Параметры сигнатуры IDS контроллера беспроводной LAN

Содержание

Введение

Этот документ описывает способ настройки подписи системы обнаружения вторжений (IDS) в беспроводной локальной сети Cisco (WLAN) с выпуском ПО контроллера WLC 3.2 и предыдущими версиями.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Сведения в этом документе основываются на выпуске ПО Контроллера беспроводной локальной сети 3.2 и позже.

Условные обозначения

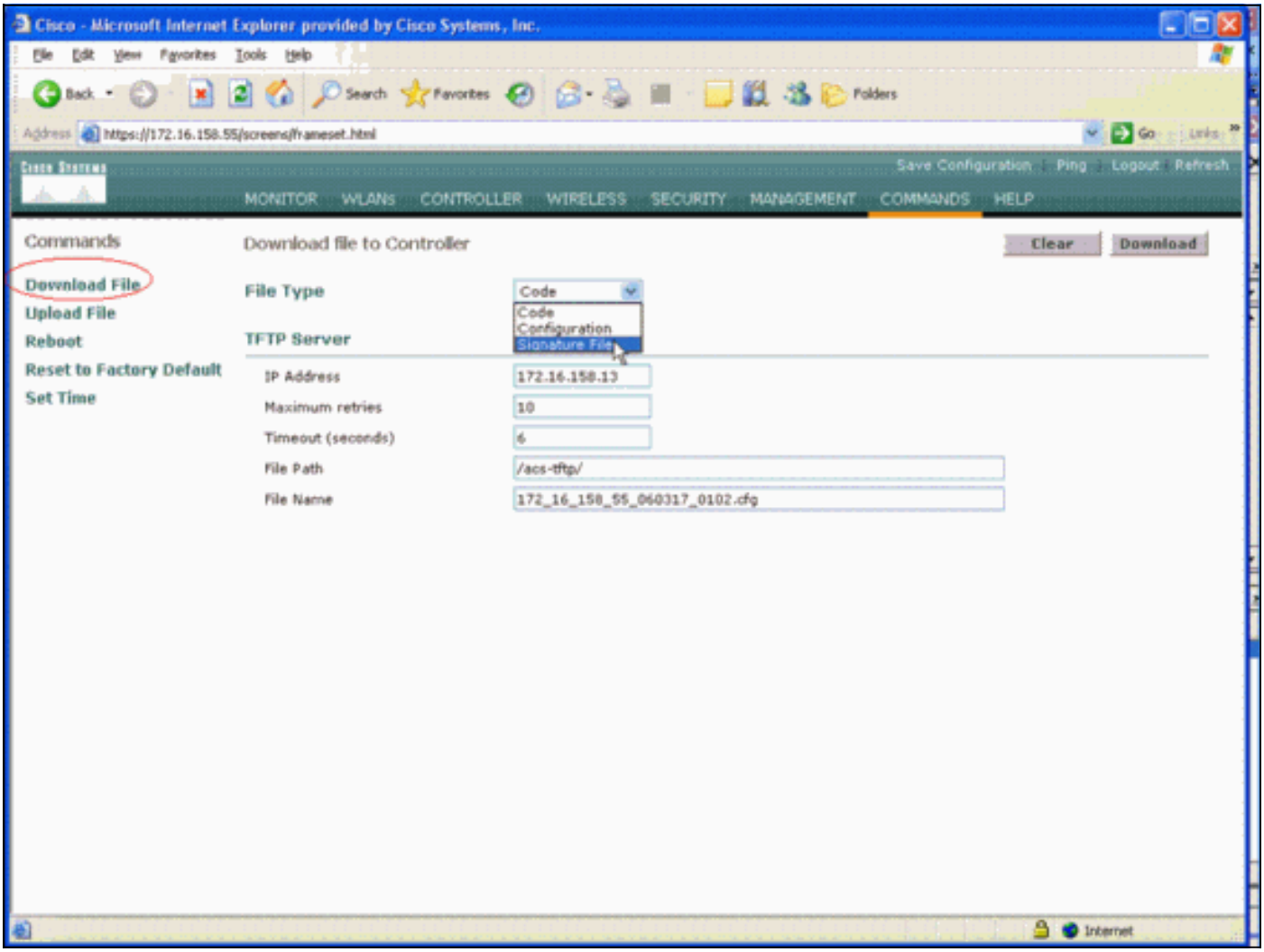
Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Общие сведения

Можно загрузить файл Подписи IDS для подписи, редактируют (или для обзора

документации). Выберите **Commands> Upload File> Signature File**. Для загрузки модифицированного файла Подписи IDS выберите **Commands> Download File> Signature File**. После загрузки Файла цифровой подписи к контроллеру все точки доступа (AP), которые связаны с контроллером, обновлены в режиме реального времени с недавно отредактированными параметрами подписи.

Это окно показывает, как загрузить Файл цифровой подписи:



Документы текстового файла Подписи IDS девять параметров для каждой Подписи IDS. Можно модифицировать эти параметры подписи и записать новые пользовательские подписи. Посмотрите формат, который предоставляет раздел Параметров контроллера IDS этого документа.

Параметры контроллера IDS

Все подписи *должны* иметь этот формат:

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

Максимальная длина линии составляет 1000 символов. Линии, которые более длинны, чем 1000, не проанализированы правильно.

Все линии, которые запускаются с # в текстовом файле IDS, считают комментариями и

пропускают. Также пропущенный все пустые строки, которые являются линиями только с пробелом или новой строкой. Первый некомментарий, непустая линия *должна* иметь ключевое слово `Revision`. Если файл является предоставленным Cisco Файлом цифровой подписи, вы не должны изменять значение `Revision`. Cisco использует это значение для управления версиями Файла цифровой подписи. Если файл содержит подписи, которые были созданы конечным пользователем, значением `Revision` *должен* быть `custom` (`Revision = custom`).

Девять параметров Подписи IDS, которые можно модифицировать:

- **`Name`** = название подписи. Это - уникальная строка, которая определяет подпись. Максимальная длина названия составляет 20 символов.
- **`Preced`** = приоритет подписи. Это - уникальный идентификатор, который указывает на приоритеты подписи среди всех подписей, которые определены в Файле цифровой подписи. *Должен* быть один маркер в сигнатуре `Preced`.
- **`FrmType`** = тип фрейма. Этот параметр может принять значения из списка `<frmType-val>`. *Должен* быть один маркер в сигнатуре `FrmType`. `<frmType-val>` может быть одним из этих двух ключевых слов только:`mgmtdata<frmType-val>` указывает, обнаруживает ли эта подпись фреймы данных или кадры управления.
- **`Pattern`** = образец подписи. Символическая стоимость используется для обнаружения пакетов, которые совпадают с подписью. *Должен* быть по крайней мере один маркер в сигнатуре `Pattern`. Может быть до пяти таких маркеров в сигнатуре. Если подпись имеет несколько таких маркеров, пакет должен совпасть со значениями всех маркеров для пакета для соответствия с подписью.Когда AP получает пакет, AP берет поток байтов, который запускается в `<offset>`, ANDs это с `<mask>`, и сравнивает результат с `<pattern>`. Если AP находит соответствие, AP считает пакет соответствием с подписью. `<pattern-format>` может предшествовать оператор отрицания "`!`". В этом случае все пакеты, которые ОТКАЗЫВАЮТ операцию соответствия, которую описывает этот раздел, считают соответствием с подписью.
- **`Freq`** = частота совпадения пакетов в пакетах/интервале. Значение этого маркера указывает, сколько пакетов на интервал измерения должно совпасть с этой подписью перед подписью, `Action` выполняется. Значение 0 указывает, что подпись, `Action` взят каждый раз, когда пакет совпадает с подписью. Максимальное значение для этого маркера 65,535. *Должен* быть один маркер в сигнатуре `Freq`.
- **`Interval`** = интервал измерения в секундах. Значение этого маркера указывает на период времени, который задает порог (т.е. `Freq`). Значение по умолчанию для этого маркера составляет 1 секунду. Максимальное значение для этого маркера 3600.
- **`Quiet`** = спокойное время в секундах. Значение этого маркера указывает на период времени, который должен пройти, во время которого AP не получает пакеты, которые совпадают с подписью, прежде чем AP решит, что спала атака, на которую указывает подпись. Если значение маркера `Freq` 0, этот маркер проигнорирован. *Должен* быть один маркер в сигнатуре `Quiet`.
- **`Action`** = действие подписи. Это указывает на то, что должен сделать AP, если пакет совпадает с подписью. Этот параметр может принять значения из списка `<action-val>`. *Должен* быть один маркер в сигнатуре `Action`. `<action-val>` может быть одним из этих двух ключевых слов только:`none` = ничего не делает.`report` = сообщает о соответствии коммутатору.
- **`Desc`** = описание сигнатуры. Это - строка, которая описывает цель подписи. Когда о соответствии подписи сообщают в Перехвате простого протокола управления сетью

(SNMP), эта строка предоставлена trap-сообщению. Максимальная длина описания составляет 100 символов. *Должен* быть один маркер в сигнатуре `Desc`.

Стандартные сигнатуры контроллера IDS

Эти Подписи IDS отправляют с контроллером как “стандартные Подписи IDS”. Можно модифицировать все эти параметры подписи, как раздел Параметров контроллера IDS описывает.

```
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"
```

Сообщения IDS

С версией 4.0 Контроллера беспроводной локальной сети вы могли бы получить это сообщение 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
```

Это сообщение IDS указывает, что поле Network Allocation Vector (NAV) 802.11 в беспроводном кадре 802.11 является слишком большим, и беспроводная сеть могла бы находиться под DOS - атакой (или существует клиент с некорректным поведением).

После получения этого сообщения IDS следующий шаг должен разыскать незаконного клиента. Необходимо определить местоположение клиента на основе его уровня сигнала с беспроводным анализатором пакетов в области вокруг точки доступа или использовать сервер местоположения для точного определения его позиции.

Поле NAV является действительным механизмом с обнаружением несущей, используемым для смягчения коллизий между скрытыми терминалами (беспроводные клиенты, которых не может обнаружить текущий беспроводной клиент, когда это передает) в передачах 802.11. Скрытые терминалы создают проблемы, потому что точка доступа могла бы получить пакеты от двух клиентов, которые могут передать к точке доступа, но не получают передачи друг друга. Когда эти клиенты передают в то же время, их пакеты сталкиваются в точке доступа, и это приводит к точке доступа, получающей никакой пакет ясно.

Каждый раз, когда беспроводной клиент хочет передать пакет данных к точке доступа, это фактически передает последовательность с четырьмя пакетами, названную RTS-CTS-DATA-ACK пакетной последовательностью. Каждый из четырех кадров 802.11 несет поле NAV, которое указывает на количество микросекунд, что канал зарезервирован для беспроводным клиентом. Во время квитирования RTS/CTS между беспроводным клиентом и точкой доступа, беспроводной клиент передает маленький кадр RTS, который включает интервал NAV, достаточно большой для завершения всей последовательности. Это включает кадр CTS, фрейм данных и последующий кадр подтверждения от точки доступа.

Когда беспроводной клиент передает его пакет RTS с набором NAV, переданное значение используется для установки таймеров NAV на всех других беспроводных клиентах, привязанных к точке доступа. Точка доступа отвечает на пакет RTS от клиента с пакетом CTS, который содержит новое значение NAV, обновленное для составления времени, уже истек во время пакетной последовательности. После того, как пакет CTS передан, каждый беспроводной клиент, который может получить от точки доступа, обновил их таймер NAV и отсрочивает все передачи, пока их таймер NAV не достигает 0. Это поддерживает канал свободным для беспроводного клиента завершить процесс передачи пакета к точке

доступа.

Атакующий мог бы использовать этот действительный механизм с обнаружением несущей путем утверждения большого времени в поле NAV. Это предотвращает других клиентов от передаваемых пакетов. Максимальное значение для NAV 32767, или примерно 32 миллисекунды на 802.11b сети. Таким образом в теории атакующий только должен передать примерно 30 пакетов в секунду для затора всего доступа к каналу.

Дополнительные сведения

- Контроллеры беспроводных LAN серии Cisco 4400
- Cisco 4100 Series Wireless LAN Controllers
- Контроллеры беспроводных LAN серии Cisco 2000
- Версия 3.1 устройств для подписи Cisco Intrusion Detection System
- Cisco Systems – техническая поддержка и документация