

Fehlerbehebung beim DNS-Dienst der sicheren Webappliance

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[DNS-Konzept](#)

[DNS-Dienst in Proxy-Bereitstellungen](#)

[DNS-Einstellungen konfigurieren](#)

[Best Practices](#)

[Konfigurieren von DNS in der GUI](#)

[Konfigurieren von DNS über CLI](#)

[CLI-DNS-Befehle](#)

[Manuellen Datensatz erstellen](#)

[dnsflush](#)

[AdvancedProxyKonfiguration](#)

[DNS-Cache](#)

[DNS-Cache aus GUI löschen](#)

Einleitung

In diesem Dokument werden die Konfiguration des Domain Name Service (DNS) und die Fehlerbehebung in der Secure Web Appliance (SWA), vormals WSA, beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Installierte physische oder virtuelle Secure Web Appliance (SWA)
- Lizenz aktiviert oder installiert
- Secure Shell (SSH)-Client
- Der Setup-Assistent ist abgeschlossen.

- Administratorzugriff auf die SWA

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

DNS-Konzept

DNS ist das System im Internet, das Objektnamen (in der Regel Hostnamen) einer IP-Adresse (Internet Protocol) oder anderen Ressourceneinträgen zuordnet.

Der Namensraum des Internets ist in Domänen unterteilt, und die Verantwortung für die Verwaltung von Namen innerhalb jeder Domäne wird delegiert, in der Regel an Systeme innerhalb jeder Domäne.

Der Bereich für den Domänennamen ist in Bereiche unterteilt, die als Zonen bezeichnet werden und Delegierungspunkte in der DNS-Struktur darstellen.

Eine Zone enthält alle Domänen ab einem bestimmten Punkt nach unten, mit Ausnahme derjenigen, für die andere Zonen autoritativ sind.

Eine Zone verfügt normalerweise über einen autoritativen Namensserver, häufig über mehr als einen.

In einer Organisation können Sie viele Nameserver haben, aber Internet-Clients können nur die abfragen, die die Stammmamensserver kennen.

Die anderen Namensserver beantworten nur interne Abfragen.

DNS basiert auf einem Client-/Server-Modell. In diesem Modell speichern Namensserver Daten zu einem Teil der DNS-Datenbank und stellen diese Clients zur Verfügung, die den Namensserver im Netzwerk abfragen.

Namensserver sind Programme, die auf einem physischen Host ausgeführt werden und Zonendaten speichern. Als Administrator einer Domäne richten Sie einen Namensserver mit der Datenbank aller Ressourceneinträge (RRs) ein, die die Hosts in Ihrer Zone oder Ihren Zonen beschreiben

DNS-Dienst in Proxy-Bereitstellungen

In der expliziten Bereitstellung: Der Proxy führt DNS-Abfragen aus

In der transparenten Bereitstellung: DNS-Abfragen werden auf dem Client ausgeführt.

DNS-Einstellungen konfigurieren

Sie können DNS sowohl über die grafische Benutzeroberfläche (GUI) als auch über die

Befehlszeilenschnittstelle (CLI) konfigurieren.

AsyncOS für Web kann die Internet-Root-DNS-Server oder Ihre eigenen DNS-Server verwenden. Wenn SWA Internet-Root-Server verwenden, können Sie alternative Server für bestimmte Domänen angeben.

Da sich ein alternativer DNS-Server auf eine einzige Domäne bezieht, muss er für diese Domäne autoritär sein (endgültige DNS-Einträge angeben).

AsyncOS unterstützt Split-DNS, wobei interne Server für bestimmte Domänen und externe oder Root-DNS-Server für andere Domänen konfiguriert werden.

Wenn SWA einen lokalen DNS-Server verwenden, können wir auch Ausnahmedomänen und den zugehörigen DNS-Server angeben.

Best Practices

Aus Sicherheitsgründen muss jedes Netzwerk zwei DNS-Resolver hosten: einen für autoritative Datensätze innerhalb einer lokalen Domäne und einen für die rekursive Auflösung von Internet-Domänen.

Um dies zu ermöglichen, lassen die SWAs DNS-Server für bestimmte Domänen konfigurieren.

Wenn ein DNS-Server sowohl für lokale als auch für rekursive Abfragen verfügbar ist, sollten Sie die zusätzliche Last berücksichtigen, die sich ergeben würde, wenn sie für alle SWA-Abfragen verwendet wird.

Die bessere Option besteht darin, den internen Resolver für lokale Domänen und den Root-Internet-Resolver für externe Domänen zu verwenden. Dies hängt vom Risikoprofil und der Toleranz des Administrators ab.

Falls der primäre DNS-Server nicht verfügbar ist, müssen sekundäre DNS-Server konfiguriert werden. Wenn alle Server mit derselben Priorität konfiguriert werden, wird die Server-IP nach dem Zufallsprinzip ausgewählt.

Abhängig von der Anzahl der konfigurierten Server ist die Zeitüberschreitung für einen bestimmten Server unterschiedlich. Die Zeitüberschreitung für eine Abfrage ist in dieser Tabelle für bis zu sechs DNS-Server angegeben:

Anzahl der DNS-Server	Abfragetimeout (in der Sequenz)
1	60
2	5, 45

3	5, 10, 45
4	1, 3, 11, 45
5	1, 3, 11, 45, 1
6	1, 3, 11, 45, 1, 1

Weitere Informationen finden Sie unter [Cisco Web Security Appliance: Best Practices-Richtlinien - Cisco](#)

Konfigurieren von DNS in der GUI

Um DNS über die GUI zu konfigurieren, gehen Sie wie folgt vor:

Schritt 1: Wählen Sie Netzwerk aus dem Top-Menü

Schritt 2: DNS auswählen

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

Alternative DNS-Server-Überschreibungen (optional): Autoritative DNS-Server für Domänen

 Hinweis: AsyncOS berücksichtigt nicht die Versionseinstellungen für transparente FTP-Anforderungen.

 Hinweis: Im Cloud Connector-Modus unterstützt die Cisco Web Security Appliance nur IPv4.

Internet-Root-DNS-Server verwenden. Wählen Sie aus, dass die Internet-Root-DNS-Server für die Suche nach Domännennamen verwendet werden, wenn die Appliance keinen Zugriff auf DNS-Server in Ihrem Netzwerk hat.

Internet-Root-DNS-Server lösen lokale Hostnamen nicht auf.

 Hinweis: Wenn die Appliance lokale Hostnamen auflösen soll, verwenden Sie einen lokalen DNS-Server, oder fügen Sie dem lokalen DNS über die Befehlszeilenschnittstelle (CLI) die entsprechenden statischen Einträge hinzu.

Domain Search List (Domänensuchliste): Eine DNS-Domänensuchliste, die verwendet wird, wenn eine Anforderung an einen reinen Hostnamen (ohne Punkt ".") gesendet wird. ").

Die angegebenen Domänen können nacheinander in der eingegebenen Reihenfolge (Von links nach rechts) überprüft werden, um festzustellen, ob eine DNS-Übereinstimmung für den Hostnamen und die Domäne gefunden werden kann.

Routingtable für DNS-Datenverkehr: Gibt an, über welche Schnittstelle der DNS-Dienst den Datenverkehr weiterleitet.

Wait Before Timing out Reverse DNS Lookups: Die Wartezeit in Sekunden vor dem Timeout bei nicht reagierenden Reverse DNS Lookups.

Die sekundären DNS-Server empfangen Hostnamenabfragen, wenn die primären DNS-Server folgende Fehler zurückgeben:

- Kein Fehler, kein Antwortabschnitt erhalten
 - Server konnte Anfrage nicht abschließen, Abschnitt "Keine Antwort"
 - Namensfehler, kein Antwortabschnitt erhalten
 - Funktion nicht implementiert
 - Server weigert sich Abfrage zu beantworten
-

 Hinweis: AsyncOS evaluiert Transaktionen auf Basis von Richtlinien, bevor es externe Abhängigkeiten evaluiert, um unnötige externe Kommunikation von der Appliance zu vermeiden. Wenn beispielsweise eine Transaktion aufgrund einer Richtlinie blockiert wird, die nicht kategorisierte URLs blockiert, schlägt die Transaktion nicht aufgrund eines DNS-

 Fehlers fehl.

Priorität: Ein Wert von 0 hat die höchste Priorität. Eine zufällige IP wird ausgewählt, wenn beide dieselbe Priorität haben.

Konfigurieren von DNS über CLI

Sie können `dnsconfig` über die CLI zum Konfigurieren der DNS-Einstellungen verwenden.

Schritt 1: Geben Sie `dnsconfig` in CLI ein:

```
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.

```
[>
```

Schritt 2: Um der Liste einen neuen DNS-Server hinzuzufügen, geben Sie `NEW` ein, und drücken Sie die Eingabetaste.

Schritt 3: Wählen Sie zwischen primären DNS-Nameservern oder sekundären DNS-Nameservern aus, denen Sie einen neuen Nameserver hinzufügen möchten.

```
[> 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
```

Schritt 4: Wählen Sie diese Option aus, um einen neuen Namenserver oder einen alternativen Domänenserver hinzuzufügen (Domänenname für die bedingte Weiterleitung).

```
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

Schritt 5: Geben Sie die IP-Adresse des neuen Namensservers ein.

Schritt 6: Geben Sie die Priorität für den neu hinzugefügten Namensserver an.

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:

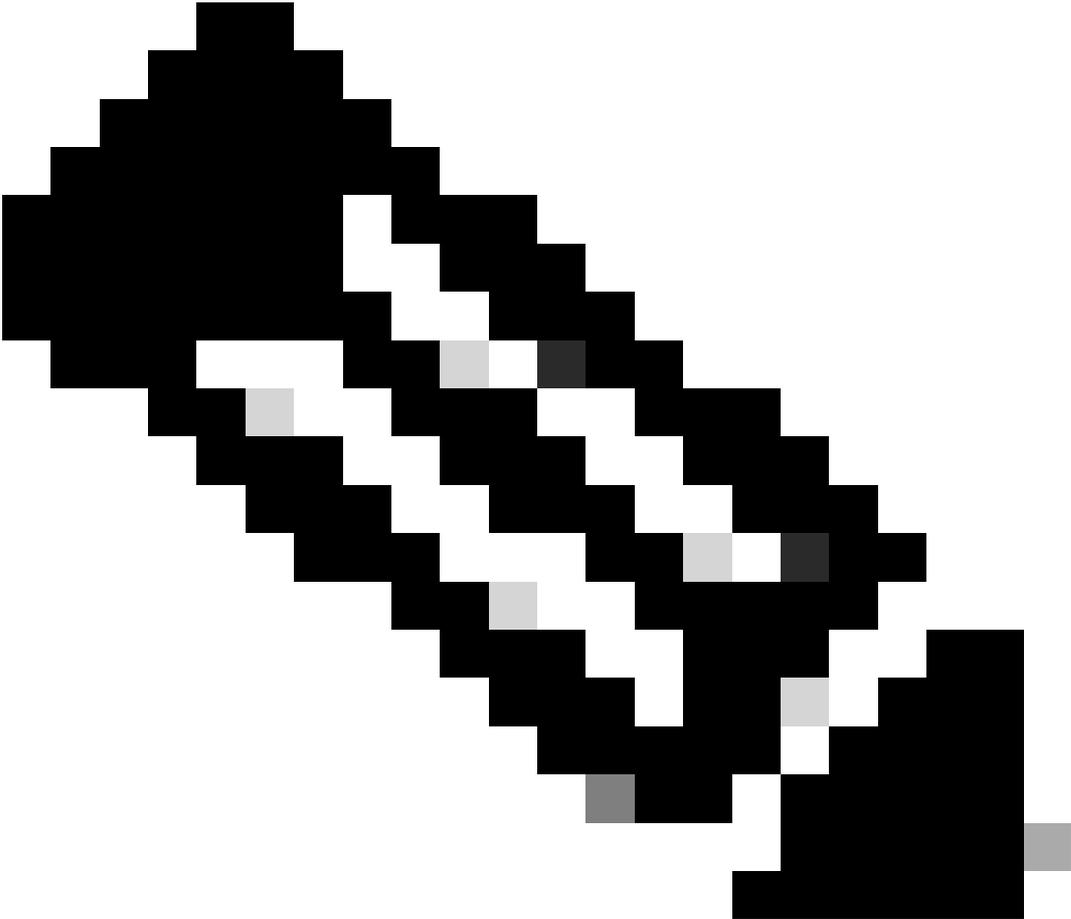
1. Priority: 0 10.1.1.1
2. Priority: 1 10.2.2.2
3. Priority: 2 10.3.3.3
4. Priority: 4 10.4.4.4

Currently using the following Secondary DNS cache servers :

1. Priority: 0 10.10.10.10

Schritt 7. Drücken Sie die Eingabetaste, um den Assistenten zu beenden.

Schritt 8: Geben Sie commit ein, um die Änderungen zu speichern.



Hinweis: Um Namensserver zu bearbeiten oder zu löschen, können Sie EDIT und DELETE aus dnsconfig auswählen.

Über die SETUP-Option können Sie die DNS-Cache-Zeit und die Offline-DNS-Erkennungseinstellungen konfigurieren:

```
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 Sekunden für den DNS-Cache: Mit dieser Option wird die minimale Anzahl von Sekunden konfiguriert, die SWA in einem Datensatz zwischengespeichert hat. Weitere Informationen finden Sie im Abschnitt zum DNS-Cache in diesem Dokument.

Geben Sie die Anzahl der fehlgeschlagenen Versuche ein, bevor ein lokaler DNS-Server offline geschaltet wird: Wenn der DNS-Server nicht auf DNS-Abfragen antwortet, wird der Zähler gestartet.

Wenn dieser definierte Wert erreicht wird, wird dieser Namenserver als Offline-DNS-Server betrachtet, und SWA vermeidet es, die DNS-Abfrage für einen vordefinierten Zeitraum an diesen Namenserver zu senden (Option "Weiter").

Wenn der DNS-Server als offline markiert ist, wird die folgende Fehlermeldung angezeigt:

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

Geben Sie das Intervall in Sekunden für das Polling eines lokalen Offline-DNS-Servers ein: Wenn ein als offline markierter DNS-Server nach diesem Zeitintervall (in Sekunden) beginnt, sendet SWA eine DNS-Abfrage an diesen Nameserver, und der Zähler für die fehlgeschlagene Antwort des DNS-Servers wird auf Null zurückgesetzt.

CLI-DNS-Befehle

Manuellen Datensatz erstellen

Um manuell "A record" zu erstellen, können Sie die Hosts-Datei nicht benutzen oder bearbeiten. Sie können den ausgeblendeten Befehl localhosts aus dnsconfig in der CLI verwenden.

Hinweis: Sie müssen die Änderungen bestätigen, nachdem Sie diese Konfigurationen geändert haben.

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

dnsflush

dnsflush entfernt alle zwischengespeicherten DNS-Einträge aus der DNS-Cachetabelle:

SWA_CLI> dnsflush

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

AdvancedProxyKonfiguration

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]>

Der HTTP 307-Statuscode (Temporary Redirect) gibt an, dass sich die Zielressource vorübergehend unter einem anderen URI (Uniform Resource Identifier) befindet, und der Benutzer-Agent DARF die Anforderungsmethode NICHT ändern, wenn er eine automatische Umleitung zu diesem URI durchführt. Da sich die Umleitung im Laufe der Zeit ändern kann, muss der Client weiterhin den ursprünglichen effektiven Anforderungs-URI verwenden.

Weitere Informationen zu : [Was ist der HTTP 307 Temporary Redirect Status Code - Kinsta](#)

Diese Optionen steuern, wie die SWA bei der Auswertung einer Clientanforderung in einer transparenten Proxy-Bereitstellung die IP-Adresse für die Verbindung festlegt. Wenn eine Anforderung empfangen wird, wird der WSA eine Ziel-IP-Adresse und ein Hostname angezeigt. Die SWA müssen entscheiden, ob sie der ursprünglichen Ziel-IP-Adresse für die TCP-Verbindung vertrauen oder ob sie eine eigene DNS-Auflösung durchführen und die aufgelöste Adresse verwenden möchten. Der Standardwert ist "0 = DNS-Antworten immer in der richtigen Reihenfolge verwenden", was bedeutet, dass SWA dem Client nicht vertraut, um die IP-Adresse anzugeben.

Option 1: SWA probiert die vom Client für die Verbindung angegebene IP-Adresse aus, greift jedoch auf die aufgelöste Adresse zurück, wenn dies fehlschlägt. Die aufgelöste Adresse wird für die Richtlinienbewertung verwendet (Webkategorie, Webreputation usw.).

Option 2: SWA verwendet nur die vom Kunden angegebene Adresse für die Verbindung und greift nicht zurück. Die aufgelöste Adresse wird für die Richtlinienbewertung verwendet (Webkategorie, Webreputation usw.).

Option 3: SWA verwendet nur die vom Kunden angegebene Adresse für die Verbindung und greift nicht zurück. Die vom Client bereitgestellte IP-Adresse wird für die Richtlinienbewertung verwendet (Webkategorie, Webreputation usw.).

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

DNS-Cache

Zur Steigerung von Effizienz und Leistung speichert Cisco SWA DNS-Einträge für Domänen, mit

denen Sie kürzlich eine Verbindung hergestellt haben. Mithilfe des DNS-Caches kann SWA exzessive DNS-Lookups derselben Domänen vermeiden. Die DNS-Cacheeinträge laufen aufgrund der TTL (Time to Live) des Datensatzes ab.

Wenn die TTL des Eintrags im DNS-Server größer ist als die TTL-Zeit des SWA dnsconfig cache, verwendet dns cache die TTL des DNS-Servers.

Wenn die TTL des Eintrags im DNS-Server kürzer als die TTL-Zeit des SWA dnsconfig cache ist, verwendet dns cache die TTL-Einstellung von WSA dnsconfig.

 Achtung: SWA haben zwei DNS-Cache, einer ist für den Proxy-Prozess konzipiert, der andere wird für den internen Prozess verwendet.

Standardmäßig zwischengespeicherte DNS-Einträge vom SWA für mindestens 30 Minuten, unabhängig vom Datensatz-TTL. Moderne Websites, die Content Delivery Networks (CDN) intensiv nutzen, verfügen aufgrund der häufigen Änderung ihrer IP-Adressen über niedrige TTL-Werte.

Dies kann dazu führen, dass ein Client eine IP-Adresse für einen bestimmten Server zwischenspeichert und SWA eine andere Adresse für denselben Server zwischenspeichert. Um dem entgegenzuwirken, kann die Standard-TTL von SWA vom Abschnitt SETUP im CLI-Befehl dsnconfig auf fünf Minuten herabgesetzt werden.

Wenn beispielsweise die "minimale TTL in Sekunden für den DNS-Cache" in der DNS-Konfiguration auf 10 Minuten festgelegt wurde und ein Datensatz eine TTL von 5 Minuten hat, wurde die TTL für den zwischengespeicherten Datensatz auf 10 Minuten erhöht.

Wenn dagegen die TTL für den Datensatz auf 15 Minuten festgelegt ist, speichert SWA den Datensatz 15 Minuten lang in seinem Cache.

Manchmal ist es jedoch erforderlich, den DNS-Cache von Einträgen zu löschen. Beschädigte oder abgelaufene DNS-Cache-Einträge können gelegentlich zu Problemen bei der Zustellung an einen oder mehrere Remotehosts führen.

Dieses Problem tritt in der Regel dann auf, wenn die Appliance aufgrund einer Netzwerkverschiebung oder anderer Umstände offline war.

DNS-Cache aus GUI löschen

Schritt 1: Wählen Sie Netzwerk aus dem Top-Menü

Schritt 2: DNS auswählen

Schritt 3: DNS-Cache löschen auswählen

 Achtung: Dieser Befehl kann eine vorübergehende Leistungsminderung verursachen,

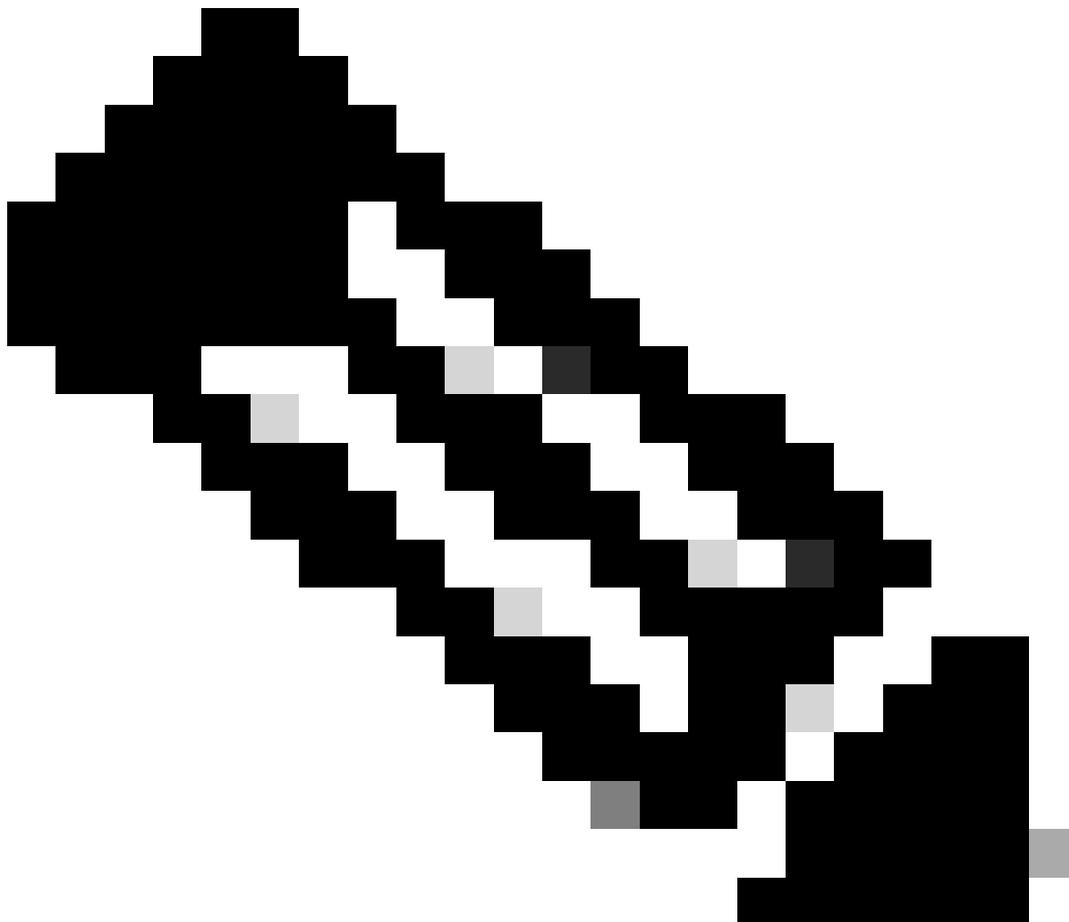
⚠ während der Cache neu aufgefüllt wird.

Löschen des DNS-Cache aus der CLI

Der DNS-Cache in der Cisco WSA kann über den Befehl `dnsflush` in der CLI gelöscht werden.

DNS-Cache anzeigen

Es gibt keine Option zum Anzeigen eines zwischengespeicherten DNS-Eintrags in SWA über die CLI oder GUI.



Hinweis: Sie können den DNS-Cache nicht über `nslookup` abfragen.

Fehlerbehebung bei DNS

DNS-Protokolle anzeigen

Einige Protokolltypen, die sich auf die Webproxykomponente beziehen, sind nicht aktiviert. Der Hauptprotokolltyp des Webproxys, der als "Standardproxyprotokolle" bezeichnet wird, ist standardmäßig aktiviert und erfasst grundlegende Informationen zu allen Webproxymodulen.

Jedes Webproxy-Modul verfügt außerdem über einen eigenen Protokolltyp, den Sie nach Bedarf manuell aktivieren können.

System Logs (Systemprotokolle), Records DNS (DNS), error (Fehler) und commit activity. (diese Option ist standardmäßig aktiviert)

 Tipp: Wenn Sie die Protokollstufe für Systemprotokolle auf DEBUG ändern, werden die DNS-Abfragen und -Antworten angezeigt. Sie können die Protokollstufe über die grafische Benutzeroberfläche und die Kommandozeile ändern.

Ändern der Protokollebene der Systemprotokolle von der GUI

Schritt 1: Wählen Sie Systemadministratoren aus dem Hauptmenü

Schritt 2: Protokoll-Subscriptions auswählen

Schritt 3: Systemprotokolle auswählen

Schritt 4: Wählen Sie DEBUG im Abschnitt Log Level (Protokollstufe) aus.

Schritt 5: Senden

Schritt 6: Änderungen bestätigen

Edit DNS

DNS Server Settings

Primary DNS Servers:	<input checked="" type="radio"/> Use these DNS Servers <table border="1" style="width: 100%; border-collapse: collapse; margin-top: 5px;"> <thead> <tr> <th style="width: 10%;">Priority ?</th> <th style="width: 70%;">Server IP Address</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">0</td> <td>10.1.1.1</td> <td style="text-align: center;">🗑️</td> </tr> <tr> <td style="text-align: center;">1</td> <td>10.2.2.2</td> <td style="text-align: center;">🗑️</td> </tr> <tr> <td style="text-align: center;">2</td> <td>10.3.3.3</td> <td style="text-align: center;">🗑️</td> </tr> </tbody> </table> <div style="margin-top: 5px;"> Alternate DNS servers Overrides (Optional): Add Row <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Domain(s)</td> <td style="width: 40%;">DNS Server IP Address(es)</td> <td style="width: 10%;"></td> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td style="text-align: center;">🗑️</td> </tr> <tr> <td><small><i>i.e., example.com, example2.com</i></small></td> <td><small><i>i.e., 10.0.0.3 or 2001:420:80:1::5</i></small></td> <td></td> </tr> </table> </div>	Priority ?	Server IP Address		0	10.1.1.1	🗑️	1	10.2.2.2	🗑️	2	10.3.3.3	🗑️	Domain(s)	DNS Server IP Address(es)		<input type="text"/>	<input type="text"/>	🗑️	<small><i>i.e., example.com, example2.com</i></small>	<small><i>i.e., 10.0.0.3 or 2001:420:80:1::5</i></small>	
Priority ?	Server IP Address																					
0	10.1.1.1	🗑️																				
1	10.2.2.2	🗑️																				
2	10.3.3.3	🗑️																				
Domain(s)	DNS Server IP Address(es)																					
<input type="text"/>	<input type="text"/>	🗑️																				
<small><i>i.e., example.com, example2.com</i></small>	<small><i>i.e., 10.0.0.3 or 2001:420:80:1::5</i></small>																					
	<input type="radio"/> Use the Internet's Root DNS Servers <div style="margin-top: 5px;"> Alternate DNS servers Overrides (Optional): Add Row <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%;">Domain</td> <td style="width: 40%;">DNS Server IP Address</td> <td style="width: 10%;"></td> </tr> <tr> <td><input type="text"/></td> <td><input type="text"/></td> <td style="text-align: center;">🗑️</td> </tr> <tr> <td colspan="2">DNS Server FQDN</td> <td></td> </tr> <tr> <td colspan="2"><input type="text"/></td> <td></td> </tr> <tr> <td colspan="3"><small><i>i.e., dns.example.com</i></small></td> </tr> </table> </div>	Domain	DNS Server IP Address		<input type="text"/>	<input type="text"/>	🗑️	DNS Server FQDN			<input type="text"/>			<small><i>i.e., dns.example.com</i></small>								
Domain	DNS Server IP Address																					
<input type="text"/>	<input type="text"/>	🗑️																				
DNS Server FQDN																						
<input type="text"/>																						
<small><i>i.e., dns.example.com</i></small>																						
Secondary DNS Servers:	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 10%;">Priority ?</th> <th style="width: 70%;">Server IP Address</th> <th style="width: 20%;"></th> </tr> </thead> <tbody> <tr> <td style="text-align: center;">0</td> <td>10.10.10.10</td> <td style="text-align: center;">🗑️</td> </tr> </tbody> </table>	Priority ?	Server IP Address		0	10.10.10.10	🗑️															
Priority ?	Server IP Address																					
0	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 <small><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></small>																					
Secure DNS:	<input type="radio"/> Enable <input checked="" type="radio"/> Disable <small><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></small>																					
Wait Before Timing out Reverse DNS Lookups:	<input type="text" value="2"/> seconds																					
Domain Search List: ?	<input style="width: 100%;" type="text"/> <small><i>Separate multiple entries with commas. Maximum allowed characters 2048.</i></small>																					

Cancel
Submit

Image - Ändern der Systemprotokolle, Protokollebene

Ändern der Protokollstufe der Systemprotokolle von CLI

Schritt 1: Bei CLI anmelden

Schritt 2: Typ logconfig

Schritt 3: BEARBEITEN auswählen

Schritt 4: Geben Sie die Nummer ein, die System_Logs zugeordnet ist.

Schritt 5: Drücken Sie die Eingabetaste, bis die Protokollstufe erreicht ist.

Schritt 6: Wählen Sie die Nummer 4 für "Debug" aus.

Schritt 7. Drücken Sie die Eingabetaste, bis Sie den Assistenten beenden.

Schritt 8: Geben Sie commit ein, um die Änderungen zu speichern.

```
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
```

 Tipp: Nachdem Sie die Fehlerbehebung durchgeführt haben, stellen Sie sicher, dass Sie die Protokollstufe wieder auf Information ändern, da sonst die Eingabe/Ausgabe (I/O) des Datenträgers sehr stark belastet und die Protokolldatei zu schnell aufgefüllt würde.

nslookup

Verwenden Sie den Befehl nslookup, um die Antwort zur Namensauflösung in SWA für verschiedene FQDNs anzuzeigen.

In diesem Beispiel wird beim ersten Versuch, den Namen aufzulösen, die TTL auf 30 Minuten festgelegt.

Beim zweiten Versuch sehen wir, dass die TTL weniger als 30 Minuten beträgt, was darauf hinweist, dass dieser Datensatz aus dem Cache aufgelöst wurde.

```
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
```

graben

dig ist ein weiterer nützlicher Befehl zum Abfragen der DNS-Einträge. Mit dig können Sie die Quellschnittstelle oder den DNS-Server angeben, in dem die Abfrage erfolgen soll:

In diesem Beispiel ist dies die Abfrage für den A-Datensatz vom 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
```

Die Verwendung von dig:

```
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

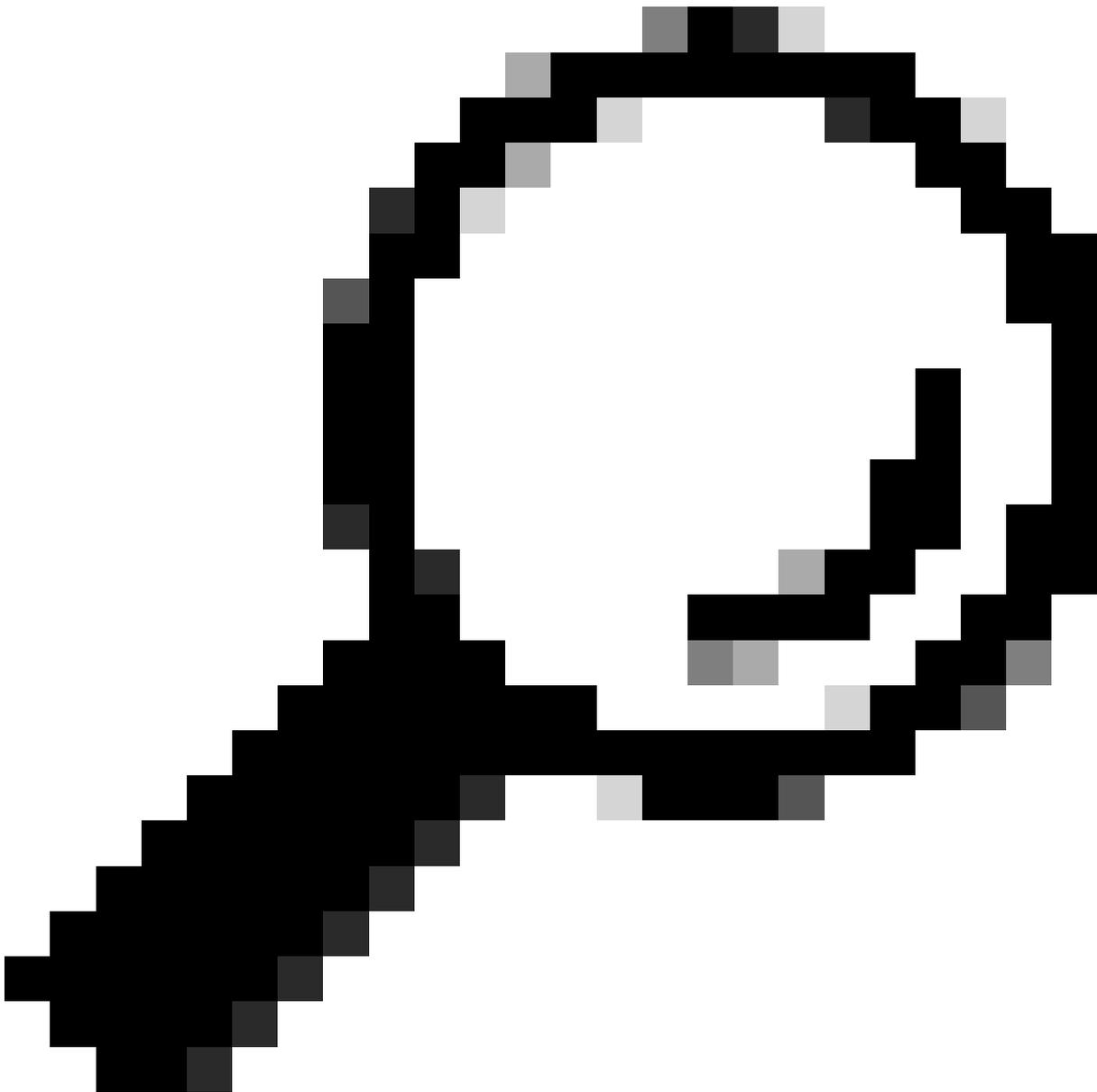
Specify the source IP address.

-t

Make query over tcp.

-x IP Address

Do a reverse lookup on this IP address.



Tipp: Sie können die Quell-IP auswählen, um die Schnittstelle auszuwählen, von der Sie die Namensauflösung abfragen möchten.

Langsame DNS-Antwort

Wenn das Laden aller oder einiger URLs länger dauerte (im Vergleich zum Aktualisieren derselben Seite), ist es besser, die DNS-Antwortzeit zu überprüfen. In SWA gibt es zwei Optionen zum Überprüfen der DNS-Antwortzeit:

- Konfigurieren des benutzerdefinierten Felds AccessLogs
- Trackstat-Protokolle.

Ändern von Zugriffsprotokollen zum Anzeigen von DNS-Statistiken

Sie können die Zugriffsprotokolle ändern, um die DNS-Zeit für jede Webanforderung anzuzeigen.

Schritt 1: Melden Sie sich bei GUI an.

Schritt 2: Wählen Sie im Menü Systemverwaltung die Option Protokoll-Subscriptions aus.

Schritt 3: Klicken Sie in der Spalte "Protokollname" auf Accesslogs oder den Namen des neu erstellten. In diesem Beispiel ist dies TAC_access_logs.

Schritt 4. Fügen Sie im Abschnitt Benutzerdefinierte Felder folgende Zeichenfolge ein:

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

Schritt 5: Änderungen übermitteln und bestätigen.

Name des benutzerdefinierten Felds	Benutzerdefiniertes Feld	W3C-Protokolle	Beschreibung
DNS-Antwort	%:<d	x-p2p-dns-wartezeit	Die Zeit, die der Webproxy benötigt, um die DNS-Anforderung (Domain Name Request) an den Webproxy-DNS-Prozess zu senden.
DNS gesamt	%:>d	x-p2p-dns-svc-zeit	Die Zeit, die der Webproxy-DNS-Prozess benötigt, um ein DNS-Ergebnis an den Webproxy zurückzusenden.

Weitere Informationen zum Bearbeiten benutzerdefinierter Felder in Access Logs finden Sie unter diesem Link: [Configure Performance Parameter in Access Logs \(Leistungsparameter konfigurieren\) - Cisco](#)

Allgemeine DNS-Reaktionszeit in Trackstat-Protokollen

Sie können Statistiken des DNS-Dienstes und anderer interner Dienste in Trackstat-Protokollen anzeigen. Sie können auf Trackstats-Protokolle zugreifen, indem Sie sich über FTP mit Ihrem SWA verbinden.

In diesem Beispiel sehen Sie die Cache-Statistiken und die Anzahl der DNS-Antworten, die nach der Zeit kategorisiert sind, die seit dem letzten Neustart von SWA vom DNS-Server vergangen ist.

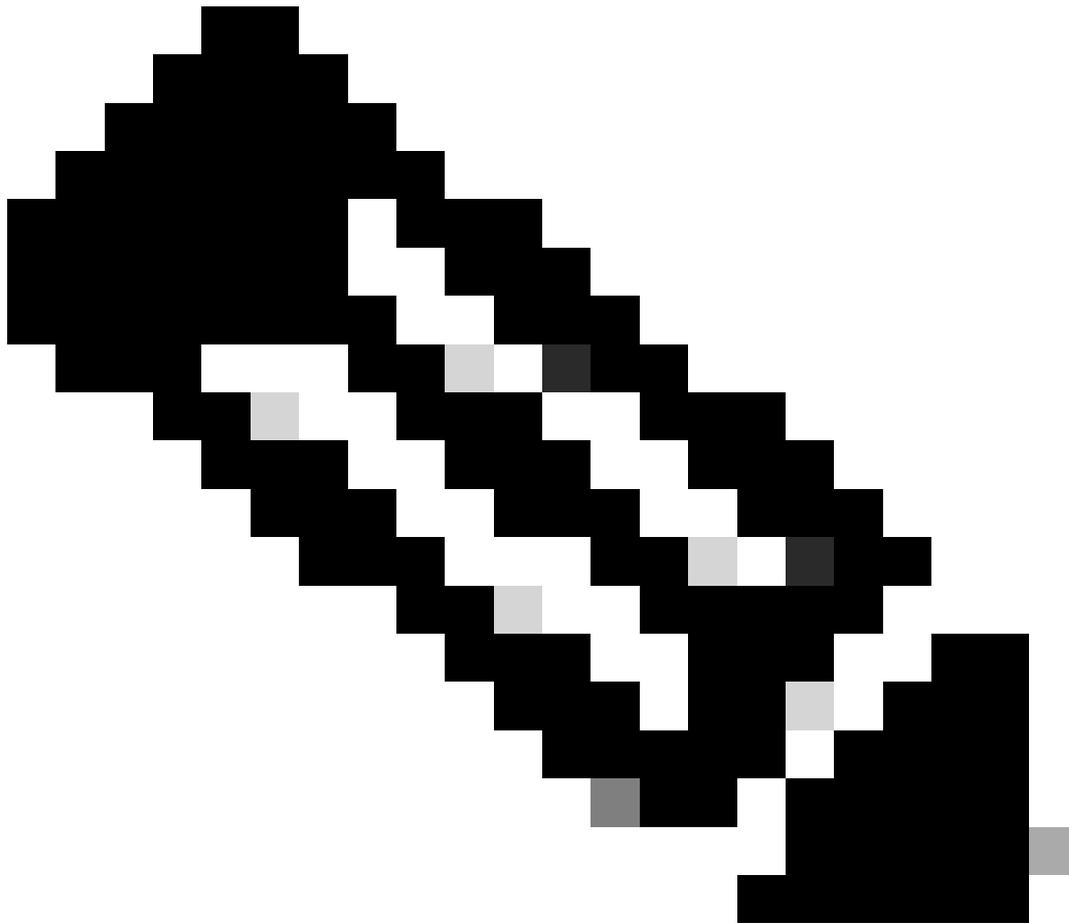
```
...
INFO: DNS Cache Stats: Entries 662, Expire 1697, Hits 88739, Misses 664, Reclaims 0
...
DNS Time      1.0 ms    349
DNS Time      1.6 ms    550
DNS Time      2.5 ms    374
DNS Time      4.0 ms     32
DNS Time      6.3 ms     35
DNS Time     10.0 ms     37
DNS Time     15.8 ms    301
DNS Time     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
```

In der letzten Zeile steht beispielsweise, dass 190 DNS-Abfragen seit dem letzten Neustart von SWA mehr als 6.309 Millisekunden (ca. 6 Sekunden) gedauert haben.

Um die genaue Anzahl in einem Zeitraum zu ermitteln, ziehen Sie diese Werte für die Startzeit und die Endzeit ab.

Wenn Sie beispielsweise die DNS-Reaktionszeit von 10:00 Uhr bis 11:00 Uhr ermitteln möchten, sammeln Sie die Statistiken für 11:00 Uhr, und ziehen Sie sie von den Statistiken für 10:00 Uhr ab.

Das Ergebnis ist die DNS-Reaktionszeit von 10:00 Uhr bis 11:00 Uhr für das gewünschte Datum.



Hinweis: Track-Statistikprotokolle werden alle 5 Minuten gesammelt.

Paketerfassung

Sie können Pakete erfassen, um die DNS-Anfragen und -Antworten anzuzeigen und nur nach DNS zu filtern, den Sie verwenden können: Port 53 .

So starten Sie die Paketerfassung über die GUI:

Schritt 1: Wählen Sie Support und Hilfe von oben rechts.

Schritt 2: Paketerfassung auswählen

Schritt 3. (Optional) Wählen Sie Einstellungen bearbeiten, um Filter hinzuzufügen

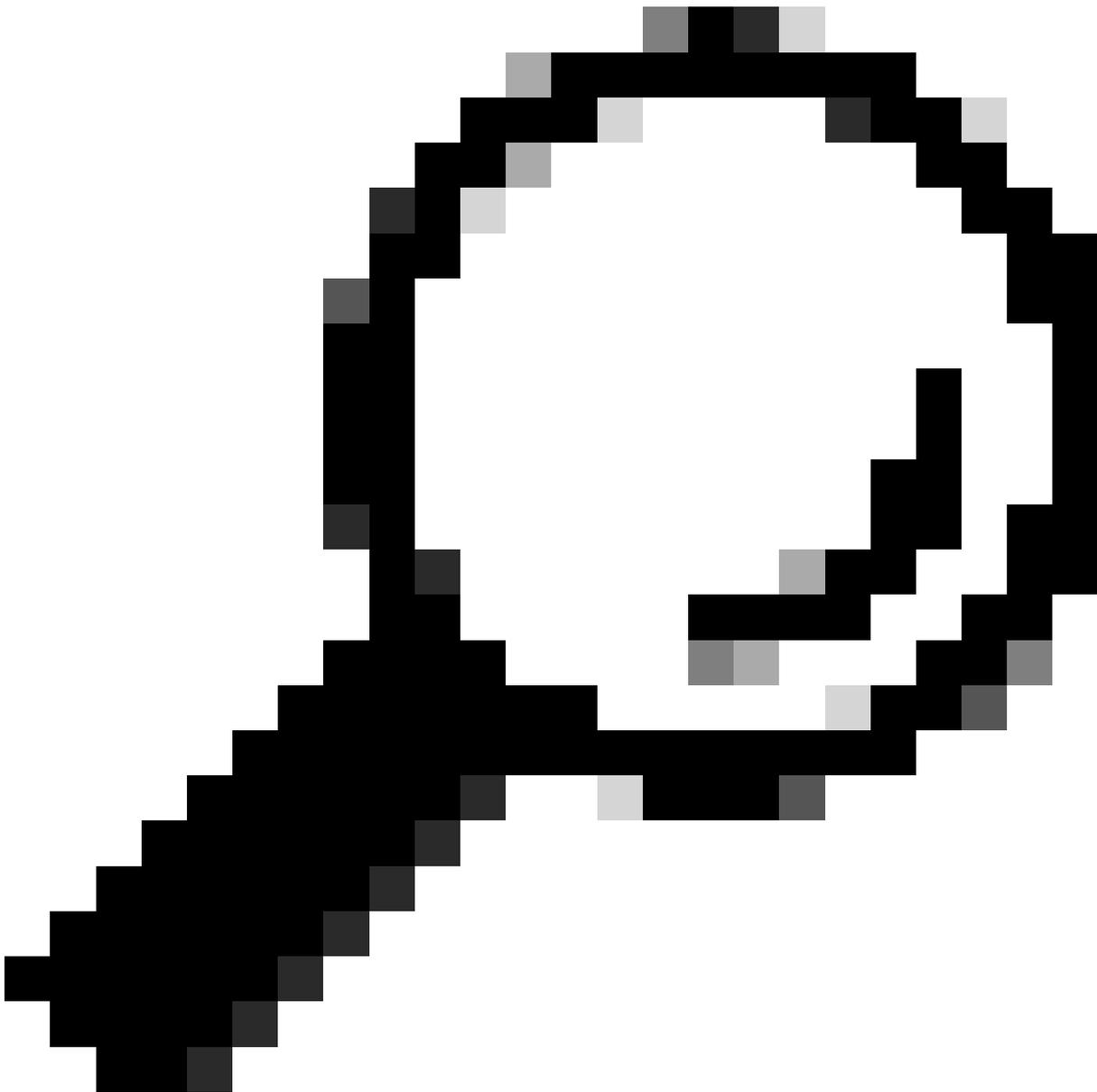
Schritt 4. (Optional) Wählen Sie Ihre Schnittstelle(n) aus, und geben Sie Port 53 in den Abschnitt Benutzerdefinierter Filter ein.

Schritt 5. (Optional) Wählen Sie Senden

Edit Packet Capture Settings

Packet Capture Settings	
Capture File Size Limit: ?	<input type="text" value="200"/> MB <small>Maximum file size is 200MB</small>
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 <small>The capture can be ended manually at any time; use the settings above to specify whether the capture should end automatically.</small>
Interfaces:	<input checked="" type="checkbox"/> M1 <input type="checkbox"/> P1 <input type="checkbox"/> P2
Packet Capture Filters	
Filters:	<small>All filters are optional. Fields are not mandatory.</small> <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"/>
<small>Note: Packet capture settings will be available for use immediately when submitted. Commit changes to save these settings permanently for future use.</small>	
<input type="button" value="Cancel"/>	<input type="button" value="Submit"/>

Image: Filter hinzufügen, um DNS-Pakete zu erfassen



Tipp: Die Paketerfassungseinstellungen können beim Übermitteln sofort verwendet werden. Bestätigen Sie die Änderungen, um diese Einstellungen zur späteren Verwendung dauerhaft zu speichern.

Schritt 6: Wählen Sie Erfassung starten aus.

Schritt 7. (Optional) Generieren Sie Datenverkehr, wenn Sie Probleme bei der Erfassung bestimmter Website oder URL-Zugriff benötigen.

Schritt 8: Erfassung beenden

Schritt 9. Warten Sie, bis die Seite aktualisiert wird, und wählen Sie dann die erste Paketerfassung aus der Liste "Manage Packet Capture Files" (Paketerfassungsdateien verwalten).

Schritt 10. Download-Datei auswählen

L4TM

Die Layer-4-Datenverkehrsüberwachung überwacht den Netzwerkverkehr, der über alle Ports auf jeder sicheren Web-Appliance eingeht, und vergleicht Domännennamen und IP-Adressen mit Einträgen in den eigenen Datenbanktabellen, um zu bestimmen, ob eingehender und ausgehender Datenverkehr zugelassen werden soll.

Wenn interne Clients mit Malware infiziert sind und versuchen, über nicht standardmäßige Ports und Protokolle eine Verbindung herzustellen, verhindert die L4-Datenverkehrsüberwachung, dass Phone-Home-Aktivitäten das Unternehmensnetzwerk verlassen.

Standardmäßig ist die L4-Datenverkehrsüberwachung aktiviert und auf die Überwachung des Datenverkehrs an allen Ports eingestellt. Dies schließt DNS und andere Dienste ein.

Weitere Informationen zur Layer-4-Datenverkehrsüberwachung finden Sie im Benutzerhandbuch.

Fehler

Benachrichtigungsseite

Standardmäßig zeigt SWA eine Benachrichtigungsseite an, auf der die Benutzer über die Blockierung und den Grund der Blockierung informiert werden.

Dateiname und Benachrichtigungstitel: ERR_DNS_FAIL (DNS-Fehler)

Beschreibung: Fehlerseite, die angezeigt wird, wenn die angeforderte URL einen ungültigen Domännennamen enthält.

Benachrichtigungstext: Die Auflösung des Hostnamens (DNS-Suche) für diesen Hostnamen <Hostname > ist fehlgeschlagen.

Die Internetadresse kann falsch geschrieben oder veraltet sein, der Host <Hostname > kann vorübergehend nicht verfügbar sein, oder der DNS-Server reagiert nicht.

Bitte überprüfen Sie die Schreibweise der eingegebenen Internetadresse. Wenn diese richtig ist, versuchen Sie es später noch einmal.

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

Bild - DNS-FEHLER

AccessLog-Ergebniscode NONE

Transaktionsergebniscode in der Zugriffsprotokolldatei beschreiben, wie die Appliance Clientanforderungen löst. Wenn im Zugriffsprotokoll der Ergebniscode NONE lautet, bedeutet dies, dass bei der Transaktion ein Fehler aufgetreten ist. Beispiel: DNS-Fehler oder Gateway-Zeitüberschreitung.

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

Fehler beim Bootstrap des DNS-Cache

Wenn beim Neustart einer Appliance eine Warnung mit der Meldung "Failed to bootstrap the DNS cache" (Fehler beim Bootstrap des DNS-Cache) generiert wird, bedeutet dies, dass das System keine Verbindung zu seinen primären DNS-Servern herstellen konnte.

Dies kann beim Booten der Fall sein, wenn das DNS-Subsystem online geht, bevor die Netzwerkverbindung hergestellt ist. Wenn diese Meldung zu einem anderen Zeitpunkt angezeigt wird, kann dies auf Netzwerkprobleme hinweisen oder darauf, dass die DNS-Konfiguration nicht auf einen gültigen Server festgelegt ist

Maximale Anzahl von Fehlern beim Abfragen des DNS-Servers erreicht

Wenn einer oder mehrere der in SWA konfigurierten DNS-Server nicht auf DNS-Abfragen antworteten, werden diese von SWA als offline betrachtet und für einen vordefinierten Zeitraum nicht an sie gesendet. Weitere Informationen finden Sie unter "Konfigurieren von DNS über CLI" in diesem Artikel.

DNS_FAIL

Wenn SWA eine HTTP-Anfrage empfängt und den Hostnamen nicht auflösen kann, gibt SWA standardmäßig eine Antwort wie die folgende zurück:

```
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
```

Diese Funktion wird als "Erweiterung des Servernamens" bezeichnet.

WSA führt dies in Versuchen durch, bei denen der umgeleitete Hostname die erwartete Seite für den Client auflösen würde.

Sie können das "URL-Format für die HTTP-307-Umleitung bei Fehlschlag der DNS-Suche" ändern. Weitere Informationen finden Sie im Abschnitt `advanceproxyconfig` in diesem Artikel.

Die WSA behandelt die DNS-Anforderung, die `ServFail` als Fehler zurückgibt.

Beispielsweise gibt `NXDOMAIN "DNS_FAIL"` anstelle von `"SERVER_NAME_EXPANSION"` zurück.

Zugehörige Informationen

[Bedienungsanleitung für AsyncOS 15.0 für Cisco Secure Web Appliance](#)

[Best Practices für sichere Web-Appliances - Cisco](#)

[Cisco Content Hub - Einführung in das Domain Name System](#)

Informationen zu dieser Übersetzung

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