Sécurisation des contrôleurs de réseau local sans fil - Forum aux questions

Contenu

Introduction

Ce document offre un aperçu de plusieurs importants aspects requis pour manipuler l'interaction de Sécurité entre les contrôleurs LAN Sans fil (WLCs) et le réseau où ils sont connectés. Ce document se concentre principalement sur le contrôle de trafic, et n'adresse pas des stratégies de sécurité, l'AAA ou le WPS WLAN.

Des thèmes affectant le trafic avec la destination « au contrôleur » sont couverts dans ce document, et pas rapportés pour trafiquer qui est lié au « utilisateur au réseau ».

Remarque: Validez les modifications avant de les appliquer à votre réseau, comme certains des exemples dans ce document peuvent bloquer l'accès administratif à vos contrôleurs si appliqués inexactement.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance de la façon configurer le WLC et le point d'accès léger (LAP) pour le fonctionnement de base
- Connaissance de base du modèle OSI
- Comprenant comment la liste de contrôle d'accès (ACL) fonctionne

Composants utilisés

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

- Cisco 2000/2100/gamme 4400 WLC qui exécute des micrologiciels 4.2.130.0, 5.2.157.0 ou plus tard

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Écoulement de trafic dans WLCs

Un élément essentiel sur la sécurité des réseaux est contrôle de trafic. Sur n'importe quel déploiement, il est très important de bloquer des types de trafic arrivant aux périphériques afin d'empêcher les questions de sécurité potentielle (DOS, perte de l'information, transmission des problèmes de privilège, etc.).

Sur le WLC, le contrôle de trafic est affecté par un important fait : il y a deux composants traitant le trafic dans le périphérique :

- CPU — Processeur principal qui prend soin de toute l'activité de gestion, de contrôle RRM, LWAPP, d'authentification, de DHCP, etc.
- NPU — Processeur de réseau qui prend soin de l'expédition rapide du trafic pour les clients authentifiés (de câble à la radio et vice versa).

Cette architecture permet un expédition rapide du trafic, et réduit le chargement sur la CPU principale, qui peut alors dédier toutes ses ressources pour des tâches de haut niveau.

Cette architecture est trouvée sur les 4400, WiSM et 3750 contrôleurs intégrés. Pour 2106 et NM-WLC et contrôleurs relatifs, l'expédition est fait en logiciel, aussi par la CPU principale. Par conséquent, il prend une taxe plus élevée sur la CPU. C'est pourquoi ces Plateformes offrent un support inférieur d'utilisateur et de compte AP.

Le trafic de contrôle

Lorsque vous voulez filtrer le trafic par rapport à un WLC, il est important de savoir si c'est un utilisateur au trafic réseau ou il est vers la CPU principale.

- Pour n'importe quel trafic à la CPU, par exemple, les protocoles de gestion tels que le SNMP, le HTTPS, le SSH, le telnet, ou les protocoles de services réseau tels que le rayon ou le DHCP, utilisent un « ACL CPU ».
- Pour n'importe quel trafic à et d'un client sans fil, y compris le trafic allant par un tunnel d'EoIP (accès invité), un ACL d'interface, un ACL WLAN, ou a par ACL d'utilisateur est utilisé.

Le trafic est défini « à la CPU », comme trafic qui entre dans le contrôleur, avec la destination à l'adresse IP de Gestion, aux interfaces dynamiques l'unes des ou à l'adresse de port de service. L'AP-gestionnaire ne traite aucun autre trafic excepté LWAPP/CAPWAP.

Gestion de contrôle Access

WLCs ont un contrôle d'accès de niveau de « session » pour des protocoles de gestion. Il est important de comprendre comment ils fonctionnent afin d'empêcher l'estimation incorrecte sur ce qu'est autorisé ou pas autorisé par le contrôleur.

Les commandes de limiter quels protocoles de gestion sont permis sont (sur une portée globale) :

- **enable de config network ssh|débronchement** — Ceci active ou désactive le service de SSH sur le contrôleur. Ceci est activé par défaut. Une fois handicapé, le port (TCP 22) ne sera pas accessible.
- **enable de config network telnet|débronchement** — Ceci active ou désactive le service de telnet sur le contrôleur. Ceci est désactivé par défaut. Une fois handicapé, le port (TCP 23) ne sera pas accessible.
- **enable de HTTP de réseau de config|débronchement** — Ceci active ou désactive le service de HTTP sur le contrôleur. Le port (TCP 80) n'est pas plus long accessible. Ceci est désactivé par défaut.
- **enable de https de réseau de config|débronchement** — Ceci active ou désactive le service de https sur le contrôleur. Ceci est activé par défaut. Une fois handicapé, le port (TCP 443) ne sera pas accessible.
- **enable du config snmp version v1|v2|v3|débronchement** — Ceci active ou désactive des versions spécifiques de service SNMP sur le contrôleur. Vous devez désactiver tous pour empêcher l'accès SNMP au contrôleur, à moins qu'utilisant un ACL.
- **enable de config network mgmt-via-wireless|débronchement** — Ceci empêche que les clients associés à ce contrôleur peuvent accéder à des protocoles de gestion à lui (ssh, https, etc.). Ceci n'empêche pas ou ferme les ports correspondants de TCP du point de vue du périphérique sans fil. Ceci signifie qu'un périphérique sans fil, quand ceci est placé pour désactiver, peut ouvrir une connexion SSH, si le protocole est activé. L'utilisateur pourrait voir une invite de nom d'utilisateur générée par le démon de SSH, toutefois la session se ferme dès que vous tenterez de taper un nom d'utilisateur.
- **enable de gestion-par l'intermédiaire-dynamique-interface de réseau de config|débronchement** — Ceci empêche que les périphériques sur le même VLAN que le contrôleur peuvent accéder à des protocoles de gestion à lui (ssh, https, etc.) à l'adresse correspondante d'interface dynamique sur ce VLAN. Ceci n'empêche pas ou ferme les ports

correspondants de TCP du point de vue du périphérique. Ceci signifie qu'un périphérique, quand ceci est placé pour désactiver, peut ouvrir une connexion SSH, si le protocole est activé. L'utilisateur pourrait voir une invite de nom d'utilisateur générée par le démon de SSH, toutefois la session se ferme dès que vous tenterez de taper un nom d'utilisateur. Supplémentaire, l'adresse de gestion demeurera toujours accessible d'une interface dynamique VLAN, à moins qu'un ACL CPU soit sur l'endroit.

Par exemple, c'est la configuration utilisant les informations ci-dessus :

```
(Cisco Controller) >show network summary


RF-Network Name............................. 4400
Web Mode.................................... Disable
Secure Web Mode............................. Enable
Secure Web Mode Cipher-Option High.......... Disable
Secure Web Mode Cipher-Option SSLv2......... Enable
Secure Shell (ssh).......................... Enable
Telnet...................................... Disable
Ethernet Multicast Mode..................... Enable   Mode: Ucast
Ethernet Broadcast Mode..................... Disable
AP Multicast Mode........................... Unicast
IGMP snooping............................... Disabled
IGMP timeout................................ 60 seconds
User Idle Timeout........................... 300 seconds
ARP Idle Timeout............................ 300 seconds
Cisco AP Default Master..................... Disable
AP Join Priority............................ Disable
Mgmt Via Wireless Interface................. Disable
Mgmt Via Dynamic Interface.................. Disable
Bridge MAC filter Config.................... Enable
Bridge Security Mode........................ EAP
Mesh Full Sector DFS........................ Enable
Over The Air Provisioning of AP's........... Enable
Apple Talk ................................. Disable
AP Fallback ................................ Enable
Web Auth Redirect Ports .................... 80
Fast SSID Change ........................... Disabled
802.3 Bridging ............................. Disable
IP/MAC Addr Binding Check .................. Enabled


(Cisco Controller) >show acl cpu

CPU Acl Name................................ NOT CONFIGURED
Wireless Traffic............................ Disabled
Wired Traffic............................... Disabled
```

Vous pouvez conclure cela :

- Le telnet et le HTTP ne seront pas disponibles, ainsi tout le trafic d'administration interactif au contrôleur sera fait par HTTPS/SSH (chiffré).
- Un utilisateur de sans fil associé à ce contrôleur ne pourra pas obtenir l'accès administratif.
- Si un utilisateur de sans fil, associé à ce contrôleur, fait un balayage de port, il show ssh et HTTP comme ouvert, quoiqu'on ne permette aucun accès administratif.
- Si un utilisateur de câble (le même VLAN comme interface dynamique) fait un balayage de port, il show ssh et HTTP comme ouvert, quoiqu'on ne permette aucun accès administratif.

Il est important de noter que dans les environnements avec plus d'un contrôleur sur le même groupe de mobilité, les relations de ce qui est un client sans fil sont seulement au contrôleur

actuellement associé. Par conséquent, si un client est associé au contrôleur A, puis pour un contrôleur B sur le même groupe de mobilité, ce client est un périphérique provenant une interface VLAN/dynamic. Il est important prendre en considération ce sur la Gestion au-dessus du paramètre sans fil. Voir le ce diagramme pour un exemple d'où mettre une restriction du trafic, et quelles commandes peuvent concerner chaque point d'entrée :

CPU ACLs

Toutes les fois que vous voulez contrôler que les périphériques peuvent parler à la CPU principale, un ACL CPU est utilisé. Il est important de mentionner plusieurs caractéristiques pour ces derniers :

- Le trafic de filtre CPU ACLs seulement vers la CPU, et aucun trafic quittant ou généré par la CPU.**Remarque:** Pour la gamme 5500 WLC dans les versions 6.0 et ultérieures, l'ACL CPU s'applique pour le trafic provenu aussi bien du WLC. Pour les autres Plateformes WLC, ce comportement est mis en application dans les versions 7.0 et ultérieures. En outre, en créant des champs de direction CPU ACLs n'ayez aucune incidence.
- Le support complet pour CPU ACLs pour toutes les Gestion et adresses dynamiques IP de contrôleur est seulement présent sur 4.2.130.0 et plus tard.
- CPU ACLs bloquant le trafic de port de service est seulement dedans 5.0 actuels et plus tard.
- Quand un ACL CPU est conçu, il est important de permettre le trafic de contrôle entre les contrôleurs. La commande **SH de règles** peut offrir une vue rapide du trafic permise à l'ACL CPU sur des conditions normales.
- Le contrôleur a un ensemble de règles de filtrage pour les processus internes, qui peuvent être vérifiés avec la commande **SH de règles**. ACLs n'affectent pas ces règles, ni peuvent ces règles être à la volée modifié. L'ACL CPU a la priorité au-dessus de eux.
- Le trafic de données LWAPP ou CAPWAP n'est pas affecté par des règles CPU ACLs sur 4400 contrôleurs basés, le trafic de contrôle est affecté (si faisant un ACL strict, vous devez le permettre explicitement).**Remarque:** Le trafic de contrôle CAPWAP n'est pas affecté par CPU ACLs.

Exemple

Par exemple, vous pourriez vouloir bloquer tout le trafic provenant l'interface/VLAN dynamique (192.168.20.0/24) où des utilisateurs sont associés, vers la CPU, mais n'importe quel autre trafic est permis. Ceci ne devrait pas empêcher des clients sans fil pour obtenir une adresse négociée par DHCP.

1. Comme première étape, une liste d'accès est créée :
2. Cliquez sur Add la **nouvelle règle**, et placez-la pour bloquer tout le trafic source provenant 192.168.20.0/24 à n'importe quelle destination.
3. Ajoutez une deuxième règle, pour le trafic DHCP, avec le port de serveur cible, mais avec l'action d'autorisation :Puis, par stratégies de sécurité d'entreprise, on permet tout autre trafic :

Test avant ACL CPU

Afin de valider l'effet de l'ACL CPU, vous pouvez exécuter un balayage rapide d'un client sans fil

associé sur l'état de PASSAGE afin de voir les ports ouverts en cours, basés sur la configuration, avant d'appliquer l'ACL CPU :

Test après l'ACL CPU

Allez à la **Sécurité > à la Gestion > à la liste de contrôle d'accès CPU**. Cliquez sur l'**ACL CPU d'enable**, et sélectionnez l'ACL qui a été précédemment créé. Puis, choisissez **chacun des deux** comme la direction afin d'assurer ceci est appliquée pour trafiquer des clients sans fil, et d'autres périphériques sur l'interface dynamique VLAN :

Remarque: Il n'y a aucune direction pour le trafic d'acl CPU à compter de 7.0 pour toutes les Plateformes WLC et seulement pour WLC5500 dans 6.0.

Maintenant, si le même balayage utilisé avant est répété, tous les ports du contrôleur sont affichés comme fermés :

CPU stricte ACLs

Si la demande de stratégies de sécurité « refusent » en tant que pour la dernière fois en rayent pour une stratégie, il est important de comprendre qu'il y a plusieurs types de trafic envoyés entre le contrôleur sur le même groupe de mobilité pour RRM, la mobilité et d'autres tâches, et que vous pourriez faire proxied le trafic par le contrôleur à lui-même pour quelques exécutions, en particulier DHCP, où le contrôleur sur le mode proxy DHCP (le par défaut) peut générer le trafic à lui-même avec l'UDP 1067 de destination pour le traitement.

Pour une liste complète de ports a autorisé par les règles par défaut internes d'expédition, vérifient la sortie de la commande **SH de règles**. L'analyse de liste complète est hors de portée de ce document.

Vous pouvez vérifier que des règles d'ACL sont frappé par le trafic avec la commande de **début de config acl counter**. Les compteurs peuvent être affichés avec la commande **SH du détail ACLNAME d'acl**.

Surveillance du plan de contrôle

Un aspect de protéger un périphérique de réseau, est de s'assurer qu'il n'est pas accablé avec plus de trafic d'administration qu'il peut traiter. Sur tous les contrôleurs, après le code 4.1, il y a une limitation plate de contrôle activée par défaut, qui donnera un coup de pied dedans si le trafic pour la CPU dépasse les 2 mbps.

Sur les réseaux occupés, il est possible d'observer la limitation en effet (par exemple, le moniteur lâché cingle à la CPU). La caractéristique peut être contrôlée avec la commande de **config advanced rate**. Vous pouvez seulement l'activer ou désactiver, mais pas placez des débits ou contre quel trafic c'agira d'abord.

Sur des fonctionnement normal, il est recommandé ceci reste activé.

Cryptage fort pour le trafic de HTTPs

Par défaut, le contrôleur offre les deux chiffrements de résistance à ciel et terre pour assurer la

compatibilité avec des navigateurs plus âgés pendant l'installation HTTPS. Le contrôleur a fourni par 40 bits RC4, DES de 56 bits, jusqu'aux bits AES 256. La sélection du chiffrement le plus fort est faite par le navigateur.

Afin de s'assurer que seulement des chiffrements forts sont utilisés, vous pouvez les activer avec la commande d'**enable de config network secureweb cipher-option high**, ainsi seulement 168 3DES ou 128 longueurs AES et plus élevées de chiffrement sont offertes par le contrôleur sur l'accès de Gestion HTTPS.

Contrôle de session

Configurations Telnet/SSH

Par défaut, le contrôleur permet un maximum de 5 utilisateurs simultanés, avec un délai d'attente de 5 minutes. Il est essentiel que ces valeurs soient configurées convenablement dans votre environnement, car l'établissement de elles à illimité (zéro) peut ouvrir la porte au déni de service potentiel contre des contrôleurs, si les utilisateurs devaient essayer une attaque de force brutale contre eux. C'est un exemple des valeurs par défaut :

```
(Cisco Controller) >show sessions

CLI Login Timeout (minutes)..... 5
Maximum Number of CLI Sessions..... 5
```

Souvenez-vous cela par conception, même si la Gestion au-dessus de la radio ou de l'interface dynamique est désactivée, un périphérique peut établir toujours une connexion SSH au contrôleur. C'est une CPU imposant la tâche, et WLC limite le nombre de sessions simultanées, et pendant combien de temps utilisant ces paramètres.

Les valeurs peuvent être ajustées avec la commande de **sessions de config**.

Port de console

Le port série a une valeur du dépassement de durée séparée, qui est placée à 5 minutes par défaut, mais elle est généralement changée à 0 (illimité) pendant les sessions de dépannage.

```
Cisco Controller) >show serial

Serial Port Login Timeout (minutes)..... 5
Baud Rate..... 9600
Character Size..... 8
Flow Control:..... Disable
Stop Bits..... 1
Parity Type:..... none
```

Il est recommandé d'utiliser le par défaut de 5 minutes. Ceci empêche n'importe qui qui a accès physique au contrôleur pour gagner l'accès administratif, au cas où un utilisateur ouvert une session sur le port de console laisserait la session ouverte. Les valeurs peuvent être ajustées avec la commande d'**interface série de config**.

Remontant tous

Après avoir vérifié l'aspect différent de sécuriser un WLC, ceci peut être récapitulé :

- Il est important d'empêcher des périphériques autres que les stations dentelées de Gestion d'accéder à WLC, désactivant non seulement des protocoles non-utilisés, mais également en limitant l'accès sur la couche 4/layer 3 avec CPU ACLs.
- La limitation de débit devrait être activée (elle est par défaut).
- L'accès de contrôle par la **Gestion au-dessus des** commandes **X** n'est pas assez pour les installations sécurisées, comme les utilisateurs peuvent encore accéder à des protocoles de gestion parlant directement à l'adresse IP de Gestion, utilisant des ressources en CPU et mémoire.

Pratiques de sécurité

Voici certaines des pratiques de sécurité :

- Créez l'ACL CPU relâchant l'accès de toute l'interface dynamique VLAN ou de sous-réseaux. Cependant, permettez le trafic DHCP au port de serveur (67) ainsi les clients peuvent obtenir l'adresse négociée par DHCP si le proxy DHCP est activé (il est par défaut). Si l'interface dynamique a une adresse IP publique, elle est recommandée d'avoir la règle d'ACL refusant tout le trafic des provenances inconnues à l'adresse d'interface dynamique.
- Placez toutes les règles d'ACL aussi d'arrivée ou avec la direction, et marquez-les qu'appliquées en tant que **chacun des deux** (de câble et option sans fil).Comment valider :`(Cisco Controller) >show acl cpu`

```
CPU Acl Name.............................. acl1
Wireless Traffic.......................... Enabled
Wired Traffic............................. Enabled
```

- Limitation plate de contrôle d'enable (elle est activée par défaut).Comment valider :`(Cisco Controller) >show advanced rate`

```
Control Path Rate Limiting.....................  Enabled
```

- Toujours protocoles de gestion chiffrés par utilisation (HTTPS, SSH). C'est la configuration par défaut pour la Gestion interactive. Pour le SNMP vous pourriez devoir permettre à V3 de permettre trafic chiffré/authentifié SNMP. Souvenez-vous pour recharger le contrôleur si vous apportez des modifications à la configuration SNMP.C'est comment valider :`(Cisco Controller) >show network summary`

```
RF-Network Name........................... 4400
Web Mode.................................. Disable
Secure Web Mode........................... Enable
Secure Web Mode Cipher-Option High........ Enable
Secure Web Mode Cipher-Option SSLv2....... Enable
Secure Shell (ssh)........................ Enable
Telnet.................................... Disable
...
```

- Cryptage élevé d'enable pour HTTPS (ceci est désactivé par défaut).
- C'est une bonne idée d'installer un certificat de serveur validé pour l'accès HTTPS à votre contrôleur (signé par votre CA de confiance), remplaçant le certificat signé d'individu installé par défaut.
- Placez le délai d'attente de session et de console à 5 minutes.`(Cisco Controller) >show serial`

```
Serial Port Login Timeout (minutes)......... 5
Baud Rate................................... 9600
```

```
Character Size.............................. 8
Flow Control:............................... Disable
Stop Bits................................... 1
Parity Type:................................ none


(Cisco Controller) >show sessions

CLI Login Timeout (minutes)..... 5
Maximum Number of CLI Sessions..... 5
```

Informations connexes

- Point d'accès léger - Forum Aux Questions
- Dépannage du contrôleur LAN sans fil (WLC) - FAQ
- Module du contrôleur LAN sans fil Cisco - Questions/réponses
- Gestion des ressources radio sous des réseaux sans fil unifiés
- Support et documentation techniques - Cisco Systems