Parámetros de firma IDS del controlador de LAN inalámbrica

Contenido

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.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en la versión 3.2 y posterior del software del controlador WLAN.

Convenciones

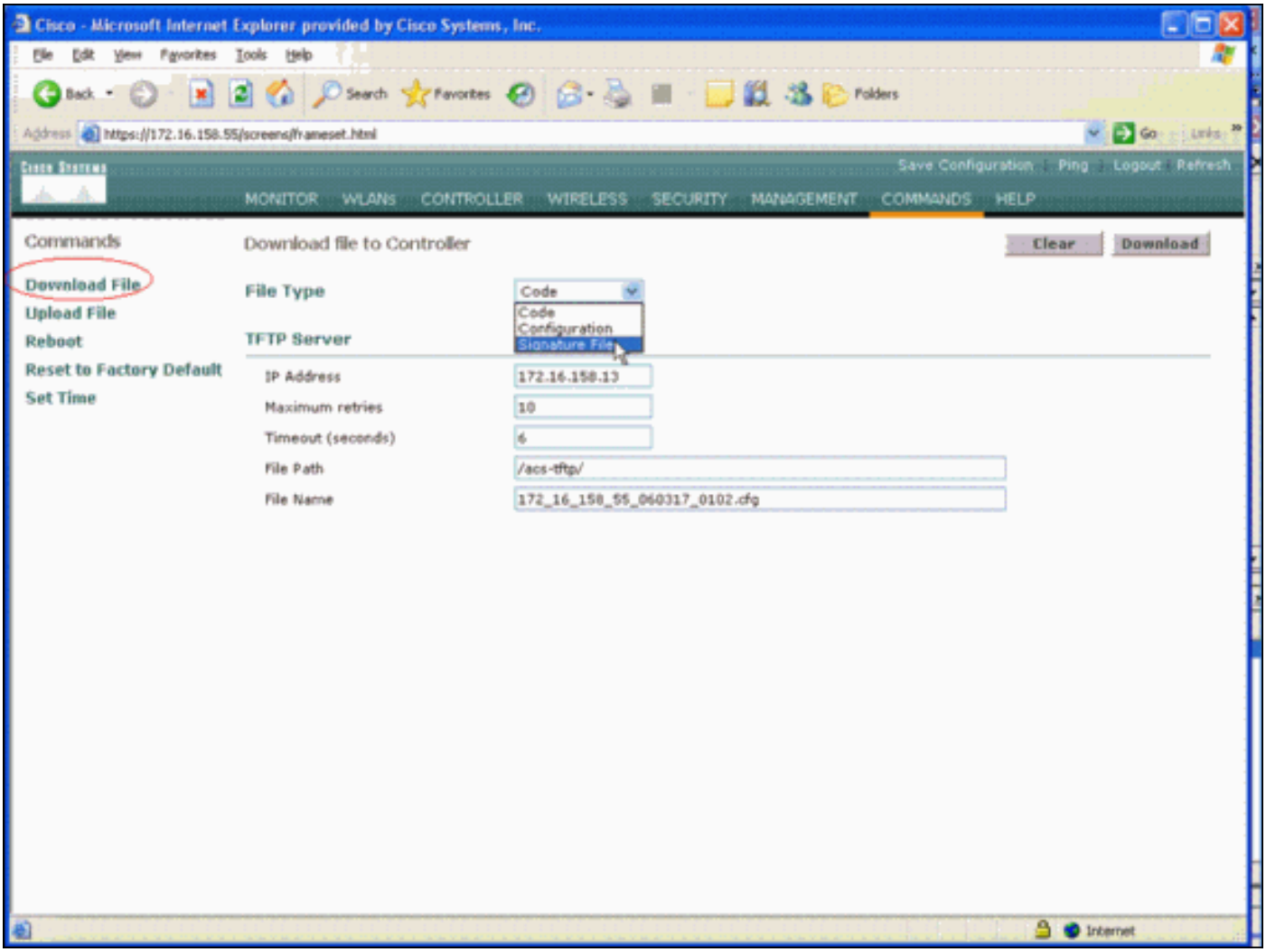
Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Puede cargar el archivo de firma IDS para la edición de firma (o para la revisión de la documentación). Elija **Commands > Upload File > Signature File**. Para descargar un archivo de

firma IDS modificado, elija **Comandos > Descargar archivo > Archivo de firma**. Después de descargar un archivo de firma al controlador, todos los puntos de acceso (AP) conectados al controlador se actualizan en tiempo real con los parámetros de firma recientemente editados.

Esta ventana muestra cómo descargar el archivo de firma:



El archivo de texto de firma IDS documenta nueve parámetros para cada firma IDS. Puede modificar estos parámetros de firma y escribir nuevas firmas personalizadas. Vea el formato que la sección 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>
```

La longitud máxima de la línea es de 1000 caracteres. Las líneas que tienen más de 1000 no se analizan correctamente.

Todas las líneas que comienzan con `#`en el archivo de texto IDS se consideran comentarios y se omiten. También se omiten todas las líneas en blanco, que son líneas con sólo espacios en blanco o líneas nuevas. La primera línea no en blanco y sin comentarios *debe* tener la palabra

clave `Revision`. Si el archivo es un archivo de firma proporcionado por Cisco, no debe cambiar el valor de `Revisión`. Cisco utiliza este valor para administrar las versiones de archivos de firma. Si el archivo contiene firmas creadas por el usuario final, el valor de `Revisión` *debe* ser `personalizado` (*Revisión = personalizada*).

Los nueve parámetros de firma IDS que puede modificar son:

- **`Nombre`** = nombre de firma. Esta es una cadena única que identifica la firma. La longitud máxima del nombre es de 20 caracteres.
- **`Preced`** = precedencia de firma. Este es un ID único que indica la precedencia de la firma entre todas las firmas definidas en el archivo de firma. Debe haber un `símbolo Preced` por firma.
- **`FrmType`** = tipo de trama. Este parámetro puede tomar valores de la lista `<frmType-val>`. Debe haber un `símbolo FormType` por firma. `<frmType-val>` sólo puede ser una de estas dos palabras clave:`mgmtdatos<frmType-val>` indica si esta firma detecta tramas de datos o de administración.
- **`Patrón`** = patrón de firma. El valor de token se utiliza para detectar los paquetes que coinciden con la firma. Debe haber al menos un `símbolo de patrón` por firma. Puede haber hasta cinco tokens por firma. Si la firma tiene más de un token de este tipo, un paquete debe coincidir con los valores de todos los tokens para que el paquete coincida con la firma.Cuando el AP recibe un paquete, el AP toma el flujo de bytes que comienza en `<offset>`, Y lo conecta con la `<máscara>` , y compara el resultado con `<patrón>`. Si el AP encuentra una coincidencia, el AP considera que el paquete coincide con la firma. El `<pattern-format>` puede ir precedido por el operador de negación "`!`". En ese caso, todos los paquetes que FALLAN la operación de coincidencia que describe esta sección se consideran coincidentes con la firma.
- **`Freq`** = frecuencia de coincidencia de paquetes en paquetes/intervalo. El valor de este token indica cuántos paquetes por intervalo de medición deben coincidir con esta firma antes de que se ejecute la `Acción` de firma. Un valor de 0 indica que la `Acción` de firma se toma cada vez que un paquete coincide con la firma. El valor máximo para este token es 65.535. Debe haber un `símbolo Freq` por firma.
- **`Intervalo`** = intervalo de medición en segundos. El valor de este token indica el período de tiempo que especifica el umbral (es decir, el `Freq`). El valor predeterminado para este token es 1 segundo. El valor máximo para este token es 3600.
- **`Silencio`** = tiempo silencioso en segundos. El valor de este token indica la cantidad de tiempo que debe pasar durante el cual el AP no recibe paquetes que coincidan con la firma antes de que el AP determine que el ataque que la firma indica ha disminuido. Si el valor del token `Freq` es 0, este token se ignora. Debe haber un `símbolo silencioso` por firma.
- **`Acción`** = acción de firma. Esto indica lo que el AP debe hacer si un paquete coincide con la firma. Este parámetro puede tomar valores de la lista `<action-val>`. Debe haber un `símbolo Action` por firma. El `<action-val>` sólo puede ser una de estas dos palabras clave:`ninguno` = no hacer nada.`informe` = informe de la coincidencia al switch.
- **`Desc`** = descripción de firma. Esta es una cadena que describe el propósito de la firma. Cuando se informa de una coincidencia de firma en una trampa SNMP, esta cadena se suministra a la trampa. La longitud máxima de la descripción es de 100 caracteres. Debe haber un `token Desc` por firma.

Firmas estándar IDS del controlador

Estas firmas IDS se envían con el controlador como "firmas IDS estándar". Puede modificar todos estos parámetros de firma, como describe la sección Parámetros IDS del controlador.

```
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"
```

Mensajes IDS

Con Wireless LAN Controller versión 4.0, puede obtener 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 de IDS indica que el campo 802.11 Network Allocation Vector (NAV) en la trama inalámbrica 802.11 es demasiado grande y la red inalámbrica puede estar bajo un ataque DOS (o hay un cliente que se comporta mal).

Después de recibir este mensaje IDS, el siguiente paso es rastrear al cliente infractor. Debe localizar el cliente en función de su potencia de señal con un sniffer inalámbrico en el área alrededor del punto de acceso o utilizar el servidor de ubicación para identificar su posición.

El campo NAV es el mecanismo virtual de detección de portadora utilizado para mitigar colisiones entre terminales ocultos (clientes inalámbricos que el cliente inalámbrico actual no puede detectar cuando transmite) en transmisiones 802.11. Los terminales ocultos crean problemas porque el punto de acceso puede recibir paquetes de dos clientes que pueden transmitir al punto de acceso pero no reciben las transmisiones de los otros. Cuando estos clientes transmiten al mismo tiempo, sus paquetes chocan en el punto de acceso y esto hace que el punto de acceso no reciba ningún paquete claramente.

Cada vez que un cliente inalámbrico desea enviar un paquete de datos al punto de acceso, en realidad transmite una secuencia de cuatro paquetes llamada secuencia de paquetes RTS-CTS-DATA-ACK. Cada una de las cuatro tramas 802.11 lleva un campo NAV que indica el número de microsegundos para los que un cliente inalámbrico reserva el canal. Durante el intercambio de señales RTS/CTS entre el cliente inalámbrico y el punto de acceso, el cliente inalámbrico envía una trama RTS pequeña que incluye un intervalo NAV lo suficientemente grande como para completar la secuencia completa. Esto incluye la trama CTS, la trama de datos y la trama de reconocimiento subsiguiente desde el punto de acceso.

Cuando el cliente inalámbrico transmite su paquete RTS con el conjunto NAV, el valor transmitido se utiliza para establecer los temporizadores NAV en todos los demás clientes inalámbricos asociados al punto de acceso. El punto de acceso responde al paquete RTS del cliente con un paquete CTS que contiene un nuevo valor NAV actualizado para tener en cuenta el tiempo que ya ha transcurrido durante la secuencia de paquetes. Después de enviar el paquete CTS, todos los clientes inalámbricos que pueden recibir desde el punto de acceso han actualizado su temporizador NAV y aplazado todas las transmisiones hasta que su temporizador NAV alcance 0. Esto mantiene el canal libre para que el cliente inalámbrico complete el proceso de transmisión de un paquete al punto de acceso.

Un atacante podría aprovechar este mecanismo virtual de detección de portadora al afirmar que se ha producido un gran aumento en el campo NAV. Esto evita que otros clientes transmitan paquetes. El valor máximo para el NAV es 32767, o aproximadamente 32 milisegundos en redes 802.11b. Por lo tanto, en teoría un atacante sólo necesita transmitir aproximadamente 30 paquetes por segundo para bloquear 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
- Cisco Intrusion Detection System Signature Engines Versión 3.1
- Soporte Técnico y Documentación - Cisco Systems