Signaturparameter für Wireless LAN Controller IDS

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie die IDS-Signaturen (Intrusion Detection System) in Version 3.2 und früheren Versionen der Cisco Wireless LAN (WLAN) Controller-Software konfigurieren.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der WLAN Controller Software Version 3.2 und höher.

Konventionen

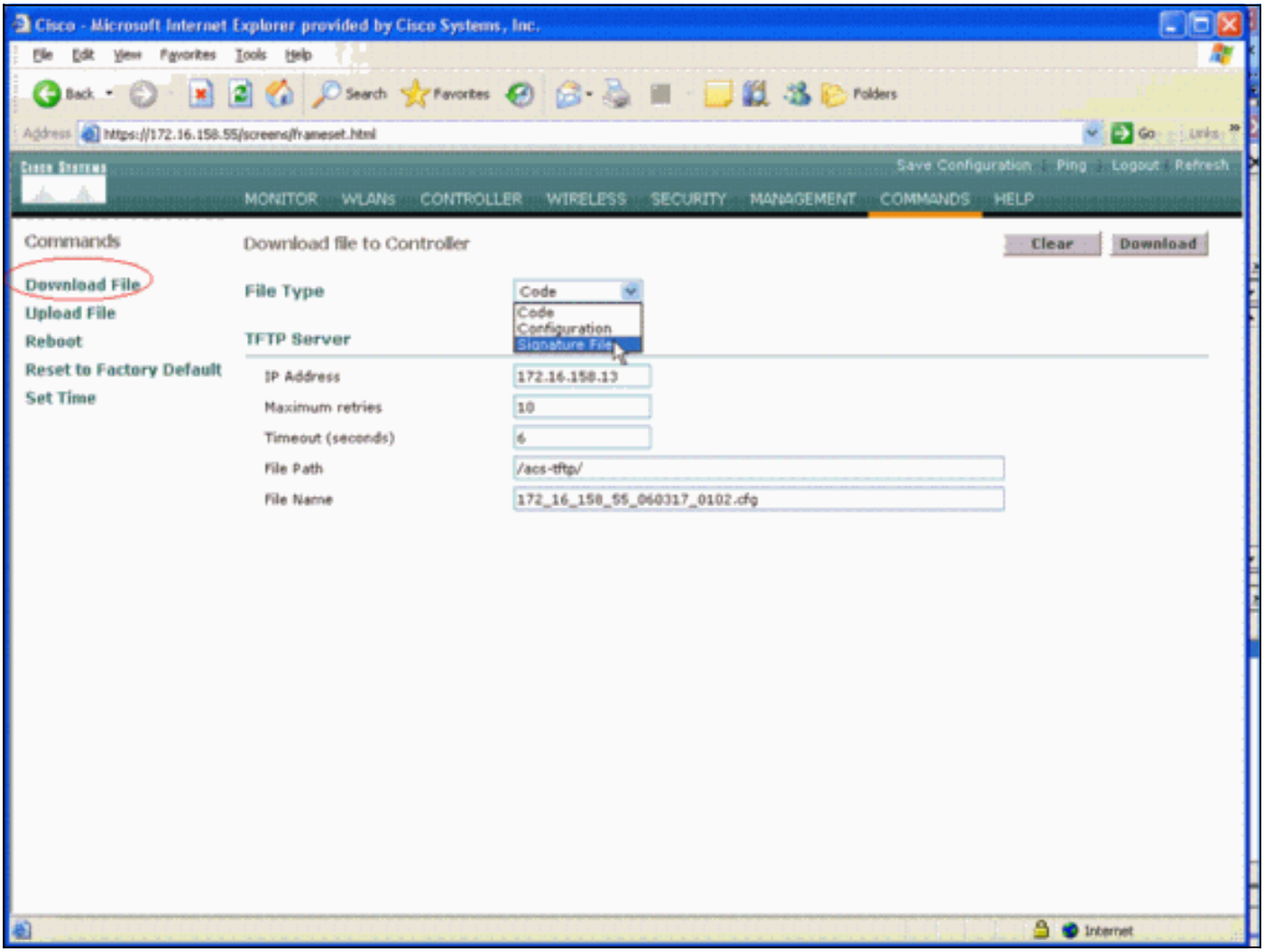
Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Sie können die IDS-Signaturdatei zur Signaturbearbeitung (oder zur Dokumentationsüberprüfung)

hochladen. Wählen Sie **Befehle > Datei hochladen > Signaturdatei aus**. Um eine geänderte IDS-Signaturdatei herunterzuladen, wählen Sie **Befehle > Download File > Signature File aus**. Nachdem Sie eine Signaturdatei auf den Controller heruntergeladen haben, werden alle mit dem Controller verbundenen Access Points (APs) in Echtzeit mit den neu bearbeiteten Signaturparametern aktualisiert.

In diesem Fenster wird das Herunterladen der Signaturdatei veranschaulicht:



Die IDS-Signatur-Textdatei dokumentiert neun Parameter für jede IDS-Signatur. Sie können diese Signaturparameter ändern und neue benutzerdefinierte Signaturen schreiben. Das Format, das der Abschnitt Controller IDS Parameters dieses Dokuments bereitstellt.

Controller-IDS-Parameter

Alle Signaturen *müssen* folgendes Format haben:

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

Die maximale Länge der Zeile beträgt 1000 Zeichen. Posten, die länger als 1000 sind, werden nicht korrekt analysiert.

Alle Zeilen, die mit # in der IDS-Textdatei beginnen, werden als Kommentare betrachtet und

übersprungen. Außerdem werden alle leeren Zeilen übersprungen, d. h. Zeilen mit nur Leerzeichen oder Zeilenumbrüchen. Die erste nicht kommentierte, nicht leere Zeile *muss* das Schlüsselwort `Revision` haben. Wenn es sich bei der Datei um eine von Cisco bereitgestellte Signaturdatei handelt, dürfen Sie den Wert von `Revision` nicht ändern. Cisco verwendet diesen Wert zur Verwaltung von Signaturdateiversionen. Wenn die Datei Signaturen enthält, die vom Endbenutzer erstellt wurden, *muss* der Wert von `Revision` `benutzerdefiniert` sein (`Revision = custom`).

Sie können die folgenden neun IDS-Signaturparameter ändern:

- **`Name`** = Signaturname. Dies ist eine eindeutige Zeichenfolge, die die Signatur identifiziert. Der Name darf maximal 20 Zeichen lang sein.
- **`Preced`** = Signaturpriorität. Diese eindeutige ID gibt die Rangfolge der Signatur aller Signaturen an, die in der Signaturdatei definiert sind. Es *muss* ein `vordefiniertes` Token pro Signatur vorhanden sein.
- **`FormType`** = Frametyp. Dieser Parameter kann Werte aus der `<frmType-val>`-Liste übernehmen. Es *muss* ein `FormType-`Token pro Signatur vorhanden sein. Bei `<frmType-val>` kann es sich nur um eines der folgenden Schlüsselwörter handeln:`MgmtDaten`Der `<frmType-val>` gibt an, ob diese Signatur Daten- oder Management-Frames erkennt.
- **`Muster`** = Signaturmuster Der Tokenwert wird verwendet, um Pakete zu erkennen, die mit der Signatur übereinstimmen. Es *muss* mindestens ein `Muster-`Token pro Signatur vorhanden sein. Pro Signatur können bis zu fünf solcher Token vorhanden sein. Wenn die Signatur über mehr als ein solches Token verfügt, muss ein Paket mit den Werten aller Token übereinstimmen, damit das Paket mit der Signatur übereinstimmt.Wenn der Access Point ein Paket empfängt, nimmt der Access Point den Bytestream, der bei `<offset>` beginnt, UNDs ihn mit der `<Maske>` und vergleicht das Ergebnis mit `<pattern>`. Wenn der Access Point eine Übereinstimmung findet, betrachtet der Access Point das Paket als Übereinstimmung mit der Signatur. Dem `<pattern-format>` kann der Negations-Operator "`!`" vorangestellt werden. In diesem Fall werden alle Pakete, bei denen die in diesem Abschnitt beschriebene Match-Operation fehlschlägt, als Übereinstimmung mit der Signatur betrachtet.
- **`Freq`** = Paketabgleichfrequenz in Paketen/Intervallen. Der Wert dieses Tokens gibt an, wie viele Pakete pro Messintervall dieser Signatur entsprechen müssen, bevor die Signatur `Action` ausgeführt wird. Ein Wert von 0 gibt an, dass die Signatur-`Aktion` jedes Mal ausgeführt wird, wenn ein Paket mit der Signatur übereinstimmt. Der Höchstwert für dieses Token beträgt 65.535. Es *muss* ein `Freq-`Token pro Signatur vorhanden sein.
- **`Intervall`** = Messintervall in Sekunden. Der Wert dieses Tokens gibt den Zeitraum an, den der Grenzwert (d. h. der `Freq`) angibt. Der Standardwert für dieses Token ist 1 Sekunde. Der Höchstwert für dieses Token ist 3600.
- **`Ruhige`** Zeit in Sekunden. Der Wert dieses Tokens gibt die Zeitspanne an, während der der WAP keine Pakete empfängt, die mit der Signatur übereinstimmen, bevor der WAP feststellt, dass der von der Signatur angegebene Angriff nachgelassen hat. Wenn der Wert des `Freq-`Tokens 0 ist, wird dieses Token ignoriert. Es *muss* ein `leises` Token pro Signatur vorhanden sein.
- **`Aktion`** = Signaturaktion Dies gibt an, was der Access Point tun muss, wenn ein Paket mit der Signatur übereinstimmt. Dieser Parameter kann Werte aus der `<action-val>` Liste übernehmen. Es *muss* ein `Action-`Token pro Signatur vorhanden sein. Bei `<action-val>` kann es sich nur um eines der folgenden Schlüsselwörter handeln:`none` = nichts tun.`report` = Melden Sie die Übereinstimmung dem Switch.
- **`Desc`** = Signaturbeschreibung. Dies ist eine Zeichenfolge, die den Zweck der Signatur

beschreibt. Wenn eine Signaturübereinstimmung in einem SNMP-Trap (Simple Network Management Protocol) gemeldet wird, wird diese Zeichenfolge an das Trap übergeben. Die Beschreibung darf maximal 100 Zeichen lang sein. Es *muss* ein `Desc`-Token pro Signatur vorhanden sein.

Controller-IDS-Standardsignaturen

Diese IDS-Signaturen werden mit dem Controller als "Standard-IDS-Signaturen" geliefert. Sie können alle diese Signaturparameter ändern, wie im Abschnitt Controller IDS Parameters beschrieben wird.

```
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"
```

IDS-Nachrichten

Bei Wireless LAN Controller Version 4.0 erhalten Sie möglicherweise diese IDS-Meldung.

```
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
```

Diese IDS-Meldung weist darauf hin, dass das 802.11 Network Allocation Vector (NAV)-Feld im 802.11-Wireless-Frame zu groß ist und das Wireless-Netzwerk möglicherweise einem DOS-Angriff (oder einem Client mit fehlerhaftem Verhalten) ausgesetzt ist.

Nachdem Sie diese IDS-Nachricht erhalten haben, müssen Sie als Nächstes den beleidigenden Client aufspüren. Sie müssen den Client basierend auf seiner Signalstärke mit einem Wireless Sniffer im Bereich um den Access Point ausfindig machen oder den Standort-Server verwenden, um dessen Position zu bestimmen.

Das NAV-Feld ist der virtuelle Carrier-Sense-Mechanismus, mit dem Kollisionen zwischen versteckten Terminals (Wireless-Clients, die der aktuelle Wireless-Client bei Übertragung nicht erkennen kann) bei 802.11-Übertragungen verhindert werden. Versteckte Terminals verursachen Probleme, da der Access Point möglicherweise Pakete von zwei Clients empfängt, die zwar an den Access Point übertragen werden können, aber keine Übertragungen der anderen Clients empfangen. Wenn diese Clients gleichzeitig übertragen werden, kollidieren ihre Pakete am Access Point, was dazu führt, dass der Access Point keines der Pakete eindeutig empfängt.

Wenn ein Wireless-Client ein Datenpaket an den Access Point senden möchte, überträgt er eine Vierpaketsequenz, die als RTS-CTS-DATA-ACK-Paketsequenz bezeichnet wird. Jeder der vier 802.11-Frames enthält ein NAV-Feld, das die Anzahl der Mikrosekunden angibt, für die der Kanal von einem Wireless-Client reserviert ist. Während des RTS/CTS-Handshake zwischen dem Wireless-Client und dem Access Point sendet der Wireless-Client einen kleinen RTS-Frame, der ein NAV-Intervall enthält, das groß genug ist, um die gesamte Sequenz abzuschließen. Dazu gehören der CTS-Frame, der Daten-Frame und der nachfolgende Bestätigungsrahmen vom Access Point.

Wenn der Wireless-Client sein RTS-Paket mit dem NAV-Satz überträgt, wird der übertragene Wert verwendet, um die NAV-Timer für alle anderen Wireless-Clients festzulegen, die dem Access Point zugeordnet sind. Der Access Point antwortet auf das RTS-Paket vom Client mit einem CTS-Paket, das einen neuen NAV-Wert enthält, der aktualisiert wird, um die bereits verstrichene Zeit während der Paketsequenz zu berücksichtigen. Nach dem Senden des CTS-Pakets hat jeder

Wireless-Client, der vom Access Point empfangen werden kann, seinen NAV-Timer aktualisiert und alle Übertragungen zurückgestellt, bis der NAV-Timer 0 erreicht hat. Dadurch bleibt der Kanal frei, sodass der Wireless-Client den Prozess der Übertragung eines Pakets an den Access Point abschließen kann.

Ein Angreifer könnte diesen virtuellen Carrier-Sense-Mechanismus ausnutzen, indem er eine große Zeit im NAV-Bereich geltend macht. Dies verhindert, dass andere Clients Pakete übertragen. Der Höchstwert für NAV beträgt 32767 bzw. in 802.11b-Netzwerken ungefähr 32 Millisekunden. Theoretisch muss ein Angreifer also nur etwa 30 Pakete pro Sekunde übertragen, um alle Zugriffe auf den Kanal zu blockieren.

Zugehörige Informationen

- Cisco Wireless LAN Controller der Serie 4400
- Cisco Wireless LAN Controller der Serie 4100
- Cisco Wireless LAN Controller der Serie 2000
- Signature-Engines für das Cisco Intrusion Detection System Version 3.1
- Technischer Support und Dokumentation - Cisco Systems