Contenu

Introduction

Ce document décrit comment exécuter l'installation initiale et la configuration d'un périphérique 5506W-X de l'appliance de sécurité adaptable Cisco (ASA) quand le système d'adressage d'IP par défaut doit être modifié pour s'insérer dans un réseau existant ou si de plusieurs VLAN sans fil sont exigés. Il y a plusieurs modifications de configuration qui sont exigées en modifiant les adresses IP par défaut afin d'accéder au point d'accès sans fil (WAP) aussi bien que s'assurer que d'autres services (tels que le DHCP) continuent à fonctionner comme prévu. En outre, ce document fournit quelques exemples de configuration CLI pour le point d'accès sans fil intégré

(WAP) pour le faciliter pour se terminer la configuration initiale du WAP. Ce document est destiné pour compléter le guide de démarrage rapide existant de Cisco ASA 5506-X disponible sur le site Web Cisco.

Conditions préalables

Ce document s'applique seulement à la configuration initiale d'un périphérique de Cisco ASA5506W-X qui contient un point d'accès sans fil et est seulement destiné pour adresser les diverses modifications requises quand vous modifiez le schéma existant d'adressage IP ou ajoute des VLAN sans fil supplémentaires. Pour des installations de configuration par défaut, le guide de démarrage rapide existant ASA 5506-X doit être mis en référence.

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Périphérique de Cisco ASA 5506W-X
- Machine cliente avec un programme d'émulation de terminal tel que le mastic, le SecureCRT, etc.
- Câble de console et adaptateur de terminal séquentiel PC (DB-9 au RJ-45)

Composants utilisés

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

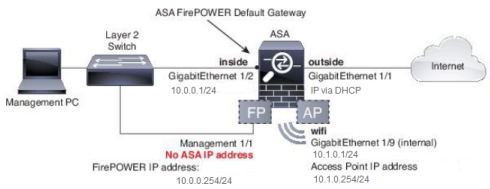
- Périphérique de Cisco ASA 5506W-X
- Machine cliente avec un programme d'émulation de terminal tel que le mastic, le SecureCRT, etc.
- Câble de console et adaptateur de terminal séquentiel PC (DB-9 au RJ-45)
- Module de puissance de feu ASA
- Point d'accès sans fil intégré de Cisco Aironet 702i (WAP intégré)

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.

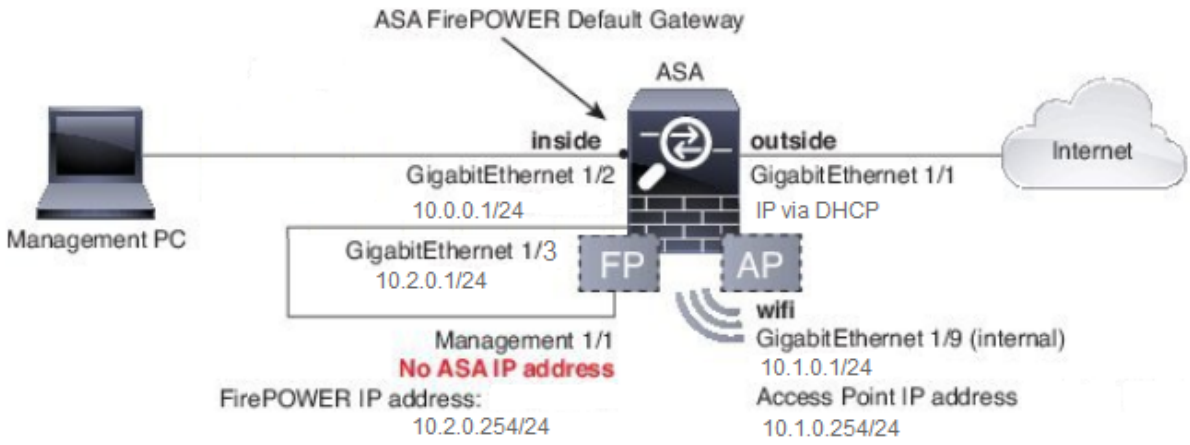
Diagrammes du réseau

Suivant les indications de cette image, exemples de l'adressage IP qui sera appliqué dans deux topologies différentes :

ASA + puissance de feu avec un commutateur intérieur :



ASA + puissance de feu sans commutateur intérieur :



Configurez

Ces étapes doivent être exécutées dans la commande après que vous mettiez sous tension et démarriez l'ASA avec le câble connecté de console au client.

Étape 1. Modifiez la configuration IP d'interface sur l'ASA

Configurez l'intérieur (GigabitEthernet 1/2) et les interfaces de wifi (GigabitEthernet 1/9) pour avoir des adresses IP comme nécessaire dans l'environnement existant. Dans cet exemple, les clients intérieurs sont sur les 10.0.0.1/24 réseaux et les clients de Wifi sont sur le réseau 10.1.0.1/24.

> Remarque: Vous obtiendrez cet avertissement quand vous changez les adresses IP ci-dessus d'interface. Ceci est prévu.

Étape 2. Modifiez les configurations de pool DHCP sur chacun des deux intérieurs et des interfaces de wifi

Cette étape est exigée si l'ASA doit être utilisée comme serveur DHCP dans l'environnement. Si un autre serveur DHCP est utilisé pour assigner des adresses IP aux clients puis le DHCP devrait être désactivé sur l'ASA totalement. Puisque vous avez maintenant changé notre schéma d'adressage IP, vous devez modifier les plages d'adresses IP existantes que l'ASA fournit aux clients. Ces commandes créeront de nouveaux groupes pour apparier la nouvelle plage d'adresses IP :

Également la modification des pools DHCP désactivera le serveur DHCP précédent sur l'ASA, et vous devrez la réactiver.

Si vous ne changez pas les adresses IP d'interface avant d'apporter les modifications DHCP puis vous recevrez cette erreur :

Étape 3. Spécifiez le serveur DNS pour passer aux clients DHCP intérieurs et de

WiFi

Quand ils assignent des adresses IP par l'intermédiaire du DHCP, la plupart des clients doivent également être assignés un serveur DNS par le serveur DHCP. Ces commandes configureront l'ASA pour inclure le serveur DNS situé à 10.0.0.250 à tous les clients. Vous devez substituer 10.0.0.250 à un serveur DNS interne ou à un serveur DNS fourni par votre ISP.

Étape 4. Modifiez la configuration d'accès HTTP sur l'ASA pour l'accès d'Adaptive Security Device Manager (ASDM) :

Puisque l'adressage IP a été changé, accès HTTP ASA aux besoins également d'être modifié de sorte que les clients sur les réseaux intérieurs et de WiFi puissent accéder à l'ASDM pour gérer l'ASA.

> Remarque: Cette configuration permet à n'importe quel client sur les interfaces intérieures ou de wifi pour accéder à l'ASA par l'intermédiaire de l'ASDM. Comme pratique recommandée de Sécurité, vous devez limiter la portée des adresses aux clients de confiance seulement.

Étape 5. Modifiez l'IP d'interface pour la Gestion de Point d'accès dans la console WLAN (interface BVI1) :

Étape 6. Modifiez la passerelle par défaut sur le WAP

Cette étape est exigée de sorte que le WAP sache où envoyer tout le trafic qui n'est pas lancé sur le sous-réseau local. Ceci est exigé pour fournir pour accéder au GUI WAP par l'intermédiaire du HTTP d'un client sur l'interface interne ASA.

Étape 7. Modifiez l'adresse IP de Gestion de module de puissance de feu (facultative)

Si vous prévoyez également de déployer le module de puissance de feu de Cisco (également connue sous le nom de SFR) puis vous devez également changer son adresse IP afin de l'accéder à de l'interface Management1/1 physique sur l'ASA. Il y a deux scénarios de base de déploiement qui déterminent comment configurer l'ASA et le module SFR :

1. Une topologie dans laquelle l'interface ASA Management1/1 est connectée à un commutateur intérieur (selon le guide de démarrage rapide normal)
2. Une topologie où un commutateur intérieur n'est pas présent.

Selon votre scénario, ce sont les étapes appropriées :

Si l'interface ASA Management1/1 est connectée à un intérieur commutez :

Vous pouvez session dans le module et le changer de l'ASA avant de la connecter à un

commutateur intérieur. Cette configuration te permet pour accéder au module SFR par l'intermédiaire de l'IP en le plaçant sur le même sous-réseau que l'interface interne ASA avec une adresse IP de 10.0.0.254.

Les lignes en gras sont spécifiques à cet exemple et sont exigées pour établir la connectivité IP.

Les lignes en italique varieront par l'environnement.

> Remarque: Il peut prendre des minutes d'un couple pour que la stratégie par défaut de contrôle d'accès s'applique sur le module SFR. Une fois qu'il est complet, vous pouvez s'échapper hors du module CLI SFR et de nouveau dans l'ASA en appuyant sur CTRL + SHIFT + 6 +X (^ CTRL X)

Si l'ASA n'est pas connectée à un intérieur commutez :

Un commutateur intérieur peut ne pas exister dans quelques petits déploiements. Dans ce type de topologie, les clients se connecteraient généralement à l'ASA par l'intermédiaire de l'interface de WiFi. Dans ce scénario, il est possible éliminent le besoin de commutateur externe et accèdent au module SFR par l'intermédiaire d'une interface distincte ASA croix-en connectant l'interface Management1/1 à une autre interface physique ASA.

Dans cet exemple, une connexion physique d'Ethernets doit exister entre l'interface ASA GigabitEthernet1/3 et l'interface Management1/1. Ensuite, vous configurez le module ASA et SFR pour être sur un sous-réseau distinct et alors vous pouvez accéder au SFR de l'ASA aussi bien que des clients situés sur les interfaces intérieures ou de wifi.

Configuration d'interface ASA :

Configuration de module SFR :

> Remarque: Il peut prendre des minutes d'un couple pour que la stratégie par défaut de contrôle d'accès s'applique sur le module SFR. Une fois qu'il est complet, vous pouvez s'échapper hors du module CLI SFR et de nouveau dans l'ASA en appuyant sur CTRL + SHIFT + 6 +X (^ CTRL X).

Une fois que la configuration SFR s'applique, vous devez pouvoir cingler l'adresse IP de Gestion SFR de l'ASA :

Si vous ne pouvez pas cingler l'interface avec succès, vérifiez la configuration et l'état de connexions physiques d'Ethernets.

Étape 8. Connectez au GUI AP pour activer des radios et pour placer l'autre configuration WAP

En ce moment vous devriez avoir la Connectivité pour gérer le WAP par l'intermédiaire du GUI de HTTP comme évoqué dans le guide de démarrage rapide. Vous l'un ou l'autre de besoin de parcourir à l'adresse IP de l'interface BVI du WAP d'un navigateur Web d'un client qui est connecté au réseau intérieur sur le 5506W ou vous pouvez appliquer l'exemple de configuration et se connecter au SSID du WAP. Si vous n'utilisez pas le CLI ci-dessous, vous devez brancher le câble d'Ethernets de votre client à l'interface Gigabit1/2 sur l'ASA.

Si vous préférez employer le CLI pour configurer le WAP, vous pouvez session dans elle de l'ASA et utiliser cet exemple de configuration. Ceci crée un SSID ouvert avec le nom de 5506W et de 5506W_5Ghz de sorte que vous puissiez utiliser un client sans fil pour se connecter à et pour gérer plus loin le WAP.

> Remarque: Après application de cette configuration vous voudrez accéder au GUI et s'appliquer la Sécurité au SSID de sorte que le trafic Sans fil soit chiffré.

La configuration WAP CLI pour un VLAN sans fil simple utilisant l'IP modifié s'étend

Àpartir de là, vous pouvez exécuter les étapes normales pour se terminer la configuration du WAP et vous devez pouvoir l'accéder à du navigateur Web d'un client connecté au SSID ci-dessus créé. Le nom d'utilisateur par défaut du Point d'accès est Cisco avec un mot de passe de Cisco avec un C capital.

Guide de démarrage rapide de gamme 5506-X de Cisco ASA

http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/5506X/5506x-quick-start.html#pgfId-138410

Vous devez utiliser l'adresse IP de 10.1.0.254 au lieu de 192.168.10.2 comme stipulé dans le guide de démarrage rapide.

Configurations

La configuration en résultant doit apparier la sortie (vous assumant a utilisé les plages, autrement la substitution IP d'exemple en conséquence :

Configuration ASA

Interfaces :

> Remarque: Les lignes en italique s'appliquent seulement si vous n'avez pas un commutateur intérieur :

DHCP :

HTTP :

Configuration de l'Aironet WAP (sans config d'exemple SSID)

Configuration de module de puissance de feu (avec le commutateur intérieur)

Configuration de module de puissance de feu (sans commutateur intérieur)

Vérifiez

Afin de vérifier que vous avez la Connectivité appropriée au WAP pour se terminer le processus d'installation :

1. Connectez votre client de test à l'interface interne ASA et assurez-vous qu'elle reçoit une adresse IP de l'ASA par l'intermédiaire du DHCP qui est dans la marge désirée IP.
2. Utilisez un navigateur Web sur votre client afin de naviguer vers https://10.1.0.254 et vérifier que le GUI AP est maintenant accessible.
3. Cinglez l'interface de gestion SFR du client intérieur et de l'ASA pour vérifier la Connectivité appropriée.

Configurez le DHCP avec de plusieurs VLAN sans fil

La configuration suppose que vous utilisez un VLAN sans fil simple. L'interface virtuelle de passerelle (BVI) sur le point d'accès sans fil peut fournir une passerelle pour le multiple VLAN. En raison de la syntaxe pour le DHCP sur l'ASA, si vous souhaitez configurer le 5506W comme serveur DHCP pour des VLAN multiples, vous devez créer des sous-interfaces sur l'interface Gigabit1/9 et donner chaque un nom. Cette section vous guide par le processus de la façon retirer la configuration par défaut et appliquer la configuration nécessaire pour établir l'ASA comme serveur DHCP pour des VLAN multiples.

Étape 1. Retirez la configuration existante DHCP sur Gig1/9

D'abord, retirez la configuration existante DHCP sur l'interface Gig1/9 (wifi) :

Étape 2. Créez les sous-interfaces pour chaque VLAN sur Gig1/9

Pour chaque VLAN que vous avez configuré sur le Point d'accès, vous devez configurer une sous-interface de Gig1/9. En cet exemple de configuration, vous ajoutez deux sous-interfaces :

-Gig1/9.5, qui aura le nameif vlan5, et correspondra à VLAN 5 et à sous-réseau 10.5.0.0/24.

-Gig1/9.30, qui aura le nameif vlan30, et correspondra à VLAN 30 et à sous-réseau 10.3.0.0/24.

Dans la pratique, il est essentiel que le VLAN et le sous-réseau configurés ici apparient le VLAN et le sous-réseau spécifiés sur le Point d'accès. Le nameif et le numéro de sous-interface peuvent être quelque chose que vous choisissez. Veuillez se référer au guide de démarrage rapide précédemment mentionné pour des liens afin de configurer le Point d'accès utilisant le GUI de Web.

Étape 3. Indiquez un pool DHCP pour chaque VLAN

Créez un pool DHCP distinct pour chaque VLAN étant configuré. La syntaxe pour cette commande exige que vous répertoriez le nameif hors dont l'ASA servira le groupe en question. Vu dans cet exemple, qui utilise VLAN 5 et 30 :

Étape 4. Configurez le Point d'accès SSID, sauvegardez le config, et remettez à l'état initial le module

En conclusion, le Point d'accès doit être configuré pour correspondre à la configuration de l'ASA. L'interface gui pour le Point d'accès te permet pour configurer des VLAN sur AP par l'intermédiaire

du client connecté à l'ASA à l'intérieur de l'interface (Gigabit1/2). Cependant, si vous préférez employer le CLI pour configurer AP par l'intermédiaire de la session de console ASA et puis pour se connecter sans fil pour gérer AP, vous pouvez utiliser cette configuration comme modèle pour créer deux SSID sur VLAN 5 et 30. Ceci doit être entré dans la console AP en mode de configuration globale :

En ce moment, la configuration de gestion de l'ASA et AP doivent être complets, et l'ASA agit en tant que serveur DHCP pour VLAN 5 et 30. Après avoir enregistré la configuration utilisant la ***write memory*** *commandez sur AP, si vous avez toujours des problèmes de connectivité alors que vous devez recharger AP utilisant la commande de* ***recharge du*** *CLI. Cependant, si vous recevez une adresse IP sur le SSID de création récente puis aucune action supplémentaire n'est exigée.*

> Remarque: Vous n'avez pas besoin de recharger le périphérique entier ASA. Vous devez seulement recharger le Point d'accès intégré.

Une fois qu'AP finit le rechargement, puis vous devez avoir la Connectivité au GUI AP d'une machine cliente sur les réseaux de wifi ou d'intérieur. Cela prend généralement environ deux minutes pour qu'AP redémarre complètement. À partir de là, vous pouvez appliquer les étapes normales pour se terminer la configuration du WAP.

Guide de démarrage rapide de gamme 5506-X de Cisco ASA

http://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/5506X/5506x-quick-start.html#pgfId-138410

Dépannez

Le dépannage de la Connectivité ASA est hors de portée de ce document puisque ceci est destiné pour la configuration initiale. Veuillez se référer aux sections de vérifier et de configuration pour s'assurer que toutes les étapes ont été correctement terminées.