Wireless LAN Controller IDS Signature Parameters

Document ID: 69366

Contents

Introduction

This document describes how to configure Intrusion Detection System (IDS) signatures in Cisco Wireless LAN (WLAN) Controller software release 3.2 and earlier releases.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the WLAN Controller software release 3.2 and later.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Background Information

You can upload the IDS signature file for signature edit (or for documentation review). Choose **Commands > Upload File > Signature File**. In order to download a modified IDS signature file, choose **Commands > Download File > Signature File**. After you download a signature file to the controller, all access points (APs) that are connected to the controller are refreshed in real time with the newly edited signature parameters.

This window shows how to download the signature file:
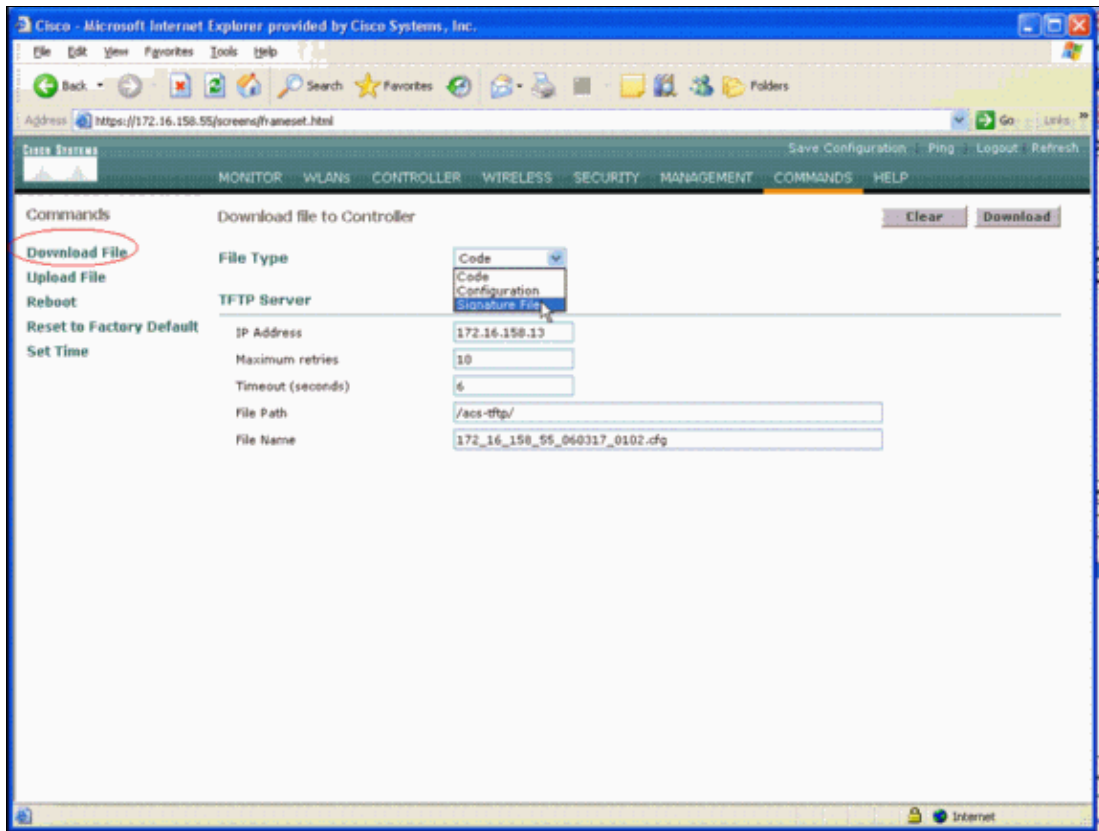
The IDS signature text file documents nine parameters for each IDS signature. You can modify these signature parameters and write new custom signatures. See the format that the Controller IDS Parameters section of this document provides.

Controller IDS Parameters

All signatures *must* have this format:

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

The maximum length of the line is 1000 characters. Lines that are longer than 1000 are not parsed correctly.

All lines that start with # in the IDS text file are considered comments and are skipped. Also skipped are all blank lines, which are lines with just whitespace or newline. The first noncomment, nonblank line *must* have the keyword Revision. If the file is a Cisco–supplied signature file, you must not change the value of Revision. Cisco uses this value to manage signature file releases. If the file contains signatures that have been created by the end user, the value of Revision *must* be custom (Revision = custom).

The nine IDS signature parameters that you can modify are:

- **Name** = signature name. This is a unique string that identifies the signature. The maximum length of the name is 20 characters.
- **Preced** = signature precedence. This is a unique ID that indicates the precedence of the signature among all the signatures that are defined in the signature file. There *must* be one Preced token per signature.
- **FrmType** = frame type. This parameter can take values from the <frmType-val> list. There *must* be one FrmType token per signature. The <frmType-val> can be one of these two keywords only:

- ♦ mgmt
- ♦ data

The `<frmType-val>` indicates if this signature detects data or management frames.
- **Pattern** = signature pattern. The token value is used to detect packets that match the signature. There *must* be at least one `Pattern` token per signature. There can be up to five such tokens per signature. If the signature has more than one such token, a packet must match the values of all the tokens in order for the packet to match the signature.

  When the AP receives a packet, the AP takes the byte stream that starts at `<offset>`, ANDs it with the `<mask>`, and compares the result with `<pattern>`. If the AP finds a match, the AP considers the packet a match with the signature. The `<pattern-format>` can be preceded by the negation operator "`!`". In that case, all packets that FAIL the match operation that this section describes are considered a match with the signature.
- **Freq** = packet match frequency in packets/interval. The value of this token indicates how many packets per measurement interval must match this signature before the signature `Action` is executed. A value of 0 indicates that the signature `Action` is taken every time that a packet matches the signature. The maximum value for this token is 65,535. There *must* be one `Freq` token per signature.
- **Interval** = measurement interval in seconds. The value of this token indicates the time period that the threshold (that is, the `Freq`) specifies. The default value for this token is 1 second. The maximum value for this token is 3600.
- **Quiet** = quiet time in seconds. The value of this token indicates the amount of time that must pass during which the AP does not receive packets that match the signature before the AP determines that the attack that the signature indicates has subsided. If the value of the `Freq` token is 0, this token is ignored. There *must* be one `Quiet` token per signature.
- **Action** = signature action. This indicates what the AP must do if a packet matches the signature. This parameter can take values from the `<action-val>` list. There *must* be one `Action` token per signature. The `<action-val>` can be one of these two keywords only:

  - ♦ `none` = do nothing.
  - ♦ `report` = report the match to the switch.
- **Desc** = signature description. This is a string that describes the purpose of the signature. When a signature match is reported in a Simple Network Management Protocol (SNMP) trap, this string is supplied to the trap. The maximum length of the description is 100 characters. There *must* be one `Desc` token per signature.

Controller IDS Standard Signatures

These IDS signatures ship with the controller as standard IDS signatures . You can modify all these signature parameters, as the Controller IDS Parameters section describes.

```
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:
                  0xffffffffffffffffffffffffffffffffffffffffffffffffffffffffffff, Freq = 1, Quiet = 600,
                  Action = report, Desc="Wellenreiter"
```

IDS Messages

With Wireless LAN Controller version 4.0, you might get this IDS message.

```
                  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
```

This IDS message indicates that the 802.11 Network Allocation Vector (NAV) field in the wireless 802.11 frame is too large and the wireless network might be under a DOS attack (or there is a misbehaving client).

After you receive this IDS message, the next step is to track down the offending client. You must locate the client based on its signal strength with a wireless sniffer in the area around the access point or use the location server to pinpoint its position.

The NAV field is the virtual carrier−sense mechanism used to mitigate collisions between hidden terminals (wireless clients the current wireless client cannot detect when it transmits) in 802.11 transmissions. Hidden terminals create problems because the access point might receive packets from two clients that can transmit to the access point but do not receive each other's transmissions. When these clients transmit at the same time, their packets collide at the access point and this results in the access point receiving neither packet clearly.

Whenever a wireless client wants to send a data packet to the access point, it actually transmits a four−packet sequence called the RTS−CTS−DATA−ACK packet sequence. Each of the four 802.11 frames carries a NAV field that indicates the number of microseconds that the channel is reserved for by a wireless client. During the RTS/CTS handshake between the wireless client and access point, the wireless client sends a small RTS frame that includes a NAV interval large enough to complete the entire sequence. This includes the CTS frame, the data frame, and the subsequent acknowledgment frame from the access point.

When the wireless client transmits its RTS packet with the NAV set, the transmitted value is used to set the NAV timers on all other wireless clients associated to the access point. The access point replies to the RTS packet from the client with a CTS packet that contains a new NAV value updated to account for the time already elapsed during the packet sequence. After the CTS packet is sent, every wireless client that can receive from the access point has updated their NAV timer and defers all transmissions until their NAV timer reaches 0. This keeps the channel free for the wireless client to complete the process of transmitting a packet to the access point.

An attacker might exploit this virtual carrier−sense mechanism by asserting a large time in the NAV field. This prevents other clients from transmitting packets. The maximum value for the NAV is 32767, or roughly 32 milliseconds on 802.11b networks. So in theory an attacker only needs to transmit roughly 30 packets a second to jam all access to the channel.

Related Information

- **Cisco 4400 Series Wireless LAN Controllers**
- **Cisco 4100 Series Wireless LAN Controllers**
- **Cisco 2000 Series Wireless LAN Controllers**
- **Cisco Intrusion Detection System Signature Engines Version 3.1**
- **Technical Support & Documentation − Cisco Systems**

Updated: May 11, 2007   Document ID: 69366