ASA : VPN d'accès à distance en mode multicontexte (AnyConnect)

Introduction

Ce document décrit comment configurer le réseau privé virtuel (VPN) d'accès à distance (RA) sur le pare-feu ASA (Adaptive Security Appliance) de Cisco en mode MC (Multiple Context) à l'aide de l'interface de ligne de commande. Il montre Cisco ASA en mode de contexte multiple, fonctionnalités prises en charge/non prises en charge et conditions de licence en ce qui concerne le VPN RA.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration SSL d'ASA AnyConnect
- Configuration de plusieurs contextes ASA

Components Used

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

- AnyConnect Secure Mobility Client version 4.4.00243
- Deux ASA5525 avec le logiciel ASA version 9.6(2)

Note: Téléchargez le package AnyConnect VPN Client à partir du téléchargement de logiciels Cisco (clients enregistrés uniquement).

Note: 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.

Informations générales

Le multicontexte est une forme de virtualisation qui permet à plusieurs copies indépendantes d'une application de s'exécuter simultanément sur le même matériel, chaque copie (ou périphérique virtuel) apparaissant comme un périphérique physique distinct pour l'utilisateur. Cela permet à un seul ASA d'apparaître comme plusieurs ASA à plusieurs utilisateurs indépendants. La famille ASA prend en charge les pare-feu virtuels depuis sa version initiale ; cependant, il n'y avait pas de prise en charge de la virtualisation pour l'accès à distance dans l'ASA. La prise en charge de VPN LAN2LAN (L2L) pour le multicontexte a été ajoutée pour la version 9.0.

Note: À partir de **9.5.2** prise en charge de la virtualisation multicontexte pour les connexions d'accès à distance VPN (RA) à l'ASA.

Àpartir de **9.6.2** nous avons le support de la Virtulaiisation Flash, ce qui signifie que nous pouvons avoir une image Anyconnect par contexte.

Historique des fonctions pour le multicontexte

Nouvelles fonctionnalités ajoutées dans ASA 9.6(2)

Fonctionnalité	Description
Fonction de préremplissage/nom d'utilisateur à partir du certificat pour le mode de contexte multiple	La prise en charge d'AnyConnect SSL est étendue, ce qui permet d'activer également les CLI de fonction pré-remplissage/nom d'utilisateur du certificat, auparavant disponibles uniquement en mode unique, en mode contexte multi
Virtualisation Flash pour VPN d'accès à distance	Le VPN d'accès à distance en mode de contexte multiple prend désormais en charge la virtualisation Flash. Chaque contexte peut disposer d'un espace de stockage privé et d'un espace de stockage partagé en fonction de la mémoire totale disponible.
Profils client AnyConnect pris en charge dans les périphériques multicontexte	Les profils client AnyConnect sont pris en charge dans les périphériques multicontexte. Pour ajouter un nouveau profil à l'aide d'ASDM, vous devez dis du client AnyConnect Secure Mobility version 4.2.00748 ou 4.3.03013 et ultéri
Basculement avec état pour les connexions AnyConnect en mode de contexte multiple	Le basculement dynamique est désormais pris en charge pour les connexions AnyConnect en mode de contexte multiple.
La politique d'accès dynamique VPN d'accès à distance (DAP) est prise en charge en mode de contexte multiple	Vous pouvez maintenant configurer DAP par contexte en mode de contexte multiple.
La CoA VPN d'accès à distance (changement d'autorisation) est prise en charge en mode de contexte multiple	Vous pouvez maintenant configurer CoA par contexte en mode de contexte multiple.
La localisation VPN d'accès à distance est prise en charge en mode de contexte multiple	La localisation est prise en charge globalement. Il n'existe qu'un seul ensembl fichiers de localisation partagés dans différents contextes.
Le stockage de capture de paquets par contexte est pris en charge.	L'objectif de cette fonctionnalité est de permettre à l'utilisateur de copier une capture directement d'un contexte vers le stockage externe ou vers le stockag privé de contexte sur flash. Cette fonctionnalité permet également de copier la capture brute dans les outils de capture de paquets externes, tels que le requi métallique, à partir d'un contexte.

Fonctionnalités d'ASA 9.5(2)

Fonctionnalité	Description
AnyConnect 4.x et versions ultérieures (VPN SSL uniquement) ; aucune prise en charge IKEv2)	Prise en charge de la virtualisation multicontexte pour les connexions d'a à distance VPN à l'ASA.
Configuration d'image AnyConnect centralisée	• Le stockage Flash n'est pas virtualisé. • L'image AnyConnect est configurée globalement dans le contexte ad et la configuration s'applique à tous les contextes
Mise à niveau de l'image AnyConnect	Les profils client AnyConnect sont pris en charge dans les périphériques multicontexte. Pour ajouter un nouveau profil à l'aide d'ASDM, vous deve disposer du client AnyConnect Secure Mobility version 4.2.00748 ou 4.3. et ultérieure.
Gestion des ressources contextuelles pour les connexions AnyConnect	• Possibilité de configuration pour contrôler l'utilisation maximale des licences par contexte • Possibilité de configuration pour autoriser le découpage de licences p contexte

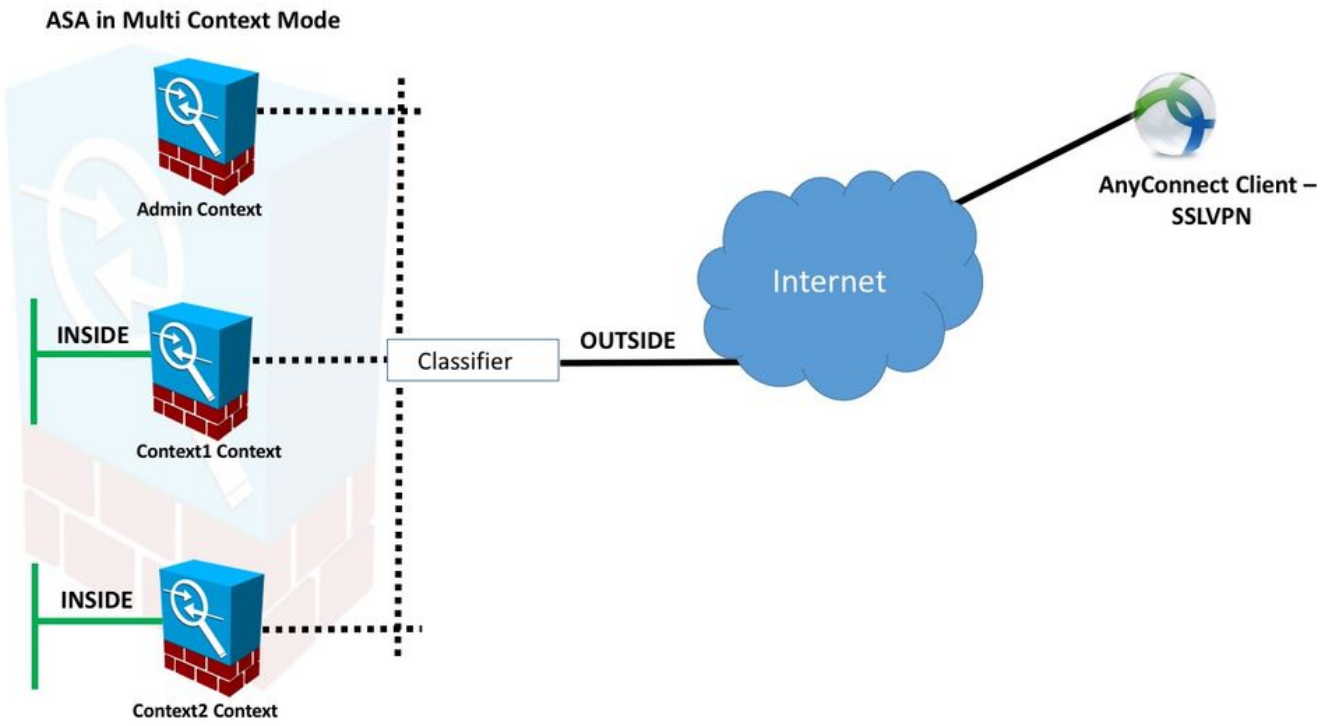
Licence

- Licence AnyConnect Apex requise
- Licences Essentials ignorées/non autorisées
- Possibilité de configuration pour contrôler l'utilisation maximale des licences par contexte
- Possibilité de configuration pour autoriser le découpage de licences par contexte

Configuration

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

Diagramme du réseau



Note: Plusieurs contextes dans cet exemple partagent une interface (OUTSIDE), puis le classificateur utilise les adresses MAC uniques (automatiques ou manuelles) de l'interface pour transférer des paquets. Pour plus d'informations sur la manière dont l'appliance de sécurité classe les paquets dans plusieurs contextes, reportez-vous à Comment l'ASA classifie les paquets

La procédure de configuration suivante est basée sur la version ASA 9.6.2 et les versions ultérieures, ce qui illustre certaines des nouvelles fonctionnalités disponibles.Les différences dans la procédure de configuration pour les versions ASA antérieures à la version 9.6.2 (et supérieure à la version 9.5.2) sont documentées dans l'annexe A du document.

Les configurations nécessaires dans le contexte système et les contextes personnalisés pour la configuration du VPN d'accès à distance sont décrites ci-dessous :

Configurations initiales dans le contexte du système

Pour commencer, dans le contexte du système, configurez le basculement, l'allocation de ressources VPN, les contextes personnalisés et la vérification de licence Apex. La procédure et les configurations sont décrites dans cette section et dans la section suivante

Étape 1. Configuration du 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
```

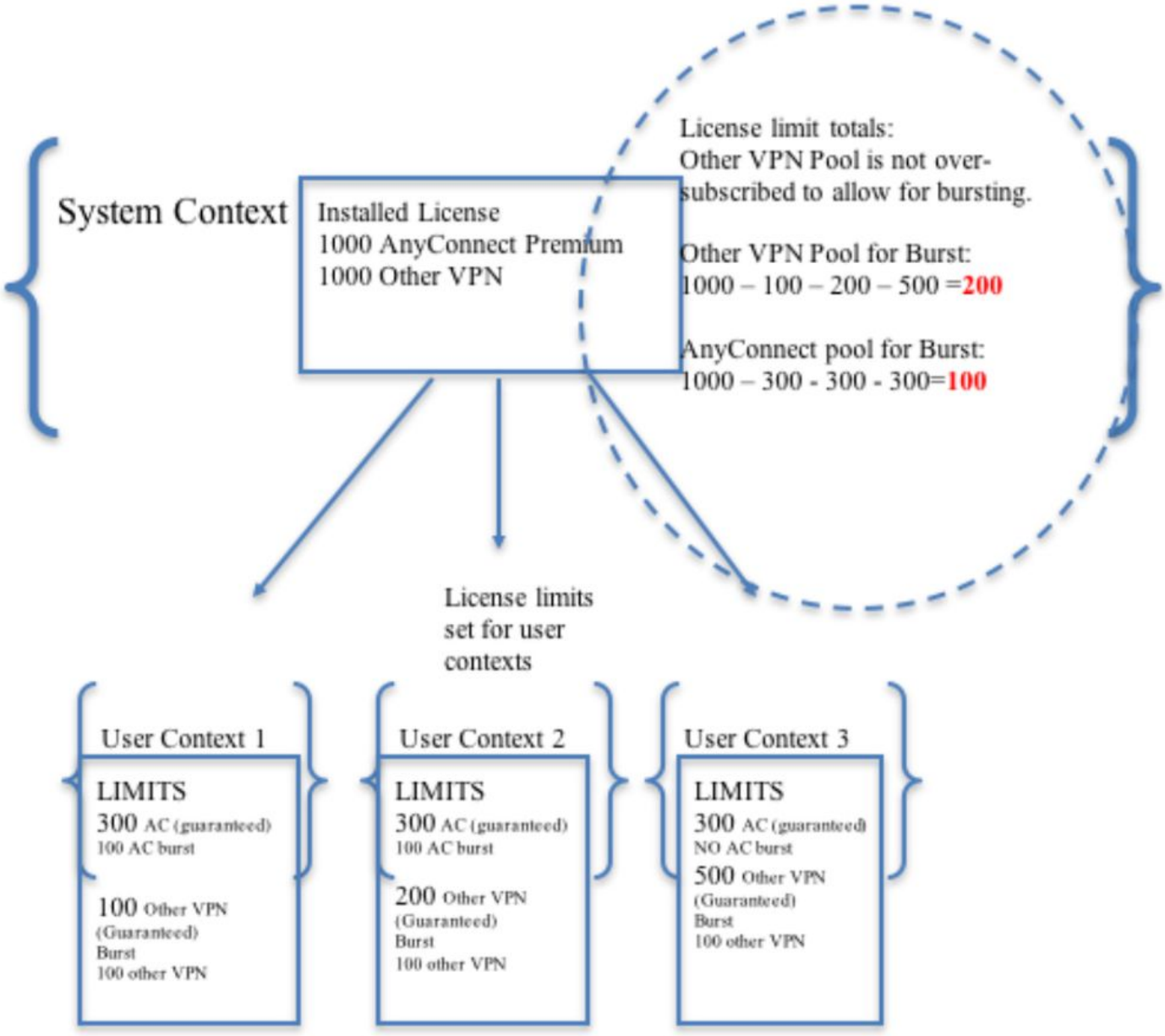
Étape 2. Allouer une ressource VPN.

Configuré via la configuration de classe existante. Les licences sont autorisées par le nombre de licences ou le pourcentage du total par contexte

Nouveaux types de ressources introduits pour MC RAVPN :

- VPN AnyConnect : Garantie à un contexte et ne peut pas être sursouscrit
- VPN Burst AnyConnect : Autoriser les licences contextuelles supplémentaires au-delà de la limite garantie. Le pool de rafales est constitué de licences non garanties à un contexte et autorisées à un contexte de rafale sur la base du premier arrivé, premier servi

Modèle de configuration de licence VPN :



Note: ASA5585 offre 10 000 sessions utilisateur Cisco AnyConnect maximum et dans cet exemple, 4 000 sessions utilisateur Cisco AnyConnect sont allouées par contexte.

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

class resource01
 limit-resource VPN AnyConnect 4000
 limit-resource VPN Burst AnyConnect 2000
```

Étape 3. Configurer des contextes et affecter des ressources.

Remarque : Dans cet exemple, GigabitEthernet0/0 est partagé entre tous les contextes.

```
admin-context admin
```

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

context context1
  member resource01
  allocate-interface GigabitEthernet0/0
  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. Vérifiez que la licence Apex est installée sur l'ASA, reportez-vous au lien ci-dessous pour plus de détails.

Activation ou désactivation des clés d'activation

Étape 5. Configurez un package d'image Anyconnect. Selon la version ASA utilisée, il existe deux façons de charger l'image Anyconnect et de configurer pour RA VPN. Si la version est 9.6.2 et supérieure, la virtualisation Flash peut être utilisée. Pour les versions antérieures à la version 9.6.2, reportez-vous à l'annexe A

> **Note:** Sur les versions 9.6.2 et ultérieures, nous avons pris en charge Flash Virtualization, ce qui signifie que nous pouvons avoir une image Anyconnect par contexte.

Virtualisation Flash

Le VPN d'accès à distance nécessite un stockage flash pour diverses configurations et images telles que les packages AnyConnect, les packages de balayage d'hôte, la configuration DAP, les modules externes, la personnalisation et la localisation, etc. En mode multicontexte avant la version 9.6.2, les contextes utilisateur ne peuvent accéder à aucune partie de la mémoire Flash et la mémoire flash est gérée et accessible à l'administrateur système uniquement via le contexte système.

Afin de résoudre cette limitation, tout en conservant la sécurité et la confidentialité des fichiers sur la mémoire Flash et en étant en mesure de partager la mémoire Flash équitablement entre les contextes, un système de fichiers virtuel est créé pour la mémoire Flash en mode multicontexte. L'objectif de cette fonctionnalité est de permettre la configuration des images AnyConnect en fonction du contexte plutôt que de les configurer globalement. Cela permet à différents utilisateurs d'avoir différentes images AnyConnect installées. En outre, en permettant le partage d'images AnyConnect, la quantité de mémoire consommée par ces images peut être réduite. Le stockage partagé est utilisé pour stocker des fichiers et des packages communs à tous les contextes.

> **Note:** L'administrateur du contexte système continuera à disposer d'un accès en lecture-écriture complet à l'intégralité du flash et aux systèmes de fichiers de stockage privé et partagé.L'administrateur système devra créer une structure de répertoire et organiser tous

les fichiers privés et partagés dans différents répertoires afin que ces répertoires puissent être configurés pour que les contextes d'accès soient partagés comme stockage et stockage privé respectivement.

Chaque contexte dispose d'autorisations de lecture/écriture/suppression sur son propre stockage privé et d'un accès en lecture seule à son stockage partagé. Seul le contexte système aura un accès en écriture au stockage partagé.

Dans les configurations ci-dessous, le contexte personnalisé 1 sera configuré pour illustrer le stockage privé et le contexte personnalisé 2 pour illustrer le stockage partagé.

Stockage privé

Vous pouvez spécifier un espace de stockage privé par contexte. Vous pouvez lire/écrire/supprimer de ce répertoire dans le contexte (ainsi que depuis l'espace d'exécution du système). Sous le chemin spécifié, l'ASA crée un sous-répertoire nommé en fonction du contexte.

Par exemple, pour context1 si vous spécifiez disk0:/private-storage pour le chemin d'accès, l'ASA crée un sous-répertoire pour ce contexte à disk0:/private-storage/context1/.

Stockage partagé

Un espace de stockage partagé en lecture seule peut être spécifié par contexte. Pour réduire la duplication des fichiers volumineux communs qui peuvent être partagés entre tous les contextes (tels que les packages AnyConnect), il est possible d'utiliser un espace de stockage partagé.

Configurations pour utiliser l'espace de stockage privé

```
!! Create a directory in the system context.
ciscoasa(config)# mkdir private_context1

!! Define the directory as private storage url in the respective context.

ciscoasa(config)# context context1 ciscoasa(config-ctx)# storage-url private
disk0:/private_context1 context1

!! Transfer the anyconnect image in the sub directory.
ciscoasa(config)# copy flash:/anyconnect-win-4.2.01035-k9.pkg flash:/private_context1/context1
```

Configurations pour utiliser l'espace de stockage partagé

```
!! Create a directory in the system context.

ciscoasa(config)# mkdir shared

!! Define the directory as shared storage url in the respective contexts.

ciscoasa(config)# context context2 ciscoasa(config-ctx)# storage-url shared disk0:/shared shared

!! Transfer the anyconnect image in the shared directory.
ciscoasa(config)# copy disk0:/anyconnect-win-4.3.05019-k9.pkg disk0:/shared
```

Vérifier l'image dans les contextes respectifs

```
!! Custom Context 1 configured for private storage.

ciscoasa(config)#changeto context context1
ciscoasa/context1(config)# show context1:
213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg

!! Custom Context 2 configured for shared storage.

ciscoasa(config)#changeto context context2
ciscoasa/context2(config)# show shared:
195 25356342 May 24 2017 08:07:02 shared:/anyconnect-win-4.3.05017-k9.pkg
```

Étape 6. Vous trouverez ci-dessous le résumé des configurations dans le contexte système qui inclut les configurations de virtualisation Flash décrites ci-dessus :

Contexte système

```
context context1
member resource01
allocate-interface GigabitEthernet0/0
 storage-url private disk0:/private_context1 context1
config-url disk0:/context1.cfg
join-failover-group 1
!
context context2
member resource02
allocate-interface GigabitEthernet0/1
storage-url shared disk0:/shared shared
config-url disk0:/context2.cfg
join-failover-group 2
```

Étape 7 : Configurez les deux contextes personnalisés comme indiqué ci-dessous

Contexte personnalisé 1

```
!! Enable WebVPN on respective interfaces

webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list 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 required connection profile for SSL VPN

access-list split standard permit 192.168.1.0 255.255.255.0

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
```

Contexte personnalisé 2

```
!! Enable WebVPN on respective interfaces

webvpn
enable outside
anyconnect image shared:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
tunnel-group-list 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 required connection profile for SSL VPN

access-list split standard permit 192.168.1.0 255.255.255.0

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
```

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vérifier si la licence Apex est installée

ASA ne reconnaît pas spécifiquement une licence AnyConnect Apex, mais applique les caractéristiques de licence d'une licence Apex qui incluent :

- AnyConnect Premium sous licence jusqu'à la limite de la plate-forme
- AnyConnect pour mobile
- AnyConnect pour téléphone VPN Cisco

- Évaluation avancée des terminaux

Un syslog est généré lorsqu'une connexion est bloquée, car aucune licence AnyConnect Apex n'est installée.

Vérifier si le package AnyConnect est disponible dans des contextes personnalisés (9.6.2 et versions ultérieures)

```
! AnyConnect package is available in context1

 ciscoasa/context1(config)# show context1:

213 19183882 Jun 12 2017 13:29:51 context1:/anyconnect-win-4.2.01035-k9.pkg

ciscoasa/pri/context1/act# show run webvpn
webvpn
enable outside
anyconnect image context1:/anyconnect-win-4.2.01035-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

Dans le cas où l'image n'est pas présente dans le contexte personnalisé, référez-vous à Configuration d'image Anyconnect (9.6.2 et plus).

Vérifier si les utilisateurs peuvent se connecter via AnyConnect dans des contextes personnalisés

> **Conseil :** Pour mieux afficher les vidéos ci-dessous en plein écran.

```
!! 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 : 0a6a2c24000010005660 60f8
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
```

Dépannage

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

Dépannage d'AnyConnect

> **Astuce :** Dans le cas où ASA n'a pas de licence Apex installée, la session AnyConnect se terminerait par syslog ci-dessous :
>
> %ASA-6-725002 : Connexion SSL du périphérique terminée avec le client OUTSIDE:10.142.168.86/51577 à 10.106.44.38/443 pour la session TLSv1
> %ASA-6-113012 : Authentification utilisateur AAA réussie : base de données locale : utilisateur = cisco
> %ASA-6-113009 : AAA a récupéré la stratégie de groupe par défaut (GroupPolicy_MC_RAVPN_1) pour l'utilisateur = cisco
> %ASA-6-113008 : ACCEPT de statut de transaction AAA : utilisateur = cisco
> %ASA-3-716057 : IP utilisateur du groupe <10.142.168.86> Session terminée, aucune licence AnyConnect Apex n'est disponible
> %ASA-4-113038 : Adresse IP de l'utilisateur du groupe <10.142.168.86> Impossible de créer la session parent AnyConnect.

Annexe A - Configuration d'image Anyconnect pour les versions antérieures à la version 9.6.2

L'image AnyConnect est configurée globalement dans le contexte d'administration pour les versions ASA antérieures à la version 9.6.2 (notez que la fonctionnalité est disponible à partir de la version 9.5.2), car le stockage Flash n'est pas virtualisé et n'est accessible que depuis le contexte système.

Étape 5.1. Copiez le fichier de package AnyConnect dans la mémoire Flash dans le contexte du système.

Contexte système :

```
ciscoasa(config)# show flash:

195 25356342 May 24 2017 08:07:02 anyconnect-win-4.3.05017-k9.pkg
```

Étape 5.2. Configurer l'image Anyconnect dans le contexte Admin.

Contexte Admin :

```
webvpn
anyconnect image disk0:/anyconnect-win-4.3.05017-k9.pkg 1
anyconnect enable
```

Note: L'image Anyconnect peut être configurée dans le contexte admin uniquement. Tous les contextes font automatiquement référence à cette configuration globale d'image Anyconnect.

Contexte personnalisé 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 personnalisé 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
```

Vérifier si le package AnyConnect est installé dans le contexte Admin et est disponible dans des contextes personnalisés (avant la version 9.6.2)

```
!! 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
```

Références

[notes de version: 9.5(2)]

[notes de version: 9.6(2)]

Informations connexes

- Dispositifs de sécurité adaptatifs de la gamme Cisco ASA 5500
- Guide de dépannage de client VPN AnyConnect – Problèmes fréquents
- Gestion, surveillance et dépannage des sessions AnyConnect
- Support et documentation techniques - Cisco Systems
- https://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asa_new_features.pdf