Commande cable source-verify et sécurité d'adresse IP

Contenu

Introduction

Cisco a mis en application des améliorations dans les Produits du système d'arrêt de modem câble Cisco (CMTS) qui empêchent certains types d'attaques par déni de service basées sur la mystification d'adresse IP et le vol d'adresse IP dans des systèmes de câble de Data-over-Cable Service Interface Specifications (DOCSIS). Ce document décrit la suite de **cable source-verify des** commandes qui font partie de ces améliorations de la sécurité d'adresse IP.

Avant de commencer

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Conditions préalables

Aucune condition préalable spécifique n'est requise pour ce document.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

L'environnement non protégé DOCSIS

Un domaine de Contrôle d'accès au support (MAC) DOCSIS est semblable en nature à un segment d'Ethernets. Si gauche non protégé, les utilisateurs dans le segment sont vulnérables à beaucoup de types d'attaques par déni de service basées de adressage de la couche 2 et de la couche 3. En outre, il est possible que les utilisateurs souffrent un niveau dégradé de service dû au malconfiguration de l'adressage sur le matériel de l'autre utilisateur. Les exemples de ceci ont pu inclure :

- Configurer les adresses IP en double sur différents Noeuds.
- Configurer les adresses MAC en double sur différents Noeuds.
- L'utilisation non autorisée des adresses IP statiques plutôt que les adresses IP assignées du protocole DHCP (DHCP).
- L'utilisation non autorisée de différents network number dans un segment.
- Configurer inexactement des Noeuds d'extrémité pour répondre à des demandes d'ARP au nom d'une partie de l'IP de sous-réseau de segment.

Tandis qu'il est facile contrôler et atténuer ces types de problèmes dans un environnement de LAN Ethernet en dépistant physiquement et en déconnectant le matériel offensant, de tels problèmes dans des réseaux DOCSIS peuvent être plus durs pour isoler, résoudre, et empêcher en raison potentiellement du de grande taille du réseau. En outre, les utilisateurs finaux qui contrôlent et configurent l'équipement client (CPE) peuvent ne pas avoir l'avantage des gens du pays EST équipe d'assistance pour s'assurer que leurs postes de travail et PC pas malconfigured intentionnellement ou involontairement.

La base de données CPE CMTS

La suite de Cisco des Produits CMTS met à jour une base de données interne dynamiquement remplie d'IP CPE et d'adresses MAC connectés. La base de données CPE contient également des détails sur les Modems câble correspondants que ces périphériques CPE appartiennent à.

Une vue partielle de la base de données CPE correspondant à un modem câble particulier peut être visualisée en exécutant le **modem** masqué **Z. du show interface cable X/Y de** commande CMTS. Ici, X est le nombre de linecard, Y est le numéro de port en aval et Z est l'indentifiant de service (SID) du modem câble. Z peut être placé à 0 pour visualiser des détails au sujet de tous les Modems câble et le CPE sur une interface en aval particulière. Voir l'exemple ci-dessous d'un résultat généré typique par cette commande.

```
CMTS# show interface cable 3/0 modem 0
SID   Priv bits  Type      State     IP address    method    MAC address
1     00         host      unknown   192.168.1.77  static    000C.422c.54d0 1     00
modem     up         10.1.1.30     dhcp      0001.9659.4447 2     00         host      unknown
192.168.1.90  dhcp      00a1.52c9.75ad 2     00         modem     up         10.1.1.44
dhcp      0090.9607.3831
```

Remarque: Puisque cette commande est masquée, elle est sujette à la modification et n'est pas garantie d'être disponible dans des toutes les releases de logiciel de Cisco IOS®.

Dans l'exemple ci-dessus, la colonne de méthode de l'hôte avec l'adresse IP 192.168.1.90 est

répertoriée comme DHCP. Ceci signifie que le CMTS s'est renseigné sur cet hôte en observant les transactions DHCP le serveur DHCP entre l'hôte et du fournisseur de services.

L'hôte avec l'adresse IP 192.168.1.77 est répertorié avec la charge statique de méthode. Ceci signifie que le CMTS n'a pas appris la première fois de cet hôte par l'intermédiaire d'une transaction DHCP entre ce périphérique et un serveur DHCP. Au lieu de cela le CMTS a vu la première fois d'autres genres de trafic IP de cet hôte. Ce trafic pourrait avoir été paquets de navigation web, d'email ou des de « ping ».

Tandis qu'il peut sembler que 192.168.1.77 a été configuré avec une adresse IP statique, il se peut que cet hôte ait en fait saisi un bail DHCP, mais le CMTS a pu avoir été redémarré puisque l'événement et donc il ne se souvient pas la transaction.

La base de données CPE est normalement remplie par les informations glanantes CMTS des transactions DHCP entre les périphériques CPE et le serveur DHCP du fournisseur de services. En outre, le CMTS peut écouter l'autre trafic IP provenant des périphériques CPE pour déterminer quels IP CPE et adresses MAC appartiennent à quels Modems câble.

La commande de cable source-verify

Cisco a mis en application la commande d'interface de câble cable source-verify [DHCP]. Cette commande fait servir le CMTS de la base de données CPE pour vérifier la validité des paquets IP que le CMTS reçoit sur ses interfaces de câble et permet au CMTS pour prendre des décisions intelligentes au sujet de si les expédier ou pas.

L'organigramme ci-dessous affiche que les figurants traitant un paquet IP reçu sur une interface de câble doivent intervenir avant d'être laissé à poursuivre par le CMTS.

Organigramme 1

Les débuts d'organigramme avec un paquet reçu par un port ascendant sur le CMTS et des extrémités avec le paquet étant laissé continuer en fonction pour une transformation plus ultérieure ou dans le paquet étant relâché.

Exemple 1 - Scénario avec les adresses IP en double

Le premier scénario de Déni de service que nous adresserons est la situation impliquant les adresses IP en double. Disons que le client A est connecté à son fournisseur de services et a obtenu un bail valide DHCP pour son PC. Le client d'adresse IP qu'A a obtenu sera connu comme X.

Un jour ou l'autre après qu'A saisisse son bail DHCP, le client B décide de configurer son PC avec une adresse IP statique qui s'avère justement être identiques que qu'actuellement étant utilisé par le matériel du client A. Les informations de base de données CPE en vue de l'adresse IP X changeraient selon quel périphérique CPE a pour la dernière fois envoyé une demande d'ARP au nom du X.

Dans un réseau non protégé DOCSIS, le client que B pourrait pouvoir convaincre le routeur du prochain saut (dans la plupart des cas, le CMTS) ce il a le droit d'utiliser l'adresse IP X en envoyant simplement une demande d'ARP au nom de X au CMTS ou au routeur du prochain saut. Ceci arrêterait le trafic du fournisseur de services de l'transmission au client R.

Par l'activation cable source-verify, le CMTS pourrait voir que les paquets IP et d'ARP pour l'adresse IP X étaient originaires du modem câble faux et par conséquent, ces paquets serait relâché, voit l'organigramme 2. Ceci inclut tous les paquets IP avec l'adresse source X et les demandes d'ARP au nom du X. Les logs CMTS afficheraient un message le long des lignes de :

%UBR7200-3-BADIPSOURCE : Interface Cable3/0, paquet IP de source non valide. IP=192.168.1.10, MAC=0001.422c.54d0, SID=10 prévu, effectif SID=11

Organigramme 2

Utilisant ces informations, les deux clients seraient identifiés et le modem câble avec l'adresse IP en double connectée peut être désactivé.

Exemple 2 - Scénario avec les adresses IP en double - Utilisant une adresse IP qui n'est pas encore utilisée

Un autre scénario est pour qu'un utilisateur assigne statiquement jusqu'à présent une adresse IP inutilisée à leur PC qui fait partie de la marge légitime des adresses CPE. Ce scénario n'entraîne aucune interruption des services à n'importe qui dans le réseau. Disons que le client B a l'adresse attribuée Y pour leur PC.

Le prochain problème qui peut surgir est ce client que le C pourrait connecter son poste de travail au fournisseur de services et saisit un bail DHCP pour l'adresse IP Y. La base de données CPE marquerait temporairement l'adresse IP Y comme appartenant derrière le modem câble du client c. Cependant, il ne pourrait pas être longtemps avant le client B, l'utilisateur non-légitime envoie l'ordre approprié du trafic ARP pour convaincre le prochain-saut qu'il était le propriétaire légitime de l'adresse IP Y, par conséquent entraînant une interruption au service du client c.

De même, le deuxième problème peut être résolu en s'activant **cable source-verify**. Quand **cable source-verify** est activé, une entrée de base de données CPE qui a été générée en glanant des détails d'une transaction DHCP ne peut pas être déplacée par d'autres genres de trafic IP. Seulement une autre transaction DHCP pour cette adresse IP ou l'entrée d'ARP sur le CMTS chronométrant pour cette adresse IP peut déplacer l'entrée. Ceci s'assure que si un utilisateur final saisit avec succès un bail DHCP pour une adresse IP donnée, ce client ne devra pas s'inquiéter du CMTS devenant confus et pensant que son adresse IP appartient à un autre utilisateur.

Le premier problème d'arrêter des utilisateurs d'utiliser jusqu'à présent les adresses IP inutilisées peut être résolu avec **cable source-verify le DHCP**. En ajoutant le paramètre DHCP à la fin de cette commande, le CMTS peut vérifier la validité de chaque nouvelle adresse IP source qu'elle entend environ en émettant un type particulier de message DHCP appelé un LEASEQUERY au serveur DHCP. Voir l'organigramme 3.

Organigramme 3

Pour une adresse IP donnée CPE, le message LEASEQUERY demande ce que sont l'adresse MAC et le modem câble correspondants. Voir le message DHCPLEASEQUERY pour plus de détails.

Dans cette situation, si le client B connecte son poste de travail au réseau câblé à l'adresse statique Y, le CMTS enverra un LEASEQUERY au serveur DHCP pour vérifier si l'adresse Y a été louée au PC du client b. Le serveur DHCP peut informer le CMTS qu'aucun bail n'a été accordé

pour l'adresse IP Y et par conséquent le client B sera refusé l'accès.

Exemple 3 - Utilisation d'un network number provisioned par le fournisseur de services

Les utilisateurs peuvent avoir des postes de travail configurés derrière leurs Modems câble avec les adresses IP statiques qui ne peuvent pas être en conflit avec les network number en cours du fournisseur de services l'un des, mais qui peut poser des problèmes à l'avenir. Par conséquent, utilisant cable source-verify, un CMTS peut filtrer des paquets provenant les adresses IP de source qui ne sont pas de la plage configurée sur l'interface de câble du CMTS.

Remarque: Pour que ceci fonctionne correctement, vous devez également configurer la commande d'**ip verify unicast reverse-path** afin d'empêcher des adresses charriées de source IP. Référez-vous aux commandes de câble : pour en savoir plus du câble s.

Quelques clients peuvent avoir un routeur comme périphérique CPE et se charger pour que le fournisseur de services conduise le trafic à ce routeur. Si le CMTS reçoit le trafic IP du routeur CPE avec une adresse IP source de Z, alors cable source-verify permettrez ce paquet si le CMTS a une artère au réseau Z appartient à par l'intermédiaire de ce périphérique CPE. Référez-vous à l'organigramme 3.

Considérez maintenant l'exemple suivant :

Sur le CMTS nous avons le config suivant :

```
interface cable 3/0
 ip verify unicast reverse-path
 ip address 10.1.1.1 255.255.255.0
 ip address 24.1.1.1 255.255.255.0 secondary
 cable source-verify
!
ip route 24.2.2.0 255.255.255.0 24.1.1.2
```

Note: This configuration shows only what is relevant for this example

Supposant qu'un paquet avec l'adresse IP source 172.16.1.10 est arrivé au CMTS du modem câble 24.2.2.10, le CMTS verrait que 24.2.2.10 ne réside pas dans la base de données CPE, **affiche le modem 0 du câble x/y international**, toutefois l'**ip verify unicast reverse-path** active l'Unicast Reverse Path Forwarding (Unicast RPF), qui vérifie chaque paquet reçu sur une interface afin de vérifier que l'adresse IP source du paquet apparaît dans les tables de routage qui appartient à cette interface. **Le cable source-verify** vérifie pour voir ce qu'est le prochain saut pour 24.2.2.10. Dans la configuration ci-dessus nous avons l'**artère 24.2.2.0 255.255.255.0 24.1.1.2 d'IP** qui signifie que le prochain saut est 24.1.1.2. Assumer maintenant 24.1.1.2 est une entrée valide dans la base de données CPE alors que le CMTS conclut que le paquet est CORRECT et par conséquent traitera le paquet selon l'organigramme 4.

Organigramme 4

Comment configurer cable source-verify

Configurer **cable source-verify** implique simplement d'ajouter la commande de **cable source-verify à l'**interface de câble sur laquelle vous voudriez lancer la fonction. Si vous utilisez le Regroupement de câbles d'interface, alors vous devez ajouter **cable source-verify à la** configuration de l'interface principale.

Comment configurer `cable source-verify le DHCP`

Remarque: cable source-verify a été introduit dans le Logiciel Cisco IOS version 12.0(7)T et est pris en charge la première fois dans des versions du logiciel Cisco IOS 12.0SC, 12.1EC et 12.1T.

Configurer **cable source-verify le DHCP** exige quelques étapes.

Assurez-vous que votre serveur DHCP prend en charge le message DHCP LEASEQUERY d'offre spéciale.

Afin de se servir de la fonctionnalité **DHCP de cable source-verify**, votre serveur DHCP doit répondre aux messages comme spécifiés par draft-ietf-dhcp-leasequery-XX.txt. Les versions 3.5 et ultérieures de Cisco Network Registrar peuvent répondre à ce message.

Assurez-vous que votre serveur DHCP prend en charge le traitement d'option de relay agent information. Veuillez voir les ces instructions.

Une autre caractéristique qui doit être prise en charge par votre serveur DHCP est traitement de dhcp relay information option. Ceci est autrement connu comme option 82 traitant. Cette option est décrite dans le dhcp relay information option (RFC 3046). L'option de relay agent information de support de versions 3.5 et ultérieures de Cisco Network Registrar le traitant cependant doit être lancée par l'intermédiaire de la ligne de commande de Cisco Network Registrar nrcmd de service avec l'ordre suivant des commandes :

nrcmd - Admin U - Changeme P - Sauvegarde-relais-agent-données d'enable DHCP de 127.0.0.1 de C

nrcmd - Admin U - Changeme P - Sauvegarde de 127.0.0.1 de C

nrcmd - Admin U - Changeme P - Recharge DHCP de 127.0.0.1 de C

Vous pouvez devoir substituer le nom d'utilisateur, le mot de passe et l'adresse IP du serveur appropriés, les valeurs par défaut ci-dessus d'expositions. Alternativement, si vous êtes à la demande de nrcmd, >nrcmd vous tapez juste ce qui suit :

sauvegarde-relais-agent-données d'enable DHCP

sauvegardez

recharge DHCP

Activez le dhcp relay information option traitant sur le CMTS.

Agent de relais

Le CMTS doit étiqueter des requêtes DHCP des Modems câble et le CPE avec l'option de relay agent information afin du du **cable source-verify le DHCP** pour être efficace. Les commandes suivantes doivent être sélectionnées en mode de configuration globale sur les versions du logiciel Cisco IOS courantes CMTS 12.1EC, 12.1T ou versions ultérieures de Cisco IOS.

ip dhcp relay information option

Si votre CMTS s'exécute le Cisco IOS de série des versions du logiciel Cisco IOS 12.0SC alors utilise la commande d'interface de câble de **cable relay-agent-option** à la place.

Faites attention à utiliser les commandes appropriées, selon la version du Cisco IOS que vous exécutez. Veillez à mettre à jour votre configuration si vous changez de séries de Cisco IOS.

Les commandes de **relay information option** ajoutent une option achat 82 d'option spéciale, ou le relay information option, au paquet DHCP transmis par relais quand le CMTS transmet par relais des paquets DHCP.

L'option 82 est remplie avec une sous-option, le Circuit-ID d'agent, qui met en référence l'interface physique sur le CMTS que la requête DHCP a été entendue en fonction. En plus de ceci, une autre sous-option, l'ID distant d'agent, est remplie avec l'adresse MAC de 6 octets du modem câble que la requête DHCP a été reçue de ou est traversée.

Ainsi, par exemple, si un PC avec l'adresse MAC 99:88:77:66:55:44 qui est derrière le modem câble aa : bb : cc : densité double : l'EE : le FF envoie une requête DHCP, le CMTS expédiera la requête DHCP plaçant l'agent sous-option distante d'ID de l'option 82 à l'adresse MAC du modem câble, aa : bb : cc : densité double : l'EE : FF.

En ayant le relay information option inclus dans la requête DHCP d'un périphérique CPE, le serveur DHCP peut stocker les informations au sujet dont le CPE appartient derrière quels Modems câble. Ceci devient particulièrement utile quand **cable source-verify le DHCP** est configuré sur le CMTS, car le serveur DHCP peut informer sûrement le CMTS au sujet de non seulement quelle adresse MAC un client particulier devrait avoir, mais à quelle client particulier de modem câble est censé être connecté.

Activez la commande DHCP de cable source-verify sous l'interface de câble appropriée.

La dernière étape est de sélectionner la commande **DHCP de cable source-verify** sous l'interface de câble sur laquelle vous comme la caractéristique lancée. Si le CMTS utilise le Regroupement de câbles d'interface puis vous devez sélectionner la commande sous le paquet principal reliez.

Conclusion

Les suites de **cable source-verify des** commandes permettent à un fournisseur de services pour protéger le réseau câblé contre des utilisateurs avec les adresses IP non autorisées pour utiliser le réseau.

La commande de cable source-verify est par lui-même une efficace et une méthode facile d'implémenter la Sécurité d'adresse IP. Tandis qu'il ne couvre pas tous les scénarios, il au bail veille que les clients avec la droite de utiliser ont assigné des adresses IP, ne rencontrera aucune interruption en ayant leur adresse IP utilisé par quelqu'un d'autre.

Sous sa forme plus simple comme décrit dans ce document, un périphérique CPE non configuré par l'intermédiaire du DHCP ne peut pas obtenir l'accès au réseau. C'est la meilleure manière de sécuriser l'espace d'adresse IP et d'augmenter la stabilité et la fiabilité des données au-dessus de service par câble. Cependant les opérateurs de plusieurs services (MSO) qui ont les services commerciaux qui ont exigé de eux d'utiliser des adresses statiques ont voulu implémenter la Sécurité stricte du commandcable source-**vérifient le DHCP**.

La version 5.5 de Cisco Network Registrar a une nouvelle capacité de répondre à la requête de

bail pour des adresses « réservées », quoique l'IP address n'ait pas été obtenu par l'intermédiaire du DHCP. Le serveur DHCP inclut des données de réservation de bail dans les réponses DHCPLEASEQUERY. Dans les releases précédentes du Network Registrar, les réponses DHCPLEASEQUERY étaient possibles seulement aux clients loués ou précédemment loués pour lesquels l'adresse MAC a été enregistrée. Les agents de relais d'ubr de Cisco, par exemple, jettent des datagrammes DHCPLEASEQUERY n'ayant pas une adresse MAC et une durée de bail (option de DHCP-bail-temps).

Le Network Registrar renvoie une durée de bail par défaut d'un an (31536000 secondes) pour les baux réservés dans une réponse DHCPLEASEQUERY. Si l'adresse est louée réellement, le Network Registrar renvoie sa durée de bail restante. Plus de caractéristiques peuvent être trouvées à la section de question de baux de configurer des portées de DHCP et des baux.

Informations connexes

- Dhcp relay information option (RFC 3046)
- Support et documentation techniques - Cisco Systems