무선 LAN 컨트롤러 IDS 서명 매개변수

목차

소개

이 문서에서는 Cisco WLAN(Wireless LAN) Controller 소프트웨어 릴리스 3.2 및 이전 릴리스에서 IDS(Intrusion Detection System) 서명을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 WLAN Controller 소프트웨어 릴리스 3.2 이상을 기반으로 합니다.

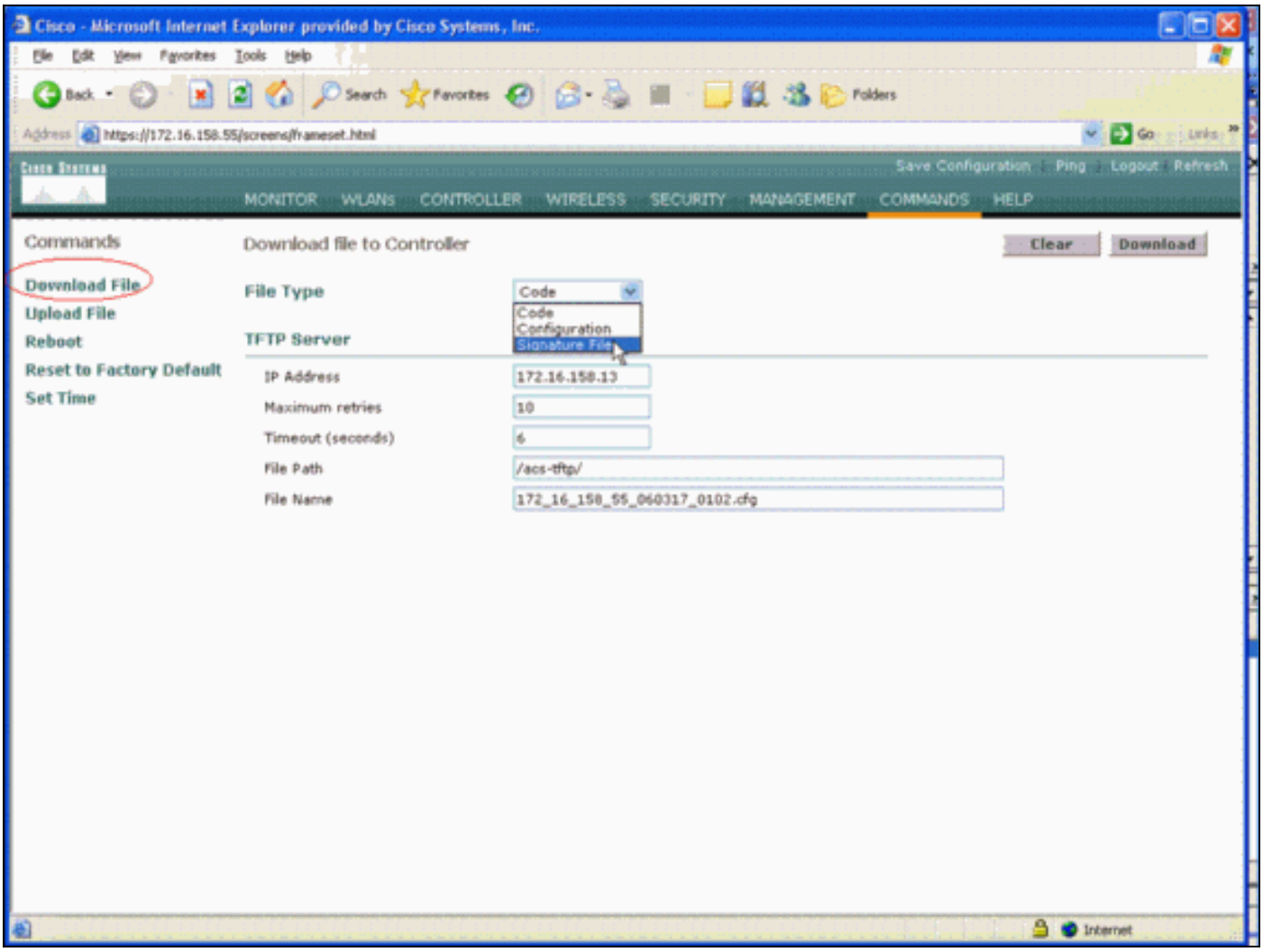
표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

서명 편집(또는 문서 검토용)을 위해 IDS 서명 파일을 업로드할 수 있습니다. Commands **> Upload File > Signature File을 선택합니다**.수정된 IDS 서명 파일을 다운로드하려면 Commands(명령) **> Download File(파일 다운로드) > Signature File(서명 파일)을** 선택합니다.컨트롤러에 시그니처 파일을 다운로드한 후 컨트롤러에 연결된 모든 액세스 포인트(AP)가 새로 편집한 시그니처 매개변수를 사용하여 실시간으로 새로 고쳐집니다.

이 창은 서명 파일을 다운로드하는 방법을 보여줍니다.



IDS 서명 텍스트 파일은 각 IDS 서명에 대해 9개의 매개 변수를 문서화합니다.이러한 서명 매개변수를 수정하고 새 사용자 지정 서명을 작성할 수 있습니다.이 문서의 Controller IDS Parameters(컨트롤러 IDS 매개변수) 섹션에서 제공하는 형식을 참조하십시오.

컨트롤러 IDS 매개변수

모든 서명은 다음 형식을 가져야 합니다.

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

최대 줄 길이는 1000자입니다.1000보다 긴 행이 올바르게 구문 분석되지 않습니다.

IDS 텍스트 파일에서 `#`으로 시작하는 모든 줄은 주석으로 간주되어 건너뜁니다.또한 생략된 줄은 모두 빈 회선이며 공백이나 줄 바꿈만 있는 줄입니다.비어 있지 않은 첫 번째 비주석 행에는 Revision 키워드*가* 있어야 .파일이 Cisco에서 제공하는 서명 파일인 경우 값을 변경하지 않아야 합니다.Cisco는 이 값을 사용하여 서명 파일 릴리스를 관리합니다.파일에 최종 사용자가 만든 서명이 포함되어 있는 경우 `Revision`의 값은 지정(`Revision = custom`)*이어야 합니다*.

수정할 수 있는 9개의 IDS 서명 매개변수는 다음과 같습니다.

- = 서명 이름입니다.시그니처를 식별하는 고유한 문자열입니다.이름의 최대 길이는 20자입니다.
- = 서명 우선 순위.시그니처 파일에 정의된 모든 시그니처 중에서 서명의 우선 순위를 나타내는 고유 ID입니다.시그니처당 하나의 `Preced` 토큰이 *있어야 합니다*.
- **`FrmType`** = 프레임 유형입니다.이 매개 변수는 `<frmType-val>` 목록에서 값을 가져올 수 있습니다.시그니처당 FrmType 토큰 하나 *있어야* 합니다.<frmType`-val`> 다음 두 키워드 중 하나일 수 있습니다.<frmType`-val`> 이 서명이 데이터 또는 관리 프레임을 탐지하는지 여부를 나타냅니다.
- = 서명 패턴토큰 값은 시그니처와 일치하는 패킷을 탐지하는 데 사용됩니다.시그니처당 토큰이 하나 이상 있어야 *합니다*.서명당 최대 5개의 해당 토큰이 있을 수 있습니다.시그니처에 이러한 토큰이 둘 이상 있는 경우 패킷이 시그니처와 일치하려면 패킷이 모든 토큰의 값과 일치해야 합니다.AP가 패킷을 수신하면 AP는 `<offset>`에서 시작하는 바이트 스트림을 `<mask>`와 가져와 `<pattern>`과 결과를 비교합니다.AP에서 일치하는 항목을 찾으면 AP는 해당 패킷을 시그니처와 일치하는 것으로 간주합니다.<pattern`-format`> 앞에 부정 연산자 "`!`"가 올 수 있습니다. 이 경우 이 섹션에서 설명하는 일치 작업에 실패한 모든 패킷은 시그니처와 일치하는 것으로 간주됩니다.
- **`Freq`** = 패킷/간격의 패킷 일치 빈도이 토큰의 값은 서명 작업이 실행되기 전에 측정 간격당 패킷 수가 이 시그니처와 일치해야 하는지 를 나타냅니다.값이 0이면 패킷이 시그니처와 일치할 때마다 시그니처 이 수행됨을 나타냅니다.이 토큰의 최대값은 65,535입니다. 시그니처당 `Freq` 토큰이 하나 *있어야 합니다*.
- = 측정 간격(초)이 토큰의 값은 임계값(즉, Freq)이 지정하는 기간을 나타냅니다.이 토큰의 기본값은 1초입니다.이 토큰의 최대값은 3600입니다.
- **`Quiet`** = 몇 초 동안 조용합니다.이 토큰의 값은 AP에서 시그니처가 나타내는 공격이 소멸되었다고 확인하기 전에 AP가 시그니처와 일치하는 패킷을 수신하지 않는 동안 전달해야 하는 시간을 나타냅니다.Freq 토큰의 값 0이면 이 토큰은 무시됩니다.서명당 하나의 `Quiet` 토큰이 *있어야 합니다*.
- = 서명 작업패킷이 시그니처와 일치할 경우 AP에서 수행해야 하는 작업을 나타냅니다.이 매개변수는 `<action-val>` 목록에서 값을 가져올 수 있습니다.시그니처당 `Action` 토큰이 하나 *있어야 합니다*.<action`-val`> 다음 두 키워드 중 하나일 수 있습니다.`none` = 아무 작업도 하지 않습니다.`report` = 스위치에 대한 일치를 보고합니다.
- **`Desc`** = 서명 설명서명의 용도를 설명하는 문자열입니다.SNMP(Simple Network Management Protocol) 트랩에서 시그니처 일치를 보고하면 이 문자열이 트랩에 제공됩니다.설명의 최대 길이는 100자입니다.시그니처당 `Desc` 토큰이 하나 *있어야* 합니다.

컨트롤러 IDS 표준 서명

이러한 IDS 서명은 컨트롤러와 함께 "표준 IDS 서명"으로 제공됩니다.Controller IDS Parameters 섹션에 설명된 대로 이러한 시그니처 매개변수를 모두 수정할 수 있습니다.

```
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 메시지

Wireless LAN Controller 버전 4.0에서는 이 IDS 메시지가 표시될 수 있습니다.

```
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
```

이 IDS 메시지는 무선 802.11 프레임의 802.11 NAV(Network Allocation Vector) 필드가 너무 커서

무선 네트워크가 DOS 공격(또는 잘못된 클라이언트)에 있을 수 있음을 나타냅니다.

이 IDS 메시지를 받은 후 다음 단계는 문제의 클라이언트를 추적하는 것입니다.액세스 포인트 주위의 영역에 무선 스니퍼를 사용하여 해당 신호 강도를 기반으로 클라이언트를 찾거나 위치 서버를 사용하여 위치를 정확히 찾아내야 합니다.

NAV 필드는 802.11 전송에서 숨겨진 터미널(현재 무선 클라이언트가 전송할 때 탐지할 수 없는 무선 클라이언트) 간의 충돌을 완화하는 데 사용되는 가상 캐리어 감지 메커니즘입니다.액세스 포인트는 액세스 포인트로 전송할 수 있지만 서로의 전송을 수신하지 않는 두 클라이언트에서 패킷을 받을 수 있으므로 숨겨진 터미널은 문제를 발생시킵니다.이러한 클라이언트가 동시에 전송되면 해당 패킷이 액세스 포인트에서 충돌하여 액세스 포인트가 두 패킷을 명확히 수신하지 못하게 됩니다
.

무선 클라이언트가 데이터 패킷을 액세스 포인트로 전송하려면 실제로 RTS-CTS-DATA-ACK 패킷 시퀀스라는 4개의 패킷 시퀀스를 전송합니다.4개의 802.11 프레임 각각에는 무선 클라이언트에서 채널이 예약되는 마이크로초의 수를 나타내는 NAV 필드가 있습니다.무선 클라이언트와 액세스 포인트 간의 RTS/CTS 핸드셰이크 동안 무선 클라이언트는 전체 시퀀스를 완료할 수 있을 만큼 큰 NAV 간격을 포함하는 작은 RTS 프레임을 전송합니다.여기에는 CTS 프레임, 데이터 프레임 및 액세스 포인트의 후속 승인 프레임이 포함됩니다.

무선 클라이언트가 NAV 세트로 RTS 패킷을 전송하면 전송된 값을 사용하여 액세스 포인트에 연결된 다른 모든 무선 클라이언트에서 NAV 타이머를 설정합니다.액세스 포인트는 CTS 패킷을 사용하여 클라이언트에서 RTS 패킷에 응답합니다. 이 패킷은 패킷 시퀀스 중에 이미 경과한 시간을 고려하여 업데이트되는 새 NAV 값을 포함합니다.CTS 패킷이 전송되면 액세스 포인트에서 수신할 수 있는 모든 무선 클라이언트가 NAV 타이머를 업데이트하고 NAV 타이머가 0에 도달할 때까지 모든 전송을 연기합니다. 이렇게 하면 무선 클라이언트가 액세스 포인트에 패킷을 전송하는 프로세스를 완료할 수 있도록 채널을 자유롭게 유지합니다.

공격자는 NAV 필드에서 많은 시간을 어설션하여 이 가상 캐리어 감지 메커니즘을 악용할 수 있습니다.이렇게 하면 다른 클라이언트가 패킷을 전송할 수 없습니다.NAV의 최대값은 32767이며, 802.11b 네트워크에서는 약 32밀리초입니다.따라서 이론적으로 공격자는 채널에 대한 모든 액세스를 차단하려면 초당 약 30개의 패킷을 전송해야 합니다.

관련 정보

- Cisco 4400 Series Wireless LAN Controller
- Cisco 4100 Series Wireless LAN Controller
- Cisco 2000 Series Wireless LAN Controller
- Cisco Intrusion Detection System Signature Engine 버전 3.1
- 기술 지원 및 문서 – Cisco Systems