

Configurer la détection des menaces pour les services VPN d'accès à distance sur Cisco Firepower Device Manager

Table des matières

Introduction

Ce document décrit le processus de configuration de la détection des menaces pour les services VPN d'accès à distance sur Cisco Firepower Device Manager (FDM).

Conditions préalables

Cisco vous recommande d'avoir des connaissances sur les sujets suivants :

- Cisco Secure Firewall Threat Defense (FTD).
- Cisco Firepower Device Manager (FDM).
- VPN d'accès à distance (RAVPN) sur FTD.

Exigences

Ces fonctions de détection des menaces sont prises en charge dans les versions de Cisco Secure Firewall Threat Defense suivantes :

- 7.0 version train-> prise en charge à partir de 7.0.6.3 et des versions plus récentes dans cette catégorie spécifique.
- 7.2 version train-> prise en charge à partir de 7.2.9 et des versions plus récentes dans cette version spécifique.
- 7.4 version train-> prise en charge à partir de 7.4.2.1 et des versions plus récentes dans cette catégorie spécifique.
- 7.6 version train-> prise en charge à partir de 7.6.0 et des versions ultérieures.



Remarque : ces fonctionnalités ne sont actuellement pas prises en charge dans les versions 7.1 ou 7.3.

Composants utilisés

Les informations décrites dans ce document sont basées sur les versions matérielles et logicielles suivantes :

- Cisco Secure Firewall Threat Defense Virtual version 7.4.2.1

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.

Informations générales

Les fonctionnalités de détection des menaces pour les services VPN d'accès à distance permettent d'empêcher les attaques par déni de service (DoS) à partir d'adresses IPv4 en bloquant automatiquement l'hôte (adresse IP) qui dépasse les seuils configurés pour empêcher toute nouvelle tentative jusqu'à ce que vous supprimiez manuellement la désactivation de l'adresse IP. Des services distincts sont disponibles pour les types d'attaques suivants :

- Tentatives d'authentification répétées et infructueuses : tentatives d'authentification répétées pour les services VPN d'accès à distance (attaques par analyse en force des noms d'utilisateur/mots de passe).
- Attaques d'initiation du client : lorsque l'attaquant démarre mais ne termine pas la connexion, tente plusieurs fois de se connecter à une tête de réseau VPN d'accès à distance à partir d'un hôte unique.
- Connection attempts to invalid remote access VPN services : Lorsque des pirates tentent de se connecter à des groupes de tunnels intégrés spécifiques destinés uniquement au fonctionnement interne du périphérique. Les terminaux légitimes n'essaient pas de se connecter à ces groupes de tunnels.

Ces attaques, même si elles échouent dans leur tentative d'accès, peuvent consommer des ressources de calcul et empêcher les utilisateurs valides de se connecter aux services VPN d'accès à distance. Lorsque vous activez ces services, le pare-feu ferme automatiquement l'hôte (adresse IP) qui dépasse les seuils configurés. Cela empêche de nouvelles tentatives jusqu'à ce que vous supprimiez manuellement le shun de l'adresse IP.



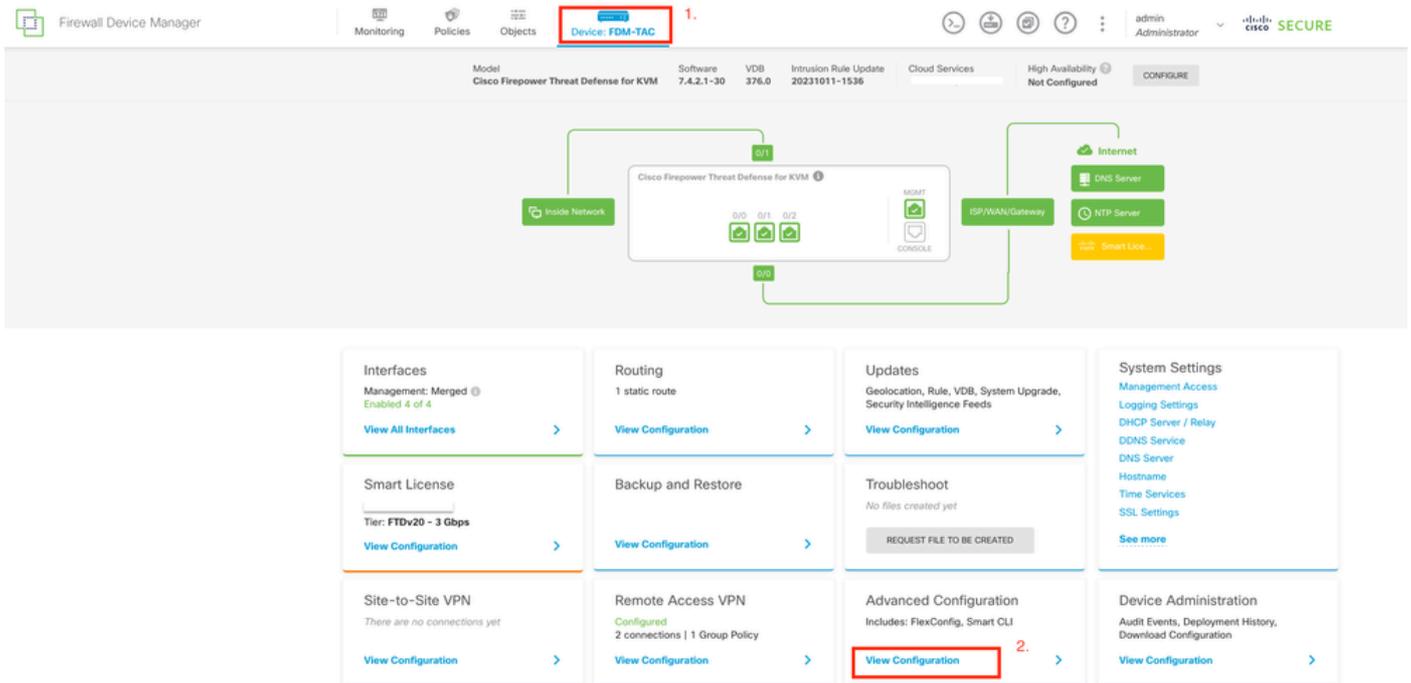
Remarque : par défaut, tous les services de détection des menaces pour les VPN d'accès à distance sont désactivés.

Configurer

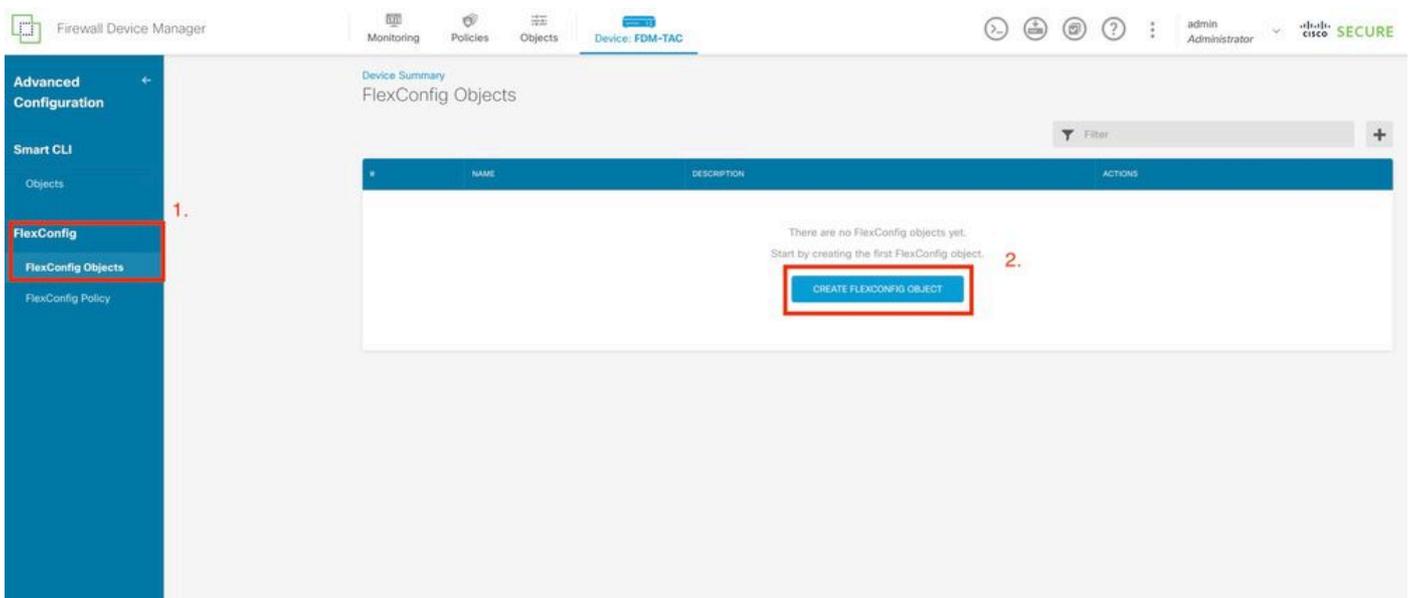


Remarque : la configuration de ces fonctions sur Secure Firewall Threat Defense est actuellement prise en charge uniquement via FlexConfig.

-
1. Connectez-vous au Gestionnaire de périphériques Firepower.
 2. Afin de configurer l'objet FlexConfig, accédez à Device > Advanced Configuration > FlexConfig > FlexConfig Objects, puis cliquez sur Create FlexConfig object.



Modifiez la configuration avancée à partir de la page d'accueil de FDM.



Créez un objet FlexConfig.

3. Une fois la fenêtre d'objet FlexConfig ouverte, ajoutez la configuration requise pour activer les fonctionnalités de détection des menaces pour le VPN d'accès à distance :

Fonctionnalité 1 : Détection des menaces pour les tentatives de connexion à des services VPN internes uniquement (non valides)

Afin d'activer ce service, ajoutez la commande threat-detection service invalid-vpn-access dans la zone de texte de l'objet FlexConfig.

Fonctionnalité 2 : Détection des menaces pour les attaques d'initiation du client VPN d'accès à distance

Afin d'activer ce service, ajoutez la commande `threat-detection service remote-access-client-initiations hold-down <minutes> threshold <count>` dans la zone de texte de l'objet FlexConfig, où :

- `hold-down <minutes>` définit la période après la dernière tentative de démarrage pendant laquelle les tentatives de connexion consécutives sont comptées. Si le nombre de tentatives de connexion consécutives atteint le seuil configuré au cours de cette période, l'adresse IPv4 du pirate est ignorée. Vous pouvez définir cette période entre 1 et 1 440 minutes.
- `threshold <count>` est le nombre de tentatives de connexion nécessaires au cours de la période de retenue pour déclencher un shun. Vous pouvez définir le seuil entre 5 et 100.

Par exemple, si la période de retenue est de 10 minutes et que le seuil est de 20, l'adresse IPv4 est automatiquement désactivée en cas de 20 tentatives de connexion consécutives dans un délai de 10 minutes.



Remarque : lorsque vous définissez les valeurs de retenue et de seuil, tenez compte de l'utilisation de la NAT. Si vous utilisez la fonction PAT, qui autorise de nombreuses requêtes à partir de la même adresse IP, envisagez des valeurs plus élevées. Cela garantit que les utilisateurs valides disposent de suffisamment de temps pour se connecter. Par exemple, dans un hôtel, de nombreux utilisateurs peuvent tenter de se connecter en peu de temps.

Fonctionnalité 3 : Détection des menaces pour les échecs d'authentification VPN d'accès à distance

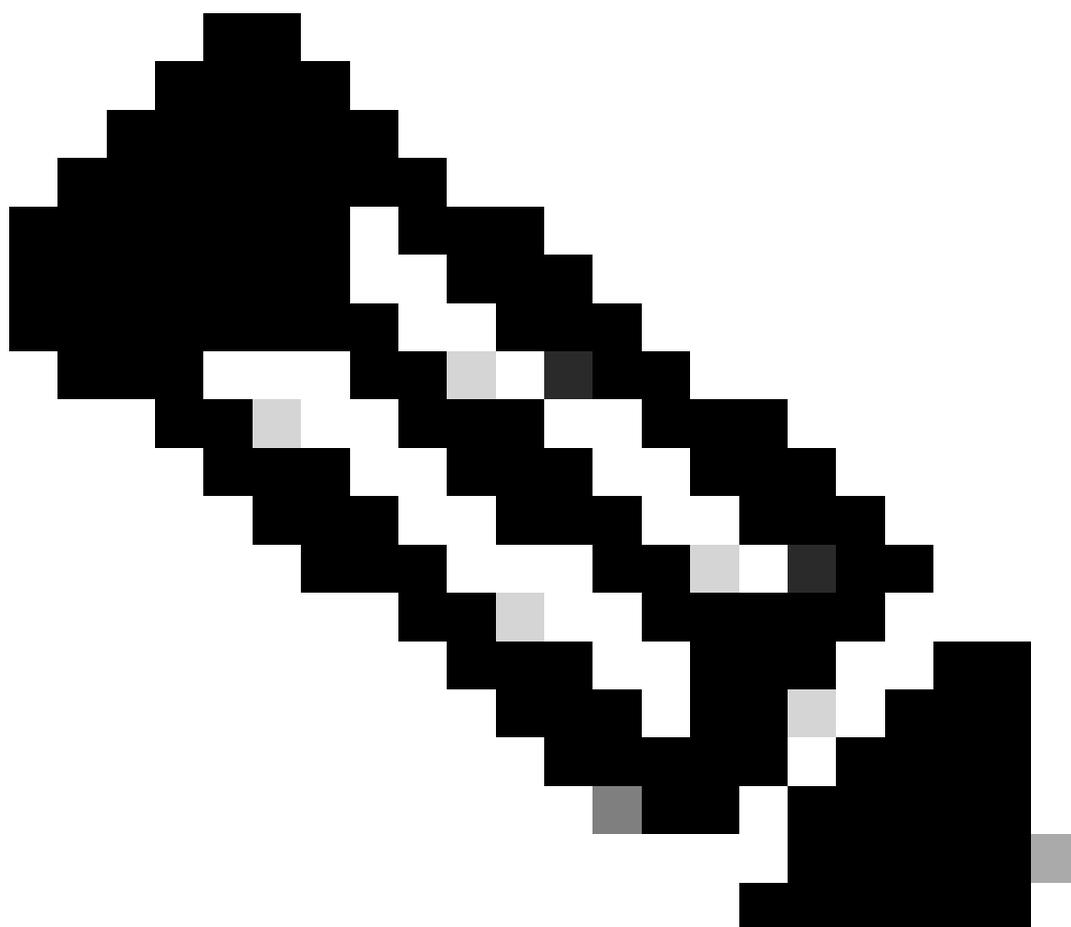
Afin d'activer ce service, ajoutez la commande `threat-detection service remote-access-authentication hold-down<minutes> threshold <count>` dans la zone de texte de l'objet FlexConfig, où :

- `hold-down <minutes>` définit la période après la dernière tentative infructueuse pendant laquelle les échecs consécutifs sont comptés. Si le nombre d'échecs d'authentification consécutifs atteint le seuil configuré au cours de cette période, l'adresse IPv4 du pirate est

ignorée. Vous pouvez définir cette période entre 1 et 1 440 minutes.

- `threshold <count>` est le nombre de tentatives d'authentification ayant échoué, nécessaires au cours de la période de retenue pour déclencher un shun. Vous pouvez définir le seuil entre 1 et 100.

Par exemple, si la période de retenue est de 10 minutes et que le seuil est de 20, l'adresse IPv4 est automatiquement désactivée en cas de 20 échecs d'authentification consécutifs au cours d'une période de 10 minutes



Remarque : lorsque vous définissez les valeurs de retenue et de seuil, tenez compte de l'utilisation de la NAT. Si vous utilisez la fonction PAT, qui autorise de nombreuses requêtes à partir de la même adresse IP, envisagez des valeurs plus élevées. Cela garantit que les utilisateurs valides disposent de suffisamment de temps pour se connecter. Par exemple, dans un hôtel, de nombreux utilisateurs peuvent tenter de se connecter en peu de temps.

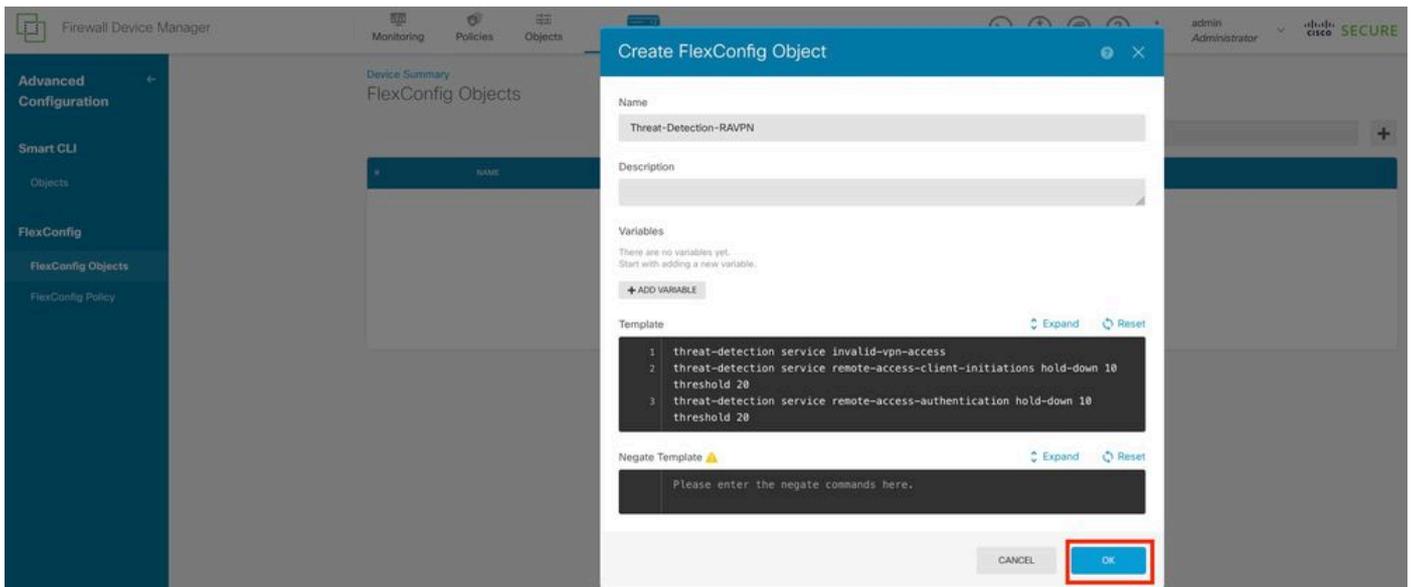


Remarque : les échecs d'authentification via SAML ne sont pas encore pris en charge.

Cet exemple de configuration active les trois services de détection des menaces disponibles pour le VPN d'accès à distance avec une période de retenue de 10 minutes et un seuil de 20 pour l'initiation du client et les tentatives d'authentification ayant échoué. Configurez les valeurs de retenue et de seuil en fonction des exigences de votre environnement.

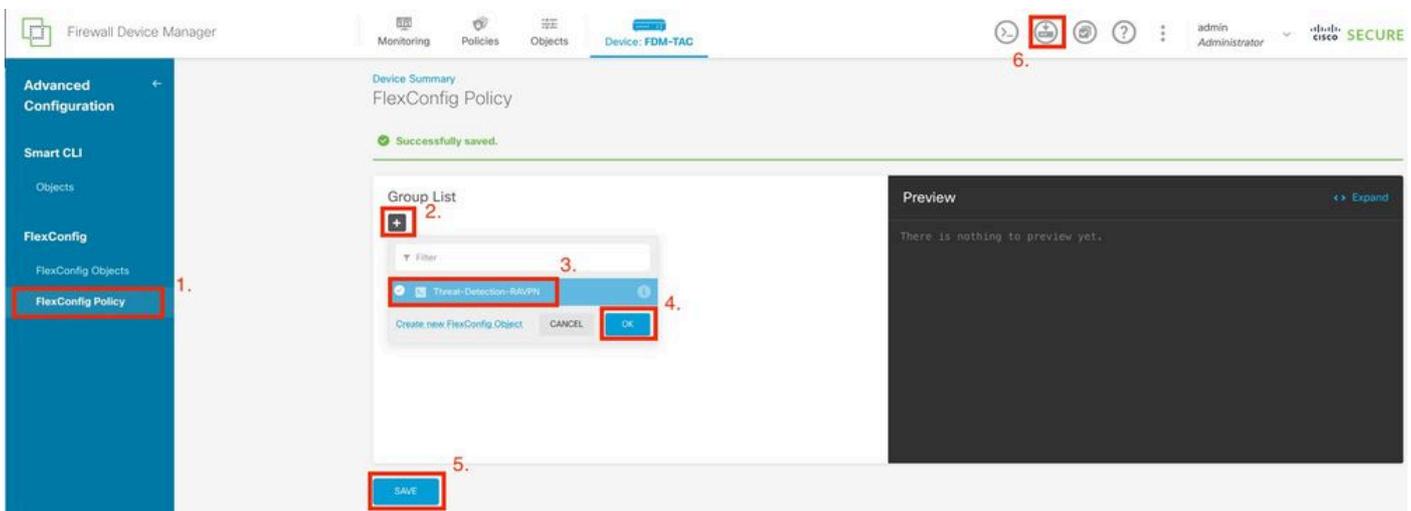
Cet exemple utilise un seul objet FlexConfig pour activer les 3 fonctionnalités disponibles.

```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```



Définissez les critères de l'objet FlexConfig.

4. Une fois l'objet FlexConfig créé, accédez à FlexConfig > FlexConfig Policy et localisez le signe plus sous Group List. Sélectionnez l'objet FlexConfig créé pour la détection des menaces RAVPN, puis cliquez sur OK pour ajouter l'objet à la liste des groupes. Cela permet de renseigner un aperçu CLI des commandes. Vérifiez cet aperçu pour vous assurer de leur exactitude. Sélectionnez ENREGISTRER et déployez les modifications dans Firepower Threat Defense (FTD).



Modifiez la stratégie FlexConfig et affectez l'objet FlexConfig.

Vérifier

Afin d'afficher des statistiques pour les services RAVPN de détection des menaces, connectez-vous à l'interface de ligne de commande du FTD et exécutez la commande `show threat-detection service [service] [entries|details]`. Où le service peut être : `remote-access-authentication`, `remote-access-client-initiations` ou `invalid-vpn-access`.

Vous pouvez limiter davantage la vue en ajoutant les paramètres suivants :

- **entries** : affiche uniquement les entrées suivies par le service de détection des menaces. Par exemple, les adresses IP dont les tentatives d'authentification ont échoué.
- **details** — Affiche les détails et les entrées du service.

Exécutez la commande `show threat-detection service` pour afficher les statistiques de tous les services de détection de menaces qui sont activés.

```
<#root>
```

```
FDM-TAC#
```

```
show threat-detection service
```

```
Service: invalid-vpn-access State : Enabled
```

```
Hold-down : 1 minutes
```

```
Threshold : 1
```

```
Stats:
```

```
failed      :          0
```

```
blocking    :          0
```

```
recording   :          0
```

```
unsupported  :          0
```

```
disabled    :          0
```

```
Total entries: 0
```

```
Service: remote-access-authentication State : Enabled
```

```
Hold-down : 10 minutes
```

```
Threshold : 20
```

```
Stats:
```

```
failed      :          0
```

```
blocking    :          1
```

```
recording   :          4
```

```
unsupported  :          0
```

```
disabled    :          0
```

```
Total entries: 2
```

```
Name: remote-access-client-initiations State : Enabled
```

```
Hold-down : 10 minutes
```

```
Threshold : 20
```

```
Stats:
```

```
failed      :          0
```

```
blocking    :          0
```

```
recording   :          0
```

```
unsupported  :          0
```

```
disabled    :          0
```

```
Total entries: 0
```

Afin d'afficher plus de détails sur les attaquants potentiels qui sont suivis pour le service d'authentification d'accès à distance, exécutez la commande `show threat-detection service <service>entries`.

<#root>

FDM-TAC#

show threat-detection service remote-access-authentication entries

Service:

remote-access-authentication

Total entries: 2

Idx	Source	Interface	Count	Age	Hold-down
1	192.168.100.101/ 32	outside		1	721
2	192.168.100.102/ 32	outside		2	486

Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.

Afin d'afficher les statistiques générales et les détails d'un service VPN d'accès à distance de détection des menaces spécifique, exécutez la commande show threat-détection service <service>details.

<#root>

FDM-TAC#

show threat-detection service remote-access-authentication details

Service:

remote-access-authentication

State :

Enabled

Hold-down : 10 minutes

Threshold : 20

Stats:

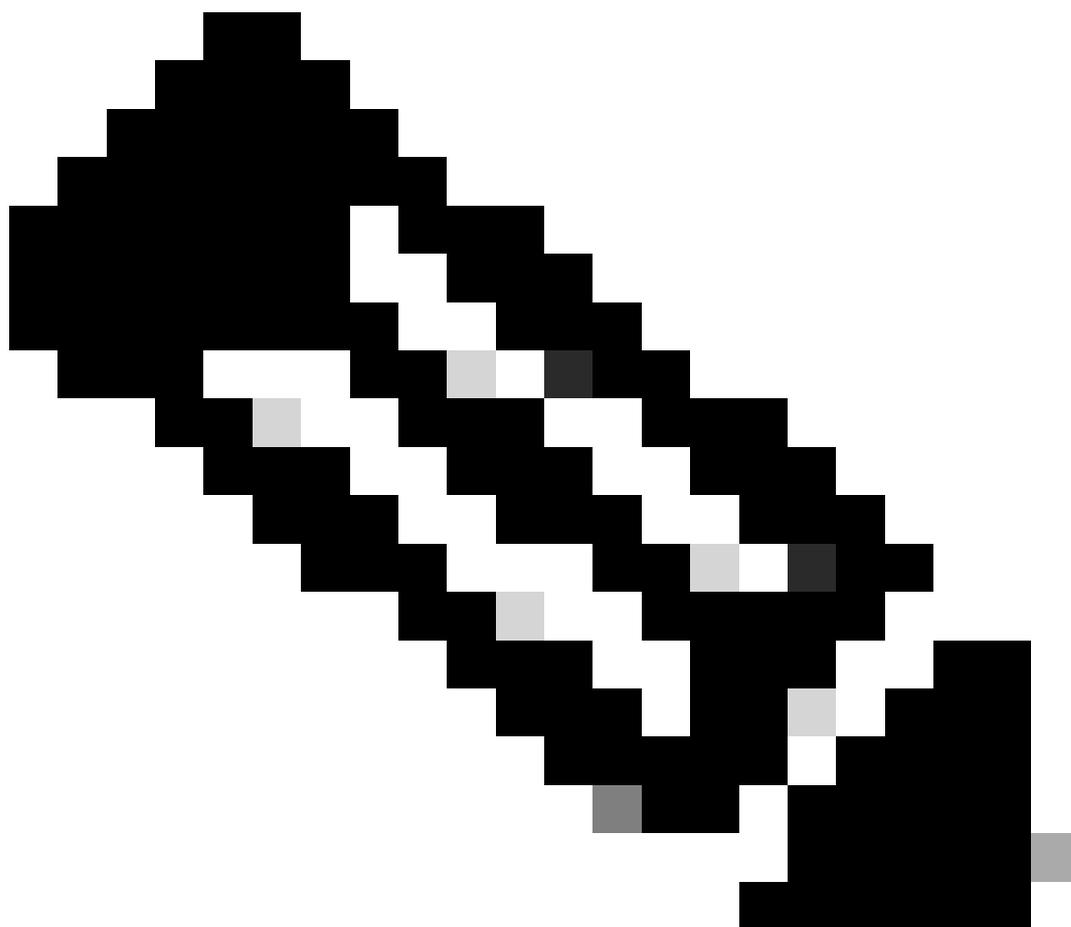
failed : 0
blocking : 1
recording : 4
unsupported : 0
disabled : 0

Total entries: 2

Idx	Source	Interface	Count	Age	Hold-down
1	192.168.100.101/ 32	outside		1	721
2	192.168.100.102/ 32	outside		2	486

Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.



Remarque : les entrées affichent uniquement les adresses IP suivies par le service de détection des menaces. Si une adresse IP remplit les conditions pour être désactivée, le nombre de blocages augmente et l'adresse IP n'est plus affichée comme entrée.

En outre, vous pouvez surveiller les shuns appliqués par les services VPN, et supprimer les shuns pour une adresse IP unique ou toutes les adresses IP avec les commandes suivantes :

- `show shun [adresse_ip]`

Affiche les hôtes désactivés, y compris ceux qui sont automatiquement désactivés par la détection des menaces pour les services VPN, ou manuellement à l'aide de la commande `shun`. Vous pouvez éventuellement limiter l'affichage à une adresse IP spécifiée.

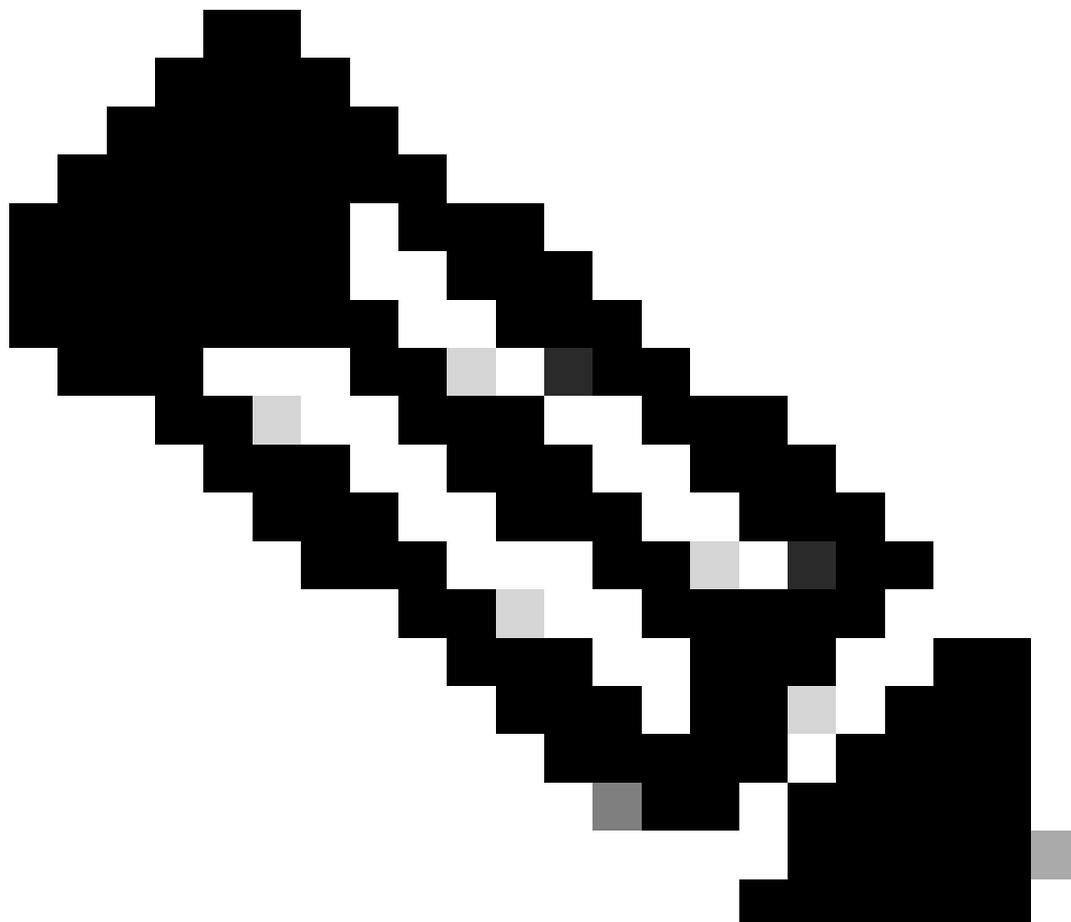
- `no shun ip_address [interface if_name]`

Supprime le shun de l'adresse IP spécifiée uniquement. Vous pouvez éventuellement spécifier le nom d'interface pour le shun, si l'adresse est shuntée sur plusieurs interfaces et que vous voulez

laisser le shun en place sur certaines interfaces.

- clear shun

Supprime le shun de toutes les adresses IP et de toutes les interfaces.



Remarque : les adresses IP rejetées par la détection des menaces pour les services VPN n'apparaissent pas dans la commande show threat-détection shun, qui s'applique uniquement à la détection des menaces d'analyse.

Afin de lire tous les détails pour chaque sortie de commande et les messages syslog disponibles liés aux services de détection des menaces pour VPN d'accès à distance, veuillez vous référer au document [Référence des commandes](#).

Informations connexes

- Pour obtenir de l'aide supplémentaire, contactez le centre d'assistance technique (TAC). Un

contrat d'assistance valide est requis : [Contacts d'assistance internationale Cisco](#).

- Vous pouvez également visiter la communauté VPN Cisco [ici](#).
- [Assistance technique de Cisco et téléchargements](#)

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.