

Solucionar problemas do serviço DNS do Secure Web Appliance

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Conceito de DNS](#)

[Serviço DNS em implantações de proxy](#)

[Definir configurações DNS](#)

[Prática recomendada](#)

[Configurar DNS na GUI](#)

[Configurar DNS a partir da CLI](#)

[Comandos CLI DNS](#)

[Criar registro manual](#)

[dnsflush](#)

[advancedproxyconfig](#)

[cache DNS](#)

[Limpar o cache DNS da GUI](#)

Introdução

Este documento descreve a configuração do Domain Name Service (DNS) e como solucionar problemas no Secure Web Appliance (SWA) anteriormente conhecido como WSA.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Dispositivo da Web seguro (SWA) físico ou virtual instalado
- Licença ativada ou instalada
- Cliente Secure Shell (SSH)
- O assistente de instalação foi concluído

- Acesso administrativo ao SWA

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conceito de DNS

O DNS é o sistema na Internet que mapeia nomes de objetos (geralmente nomes de host) em endereços IP (Internet Protocol) ou outros valores de registro de recursos.

O espaço de nomes da Internet é dividido em domínios, e a responsabilidade de gerenciar nomes dentro de cada domínio é delegada, normalmente aos sistemas dentro de cada domínio.

O espaço do nome de domínio é dividido em áreas chamadas zonas que são pontos de delegação na árvore DNS.

Uma zona contém todos os domínios de um certo ponto para baixo, exceto aqueles para os quais outras zonas são autoritativas.

Uma zona geralmente tem um servidor de nome autoritativo, geralmente mais de um.

Em uma organização, você pode ter muitos servidores de nome, mas os clientes da Internet podem consultar somente aqueles que os servidores de nome raiz conhecem.

Os outros servidores de nomes respondem somente a consultas internas.

O DNS é baseado em um modelo cliente/servidor. Neste modelo, os servidores de nome armazenam dados sobre uma parte do banco de dados DNS e os fornecem aos clientes que consultam o servidor de nome através da rede.

Os servidores de nome são programas executados em um host físico e armazenam dados de zona. Como administrador de um domínio, você configura um servidor de nomes com o banco de dados de todos os Registros de Recursos (RRs) descrevendo os hosts na sua zona ou zonas

Serviço DNS em implantações de proxy

Na implantação explícita: o proxy executa consultas DNS

Na implantação transparente: as consultas DNS são executadas no cliente.

Definir configurações DNS

Você pode configurar o DNS na interface gráfica do usuário (GUI) e na interface de linha de comando (CLI).

O AsyncOS para Web pode usar os servidores DNS raiz da Internet ou seus próprios servidores

DNS. Se o SWA usar servidores raiz da Internet, você poderá especificar servidores alternativos para usar em domínios específicos.

Como um servidor DNS alternativo se aplica a um único domínio, ele deve ser autoritativo (fornecer registros DNS definitivos) para esse domínio.

O AsyncOS suporta DNS dividido, em que os servidores internos são configurados para domínios específicos e os servidores DNS externos ou raiz são configurados para outros domínios.

Se o SWA usar o servidor DNS local, também podemos especificar domínios de exceção e o servidor DNS associado.

Prática recomendada

As melhores práticas de segurança sugerem que cada rede deve hospedar dois resolvedores de DNS: um para registros autoritativos de dentro de um domínio local e um para resolução recursiva de domínios da Internet.

Para acomodar isso, o SWA permite que os servidores DNS sejam configurados para domínios específicos.

No caso de um servidor DNS disponível para consultas locais e recursivas, considere a carga adicional que isso adicionaria se fosse usado para todas as consultas SWA.

A melhor opção pode ser usar o resolvedor interno para domínios locais e os resolvedores de Internet raiz para domínios externos. Isso depende do perfil de risco e da tolerância do administrador.

Os servidores DNS secundários devem ser configurados caso o primário não esteja disponível. Se todos os servidores forem configurados com a mesma prioridade, o IP do servidor será escolhido aleatoriamente.

Dependendo do número de servidores configurados, o tempo limite de um determinado servidor varia. O tempo limite de uma consulta é fornecido nesta tabela, para até seis servidores DNS:

Número de servidores DNS	Tempo limite da consulta (em sequência)
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

Para obter mais informações, visite : [Diretrizes de melhores práticas do Cisco Web Security Appliance - Cisco](#)

Configurar DNS na GUI

Para configurar o DNS a partir da GUI, siga estas etapas:

Etapa 1. Escolha Network no menu superior

Etapa 2. Escolher 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


Substituições de servidores DNS alternativos (opcional): servidores DNS autoritativos para domínios

 Observação: o AsyncOS não honra a preferência de versão para solicitações de FTP transparentes.

 Observação: no modo de conector de nuvem, o Cisco Web Security Appliance oferece suporte somente a IPv4

Use os servidores DNS da raiz da Internet. Escolha usar os servidores DNS raiz da Internet para pesquisas de serviço de nomes de domínio quando o equipamento não tiver acesso aos servidores DNS na rede.

Os servidores DNS da raiz da Internet não resolvem nomes de host locais.

 Observação: se você precisar que seu equipamento resolva nomes de host locais, use um servidor DNS local ou adicione as entradas estáticas apropriadas ao DNS local a partir da CLI (Command Line Interface Interface Interface Interface de Linha de Comando).

Lista de pesquisa de domínio: uma lista de pesquisa de domínio DNS usada quando uma solicitação é enviada a um nome de host vazio (sem ponto " . ").


Cada um dos domínios especificados pode ser tentado, na ordem inserida (da esquerda para a direita), para ver se uma correspondência de DNS para o nome de host mais o domínio pode ser encontrada.


Tabela de Roteamento para Tráfego DNS: Especifica por qual interface o serviço DNS roteia o tráfego.

Aguardar Antes de Atingir o Tempo Limite de Pesquisas de DNS Reverso: O tempo de espera em segundos antes de atingir o tempo limite de pesquisas de DNS reverso sem resposta.

Os servidores DNS secundários recebem consultas de nome de host quando os servidores DNS primários retornam estes erros:

- Sem erro, sem seção de resposta recebida
 - Falha do servidor ao concluir a solicitação, seção sem resposta
 - Erro de nome, nenhuma seção de resposta recebida
 - Função não implementada
 - Servidor se recusou a responder à consulta
-

 Observação: o AsyncOS avalia transações com base em políticas antes de avaliar dependências externas para evitar comunicação externa desnecessária do dispositivo. Por

 exemplo, se uma transação for bloqueada com base em uma política que bloqueia URLs sem categoria, a transação não falhará com base em um erro de DNS.

Prioridade: Um valor de 0 tem a prioridade mais alta. Um IP aleatório será selecionado se ambos tiverem a mesma prioridade.

Configurar DNS a partir da CLI

Você pode usar `dnsconfig` da CLI para definir as configurações de DNS.

Etapa 1. Digite `dnsconfig` na 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.

```
[>
```

Etapa 2. Para adicionar um novo servidor DNS à lista, digite `NEW` e pressione `Enter`.

Etapa 3. Escolha entre servidores de nomes DNS primário ou servidores de nomes DNS secundário, aos quais você deseja adicionar um novo servidor de nomes.

```
[> 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
```

Etapa 4. Escolha adicionar um novo servidor de nomes ou um servidor de domínio alternativo (nome de domínio de encaminhamento condicional)

```
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

Etapa 5. Forneça o endereço IP do novo servidor de nomes

Etapa 6. Forneça a prioridade para o servidor de nomes recém-adicionado.

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

Passo 7. Pressione Enter para sair do assistente.

Etapa 8. Digite commit para salvar as alterações.

Observação: para editar ou excluir qualquer servidor de nomes, você pode escolher EDIT e DELETE no dnsconfig.

Na opção SETUP, você pode definir as configurações de tempo de cache de DNS e detecção de DNS offline:

```
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]>

TTL mínimo em segundos para cache DNS: esta opção é para configurar o mínimo de segundos que o SWA armazenou em cache um registro. para obter mais informações, visite a seção cache DNS neste documento.

Digite o número de tentativas falhas antes de considerar um servidor DNS local como offline: se o servidor DNS não estiver respondendo a nenhuma consulta DNS, o contador será iniciado.

Quando atinge esse valor definido, esse servidor de nomes é considerado como servidor DNS offline e o SWA evita enviar a consulta DNS para esse servidor de nomes por uma duração de tempo predefinida (opção Avançar).

Quando o servidor DNS está marcado como offline, você pode ver esta mensagem de erro:

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

Insira o intervalo em segundos para sondar um servidor DNS local offline: quando um servidor DNS marcado como offline, após esse intervalo de tempo (em segundos), o SWA começa a enviar a consulta DNS para esse servidor de nome e o contador desse servidor DNS falha, a resposta é redefinida para zero.

Comandos CLI DNS

Criar registro manual

Para criar o manual "Um registro" você não pode usar ou editar o arquivo Hosts. Você pode usar o comando `localhosts hidden` de `dnsconfig` na CLI.

Observação: você deve confirmar as alterações depois de alterar essas configurações.

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 remove todos os registros DNS em cache da tabela de cache DNS:

```
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]>

O código de status HTTP 307 (Redirecionamento Temporário) indica que o recurso de destino reside temporariamente em um Uniform Resource Identifier (URI) diferente e o agente de usuário NÃO DEVERÁ alterar o método de solicitação se executar um redirecionamento automático para esse URI. Como o redirecionamento pode mudar com o tempo, o cliente deve continuar a usar o URI de solicitação efetiva original.

Mais detalhes sobre : [Qual é o Código de Status de Redirecionamento Temporário HTTP 307 - Kinsta](#)

Essas opções controlam como o SWA decide o endereço IP ao qual se conectar, ao avaliar uma solicitação de cliente na implantação de proxy transparente. Quando uma solicitação é recebida, o WSA vê um endereço IP de destino e um nome de host. O SWA deve decidir se confia no endereço IP destino original para a conexão TCP ou fazer sua própria resolução DNS e usar o endereço resolvido. O padrão é "0 = Sempre usar as respostas DNS em ordem", o que significa que o SWA não confia no cliente para fornecer o endereço IP.

Opção 1: SWA tenta o endereço IP fornecido pelo cliente para a conexão, mas retorna ao endereço resolvido se isso falhar. O endereço resolvido é usado para avaliação de política (categoria da Web, reputação da Web e assim por diante).

Opção 2: O SWA usa apenas o endereço fornecido pelo cliente para a conexão e não retorna. O endereço resolvido é usado para avaliação de política (categoria da Web, reputação da Web e assim por diante).

Opção 3: O SWA usa apenas o endereço fornecido pelo cliente para a conexão e não retorna. O endereço IP fornecido pelo cliente é usado para avaliação de política (categoria da Web, reputação da Web e assim por diante).

A opção escolhida depende da confiança que o administrador deve depositar no cliente ao determinar o endereço resolvido para um determinado nome de host. Se o cliente for um proxy de downstream, escolha a opção 3 para evitar a latência adicionada de pesquisas desnecessárias de DNS.


cache DNS

Para aumentar a eficiência e o desempenho, o Cisco SWA armazena entradas DNS para domínios aos quais você se conectou recentemente. O cache DNS permite que o SWA evite

pesquisas excessivas de DNS nos mesmos domínios. As entradas do cache DNS expiram devido ao TTL (Time to Live, tempo de vida restante) do registro.

Quando o TTL do registro no servidor DNS for maior que o tempo TTL do cache SWA dnsconfig, o cache dns usará o TTL do servidor DNS.

Quando o TTL do registro no servidor DNS for menor do que o tempo TTL do cache SWA dnsconfig, o cache dns usará o TTL da configuração dnsconfig do WSA.

 Cuidado: o SWA tem dois caches DNS, um é projetado para o processo Proxy e o outro é usado para o processo Interno.

Por padrão, o SWA armazenou em cache registros DNS por no mínimo 30 minutos, independentemente do TTL do registro. Os sites modernos que fazem uso intenso de redes de distribuição de conteúdo (CDN) teriam registros TTL baixos, já que seus endereços IP mudam com frequência.

Isso pode resultar em um cache de cliente com um endereço IP para um determinado servidor e o SWA armazenou em cache um endereço diferente para o mesmo servidor. Para combater isso, o TTL padrão do SWA pode ser reduzido para cinco minutos na seção SETUP no comando da CLI dsncfig.

Por exemplo, se o "TTL mínimo em segundos para o cache DNS" na configuração DNS tiver sido definido como 10 minutos e um registro tiver um TTL de 5 minutos, o TTL para o registro em cache aumentará para 10 minutos.

Por outro lado, se o TTL do registro for definido como 15 minutos, o SWA armazenará o registro por 15 minutos em seu cache.

No entanto, às vezes é necessário limpar o cache DNS das entradas. Entradas de cache DNS corrompidas ou expiradas podem ocasionalmente causar problemas com a entrega a um ou mais hosts remotos.


Esse problema geralmente ocorre depois que o equipamento está off-line para uma mudança de rede ou alguma outra circunstância.

Limpar o cache DNS da GUI

Etapa 1. Escolha Network no menu superior

Etapa 2. Escolher DNS

Etapa 3. Escolha Limpar Cache DNS

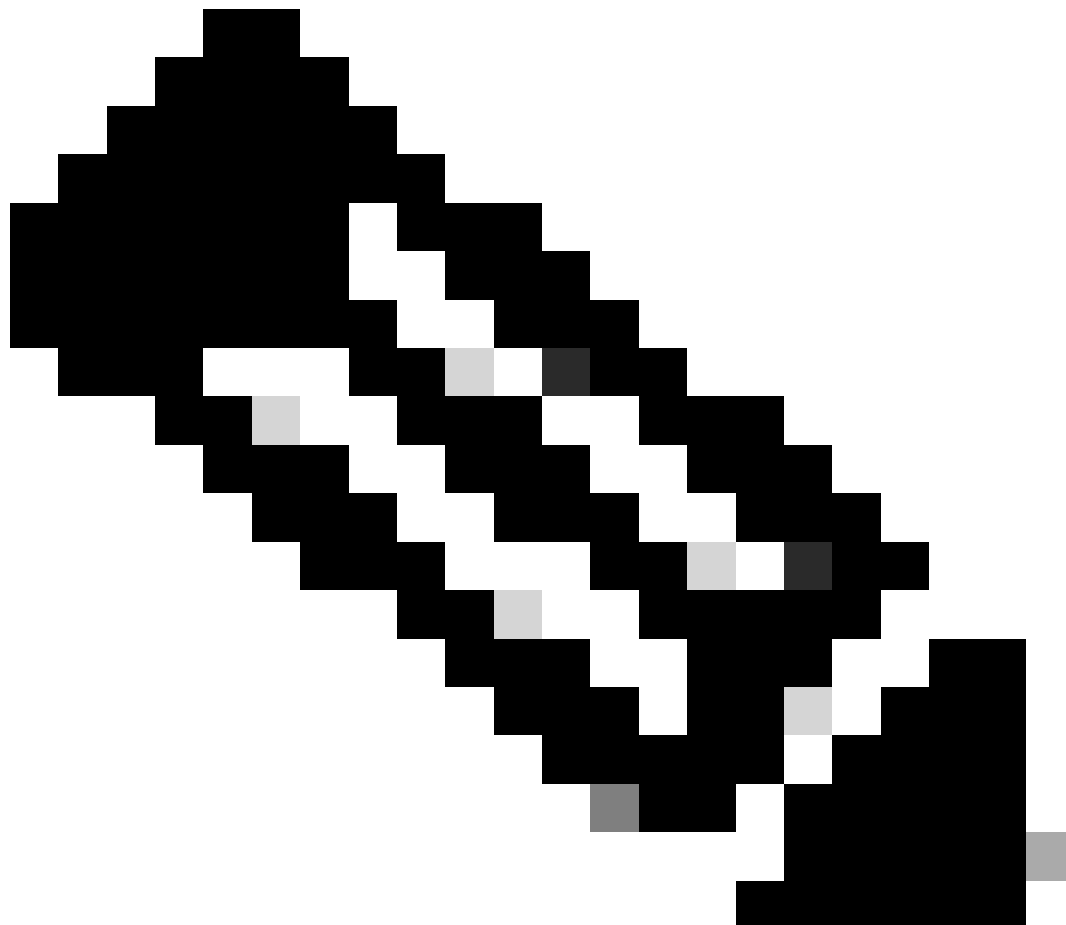
 Cuidado: este comando pode causar uma degradação temporária do desempenho enquanto o cache é preenchido novamente

Limpar o cache DNS da CLI

O cache DNS no Cisco WSA pode ser limpo pelo comando `dnsflushna CLI`.

Exibir cache DNS

Não há opção para visualizar o registro DNS em cache no SWA a partir da CLI ou da GUI.



Observação: não é possível consultar o cache DNS via `nslookup`.

Solucionar problemas de DNS

Exibir logs de DNS

Alguns tipos de log relacionados ao componente proxy da Web não estão habilitados. O tipo de log principal do proxy da Web, chamado de "Logs de Proxy Padrão", é ativado por padrão e

captura informações básicas em todos os módulos do Web Proxy.

Cada módulo Web Proxy também tem seu próprio tipo de log, que pode ser habilitado manualmente, conforme necessário.

Logs do sistema, Registra DNS, erro e atividade de confirmação, que é habilitada por padrão



Dica: se você alterar o nível de log dos logs do sistema para DEBUG, poderá ver as consultas e respostas DNS. Você pode alterar o nível de log da GUI e da CLI.

Alterar o nível de log dos logs do sistema a partir da GUI

Etapa 1. Escolha System Administrations no menu superior

Etapa 2. Escolher Inscrições de Log

Etapa 3. Escolher Logs do Sistema

Etapa 4. Escolha DEBUG na seção Nível de log

Etapa 5. Enviar

Etapa 6. Confirmar alterações

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> Add Row	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

Imagem - Alterar registros do sistema, nível de registro

Alterar o nível de log dos logs do sistema a partir da CLI

Etapa 1. Fazer login na CLI

Etapa 2. Digite logconfig

Etapa 3. Escolha EDITAR

Etapa 4. Insira o número associado a System_Logs

Etapa 5. Pressione Enter até atingir o nível Log

Etapa 6. Escolha o número 4, que é para Depuração

Passo 7. Pressione Enter até sair do assistente

Etapa 8. Para salvar as alterações, digite 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
```

 Dica: Depois de solucionar o problema, verifique se alterou o nível de log novamente para Information, caso contrário, haveria uma carga enorme no disco Input / Output (I/O) e o arquivo de log seria preenchido rapidamente.

nslookup

Use o comando nslookup para ver a resposta de resolução de nome em SWA para FQDNs diferentes.

Neste exemplo, na primeira tentativa de resolver o nome, o TTL é definido como 30 minutos.

Na segunda tentativa, podemos ver que o TTL é inferior a 30 minutos, o que indica que esse registro foi resolvido a partir do cache.

```
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
```

dig

dig é outro comando útil para consultar os registros DNS. Com o dig você pode especificar a interface de origem ou o servidor DNS no qual queremos consultar:

Neste exemplo, aqui está a consulta para o A-Record do servidor 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
```

O uso de 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

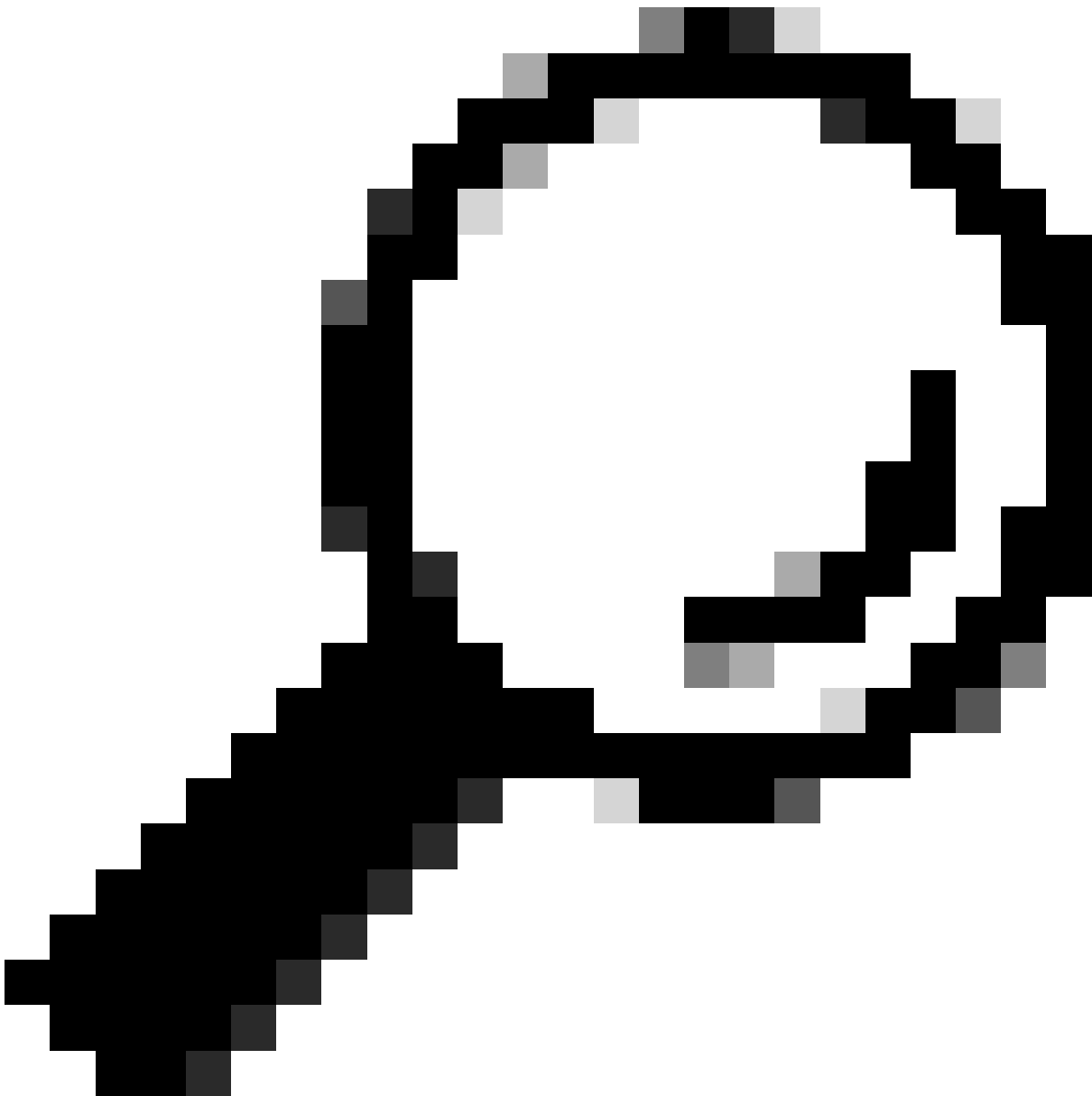
Specify the source IP address.

-t

Make query over tcp.

-x IP Address

Do a reverse lookup on this IP address.



Dica: você pode escolher o IP de origem a partir de qual interface deseja consultar a resolução de nome.

Resposta DNS lenta

Se o carregamento de todas ou algumas URLs levou mais tempo (em comparação com quando você atualiza a mesma página), é melhor verificar o tempo de resposta DNS. Há duas opções no SWA para verificar o tempo de resposta DNS:

- Configure o campo personalizado AccessLogs.
- Registros Trackstat.

Modificar logs de acesso para exibir estatísticas de DNS

Você pode modificar os logs de acesso para exibir a hora do DNS para cada solicitação da Web.

Etapa 1. Faça login na GUI.

Etapa 2. No menu Administração do sistema, escolha Inscrições de log.

Etapa 3. Na coluna Log Name, clique em accesslogs, ou no nome do recém-criado. Neste exemplo, TAC_access_logs.

Etapa 4. Na seção Campos personalizados, cole esta cadeia de caracteres:

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

Etapa 5. Enviar e confirmar as alterações.

Nome do campo personalizado	Campo Personalizado	Logs W3C	Descrição
resposta DNS	%:<d	x-p2p-dns-wait-time	Tempo gasto pelo Web Proxy para enviar a solicitação de DNS (Domain Name Request) ao processo DNS do Web Proxy.
Total de DNS	%:>d	x-p2p-dns-svc-time	Tempo gasto pelo processo DNS do Web Proxy para enviar de volta um resultado DNS ao Web Proxy.

Para obter mais informações sobre como editar campos personalizados em registros de acesso, você pode visitar este link: [Configurar parâmetro de desempenho em registros de acesso - Cisco](#)

Tempo total de resposta DNS em logs Trackstat

Você pode exibir estatísticas do serviço DNS e outros serviços internos nos logs trackstat. Você pode acessar logs trackstats conectando-se via FTP ao seu SWA.

Neste exemplo, você pode ver as estatísticas de cache e o número de respostas DNS, categorizadas por tempo decorrido do servidor DNS desde que o SWA foi reinicializado pela

última vez.

```
...  
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
```

Por exemplo, na última linha, indica que 190 consultas DNS levaram mais de 6.309 milissegundos (aproximadamente 6 segundos) para serem concluídas desde que o SWA foi reinicializado pela última vez.

Para descobrir o número exato em um período de tempo, subtraia esses valores para a hora inicial e final.

Por exemplo, para identificar o tempo de resposta DNS de 10:00 AM às 11:00 AM, colete estatísticas para 11:00 AM e subtraia-as das estatísticas de 10:00 AM.

O resultado é o tempo de resposta DNS das 10:00 às 11:00 para a data desejada.



Observação: os logs de monitoramento de estatísticas são coletados a cada 5 minutos.

Captura do pacote

Você pode capturar pacotes para visualizar as solicitações e respostas DNS, para filtrar apenas para DNS que você pode usar: porta 53 .

Para iniciar a captura de pacotes a partir da GUI:

Etapa 1. Escolha Support and Help no canto superior direito

Etapa 2. Escolha a captura de pacotes

Etapa 3. (Opcional) Escolha Editar configurações para adicionar filtro

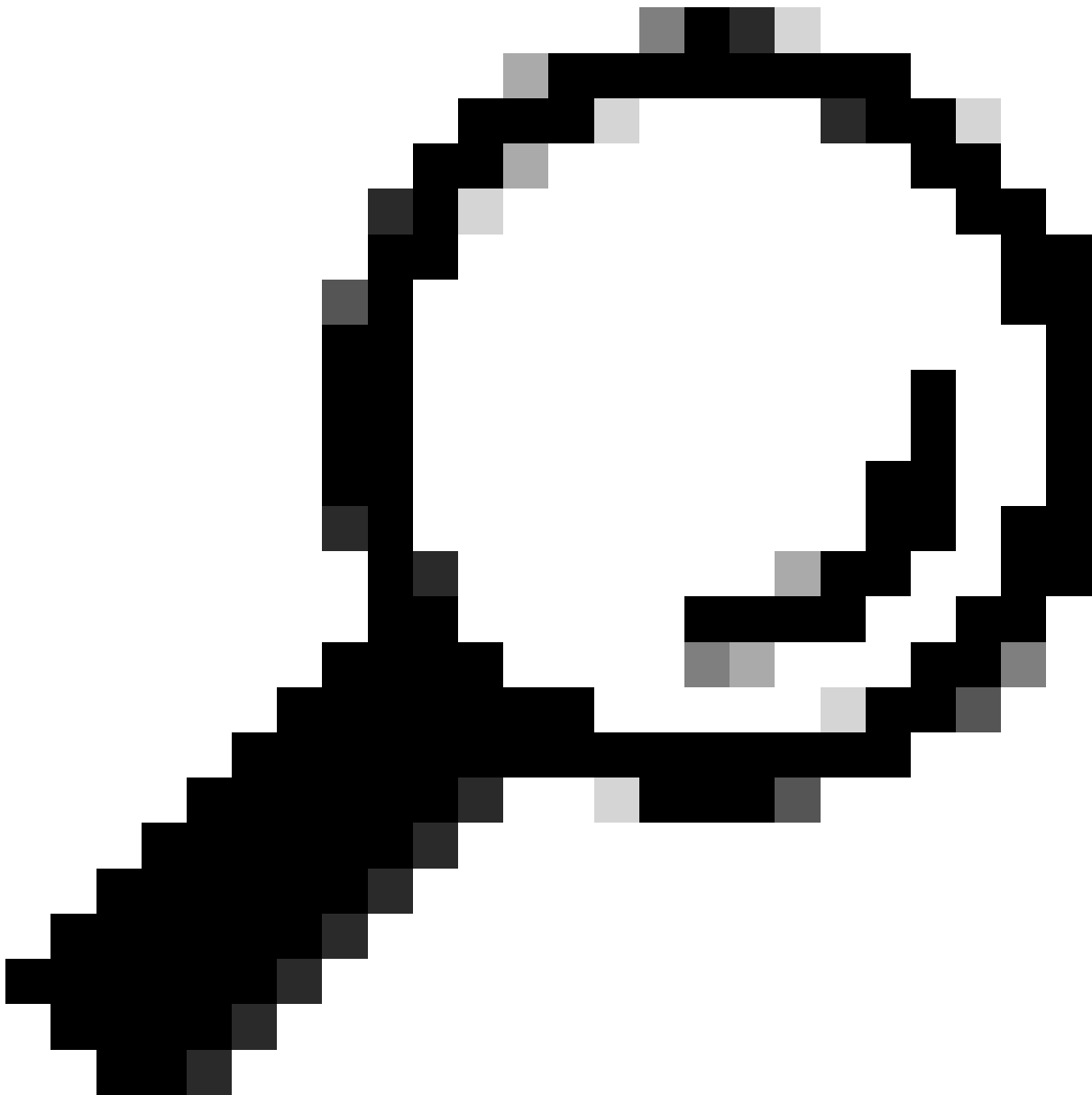
Etapa 4. (Opcional) Escolha sua(s) interface(s) e digite a porta 53 na seção Filtro personalizado.

Etapa 5. (Opcional) Escolha Enviar

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"/>

Imagem - Adicionar filtro para capturar pacotes DNS



Dica: as configurações de captura de pacote estão disponíveis para uso imediato quando enviadas. Confirme as alterações para salvar estas configurações permanentemente para uso futuro.

Etapa 6. Escolha Start Capture.

Etapa 7. (Opcional) Gere tráfego se precisar solucionar problemas de um site específico ou acesso a URL.

Etapa 8. Parar captura

Etapa 9. Aguarde a página ser atualizada e, em seguida, escolha a primeira captura de pacote na lista "Gerenciar Arquivos de Captura de Pacotes"

Etapa 10. Escolha Download File

L4TM

O Monitor de tráfego da camada 4 escuta o tráfego de rede que chega por todas as portas em cada Secure Web Appliance e compara nomes de domínio e endereços IP com entradas em suas próprias tabelas de banco de dados para determinar se o tráfego de entrada e saída deve ser permitido.

Quando os clientes internos são infectados com malware e tentam se comunicar através de portas e protocolos fora do padrão, o L4 Traffic Monitor impede a atividade de se comunicar com a residência para sair da rede corporativa.

Por padrão, o L4 Traffic Monitor é ativado e definido para monitorar o tráfego em todas as portas, incluindo DNS e outros serviços.

Para obter mais informações sobre o monitor de tráfego de Camada 4, consulte o guia do usuário.

Erros

Página de Notificação

Por padrão, o SWA exibe uma página de notificação para informar aos usuários que eles foram bloqueados e o motivo do bloqueio

Nome do Arquivo e Título da Notificação: ERR_DNS_FAIL (Falha de DNS)

Descrição: página de erro exibida quando a URL solicitada contém um nome de domínio inválido.

Texto de Notificação: A resolução do nome do host (pesquisa DNS) para este nome de host <hostname > falhou.

O endereço de Internet pode estar com erro de ortografia ou obsoleto, o host <nome do host > pode estar temporariamente indisponível ou o servidor DNS pode estar sem resposta.

Verifique a ortografia do endereço de Internet inserido. Se estiver correto, tente esta solicitação mais tarde.

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

Imagem - Erro de DNS FAIL

Código de Resultado do Log de Acesso NENHUM

Os códigos de resultado de transação no arquivo de registro de acesso descrevem como o equipamento resolve as solicitações do cliente. Se no log de acesso o Código do resultado for NONE, isso significa que houve um erro na transação. Por exemplo, uma falha de DNS ou tempo limite de gateway.

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

Falha ao inicializar o cache DNS

Se um alerta com a mensagem "Falha ao inicializar o cache DNS" for gerado quando um equipamento for reinicializado, isso significa que o sistema não pôde entrar em contato com seus servidores DNS primários.

Isso pode acontecer no momento da inicialização se o subsistema DNS ficar on-line antes que a conectividade de rede seja estabelecida. Se essa mensagem for exibida em outras ocasiões, pode indicar problemas de rede ou que a configuração DNS não está definida como um servidor válido

Máximo de falhas de consulta ao servidor DNS atingido

Se um ou alguns dos servidores DNS configurados no SWA não responderem às consultas DNS, o SWA os considerará como off-line e não enviará as consultas DNS a eles por um período de tempo predefinido. Para obter mais informações, leia "Configure DNS from CLI" neste artigo.

DNS_FAIL

Quando o SWA recebe uma solicitação HTTP e não consegue resolver o nome do host, por padrão, o SWA retornaria uma resposta como:

```
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
```

Esse recurso é chamado de "expansão do nome do servidor".

O WSA faz isso em tentativas que o nome de host redirecionado resolveria a página esperada para o cliente.

Você pode alterar o "formato de URL para o redirecionamento HTTP 307 em falha de pesquisa de DNS", para obter mais informações, consulte a seção [advanceproxyconfig](#) neste artigo.

O WSA trata a solicitação DNS que retorna ServFail como uma falha.

Por exemplo, NXDOMAIN retornaria "DNS_FAIL" em vez de "SERVER_NAME_EXPANSION"

Informações Relacionadas

[Manual do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance](#)

[Use as práticas recomendadas de dispositivos da Web seguros - Cisco](#)

[Cisco Content Hub - Introdução ao Sistema de Nomes de Domínio](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.