Dépannage du service DNS de l'appliance Web sécurisée

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Concept DNS
  - Service DNS dans les déploiements de proxy
- Configuration des paramètres DNS
  - Meilleure pratique
  - Configurer DNS dans l'interface utilisateur graphique
  - Configurer DNS à partir de CLI
- Commandes CLI DNS
  - Créer un enregistrement manuel
  - rinçage
  - advanced proxyconfig
- Cache DNS
  - Effacer le cache DNS de l'interface utilisateur graphique
  - Effacer le cache DNS de la CLI
  - Afficher le cache DNS
- Dépannage de DNS
  - Afficher les journaux DNS
    - Modifier le niveau du journal des journaux système depuis l'interface utilisateur
    - Modifier le niveau du journal des journaux système depuis CLI
  - nslookup
  - fouiller
  - Réponse DNS lente
    - Modifier les journaux d'accès pour afficher les statistiques DNS
    - Temps de réponse DNS global dans TrackstatLogs
  - Capture de paquets
- L4TM
- Erreurs
  - Page Notification
  - Code de résultat ACCESSLOG AUCUN
  - Échec du démarrage du cache DNS
  - Nombre maximal d'échecs de requête de serveur DNS atteint
  - ÉCHEC_DNS
- Autres informations utiles

Introduction

Ce document décrit la configuration du service de noms de domaine (DNS) et comment dépanner dans l'appareil Web sécurisé (SWA).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appareil Web sécurisé physique ou virtuel (SWA) installé.
- Licence activée ou installée.
- Client Secure Shell (SSH).
- L'Assistant de configuration est terminé.

- Accès administratif au SWA.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Concept DNS

DNS est le système Internet qui mappe les noms d'objets (généralement des noms d'hôtes) en adresses IP (Internet Protocol) ou en autres valeurs d'enregistrement de ressources.

- L'espace de noms d'Internet est divisé en domaines et la responsabilité de la gestion des noms au sein de chaque domaine est déléguée, généralement aux systèmes au sein de chaque domaine.
- L'espace de noms de domaine est divisé en zones appelées zones qui sont des points de délégation dans l'arborescence DNS.

Une zone contient tous les domaines d'un certain point vers le bas, à l'exception de ceux pour lesquels d'autres zones font autorité. Une zone possède généralement un serveur de noms faisant autorité, souvent plusieurs.

Dans une organisation, vous pouvez avoir de nombreux serveurs de noms, mais les clients Internet ne peuvent interroger que ceux que les serveurs de noms racine connaissent.

Les autres serveurs de noms répondent uniquement aux requêtes internes.

Le DNS est basé sur un modèle client/serveur. Dans ce modèle, les serveurs de noms stockent des données sur une partie de la base de données DNS et les fournissent aux clients qui interrogent le serveur de noms sur le réseau.

Les serveurs de noms sont des programmes qui s'exécutent sur un hôte physique et stockent des données de zone. En tant qu'administrateur d'un domaine, vous configurez un serveur de noms avec la base de données de tous les enregistrements de ressources (RR) décrivant les hôtes dans votre ou vos zones

Service DNS dans les déploiements de proxy

Dans le déploiement explicite : le proxy exécute des requêtes DNS

Dans Transparent Deployment : les requêtes DNS s'exécutent sur l'ordinateur client.

Configuration des paramètres DNS

Vous pouvez configurer DNS à partir de l'interface graphique utilisateur (GUI) et de l'interface de ligne de commande (CLI).

AsyncOS for Web peut utiliser les serveurs DNS racine Internet ou vos propres serveurs DNS. Si SWA utilise des serveurs DNS racine Internet, vous pouvez spécifier d'autres serveurs à utiliser pour des domaines spécifiques.

Étant donné qu'un autre serveur DNS s'applique à un seul domaine, il doit faire autorité (fournir des enregistrements DNS définitifs) pour ce domaine.

AsyncOS prend en charge le DNS partagé, où les serveurs internes sont configurés pour des domaines spécifiques et les serveurs DNS externes ou racine sont configurés pour d'autres domaines.

Si SWA utilise un serveur DNS sur site, nous pouvons également spécifier les domaines d'exception et le serveur DNS associé.

Meilleure pratique

Les meilleures pratiques en matière de sécurité suggèrent que chaque réseau doit héberger deux résolveurs DNS : un pour les enregistrements faisant autorité au sein d'un domaine local et un pour la résolution récursive des domaines Internet.

Pour y remédier, le SWA permet de configurer des serveurs DNS pour des domaines spécifiques.

Dans le cas d'un serveur DNS disponible pour les requêtes locales et récursives, tenez compte de la charge supplémentaire que cela ajouterait s'il est utilisé pour toutes les requêtes SWA.

La meilleure option peut être d'utiliser le résolveur interne pour les domaines locaux et les résolveurs Internet racine pour les domaines externes. Cela dépend du profil de risque et de la tolérance de l'administrateur.

Les serveurs DNS secondaires doivent être configurés au cas où le serveur principal ne serait pas disponible. Si tous les serveurs sont configurés avec la même priorité, l'adresse IP du serveur est choisie au hasard.

Selon le nombre de serveurs configurés, le délai d'attente d'un serveur donné varie. Le délai d'attente d'une requête est indiqué dans ce tableau, pour un maximum de six serveurs DNS :

Nombre de serveurs DNS	Délai de requête (dans l'ordre)
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

Pour plus d'informations, consultez : Cisco Web Security Appliance Best Practices Guidelines - Cisco

Configurer DNS dans l'interface utilisateur graphique

Pour configurer DNS à partir de l'interface utilisateur graphique, procédez comme suit :

Étape 1. Choisissez Network dans le menu supérieur.

Étape 2 : sélectionnez DNS.

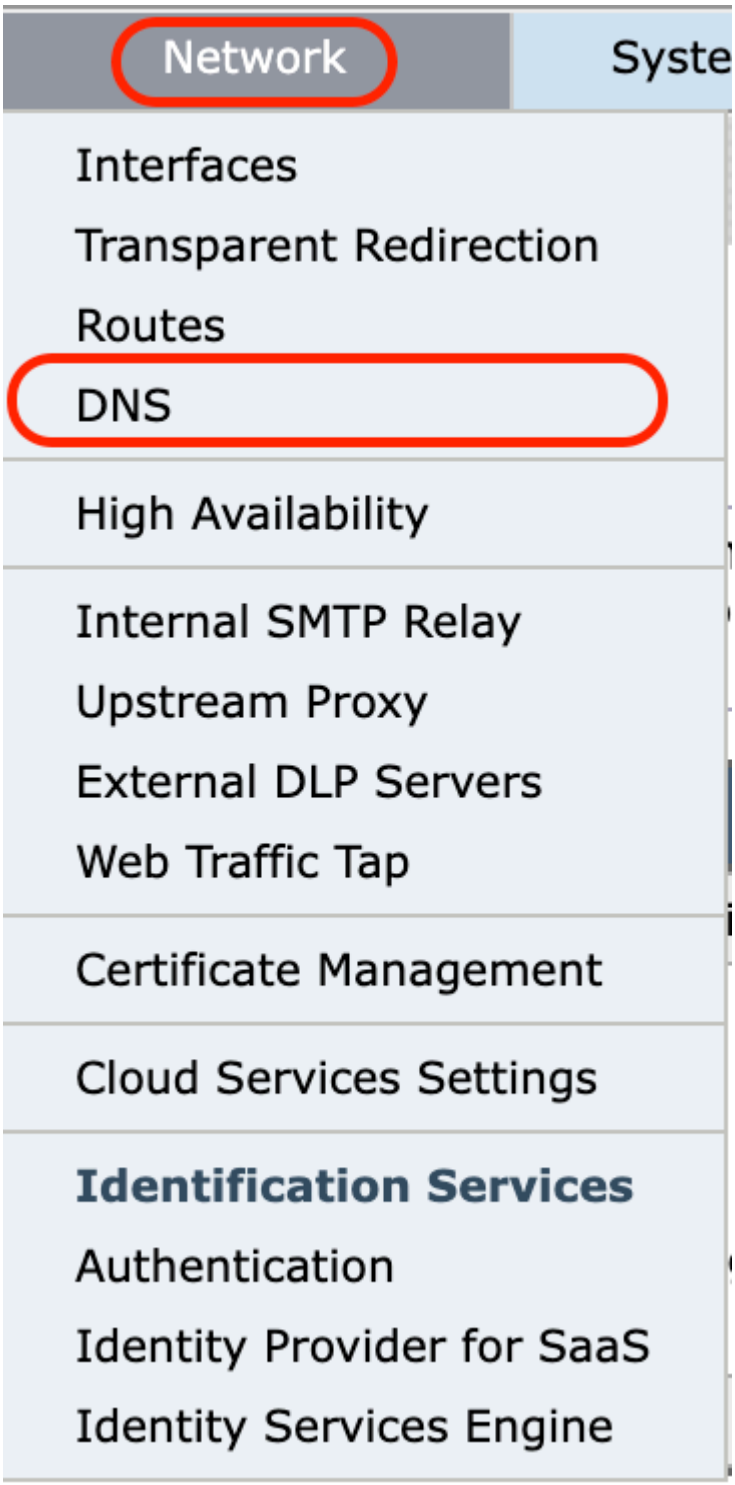


Image-GUI - Configuration des paramètres DNS

Étape 3. Sélectionnez Modifier les paramètres.
Étape 4 : configuration des paramètres DNS selon les besoins

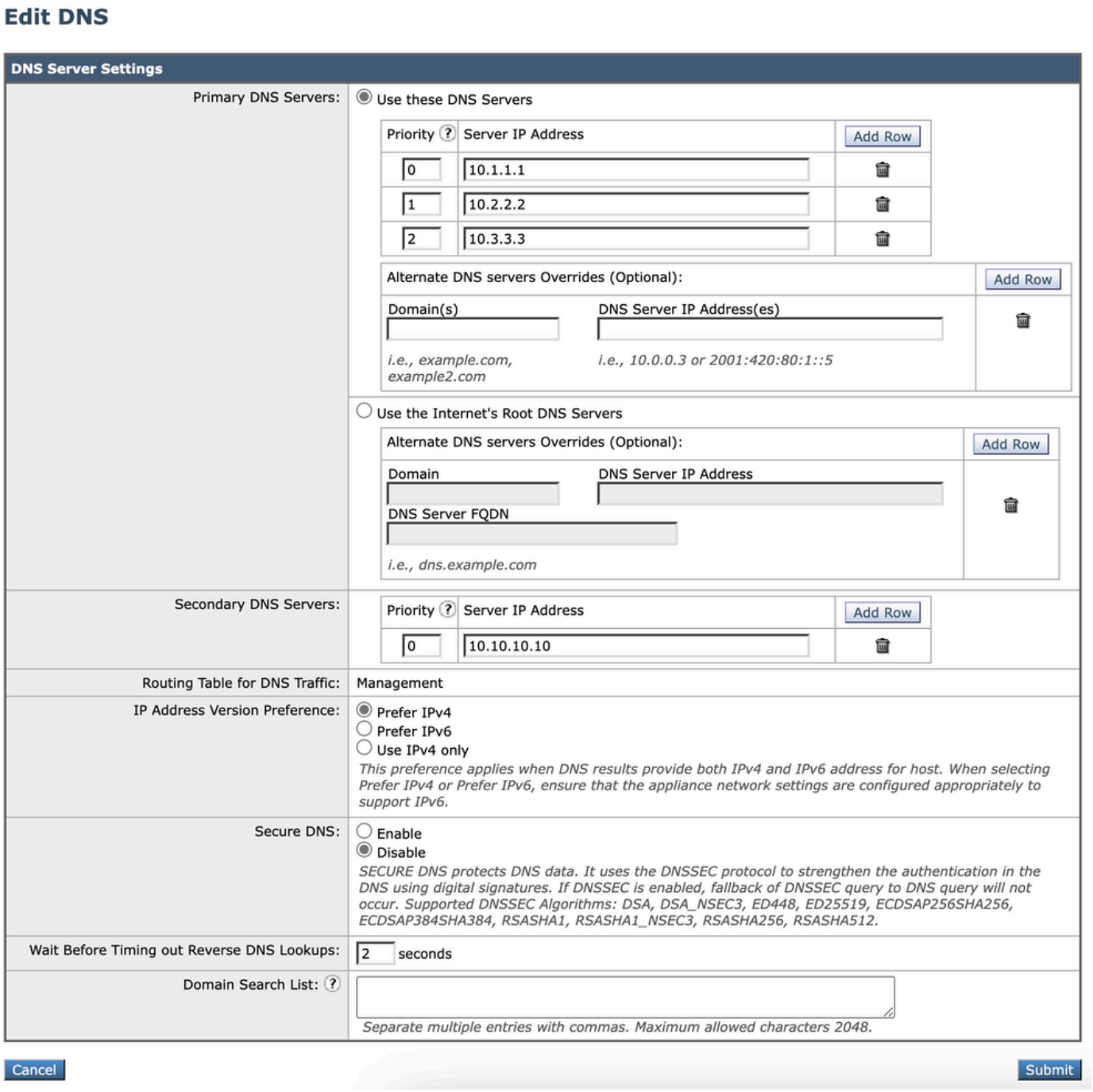


Image - Configuration DNS

- Utilisez les serveurs DNS suivants : Le ou les serveurs DNS locaux que l'appliance peut utiliser pour résoudre les noms d'hôte.
- Remplacement des serveurs DNS secondaires (facultatif) : Serveurs DNS de référence pour les domaines.

Remarque : AsyncOS ne respecte pas la préférence de version pour les requêtes FTP transparentes.

Remarque : En mode connecteur cloud, l'appliance de sécurité Web Cisco prend en charge

IPv4 uniquement

- Utilisez les serveurs DNS racine Internet. Choisissez d'utiliser les serveurs DNS racine Internet pour les recherches de service de noms de domaine lorsque l'appliance n'a pas accès aux serveurs DNS sur votre réseau.

Les serveurs DNS racine Internet ne résolvent pas les noms d’hôtes locaux.

Remarque : Si vous avez besoin que votre appliance résolve les noms d'hôtes locaux, utilisez un serveur DNS local ou ajoutez les entrées statiques appropriées au DNS local à partir de l'interface de ligne de commande (CLI).

- Domain Search List : liste de recherche de domaine DNS utilisée lorsqu'une demande est envoyée à un nom d'hôte nu sans point (.). Les domaines spécifiés peuvent être essayés tour à tour, dans l'ordre entré (de gauche à droite), pour voir si une correspondance DNS pour le nom d'hôte plus le domaine peut être trouvée.

- Routing Table for DNS Traffic : spécifie l'interface par laquelle le service DNS achemine le trafic.
- Wait Before Timing out Reverse DNS Lookups : temps d'attente en secondes avant l'expiration des recherches DNS inversées sans réponse.

Les serveurs DNS secondaires reçoivent des requêtes de nom d'hôte lorsque les serveurs DNS principaux renvoient les erreurs suivantes :

- "Aucune erreur", aucune réponse reçue
- Section « Le serveur n'a pas pu terminer la demande » sans réponse
- "Erreur de nom", aucune réponse reçue
- "Fonction non implémentée"
- "Le serveur a refusé de répondre à la requête"

Remarque : AsyncOS évalue les transactions en fonction des stratégies avant d'évaluer les dépendances externes pour éviter toute communication externe inutile de la part de l'appliance. Par exemple, si une transaction est bloquée en fonction d'une stratégie qui bloque les URL non classées, la transaction n'échouera pas en raison d'une erreur DNS.

- Priority : une valeur de 0 a la priorité la plus élevée. Une adresse IP aléatoire est sélectionnée si les deux ont la même priorité.

Configurer DNS à partir de CLI

Vous pouvez utiliser dnsconfig à partir de l'interface de ligne de commande pour configurer les paramètres DNS.

Étape 1. Tapez dnsconfig dans 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.
[]>
```

Étape 2. Pour ajouter un nouveau serveur DNS à la liste, tapez NEW et appuyez sur Entrée.

Étape 3. Choisissez entre les serveurs de noms DNS principaux ou les serveurs de noms DNS secondaires auxquels vous souhaitez ajouter un nouveau serveur de noms.

```
[]> 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
```

Étape 4. Choisissez d’ajouter un nouveau serveur de noms ou un autre serveur de domaine (transfert conditionnel du nom de domaine)

```
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
```

Étape 5. Fournissez l’adresse IP du nouveau serveur de noms

Étape 6. Indiquez la priorité du nouveau serveur de noms ajouté.

```
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
```

Étape 7. Appuyez sur Entrée pour quitter l'assistant.

Étape 8. Tapez commit pour enregistrer les modifications.



Remarque : Pour modifier ou supprimer des serveurs de noms, vous pouvez choisir EDIT et DELETE dans dnsconfig.

À partir de l'option SETUP, vous pouvez configurer l'heure de cache DNS et les paramètres de détection DNS hors connexion :

```
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 compatibilit
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]>
```

- Durée de vie minimale en secondes pour le cache DNS : Cette option permet de configurer les secondes minimales pendant lesquelles SWA a mis un enregistrement en cache. pour plus d'informations, consultez la section cache DNS de ce document.
- Entrez le nombre de tentatives ayant échoué avant de considérer un serveur DNS local comme hors connexion : Si le serveur DNS ne répond à aucune requête DNS, le compteur démarre. Lorsqu'il atteint cette valeur définie, ce serveur de noms est considéré comme un serveur DNS hors connexion et SWA évite d'envoyer la requête DNS à ce serveur de noms pour une durée prédéfinie (option Suivant). Lorsque le serveur DNS est marqué comme hors connexion, le message d'erreur suivant s'affiche :

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

- Entrez l'intervalle en secondes pour l'interrogation d'un serveur DNS local hors connexion : Lorsqu'un serveur DNS est marqué comme hors connexion, après cet intervalle de temps (en secondes), SWA commence à envoyer une requête DNS à ce serveur de noms et le compteur pour ce serveur DNS en échec de réponse est remis à zéro.

Commandes CLI DNS

Créer un enregistrement manuel

Pour créer un enregistrement manuel, vous ne pouvez pas utiliser ou modifier le fichier Hosts. Vous pouvez utiliser la commande localhosts hidden de dnsconfig dans l'interface de ligne de commande (CLI).



Remarque : Vous devez valider les modifications après avoir modifié ces configurations.

```
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
```

rinçage

dnsflush supprime tous les enregistrements DNS mis en cache de la table de cache DNS :

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

advanced proxyconfig

```
 advancedproxyconfig

Choose a parameter group:
- AUTHENTICATION - Authentication related parameters
- CACHING - Proxy Caching related parameters
- DNS - DNS related parameters
- EUN - EUN related parameters
- NATIVEFTP - Native FTP related parameters
- FTPOVERHTTP - FTP Over HTTP related parameters
- HTTPS - HTTPS related parameters
- SCANNING - Scanning related parameters
```

```
- PROXYCONN - Proxy connection header related parameters
- CUSTOMHEADERS - Manage custom request headers for specific domains
- MISCELLANEOUS - Miscellaneous proxy related parameters
- SOCKS - SOCKS Proxy parameters
- CONTENT-ENCODING - Block content-encoding types
- SCANNERS - Scanner related parameters
[]> DNS

Enter values for the DNS options:

Enter the URL format for the HTTP 307 redirection on DNS lookup failure.
[%P://www.%H.com/%u]>

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

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

Select one of the following options:
0 = Always use DNS answers in order
1 = Use client-supplied address then DNS
2 = Limited DNS usage
3 = Very limited DNS usage

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

For all options, DNS will be used when Destination IP Addresses are used in
policy membership.
Find web server by:
[0]>
```

Le code d'état HTTP 307 (Redirection temporaire) indique que la ressource cible réside temporairement sous un URI (Uniform Resource Identifier) différent et que l'agent utilisateur NE DOIT PAS modifier la méthode de requête s'il effectue une redirection automatique vers cet URI. Comme la redirection peut changer au fil du temps, le client doit continuer à utiliser l'URI de demande effective d'origine.

Plus de détails : [Qu'est-ce que le code d'état de redirection temporaire HTTP 307 - Kinsta]

Ces options contrôlent la façon dont SWA décide de l'adresse IP à laquelle se connecter, lors de l'évaluation d'une requête client dans un déploiement de proxy transparent. Lorsqu'une demande est reçue, SWA voit une adresse IP de destination et un nom d'hôte. SWA doit décider s'il doit faire confiance à l'adresse IP de destination d'origine pour la connexion TCP ou s'il doit effectuer sa propre résolution DNS et utiliser l'adresse résolue. La valeur par défaut est 0 = Toujours utiliser les réponses DNS dans l'ordre, ce qui signifie que SWA n'approuve pas le client pour fournir l'adresse IP.

Option 1 : SWA tente l'adresse IP fournie par le client pour la connexion, mais revient à l'adresse

résolue si cela échoue. L'adresse résolue est utilisée pour l'évaluation des stratégies (catégorie Web, réputation Web, etc.).

Option 2 : SWA utilise uniquement l'adresse fournie par le client pour la connexion et ne se rétablit pas. L'adresse résolue est utilisée pour l'évaluation des stratégies (catégorie Web, réputation Web, etc.).

Option 3 : SWA utilise uniquement l'adresse fournie par le client pour la connexion et ne se rétablit pas. L'adresse IP fournie par le client est utilisée pour l'évaluation des stratégies (catégorie Web, réputation Web, etc.).

L'option choisie dépend de la confiance que l'administrateur doit accorder au client lorsqu'il détermine l'adresse résolue pour un nom d'hôte donné. Si le client est un proxy en aval, choisissez l'option 3 pour éviter la latence ajoutée des recherches DNS inutiles.

Cache DNS

Pour améliorer l'efficacité et les performances, Cisco SWA stocke les entrées DNS des domaines auxquels vous vous êtes récemment connecté. Le cache DNS permet à SWA d'éviter les recherches DNS excessives des mêmes domaines. Les entrées du cache DNS expirent en raison de la durée de vie (TTL) de l'enregistrement.

- Lorsque la durée de vie de l'enregistrement dans le serveur DNS est supérieure à la durée de vie du cache dnsconfig SWA, le cache dns utilise la durée de vie du serveur DNS.
- Lorsque la durée de vie de l'enregistrement dans le serveur DNS est inférieure à la durée de vie du cache dnsconfig SWA, le cache dns utilise la durée de vie du paramètre dnsconfig SWA.

⚠ Mise en garde : SWA a deux cache DNS, l'un est conçu pour le processus Proxy et l'autre est utilisé pour le processus interne.

Par défaut, le SWA a mis en cache les enregistrements DNS pendant au moins 30 minutes, quelle que soit la durée de vie de l'enregistrement. Les sites Web modernes qui font un usage intensif des réseaux de diffusion de contenu (CDN) auraient des enregistrements TTL faibles car leurs adresses IP changent fréquemment.

Cela peut entraîner la mise en cache par un client d'une adresse IP pour un serveur donné et la mise en cache par SWA d'une adresse différente pour le même serveur. Pour contrer cela, la durée de vie par défaut de SWA peut être réduite à cinq minutes à partir de la section SETUP dans la commande dsnconfig CLI.

Par exemple, si la durée de vie minimale en secondes pour le cache DNS dans la configuration DNS a été définie sur 10 minutes et qu'un enregistrement a une durée de vie de 5 minutes, la durée de vie pour l'enregistrement mis en cache a augmenté à 10 minutes.

D'autre part, si la durée de vie de l'enregistrement est définie sur 15 minutes, SWA stocke l'enregistrement pendant 15 minutes dans son cache. Cependant, il est parfois nécessaire d'effacer les entrées du cache DNS. Des entrées de cache DNS endommagées ou expirées peuvent occasionnellement entraîner des problèmes de livraison à un ou plusieurs hôtes distants. Ce problème se produit généralement après que l'appliance a été hors connexion pour un déplacement réseau ou dans d'autres circonstances.

Effacer le cache DNS de l'interface utilisateur graphique

Étape 1. Choisissez Network dans le menu supérieur.

Étape 2. Sélectionnez DNS.

Étape 3. Sélectionnez Clear DNS Cache.

⚠ Mise en garde : Cette commande peut entraîner une dégradation temporaire des performances lorsque le cache est rechargé

Effacer le cache DNS de la CLI

Le cache DNS dans Cisco SWA peut être effacé par la commande dnsflush de l'interface de ligne de commande.

Afficher le cache DNS

Il n'y a aucune option pour afficher l'enregistrement DNS mis en cache dans SWA depuis CLI ou GUI.

Remarque : Vous ne pouvez pas interroger le cache DNS via nslookup.

Dépannage de DNS

Afficher les journaux DNS

Certains types de journaux associés au composant proxy Web ne sont pas activés. Le type de journal de proxy Web principal, appelé « Journaux de proxy par défaut », est activé par défaut et capture les informations de base sur tous les modules de proxy Web.

Chaque module Proxy Web possède également son propre type de journal que vous pouvez activer manuellement selon vos besoins.

Journaux système, enregistre le DNS, les erreurs et les activités de validation. qui est activé par défaut

---

Conseil : Si vous modifiez le niveau de journalisation des journaux système en DEBUG, vous pouvez voir les requêtes et les réponses DNS.Vous pouvez modifier le niveau de journalisation à partir de l'interface graphique et de l'interface de ligne de commande.

Modifier le niveau du journal des journaux système depuis l'interface utilisateur

Étape 1. Sélectionnez System Administrations dans le menu supérieur.

Étape 2. Choisissez Log Subscriptions.

Étape 3. Sélectionnez Journaux système.

Étape 4. Choisissez DEBUG dans la section Log Level.

Étape 5. Envoyer.

Étape 6. Validez les modifications.

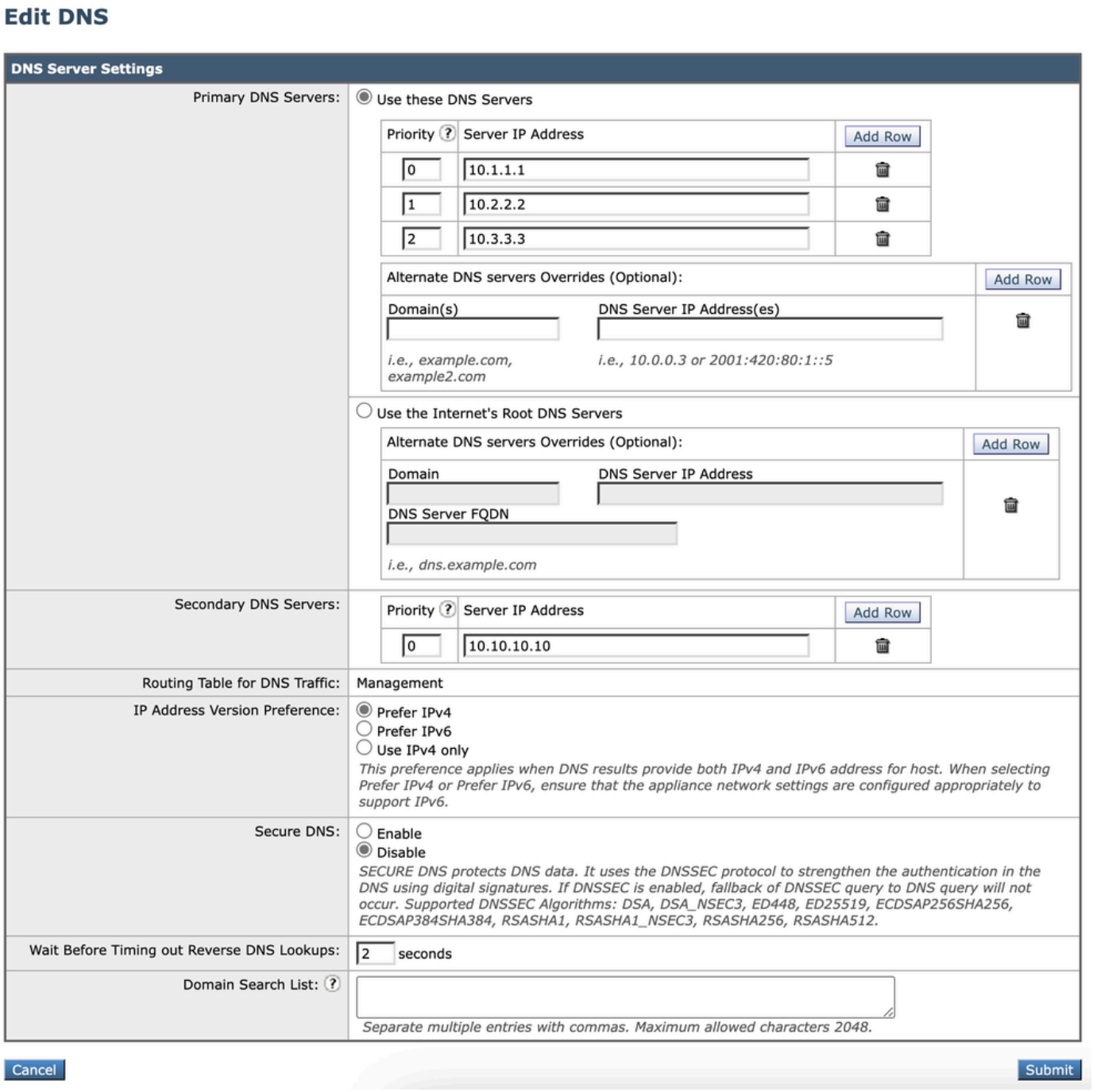


Image - Modifier les journaux système, niveau de journal

Modifier le niveau du journal des journaux système depuis CLI

Étape 1. Connectez-vous à l’interface de ligne de commande

Étape 2. Tapez logconfig.

Étape 3. Sélectionnez MODIFIER.

Étape 4. Entrez le numéro associé à System_Logs.

Étape 5. Appuyez sur Entrée jusqu'à atteindre le niveau de consignation.

Étape 6. Choisissez le numéro 4 pour le débogage

Étape 7. Appuyez sur Entrée jusqu'à ce que vous quittiez l'assistant.

Étape 8. Pour enregistrer les modifications, tapez 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
```


Conseil : une fois le dépannage terminé, assurez-vous de redéfinir le niveau du journal sur Information, sinon il y aurait une charge énorme sur le disque Entrée / Sortie (E/S) et le fichier journal serait rempli trop rapidement.

nslookup

Utilisez la commande nslookup pour voir la réponse de résolution de nom dans SWA pour différents FQDN.

Dans cet exemple, lors de la première tentative de résolution du nom, la durée de vie est définie sur 30 minutes.

Lors de la deuxième tentative, nous pouvons voir que la durée de vie est inférieure à 30 minutes, ce qui indique que cet enregistrement a été résolu à partir du 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
```

fouiller

dig est une autre commande utile pour interroger les enregistrements DNS. Avec dig, vous pouvez spécifier l'interface source ou le serveur DNS dans lequel nous voulons interroger :

Dans cet exemple, voici la requête pour A-Record du serveur 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
```

L'utilisation 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.
```



Conseil : Vous pouvez choisir l'adresse IP source à partir de laquelle vous souhaitez

interroger la résolution de nom.

Réponse DNS lente

Si le chargement de l'ensemble ou d'une partie des URL a pris plus de temps (par rapport à l'actualisation de la même page), il est préférable de vérifier le temps de réponse DNS. Il existe deux options dans SWA pour vérifier le temps de réponse DNS :

- Configurez le champ personnalisé AccessLogs.
- Journaux Trackstat.

Modifier les journaux d'accès pour afficher les statistiques DNS

Vous pouvez modifier les journaux d'accès pour afficher l'heure DNS de chaque demande Web.

Étape 1. Connectez-vous à l’interface graphique utilisateur.

Étape 2. Dans le menu System Administration, sélectionnez Log Subscriptions.

Étape 3. Dans la colonne Nom du journal, cliquez sur Accéder aux journaux ou sur le nom du journal nouvellement créé. Dans cet exemple, TAC_access_logs.

Étape 4. Dans la section Champs personnalisés, collez cette chaîne :

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

Étape 5. Soumettre et valider les modifications

Nom du champ personnalisé	Champ personnalisé	Journaux W3C	Description
réponse DNS	% : <d	x-p2p-dns-wait-time	Temps nécessaire au proxy Web pour envoyer la demande DNS (Domain Name Request) au processus

			DNS du proxy Web.
Total DNS	%:>d	x-p2p-dns-svc-time	Temps nécessaire au processus DNS du proxy Web pour renvoyer un résultat DNS au proxy Web.

Pour plus d'informations sur la façon de modifier les champs personnalisés dans les journaux d'accès, vous pouvez visiter ce lien : Configurer le paramètre de performance dans les journaux d'accès - Cisco

Temps de réponse DNS global dans les journaux Trackstat

Vous pouvez afficher les statistiques du service DNS et d'autres services internes dans les journaux trackstat. Vous pouvez accéder aux journaux trackstats en vous connectant via FTP à votre SWA.

Dans cet exemple, vous pouvez voir les statistiques du cache et le nombre de réponses DNS, classées par temps écoulé depuis le dernier redémarrage de SWA depuis le serveur DNS.

```
...
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
```

Par exemple, dans la dernière ligne, elle indique que 190 requêtes DNS ont mis plus de 6 309 millisecondes (environ 6 secondes) à se terminer depuis le dernier redémarrage de SWA.

Pour connaître le nombre exact dans une période, soustrayez ces valeurs pour l'heure de début et l'heure de fin.

Par exemple, pour identifier le temps de réponse DNS de 10:00 à 11:00, collectez les statistiques pour 11:00 et soustrayez-les des statistiques de 10:00.

Le résultat est le temps de réponse DNS de 10:00 à 11:00 pour la date souhaitée.



Remarque : Les journaux d'état des pistes sont collectés toutes les 5 minutes.

Capture de paquets

Vous pouvez capturer des paquets pour afficher les requêtes et les réponses DNS, pour filtrer uniquement les DNS que vous pouvez utiliser : port 53.

Pour démarrer la capture de paquets à partir de la GUI :

Étape 1. Choisissez Support and Help en haut à droite

Étape 2 : choisissez Packet Capture

Étape 3. (Facultatif) Choisissez Edit Settings pour ajouter un filtre

Étape 4. (Facultatif) Choisissez vos interfaces et tapez port 53 dans la section Custom Filter

Étape 5. (Facultatif) Cliquez sur Lancer

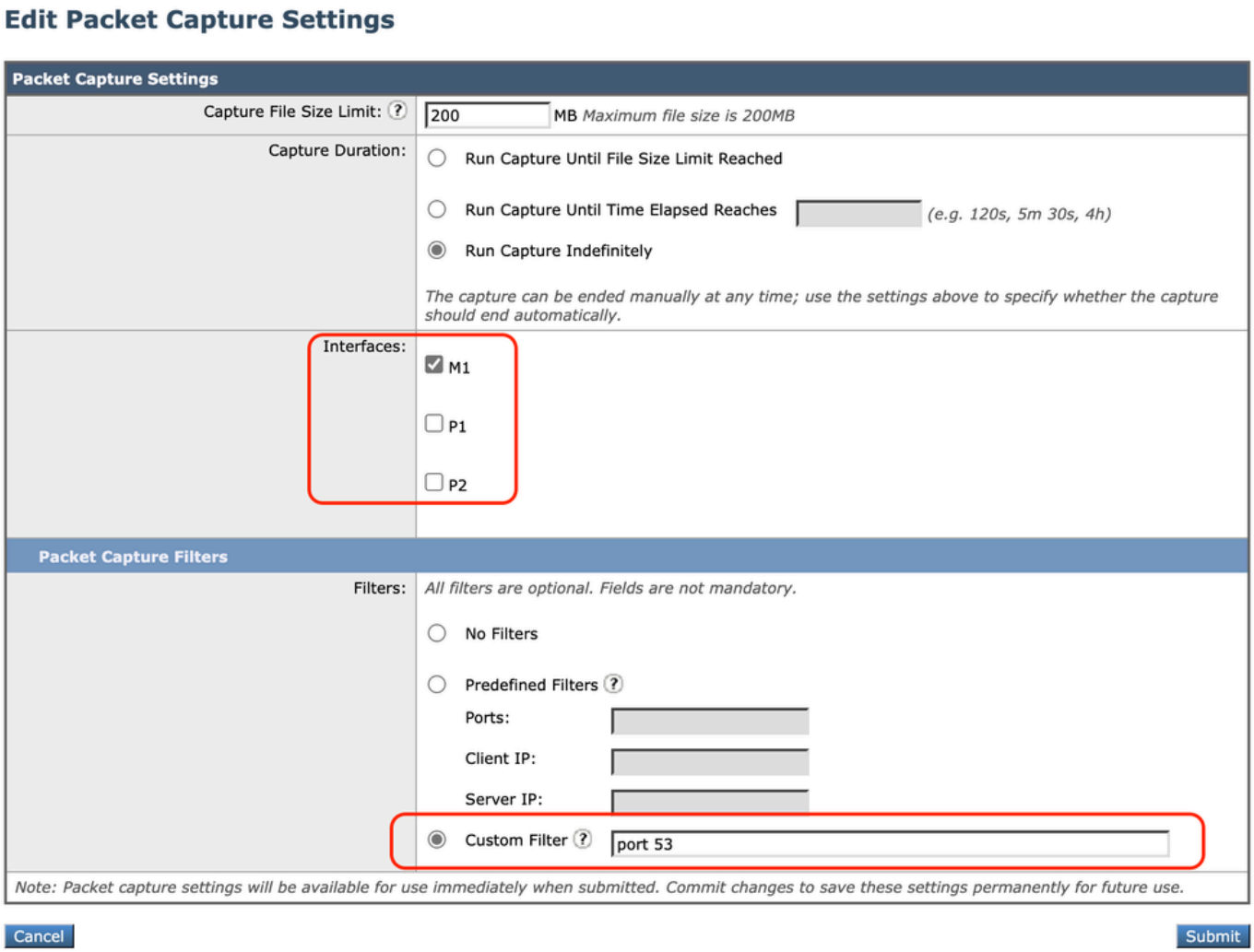


Image - Ajouter un filtre pour capturer les paquets DNS

Conseil : Les paramètres de capture de paquets peuvent être utilisés immédiatement une fois envoyés. Validez les modifications pour enregistrer ces paramètres de façon permanente en vue d'une utilisation ultérieure.

Étape 6. Sélectionnez Start Capture.

Étape 7. (Facultatif) Générez du trafic si vous avez besoin de dépanner un site spécifique ou un accès à une URL.

Étape 8. Arrêter la capture

Étape 9. Attendez que la page soit actualisée, puis choisissez la première capture de paquets dans la liste « Gérer les fichiers de capture de paquets »

Étape 10. Sélectionnez Télécharger le fichier

L4TM

Le Moniteur de trafic de couche 4 écoute le trafic réseau qui arrive sur tous les ports de chaque appareil Web sécurisé et compare les noms de domaine et les adresses IP aux entrées de ses propres tables de base de données pour déterminer s'il faut autoriser le trafic entrant et sortant. Lorsque des clients internes sont infectés par un programme malveillant et tentent d'établir une connexion téléphonique à domicile via des ports et des protocoles non standard, L4 Traffic Monitor empêche l'activité de connexion téléphonique à domicile de quitter le réseau d'entreprise.

Par défaut, le Moniteur du trafic de couche 4 est activé et configuré pour surveiller le trafic sur tous les ports, y compris le DNS et d'autres services.

Pour plus d'informations sur le moniteur de trafic de couche 4, reportez-vous au guide de l'utilisateur.

Erreurs

Page Notification

Par défaut, SWA affiche une page de notification pour informer les utilisateurs qu'ils ont été bloqués et de la raison du blocage

- Nom du fichier et titre de la notification : ERR_DNS_FAIL (Échec DNS)
- Description : page d'erreur affichée lorsque l'URL demandée contient un nom de domaine non valide.
- Texte de notification : la résolution du nom d'hôte (recherche DNS) pour ce nom d'hôte <nom d'hôte > a échoué.
- L'adresse Internet peut être mal orthographiée ou obsolète, l'hôte <hostname > peut être temporairement indisponible ou le serveur DNS peut ne pas répondre.
- Vérifiez l'orthographe de l'adresse Internet saisie. Si elle est correcte, essayez cette requête ultérieurement.



Image - Erreur DNS FAIL

Code de résultat ACCESSLOG AUCUN

Les codes de résultat de transaction du fichier d'accs décrivent la façon dont l'appliance résout les requêtes des clients. Si dans le journal d'accès le code de résultat est NONE cela signifie qu'il y a eu une erreur dans la transaction. Par exemple, une défaillance DNS ou un dépassement du délai de la passerelle.

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

Échec du démarrage du cache DNS

Si une alerte avec le message « Failed to bootstrap the DNS cache » est générée lors du redémarrage d'une appliance, cela signifie que le système n'a pas pu contacter ses serveurs DNS principaux.

Cela peut se produire au démarrage si le sous-système DNS se met en ligne avant que la connectivité réseau ne soit établie. Si ce message apparaît à d'autres moments, il peut indiquer des problèmes réseau ou que la configuration DNS n'est pas définie sur un serveur valide

Nombre maximal d'échecs de requête de serveur DNS atteint

Si un ou plusieurs des serveurs DNS configurés dans SWA ne répondaient pas aux requêtes DNS, SWA les considère comme étant hors ligne et ne leur enverrait pas les requêtes DNS pour une durée prédéfinie. Pour plus d'informations, lisez Configurer DNS à partir de CLI dans cet article.

ÉCHEC_DNS

Lorsque SWA reçoit une requête HTTP et ne parvient pas à résoudre le nom d'hôte, par défaut SWA renvoie une réponse comme :

```
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
```

Cette fonctionnalité est appelée extension de nom de serveur.
SWA effectue cette opération lors des tentatives pour que le nom d'hôte redirigé résolve la page attendue pour le client.

Vous pouvez modifier le format d'URL pour la redirection HTTP 307 en cas d'échec de la recherche DNS. Pour plus d'informations, consultez la section advanceproxyconfig de cet article.

SWA traite la requête DNS qui renvoie ServFail comme une défaillance.

Par exemple, NXDOMAIN retournerait DNS_FAIL au lieu de SERVER_NAME_EXPANSION.

Autres informations utiles

- Guide de l'utilisateur d'AsyncOS 15.0 pour Cisco Secure Web Appliance
- Utilisation des meilleures pratiques d'appliance Web sécurisé - Cisco

- Cisco Content Hub - Introduction au système de noms de domaine

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.