Parámetros de la firma IDS del regulador del Wireless LAN

Contenido

[Introducción](#)
[prerrequisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Antecedentes](#)
[Parámetros IDS del controlador](#)
[Firmas IDS estándar del controlador](#)
[Mensajes IDS](#)
[Información Relacionada](#)

Introducción

Este documento escribe cómo configurar firmas de Intrusion Detection System (IDS) en el software Cisco Wireless LAN (WLAN) Controller versión 3.2 y anteriores.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el Software Release 3.2 y Posterior del controlador de WLAN.

Convenciones

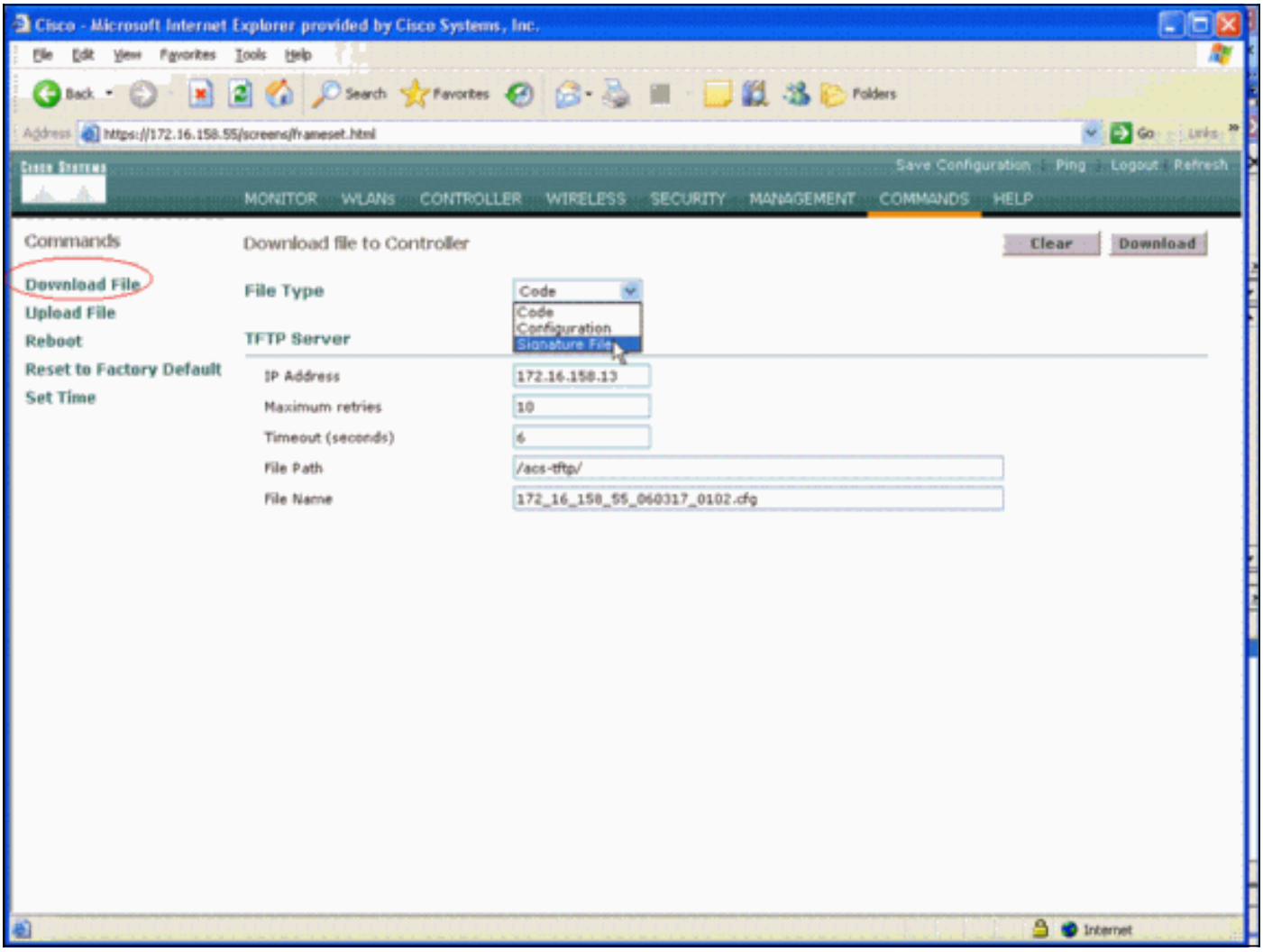
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Usted puede cargar el archivo de firma IDS para la firma edita (o para la revisión de la documentación). Elija los **comandos > el archivo > el archivo de firma de la carga**. Para descargar

un archivo de firma IDS modificado, elija los **comandos > el archivo > el archivo de firma de la descarga**. Después de que usted descargue un archivo de firma al regulador, todo el (APS) de los Puntos de acceso que está conectado con el regulador se restaura en el tiempo real con los parámetros nuevamente editados de la firma.

Esta ventana muestra cómo descargar el archivo de firma:



Los parámetros de los documentos nueve del archivo de texto de la firma IDS para cada firma IDS. Usted puede modificar estos parámetros de la firma y escribir las nuevas firmas de encargo. Vea el formato que la sección de los parámetros IDS del controlador de este documento proporciona.

Parámetros IDS del controlador

Todas las firmas *deben* tener este formato:

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

El Largo máximo de la línea es 1000 caracteres. Las líneas que son más largas de 1000 no se analizan correctamente.

Todas las líneas con las cuales comience # en el archivo de texto IDS se consideran los comentarios y se saltan. También se saltan todas las líneas vacías, que son líneas con apenas el

whitespace o el newline. El primer noncomment, línea del nonblank *debe* tener la revisión de palabra clave. Si el archivo es un archivo de firma Cisco-proveído, usted no debe cambiar el valor de la `revisión`. Cisco utiliza este valor para manejar las versiones del archivo de firma. Si el archivo contiene las firmas que han sido creadas por el usuario final, el valor de la `revisión` *debe* ser `de encargo` (`revisión = aduana`).

Los nueve parámetros de la firma IDS que usted puede modificar son:

- Nombre de la firma del **`name=`**. Ésta es una cadena única que identifica la firma. El Largo máximo del nombre es 20 caracteres.
- **`Preced`** = precedencia de firma. Éste es un ID único que indica la precedencia de la firma entre todas las firmas que se definen en el archivo de firma. *Debe* haber un `token Preced por firma`.
- **`FrmType`** = tipo de trama. Este parámetro puede tomar los valores de la lista del `<frmType-val>`. *Debe* haber un `token FrmType por firma`. `El <frmType-val>` puede ser una de estas dos palabras claves solamente:`mgmtdatosEl <frmType-val>` indica si esta firma detecta los datos o las tramas de la Administración.
- **`Modelo`** = modelo de la firma. El valor simbólico se utiliza para detectar los paquetes que hacen juego la firma. *Debe* haber por lo menos un token por firma del `modelo`. Puede haber hasta cinco tales tokenes por firma. Si la firma tiene más de un tal token, un paquete debe hacer juego los valores de todos los tokens para que el paquete haga juego la firma.Cuando el AP recibe un paquete, el AP toma el flujo de bytes que comienza en `<offset>`, los AND él con el `<mask>`, y compara el resultado con `<pattern>`. Si el AP encuentra una coincidencia, el AP considera el paquete una coincidencia con la firma. `El <pattern-format>` se puede preceder por el operador de negación "`!`". En ese caso, todos los paquetes que FALLAN la operación de la coincidencia que esta sección describe se consideran una coincidencia con la firma.
- **`Freq`** = frecuencia de coincidencia de paquetes en los paquetes/intervalo. El valor de este token indica cuántos paquetes por el intervalo de medición deben hacer juego esta firma antes de que se ejecute la acción de la firma. Un valor de 0 indica que la acción de la firma está tomada cada vez que un paquete hace juego la firma. El valor máximo para este token es 65,535. *Debe* haber un `Freq token por firma`.
- **`Intervalo`** = intervalo de medición en los segundos. El valor de este token indica el período de tiempo que el umbral (es decir, el `Freq`) especifica. El valor predeterminado para este token es 1 segundo. El valor máximo para este token es 3600.
- **`Tranquilidad`** = tiempo reservado en los segundos. El valor de este token indica la cantidad de tiempo que debe pasar durante cuál no recibe el AP los paquetes que corresponden con la firma antes de que el AP determine que el ataque que la firma indica se ha desplomado. Si el valor del `Token frecuente` es 0, se ignora este token. *Debe* haber un token por firma `reservado`.
- **`Acción`** = acción de la firma. Esto indica lo que debe hacer el AP si un paquete hace juego la firma. Este parámetro puede tomar los valores de la lista del `<action-val>`. *Debe* haber un `token de acción por firma`. `El <action-val>` puede ser una de estas dos palabras claves solamente:`ningunos` = no hacen nada.`informe` = informe la coincidencia al Switch.
- **`Desc`** = descripción de la firma. Ésta es una cadena que describe el propósito de la firma. Cuando una coincidencia de la firma está señalada en un Trap del Simple Network Management Protocol (SNMP), esta cadena se suministra al desvío. El Largo máximo de la descripción es 100 caracteres. *Debe* haber un `token Desc por firma`.

Firmas IDS estándar del controlador

Estas firmas IDS envían con el regulador como “firmas IDS estándar”. Usted puede modificar todos estos parámetros de la firma, pues la sección de los parámetros IDS del controlador describe.

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

Mensajes IDS

Con la versión 4.0 del regulador del Wireless LAN, usted puede ser que consiga este mensaje IDS.

```
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
```

Este mensaje IDS indica que el campo del vector de la asignación de la red del 802.11 (NAV) en la trama inalámbrica del 802.11 es demasiado grande y la red inalámbrica pudo estar bajo ataque DOS (o hay un cliente que se comporta mal).

Después de que usted reciba este mensaje IDS, el siguiente paso es rastrear al cliente que ofende. Usted debe localizar al cliente basado en su potencia de la señal con un sniffer inalámbrico en el área alrededor del Punto de acceso o utilizar el servidor de la ubicación para establecer claramente su posición.

El campo de NAV es el mecanismo virtual de la detección de portadora usado para atenuar las colisiones entre las terminales ocultadas (clientes de red inalámbrica que el cliente de red inalámbrica actual no puede detectar cuando transmite) en las transmisiones del 802.11. Las terminales ocultadas crean los problemas porque el Punto de acceso pudo recibir los paquetes a partir de dos clientes que pueden transmitir al Punto de acceso pero no recibe las transmisiones de cada uno. Cuando estos clientes transmiten al mismo tiempo, sus paquetes chocan en el Punto de acceso y éste da lugar al Punto de acceso que no recibe ningún paquete claramente.

Siempre que un cliente de red inalámbrica quiera enviar un paquete de datos al Punto de acceso, transmite realmente una secuencia del cuatro-paquete llamada la secuencia del paquete RTS-CTS-DATA-ACK. Cada uno de los cuatro bastidores del 802.11 lleva un campo de NAV que indique el número de microsegundos que el canal sea reservado para por un cliente de red inalámbrica. Durante el apretón de manos RTS/CTS entre el cliente de red inalámbrica y el Punto de acceso, el cliente de red inalámbrica envía una pequeña trama RTS que incluya un intervalo de NAV bastante grande para completar la secuencia entera. Esto incluye la trama CTS, el marco de datos, y la trama subsiguiente del acuse de recibo del Punto de acceso.

Cuando el cliente de red inalámbrica transmite su paquete RTS con NAV fijado, el valor transmitido se utiliza para fijar los temporizadores de NAV en el resto de los clientes de red inalámbrica asociados al Punto de acceso. El Punto de acceso contesta al paquete RTS del cliente con un paquete CTS que contenga un nuevo valor de NAV actualizado para explicar el tiempo transcurrió ya durante la secuencia del paquete. Después de que se envíe el paquete CTS, cada cliente de red inalámbrica que puede recibir del Punto de acceso ha puesto al día su temporizador de NAV y difiere todas las transmisiones hasta que su temporizador de NAV alcance 0. Esto mantiene el canal libre para que el cliente de red inalámbrica complete el proceso de transmitir un paquete al Punto de acceso.

Un atacante pudo explotar este mecanismo virtual de la detección de portadora afirmando un rato grande en el campo de NAV. Esto previene a otros clientes de los paquetes transmisores. El valor máximo para NAV es 32767, o áspero 32 milisegundos en las redes del 802.11b. Tan en la teoría un atacante necesita solamente transmitir áspero 30 paquetes al segundo para atascar todo el acceso al canal.

Información Relacionada

- Controladores LAN inalámbricos Cisco de la serie 4400
- Controladores LAN inalámbricos Cisco de la serie 4100
- Controladores LAN inalámbricos Cisco de la serie 2000
- Versión 3.1 de los motores de firma del Sistema de detección de intrusos de Cisco
- Soporte Técnico y Documentación - Cisco Systems