無線 LAN コントローラの IDS シグニチャ パラメータ

内容

概要

このドキュメントでは、Cisco ワイヤレス LAN（WLAN）コントローラ ソフトウェア リリース 3.2 およびそれよりも前のリリースで、Intrusion Detection System（IDS; 侵入検知システム）のシグニチャを設定する方法について説明しています。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、WLAN コントローラ ソフトウェア リリース 3.2 およびそれ以降のリリースに基づくものです。

表記法

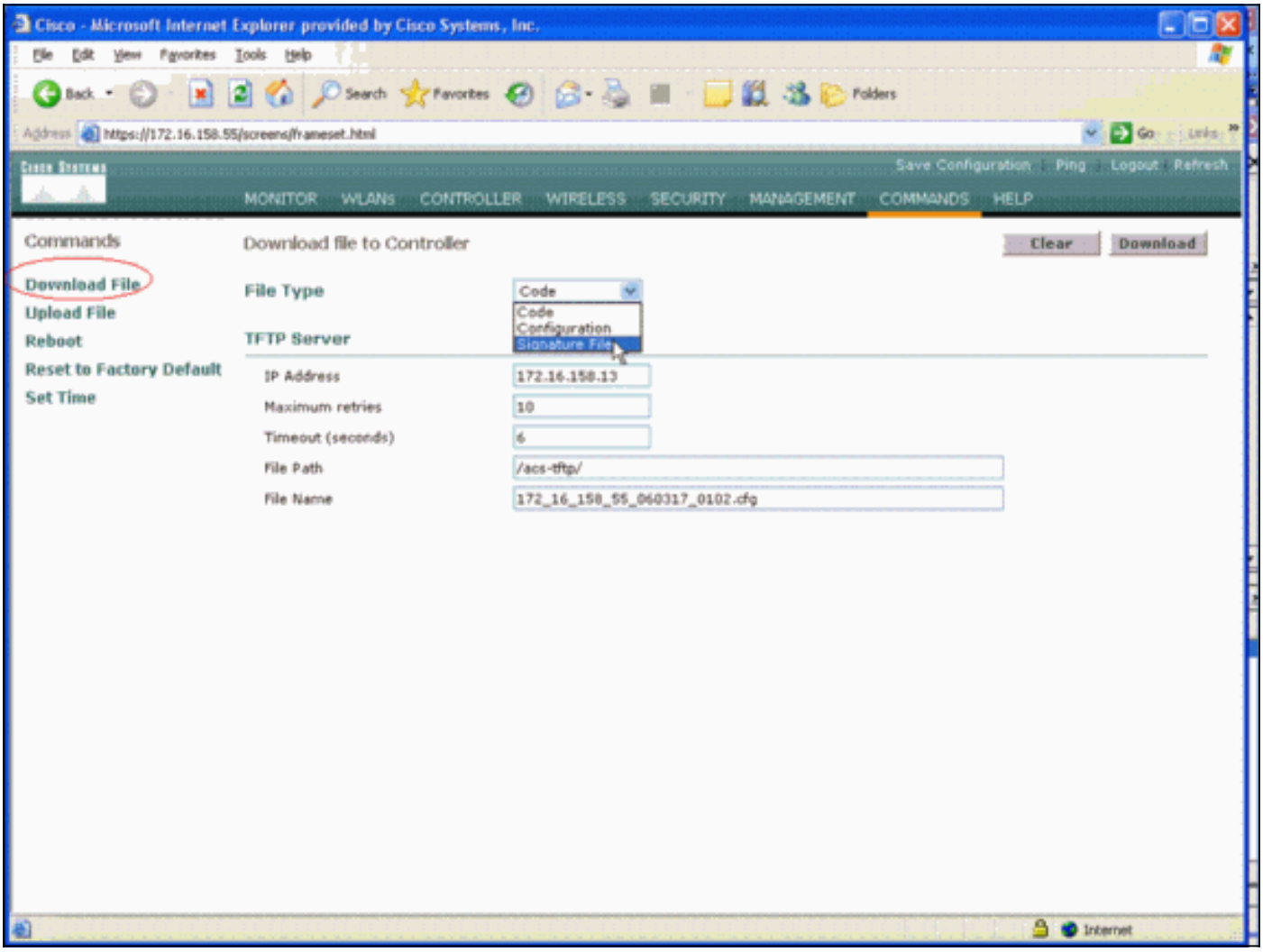
ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

背景説明

シグニチャの編集（またはドキュメントの確認）用に IDS シグニチャ ファイルのアップロードが可能です。 [Commands] > [Upload File] > [Signature File] を選択します。変更された IDS シグニ

チャ ファイルをダウンロードするには、[Commands] > [Download File] > [Signature File] を選択します。シグニチャ ファイルをコントローラにダウンロードすると、そのコントローラに接続されているすべてのアクセス ポイント（AP）が、新たに編集されたシグニチャ パラメータでリアルタイムに更新されます。

次のウィンドウはシグニチャ ファイルをダウンロードする方法を示しています。



IDS シグニチャ テキスト ファイルには、IDS シグニチャごとにパラメータが 9 つ指定されています。これらのシグニチャ パラメータを修正して、新しいカスタム シグニチャを書き込めます。このドキュメントの「コントローラの IDS パラメータ」セクションで説明されているフォーマットを参照してください。

コントローラの IDS パラメータ

すべてのシグニチャをこのフォーマットにする*必要があります。*

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

行の最大長は 1000 文字です。1000 文字を超える行は正しく解析されません。

IDS テキスト ファイル内の `#` 空白または改行だけの空白行もすべてスキップされます。コメントでも空白でもない最初の行には、`Revision` *必要があります。*Cisco から提供されたシグニチャ フ

ァイルの場合は、Revision の値を変更しないでください。Cisco ではこの値を使用してシグニチャ ファイルのリリースを管理しています。エンド ユーザが作成したシグニチャが含まれるファイルの場合は、Revision *の値を custom (* Revision = custom*必要があります。*

修正できる 9 つの IDS シグニチャ パラメータを次に示します。

- **Name** = シグニチャの名前。シグニチャを識別する一意な文字列です。名前の最大長は 20 文字です。
- **Preced** = シグニチャの優先順位。シグニチャ ファイル内に定義されているすべてのシグニチャの中でのシグニチャの優先順位を示す一意な ID です。シグニチャごとに 1 つの Preced *必要です。*
- **FrmType** = フレーム タイプ。このパラメータは <frmType-val> シグニチャごとに 1 つの FrmType *必要です。*<frmType-val> 2 mgmtdata<frmType-val>
- **Pattern** = シグニチャのパターン。このトークン値はシグニチャに一致するパケットを検出するために使用されます。シグニチャごとに 1 つの Pattern *必要です。*このトークンはシグニチャごとに最大 5 つまで指定できます。シグニチャに複数のトークンがある場合、パケットがシグニチャに一致するためには、すべてのトークンの値と一致する必要があります。AP がパケットを受信すると、AP は <offset> から始まるバイト ストリームを取得して <mask> との論理積をとり、その結果を <pattern> と比較します。一致していれば、パケットがシグニチャと一致したと見なされます。<pattern-format> !」という否定演算子を付加できます。 その場合、このセクションで説明した照合操作で一致しなかったすべてのパケットがシグニチャと一致したと見なされます。
- **Freq** = パケット数/間隔単位のパケット一致頻度。このトークンの値は、シグニチャの Action 値が 0 の場合は、パケットがシグニチャに一致すると毎回シグニチャの Action このトークンの最大値は65,535です。シグネチャごとに*Freq*トークン1必要があります。
- **Interval** = 秒単位の測定間隔。このトークンの値は、しきい値 (つまり Freq) で指定されている期間を示しています。このトークンのデフォルト値は 1 秒です。このトークンの最大値は 3600 です。
- **Quiet** = 秒単位の待機時間。このトークンの値は、シグニチャに一致するパケットをどれくらいの期間 AP が受信しないと、シグニチャが示す攻撃が沈静化したと AP が判断するかを示しています。Freq 0 シグニチャごとに 1 つの Quiet *必要です。*
- **Action** = シグニチャのアクション。このパラメータは、パケットがシグニチャに一致した場合に AP が実行する必要がある事柄を示しています。このパラメータは <action-val> シグニチャごとに 1 つの Action *必要です。*<action-val> 2 none = report =
- **Desc** = シグニチャの説明。このシグニチャの目的を説明する文字列です。シグニチャが一致したことが Simple Network Management Protocol (SNMP; 簡易ネットワーク管理プロトコル) トラップでレポートされる際に、この文字列がトラップに渡されます。説明の最大長は 100 文字です。シグニチャごとに 1 つの Desc *必要です。*

コントローラ IDS の標準シグニチャ

次の IDS シグニチャが「標準 IDS シグニチャ」としてコントローラとともに提供されています。「コントローラの IDS パラメータ」セクションで説明するように、これらのシグニチャ パラメータはすべて変更可能です。

```
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 メッセージ

ワイヤレス LAN コントローラ バージョン 4.0 では、次の IDS メッセージが表示される場合があります。

```
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
```

この IDS メッセージは、ワイヤレス 802.11 フレームの 802.11 Network Allocation Vector（NAV）フィールドが大きすぎるので、ワイヤレス ネットワークが DOS 攻撃にさらされている（または誤動作しているクライアントがある）可能性があることを示しています。

この IDS メッセージを受信したら、次に、問題を引き起こしているクライアントを追跡調査します。アクセス ポイントの周辺エリアでワイヤレス スニファを使用して信号強度に基づいてクライアントを特定するか、ロケーション サーバーを使用して位置を特定します。

NAV フィールドは 802.11 送信時の隠れターミナル（現在のワイヤレス クライアントが送信時に検知できないワイヤレス クライアント）同士の衝突を緩和するために使用される仮想キャリア検知メカニズムです。隠れターミナルがあると、アクセス ポイントには送信できるが相互には送信を受信しない 2 つのクライアントからのパケットをアクセス ポイントが受信する可能性があるので問題が発生します。これらのクライアントが同時に送信すると、アクセス ポイントでパケットが衝突し、アクセス ポイントはどちらのパケットも明瞭に受信できなくなります。

ワイヤレス クライアントがデータ パケットをアクセス ポイントに送信するときには常に、実際には RTS-CTS-DATA-ACK パケット シーケンスと呼ばれる 4 つのパケットのシーケンスを送信します。この 4 つの 802.11 フレームにはそれぞれ NAV フィールドがあり、ワイヤレス クライアントによってチャネルが予約される期間がマイクロ秒単位で示されています。ワイヤレス クライアントとアクセス ポイント間の RTS/CTS ハンドシェイク中に、シーケンス全体を完了するのに十分な長さの NAV 間隔が設定された小さな RTS フレームがワイヤレス クライアントによって送信されます。このシーケンスには、CTS フレーム、データ フレーム、およびその後のアクセス ポイントからの確認応答フレームが含まれます。

NAV が設定された RTS パケットをワイヤレス クライアントが送信すると、アクセス ポイントに関連付けられている他のすべてのワイヤレス クライアントの NAV タイマーに、その送信された値が設定されます。アクセス ポイントはクライアントからの RTS パケットに対して、パケット シーケンス中のすでに経過した時間を差し引いた新しい NAV 値が格納された CTS パケットを応答します。CTSパケットの送信後、アクセスポイントから受信できるすべてのワイヤレスクライアントはNAVタイマーを更新し、NAVタイマーが0になるまで送信を延期します。これにより、ワイヤレスクライアントはパケットをアクセスポイントに送信するプロセスを完了します。

NAV フィールドに大きな時間をアサートして攻撃者がこの仮想キャリア検知メカニズムを悪用する可能性があります。この場合、他のクライアントはパケットを送信できなくなります。NAV の最大値は 802.11b ネットワークでは 32767 つまり約 32 ミリ秒です。そのため理論上は、攻撃者が 1 秒間に約 30 個のパケットを送信するだけでチャネルのすべてのアクセスを妨害できることになります。

関連情報

- Cisco 4400 シリーズ ワイアレス LAN コントローラ
- Cisco 4100 シリーズ ワイアレス LAN コントローラ
- Cisco 2000 シリーズ ワイアレス LAN コントローラ
- Cisco Intrusion Detection System シグニチャ エンジン バージョン 3.1
- テクニカル サポートとドキュメント – Cisco Systems