Surveillance et résolution des problèmes de VPN dans CDO

Surveiller les sessions VPN d’accès à distance

Le tableau de bord CDO de surveillance de l’accès à distance peut être utilisé pour afficher des informations consolidées sur les utilisateurs du VPN d'accès à distance, y compris l’état actuel des utilisateurs, les types de périphériques, les applications client, les informations de géolocalisation des utilisateurs et la durée des connexions. Vous pouvez également déconnecter les sessions de VPN d'accès à distance au besoin.

Effectuez les opérations suivantes pour voir les sessions VPN :

1. Dans la page Cloud-Delivered Firewall Management Center (centre de gestion de pare-feu en nuage), cliquez sur **Retour à l’accueil**.
2. Dans le volet de navigation CDO, cliquez sur **VPN** > **Remote Access VPN Monitoring** (Surveillance du VPN d'accès à distance).

Consultez la section Surveiller les sessions de réseau privé virtuel d’accès distant pour de plus amples renseignements.

Messages système

Le centre de messages est l’endroit où commencer votre dépannage. Cette fonctionnalité vous permet d’afficher les messages qui sont générés en permanence à propos des activités et de l’état du système. Pour ouvrir le centre de messages, cliquez sur **System Status**(état du système), situé immédiatement à droite du bouton **Deploy** (déployer) dans le menu principal.

Journaux système VPN

Vous pouvez activer la journalisation du système (syslog) pour les périphériques défense contre les menaces . Les informations de journalisation peuvent vous aider à cerner et isoler les problèmes de configuration du réseau ou des périphériques. Lorsque vous activez la journalisation VPN, les périphériques défense contre les menaces envoient des journaux système VPN aux centre de gestion pour analyse et archivage.

Tous les journaux système VPN s'affichent avec le niveau de gravité par défaut « ERROR » ou plus (sauf s'il a été modifié). Vous pouvez gérer la journalisation VPN via les paramètres de la plateforme défense contre les menaces . Vous pouvez ajuster le niveau de gravité du message en modifiant les paramètres de **journalisation VPN** dans la politique des paramètres de plateforme pour les périphériques ciblés défense contre les menaces (**Platform Settings** > **Syslog** > **Logging Setup**) Paramètres de la plateforme > Syslog > Configuration de la journalisation). Consultez Syslog pour en savoir plus sur l'activation de la journalisation VPN, la configuration des serveurs Syslog et l'affichage des journaux du système.

Nous vous recommandons de définir le niveau de journalisation des journaux VPN au niveau 3 (Erreurs). La définition du niveau de journalisation VPN au niveau 4 et plus (Avertissements, Notifications, Information ou Débogage) pourrait surcharger le centre de gestion.

Remarque Lorsque vous configurez un périphérique avec un VPN de site à site ou d'accès à distance, il active automatiquement l'envoi des journaux système VPN à centre de gestion.

Affichage des journaux système VPN

Le système enregistre des informations d'événement pour vous aider à recueillir des informations supplémentaires sur la source de vos problèmes VPN. Tous les journaux système VPN affichés ont un niveau de gravité par défaut « ERROR » ou un niveau supérieur (à moins qu'il ne soit modifié). Par défaut, les lignes sont triées en fonction de la colonne **Heure**.

Vous devez être un utilisateur administrateur dans un domaine descendant pour effectuer cette tâche.

Avant de commencer

Activez la journalisation VPN en cochant la case **Enable Logging to FMC** dans les paramètres de la plateforme défense contre les menaces (**Devices** > **Platform Settings** > **Syslog** > **Logging Setup**) (Périphériques > Paramètres de la plateforme > Syslog > Configuration de la journalisation). Consultez Syslog pour en savoir plus sur l'activation de la journalisation VPN, la configuration des serveurs Syslog et l'affichage des journaux du système.

Procédure

Étape 1 Choisissez **Devices** > **VPN** > **Troubleshooting** (Périphériques > VPN > Dépannage).

Étape 2 Vous avez les options suivantes :

- Search (rechercher) : pour filtrer les informations du message actuel, cliquez sur **Edit Search**(modifier la recherche).

- View (afficher) : pour afficher les détails du VPN associés au message sélectionné dans la vue, cliquez sur **View** (Afficher).
- View All (afficher tout) : pour afficher les détails du VPN pour tous les messages dans la vue, cliquez sur **View All** 5afficher tout).
- Delete (supprimer) : pour supprimer les messages sélectionnés de la base de données, cliquez sur **Delete** (supprimer) ou sur **Delete All** (supprimer tout) pour supprimer tous les messages.

Commandes de débogage

Cette section explique comment utiliser les commandes de débogage pour vous aider à diagnostiquer et à résoudre les problèmes liés au VPN. Les commandes décrites ici ne sont pas exhaustives, cette section comprend les commandes en fonction de leur utilité pour vous aider à diagnostiquer les problèmes liés au VPN.

Instructions d'utilisation

Comme les résultats du débogage obéissent à un niveau de priorité élevé dans le processus du CPU, ils sont susceptibles de rendre le système inutilisable. Par conséquent, les commandes **debug** doivent uniquement être utilisées pour résoudre des problèmes spécifiques ou au cours de séances de dépannage effectuées avec le TAC (ou centre d'assistance technique Cisco). De plus, il est préférable d'utiliser les commandes **debug** en dehors des périodes d'affluence de trafic et lorsque peu d'utilisateurs sont connectés au réseau. En effectuant le débogage pendant ces périodes, il y moins de chance que des frais généraux d'administration accrus associés à l'exécution de la commande **debug** aient des répercussions sur l'utilisation du système.

Vous pouvez afficher la sortie de débogage uniquement dans une session de l'interface de ligne de commande. La sortie est accessible directement lorsqu'elle est connectée au port de console ou dans l'interface de ligne de commande de diagnostic (entrez **system support diagnostic-cli**). Vous pouvez également afficher la sortie à partir de l'interface de ligne de commande de Firepower Threat Defense régulière à l'aide de la commande **show console-output**.

Pour afficher les messages de débogage pour une fonctionnalité donnée, utilisez la commande **debug**. Pour désactiver l'affichage des messages de débogage, utilisez la forme **no** de cette commande. Utilisez **no debug all** pour désactiver toutes les commandes de débogage.

debug *feature* [*subfeature*] [*level*]
no debug *feature* [*subfeature*]

Description de la syntaxe

feature	Spécifie la fonctionnalité pour laquelle vous souhaitez activer le débogage. Pour voir les fonctionnalités disponibles, utilisez la commande **debug ?** pour obtenir de l'aide sur l'interface de ligne de commande.
subfeature	(Facultatif) Selon la fonctionnalité, vous pouvez activer les messages de débogage pour une ou plusieurs sous-fonctionnalités. Utilisez ? pour voir les sous-fonctions offertes.
level	(Facultatif) Spécifie le niveau de débogage. Utilisez ? pour voir les niveaux disponibles.

Commande par défaut

Le niveau de débogage par défaut est 1.

Exemple

Comme plusieurs sessions s'exécutent sur le VPN d'accès à distance, le dépannage peut être difficile, compte tenu de la taille des journaux. Vous pouvez utiliser la commande **debug webvpn condition** pour configurer des filtres afin de cibler votre processus de débogage plus précisément.

debug webvpn condition {**group** *name* | **p-ipaddress** *ip_address* [{**subnet** *subnet_mask* | **prefix** *length*}] | **reset** | **user** *name*}

Lieu :

- les filtres **group** *name* sur une politique de groupe (pas un groupe de tunnels ou un profil de connexion).
- **p-ipaddress** *ip_address* [{ **subnet** *subnet_mask* | **prefix** *longueur*}] sur l'adresse IP publique du client. Le masque de sous-réseau (pour IPv4) ou le préfixe (pour IPv6) est facultatif.
- **reset** réinitialise tous les filtres. Vous pouvez utiliser la commande **no debug webvpn condition** pour désactiver un filtre en particulier.
- **user** *name* filtre par nom d'utilisateur.

Si vous configurez plus d'une condition, les conditions sont conjointes (ET), de sorte que les débogages n'apparaissent que si toutes les conditions sont respectées.

Après avoir configuré le filtre de condition, utilisez la commande de base **debug webvpn** pour activer le débogage. Définir les conditions à elles seules n'active pas le débogage. Utilisez les commandes **show debug** et **show webvpn debug-condition** pour afficher l'état actuel du débogage.

Ce qui suit montre un exemple d'activation d'un débogage conditionnel sur l'utilisateur jdoe.

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

firepower# debug webvpn
INFO: debug webvpn  enabled at level 1.

firepower# show debug
debug webvpn  enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

Commandes associées

Commande	Description
show debug	Affiche les paramètres de débogage actuellement actifs.
undebug	Désactive le débogage pour une fonctionnalité. Cette commande est un synonyme de **no debug**.

déboguer aaa

Consultez les commandes suivantes pour connaître les configurations de débogage ou les paramètres d'authentification, d'autorisation et de gestion des comptes (AAA).

debug *aaa* [*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*]

Description de la syntaxe

aaa	Active le débogage pour AAA. Utilisez ? pour voir les sous-fonctions offertes.
accounting	(Facultatif) Active le débogage de la comptabilité AAA.
authentication	(Facultatif) Active le débogage de l'authentification AAA.
authorization	(Facultatif) Active le débogage de l'autorisation AAA.
common	(Facultatif) Spécifie le niveau de débogage commun AAA. Utilisez ? pour voir les niveaux disponibles.
internal	(Facultatif) Active le débogage interne AAA.
shim	(Facultatif)) Spécifie le niveau de débogage de AAA shim. Utilisez ? pour voir les niveaux disponibles.
url-redirect	(Facultatif) Active le débogage de redirection d'URL AAA.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug aaa	Affiche les paramètres de débogage actuellement actifs pour AAA.
undebug aaa	Désactive le débogage pour AAA. Cette commande est un synonyme de **no debug aaa**.

déboguer le chiffrement

Consultez les commandes suivantes pour déboguer les configurations ou les paramètres associés à la gestion des chiffrements.

debug *crypto* [*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*]

Description de la syntaxe

crypto	Active le débogage pour le *chiffrement*. Utilisez ? pour voir les sous-fonctions offertes.
ca	(Facultatif) Spécifie les niveaux de débogage de l'infrastructure de clé publique (PKI). Utilisez ? pour voir les sous-fonctions offertes.
condition	(Facultatif) Spécifie les filtres de débogage IPsec/ISAKMP. Utilisez ? pour voir les filtres disponibles.

engine	(Facultatif) Spécifie les niveaux de débogage du moteur de chiffrement. Utilisez ? pour voir les niveaux disponibles.
ike-common	(Facultatif) Spécifie les niveaux courants de débogage IKE. Utilisez ? pour voir les niveaux disponibles.
ikev1	(Facultatif) Spécifie les niveaux de débogage d'IKE version 1. Utilisez ? pour voir les niveaux disponibles.
ikev2	(Facultatif) Spécifie les niveaux de débogage d'IKE version 2. Utilisez ? pour voir les niveaux disponibles.
ipsec	(Facultatif) Spécifie les niveaux de débogage IPsec. Utilisez ? pour voir les niveaux disponibles.
condition	(Facultatif) Spécifie les niveaux de débogage de l'API Crypto Secure Socket. Utilisez ? pour voir les niveaux disponibles.
vpnclient	(Facultatif) Spécifie les niveaux de débogage du client EasyVPN. Utilisez ? pour voir les niveaux disponibles.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug crypto	Affiche les paramètres de débogage actuellement actifs pour les paramètres de chiffrement.
undebug crypto	Désactive le débogage pour le chiffrement. Cette commande est un synonyme de **no debug crypto**.

debug crypto ca

Consultez les commandes suivantes pour savoir comment déboguer les configurations ou les paramètres associés à crypto ca.

debug *crypto ca* [*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*] [*1-255*]

Description de la syntaxe

crypto ca	Active le débogage pour *crypto ca*. Utilisez ? pour voir les sous-fonctions offertes.
cluster	(Facultatif) Spécifie le niveau de débogage de la grappe PKI. Utilisez ? pour voir les niveaux disponibles.
cmp	(Facultatif) Spécifie le niveau de débogage des transactions CMP. Utilisez ? pour voir les niveaux disponibles.
messages	(Facultatif) Spécifie le niveau de débogage du message d'entrée/sortie de l'infrastructure de clé publique (PKI). Utilisez ? pour voir les niveaux disponibles.
periodic-authentication	(Facultatif) Spécifie le niveau de débogage de l'authentification périodique de l'infrastructure PKI. Utilisez ? pour voir les niveaux disponibles.

scep-proxy	(Facultatif) Spécifie le niveau de débogage du proxy SCEP. Utilisez ? pour voir les niveaux disponibles.
server	(Facultatif) Spécifie le niveau de débogage du serveur d'autorité de certification local. Utilisez ? pour voir les niveaux disponibles.
transactions	(Facultatif) Spécifie le niveau de débogage de la transaction PKI. Utilisez ? pour voir les niveaux disponibles.
trustpool	(Facultatif) Spécifie le niveau de débogage du pool de confiance. Utilisez ? pour voir les niveaux disponibles.
1-255	(Facultatif) Spécifie le niveau de débogage.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug crypto ca	Affiche les paramètres de débogage actuellement actifs pour crypto ca.
undebug	Désactive le débogage pour crypto ca. Cette commande est un synonyme de **no debug crypto ca**.

déboguer le chiffrement IKEv1

Consultez les commandes suivantes pour connaître les configurations ou les paramètres associés à Internet Key Exchange version 1 (IKEv1).

Minuteries] [**debug** *de chiffrement IKEv1 1 à* [*255*]

Description de la syntaxe

ikev1	Active le débogage pour *IKEv1*. Utilisez ? pour voir les sous-fonctions offertes.
timers	(Facultatif) Active le débogage pour les minuteries IKEv1.
1-255	(Facultatif) Spécifie le niveau de débogage.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug crypto ikev1	Affiche les paramètres de débogage actuellement actifs pour IKEv1.
undebug crypto ikev1	Désactive le débogage pour IKEv1. Cette commande est un synonyme de **no debug crypto ikev1**.

déboguer le chiffrement IKEv2

Consultez les commandes suivantes pour connaître les configurations ou les paramètres associés à Internet Key Exchange version 2 (IKEv2).

debug *crypto ikev2* [*ha* | *platform* | *protocol* | *timers*]

Description de la syntaxe

ikev2	Active le débogage *ikev2*. Utilisez ? pour voir les sous-fonctions offertes.
ha	(Facultatif) Spécifie le niveau de débogage d'IKEv2 à haute disponibilité. Utilisez ? pour voir les niveaux disponibles.
platform	(Facultatif) Spécifie le niveau de débogage de la plateforme IKEv2. Utilisez ? pour voir les niveaux disponibles.
protocol	(Facultatif) Spécifie le niveau de débogage du protocole IKEv2. Utilisez ? pour voir les niveaux disponibles.
timers	(Facultatif) Active le débogage pour les minuteries IKEv2.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug crypto ikev2	Affiche les paramètres de débogage actuellement actifs pour IKEv2.
undebugcrypto ikev2	Désactive le débogage pour IKEv2. Cette commande est un synonyme de **no debug crypto ikev2**.

debug crypto ipsec

Consultez les commandes suivantes pour le débogage des configurations ou des paramètres associés à IPsec.

debug *crypto ipsec* [*1-255*]

Description de la syntaxe

ipsec	Active le débogage pour *ipsec*. Utilisez ? pour voir les sous-fonctions offertes.
1-255	(Facultatif) Spécifie le niveau de débogage.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug crypto ipsec	Affiche les paramètres de débogage actuellement actifs pour IPsec.
undebugcrypto ipsec	Désactive le débogage pour IPsec. Cette commande est un synonyme de **no debug crypto ipsec**.

debug ldap

Consultez les commandes suivantes pour le débogage des configurations ou des paramètres associés à LDAP (Lightweight Directory Access Protocol).

debug *ldap* [*1-255*]

Description de la syntaxe

ldap	Active le débogage pour LDAP. Utilisez ? pour voir les sous-fonctions offertes.
1-255	(Facultatif) Spécifie le niveau de débogage.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug ldap	Affiche les paramètres de débogage actuellement actifs pour LDAP.
undebugldap	Désactive le débogage pour LDAP. Cette commande est un synonyme de **no debug ldap**.

debug ssl

Consultez les commandes suivantes pour connaître les configurations ou les paramètres associés aux sessions SSL.

debug *ssl* [*cipher* | *device*] [*1-255*]

Description de la syntaxe

ssl	Active le débogage pour SSL. Utilisez ? pour voir les sous-fonctions offertes.
cipher	(Facultatif) Spécifie le niveau de débogage du chiffrement SSL. Utilisez ? pour voir les niveaux disponibles.
device	(Facultatif) Spécifie le niveau de débogage du périphérique SSL. Utilisez ? pour voir les niveaux disponibles.
1-255	(Facultatif) Spécifie le niveau de débogage.

Commande par défaut Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug ssl	Affiche les paramètres de débogage actuellement actifs pour SSL.
undebug ssl	Désactive le débogage pour SSL. Cette commande est un synonyme de **no debug ssl**.

debug webvpn

Consultez les commandes suivantes pour déboguer les configurations ou les paramètres associés à WebVPN.

debug *webvpn* [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

Description de la syntaxe

webvpn	Active le débogage pour WebVPN. Utilisez ? pour voir les sous-fonctions offertes.
anyconnect	(Facultatif) Spécifie le niveau de débogage Secure Client du WebVPN. Utilisez ? pour voir les niveaux disponibles.
chunk	(Facultatif) Spécifie le niveau de débogage du bloc WebVPN. Utilisez ? pour voir les niveaux disponibles.
cifs	(Facultatif) Spécifie le niveau de débogage CIFS de WebVPN. Utilisez ? pour voir les niveaux disponibles.
citrix	(Facultatif) Spécifie le niveau de débogage WebVPN Citrix. Utilisez ? pour voir les niveaux disponibles.
compression	(Facultatif) Spécifie le niveau de débogage de la compression WebVPN. Utilisez ? pour voir les niveaux disponibles.
condition	(Facultatif) Spécifie le niveau de débogage des conditions de filtre WebVPN. Utilisez ? pour voir les niveaux disponibles.
cstp-auth	(Facultatif) Spécifie le niveau de débogage de l'authentification CSTP de WebVPN. Utilisez ? pour voir les niveaux disponibles.
customization	(Facultatif) Spécifie le niveau de débogage de la personnalisation WebVPN. Utilisez ? pour voir les niveaux disponibles.
failover	(Facultatif) Spécifie le niveau de débogage du basculement de WebVPN. Utilisez ? pour voir les niveaux disponibles.
html	(Facultatif) Spécifie le niveau de débogage HTML de WebVPN. Utilisez ? pour voir les niveaux disponibles.
javascript	(Facultatif) Spécifie le niveau de débogage Javascript de WebVPN. Utilisez ? pour voir les niveaux disponibles.
kcd	(Facultatif) Spécifie le niveau de débogage du KCD WebVPN. Utilisez ? pour voir les niveaux disponibles.
listener	(Facultatif) Spécifie le niveau de débogage de l'auditeur WebVPN. Utilisez ? pour voir les niveaux disponibles.
mus	(Facultatif) Spécifie le niveau de débogage MUS du WebVPN. Utilisez ? pour voir les niveaux disponibles.
nfs	(Facultatif) Spécifie le niveau de débogage NFS de WebVPN. Utilisez ? pour voir les niveaux disponibles.
request	(Facultatif) Spécifie le niveau de débogage de la demande WebVPN. Utilisez ? pour voir les niveaux disponibles.
response	(Facultatif) Spécifie le niveau de débogage de la réponse WebVPN. Utilisez ? pour voir les niveaux disponibles.
saml	(Facultatif) Spécifie le niveau de débogage SAML WebVPN. Utilisez ? pour voir les niveaux disponibles.

session	(Facultatif) Spécifie le niveau de débogage de la session WebVPN. Utilisez ? pour voir les niveaux disponibles.
task	(Facultatif) Spécifie le niveau de débogage de la tâche WebVPN. Utilisez ? pour voir les niveaux disponibles.
transformation	(Facultatif) Spécifie le niveau de débogage de la transformation WebVPN. Utilisez ? pour voir les niveaux disponibles.
url	(Facultatif) Spécifie le niveau de débogage de l'URL WebVPN. Utilisez ? pour voir les niveaux disponibles.
util	(Facultatif) Spécifie le niveau de débogage de l'utilitaire WebVPN. Utilisez ? pour voir les niveaux disponibles.
xml	(Facultatif) Spécifie le niveau de débogage XML de WebVPN. Utilisez ? pour voir les niveaux disponibles.

Commande par défaut

Le niveau de débogage par défaut est 1.

Commandes associées

Commande	Description
show debug webvpn	Affiche les paramètres de débogage actuellement actifs pour WebVPN.
undebug webvpn	Désactive le débogage pour WebVPN. Cette commande est un synonyme de **no debug webvpn**.

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.