Parametri della firma IDS del controller LAN wireless

Sommario

Introduzione

In questo documento viene descritto come configurare le firme IDS (Intrusion Detection System) nel software Cisco Wireless LAN (WLAN) Controller versione 3.2 e precedenti.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Per la stesura del documento, è stato usato il software WLAN Controller versione 3.2 e successive.

Convenzioni

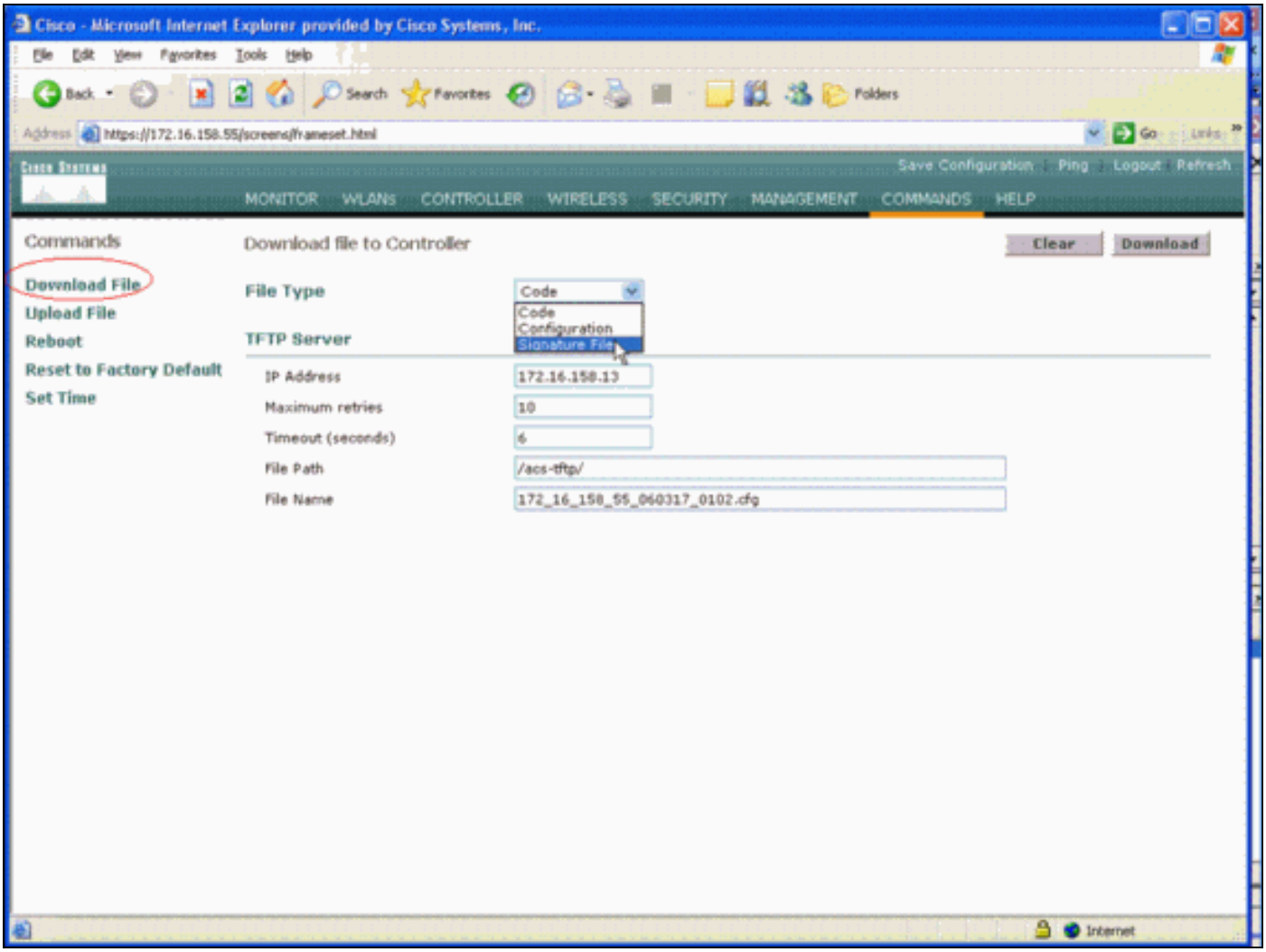
Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

È possibile caricare il file della firma IDS per la modifica della firma (o per la revisione della documentazione). Scegliere **Comandi > Carica file > File della firma**. Per scaricare un file di firma

IDS modificato, scegliere **Comandi > Scarica file > File della firma**. Dopo aver scaricato un file di firma nel controller, tutti i punti di accesso connessi al controller vengono aggiornati in tempo reale con i parametri di firma appena modificati.

In questa finestra viene illustrato come scaricare il file della firma:



Il file di testo della firma IDS contiene nove parametri per ciascuna firma IDS. È possibile modificare questi parametri di firma e scrivere nuove firme personalizzate. Vedere il formato fornito dalla sezione Parametri IDS controller di questo documento.

Parametri IDS controller

Tutte le firme *devono* avere il seguente 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 lunghezza massima della riga è di 1000 caratteri. Le righe più lunghe di 1000 non vengono analizzate correttamente.

Tutte le righe che iniziano con # nel file di testo IDS sono considerate commenti e vengono ignorate. Vengono inoltre ignorate tutte le righe vuote, ovvero le righe contenenti solo uno spazio o una nuova riga. La prima riga non vuota e senza commento *deve* contenere la parola chiave

`Revision`. Se il file è un file di firma fornito da Cisco, non è necessario modificare il valore di `Revision`. Cisco utilizza questo valore per gestire le versioni dei file delle firme. Se il file contiene firme create dall'utente finale, il valore di `Revision` deve essere `personalizzato` (`Revision = custom`).

I nove parametri di firma IDS che è possibile modificare sono:

- **`Name`** = nome della firma. Stringa univoca che identifica la firma. La lunghezza massima del nome è 20 caratteri.
- **`Preced`** = precedenza della firma. Si tratta di un ID univoco che indica la precedenza della firma tra tutte le firme definite nel file di firma. Per ogni firma *deve* essere presente un `precedente` token.
- **`FrmType`** = tipo di cornice. Questo parametro può accettare valori dall'elenco `<frmType-val>`. È *necessario* che sia presente un token `FrmType` per firma. L'elemento `<frmType-val>` può essere rappresentato solo da una delle due parole chiave seguenti:`gestionedati`Il `<frmType-val>` indica se la firma rileva frame di dati o di gestione.
- **`Pattern`** = modello di firma. Il valore del token viene utilizzato per rilevare i pacchetti che corrispondono alla firma. È *necessario* che sia presente almeno un token `Pattern` per firma. Possono essere presenti fino a cinque token per firma. Se la firma ha più di un token, un pacchetto deve corrispondere ai valori di tutti i token affinché il pacchetto corrisponda alla firma.Quando l'access point riceve un pacchetto, prende il flusso di byte che inizia in corrispondenza di `<offset>`, lo invia con la `<maschera>` e confronta il risultato con `<pattern>`. Se trova una corrispondenza, l'access point considera il pacchetto come una corrispondenza con la firma. Il `<pattern-format>` può essere preceduto dall'operatore di negazione "`!`". In questo caso, tutti i pacchetti che non superano l'operazione di corrispondenza descritta in questa sezione vengono considerati una corrispondenza con la firma.
- **`Freq`** = frequenza di corrispondenza pacchetto in pacchetti/intervallo. Il valore di questo token indica il numero di pacchetti per intervallo di misurazione che devono corrispondere alla firma prima dell'esecuzione dell'`azione di` firma. Il valore 0 indica che l'`azione` firma viene eseguita ogni volta che un pacchetto corrisponde alla firma. Il valore massimo per questo token è 65.535. *Deve* essere presente un token `Freq` per firma.
- **`Interval`** = intervallo di misurazione in secondi. Il valore di questo token indica il periodo di tempo specificato dalla soglia, ovvero il `Freq`. Il valore predefinito per questo token è 1 secondo. Il valore massimo per questo token è 3600.
- **`Quiet`** = tempo di attesa in secondi. Il valore di questo token indica il tempo che deve trascorrere prima che l'access point non riceva i pacchetti che corrispondono alla firma prima che determini che l'attacco indicato dalla firma sia cessato. Se il valore del token `Freq` è 0, il token viene ignorato. È *necessario* che sia presente un token `Quiet` per firma.
- **`Action`** = azione firma. Indica le operazioni che l'access point deve eseguire se un pacchetto corrisponde alla firma. Questo parametro può accettare valori dall'elenco `<action-val>`. Per firma *deve* essere presente un `codice Action`. L'`<action-val>` può essere solo una delle due parole chiave seguenti:`none` = nessuna operazione.`report` = rapporto sulla corrispondenza con lo switch.
- **`Desc`** = descrizione della firma. Stringa che descrive lo scopo della firma. Quando viene segnalata una corrispondenza di firma in una trap SNMP (Simple Network Management Protocol), questa stringa viene fornita alla trap. La lunghezza massima della descrizione è di 100 caratteri. Per ogni firma *deve* essere presente un token `Desc`.

Firme standard IDS controller

Queste firme IDS vengono fornite con il controller come "firme IDS standard". È possibile modificare tutti questi parametri di firma, come descritto nella sezione Parametri IDS controller.

```
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"
```

Messaggi IDS

Con Wireless LAN Controller versione 4.0, è possibile che venga visualizzato questo messaggio 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
```

Questo messaggio IDS indica che il campo NAV (Network Allocation Vector) 802.11 nel frame wireless 802.11 è troppo grande e che la rete wireless potrebbe essere sotto attacco DOS (o il client potrebbe funzionare in modo errato).

Dopo aver ricevuto questo messaggio IDS, il passaggio successivo consiste nell'individuare il client che ha causato l'errore. È necessario individuare il client in base alla potenza del segnale con uno sniffer wireless nell'area intorno al punto di accesso o utilizzare il server di posizione per individuarne la posizione.

Il campo NAV è il meccanismo di rilevamento della portante virtuale utilizzato per ridurre le collisioni tra terminali nascosti (client wireless che il client wireless corrente non è in grado di rilevare quando trasmette) nelle trasmissioni 802.11. I terminali nascosti creano problemi perché il punto di accesso potrebbe ricevere pacchetti da due client che possono trasmettere al punto di accesso ma che non ricevono le reciproche trasmissioni. Quando questi client trasmettono contemporaneamente, i loro pacchetti si scontrano sul punto di accesso e questo fa sì che il punto di accesso non riceva chiaramente alcun pacchetto.

Quando un client wireless desidera inviare un pacchetto di dati al punto di accesso, in realtà trasmette una sequenza di quattro pacchetti chiamata sequenza di pacchetti RTS-CTS-DATA-ACK. Ognuno dei quattro frame 802.11 ha un campo NAV che indica il numero di microsecondi per cui il canale è riservato da un client wireless. Durante l'handshake RTS/CTS tra il client wireless e il punto di accesso, il client wireless invia un frame RTS di piccole dimensioni che include un intervallo NAV sufficientemente grande da completare l'intera sequenza. Sono inclusi il frame CTS, il frame dati e il frame di conferma successivo dal punto di accesso.

Quando il client wireless trasmette il pacchetto RTS con il NAV impostato, il valore trasmesso viene utilizzato per impostare i timer NAV su tutti gli altri client wireless associati al punto di accesso. Il punto di accesso risponde al pacchetto RTS dal client con un pacchetto CTS contenente un nuovo valore NAV aggiornato per tenere conto del tempo già trascorso durante la sequenza del pacchetto. Dopo l'invio del pacchetto CTS, tutti i client wireless che possono ricevere dal punto di accesso hanno aggiornato il proprio timer NAV e rinviano tutte le trasmissioni fino a quando il timer NAV raggiunge 0. In questo modo, il client wireless non avrà più il diritto di completare il processo di trasmissione di un pacchetto al punto di accesso.

Un utente non autorizzato potrebbe sfruttare questo meccanismo di rilevamento della portante virtuale asserendo un tempo elevato nel campo NAV. In questo modo si impedisce ad altri client di trasmettere i pacchetti. Il valore massimo per NAV è 32767, ovvero circa 32 millisecondi sulle reti 802.11b. In teoria, un aggressore deve solo trasmettere circa 30 pacchetti al secondo per bloccare l'accesso al canale.

Informazioni correlate

- Cisco serie 4400 Wireless LAN Controller
- Cisco serie 4100 Wireless LAN Controller
- Cisco serie 2000 Wireless LAN Controller
- Cisco Intrusion Detection System Signature Engine versione 3.1
- Documentazione e supporto tecnico – Cisco Systems