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.

Components Used

Les informations de ce document sont basées sur le logiciel WLAN Controller version 3.2 et ultérieure.

Conventions

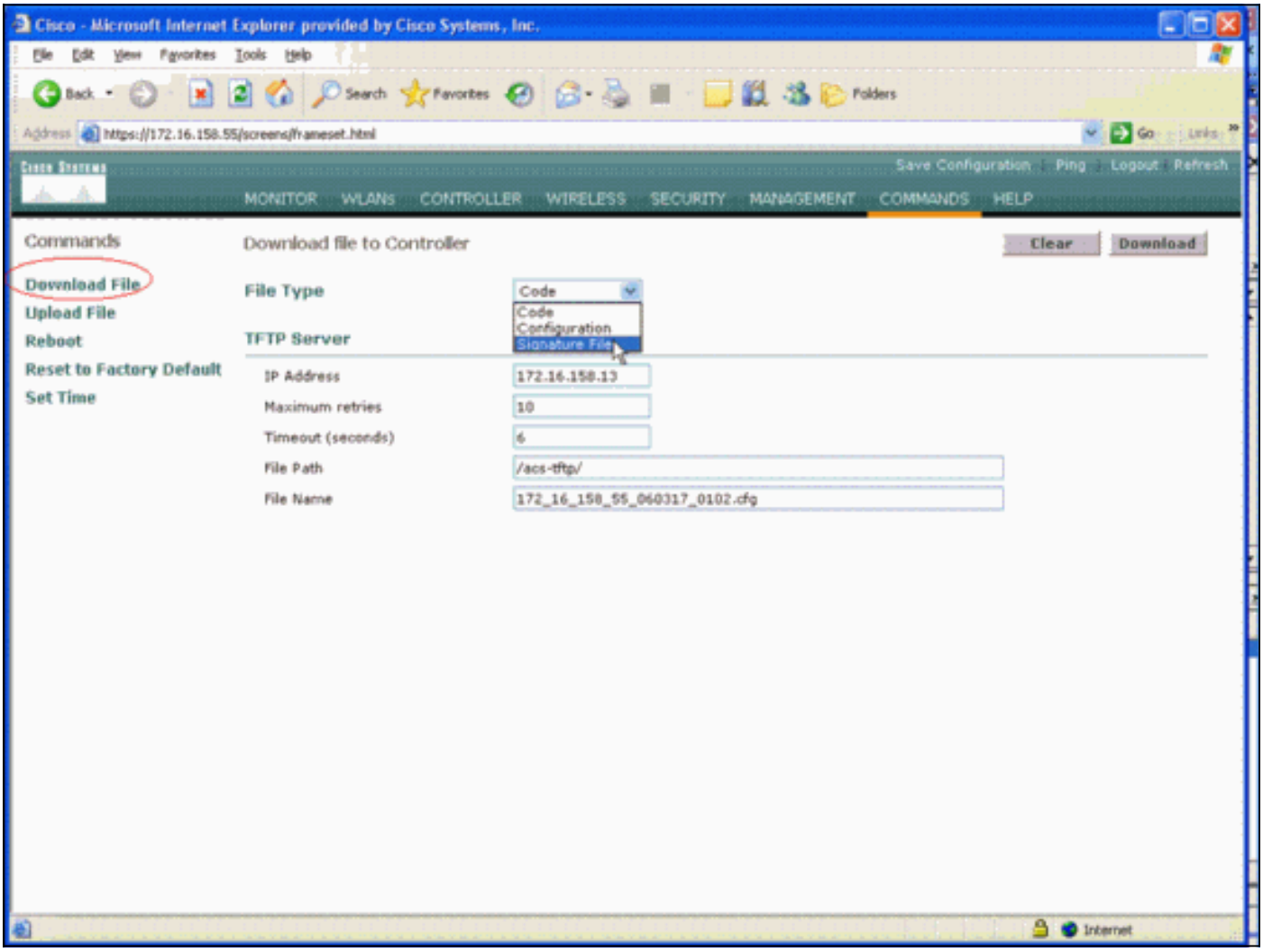
Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Vous pouvez télécharger le fichier de signature IDS pour modification de signature (ou pour examen de la documentation). Choisissez **Commandes > Upload File > Signature File**. Afin de

télécharger un fichier de signature IDS modifié, choisissez **Commandes > Télécharger le fichier > Fichier de signature**. Après avoir téléchargé un fichier de signature sur le contrôleur, tous les points d'accès (AP) connectés au contrôleur sont actualisés en temps réel avec les paramètres de signature récemment modifiés.

Cette fenêtre indique comment télécharger le fichier de signature :



Le fichier texte de signature IDS documente neuf paramètres pour chaque signature IDS. Vous pouvez modifier ces paramètres de signature et écrire de nouvelles signatures personnalisées. Voir le format que fournit la section Paramètres IDS du contrôleur de ce document.

Paramètres IDS du contrôleur

Toutes les signatures *doivent* avoir le format suivant :

```
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 de 1 000 caractères. Les lignes de plus de 1 000 ne sont pas analysées correctement.

Toutes les lignes commençant par # dans le fichier texte IDS sont considérées comme des commentaires et sont ignorées. Toutes les lignes vides sont également ignorées, c'est-à-dire les

lignes avec un espace vide ou une nouvelle ligne. La première ligne non-commentaire, non vide *doit* avoir le mot clé `Revision`. Si le fichier est un fichier de signature fourni par Cisco, vous ne devez pas modifier la valeur de `révision`. Cisco utilise cette valeur pour gérer les versions des fichiers de signatures. Si le fichier contient des signatures qui ont été créées par l'utilisateur final, la valeur de `révision` *doit* être `personnalisée` (`révision = personnalisée`).

Les neuf paramètres de signature IDS que vous pouvez modifier sont les suivants :

- **`Nom`** = nom de la signature. Il s'agit d'une chaîne unique qui identifie la signature. La longueur maximale du nom est de 20 caractères.
- **`Précédent`** = priorité de signature. Il s'agit d'un ID unique qui indique la priorité de la signature parmi toutes les signatures définies dans le fichier de signature. Il *doit* y avoir un jeton `Preced` par signature.
- **`FrmType`** = type de trame. Ce paramètre peut prendre des valeurs de la liste `<frmType-val>`. Il *doit* y avoir un jeton `FrmType` par signature. Le `<frmType-val>` ne peut être que l'un de ces deux mots clés :`gestiondonnées`Le `<frmType-val>` indique si cette signature détecte des trames de données ou de gestion.
- **`Modèle`** = modèle de signature. La valeur de jeton est utilisée pour détecter les paquets qui correspondent à la signature. Il *doit* y avoir au moins un jeton de `modèle` par signature. Il peut y avoir jusqu'à cinq jetons de ce type par signature. Si la signature comporte plusieurs jetons de ce type, un paquet doit correspondre aux valeurs de tous les jetons pour que le paquet corresponde à la signature.Lorsque le point d'accès reçoit un paquet, il prend le flux d'octets qui commence à `<offset>`, et le prend avec le `<masque>`, et compare le résultat avec `<pattern>`. Si le point d'accès trouve une correspondance, le point d'accès considère que le paquet correspond à la signature. Le `<pattern-format>` peut être précédé par l'opérateur de négation "`!`« . Dans ce cas, tous les paquets qui échouent à l'opération de correspondance décrite dans cette section sont considérés comme correspondant à la signature.
- **`Freq`** : fréquence de correspondance de paquets en paquets/intervalle. La valeur de ce jeton indique combien de paquets par intervalle de mesure doivent correspondre à cette signature avant que l'`action` de signature soit exécutée. La valeur 0 indique que l'`action` de signature est prise chaque fois qu'un paquet correspond à la signature. La valeur maximale de ce jeton est 65 535. Il *doit* y avoir un jeton `Freq` par signature.
- **`Intervalle`** = intervalle de mesure en secondes. La valeur de ce jeton indique la période que le seuil (c'est-à-dire le Freq) spécifie. La valeur par défaut de ce jeton est de 1 seconde. La valeur maximale de ce jeton est 3600.
- **`Calme`** = temps calme en secondes. La valeur de ce jeton indique le temps qui doit passer pendant lequel le point d'accès ne reçoit pas de paquets qui correspondent à la signature avant que le point d'accès détermine que l'attaque que la signature indique a été annulée. Si la valeur du jeton `Freq` est 0, ce jeton est ignoré. Il *doit* y avoir un jeton `silencieux` par signature.
- **`Action`** = action de signature. Ceci indique ce que le point d'accès doit faire si un paquet correspond à la signature. Ce paramètre peut prendre des valeurs de la liste `<action-val>`. Il *doit* y avoir un jeton `Action` par signature. Le mot `<action-val>` ne peut être que l'un de ces deux mots clés :`aucun` = ne rien faire.`report` = signaler la correspondance au commutateur.
- **`Desc`** = description de la signature. Il s'agit d'une chaîne qui décrit l'objectif de la signature. Lorsqu'une correspondance de signature est signalée dans un déroutement SNMP (Simple Network Management Protocol), cette chaîne est fournie dans le déroutement. La longueur maximale de la description est de 100 caractères. Il *doit* y avoir un jeton `Desc` par signature.

Signatures standard IDS du contrôleur

Ces signatures IDS sont livrées avec le contrôleur comme ” de signatures IDS standard “. Vous pouvez modifier tous ces paramètres de signature, comme le décrit la section Paramètres IDS du contrôleur.

```
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 IDS

Avec Wireless LAN Controller version 4.0, vous pouvez recevoir ce message IDS.

```
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 IDS indique que le champ NAV (Network Allocation Vector) 802.11 de la trame 802.11 sans fil est trop volumineux et que le réseau sans fil peut être victime d'une attaque DOS (ou d'un comportement incorrect du client).

Une fois que vous avez reçu ce message IDS, l'étape suivante consiste à rechercher le client incriminé. Vous devez localiser le client en fonction de sa puissance de signal avec un analyseur sans fil dans la zone autour du point d'accès ou utiliser le serveur d'emplacement pour localiser sa position.

Le champ NAV est le mécanisme de détection de porteuse virtuelle utilisé pour atténuer les collisions entre les terminaux cachés (les clients sans fil que le client sans fil actuel ne peut détecter lorsqu'il transmet) dans les transmissions 802.11. Les terminaux masqués créent des problèmes car le point d'accès peut recevoir des paquets de deux clients qui peuvent transmettre au point d'accès mais ne reçoivent pas les transmissions de l'autre. Lorsque ces clients transmettent en même temps, leurs paquets entrent en collision au niveau du point d’accès, ce qui signifie que le point d’accès ne reçoit aucun paquet clairement.

Chaque fois qu'un client sans fil veut envoyer un paquet de données au point d'accès, il transmet en fait une séquence de quatre paquets appelée séquence de paquets RTS-CTS-DATA-ACK. Chacune des quatre trames 802.11 porte un champ NAV qui indique le nombre de microsecondes pour lesquelles le canal est réservé par un client sans fil. Au cours de la connexion RTS/CTS entre le client sans fil et le point d'accès, le client sans fil envoie une petite trame RTS qui inclut un intervalle NAV suffisamment grand pour terminer la séquence entière. Cela inclut la trame CTS, la trame de données et la trame d’accusé de réception subséquente à partir du point d’accès.

Lorsque le client sans fil transmet son paquet RTS avec le jeu NAV, la valeur transmise est utilisée pour définir les compteurs NAV sur tous les autres clients sans fil associés au point d'accès. Le point d'accès répond au paquet RTS du client avec un paquet CTS qui contient une nouvelle valeur NAV mise à jour pour tenir compte du temps déjà écoulé au cours de la séquence de paquets. Une fois le paquet CTS envoyé, chaque client sans fil pouvant recevoir depuis le point d'accès a mis à jour son compteur NAV et reporte toutes les transmissions jusqu'à ce que le compteur NAV atteigne 0. Cela permet au client sans fil de libérer le canal pour terminer le processus de transmission d’un paquet au point d’accès.

Un attaquant peut exploiter ce mécanisme de détection de porteuse virtuelle en affirmant une grande partie du champ NAV. Cela empêche les autres clients de transmettre des paquets. La

valeur maximale de la NAV est de 32 767, soit environ 32 millisecondes sur les réseaux 802.11b. Donc en théorie, un attaquant n'a besoin que de transmettre environ 30 paquets par seconde pour bloquer tout 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
- Moteurs de signature Cisco Intrusion Detection System Version 3.1
- Support et documentation techniques - Cisco Systems