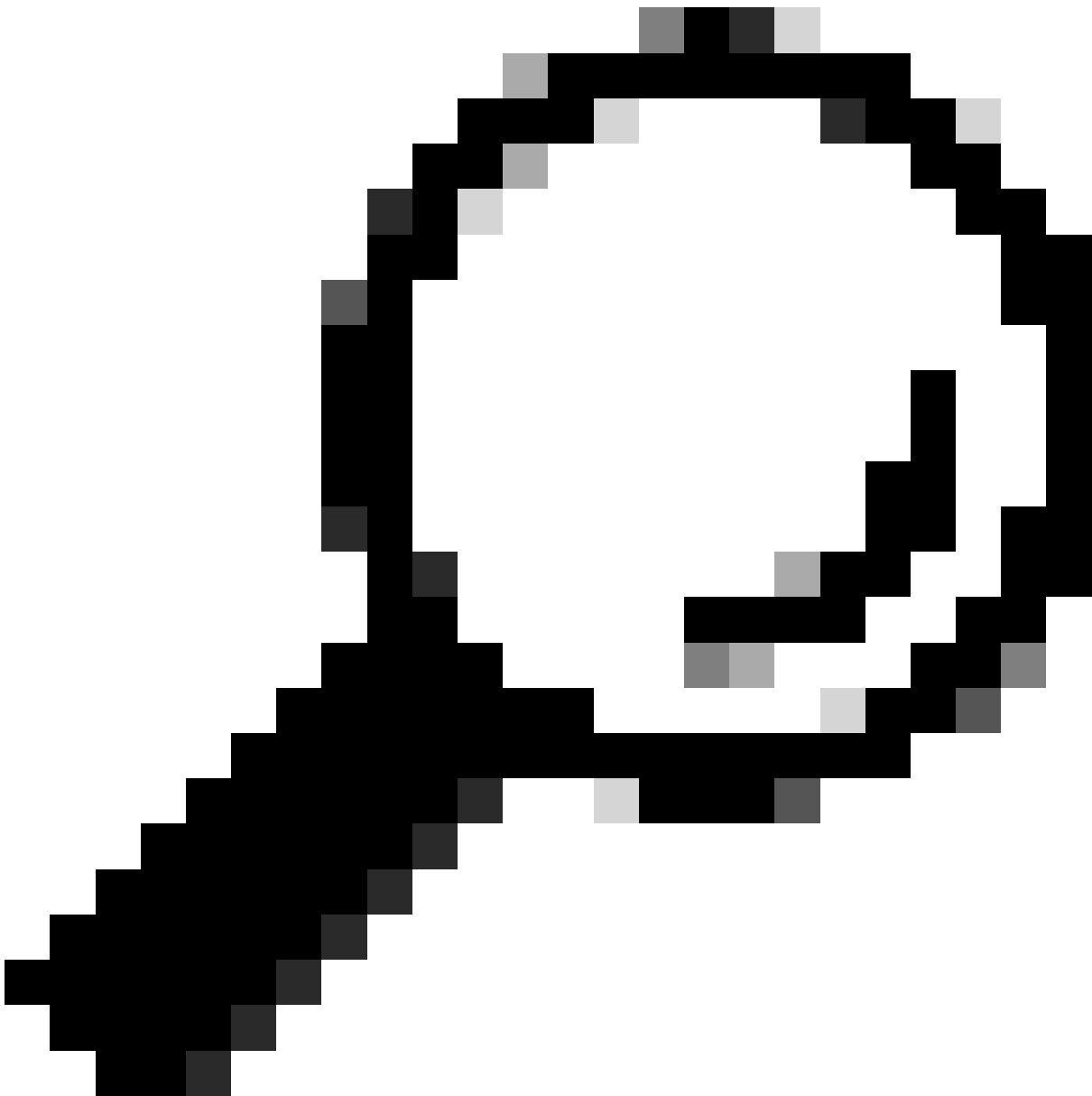
Specify the source IP address.

-t

Make query over tcp.

-x IP Address

Do a reverse lookup on this IP address.



Tip: U kunt kiezen uit de IP-bron om te kiezen uit welke interface u de naamresolutie wilt opvragen.

Langzame DNS-respons

Als het laden van alle of een aantal URL's een langere tijd in beslag nam (vergeleken met wanneer u dezelfde pagina vernieuwt), is het beter om de DNS-responstijd te controleren. Er zijn twee opties in SWA om de DNS reactietijd te controleren:

- Aangepast veld Access Logs configureren.
- Trackstatlogboeken.

Access logs wijzigen om DNS-statistieken te bekijken

U kunt Access logs wijzigen om DNS-tijd voor elk webverzoek te bekijken.

Stap 1. Log in op GUI.

Stap 2. Kies in het menu Systeembeheer de optie Logabonnementen.

Stap 3. Klik in de kolom Lognaam op toegangslogs of op de naam van de nieuwe naam. In dit voorbeeld, TAC_access_logs.

Stap 4. Plak in het gedeelte Aangepaste velden deze tekenreeks:

[DNS response = %:<d, DNS total = %:>d]

Stap 5. Verzend en leg veranderingen vast.

Aangepaste veldnaam	Aangepast veld	W3C-logs	Beschrijving
DNS-respons	%:<d	x-p2p-dns-wachttijd	Tijd genomen door de Web Proxy om het Domain Name Verzoek (DNS) verzoek naar het Web Proxy DNS proces te verzenden.
DNS totaal	%>d	x-p2p-dns-svc-tijd	Tijd genomen door het Web Proxy DNS proces om een DNS resultaat naar de Web Proxy terug te sturen.

Voor meer informatie hoe u aangepaste velden in Access logs kunt bewerken, gaat u naar deze link: [Configure Performance Parameter in Access Logs - Cisco](#)

Algemene DNS-responstijd in Trackstatlogboeken

U kunt statistieken van DNS-dienst en andere interne diensten in trackstatlogboeken bekijken. U kunt trackstats logbestanden benaderen door via FTP verbinding te maken met uw SWA.

In dit voorbeeld kunt u de cachestatistieken, en het aantal DNS reacties, gecategoriseerd door tijd die van DNS server is verstreken sinds SWA het laatst werd herstart zien.

...

INFO: DNS Cache Stats: Entries 662, Expire 1697, Hits 88739, Misses 664, Reclaims 0

...

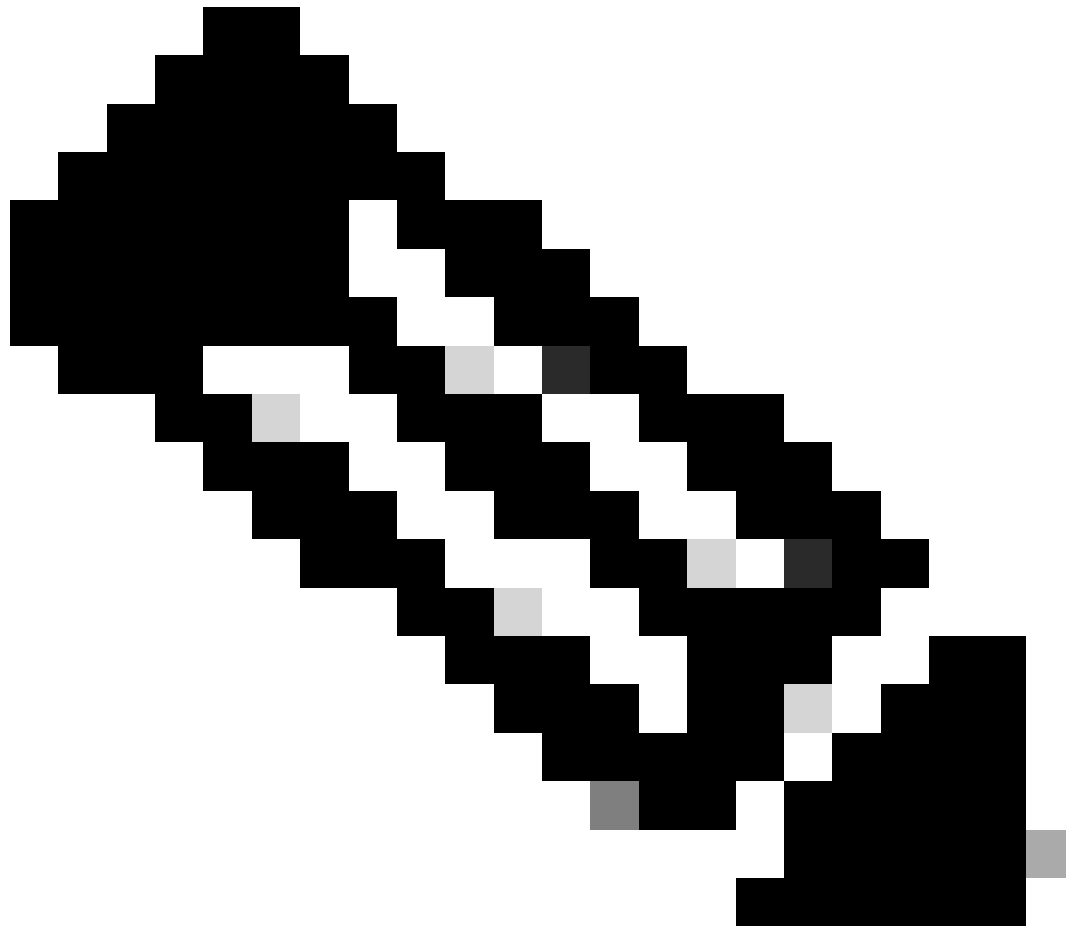
DNS Time	1.0 ms	349
DNS Time	1.6 ms	550
DNS Time	2.5 ms	374
DNS Time	4.0 ms	32
DNS Time	6.3 ms	35
DNS Time	10.0 ms	37
DNS Time	15.8 ms	301
DNS Time	25.1 ms	80
DNS Time	39.8 ms	136
DNS Time	63.1 ms	91
DNS Time	100.0 ms	12
DNS Time	158.5 ms	33
DNS Time	251.2 ms	14
DNS Time	398.1 ms	12
DNS Time	631.0 ms	45
DNS Time	1000.0 ms	120
DNS Time	1584.9 ms	73
DNS Time	2511.9 ms	296
DNS Time	3981.1 ms	265
DNS Time	6309.6 ms	190

Bijvoorbeeld, in de laatste lijn, wijst het erop dat 190 DNS vragen meer dan 6.309 milliseconden (ongeveer 6 seconden) namen te eindigen aangezien SWA het laatst werd herstart.

Om het exacte aantal in een tijdsperiode te weten te komen, moet u deze waarden aftrekken voor de begintijd en eindtijd.

Bijvoorbeeld, om de DNS reactietijd van 10:00 AM aan 11:00 AM te identificeren, verzamel statistieken voor 11:00 AM en trek hen van statistieken van 10:00 AM af.

Het resultaat is de DNS reactietijd van 10:00 AM tot 11:00 AM voor de gewenste datum.



Opmerking: de logbestanden met trackstatistieken worden elke 5 minuten verzameld.

PacketCapture

U kunt pakketten opnemen om de DNS-verzoeken en antwoorden te bekijken, om alleen voor DNS te filteren u kunt gebruiken: poort 53 .

Om pakketopname van GUI te starten:

Stap 1. Ondersteuning en Help kiezen rechtsboven

Stap 2. Packet Capture kiezen

Stap 3. (optioneel) Kies Instellingen bewerken om filter toe te voegen

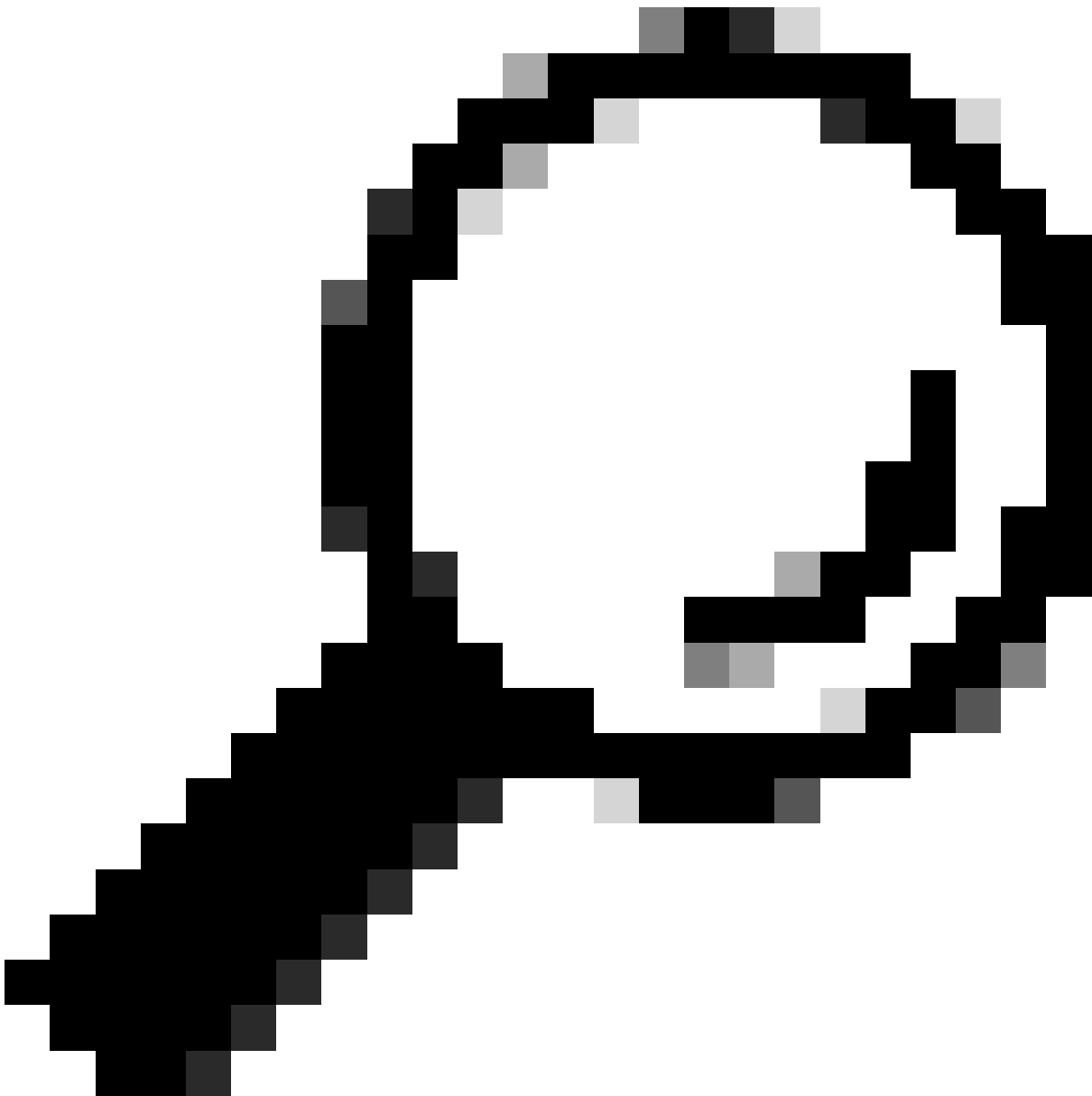
Stap 4. (optioneel) Kies uw interface(s) en type poort 53 in het gedeelte Aangepaste filter

Stap 5. (optioneel) Kies Verzenden

Edit Packet Capture Settings

Packet Capture Settings	
Capture File Size Limit: ?	<input type="text" value="200"/> MB <i>Maximum file size is 200MB</i>
Capture Duration:	<input type="radio"/> Run Capture Until File Size Limit Reached <input type="radio"/> Run Capture Until Time Elapsed Reaches <input type="text"/> (e.g. 120s, 5m 30s, 4h) <input checked="" type="radio"/> Run Capture Indefinitely
<i>The capture can be ended manually at any time; use the settings above to specify whether the capture should end automatically.</i>	
Interfaces:	<input checked="" type="checkbox"/> M1 <input type="checkbox"/> P1 <input type="checkbox"/> P2
Packet Capture Filters	
Filters:	<i>All filters are optional. Fields are not mandatory.</i>
	<input type="radio"/> No Filters <input type="radio"/> Predefined Filters ?
	Ports: <input type="text"/>
	Client IP: <input type="text"/>
	Server IP: <input type="text"/>
	<input checked="" type="radio"/> Custom Filter ? <input type="text" value="port 53"/>
<i>Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.</i>	

Afbeelding - Filter toevoegen om DNS-pakketten op te nemen



Tip: de Packet Capture instellingen zijn beschikbaar om direct te gebruiken wanneer ze worden verzonden. Verander deze instellingen permanent op om ze voor later gebruik op te slaan.

Stap 6. Kies Opname starten.

Stap 7. (Optioneel) Generate traffic, als u problemen moet met schieten specifieke site of URL-toegang.

Stap 8. Opname stoppen

Stap 9. Wacht tot de pagina is opgefrist en kies vervolgens de eerste pakketopname in de lijst "Packet Capture Files beheren".

Stap 10. Downloadbestand kiezen

L4TM

Layer 4 Traffic Monitor luistert naar netwerkverkeer dat via alle poorten op elke Secure Web-applicatie wordt geleverd en past domeinnamen en IP-adressen aan tegen vermeldingen in zijn eigen databasetabellen om te bepalen of inkomend en uitgaand verkeer moet worden toegestaan.

Wanneer interne clients zijn geïnfecteerd met malware en proberen te bellen naar huis via niet-standaard poorten en protocollen, voorkomt de L4 Traffic Monitor dat de activiteit van de telefoon-home het bedrijfsnetwerk verlaat.

Standaard is de L4 Traffic Monitor ingeschakeld en ingesteld om verkeer op alle poorten te bewaken, waaronder DNS en andere services.

Raadpleeg de gebruikershandleiding voor meer informatie over Layer 4 Traffic Monitor.

Fouten

Meldingspagina

Standaard toont SWA een meldingspagina om gebruikers te informeren dat ze zijn geblokkeerd en de reden voor de blokkering

Bestandsnaam en kennisgevingstitel: ERR_DNS_FAIL (DNS-fout)

Beschrijving: Foutpagina die wordt weergegeven wanneer de gevraagde URL een ongeldige domeinnaam bevat.

Melding Tekst: De hostname resolutie (DNS lookup) voor deze hostname <hostname > is mislukt.

Het internetadres kan verkeerd worden gespeld of verouderd, de host <hostname > kan tijdelijk niet beschikbaar zijn of de DNS server kan niet reageren.

Controleer de spelling van het opgegeven internetadres. Als het juist is, probeer dan later dit verzoek.

This Page Cannot Be Displayed

The host name resolution (DNS lookup) for this host name (invalidurl.cisco.com) has failed. The Internet address may be misspelled or obsolete, the host (invalidurl.cisco.com) may be temporarily unavailable, or the DNS server may be unresponsive.

Please check the spelling of the Internet address entered. If it is correct, try this request later.

If you have questions, please contact your organization's network administrator and provide the codes shown below.

Date: Sun, 02 Jul 2023 12:16:14 CEST

Username:

Source IP: 10.61.66.65

URL: GET http://invalidurl.cisco.com/

Category: Computers and Internet

Reason: UNKNOWN

Notification: DNS_FAIL

Afbeelding - DNS FAIL-fout

Resultaatcode van toegangsglogboek Geen

De codes van de transactieresultaten in het accessoire-bestand beschrijven hoe het apparaat clientverzoeken oplost. Als in de accessoire de Resultaatcode NIETS is betekent dit dat er een fout in transactie was. Bijvoorbeeld een DNS-fout of gateway-tijdelijke versie.

```
1688292974.527 20 10.61.66.65 NONE/503 0 GET http://invalidurl.cisco.com/ - NONE/invalidurl.cisco.com -
```

Opstarten van DNS-cache mislukt

Als er een waarschuwing met het bericht "De DNS-cache is niet opgestart" wordt gegenereerd wanneer een apparaat opnieuw wordt opgestart, betekent dit dat het systeem geen contact kan opnemen met de primaire DNS-servers.

Dit kan gebeuren tijdens de opstarttijd als het DNS-subsysteem online komt voordat de netwerkverbinding tot stand is gebracht. Als dit bericht op andere momenten verschijnt, kan het wijzen op netwerkproblemen of dat de DNS configuratie niet is ingesteld op een geldige server

Maximum aantal fouten bij het opvragen van DNS-server

Als een of meerdere DNS-servers geconfigureerd in SWA, niet terugantwoordden op DNS-vragen, beschouwen SWA deze als offline en zouden de DNS-vragen niet naar hen sturen voor vooraf

bepaalde tijd. Voor meer informatie, lees "Configure DNS from CLI" in dit artikel.

DNS_FAIL

Wanneer SWA een HTTP verzoek ontvangt en er niet in slaagt om de hostname op te lossen, zou SWA standaard een antwoord als als:

```
GET http://cisco HTTP/1.1
User-Agent: curl/7.19.7 (universal-apple-darwin10.0) libcurl/7.19.7 OpenSSL/0.9.8l zlib/1.2.3
Host: hostname
Accept: */*
Proxy-Connection: Keep-Alive
```

```
HTTP/1.1 307 Temporarily Moved for Domain Name Expansion
Mime-Version: 1.0
Date: Wed, 15 Sep 2022 13:05:02 EST
Proxy-Connection: keep-alive
Location: http://www.cisco.com/
Content-Length: 2068
```

Deze functie wordt "server name extension" genoemd.

WSA doet dit in pogingen dat omgeleid hostname de verwachte pagina voor de client zou oplossen.

U kunt "URL-formaat voor de HTTP 307-omleiding op DNS-lookup-fout" wijzigen, voor meer informatie review advancedproxyconfig sectie in dit artikel.

WSA behandelt DNS verzoek dat ServFail als mislukking terugkeert.

Bijvoorbeeld, NXDOMAIN zou "DNS_FAIL" in plaats van "SERVER_NAME_EXPANSION" teruggeven

Gerelateerde informatie

[Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web applicatie](#)

[Best practices voor beveiligde web applicatie gebruiken - Cisco](#)

[Cisco Content Hub - Inleiding tot het Domain Name System](#)

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.