ASA : Remote-access de mode de Multi-contexte (AnyConnect) VPN

Contenu

Introduction

Ce document décrit comment configurer le réseau privé virtuel d'Accès à distance (RA) (VPN) sur le Pare-feu de l'appliance de sécurité adaptable Cisco (ASA) en plusieurs mode de contexte (MC). Il affiche Cisco ASA dans le mode de contexte multiple pris en charge/fonctions non prises en charge et condition d'autorisation en ce qui concerne le RA VPN.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration SSL ASA AnyConnect

- Plusieurs configuration de contexte ASA

Composants utilisés

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

- Deux code s'exécutant ASA 5585 9.5(2)
- Client 3.1.10010 d'AnyConnect

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 vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande

Informations générales

le Multi-contexte est une forme de la virtualisation qui permet à de plusieurs copies indépendantes d'une application pour fonctionner simultanément sur le même matériel, avec chaque copie (ou périphérique virtuel) apparaissant comme périphérique physique distinct à l'utilisateur. Ceci permet à une ASA simple pour apparaître comme multiple ASA à de plusieurs utilisateurs indépendants. La famille ASA a pris en charge des Pare-feu virtuels depuis sa version initiale ; cependant, il n'y avait aucun soutien de virtualisation d'Accès à distance dans l'ASA. Le soutien VPN LAN2LAN (L2L) du multi-contexte a été ajouté pour la release 9.0. Du multi-contexte **9.5.2** basé soutien de virtualisation des connexions d'Accès à distance VPN (RA) à l'ASA.

Caractéristiques prises en charge

- Connectivité SSL d'AnyConnect 3.X+ (ipv4, IPv6)
- Configuration centralisée d'image d'AnyConnect
- Mise à niveau d'image d'AnyConnect

Fonctions non prises en charge

- IKEv2, IKEv1
- Basculement dynamique
- Virtualisation instantanée
- Configuration d'image d'AnyConnect par contexte
- WebLaunch
- Téléchargement de profil de client
- DAP et CoA
- CSD/Hostscan
- Équilibrage de charge VPN
- Nom d'utilisateur-de-certificat et préremplissage-nom d'utilisateur
- Personnalisation/localisation

Autorisation

- Licence requise d'apex d'AnyConnect

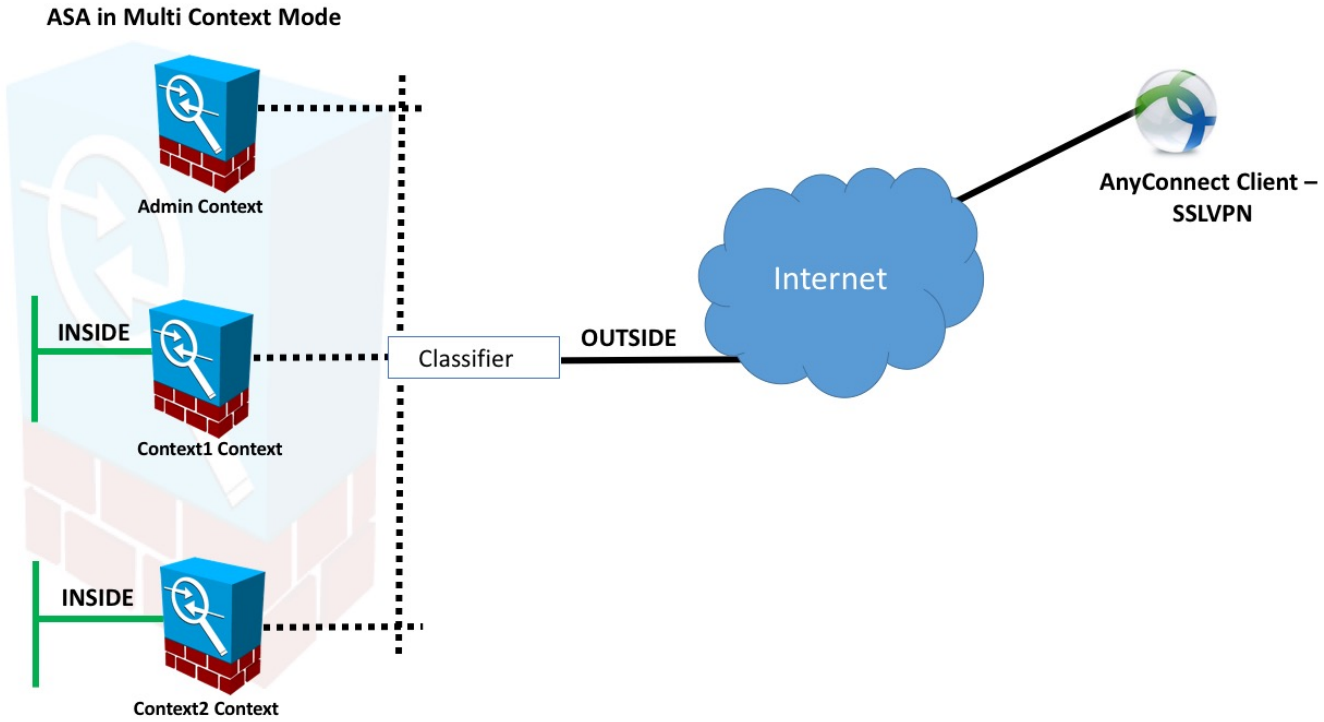
- Les essentiel autorise ignoré/non laissé
- Configurabilité pour contrôler l'utilisation maximum de permis par contexte
- Configurabilité pour permettre le permis éclatant par contexte

Configurez

Cette section décrit comment configurer Cisco ASA en tant que serveur des gens du pays CA.

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau



> **Remarque:** Les plusieurs contextes dans cet exemple partage une interface (DEHORS), puis le classificateur emploie les seules (automatique ou manuel) adresses MAC d'interface pour expédier des paquets. Pour plus de détails sur la façon dont les dispositifs de sécurité classifient des paquets dans le plusieurs contexte référez-vous comment l'ASA classifie des paquets

Configurations

Contexte de système

Étape 1. Configuration de Basculement.

```
!! Active Firewall
```

```
failover
failover lan unit primary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2

 !! Secondary Firewall

failover
failover lan unit secondary
failover lan interface LAN_FAIL GigabitEthernet0/3
failover link LAN_FAIL GigabitEthernet0/3
failover interface ip LAN_FAIL 10.1.1.1 255.255.255.252 standby 10.1.1.2
failover group 1
failover group 2
```

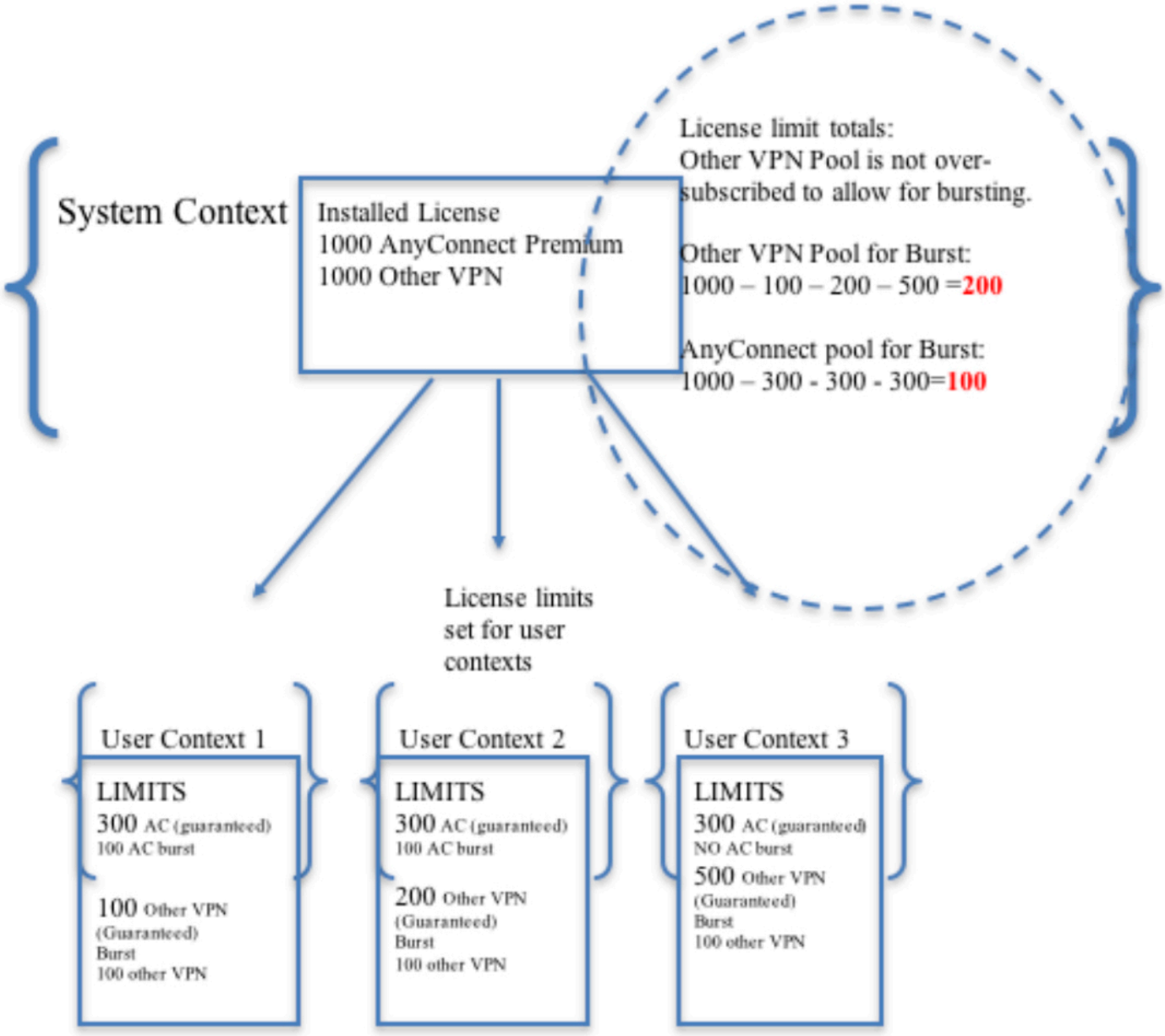
Étape 2. Allouez VPN Resouce.

Configuré par l'intermédiaire de la configuration existante de classe…. On permet des permis par le nombre de permis ou les % du total par contexte

Nouveaux types de ressource introduits pour MC RAVPN :

- VPN AnyConnect : Garanti à un contexte et ne peut pas être oversubscribed
- Rafale AnyConnect VPN : Permettez à contexte les permis supplémentaires au delà de la limite garantie. Le groupe de rafale se compose de tous les permis non garantis à un contexte et est autorisé à un sur la base du premier arrivé premier servi de éclatement de contexte

Modèle de ravitaillement de permis VPN :



Remarque: ASA5585 offre 10,000 sessions d'utilisateur maximum de Cisco AnyConnect et dans ce Cisco AnyConnect de l'exemple 4000 la session d'utilisateur est allouée par contexte.

```
class resource02
 limit-resource VPN AnyConnect  4000
 limit-resource VPN Burst AnyConnect  2000

class resource01
 limit-resource VPN AnyConnect 4 000
 limit-resource VPN Burst AnyConnect  2000
```

Étape 3. Configurez les contextes et assignez les ressources.

Remarque: Dans cet exemple GigabitEthernet0/0 est partagé parmi tout le contexte.

```
admin-context admin
context admin
  allocate-interface GigabitEthernet0/0
  config-url disk0:/admin
```

```
context context1
  member resource01
  allocate-interfaceGigabitEthernet0/0
  allocate-interface GigabitEthernet0/1
  config-url disk0:/context1
  join-failover-group 1

context context2
  member resource02
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/2
  config-url disk0:/context2
  join-failover-group 2
```

Étape 4. Installez le permis d'apex sur le Pare-feu.

Lançant ou désactivant des clés d'activation

Contexte d'admin

Étape 1. Installez le module de client d'AnyConnect.

> **Remarque:** 1. La mémoire instantanée n'est pas virtualisée et elle est seulement accessible du contexte de système.
> 2. Copiez les fichiers sur l'éclair dans l'image d'AnyConnect de contexte de système c.-à-d.
> 3. L'image d'AnyConnect est une configuration partagée.
> 4. Configuré dans le contexte d'admin seulement. Non disponible dans d'autres contextes.
> 5. Tous les contextes se rapportent automatiquement à cette configuration globale d'image d'AnyConnect.

```
webvpn
 anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
 anyconnect enable
```

Contexte fait sur commande 1

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 10.106.44.38  255.255.255.0 standby 10.106.44.39

!! Enable WebVPN on respective interfaces

webvpn
 enable OUTSIDE
 anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.1.1-192.168.50.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_1 internal
group-policy GroupPolicy_MC_RAVPN_1 attributes
```

```
 banner value "Welcome to Context1 SSLVPN"
 wins-server none
 dns-server value 192.168.20.10
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com

tunnel-group MC_RAVPN_1 type remote-access
tunnel-group MC_RAVPN_1 general-attributes
 address-pool mypool
 default-group-policy GroupPolicy_MC_RAVPN_1
tunnel-group MC_RAVPN_1 webvpn-attributes
 group-alias MC_RAVPN_1 enable
 group-url https://10.106.44.38/context1  enable
```

Contexte fait sur commande 2

```
 !! Shared interface configuration - OUTSIDE (GigabitEthernet0/0)

interface GigabitEthernet0/0
 nameif OUTSIDE
 security-level 0
 ip address 10.106.44.36  255.255.255.0 standby 10.106.44.37

!! Enable WebVPN on respective interface

webvpn
 enable OUTSIDE
 anyconnect enable

!! IP pool and username configuration

ip local pool mypool 192.168.51.1-192.168.101.1 mask 255.255.0.0

username cisco password cisco

!! Configure the require connection profile for SSL VPN

group-policy GroupPolicy_MC_RAVPN_2 internal
group-policy GroupPolicy_MC_RAVPN_2 attributes
 banner value "Welcome to Context2 SSLVPN"
 wins-server none
 dns-server value 192.168.60.10
 vpn-tunnel-protocol ssl-client
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value split
 default-domain value cisco.com

tunnel-group MC_RAVPN_2 type remote-access
tunnel-group MC_RAVPN_2 general-attributes
 address-pool mypool
 default-group-policy GroupPolicy_MC_RAVPN_2
tunnel-group MC_RAVPN_2 webvpn-attributes
 group-alias MC_RAVPN_2 enable
 group-url https://10.106.44.36/context2 enable
```

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Remarque: L'Output Interpreter Tool (clients enregistrés seulement) prend en charge

certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Vérifiez si le permis d'apex est installé

L'ASA n'identifie pas spécifiquement un permis d'apex d'AnyConnect mais elle impose les caractéristiques de permis d'un permis d'apex qui incluent :

- Premium d'AnyConnect autorisé à la limite de plate-forme
- AnyConnect pour le mobile
- AnyConnect pour le téléphone de Cisco VPN
- Estimation avancée de point final

Vérifiez si le module d'AnyConnect est installé dans le contexte d'admin et est disponible dans des contextes faits sur commande

```
 !! AnyConnect package is installed in Admin Context

ciscoasa/pri/ admin/act# show run webvpn
webvpn
 anyconnect image disk0:/anyconnect-win-3.1.10010-k9.pkg 1
 anyconnect enable

ciscoasa/pri/admin/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,1,10010
  Hostscan Version 3.1.10010
  Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed

!! AnyConnect package is available in context1
ciscoasa/pri/admin/act# changeto context context1

ciscoasa/pri/context1/act# show run webvpn
webvpn
 enable OUTSIDE
 anyconnect enable
 tunnel-group-list enable

ciscoasa/pri/context1/act# show webvpn anyconnect
1. disk0:/anyconnect-win-3.1.10010-k9.pkg 1 dyn-regex=/Windows NT/
  CISCO STC win2k+
  3,1,10010
  Hostscan Version 3.1.10010
  Wed 07/22/2015 12:06:07.65

1 AnyConnect Client(s) installed
```

Vérifiez si les utilisateurs peuvent se connecter par l'intermédiaire d'AnyConnect sur des contextes faits sur commande

Conseil : Pour une meilleure montre d'affichage au-dessous des vidéos dans pleine page.

```
 !! One Active Connection on Context1
```

```
ciscoasa/pri/context1/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 5
Assigned IP  : 192.168.1.1            Public IP    : 10.142.168.102
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium, AnyConnect for Mobile
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES-GCM-256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA384  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 3186                   Bytes Rx     : 426
Group Policy : GroupPolicy_MC_RAVPN_1 Tunnel Group : MC_RAVPN_1
Login Time   : 15:33:25 UTC Thu Dec 3 2015
Duration     : 0h:00m:05s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6a2c2600005000566060c5
Security Grp : none

!! Changing Context to Context2

ciscoasa/pri/context1/act# changeto context context2

!! One Active Connection on Context2

ciscoasa/pri/context2/act# show vpn-sessiondb anyconnect

Session Type: AnyConnect

Username     : cisco                  Index        : 1
Assigned IP  : 192.168.51.1           Public IP    : 10.142.168.94
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License      : AnyConnect Premium
Encryption   : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)AES256  DTLS-Tunnel: (1)AES256
Hashing      : AnyConnect-Parent: (1)none  SSL-Tunnel: (1)SHA1  DTLS-Tunnel: (1)SHA1
Bytes Tx     : 10550                  Bytes Rx     : 1836
Group Policy : GroupPolicy_MC_RAVPN_2 Tunnel Group : MC_RAVPN_2
Login Time   : 15:34:16 UTC Thu Dec 3 2015
Duration     : 0h:00m:17s
Inactivity   : 0h:00m:00s
VLAN Mapping : N/A                    VLAN         : none
Audt Sess ID : 0a6a2c2400001000566060f8
Security Grp : none

!! Changing Context to System

ciscoasa/pri/context2/act# changeto system

!! Notice total number of connections are two (for the device)

ciscoasa/pri/act# show vpn-sessiondb license-summary
----------------------------------------------------------------------------
VPN Licenses and Configured Limits Summary
----------------------------------------------------------------------------
                                   Status : Capacity : Installed :  Limit
                                 ----------------------------------------
AnyConnect Premium               :  ENABLED :    10000 :     10000 :   NONE
Other VPN (Available by Default) :  ENABLED :    10000 :     10000 :   NONE
AnyConnect for Mobile            :  ENABLED(Requires Premium or Essentials)
Advanced Endpoint Assessment     :  ENABLED(Requires Premium)
AnyConnect for Cisco VPN Phone   :  ENABLED
VPN-3DES-AES                     :  ENABLED
VPN-DES                          :  ENABLED
```

```
-------------------------------------------------------------------------

-------------------------------------------------------------------------
VPN Licenses Usage Summary
-------------------------------------------------------------------------
                        Local : Shared :   All  :   Peak :  Eff.  :
                       In Use : In Use : In Use : In Use :  Limit : Usage
                      ---------------------------------------------------
AnyConnect Premium     :      2 :      0 :       2 :      2 :  10000 :    0%
 AnyConnect Client    :                 :      2 :      2          :    0%
   AnyConnect Mobile  :                 :      2 :      2          :    0%
Other VPN              :                 :      0 :      0 :  10000 :    0%
 Site-to-Site VPN     :                 :      0 :      0          :    0%
-------------------------------------------------------------------------

!! Notice the resource usage per Context

ciscoasa/pri/act# show resource usage all resource VPN AnyConnect
Resource                 Current        Peak      Limit        Denied Context
AnyConnect                     1           1       4000             0 context1
AnyConnect                     1           1       4000             0 context2
```

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage d'AnyConnect

> **Conseil :** Au cas où l'ASA n'aurait pas le permis d'apex installé, la session d'AnyConnect serait terminée avec le Syslog ci-dessous :
>
> %ASA-6-725002 : Le périphérique s'est terminé la prise de contact SSL avec le client OUTSIDE:10.142.168.86/51577 à 10.106.44.38/443 pour la session TLSv1
> %ASA-6-113012 : Authentification de l'utilisateur d'AAA réussie : base de données locale : utilisateur = Cisco
> %ASA-6-113009 : L'AAA a récupéré la stratégie de groupe par défaut (GroupPolicy_MC_RAVPN_1) pour l'utilisateur = le Cisco
> %ASA-6-113008 : État de transaction d'AAA ACCEPT : utilisateur = Cisco
> %ASA-3-716057 : Groupez la session IP <10.142.168.86> d'utilisateur terminée, aucun permis d'apex d'AnyConnect disponible
> %ASA-4-113038 : Groupez IP <10.142.168.86> d'utilisateur incapable de créer la session de parent d'AnyConnect.

Références

Notes de mise à jour : 9.5(2)

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Guide de dépannage d'AnyConnect VPN Client - Problèmes courants
- Gérant, surveillant, et dépannage des sessions d'AnyConnect
- Support et documentation techniques - Cisco Systems