

ASA 8.X : Autoriser l'application utilisateur à s'exécuter avec le rétablissement du tunnel VPN L2L

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Configuration](#)

[Diagramme du réseau](#)

[Détails de compatibilité pour cette fonctionnalité](#)

[Configurations](#)

[Activer cette fonctionnalité](#)

[Vérification](#)

[Dépannage](#)

[Définir la valeur de vie IKE sur zéro](#)

[Message d'erreur lors de la suppression du tunnel](#)

[En quoi cette fonction diffère-t-elle de l'option reclassify-vpn ?](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit des informations sur la fonctionnalité de flux tunnelés IPsec persistants et sur la façon de conserver le flux TCP lors de la perturbation d'un tunnel VPN.

[Conditions préalables](#)

[Conditions requises](#)

Les lecteurs de ce document doivent avoir une compréhension de base du fonctionnement du VPN. Référez-vous à ces documents pour plus d'informations :

- [Exemple de configuration de VPN L2L](#)
- [VPN L2L avec ASA](#)

[Components Used](#)

Les informations de ce document sont basées sur l'appliance de sécurité adaptative (ASA) Cisco avec les versions 8.2 et ultérieures.

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. If your network is live, make sure that you understand the potential impact of any command.

Conventions

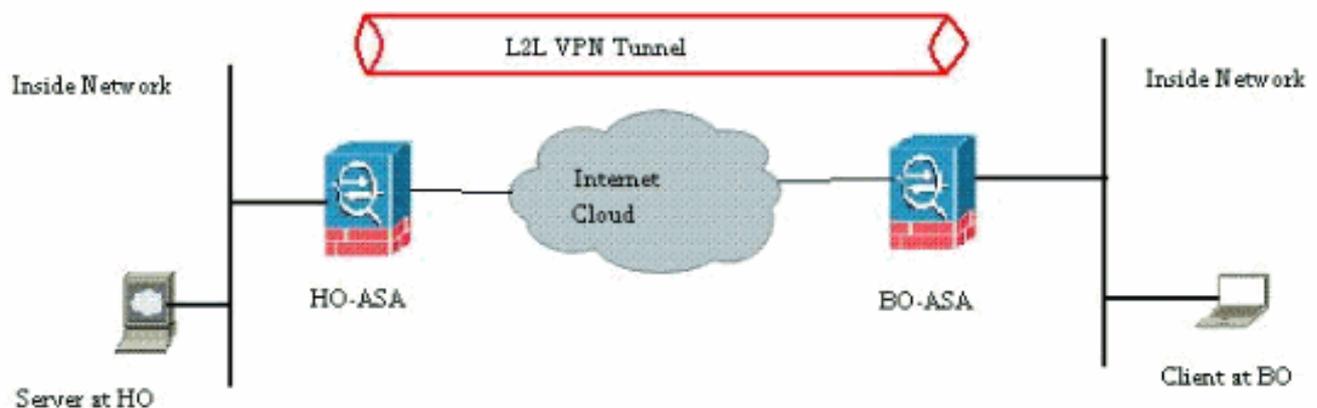
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Configuration

Comme le montre le schéma de réseau, la succursale (BO) est connectée au siège social (HO) via le VPN site à site. Prenons l'exemple d'un utilisateur final de la succursale qui tente de télécharger un fichier volumineux à partir du serveur situé au siège social. Le téléchargement dure des heures. Le transfert de fichiers fonctionne correctement jusqu'à ce que le VPN fonctionne correctement. Cependant, lorsque le VPN est perturbé, le transfert de fichiers est suspendu et l'utilisateur doit relancer la demande de transfert de fichiers à partir du début après l'établissement du tunnel.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Ce problème est dû à la fonctionnalité intégrée du fonctionnement de l'ASA. L'ASA surveille chaque connexion qui la traverse et met à jour une entrée dans sa table d'état selon la fonction d'inspection d'applications. Les détails chiffrés du trafic qui traversent le VPN sont mis à jour sous forme de base de données de l'association de sécurité (SA). Pour le scénario de ce document, il gère deux flux de trafic différents. L'une est le trafic chiffré entre les passerelles VPN et l'autre est le flux de trafic entre le serveur du siège social et l'utilisateur final de la succursale. Quand la connexion VPN se termine, les détails d'écoulement pour cette SA particulière sont supprimés. Cependant, l'entrée du tableau d'état mis à jour par l'ASA pour cette connexion TCP devient éventée en raison de l'absence d'activité, qui entrave le téléchargement. Ceci signifie que l'ASA retiendra toujours la connexion TCP pour ce flux particulier tandis que l'application utilisateur se termine. Cependant, les connexions TCP deviendront erratiques et éventuellement s'interrompre après que le seuil du délai d'inactivité TCP est franchi.

Ce problème a été résolu en introduisant une caractéristique appelée flux IPSec en tunnel persistents. Une nouvelle commande a été intégrée dans Cisco ASA pour conserver les informations de la table d'état lors de la renégociation du tunnel VPN. La commande est affichée ici :

```
sysopt connection preserve-vpn-flows
```

Par défaut, cette commande est désactivée. En activant cette option, Cisco ASA conserve les informations de la table d'état TCP lorsque le VPN L2L récupère de la perturbation et rétablit le tunnel.

Dans ce scénario, cette commande doit être activée aux deux extrémités du tunnel. S'il s'agit d'un périphérique autre que Cisco à l'autre extrémité, l'activation de cette commande sur Cisco ASA devrait suffire. Si la commande est activée lorsque les tunnels étaient déjà actifs, les tunnels doivent être effacés et rétablis pour que cette commande prenne effet. Pour plus de détails sur le déblaiement et le rétablissement des tunnels, reportez-vous à [Effacer les associations de sécurité](#).

Détails de compatibilité pour cette fonctionnalité

Cette fonctionnalité a été introduite dans le logiciel Cisco ASA version 8.0.4 et ultérieure. Ceci est pris en charge uniquement pour ces types de VPN :

- Tunnels LAN à LAN
- Tunnels d'accès à distance en mode d'extension réseau (NEM)

Cette fonctionnalité n'est pas prise en charge pour ces types de VPN :

- Tunnels d'accès à distance IPSec en mode client
- Tunnels VPN AnyConnect ou SSL

Cette fonctionnalité n'existe pas sur ces plates-formes :

- Cisco PIX avec la version logicielle 6.0
- Concentrateurs VPN Cisco
- Plates-formes Cisco IOS®

L'activation de cette fonctionnalité ne crée pas de surcharge supplémentaire sur le traitement du processeur interne de l'ASA, car elle va conserver les mêmes connexions TCP que le périphérique lorsque le tunnel est actif.

Remarque : cette commande s'applique uniquement aux connexions TCP. Il n'a aucun effet sur le trafic UDP. Les connexions UDP expireront en fonction du délai d'attente configuré.

Configurations

Remarque : utilisez l'[outil de recherche de commandes](#) (clients [enregistrés](#) uniquement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Ce document utilise la configuration suivante :

- CiscoASA

Voici un exemple de résultat de configuration en cours du pare-feu Cisco ASA à une extrémité du tunnel VPN :

```
CiscoASA
ASA Version 8.2(1)
!
hostname CiscoASA
domain-name example.com
enable password <removed>
passwd <removed>
names
!
interface Ethernet0/0
  speed 100
  duplex full
  nameif outside
  security-level 0
  ip address 209.165.201.2 255.255.255.248
!
interface Ethernet0/1
  nameif inside
  security-level 100
  ip address 10.224.9.5 255.255.255.0
!
interface Ethernet0/2
  shutdown
  no nameif
  no security-level
  no ip address
!
!
interface Management0/0
  nameif management
  security-level 100
  ip address 10.224.14.10 255.255.255.0
!
boot system disk0:/asa822-k8.bin
ftp mode passive
  !---Output Suppressed ! access-list test extended
permit ip 10.224.228.0 255.255.255.128 any access-list
test extended permit ip 10.224.52.0 255.255.255.128 any
access-list 100 extended permit ip 10.224.228.0
255.255.255.128 any access-list 100 extended permit ip
10.224.52.0 255.255.255.128 any access-list
inside_access_out extended permit ip any 10.224.228.0
255.255.255.1 ! !---Output Suppressed global (outside) 1
interface nat (inside) 0 access-list test nat (inside) 1
10.224.10.0 255.255.255.0 ! !---Output Suppressed route
inside 10.0.0.0 255.0.0.0 10.224.9.1 1 route outside
0.0.0.0 255.255.255.255 209.165.201.1 1 timeout xlate
3:00:00 timeout conn 1:00:00 half-closed 0:10:00 udp
0:02:00 icmp 0:00:02 timeout sunrpc 0:10:00 h323 0:05:00
h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 timeout sip
0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-
disconnect 0:02:00 timeout sip-provisional-media 0:02:00
uauth 0:05:00 absolute timeout tcp-proxy-reassembly
0:01:00 dynamic-access-policy-record DfltAccessPolicy !
!---Output Suppressed http server idle-timeout 40 http
10.224.3.0 255.255.255.0 management http 0.0.0.0 0.0.0.0
inside ! snmp-server enable traps snmp authentication
```

```

linkup linkdown coldstart ! !--- To preserve and resume
stateful (TCP) tunneled IPsec LAN-to-LAN traffic within
the timeout period after the tunnel drops and recovers.
sysopt connection preserve-vpn-flows
service resetoutside
!
crypto ipsec transform-set ESP-AES-256-MD5 esp-aes-256
esp-md5-hmac
crypto ipsec transform-set testSET esp-3des esp-md5-hmac
crypto map map1 5 match address 100
crypto map map1 5 set peer 209.165.200.10
crypto map map1 5 set transform-set testSET
crypto map map1 interface outside
crypto isakmp enable outside
crypto isakmp policy 5
  authentication pre-share
  encryption 3des
  hash sha
  group 2
  lifetime 86400
crypto isakmp policy 10
  authentication pre-share
  encryption des
  hash sha
  group 2
  lifetime 86400
!---Output Suppressed ! telnet timeout 5 ssh timeout 5
console timeout 0 threat-detection basic-threat threat-
detection statistics access-list ! !---Output Suppressed
! tunnel-group 209.165.200.10 type ipsec-l2l tunnel-
group 209.165.200.10 ipsec-attributes pre-shared-key *
!---Output Suppressed class-map inspection_default match
default-inspection-traffic ! policy-map type inspect dns
preset_dns_map parameters message-length maximum 512
policy-map global_policy class inspection_default
inspect dns preset_dns_map inspect ftp inspect h323 h225
inspect h323 ras inspect rsh inspect rtsp inspect esmtp
inspect sqlnet inspect skinny inspect sunrpc inspect
xdmcp inspect sip inspect netbios inspect tftp !
service-policy global_policy global prompt hostname
state Cryptochecksum:5c228e7131c169f913ac8198ecf8427e :
end

```

Activer cette fonctionnalité

Par défaut, cette fonction est désactivée. Cette commande peut être activée à l'aide de l'interface de ligne de commande de l'ASA :

```
CiscoASA(config)#sysopt connection preserve-vpn-flows
```

Vous pouvez afficher ce message à l'aide de cette commande :

```

CiscoASA(config)#show run all sysopt
no sysopt connection timewait
sysopt connection tcpmss 1380
sysopt connection tcpmss minimum 0
sysopt connection permit-vpn
sysopt connection reclassify-vpn
sysopt connection preserve-vpn-flows

```

```
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
no sysopt noproxyarp outside
```

Lorsque vous utilisez l'ASDM, cette fonctionnalité peut être activée en suivant le chemin suivant :

Configuration > Remote Access VPN > Network (Client) Access > Advanced > IPsec > System Options.

Ensuite, cochez l'option *Préserver les flux VPN avec état lorsque le tunnel tombe en mode d'extension réseau (NEM)*.

Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- **show asp table vpn-context detail** - Affiche le contenu du contexte VPN du chemin de sécurité accéléré, qui peut vous aider à résoudre un problème. Voici un exemple de sortie de la commande **show asp table vpn-context** lorsque la fonction de flux tunnelisés IPsec persistants est activée. Notez qu'il contient un indicateur **PRESERVE** spécifique.

```
CiscoASA(config)#show asp table vpn-context
```

```
VPN CTX=0x0005FF54, Ptr=0x6DE62DA0, DECR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000, gc=0
```

```
VPN CTX=0x0005B234, Ptr=0x6DE635E0, ENCR+ESP+PRESERVE, UP, pk=0000000000, rk=0000000000, gc=0
```

Dépannage

Dans cette section, certains contournements sont présentés afin d'éviter le battement des tunnels. Les avantages et les inconvénients des solutions de contournement sont également détaillés.

Définir la valeur de vie IKE sur zéro

Vous pouvez faire en sorte qu'un tunnel VPN reste en vie pendant une durée infinie, mais pas pour renégocier, en conservant la valeur de durée de vie IKE à zéro. Les informations relatives à la SA sont conservées par les homologues VPN jusqu'à l'expiration de la durée de vie. En attribuant une valeur égale à zéro, vous pouvez faire durer cette session IKE pour toujours. Par ce biais, vous pouvez éviter les problèmes de déconnexion de flux intermittents lors du recadrage du tunnel. Pour cela, utilisez la commande suivante :

```
CiscoASA(config)#crypto isakmp policy 50 lifetime 0
```

Cependant, ceci présente un inconvénient spécifique en termes de compromission du niveau de sécurité du tunnel VPN. La copie de la session IKE dans des intervalles de temps spécifiés fournit plus de sécurité au tunnel VPN en termes de clés de chiffrement modifiées à chaque fois et il devient difficile pour un intrus de décoder les informations.

Remarque : la désactivation de la durée de vie IKE ne signifie pas que le tunnel ne recouvre pas du tout la clé. Néanmoins, l'association de sécurité IPSec retouche la clé à l'intervalle de temps spécifié, car elle ne peut pas être définie sur zéro. La valeur de durée de vie minimale autorisée pour une SA IPSec est de 120 secondes et la valeur maximale est de 214783647 secondes. Pour plus d'informations à ce sujet, référez-vous à [durée de vie de SA IPSec](#).

[Message d'erreur lors de la suppression du tunnel](#)

Lorsque cette fonctionnalité n'est pas utilisée dans la configuration, Cisco ASA renvoie ce message de journal lorsque le tunnel VPN est interrompu :

```
%ASA-6-302014 : Arrêter la connexion TCP 57983 pour outside:XX.XX.XX.XX/80 à  
inside:10.0.0.100/1135 durée 0:00:36 octets 53947 Le tunnel a été désactivé
```

Vous pouvez voir que la raison en est que le **tunnel a été détruit**.

Remarque : la journalisation de niveau 6 doit être activée pour afficher ce message.

[En quoi cette fonction diffère-t-elle de l'option reclassify-vpn ?](#)

L'option [préserver-vpn-flow](#) est utilisée lorsqu'un tunnel rebondit. Cela permet à un flux TCP précédent de rester ouvert de sorte que lorsque le tunnel redémarre, le même flux peut être utilisé.

Lorsque la commande **sysopt connection reclassify-vpn** est utilisée, elle efface tout flux précédent qui se rapporte au trafic tunnelisé et classe le flux pour passer par le tunnel. L'option reclassify-vpn est utilisée dans une situation où un flux TCP a déjà été créé qui n'est pas lié au VPN. Cela crée une situation où le trafic ne traverse pas le tunnel après l'établissement du VPN. Pour plus d'informations à ce sujet, référez-vous à [sysopt reclassify-vpn](#).

[Informations connexes](#)

- [VPN site à site \(L2L\) avec ASA](#)
- [Page de documentation Cisco ASA](#)
- [Support et documentation techniques - Cisco Systems](#)