Paramètres de signature IDS sur les contrôleurs de réseau local sans fil

Contenu

Introduction

Ce document explique comment configurer des signatures de systèmes de détection d'intrusions (IDS) dans les versions 3.2 et antérieures du logiciel du contrôleur de réseau local sans fil Cisco.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées sur la version de logiciel 3.2 et ultérieures de contrôleur WLAN.

Conventions

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

Informations générales

Vous pouvez télécharger les ID que le fichier de signatures pour la signature éditent (ou pour l'examen de documentation). Choisissez le **Commands > Upload File > le fichier de signatures**.

Afin de télécharger un fichier de signatures modifié d'ID, choisissez le **Commands > Download File > le fichier de signatures**. Après que vous téléchargiez un fichier de signatures au contrôleur, tous les Points d'accès (aps) que sont connectés au contrôleur sont régénérés en temps réel avec les paramètres nouvellement édités de signature.

Cette fenêtre affiche comment télécharger le fichier de signatures :

Les paramètres des documents neuf de fichier texte de signature d'ID pour chaque signature d'ID. Vous pouvez modifier ces paramètres de signature et écrire de nouvelles signatures faites sur commande. Voyez le format que la section de paramètres d'ID de contrôleur de ce document fournit.

Paramètres d'ID de contrôleur

Toutes les signatures *doivent* avoir ce format :

```
Name = <str>, Ver = <int>, Preced = <int>, FrmType = <frmType-type>, Pattern =
<pattern-format>, Freq = <int>, Interval = <int>, Quiet = <int>, Action = <action-val>,
Desc = <str>
```

La longueur maximale de la ligne est 1000 caractères. Des lignes qui sont plus longues que 1000 ne sont pas analysées correctement.

Toutes les lignes avec lesquelles commencez `#` dans le fichier texte d'ID sont considérées des commentaires et sont ignorées. Également ignorées sont toutes les lignes vides, qui sont des lignes avec juste le whitespace ou le saut de ligne. Le premier noncomment, ligne de nonblank *doit* avoir la `révision de` mot clé. Si le fichier est un fichier de signatures Cisco-fourni, vous ne devez pas changer la valeur de la `révision`. Cisco emploie cette valeur pour gérer des releases de fichier de signatures. Si le fichier contient les signatures qui ont été créées par l'utilisateur final, la valeur de la `révision` *doit* être `faite sur commande` (`révision = coutume`).

Les neuf paramètres de signature d'ID que vous pouvez modifier sont :

- **`Nom`** = nom de signature. C'est une seule chaîne qui identifie la signature. La longueur maximale du nom est 20 caractères.
- **`Preced`** = priorité de signature. C'est un identificateur unique qui indique la priorité de la signature parmi toutes les signatures qui sont définies dans le fichier de signatures. Il *doit* y avoir un jeton de `Preced` par signature.
- **`FrmType`** = type de trame. Ce paramètre peut prendre des valeurs de la liste de `<frmType-val>`. Il *doit* y avoir un jeton de `FrmType` par signature. `Le <frmType-val>` peut être l'un de ces deux mots clé seulement :`mgmtdonnéesLe <frmType-val>` indique si cette signature détecte des trames de données ou de Gestion.
- **`Modèle`** = modèle de signature. La valeur symbolique est utilisée pour détecter les paquets qui apparient la signature. Il *doit* y avoir au moins un jeton de `modèle` par signature. Il peut y avoir jusqu'à cinq tels jetons par signature. Si la signature a plus d'un tel jeton, un paquet doit apparier les valeurs de tous les jetons pour que le paquet apparie la signature.Quand AP reçoit un paquet, AP prend le flot d'octet qui commence au `<offset>`, ANDs il avec le `<mask>`, et compare le résultat au `<pattern>`. Si AP trouve une correspondance, AP considère le paquet une correspondance avec la signature. `Le <pattern-format>` peut être précédé par l'opérateur de négation « `!` ». Dans ce cas, tous les paquets qui ÉCHOUENT l'exécution de correspondance que cette section décrit sont considérés une correspondance avec la

signature.

- **`Freq`** = fréquence de correspondance de paquet en paquets/intervalle. La valeur de ce jeton indique combien de paquets par intervalle de mesure doivent apparier cette signature avant que l'`action de` signature soit exécutée. Une valeur de 0 indique que la `mesure de` signature est prise chaque fois qu'un paquet apparie la signature. La valeur maximale pour ce jeton est 65,535. Il *doit* y avoir un jeton de `Freq` par signature.
- **`Intervalle`** = intervalle de mesure en quelques secondes. La valeur de ce jeton indique le délai prévu que le seuil (c'est-à-dire, le `Freq`) spécifie. La valeur par défaut pour ce jeton est 1 seconde. La valeur maximale pour ce jeton est 3600.
- Temps **`tranquille`** = tranquille en quelques secondes. La valeur de ce jeton indique la durée qui doit passer pendant le ce qu'AP ne reçoit pas les paquets qui apparient la signature avant qu'AP détermine que l'attaque que la signature indique s'est abaissé. Si la valeur du jeton de `Freq` est 0, ce jeton est ignoré. Il *doit* y avoir un jeton `tranquille` par signature.
- **`Action`** = action de signature. Ceci indique ce qu'AP doit faire si un paquet apparie la signature. Ce paramètre peut prendre des valeurs de la liste de `<action-val>`. Il *doit* y avoir un jeton d'`action` par signature. `Le <action-val>` peut être l'un de ces deux mots clé seulement :`aucun` = ne fait rien.`état` = état la correspondance au commutateur.
- **`Desc`** = description de signature. C'est une chaîne qui décrit le but de la signature. Quand une correspondance de signature est signalée dans un déroutement de Protocole SNMP (Simple Network Management Protocol), cette chaîne est fournie au déroutement. La longueur maximale de la description est 100 caractères. Il *doit* y avoir un jeton de `Desc` par signature.

Signatures de norme d'ID de contrôleur

Ces signatures d'ID se transportent avec le contrôleur en tant que « signatures standard d'ID ». Vous pouvez modifier tous ces paramètres de signature, car la section de paramètres d'ID de contrôleur décrit.

```
Revision = 1.000
Name = "Bcast deauth", Ver = 0, Preced= 1, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF,
Pattern = 4:0x01:0x01, Freq=30, Quiet = 300, Action = report, Desc="Broadcast
Deauthentication Frame"

Name = "NULL probe resp 1", Ver = 0, Preced = 2, FrmType = mgmt, Pattern =
0:0x0050:0x03FF, Pattern = 36:0x0000:0xFFFF, Freq=1, Quiet = 300, Action = report, Desc =
"NULL Probe Response - Zero length SSID element"

Name = "NULL probe resp 2", Ver = 0, Preced = 3, FrmType = mgmt, Pattern =
0:0x0050:0x03FF, Pattern = !36:0x00:0xFF, Freq=1, Quiet = 300, Action = report, Desc =
"NULL Probe Response - No SSID element"

Name = "Assoc flood", Ver = 0, Preced= 4, FrmType = mgmt, Pattern = 0:0x0000:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Association Request flood"

Name = "Auth Flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0: 0x00b0: 0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Authentication Request flood"

Name = "Reassoc flood", Ver = 0, Preced= 5, FrmType = mgmt, Pattern = 0:0x0020:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Reassociation Request flood"

Name = "Broadcast Probe flood", Ver = 0, Preced= 6, FrmType = mgmt, Pattern =
0:0x0040:0x03FF, Pattern = 4:0x01:0x01, Pattern = 24:0x0000:0xFFFF, Freq=50, Quiet = 600,
Action = report, Desc="Broadcast Probe Request flood"
```

```
Name = "Disassoc flood", Ver = 0, Preced= 7, FrmType = mgmt, Pattern = 0:0x00A0:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Disassociation flood"

Name = "Deauth flood", Ver = 0, Preced= 8, FrmType = mgmt, Pattern = 0:0x00C0:0x03FF,
Freq=50, Quiet = 600, Action = report, Desc="Deauthentication flood"

Name = "Res mgmt 6 & 7", Ver = 0, Preced= 9, FrmType = mgmt, Pattern = 0:0x0060:0x03EF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types 6 and 7"

Name = "Res mgmt D", Ver = 0, Preced= 10, FrmType = mgmt, Pattern = 0:0x00D0:0x03FF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-type D"

Name = "Res mgmt E & F", Ver = 0, Preced= 11, FrmType = mgmt, Pattern = 0:0x00E0:0x03EF,
Freq=5, Quiet = 600, Action = report, Desc="Reserved management sub-types E and F"

Name = "EAPOL flood", Ver = 0, Preced= 12, FrmType = data, Pattern = 0:0x0108:0x03FF,
Pattern = 30:0x888E:0xFFFF, Freq=50, Quiet = 300, Action = report, Desc="EAPOL Flood
Attack"

Name = "NetStumbler 3.2.0", Ver = 0, Preced= 13, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
36:0x466c7572:0xFFFFFFFF, Freq = 1, Quiet = 300, Action = report, Desc="NetStumbler 3.2.0"

Name = "NetStumbler 3.2.3", Ver = 0, Preced= 14, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
36:0x416C6C20:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.2.3"

Name = "NetStumbler 3.3.0", Ver = 0, Preced= 15, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Pattern =
36:0x20202020:0xFFFFFFFF, Freq = 1, Quiet = 600, Action = report, Desc="NetStumbler 3.3.0"

Name = "NetStumbler generic", Ver = 0, Preced= 16, FrmType = data, Pattern =
0:0x0108:0x03FF, Pattern = 27:0x00601d:0xFFFFFF, Pattern = 30:0x0001:0xFFFF, Freq = 1,
Quiet = 600, Action = report, Desc="NetStumbler"

Name = "Wellenreiter", Ver = 0, Preced= 17, FrmType = mgmt, Pattern = 0:0x0040:0x03FF,
Pattern = 24:0x001d746869735f69735f757365645f666f725f77656c6c656e726569:
0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff, Freq = 1, Quiet = 600,
Action = report, Desc="Wellenreiter"
```

Messages d'ID

Avec la version 4.0 Sans fil de contrôleur LAN, vous pourriez recevoir ce message d'ID.

```
Big NAV Dos attack from AP with Base Radio MAC 00:0f:23:xx:xx:xx,
Slot ID 0 and Source MAC 00:00:00:00:00:00
```

Ce message d'ID indique que le champ de vecteur d'allocation de réseau de 802.11 (NAV) dans la trame Sans fil de 802.11 est trop grand et le réseau Sans fil pourrait être soumis à une attaque DoS (ou il y a un client de mauvaise conduite).

Après que vous receviez ce message d'ID, l'étape suivante est de dépister le client offensant. Vous devez localiser le client basé sur sa force du signal avec un renifleur Sans fil dans la zone autour du Point d'accès ou utiliser le serveur d'emplacement pour indiquer exactement sa position.

Le champ de NAV est le mécanisme virtuel d'écoute de porteuse utilisé pour atténuer des collisions entre les terminaux masqués (clients sans fil que le client sans fil en cours ne peut pas le détecter quand il transmet) dans des transmissions de 802.11. Les terminaux masqués créent des problèmes parce que le Point d'accès pourrait recevoir des paquets de deux clients qui peuvent transmettre au Point d'accès mais ne reçoit pas les transmissions de chacun. Quand ces clients transmettent en même temps, leurs paquets se heurtent au Point d'accès et ceci a comme

conséquence le Point d'accès ne recevant ni l'un ni l'autre de paquet clairement.

Toutes les fois qu'un client sans fil veut envoyer un paquet de données au Point d'accès, il transmet réellement un ordre de quatre-paquet appelé l'ordre de paquet RTS-CTS-DATA-ACK. Chacune des quatre trames de 802.11 porte un champ de NAV qui indique le nombre de microsecondes qui le canal est réservé pour par un client sans fil. Pendant la prise de contact RTS/CTS entre le client sans fil et le Point d'accès, le client sans fil envoie une petite trame de RTS qui inclut un intervalle de NAV assez grand pour se terminer l'ordre entier. Ceci inclut la trame CTS, la trame de données, et la trame ultérieure d'accusé de réception du Point d'accès.

Quand le client sans fil transmet son paquet de RTS avec NAV réglé, la valeur transmise est utilisée pour placer les temporisateurs de NAV sur tous autres clients sans fil associés au Point d'accès. Le Point d'accès répond au paquet de RTS du client avec un paquet CTS qui contient une nouvelle valeur de NAV mise à jour pour expliquer le temps s'est déjà écoulé pendant l'ordre de paquet. Après que le paquet CTS soit envoyé, chaque client sans fil qui peut recevoir du Point d'accès a mis à jour leur temporisateur de NAV et reporte toutes les transmissions jusqu'à ce que leur temporisateur de NAV atteigne 0. Ceci maintient le canal libre pour que le client sans fil complète le processus de transmettre un paquet au Point d'accès.

Un attaquant pourrait exploiter ce mécanisme virtuel d'écoute de porteuse en affirmant un grand temps dans le domaine de NAV. Ceci empêche d'autres clients des paquets de transmission. La valeur maximale pour NAV est de 32767, ou approximativement 32 millisecondes sur les réseaux 802.11b. Ainsi dans la théorie un attaquant doit seulement transmettre approximativement 30 paquets par seconde pour bloquer tout l'accès au canal.

Informations connexes

- Contrôleurs de réseau LAN fil de la gamme Cisco 4400
- Contrôleurs de LAN sans fil de la gamme Cisco 4100
- Contrôleurs de LAN sans fil de la gamme Cisco 2000
- Version 3.1 d'engines de signature de Detection System de Cisco Intrusion
- Support et documentation techniques - Cisco Systems