无线局域网控制器IDS签名参数

目录

简介

本文描述如何配置在Cisco无线LAN (WLAN)控制器软件版本3.2和以下版本的入侵检测系统(IDS)签名。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息根据WLAN控制器软件版本3.2和以上。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

背景信息

您能上传签名的IDS签名文件编辑(或文档回顾)。选择**命令>上传文件>签名文件**。为了下载一个已修改IDS签名文件，请选择**命令>下载File>签名文件**。在您下载签名文件到控制器后，所有接入点(AP)连接到控制器在与新编出签名参数的实时刷新。

此窗口表示如何下载签名文件：

每个IDS签名的IDS签名文本文件文档九参数。您能修改这些签名参数和写入新建的自定义签名。请参阅本文控制器IDS参数部分提供的格式。

控制器IDS参数

所有签名*必须*有此格式：

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

线路的最大长度是1000个字符。比1000长的线路没有正确地解析。

请开始#在IDS文本文件的所有线路认为注释和被跳过。并且被跳过所有空行，是有空白或换行符的线路。第一非注释， nonblank线路*必须*有关键字。如果文件是一个Cisco提供的签名文件，您不能更改值。思科使用此值管理签名文件版本。如果文件包含由最终用户创建的签名，值一定是(=)。

您能修改的九个IDS签名参数是：

- **Name**=签名名称。这是识别签名的唯一字符串。名称的最大长度是20个字符。
- **Preced** =签名优先。指示签名优先在所有签名中的在签名文件定义的这是唯一的ID。*必须*有每个签名一Preced标记。
- **FrmType** =帧类型。此参数能占用从<frmType-val>列表的值。*必须*有每个签名一FrmType标记。<frmType-val>可以只是这两个关键字之一：mgmt<frmType-val>指示此签名是否检测数据或管理帧。
- =签名模式。令牌的值用于检测匹配签名的数据包。*必须*有每个签名至少一标记。可以有每个签名五个这样令牌。如果签名有超过一这样标记，数据包必须匹配值所有令牌为了数据包能匹配签名。当AP收到数据包时， AP采取开始在<offset>， ANDs它与<mask>，并且结果与<pattern>字节流。如果AP查找一匹配， AP凝视数据包与签名的一匹配。<pattern-format>可以在相反的操作员之后“!”。在那种情况下， FAIL匹配操作此部分描述凝视与签名的一匹配的所有信息包。
- **Freq** =在数据包/间隔的数据包匹配频率。值此标记指示多少数据包每个测量间隔必须匹配此签名，在签名被执行前。值为0表明签名每次采取数据包匹配签名。此标记的最大值是65,535。*必须*有每个签名一Freq标记。
- =测量间隔以秒钟。值此标记指示阈值的时间(即Freq)指定。此标记的默认值是1秒。此标记的最大值是3600。
- =平静的时间以秒钟。值此标记指示必须通过在的时间哪些期间AP不收到匹配签名的数据包，在AP确定前签名指示消退的攻击。如果Freq标记的值是0，此标记忽略。*必须*有每个签名一标记。
- **Action**=签名操作。这指示什么AP必须执行，如果数据包匹配签名。此参数能占用从<action-val>列表的值。*必须*有每个签名一标记。<action-val>可以只是这两个关键字之一：=不执行。=报告对交换机的匹配。
- **Desc** =签名说明。这是描述签名的目的字符串。当签名匹配在简单网络管理协议(SNMP)陷阱时报告，此字符串被提供给陷阱。说明的最大长度是100个字符。*必须*有每个签名一Desc标记。

控制器IDS英文虎报签名

这些IDS签名装备控制器作为“标准的IDS签名”。因为控制器IDS参数部分描述，您能修改所有这些签名参数。

```
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消息

使用无线局域网控制器版本4.0，您也许收到此IDS消息。

```
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消息表明无线802.11帧的802.11网络分配矢量(NAV)字段太大，并且无线网络也许受到DOS攻击(或有一个行为不端的客户端)。

在您收到此IDS消息后，下一步是搜寻触犯的客户端。您必须找出根据其信号强度的客户端用一个无线嗅探器在区域在接入点附近或使用位置服务器精确定位其位置。

NAV字段是用于的虚拟载波侦听机制缓和在隐藏的终端(当前无线客户端不能检测的无线客户端之间的冲突，当传送)时802.11发射的。隐藏的终端制造问题，因为接入点也许收到从能传达给接入点的两个客户端的数据包，但是不接收彼此的发射。当这些客户端同时时传送，他们的数据包碰撞在接入点，并且这不导致清楚地接收数据包的接入点。

每当无线客户端要发送数据包到接入点，实际上传送呼叫RTS-CTS-DATA-ACK数据包序列的四个数据包顺序。四802.11帧中的每一运载指示微秒数量信道为由无线客户端保留的一个NAV字段。在无线客户端和接入点之间的RTS/CTS握手期间，无线客户端发送包括足够大NAV的间隔完成整个顺序的一小RTS帧。这包括CTS帧、数据帧和随后的确认帧从接入点。

当无线客户端传送其有设置时的NAV的RTS数据包，已发送值用于设置在其他无线客户端的NAV计时器关联对接入点。在数据包序列期间，接入点回复到从客户端的RTS数据包用包含更新的一个新的NAV值已经占时间的CTS数据包流逝了。在CTS数据包发送后，能从接入点接收的每个无线客户端更新他们的NAV计时器并且延迟所有发射，直到他们的NAV计时器到达0。这保持信道自由为了无线客户端能完成传送数据包进程对接入点。

攻击者也许通过主张大时光利用此虚拟载波侦听机制在NAV字段。这防止其他客户端传送信息包。NAV的最大值是在802.11b网络的32767或者大致32毫秒。因此在理论上攻击者只需要传送大致30数据包每秒钟阻塞对信道的所有访问。

相关信息

- Cisco 4400 系列无线局域网控制器
- Cisco 4100 系列无线局域网控制器
- Cisco 2000 系列无线局域网控制器
- Cisco入侵检测系统签名引擎版本3.1
- 技术支持和文档 - Cisco Systems