

Configurer le délai de connexion pour un trafic spécifique sur ASA avec ASDM

Table des matières

[Introduction](#)

- [Exigences](#)
- [Composants utilisés](#)
- [Valeurs par défaut](#)

[Configurer le délai de connexion](#)

- [ASDM](#)
- [CLI ASA](#)

[Vérifier](#)

[Références](#)

Introduction

Ce document décrit la configuration du délai de connexion sur ASA et ASDM pour un protocole d'application spécifique tel que HTTP, HTTPS, FTP, ou tout autre protocole. Le délai d'inactivité de la connexion est la période d'inactivité après laquelle un pare-feu ou un périphérique réseau met fin à une connexion inactive pour libérer des ressources et améliorer la sécurité. À l'avance, la première question est : Quelle est la condition requise pour cette configuration ? Si les applications disposent des paramètres de test d'activité TCP appropriés, la configuration du délai de connexion sur un pare-feu est souvent inutile. Cependant, si les applications ne disposent pas de paramètres de test d'activité ou de configuration de délai d'attente appropriés, la configuration du délai d'attente de connexion sur un pare-feu est alors essentielle pour gérer les ressources, améliorer la sécurité, améliorer les performances réseau, assurer la conformité et optimiser l'expérience utilisateur.

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Liste de contrôle d'accès (ACL)

- Politique de service
- Délai de connexion

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ASA 9.17(1)
- ASDM 7.17(1)

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.

Valeurs par défaut



Remarque : délai d'attente par défaut

Le délai embryonnaire par défaut est de 30 secondes.

Le délai d'inactivité demi-fermé par défaut est de 10 minutes.

La valeur `dcd max_retries` par défaut est 5.

La valeur par défaut `dcd retry_interval` est 15 secondes.

Le délai d'inactivité `tcp` par défaut est de 1 heure.

Le délai d'inactivité `udp` par défaut est de 2 minutes.

Le délai d'inactivité `icmp` par défaut est de 2 secondes.

Le délai d'inactivité `sip` par défaut est de 30 minutes.

Le délai d'inactivité `sip_media` par défaut est de 2 minutes.

Le délai d'attente par défaut `esp` et `ha idle` est de 30 secondes.

Pour tous les autres protocoles, le délai d'inactivité par défaut est de 2 minutes.

Pour ne jamais expirer, saisissez `0:0:0`.

Configurer le délai de connexion

ASDM

Si un trafic particulier a une table de connexion, il a un délai d'inactivité spécifique ; par exemple, dans cet article, nous modifions le délai de connexion pour le trafic DNS.

Voici de nombreuses options pour configurer le délai d'attente de connexion pour un trafic spécifique, en tenant compte du schéma de réseau de ce trafic :

Client ----- [Interface : MNG] Pare-feu [Interface : OUT] ----- Serveur

Il est possible d'attribuer une liste de contrôle d'accès à l'interface.

Étape 1 : créez une liste de contrôle d'accès

Nous pouvons attribuer une source, une destination ou un service

ASDM > Configuration > Firewall > Advanced > ACL Manager

The screenshot shows the 'Edit ACE' dialog box. The 'Action' is set to 'Permit'. Under 'Source Criteria', 'Source' is 'any', 'User' is empty, and 'Security Group' is empty. Under 'Destination Criteria', 'Destination' is 'any', 'Security Group' is empty, and 'Service' is 'udp/domain'. The 'Description' field is empty. 'Enable Logging' is checked, and 'Logging Level' is set to 'Default'. At the bottom, there are 'Help', 'Cancel', and 'OK' buttons.

Étape 2 : Créer une règle de stratégie de service

Vous pouvez ignorer la dernière étape si vous disposez déjà de votre liste de contrôle d'accès ou vous pouvez attribuer l'un de ces paramètres (source, destination ou service) à la stratégie de

service de l'interface.

ASDM > Configuration > Firewall > Règles de stratégie de service

Add Service Policy Rule Wizard - Service Policy

Adding a new service policy rule requires three steps:

- Step 1: Configure a service policy.
- Step 2: Configure the traffic classification criteria for the service policy rule.
- Step 3: Configure actions on the traffic classified by the service policy rule.

Create a Service Policy and Apply To:

Only one service policy can be configured per interface or at global level. If a service policy already exists, then you can add a new rule into the existing service policy. Otherwise, you can create a new service policy.

Interface:

Policy Name:

Description:

Drop and log unsupported IPv6 to IPv6 traffic

Global - applies to all interfaces

Policy Name:

Description:

Drop and log unsupported IPv6 to IPv6 traffic

< Back Next > Cancel Help

Étape 3 : créez une classe de trafic

Il est possible de choisir l'adresse IP source et de destination (utilise la liste de contrôle d'accès)

Add Service Policy Rule Wizard - Traffic Classification Criteria

Create a new traffic class:

Description (optional):

Traffic Match Criteria

- Default Inspection Traffic
- Source and Destination IP Address (uses ACL)
- Tunnel Group
- TCP or UDP or SCTP Destination Port
- RTP Range
- IP DiffServ CodePoints (DSCP)
- IP Precedence
- Any traffic

Use an existing traffic class:

Use class-default as the traffic class.

If traffic does not match a existing traffic class, then it will match the class-default traffic class. Class-default can be used in catch all situation.


< Back Next > Cancel Help

Étape 4 : attribution de la liste de contrôle


Dans cette étape, vous pouvez attribuer la liste de contrôle d'accès existante ou sélectionner des conditions de correspondance (source, destination ou service)


Add Service Policy Rule Wizard - Traffic Match - Source and Destination Address


Action: Match Do not match

Existing ACL: ExistingACL 


Source Criteria


Source: 


User: 

Security Group: 

Destination Criteria

Destination: 

Security Group: 

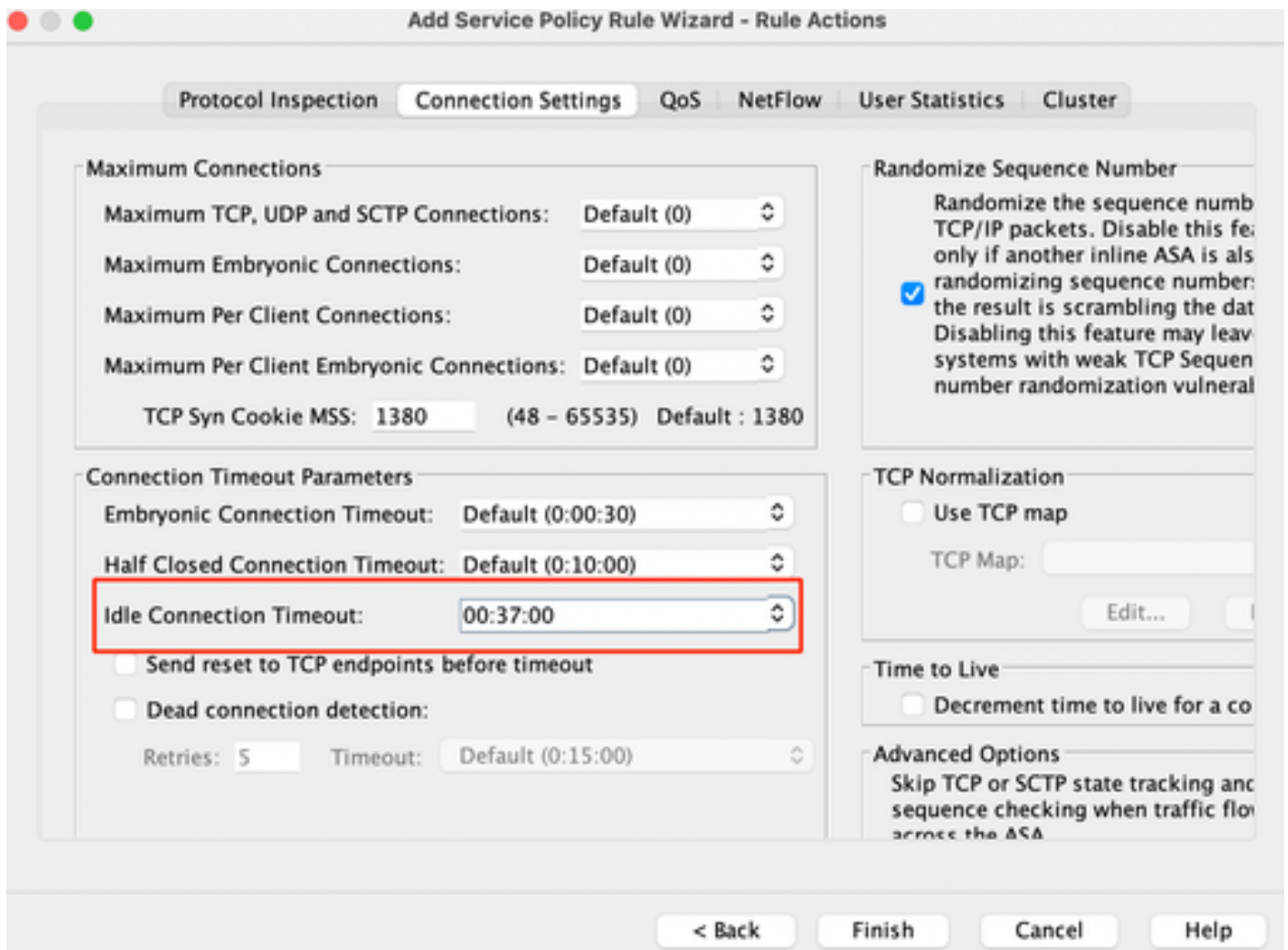
Service: 

Description:

More Options

Étape 5 : configurez le paramètre Idle Timeout

Sur la base du format HH:MM:SS valide, configurez le délai d'inactivité.



Effacer les connexions pour ce trafic particulier :

```
#clear conn addressEntrez une adresse IP ou une plage d'adresses IP
#clear conn protocolEntrez ce mot clé pour effacer uniquement les connexions SCP/TCP/UDP
```

CLI ASA

Vous pouvez configurer tous ces paramètres via l'interface de ligne de commande :

```
ACL :
access-list DNS_TIMEOUT extended permit udp any any eq domain

Carte-classe :
class-map
match access-list DNS_TIMEOUT


Correspondance de politique:
```

```
policy-map MNG-policy
class MNG-class
set connection timeout idle 0:37:00
```

Appliquez la carte de stratégie sur l'interface :

```
service-policy MNG-policy interface MNG
```

Vérifier

 Conseil : si nous exécutons cette commande, nous pouvons confirmer le délai d'expiration de la connexion du trafic DNS :

CLI ASA > mode enable > show conn long

Exemple : show conn long address 192.168.1.1

```
UDP MNG : 192.168.1.1/53 (192.168.1.1/53) OUT : 10.10.10.30/63327 (10.10.10.30/63327),
indicateurs - , inactifs 17, temps de disponibilité 17, délai d'expiration 2m0s, octets 36
```

```
UDP MNG : 192.168.1.1/53 (192.168.1.1/53) OUT : 10.10.10.30/62558 (10.10.10.30/62558),
indicateurs - , 40 inactifs, 40 temps de disponibilité, délai d'expiration 2m0s, octets 36
```

Ensuite, après la configuration, nous pouvons confirmer la configuration du délai d'inactivité :

Exemple : show conn long address 192.168.1.1

```
UDP MNG : 192.168.1.1/53 (192.168.1.1/53) OUT : 10.10.10.30/63044 (10.10.10.30/63044),
indicateurs - , 8 inactifs, 8 temps de disponibilité, délai d'expiration 37 m0, octets 37
```

```
UDP MNG : 192.168.1.1/53 (192.168.1.1/53) OUT : 10.10.10.30/63589 (10.10.10.30/63589),
drapeaux - , inactif 5s, uptime 5s, timeout 37m0s, octets 41
```

Références

[Quels sont les paramètres de connexion ?](#)

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.