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

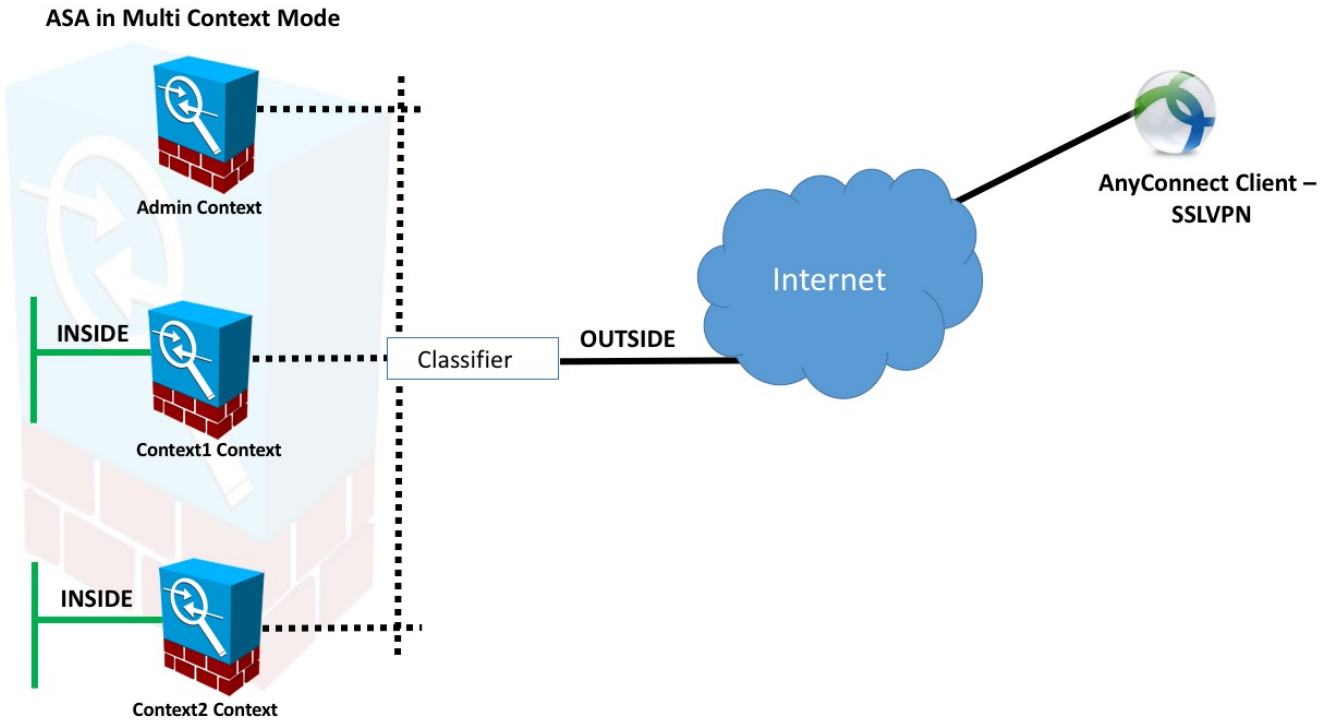
- Licence requise d'apex d'AnyConnect
- Les essentiel autorise ignoré/non laissé
- Configurabilité pour contrôler l'utilisation maximum de permis par contexte
- Configurabilité pour permettre le permis éclatant par contexte

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.

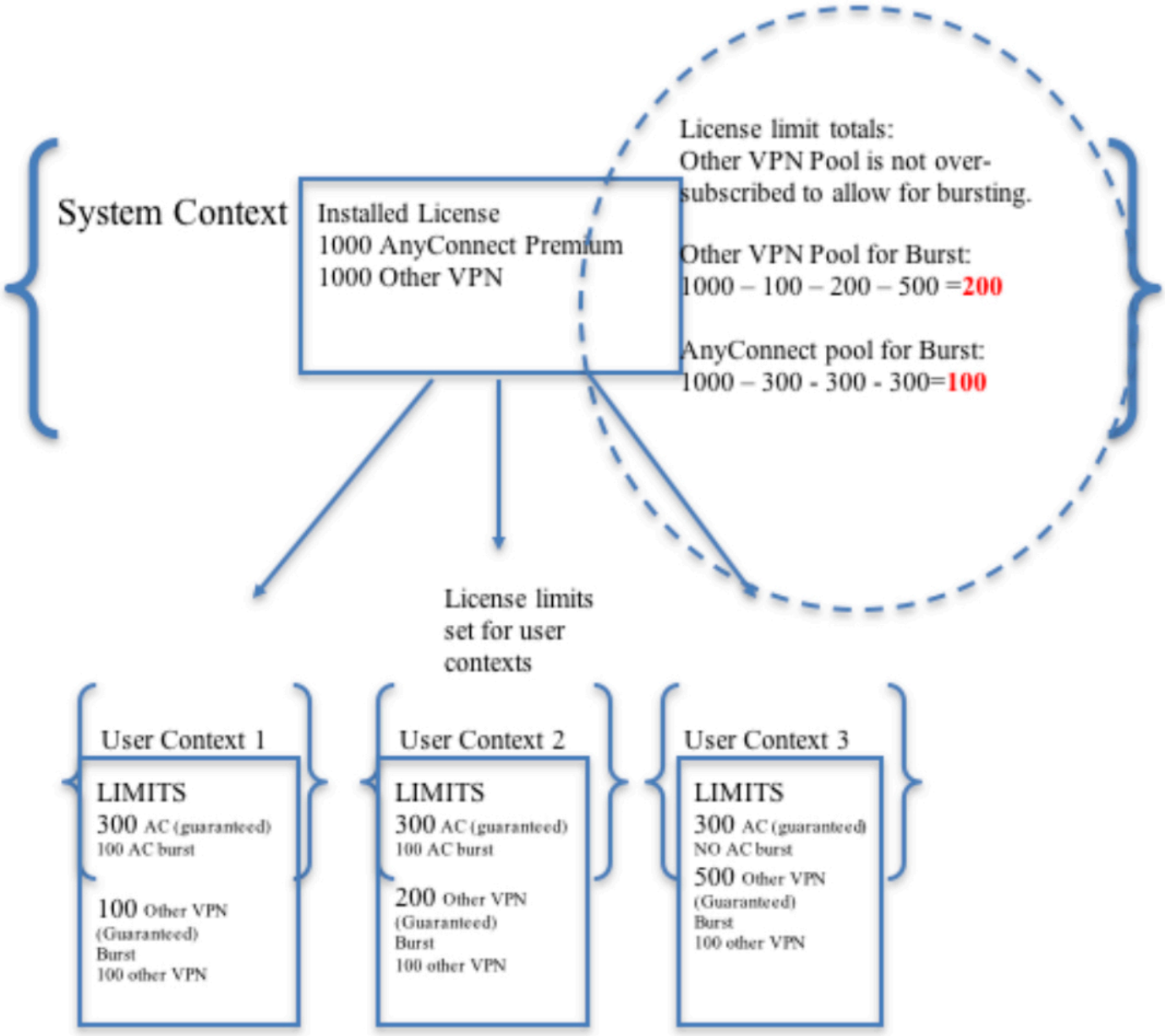
Étape 2. Allouez VPN Resouce.

Configuré par l'intermédiaire de la classe existante ? configuration. 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 pouvez ? t soit 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.

Étape 3. Configurez les contextes et assignez les ressources.

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

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.

Contexte fait sur commande 1

Contexte fait sur commande 2

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

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.

Dépannez

Dépannez l'AnyConnect Cet exemple de débogage montre que le permis d'apex est 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