

Secure Web Appliance DNS 서비스 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[DNS 개념](#)

[프록시 구축의 DNS 서비스](#)

[DNS 설정 구성](#)

[모범 사례](#)

[GUI에서 DNS 구성](#)

[CLI에서 DNS 구성](#)

[CLI DNS 명령](#)

[수동 레코드 만들기](#)

[dns플러시](#)

[advancedproxyconfig](#)

[DNS 캐시](#)

[GUI에서 DNS 캐시 지우기](#)

소개

이 문서에서는 DNS(Domain Name Service) 컨피그레이션 및 이전에 WSA로 알려진 SWA(Secure Web Appliance)의 트러블슈팅 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 물리적 또는 가상 SWA(Secure Web Appliance) 설치됨
- 라이선스가 활성화되었거나 설치됨
- SSH(Secure Shell) 클라이언트
- 설치 마법사가 완료되었습니다.

- SWA에 대한 관리 액세스

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

DNS 개념

DNS는 개체의 이름(일반적으로 호스트 이름)을 IP(인터넷 프로토콜) 주소 또는 기타 리소스 레코드 값에 매핑하는 인터넷의 시스템입니다.

인터넷의 네임스페이스는 도메인으로 나뉘며, 각 도메인 내의 이름을 관리하는 책임은 일반적으로 각 도메인 내의 시스템에 위임됩니다.

도메인 이름 공간은 DNS 트리에서 위임 지점인 영역이라고 하는 영역으로 나뉩니다.

영역은 다른 영역이 신뢰할 수 있는 도메인을 제외하고 특정 지점 아래쪽의 모든 도메인을 포함합니다.

일반적으로 영역에는 권한 있는 이름 서버가 있으며, 이 서버는 둘 이상인 경우가 많습니다.

조직에서 여러 이름 서버를 가질 수 있지만 인터넷 클라이언트는 루트 이름 서버가 알고 있는 이름만 쿼리할 수 있습니다.

다른 이름 서버는 내부 쿼리에만 응답합니다.

DNS는 클라이언트/서버 모델을 기반으로 합니다. 이 모델에서는 이름 서버가 DNS 데이터베이스의 일부에 대한 데이터를 저장하고 네트워크를 통해 이름 서버를 쿼리하는 클라이언트에 제공합니다.

이름 서버는 물리적 호스트에서 실행되고 영역 데이터를 저장하는 프로그램입니다. 도메인의 관리자는 영역의 호스트를 설명하는 모든 RR(리소스 레코드)의 데이터베이스로 이름 서버를 설정합니다.

프록시 구축의 DNS 서비스

명시적 배포에서: 프록시가 DNS 쿼리를 실행합니다.

투명 구축에서는 DNS 쿼리가 클라이언트에서 실행됩니다.

DNS 설정 구성

GUI(Graphical User Interface) 및 CLI(Command Line Interface)에서 모두 DNS를 구성할 수 있습니다.

AsyncOS for Web은 인터넷 루트 DNS 서버 또는 자체 DNS 서버를 사용할 수 있습니다. SWA가 인터넷 루트 서버를 사용할 경우, 특정 도메인에 사용할 대체 서버를 지정할 수 있습니다.

대체 DNS 서버는 단일 도메인에 적용되므로 해당 도메인에 대해 신뢰할 수 있어야 합니다(확실한 DNS 레코드 제공).

AsyncOS는 내부 서버가 특정 도메인에 대해 구성되고 외부 또는 루트 DNS 서버가 다른 도메인에 대해 구성되는 스플릿 DNS를 지원합니다.

SWA가 온프레미스 DNS 서버를 사용하는 경우 예외 도메인 및 관련 DNS 서버도 지정할 수 있습니다.

모범 사례

보안 모범 사례에서는 모든 네트워크에서 두 개의 DNS 리졸버를 호스팅해야 한다고 제안합니다. 하나는 로컬 도메인 내의 권한 있는 레코드용이고 다른 하나는 인터넷 도메인의 재귀적 확인용입니다.

이를 수용하기 위해 SWA는 DNS 서버가 특정 도메인에 대해 구성되도록 허용합니다.

로컬 및 재귀 쿼리 둘 다에 사용할 수 있는 DNS 서버 1대의 경우, 모든 SWA 쿼리에 사용되는 경우 이 서버가 추가하는 추가 로드를 고려하십시오.

로컬 도메인에는 내부 확인기를 사용하고 외부 도메인에는 루트 인터넷 확인기를 사용하는 것이 더 좋습니다. 이는 관리자 위험 프로필 및 허용 한도에 따라 달라집니다.

기본 DNS를 사용할 수 없는 경우 보조 DNS 서버를 구성해야 합니다. 모든 서버가 동일한 우선 순위로 구성된 경우 서버 IP가 임의로 선택됩니다.

구성된 서버 수에 따라 지정된 서버에 대한 시간 초과는 달라집니다. 최대 6개의 DNS 서버에 대한 쿼리 시간 제한이 이 테이블에 제공됩니다.

DNS 서버 수	쿼리 시간 초과(시퀀스)
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

자세한 내용은 [Cisco Web Security Appliance 모범 사례 지침 - Cisco](#)를 참조하십시오.

GUI에서 DNS 구성

GUI에서 DNS를 구성하려면 다음 단계를 수행합니다.

1단계. 상단 메뉴에서 네트워크 선택

2단계. DNS 선택

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

대체 DNS 서버 재정의(선택 사항): 도메인에 대한 권한 있는 DNS 서버

 참고: AsyncOS는 투명 FTP 요청에 대한 버전 기본 설정을 적용하지 않습니다.

 참고: 클라우드 커넥터 모드에서는 Cisco Web Security Appliance가 IPv4만 지원합니다

인터넷 루트 DNS 서버를 사용합니다. 어플라이언스가 네트워크의 DNS 서버에 액세스할 수 없을 때 도메인 이름 서비스 조회에 인터넷 루트 DNS 서버를 사용하도록 선택합니다.

인터넷 루트 DNS 서버가 로컬 호스트 이름을 확인하지 않습니다.

 참고: 어플라이언스에서 로컬 호스트 이름을 확인해야 하는 경우, 로컬 DNS 서버를 사용하거나 CLI(Command Line Interface)에서 로컬 DNS에 적절한 고정 엔트리를 추가합니다.

Domain Search List(도메인 검색 목록): 요청이 베어 호스트 이름(점 없음)으로 전송될 때 사용되는 DNS 도메인 검색 목록입니다. ").

호스트 이름과 도메인에 대한 DNS 일치 여부를 찾을 수 있는지 확인하기 위해 각 지정된 도메인을 입력한 순서(왼쪽에서 오른쪽)로 차례로 시도합니다.

DNS 트래픽용 라우팅 테이블: DNS 서비스가 트래픽을 라우팅하는 인터페이스를 지정합니다.

Wait Before Timing out Reverse DNS Lookups: 응답이 없는 역방향 DNS 조회가 시간 초과되기 전 대기 시간(초)입니다.

기본 DNS 서버가 다음 오류를 반환하면 보조 DNS 서버는 호스트 이름 쿼리를 받습니다.

- 오류 없음, 응답 섹션 없음
 - 서버가 요청을 완료하지 못했습니다. 응답 섹션이 없습니다.
 - 이름 오류, 응답 섹션 없음
 - 구현되지 않은 기능
 - 서버가 쿼리에 응답하지 않음
-

 참고: AsyncOS는 어플라이언스에서 불필요한 외부 통신을 방지하기 위해 외부 종속성을 평가하기 전에 정책을 기반으로 트랜잭션을 평가합니다. 예를 들어 분류되지 않은 URL을 차단하는 정책에 따라 트랜잭션이 차단되는 경우, DNS 오류에 따라 트랜잭션이 실패하지 않습니다.

우선순위: 0의 값이 우선순위가 가장 높습니다. 두 IP 모두 우선순위가 동일한 경우 임의의 IP가 선택됩니다.

CLI에서 DNS 구성

CLI에서 dnsconfig를 사용하여 DNS 설정을 구성할 수 있습니다.

1단계. CLI에서 dnsconfig를 입력합니다.

```
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.

```
[>
```

2단계. 목록에 새 DNS 서버를 추가하려면 NEW를 입력하고 Enter를 누릅니다.

3단계. 새 네임서버를 추가할 기본 DNS 네임서버 또는 보조 DNS 네임서버 중에서 선택합니다.

```
[> 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
```

4단계. 새 이름 서버 또는 대체 도메인 서버(조건부 전달 도메인 이름)를 추가하도록 선택합니다.

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
```

5단계. 새 이름 서버의 IP 주소 제공

6단계. 새로 추가된 이름 서버에 대한 우선순위를 제공합니다.

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

7단계. Enter를 눌러 마법사를 종료합니다.

8단계. commit을 입력하여 변경 사항을 저장합니다.

참고: 이름 서버를 수정하거나 삭제하려면 dnsconfig에서 EDIT 및 DELETE를 선택할 수 있습니다.

SETUP 옵션에서 DNS 캐시 시간 및 오프라인 DNS 탐지 설정을 구성할 수 있습니다.

```
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]>

DNS 캐시의 최소 TTL(초): 이 옵션은 SWA가 레코드를 캐시한 최소 시간(초)을 구성하는 것입니다. 자세한 내용은 이 문서의 DNS 캐시 섹션을 참조하십시오.

로컬 DNS 서버를 오프라인으로 고려하기 전에 실패한 시도 횟수를 입력합니다. DNS 서버가 DNS 쿼리에 응답하지 않는 경우 카운터가 시작됩니다.

이 정의된 값에 도달하면 해당 이름 서버는 오프라인 DNS 서버로 간주되며 SWA는 미리 정의된 기간 동안 해당 이름 서버로 DNS 쿼리를 보내지 않습니다(Next 옵션).

DNS 서버가 오프라인으로 표시된 경우 다음 오류 메시지가 표시됩니다.

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

오프라인 로컬 DNS 서버를 폴링하는 간격(초)을 입력합니다. DNS 서버가 오프라인으로 표시된 경우 이 시간 간격(초) 이후에 SWA가 DNS 쿼리를 해당 네임서버로 보내기 시작하며 해당 DNS 서버에 대한 응답 실패 카운터가 0으로 재설정됩니다.

CLI DNS 명령

수동 레코드 만들기

수동 "A 레코드"를 생성하려면 Hosts 파일을 사용하거나 편집할 수 없습니다. CLI의 dnsconfig에서 localhost hidden 명령을 사용할 수 있습니다.

참고: 이 컨피그레이션을 변경한 후 변경 사항을 커밋해야 합니다.

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
```

dns플러시

dnsflush는 캐시된 모든 DNS 레코드를 DNS 캐시 테이블에서 제거합니다.

```
SWA_CLI> dnsflush
```

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

advancedproxyconfig

```
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]>

HTTP 307(Temporary Redirect) 상태 코드는 대상 리소스가 일시적으로 다른 URI(Uniform Resource Identifier) 아래에 있음을 나타내며, 사용자 에이전트가 해당 URI로 자동 리디렉션을 수행하는 경우 요청 방법을 변경하지 않아야 합니다. 리디렉션은 시간이 지남에 따라 변경될 수 있으므로 클라이언트는 원래의 유효 요청 URI를 계속 사용해야 합니다.

에 대한 자세한 내용 : [HTTP 307 임시 리디렉션 상태 코드 - Kinsta란 무엇입니까?](#)

이러한 옵션은 SWA가 연결할 IP 주소를 결정하는 방법을 제어하며, 투명 프록시 구축에서 클라이언트 요청을 평가할 때 사용됩니다. 요청이 수신되면 WSA에 대상 IP 주소 및 호스트 이름이 표시됩니다. SWA는 TCP 연결을 위해 원래 목적지 IP 주소를 신뢰할지 아니면 자체 DNS 확인을 수행하고 확인된 주소를 사용할지 결정해야 합니다. 기본값은 "0 = 항상 DNS 응답을 순서대로 사용"입니다. 즉, SWA는 클라이언트가 IP 주소를 제공하도록 신뢰하지 않습니다.

옵션 1: SWA는 클라이언트에 제공된 IP 주소를 연결에 대해 시도하지만, 실패한 경우 확인된 주소로 폴백됩니다. 확인된 주소는 정책 평가(웹 카테고리, 웹 평판 등)에 사용됩니다.

옵션 2: SWA는 연결에 클라이언트 제공 주소만 사용하며 폴백되지 않습니다. 확인된 주소는 정책 평가(웹 카테고리, 웹 평판 등)에 사용됩니다.

옵션 3: SWA는 연결에 클라이언트 제공 주소만 사용하며 폴백되지 않습니다. 클라이언트 제공 IP 주소는 정책 평가에 사용됩니다(웹 카테고리, 웹 평판 등).

선택한 옵션은 지정된 호스트 이름에 대해 확인된 주소를 확인할 때 관리자가 클라이언트에 어느 정도의 신뢰도를 두어야 하는지에 따라 달라집니다. 클라이언트가 다운스트림 프록시인 경우 옵션 3을 선택하여 불필요한 DNS 조회가 추가로 지연되는 것을 방지합니다.

DNS 캐시

효율성과 성능을 높이기 위해 Cisco SWA는 최근에 연결한 도메인에 대한 DNS 항목을 저장합니다. DNS 캐시는 SWA가 동일한 도메인의 과도한 DNS 조회를 방지할 수 있게 합니다. 레코드의 TTL(Time to Live) 때문에 DNS 캐시 엔트리가 만료됩니다.

DNS 서버에 있는 레코드의 TTL이 SWA dnsconfig 캐시 TTL 시간보다 크면 dns 캐시는 DNS 서버의 TTL을 사용합니다.

DNS 서버에 있는 레코드의 TTL이 SWA dnsconfig 캐시 TTL 시간보다 작으면 dns 캐시는 WSA dnsconfig 설정의 TTL을 사용합니다.

 주의: SWA에는 2개의 DNS 캐시가 있으며, 하나는 프록시 프로세스용으로 설계되고 다른 하나는 내부 프로세스용으로 사용됩니다.

기본적으로 SWA는 레코드 TTL과 상관없이 최소 30분 동안 캐시된 DNS 레코드를 사용합니다. CDN(Content Delivery Networks)을 많이 사용하는 최신 웹 사이트는 IP 주소가 자주 변경되므로 TTL 기록이 낮습니다.

이렇게 하면 클라이언트가 지정된 서버에 대해 하나의 IP 주소를 캐시하고 SWA가 동일한 서버에 대해 다른 주소를 캐시할 수 있습니다. 이에 대응하기 위해 SWA 기본 TTL을 `dsncfig CLI` 명령의 `SETUP` 섹션에서 5분으로 낮출 수 있습니다.

예를 들어 DNS 컨피그레이션에서 "DNS 캐시에 대한 최소 TTL(초)"이 10분으로 설정되어 있고 레코드의 TTL이 5분인 경우 캐시된 레코드의 TTL은 10분으로 증가합니다.

반면, 레코드의 TTL이 15분으로 설정된 경우 SWA는 15분 동안의 레코드를 캐시에 저장합니다.

그러나 항목의 DNS 캐시를 지워야 하는 경우도 있습니다. 손상되거나 만료된 DNS 캐시 엔트리는 원격 호스트로의 전달에 문제를 일으킬 수 있습니다.

이 문제는 일반적으로 어플라이언스가 네트워크 이동 또는 기타 상황으로 인해 오프라인된 후에 발생합니다.

GUI에서 DNS 캐시 지우기

1단계. 상단 메뉴에서 네트워크 선택

2단계. DNS 선택

3단계. Clear DNS Cache(DNS 캐시 지우기)를 선택합니다

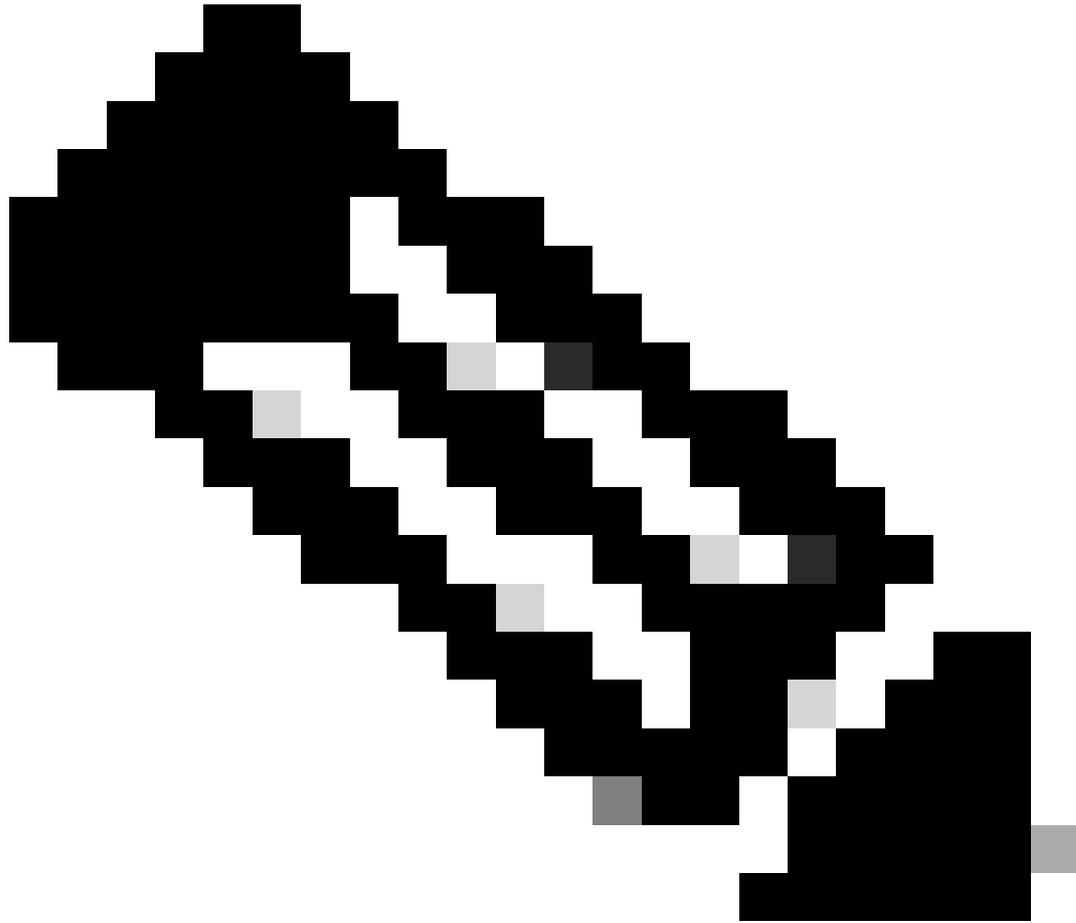
 주의: 이 명령은 캐시가 다시 채워지는 동안 일시적인 성능 저하를 일으킬 수 있습니다

CLI에서 DNS 캐시 지우기

Cisco WSA의 DNS 캐시는 CLI에서 `dnsflushcommand`를 통해 지울 수 있습니다.

DNS 캐시 보기

CLI 또는 GUI에서 SWA의 캐시된 DNS 레코드를 보는 옵션은 없습니다.



참고: nslookup을 통해 DNS 캐시를 쿼리할 수 없습니다.

DNS 트러블슈팅

DNS 로그 보기

웹 프록시 구성 요소와 관련된 일부 로그 유형이 활성화되지 않았습니다. "기본 프록시 로그"라고 하는 기본 웹 프록시 로그 유형은 기본적으로 활성화되어 있으며 모든 웹 프록시 모듈에 대한 기본 정보를 캡처합니다.

각 웹 프록시 모듈에는 필요에 따라 수동으로 활성화할 수 있는 자체 로그 유형도 있습니다.

시스템 로그, DNS 기록, 오류 및 커밋 활동. 기본적으로 활성화됨

 **팁:** 시스템 로그의 로그 레벨을 DEBUG로 변경하면 DNS 쿼리 및 응답을 볼 수 있습니다. GUI 및 CLI에서 로그 레벨을 변경할 수 있습니다.

GUI에서 시스템 로그 로그 레벨 변경

1단계. 상단 메뉴에서 System Administration(시스템 관리)을 선택합니다.

2단계. 로그 서브스크립션 선택

3단계. 시스템 로그 선택

4단계. Log Level(로그 레벨) 섹션에서 DEBUG(디버그)를 선택합니다.

5단계. 제출

6단계. 변경 사항 커밋

Edit DNS

DNS Server Settings

Primary DNS Servers: Use these DNS Servers

Priority ?	Server IP Address	
<input type="text" value="0"/>	<input type="text" value="10.1.1.1"/>	<input type="button" value="Add Row"/>
<input type="text" value="1"/>	<input type="text" value="10.2.2.2"/>	<input type="button" value="Add Row"/>
<input type="text" value="2"/>	<input type="text" value="10.3.3.3"/>	<input type="button" value="Add Row"/>

Alternate DNS servers Overrides (Optional):

Domain(s)	DNS Server IP Address(es)	
<input type="text"/>	<input type="text"/>	<input type="button" value="Add Row"/>

i.e., example.com, example2.com i.e., 10.0.0.3 or 2001:420:80:1::5

Use the Internet's Root DNS Servers

Alternate DNS servers Overrides (Optional):

Domain	DNS Server IP Address	
<input type="text"/>	<input type="text"/>	<input type="button" value="Add Row"/>

i.e., dns.example.com

Secondary DNS Servers:

Priority ?	Server IP Address	
<input type="text" value="0"/>	<input type="text" value="10.10.10.10"/>	<input type="button" value="Add Row"/>

Routing Table for DNS Traffic: Management

IP Address Version Preference: Prefer IPv4
 Prefer IPv6
 Use IPv4 only
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.

Secure DNS: Enable
 Disable
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.

Wait Before Timing out Reverse DNS Lookups: seconds

Domain Search List: ?

Separate multiple entries with commas. Maximum allowed characters 2048.

CLI에서 시스템 로그 로그 레벨 변경

1단계. CLI에 로그인

2단계. 유형 logconfig

3단계. 편집을 선택합니다

4단계. System_Logs에 연결된 번호를 입력합니다.

5단계. 로그 레벨에 도달할 때까지 Enter를 누릅니다

6단계. Debug(디버그)에 대한 숫자 4를 선택합니다.

7단계. 마법사를 종료할 때까지 Enter 키를 누릅니다

8단계. 변경 사항을 저장하려면 commit을 입력합니다.

```
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
```

 **팁:** 트러블슈팅을 수행한 후에는 로그 레벨을 다시 Information(정보)으로 변경해야 합니다. 그렇지 않으면 디스크 I/O(Input/Output)에 큰 로드가 발생하고 로그 파일이 빠르게 채워집니다.

nslookup

nslookup 명령을 사용하여 다른 FQDN에 대한 SWA의 이름 확인 응답을 확인합니다.

이 예에서는 이름을 확인하는 첫 번째 시도에서 TTL이 30분으로 설정됩니다.

두 번째 시도에서 TTL이 30분 미만임을 확인할 수 있으며, 이는 이 레코드가 캐시에서 해결되었음을 나타냅니다.

```
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
```

파기

dig는 DNS 레코드를 쿼리하는 또 다른 유용한 명령입니다. dig를 사용하면 쿼리할 소스 인터페이스 또는 DNS 서버를 지정할 수 있습니다.

이 예에서는 서버 10.1.1.1의 A 레코드에 대한 쿼리입니다

```
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
```

dig의 사용:

```
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

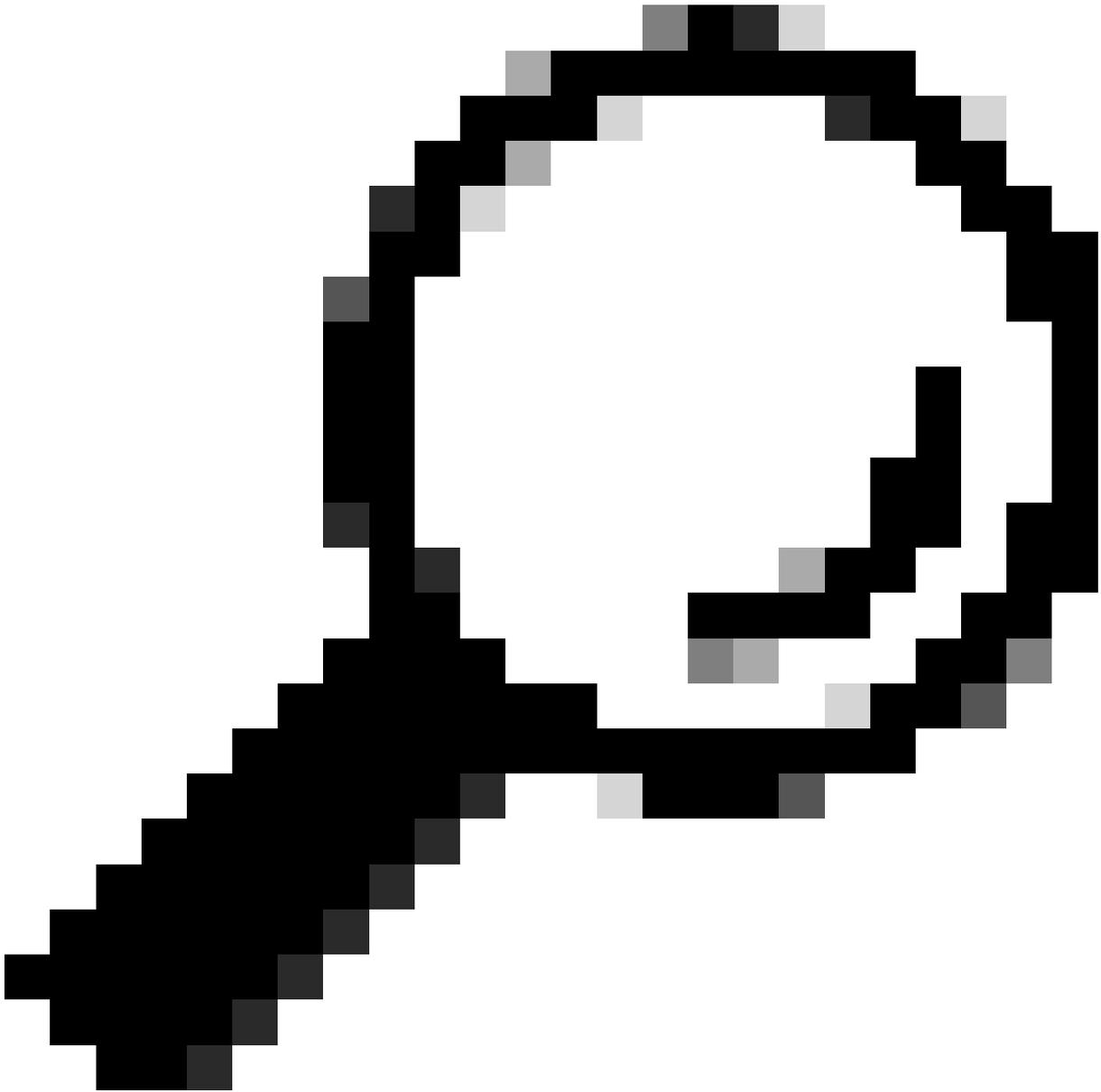
Specify the source IP address.

-t

Make query over tcp.

-x IP Address

Do a reverse lookup on this IP address.



팁: 소스 IP를 선택하여 이름 확인을 쿼리할 인터페이스를 선택할 수 있습니다.

느린 DNS 응답

모든 URL 또는 일부 URL을 로드하는 데 시간이 더 오래 걸린 경우(동일한 페이지를 새로 고치는 경우보다) DNS 응답 시간을 확인하는 것이 좋습니다. SWA에는 DNS 응답 시간을 확인하는 두 가지 옵션이 있습니다.

- AccessLogs 사용자 지정 필드를 구성합니다.
- 추적 로그.

액세스 로그를 수정하여 DNS 통계 보기

각 웹 요청에 대한 DNS 시간을 보려면 액세스 로그를 수정할 수 있습니다.

1단계. GUI에 로그인합니다.

2단계. System Administration(시스템 관리) 메뉴에서 Log Subscriptions(로그 서브스크립션)를 선택합니다.

3단계. Log Name(로그 이름) 열에서 accesslogs(액세스 로그) 또는 새로 만든 이름을 클릭합니다. 이 예에서는 TAC_access_logs입니다.

4단계. Custom Fields(맞춤형 필드) 섹션에서 다음 문자열을 붙여넣습니다.

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

5단계. 변경 사항을 제출하고 커밋합니다.

사용자 지정 필드 이름	사용자 지정 필드	W3C 로그	설명
DNS 응답	%:<d	x-p2p-dns-wait-time	웹 프록시에서 DNS(Domain Name Request) 요청을 웹 프록시 DNS 프로세스로 보내는 데 걸린 시간입니다.
DNS 합계	%:>d	x-p2p-dns-svc-시간	웹 프록시 DNS 프로세스가 DNS 결과를 웹 프록시로 다시 전송하는 데 걸린 시간입니다.

Access Logs(액세스 로그)에서 사용자 정의 필드를 수정하는 방법에 대한 자세한 내용은 Configure Performance Parameter in Access Logs(액세스 로그의 성능 매개변수 구성) - Cisco 링크를 참조하십시오.

Trackstat 로그의 전체 DNS 응답 시간

trackstat 로그에서 DNS 서비스 및 기타 내부 서비스의 통계를 볼 수 있습니다. FTP를 통해 SWA에 연결하여 추적 통계 로그에 액세스할 수 있습니다.

이 예에서는 SWA가 마지막으로 리부팅된 이후 DNS 서버에서 경과된 시간을 기준으로 범주화된 캐시 통계 및 DNS 응답 수를 확인할 수 있습니다.

...
 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

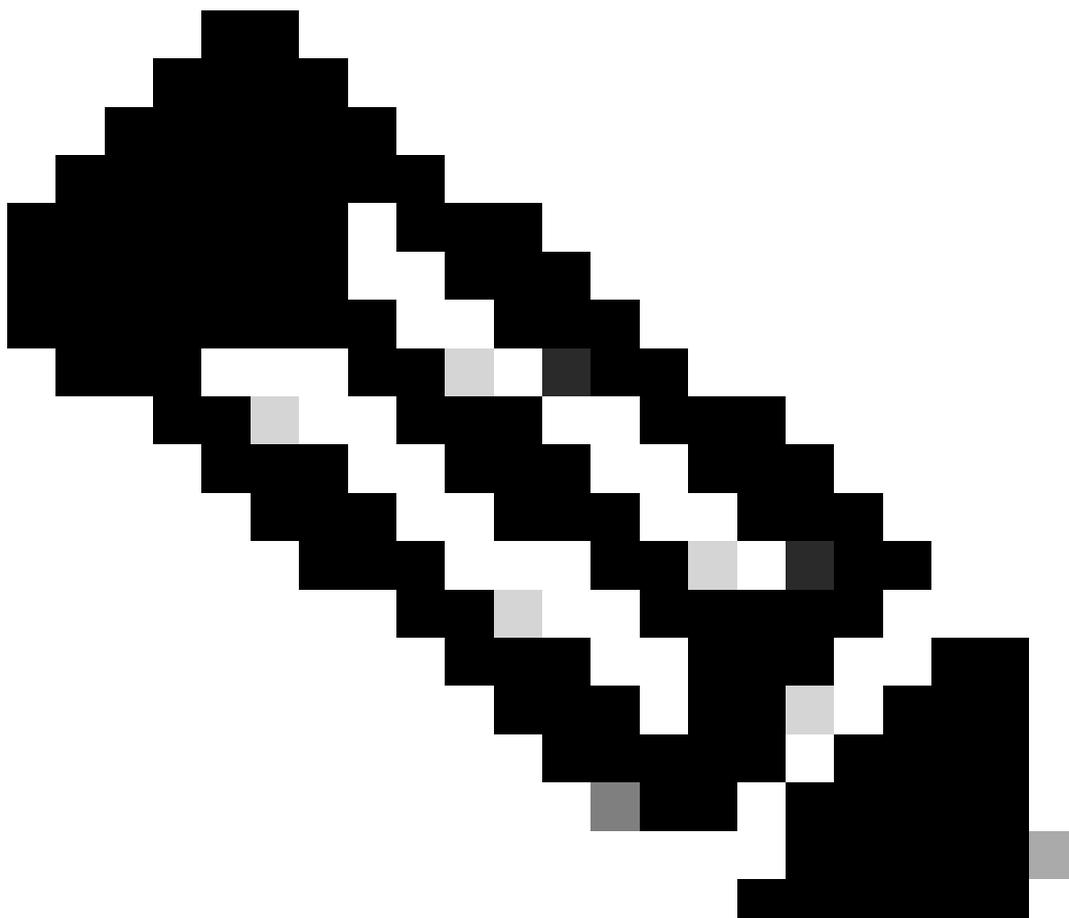
```

예를 들어, 마지막 행에서 190개의 DNS 쿼리가 SWA가 마지막으로 리부팅된 이후 6,309밀리초(약 6초) 이상 소요되었음을 나타냅니다.

특정 기간의 정확한 수를 확인하려면 시작 시간과 종료 시간에 대해 이 값을 빼십시오.

예를 들어 오전 10:00부터 오전 11:00까지의 DNS 응답 시간을 식별하려면 오전 11:00에 대한 통계를 수집한 다음 오전 10:00의 통계에서 뺍니다.

결과는 원하는 날짜의 DNS 응답 시간이 오전 10:00에서 오전 11:00까지입니다.



참고: 추적 통계 로그는 5분마다 수집됩니다.

패킷 캡처

패킷을 캡처하여 DNS 요청 및 응답을 보고, 사용할 수 있는 DNS만 필터링할 수 있습니다. 포트 53.

GUI에서 패킷 캡처를 시작하려면

1단계. 오른쪽 위에서 Support and Help(지원 및 도움말)를 선택합니다.

2단계. 패킷 캡처 선택

3단계. (선택 사항) 필터를 추가하려면 Edit Settings(설정 편집)를 선택합니다

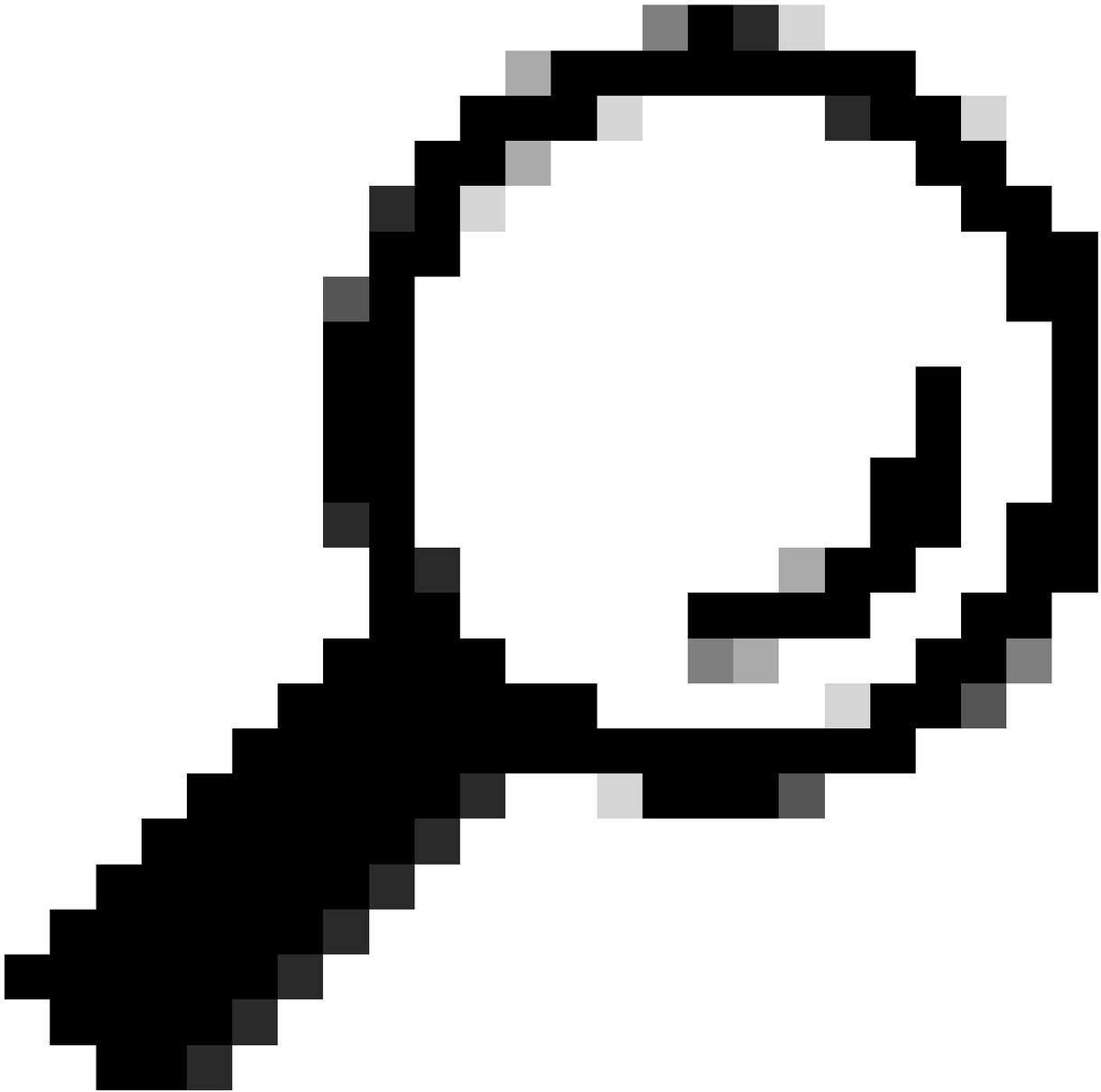
4단계. (선택 사항) 인터페이스를 선택하고 Custom Filter(사용자 지정 필터) 섹션에 포트 53을 입력합니다

5단계. (선택 사항) Submit(제출)을 선택합니다

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>	

Image(이미지) - DNS 패킷을 캡처할 필터 추가



팁: 패킷 캡처 설정은 제출되는 즉시 사용할 수 있습니다. 변경 내용을 커밋하여 나중에 사용할 수 있도록 이 설정을 영구적으로 저장합니다.

6단계. Start Capture(캡처 시작)를 선택합니다.

7단계(선택 사항) 특정 사이트 또는 URL 액세스에 문제가 발생할 경우 트래픽을 생성합니다.

8단계. 캡처 중지

9단계. 페이지가 새로 고쳐질 때까지 기다린 다음 "Manage Packet Capture Files(패킷 캡처 파일 관리)" 목록에서 첫 번째 패킷 캡처를 선택합니다.

10단계. Download File(파일 다운로드)을 선택합니다

L4TM

레이어 4 트래픽 모니터는 각 Secure Web Appliance의 모든 포트를 통해 들어오는 네트워크 트래픽을 수신하고 도메인 이름 및 IP 주소를 자체 데이터베이스 테이블의 항목과 비교하여 수신 및 발신 트래픽을 허용할지 여부를 결정합니다.

내부 클라이언트가 악성코드에 감염되고 비표준 포트 및 프로토콜을 통해 phone-home을 시도하는 경우 L4 트래픽 모니터는 회사 네트워크를 종료하기 위한 phone-home 활동을 방지합니다.

기본적으로 L4 Traffic Monitor가 활성화되고 모든 포트의 트래픽을 모니터링하도록 설정됩니다. 여기에는 DNS 및 기타 서비스가 포함됩니다.

레이어 4 트래픽 모니터에 대한 자세한 내용은 사용 설명서를 참조하십시오.

오류

알림 페이지

기본적으로 SWA는 사용자에게 차단되었음을 알리는 알림 페이지와 차단 이유를 표시합니다

파일 이름 및 알림 제목: ERR_DNS_FAIL(DNS 실패)

설명: 요청된 URL에 잘못된 도메인 이름이 포함된 경우 표시되는 오류 페이지입니다.

알림 텍스트: 이 호스트 이름 <hostname>에 대한 호스트 이름 확인(DNS 조회)에 실패했습니다.

인터넷 주소의 철자가 잘못되었거나 더 이상 사용되지 않을 수 있습니다. 호스트 <hostname>을(를) 일시적으로 사용할 수 없거나 DNS 서버가 응답하지 않을 수 있습니다.

입력한 인터넷 주소의 철자를 확인하십시오. 올바른 경우 나중에 이 요청을 시도하십시오.

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

이미지 - DNS FAIL 오류

Accesslog 결과 코드 없음

액세스 로그 파일의 트랜잭션 결과 코드는 어플라이언스가 클라이언트 요청을 해결하는 방법을 설명합니다. 액세스 로그에서 결과 코드가 NONE이면 트랜잭션에 오류가 발생했음을 의미합니다. 예를 들어, DNS 실패 또는 게이트웨이 시간 초과입니다.

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

DNS 캐시를 부트스트랩하지 못했습니다.

어플라이언스를 재부팅할 때 "DNS 캐시를 부트스트랩하지 못했습니다"라는 메시지가 포함된 알림이 생성되면 시스템이 기본 DNS 서버에 연결할 수 없음을 의미합니다.

네트워크 연결이 설정되기 전에 DNS 하위 시스템이 온라인 상태로 전환되는 경우 부팅 시 이 문제가 발생할 수 있습니다. 이 메시지가 다른 시간에 나타나면 네트워크 문제를 나타내거나 DNS 컨피그레이션이 유효한 서버로 설정되지 않았음을 나타낼 수 있습니다

DNS 서버를 쿼리하는 최대 실패 수에 도달했습니다.

SWA에 구성된 DNS 서버 중 하나 또는 일부가 DNS 쿼리에 회신하지 않은 경우, SWA는 이를 오프라인으로 간주하고 미리 정의된 시간 동안 DNS 쿼리를 SWA에 전송하지 않습니다. 자세한 내용은 이 문서의 "CLI에서 DNS 구성"을 참조하십시오.

DNS_FAIL

SWA가 HTTP 요청을 받고 호스트 이름 확인에 실패하면 기본적으로 SWA는 다음과 같은 응답을 반환합니다.

```
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
```

이 기능을 "서버 이름 확장"이라고 합니다.

WSA는 리디렉션된 호스트 이름이 클라이언트에 대한 예상 페이지를 확인하려고 시도할 때 이 작업을 수행합니다.

이 문서의 `advanceproxyconfig` 섹션에 대한 자세한 내용을 보려면 "DNS 조회 실패 시 HTTP 307 리디렉션의 URL 형식"을 변경할 수 있습니다.

WSA는 `ServFail`을 반환하는 DNS 요청을 실패로 처리합니다.

예를 들어 `NXDOMAIN`은 "SERVER_NAME_EXPANSION" 대신 "DNS_FAIL"을 반환합니다.

관련 정보

[AsyncOS 15.0 for Cisco Secure Web Appliance 사용 설명서](#)

[Use Secure Web Appliance 모범 사례 - Cisco](#)

[Cisco Content Hub - Domain Name System 소개](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.