無線LAN控制器IDS簽名引數

目錄

簡介

本檔案介紹如何在思科無線LAN(WLAN)控制器軟體版本3.2和較低版本中設定入侵偵測系統(IDS)簽章。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據WLAN控制器軟體版本3.2及更新版本。

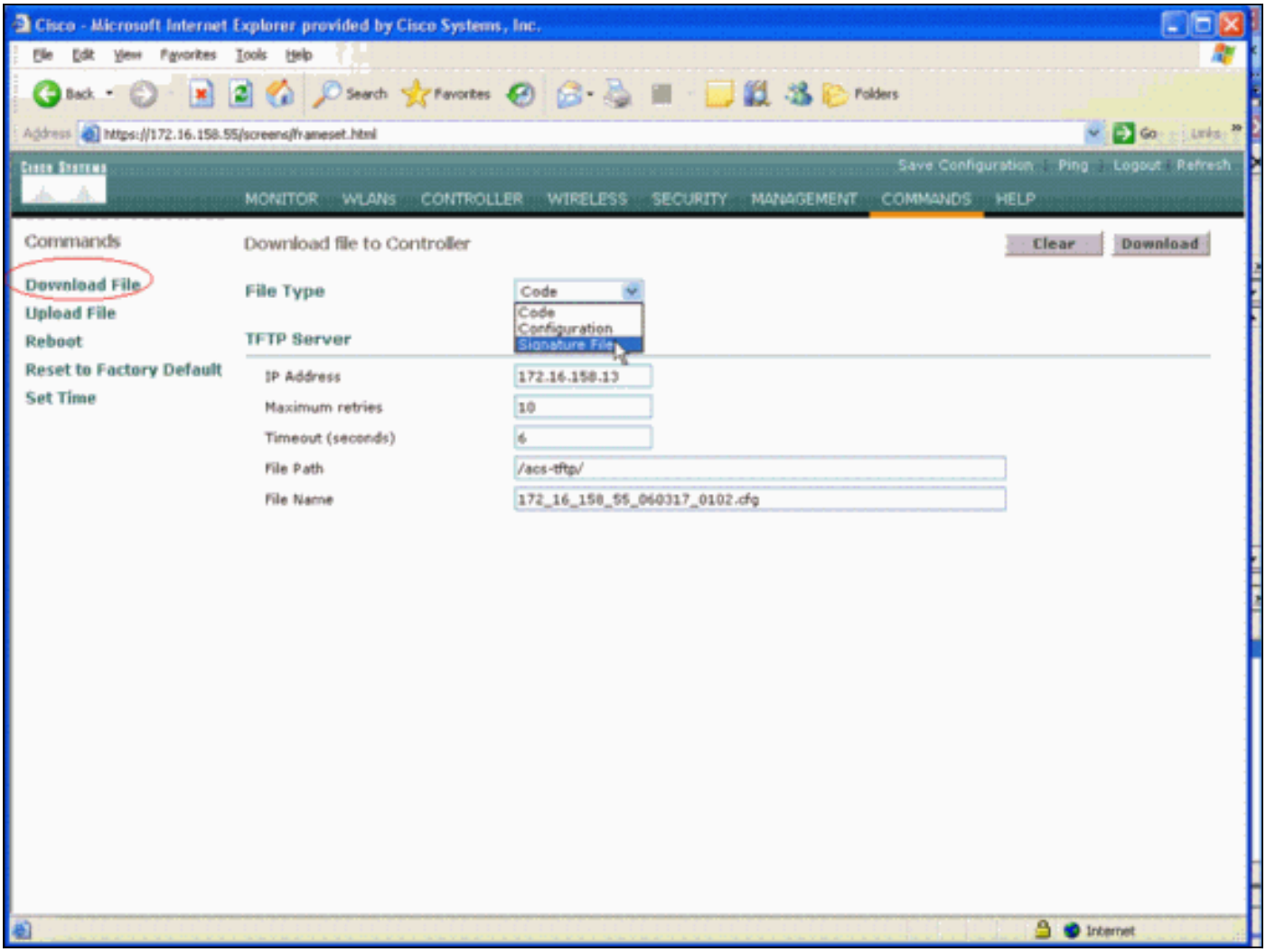
慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

背景資訊

您可以上傳IDS簽名檔案以進行簽名編輯（或檢視文檔）。 選擇**Commands > Upload File > Signature File**。要下載修改的IDS簽名檔案，請選擇**Commands > Download File > Signature File**。將簽名檔案下載到控制器後，連線到控制器的所有接入點(AP)都會使用新編輯的簽名引數即時刷新。

此視窗顯示如何下載簽名檔案：



IDS簽名文本檔案記錄每個IDS簽名的九個引數。您可以修改這些簽名引數並編寫新的自定義簽名。請參閱本文檔的控制器IDS引數部分提供的格式。

控制器IDS引數

所有簽名*必須*採用以下格式：

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

線路的最大長度為1000個字元。超過1000的線路未正確分析。

IDS文本檔案中以#開頭的所有行均被視為註釋，並會被跳過。也跳過所有空白行，這些行僅包含空格或換行符。第一個非註釋非空白行*必須*具有關鍵字`Revision`。如果該檔案是思科提供的簽名檔案，則不得更改`Revision`的值。思科使用此值管理特徵碼檔案版本。如果檔案包含終端使用者建立的簽名，則`Revision` 的值必須是custom(`Revision = custom`)。

您可以修改的九個IDS簽名引數包括：

- =簽名名稱。這是標識簽名的唯一字串。名稱的最大長度為20個字元。
- =簽名優先順序。這是一個唯一ID，表示簽名在簽名檔案中定義的所有簽名中的優先順序。每個簽名*必*須有一個令牌。
- **`FrmType`** =幀型別。此引數可以採用<`frmType-val`>值。每個簽*名必*須有一個`FrmType`標籤。

<frmType-val>只能是以下兩個關鍵字之一：<frmType-val>指示此簽名是否檢測到資料或管理幀。

- =簽名模式。令牌值用於檢測與簽名匹配的資料包。每個簽*名*必須至少有一個令牌。每個簽名最多可以有五個這樣的令牌。如果簽名有多個此類標籤，則資料包必須匹配所有標籤的值，以便資料包與簽名匹配。當AP收到資料包時，AP會獲取以<offset>開頭的位元組流，並使用<mask>進行匹配，然後將結果與<pattern>。如果AP找到匹配項，則AP會將該資料包視為與簽名匹配。<pattern-format>以加上否定運算子「。 在這種情況下，本節描述的所有匹配操作失敗的資料包都被視為與簽名匹配。
- **Freq** =資料包匹配頻率（以資料包/時間間隔為單位）。此令牌的值表示在執行簽名操作，每個測量間隔必須與此簽名匹配的資料包數。值0表示每當資料包與簽名匹配時都會採取簽名Action。此令牌的最大值為65,535。每個簽*名*必須個Freq令牌。
- =測量間隔（秒）。此令牌的值表示閾值(即Freq)指定的時間段。此權杖的預設值為1秒。此權杖的最大值為3600。
- **Quiet** =安靜時間（以秒為單位）。此令牌的值表示在AP確定簽名所指示的攻擊已經消退之前，AP必須經過多長時間，在此期間不會收到與簽名匹配的資料包。如果Freq令牌的值是0，則會忽略此令牌。每個簽名*必*須有一個Quiet令牌。
- **Action** =簽名操作。這表示如果資料包與簽名匹配，AP必須做什麼。此引數可以從<action-val>值。每個簽名*必*須有一個Action令牌。<action-val>只能是以下兩個關鍵字之一：none =什麼都不做。report =向交換機報告匹配項。
- **Desc** =簽名說明。這是一個描述簽名目的的字串。在簡單網路管理協定(SNMP)陷阱中報告特徵碼匹配時，此字串將提供給陷阱。描述的最大長度為100個字元。每個簽名*必*須有一個Desc令牌。

控制器IDS標準簽名

這些IDS簽名隨控制器一起作為「標準IDS簽名」提供。您可以修改控制器IDS引數一節介紹的所有這些特徵碼引數。

```
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訊息

使用無線LAN控制器4.0版時，可能會收到此IDS訊息。

```
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
```

此IDS消息表示無線802.11幀中的802.11 Network Allocation Vector(NAV)欄位過大，無線網路可能受到DOS攻擊（或存在行為不當的客戶端）。

收到此IDS消息後，下一步是跟蹤違規的客戶端。您必須在接入點周圍的區域使用無線嗅探器根據客戶端的訊號強度定位客戶端，或者使用定位伺服器來確定客戶端的位置。

NAV欄位是用於緩解802.11傳輸中隱藏終端（當前無線客戶端傳輸時無法檢測到的無線客戶端）之間的衝突的虛擬載波偵聽機制。隱藏的終端會產生問題，因為接入點可能從兩個客戶端接收資料包，這兩個客戶端可以傳輸到接入點，但不會接收彼此的傳輸。當這些使用者端同時傳輸時，其封包會在存取點發生衝突，導致存取點無法明確地接收任何封包。

每當無線客戶端想向接入點傳送資料包時，它實際上會傳輸一個稱為RTS-CTS-DATA-ACK資料包

序列的四個資料包序列。四個802.11幀中的每個幀都帶有指示無線客戶端為通道保留的微秒數的NAV欄位。在無線客戶端和接入點之間的RTS/CTS握手期間，無線客戶端傳送包含足夠大以完成整個序列的NAV間隔的小型RTS幀。這包括來自接入點的CTS幀、資料幀和後續確認幀。

當無線客戶端傳送具有NAV集的RTS分組時，所傳送的值用於在與接入點相關聯的所有其它無線客戶端上設定NAV計時器。接入點使用包含新的NAV值的CTS資料包來回覆來自客戶端的RTS資料包，該NAV值被更新以說明在資料包序列期間已經經過的時間。在傳送CTS資料包後，可以從接入點接收的每個無線客戶端都更新了其NAV計時器，並推遲所有傳輸，直到其NAV計時器達到0。這樣可讓無線客戶端自由完成向接入點傳輸資料包的過程。

攻擊者可通過在NAV欄位中大量宣告來利用此虛擬載波偵聽機制。這可以防止其他客戶端傳輸資料包。NAV的最大值為32767，在802.11b網路上大約為32毫秒。因此，從理論上講，攻擊者只需每秒傳輸大約30個資料包，即可阻塞對通道的所有訪問。

相關資訊

- Cisco 4400系列無線LAN控制器
- Cisco 4100系列無線LAN控制器
- Cisco 2000系列無線LAN控制器
- 思科入侵偵測系統特徵碼引擎版本3.1
- 技術支援與文件 - Cisco Systems