Cisco Адаптивная wIPS Конфигурация Расширенного автономного режима (ELM) и Руководство по развертыванию

Содержание

Введение

Cisco Адаптивная беспроводная Система предотвращения вторжений (wIPS) решение добавляет опцию Расширенного автономного режима (ELM), позволяя администраторам использовать их развернутые точки доступа (AP) для обеспечивания всесторонней защиты без потребности в отдельной оверлейной сети (рисунок 1). До ELM и в традиционных Адаптивных wIPS развертываниях, выделенные AP режима отслеживания (MM) требуются, чтобы предоставлять потребности Соответствия PCI или защиту от неавторизованной безопасности доступа, проникновения и атак (рисунок 2). ELM фактически реализует сопоставимое решение, которое упрощает обеспечение безопасности беспроводной сети при снижении капитальных и эксплуатационных затрат. Этот документ только фокусируется на ELM и не модифицирует существующих wIPS преимуществ развертываний с AP MM.

Рисунок 1 - расширенные развертывания точки доступа в локальном режиме

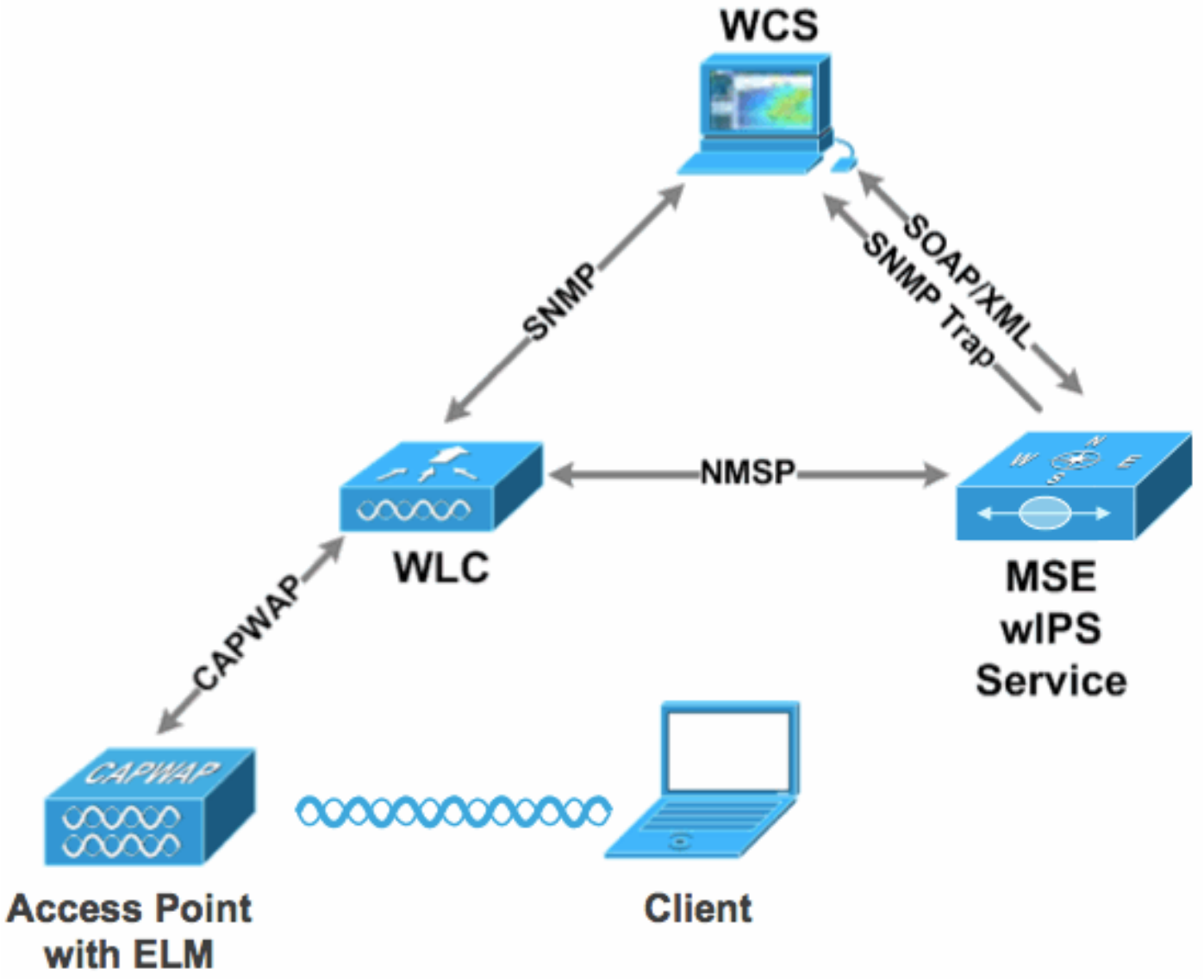
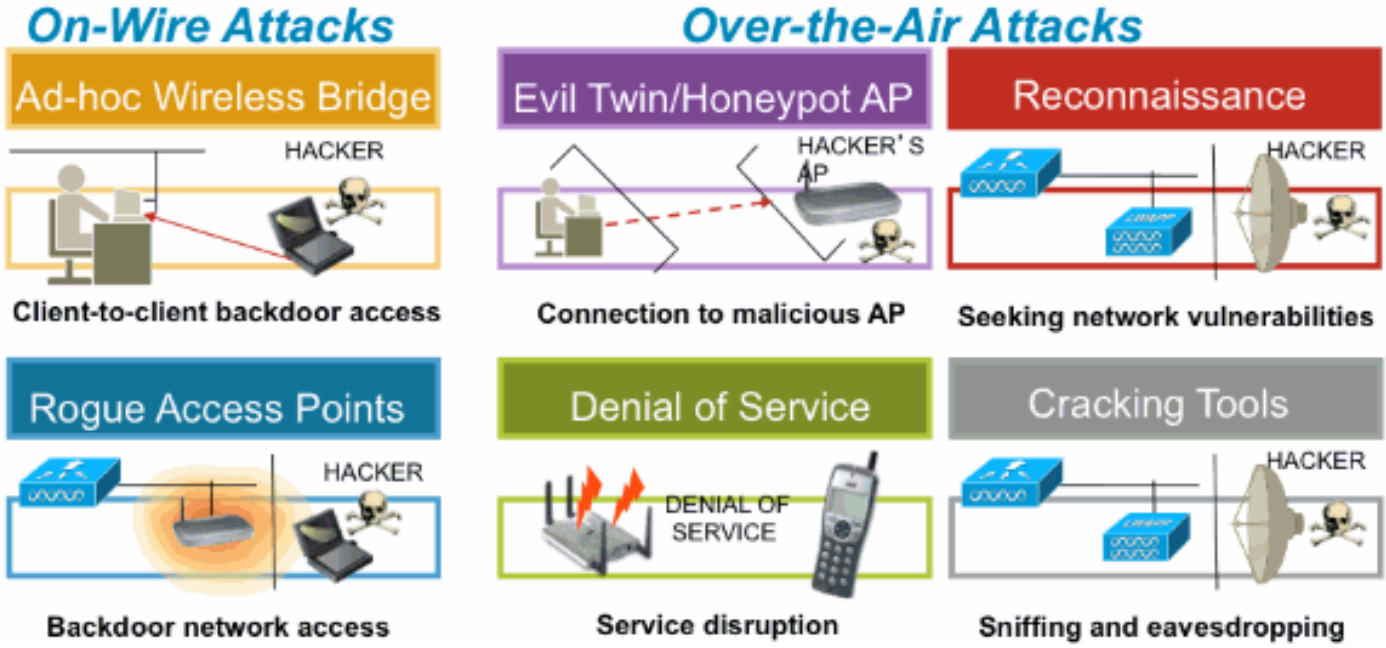


Рисунок 2 - главные угрозы безопасности беспроводной связи



Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Требуемые компоненты ELM и версии минимального кода

- Контроллер беспроводной локальной сети (WLC) - Версия 7.0.116.xx или позже
- AP - Версия 7.0.116.xx или позже
- Wireless Control System (WCS) - Версия 7.0.172.xx или позже
- Cisco Mobility Services Engine - Версия 7.0.201.xx или позже

Поддержка платформ WLC

ELM поддерживается на WLC5508, WLC4400, WLC 2106, WLC2504, WiSM 1 и платформах WiSM-2WLC.

Поддержка AP

ELM поддерживается на 11n AP включая 3500, 1250, 1260, 1040, и 1140.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

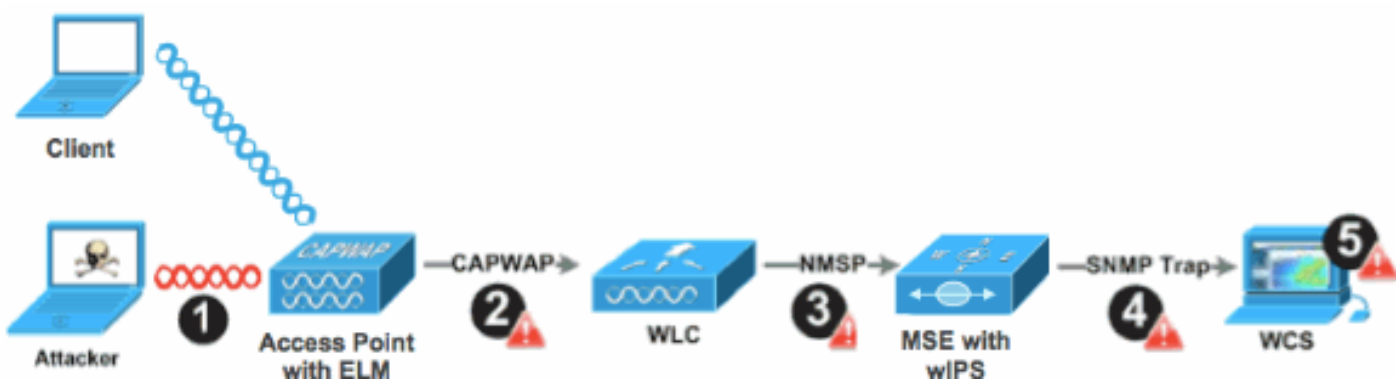
Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

Поток аварийных сигналов ELM wIPS

Атаки только релевантны, когда они происходят на доверяемых AP инфраструктуры. AP ELM обнаружат и свяжутся с контроллером и коррелятом с MSE для создания отчетов с управлением WCS. Рисунок 3 предоставляет поток аварийных сигналов с точки зрения администратора:

1. Атака запустила против устройства, относящегося к инфраструктуре ("доверял" AP),
2. Обнаруженный на AP ELM связался через CAPWAP с WLC
3. Переданный прозрачно к MSE через NMSP
4. Вошедший wIPS База данных по MSE, Передаваемому WCS через trap-сообщение SNMP
5. Отображенный в WCS

Рисунок 3 - обнаружение угрозы и поток аварийных сигналов



Вопросы развертывания для ELM

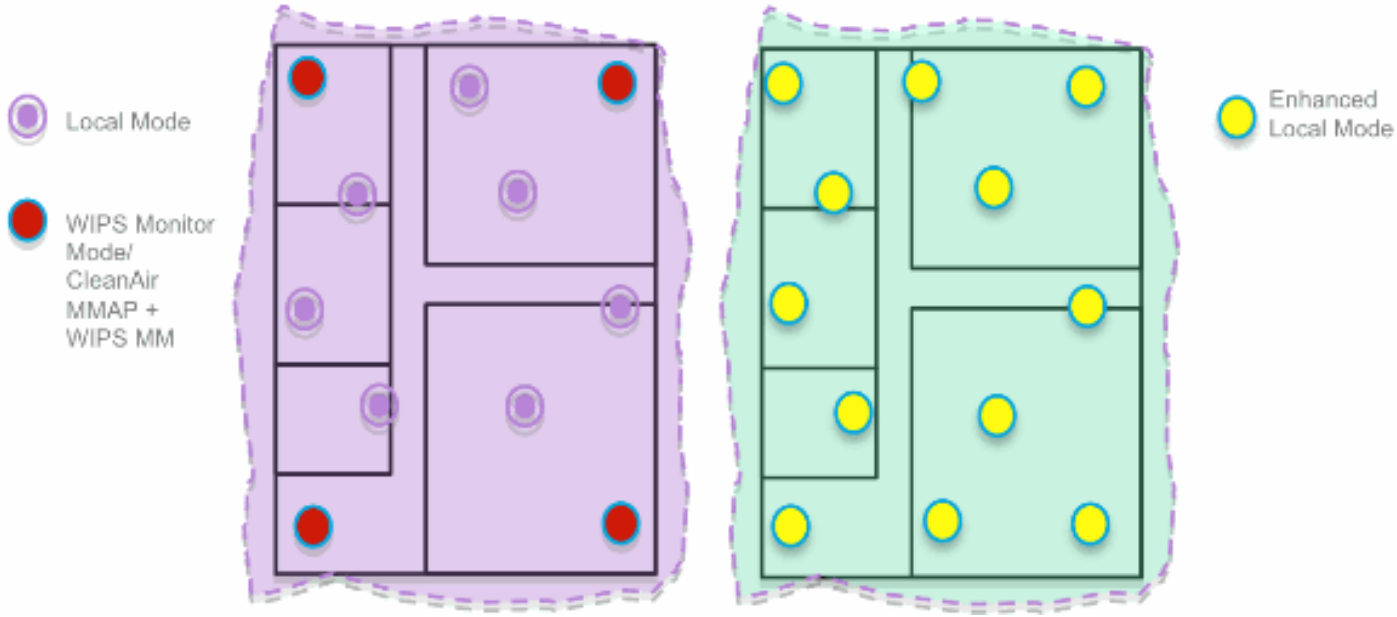
Cisco рекомендует, чтобы путем включения ELM на каждом AP в сети удовлетворили большинство потребностей безопасности клиента, когда сетевое наложение и/или затраты являются частью рассмотрения. ELM основная функция работает эффективно для атак на канале, без любого компромисса к производительности на данных, голосе и видео клиентах и сервисах.

ELM по сравнению со специализированным MM

Рисунок 4 предоставляет общий контраст между стандартными развертываниями AP wIPS MM и ELM. В анализе предлагает типичная зона охвата для режимов Both:

- Специализированный wIPS MM AP, как правило, покрывает 15 000-35 000 квадратных футов
- Служащий клиенту AP будет, как правило, покрывать от 3 000-5 000 квадратных футов

Рисунок 4 - наложение MM по сравнению со всеми AP ELM



В традиционных Адаптивных wIPS развертываниях Cisco рекомендует соотношение AP на 1 MM к каждым 5 AP автономного режима, которые могут также варьироваться на основе организации сети и опытного руководства лучшим покрытием. Путем рассмотрения ELM администратор просто включает программную характеристику ELM для всех существующих AP, эффективно добавляя MM wIPS операции к служащему локальным данным AP режима

при поддержании производительности.

Производительность вне канала и на канале

AP MM использует 100% времени радио для сканирования всех каналов, поскольку это не служит никаким клиентам WLAN. Основная функция ELM работает эффективно для атак на канале, без любого компромисса к производительности на данных, голосе и видео клиентах и сервисах. Основное различие находится в автономном режиме, варьирующемся сканирование вне канала; в зависимости от действия сканирование вне канала предоставляет минимальный, живут время для сбора достаточного количества доступной информации, чтобы классифицировать и определить атаку. Пример может быть с речевыми клиентами, которые привязаны и где сканирование RRM AP отсрочено, пока речевой клиент не разъединен, чтобы удостовериться, что не влияют на сервис. Для этого рассмотрения обнаружение ELM во время вне канала считают оптимальным уровнем. Гранича с AP ELM, воздействующими на все, каналы страны или DCA увеличивают эффективность, следовательно рекомендация для включения ELM на каждой точке доступа в локальном режиме для покрытия максимальной защиты. Если требование для специализированного сканирования на всем полном рабочем дне каналов, рекомендация будет состоять в том, чтобы развернуть AP MM.

Эти точки рассматривают различия AP MM и автономного режима:

- Точка доступа в локальном режиме - Служит клиентам WLAN с квантованием времени сканирование вне канала, прислушивается к 50 мс на каждом канале и функциям конфигурируемое сканирование для all/country/DCA каналов.
- Точка доступа в режиме мониторинга - Не служит клиентам WLAN, выделенным сканированию только, прислушивается к 1.2 с на каждом канале и просматривает все каналы.

ELM через каналы WAN

Cisco сделала большие усилия для оптимизации функций в стимулирующих сценариях, таких как развертывающиеся AP ELM через низкую пропускную способность каналы WAN. Функция ELM вовлекает предварительную обработку в определение подписей атаки в AP и оптимизирована для переработки медленных соединений. Как оптимальные методы, рекомендуется протестировать и измерить срок для проверки производительности с ELM по глобальной сети (WAN).

Интеграция CleanAir

Функция ELM высоко поздравление операции CleanAir с подобной производительностью и преимуществами к развертываниям AP MM с этими существующими CleanAir осведомленные о спектре преимущества:

- Специализированный интеллект RF кремниевого уровня
- Осведомленный о спектре, самовосстановление и самооптимизация
- Нестандартная угроза канала и интерференционное обнаружение и смягчение
- Обнаружение Wi-Fi non, такое как Bluetooth, микроволна, беспроводные телефоны, и т.д.

- Обнаружьте и найдите DOS - атаки уровня RF, такие как передатчики помех RF

Функции и преимущества ELM

- Адаптивный wIPS, просматривающий в данных, служащих локальному и AP H-REAP
- Защита, не требуя отдельной оверлейной сети
- Доступный как свободная SW загрузка для существующих wIPS клиентов
- Соответствие PCI поддержек для беспроводных локальных сетей
- Полный 802.11 и обнаружение атак не802.11
- Добавляют судебная экспертиза и создание отчетов о возможностях
- Интегрируется с существующим CUWM и управлением WLAN
- Гибкость для установки интегрированных или выделенных AP MM
- Предварительная обработка в AP минимизирует обратный рейс данных (т.е. перерабатывает очень каналы с низкой пропускной способностью),
- Низкое влияние на служащие данные

Лицензирование ELM

ELM wIPS добавляет новую лицензию на заказ:

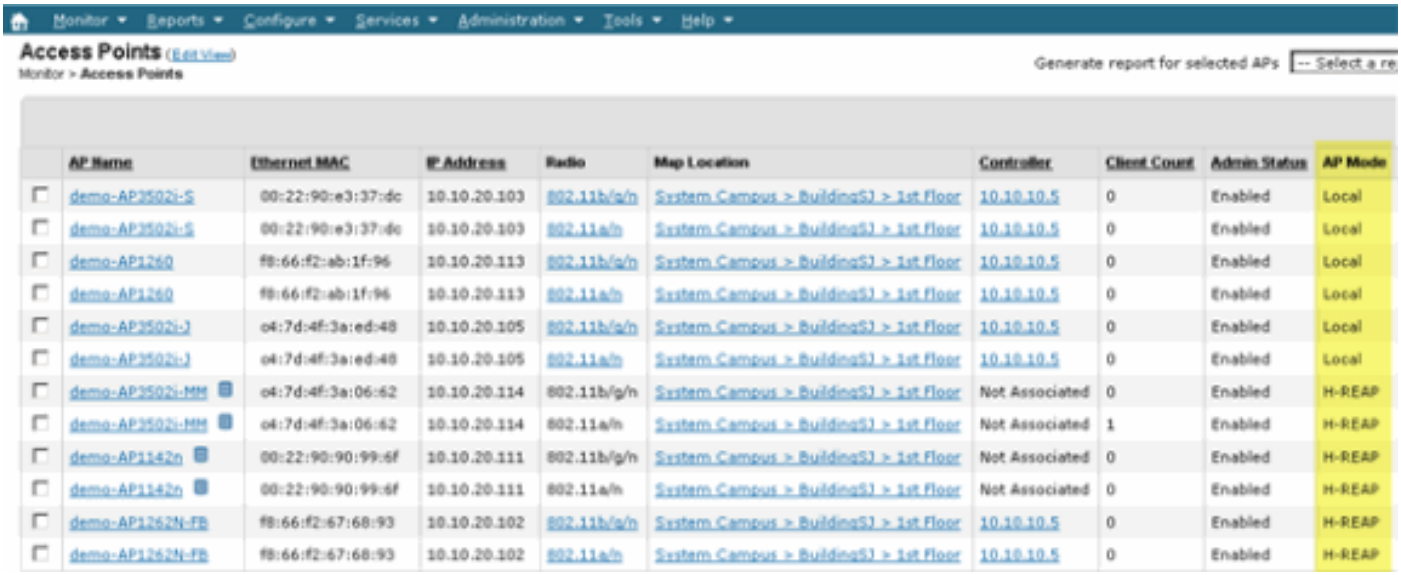
- AIR-LM-WIPS-xx - Лицензия Cisco ELM wIPS
- AIR-WIPS-AP-xx - Беспроводная связь Cisco wIPS Лицензия

Дополнительные примечания лицензирования ELM:

- Если лицензия wIPS MM AP SKU (s) уже установлена, те лицензии могут также использоваться для AP ELM.
- лицензии wIPS и лицензии ELM вместе рассчитывают к ограничениям лицензии платформы для wIPS механизма; 2000 AP на 3310 и 3000 AP на 335x, соответственно.
- Лицензия на пробное пользование будет включать 10 AP для wIPS и 10 для ELM сроком на максимум 60 дней. До ELM лицензия на пробное пользование позволила до 20 AP wIPS MM. Минимальное требование версий программного обеспечения, поддерживающих ELM, должно быть удовлетворено.

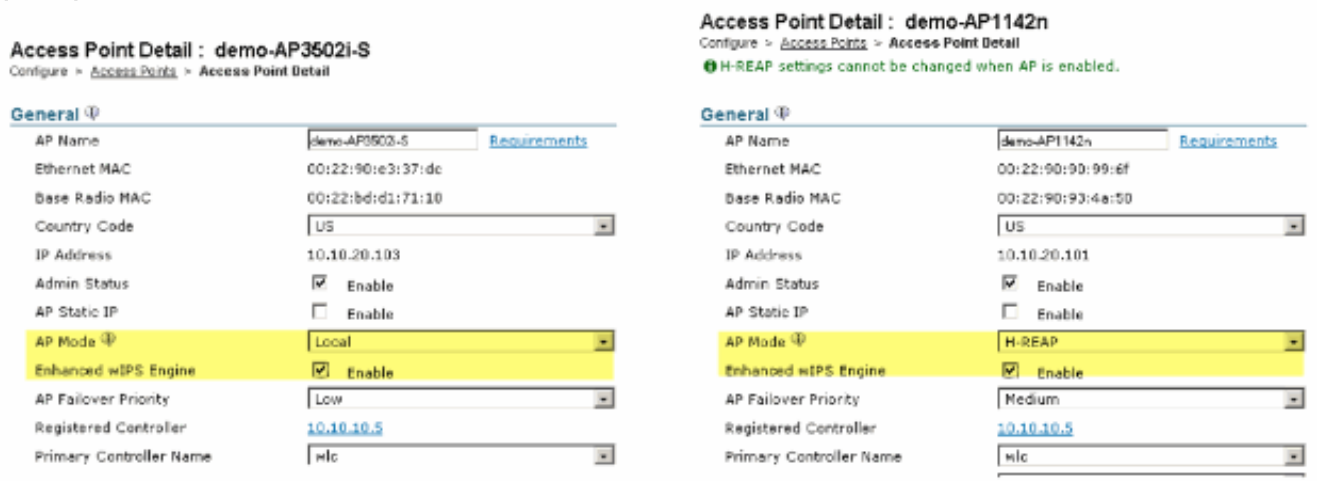
Настройте ELM с WCS

Рисунок 5 - Использование WCS для Настройки ELM

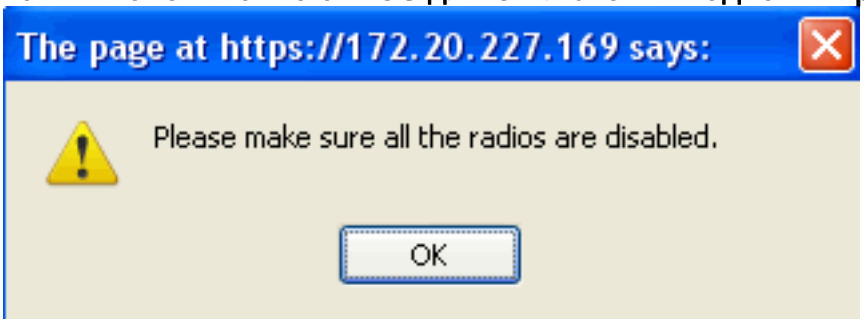


AP Name	Ethernet MAC	IP Address	Radio	Map Location	Controller	Client Count	Admin Status	AP Mode
demo-AP3502i-S	00:22:90:e3:37:dc	10.10.20.103	802.11b/g/n	System Campus > Building5J > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP3502i-S	00:22:90:e3:37:dc	10.10.20.103	802.11a/n	System Campus > Building5J > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP1260	f8:66:f2:ab:1f:96	10.10.20.113	802.11b/g/n	System Campus > Building5J > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP1260	f8:66:f2:ab:1f:96	10.10.20.113	802.11a/n	System Campus > Building5J > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP3502i-J	o4:7d:4f:3a:ed:48	10.10.20.105	802.11b/g/n	System Campus > Building5J > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP3502i-J	o4:7d:4f:3a:ed:48	10.10.20.105	802.11a/n	System Campus > Building5J > 1st Floor	10.10.10.5	0	Enabled	Local
demo-AP3502i-MM	o4:7d:4f:3a:06:62	10.10.20.114	802.11b/g/n	System Campus > Building5J > 1st Floor	Not Associated	0	Enabled	H-REAP
demo-AP3502i-MM	o4:7d:4f:3a:06:62	10.10.20.114	802.11a/n	System Campus > Building5J > 1st Floor	Not Associated	1	Enabled	H-REAP
demo-AP1142n	00:22:90:90:99:6f	10.10.20.111	802.11b/g/n	System Campus > Building5J > 1st Floor	Not Associated	0	Enabled	H-REAP
demo-AP1142n	00:22:90:90:99:6f	10.10.20.111	802.11a/n	System Campus > Building5J > 1st Floor	Not Associated	0	Enabled	H-REAP
demo-AP1262N-FB	f8:66:f2:67:68:93	10.10.20.102	802.11b/g/n	System Campus > Building5J > 1st Floor	10.10.10.5	0	Enabled	H-REAP
demo-AP1262N-FB	f8:66:f2:67:68:93	10.10.20.102	802.11a/n	System Campus > Building5J > 1st Floor	10.10.10.5	0	Enabled	H-REAP

1. От WCS отключите и 802.11b/g и 802.11a радио AP прежде, чем включить “Улучшенный wIPS Механизм”.**Примечание:** Все связанные клиенты будут разъединены и не присоединятся, пока не включат радио.
2. Настройте один AP или используйте шаблон конфигурации WCS для множественных легковесных AP. (См. рис. 6.)**Рисунок 6 - Включает Расширенный wIPS Механизм (ELM) sub режим**

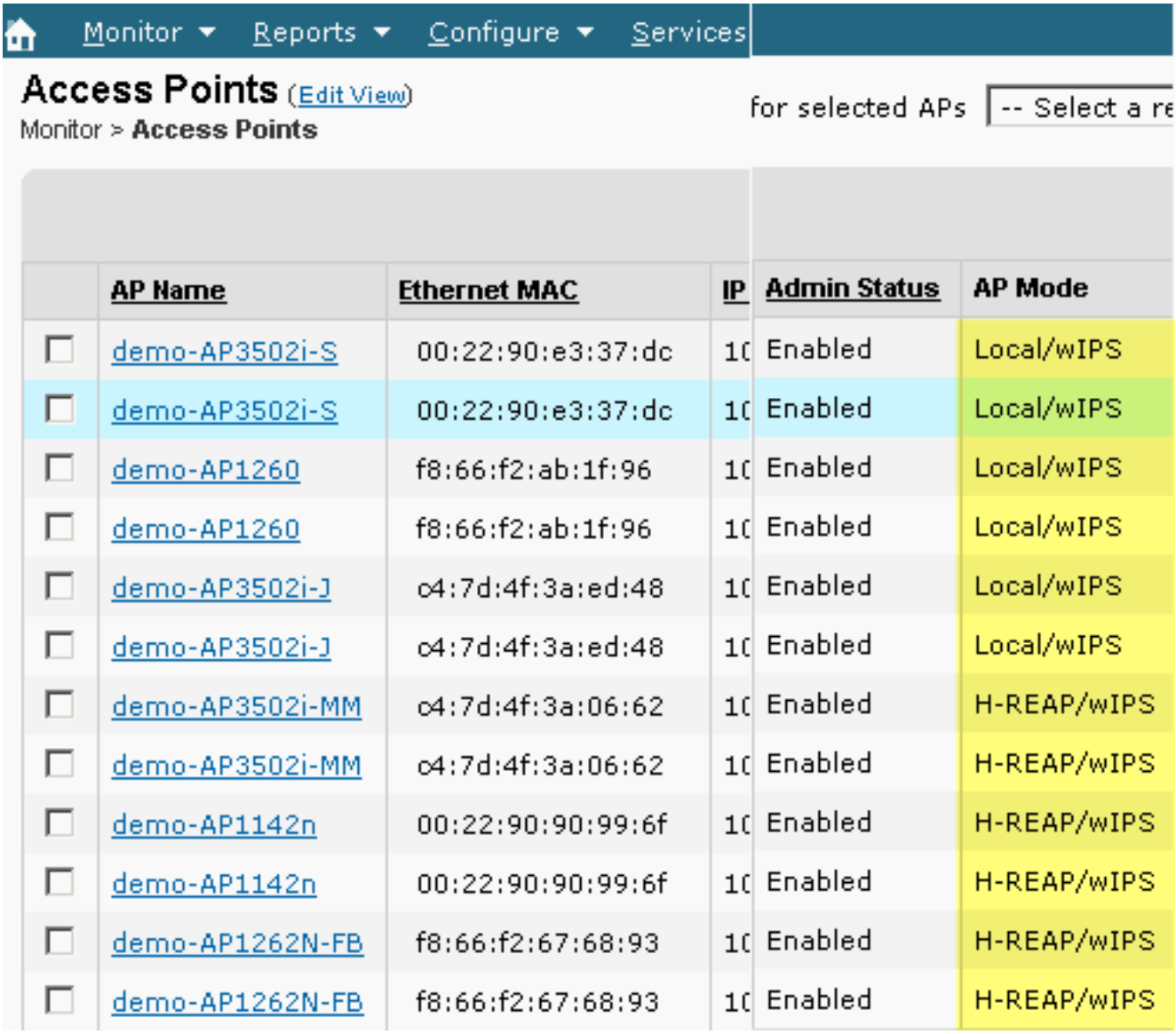


3. Выберите **Enhanced wIPS Engine** и нажмите **Save**.Включение Расширенного wIPS Механизма не вызовет AP к перезагрузке.H-REAP поддерживается; включите тот же путь что касается точки доступа в локальном режиме.**Примечание:** Если любому из радио этого AP включат, то WCS проигнорирует конфигурацию и бросит ошибку в рисунок 7.**Рисунок 7 - Напоминание о WCS для Отключения Радио AP прежде, чем Включить ELM**



4. Успех конфигурации может быть проверен путем наблюдения изменения в Режиме AP от “Локальной переменной или H-REAP” к **Local/wIPS** или **H-REAP/wIPS**. (См. рис. 8.)**Рисунок 8 - Режим AP Отображения WCS для Включения wIPS с Локальным и/или**

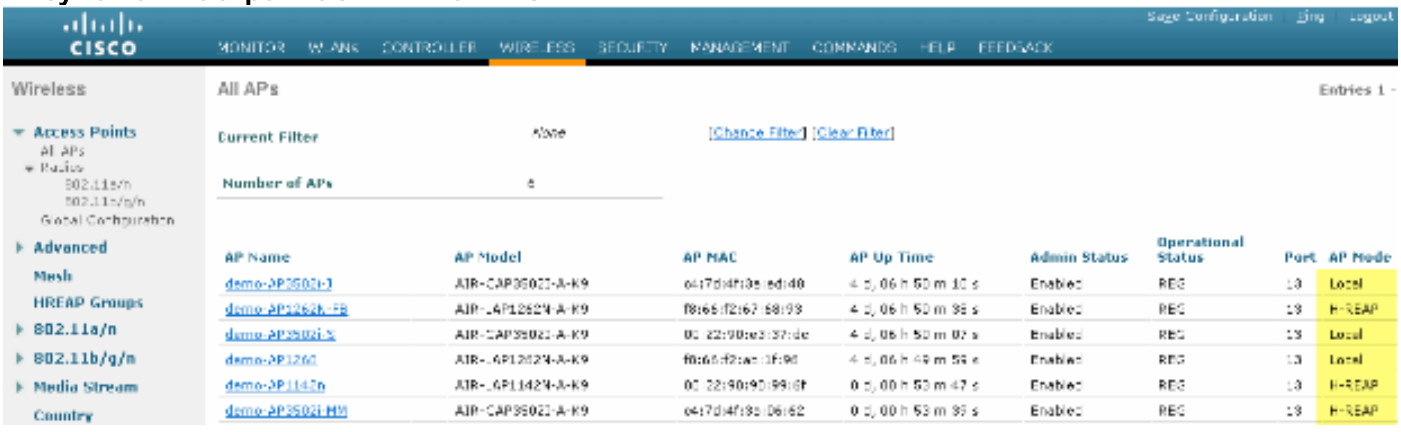
H-REAP



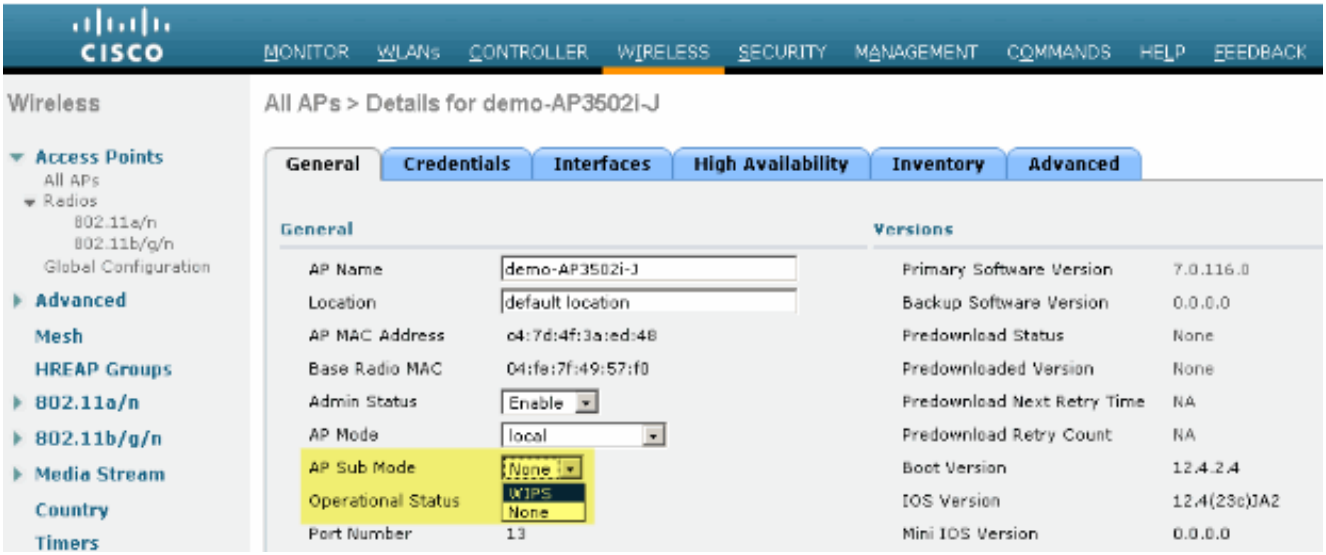
5. Включите радио что, где отключено в Шаге 1.
6. Создайте профиль wIPS и выдвиньте его к контроллеру для конфигурации завершать.**Примечание:** Для завершенных сведений о конфигурации на wIPS обратитесь к Cisco Адаптивное wIPS Руководство по развертыванию.

Конфигурация от WLC

Рисунок 9 - настраивает ELM с WLC



1. Выберите AP из **вкладки Wireless.Рисунок 10 - AP Изменения WLC sub режим для Включения wIPS ELM**



2. От AP раскрывающееся меню Режима Sub выберите **wIPS** (Figure 10).
3. Применитесь, и затем сохраните конфигурацию.

Примечание: Для функциональности ELM для работы MSE и WCS требуются с лицензированием wIPS. Изменение AP sub режим от одного только WLC не включит ELM.

Атаки, обнаруженные в ELM

Таблица 1 - wIPS Матрица поддержки Подписей

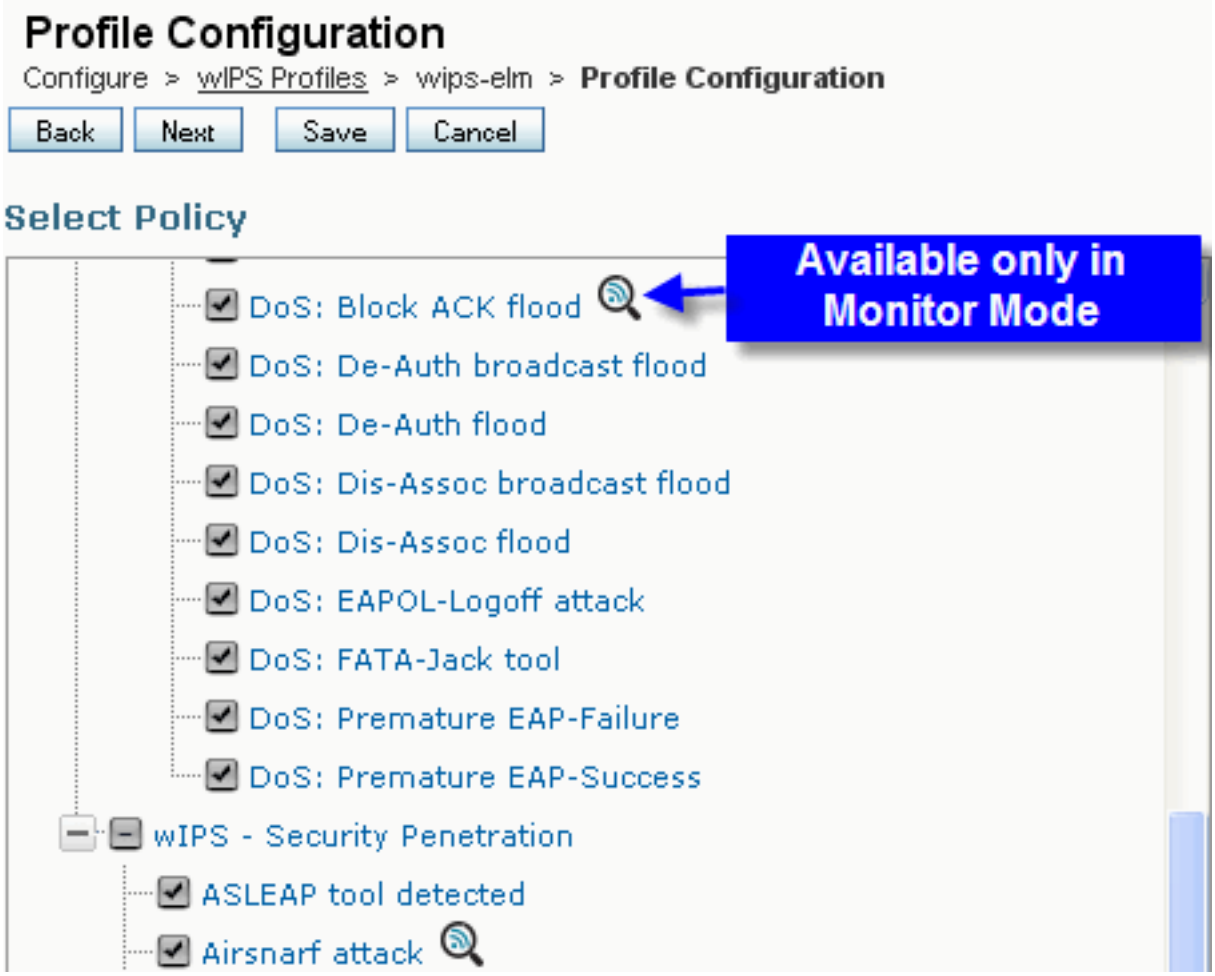
Обнаруженные атаки	ELM	MM
Атака DoS на AP		
Лавинная рассылка ассоциации	Y	Y
Переполнение таблицы сопоставлений	Y	Y
Опознавательная лавинная рассылка	Y	Y
Запустите EAPOL атаку	Y	Y
Лавинная рассылка Опроса PS	Y	Y
Тестовая лавинная рассылка запроса	N	Y
Не прошедшая поверку подлинности ассоциация	Y	Y
Атака DoS на инфраструктуру		
Лавинная рассылка CTS	N	Y
Квинслендское использование технологического университета	N	Y
Затор RF	Y	Y
Лавинная рассылка RTS	N	Y
Действительная атака Носителя	N	Y
Атака DoS на станцию		
Атака ошибки проверки подлинности	Y	Y
Блочная лавинная рассылка ACK	N	Y

Де-От передавал лавинную рассылку	Y	Y
Лавинная рассылка Де-Ота	Y	Y
Помощник скидки передавал лавинную рассылку	Y	Y
Лавинная рассылка помощника скидки	Y	Y
Атака Выхода из системы EAPOL	Y	Y
Программное средство FATA-Jack	Y	Y
Преждевременный сбой EAP	Y	Y
Преждевременный успех EAP	Y	Y
Атаки проникновения безопасности		
Программное средство ASLEAP обнаружено	Y	Y
Атака Airsnarf	N	Y
Атака ChopChop	Y	Y
Атака День Зеро аномалией безопасности беспроводных сетей	N	Y
Атака День Зеро аномалией безопасности устройства	N	Y
Зондирование устройства для AP	Y	Y
Подбор пароля по словарю на методах EAP	Y	Y
Атака EAP на аутентификацию 802.1x	Y	Y
Обнаружены поддельные AP	Y	Y
Поддельный сервер DHCP обнаружен	N	Y
WEP FAST взламывает обнаруженное программное средство	Y	Y
Атака фрагментации	Y	Y
AP ловушки обнаружен	Y	Y
Программное средство Hotspotter обнаружено	N	Y
Неподходящие широковещательные кадры	N	Y
Обнаружены неправильно сформированные пакеты 802.11	Y	Y
Man в средней атаке	Y	Y
Netstumbler обнаружен	Y	Y
Жертва Netstumbler обнаружена	Y	Y
Нарушение PSPF обнаружено	Y	Y
Мягкий AP или AP хоста обнаружены	Y	Y
Поддельный MAC-адрес обнаружен	Y	Y
Подозрительный трафик после закрытия обнаружен	Y	Y
Неавторизованная ассоциация списком поставщика	N	Y
Неавторизованная ассоциация	Y	Y

обнаружена		
Wellenreiter обнаружен	Y	Y

Примечание: Добавление CleanAir также включит обнаружение атак не802.11.

Рисунок 11 - Представление Профиля WCS wIPS



На рисунке 11 настройте профиль wIPS от WCS, значок указывает, что атака будет обнаружена только, когда AP будет в MM, в то время как только оптимальный уровень когда в ELM.

ELM устранения неполадок

Проверьте эти элементы:

- Удостоверьтесь, что настроен NTP.
- Удостоверьтесь, что настройка времени MSE находится в UTC.
- Если группа устройств не работает, используйте SSID профиля наложения с Любым. Перезагрузите AP.
- Удостоверьтесь лицензируя, настроен (В настоящее время, AP ELM используют лицензии KAM),
- Если профили wIPS изменяются слишком часто, синхронизируют MSE-контроллер снова. Удостоверьтесь, что профиль активен на WLC.
- Удостоверьтесь, что WLC является частью MSE, использующего CLI MSE:SSH или telnet к вашему MSE.Выполните**/opt/mse/wips/bin/wips_cli** - Эта консоль может

использоваться для доступа к следующим командам для сбора информации относительно состояния адаптивной wIPS системы.**покажите wlc все** – Проблема в wIPS консоли. Эта команда используется для проверки контроллеров, которые активно связываются с wIPS сервисом на MSE. (См. рис. 12.).**Рисунок 12 - WLC Проверки CLI MSE, Активный с сервисами MSE wIPS**`wIPS>show wlc all WLC MAC Profile Profile Status IP Onx Status Status ---------- ---------- ---------- ---------- ---------- ---- 00:21:55:06:F2:80 WCS-Default Policy active on controller 172.20.226.197 Active`

- Удостоверьтесь, что сигналы тревоги становятся обнаруженными на MSE, использующем CLI MSE.**покажите список аварийных сигналов** - Проблема в wIPS консоли. Эта команда используется для распечатки сигналов тревоги, в настоящее время содержавшихся в wIPS сервисной базе данных. Ключевое поле является уникальным ключом хэша, назначенным на определенный сигнал тревоги. Поле Type является типом сигнала тревоги. Эта диаграмма на рисунке 13 показывает список сигнальных ID и описаний:**Рисунок 13 - CLI MSE показывает список аварийных сигналов Команда**`wIPS>show alarm list Key Type Src MAC LastTime Active First Time ---------- ---------- ---------- ---------- ---------- 89 89 00:00:00:00:00:00 2008/09/04 18:19:26 2008/09/07 02:16:58 1 65631 95 00:00:00:00:00:00 2008/09/04 17:18:31 2008/09/04 17:18:31 0 1989183 99 00:1A:1E:80:5C:40 2008/09/04 18:19:44 2008/09/04 18:19:44 0` Когда сигнал тревоги был обнаружен, поля First Time и Last Time показывают метки времени; они сохранены во время UTC. Если сигнал тревоги в настоящее время обнаруживается, Активное поле выделяет.
- Очистите базу данных MSE.При столкновении с ситуацией, где база данных MSE повреждена, или никакие другие методы устранения проблем не будут работать, может быть лучше очистить базу данных и запуститься.**Рисунок 14 - Команда сервисов MSE**`1. /etc/init.d/msed stop 2. Remove the database using the command 'rm /opt/mse/locserver/db/linux/server-eng.db' 3. /etc/init.d/msed start`

Дополнительные сведения

- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 7.0.116.0
- Руководство по конфигурированию Cisco Wireless Control System, выпуск 7.0.172.0
- Cisco Systems – техническая поддержка и документация