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

Contenu

Introduction

Ce document fournit des informations au sujet de la caractéristique persistante d'écoulements percée un tunnel par IPSec et comment retenir l'écoulement de TCP au-dessus de l'interruption d'un tunnel VPN.

Conditions préalables

Conditions requises

Les lecteurs de ce document devraient avoir la compréhension de base sur la façon dont le VPN fonctionne. Référez-vous à ces documents pour plus d'informations :

- Configuration du VPN de l'échantillon L2L
- L2L VPN avec l'ASA

Composants utilisés

Les informations dans ce document sont basées sur l'appliance de sécurité adaptable Cisco (ASA) avec la version 8.2 et ultérieures.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

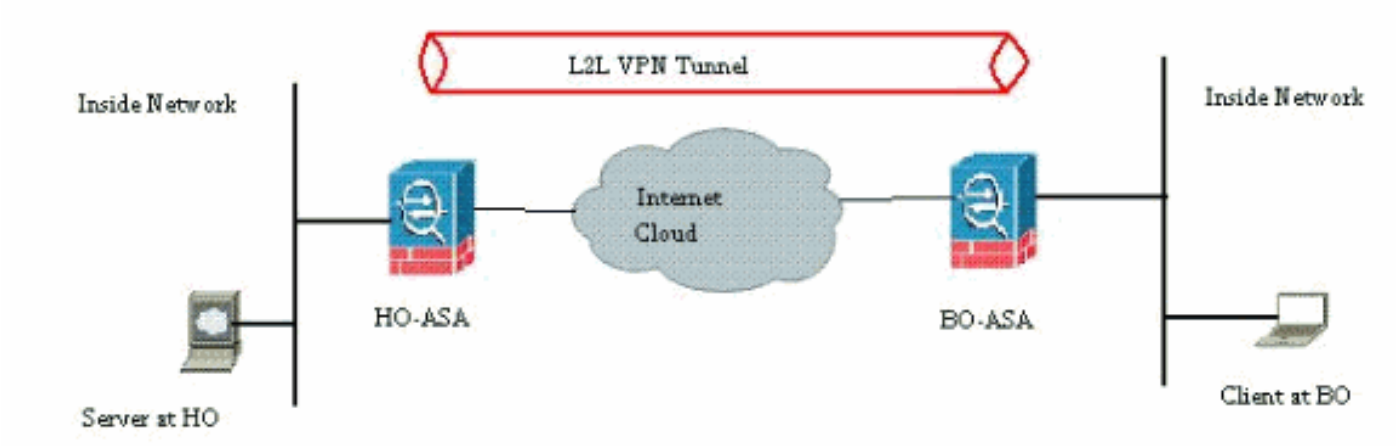
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Suivant les indications du schéma de réseau, la succursale (BO) est connectée au siège social (HO) par le site à site VPN. Considérez un utilisateur final à la succursale tentant de télécharger un gros fichier du serveur situé dans le siège social. Le téléchargement dure des heures. Le transfert de fichiers fonctionne bien jusqu'à ce que le VPN fonctionne bien. Cependant, quand le VPN est perturbé, le transfert de fichiers est arrêté et l'utilisateur doit re-initié la demande de transfert de fichiers de nouveau du début après que le tunnel soit établi.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Ce problème surgit en raison de la fonctionnalité intégrée sur la façon dont l'ASA fonctionne. L'ASA surveille chaque connexion qui la traverse et met à jour une entrée dans sa table d'état selon la caractéristique d'inspection d'application. 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 met à jour les deux circulations différentes. On est le trafic chiffré entre les passerelles VPN et l'autre est la circulation entre le serveur au siège social et l'utilisateur à la succursale. Quand le VPN est terminé, les détails d'écoulement pour cette SA particulière sont supprimés. Cependant, l'entrée de table d'état mise à jour par l'ASA pour cette connexion TCP devient éventée en raison d'aucune 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 bête perdue et par la suite délai d'attente après que le compteur de durée d'inactivité de TCP expire.

Ce problème a été résolu en introduisant une caractéristique appelée les écoulements percés un tunnel IPSec de Persistent. Une nouvelle commande a été intégrée dans Cisco ASA de retenir les informations de table d'état à la renégociation du tunnel VPN. La commande est affichée ici :

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

Par défaut, cette commande est désactivée. En activant ceci, Cisco ASA mettra à jour les informations de table d'état de TCP quand le L2L VPN récupère de l'interruption et rétablit le tunnel.

Dans ce scénario, cette commande doit être activée sur les deux extrémités du tunnel. Si c'est un périphérique non-Cisco à l'autre extrémité, l'activation de cette commande sur Cisco ASA devrait suffire. Si la commande est activée quand les tunnels étaient déjà en activité, les tunnels doivent être effacés et rétablis pour que cette commande la prenne effet. Pour plus de détails sur l'effacement et rétablir les tunnels, référez-vous clairement aux associations de sécurité.

Détails de compatibilité pour cette caractéristique

Cette caractéristique a été introduite dans la version de logiciel 8.0.4 de Cisco ASA et plus tard. Ceci est pris en charge seulement pour ces types de VPN :

- RÉSEAU LOCAL aux tunnels de RÉSEAU LOCAL
- Tunnels d'Accès à distance dans le mode d'extension réseau (PAS MENTIONNÉ AILLEURS)

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

- Tunnels d'Accès à distance d'IPSec en mode de client
- AnyConnect ou tunnels de VPN SSL

Cette caractéristique n'existe pas sur ces Plateformes :

- Cisco PIX avec la version de logiciel 6.0
- Concentrateurs de Cisco VPN
- Plateformes de Cisco IOS®

L'activation de cette caractéristique ne crée aucune surcharge supplémentaire sur le traitement interne CPU de l'ASA parce qu'elle va garder les mêmes connexions TCP que le périphérique a quand le tunnel est.

Remarque: Cette commande s'applique pour des connexions TCP seulement. Il n'exerce aucun effet sur le trafic UDP. Les connexions d'UDP veulent le délai d'attente selon le délai d'inactivité configuré.

Configurations

Remarque: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) 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

C'est un résultat de configuration en cours d'échantillon du Pare-feu de 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
```

Activez cette caractéristique

Par défaut, cette caractéristique est désactivée. Ceci peut être activé à l'aide de cette commande au CLI de l'ASA :

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

Ceci peut être visualisé 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
```

En utilisant l'ASDM, cette caractéristique peut être activée en suivant ce chemin :

La configuration > l'Accès à distance VPN > réseau (client) Access > ont avancé > IPsec > options de système.

Puis, vérifiez les *écoulements de l'avec état VPN de conserve quand le tunnel relâche pour l'*option de *mode d'extension réseau (PAS MENTIONNÉ AILLEURS)*.

Vérifiez

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** .

- **affichez le détail de VPN-contexte de table d'asp** — Affiche les teneurs en contexte VPN du

chemin accéléré de Sécurité, qui pourrait vous aider à dépanner un problème. Ce qui suit est un résultat témoin de la commande de VPN-**contexte de table d'asp d'exposition** quand l'IPSec persistant a percé un tunnel des écoulements que la caractéristique est activée. Notez qu'il contient un indicateur spécifique de **CONSERVE**.`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`

Dépannez

Dans cette section, certains contournements sont présentés pour éviter le lien instable des tunnels. Les avantages - et - des inconvénients des contournements sont également détaillés.

Placez la valeur de vie d'IKE à zéro

Vous pouvez faire un tunnel VPN pour rester actif pendant un temps infini, mais pour ne pas renégocier, en gardant la valeur de vie d'IKE en tant que zéro. Les informations sur SA sont retenues par les homologues VPN jusqu'à ce que la vie expire. En assignant une valeur en tant que zéro, vous pouvez faire ce bout de session d'IKE pour toujours. Par ceci, vous pouvez éviter les questions intermittentes de déconnexion d'écoulement pendant la nouvelle saisie du tunnel. Ceci peut être fait avec cette commande :

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

Cependant, ceci a un inconvénient spécifique en termes de compromettre le niveau de Sécurité du tunnel VPN. La nouvelle saisie de la session d'IKE dans des intervalles de temps spécifiés fournit plus de Sécurité au tunnel VPN en termes de clés de chiffrement modifiées chaque fois et il devient difficile que n'importe quel intrus décode les informations.

Remarque: Désactiver la vie d'IKE ne signifie pas que le tunnel ne réintroduit pas du tout. Toujours, IPSec SA réintroduira à l'intervalle de temps spécifié parce que cela ne peut pas être placé à zéro. La valeur minimum de vie permise pour IPSec SA est de 120 secondes et le maximum est de 214783647 secondes. Pour plus d'informations sur ceci, référez-vous à la vie d'IPSec SA.

Message d'erreur quand le tunnel relâche

Quand cette caractéristique n'est pas utilisée dans la configuration, Cisco ASA renvoie ce message de log quand le tunnel VPN est perturbé :

```
%ASA-6-302014 : La connexion TCP de démontage 57983 pour outside:XX.XX.XX.XX/80
inside:10.0.0.100/1135 au tunnel des octets 53947 de la durée 0:00:36 a été démolie
```

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

Remarque: Le niveau 6 se connectant doit être activé voir ce message.

Comment cette caractéristique diffère avec l'option de reclassifier-VPN

L'option de conserve-VPN-écoulement est utilisée quand un tunnel rebondit. Ceci permet à un écoulement précédent de TCP pour rester ouvert ainsi quand le tunnel se réactive, le même écoulement peut être utilisé.

Quand la commande de reclassifier-**VPN de connexion de sysopt** est utilisée, elle efface n'importe quel écoulement précédent qui concerne le trafic percé un tunnel et classifie l'écoulement pour passer par le tunnel. L'option de reclassifier-VPN est utilisée dans une situation quand on a déjà créé un écoulement de TCP qui n'est pas VPN associé. Ceci crée une situation où le trafic ne circule pas à travers le tunnel après que le VPN soit établi. Pour plus d'informations sur ceci, référez-vous au sysopt reclassifier-VPN.

Informations connexes

- Site à site VPN (L2L) avec l'ASA
- Page de documentation de Cisco ASA
- Support et documentation techniques - Cisco Systems