Cisco Wireless Intrusion Prevention System

Cisco® Wireless Intrusion Prevention System (wIPS) встраивает в инфраструктуру беспроводной сети полный набор возможностей для обнаружения и нейтрализации беспроводных угроз. Благодаря этому данное решение является наиболее полным, точным и экономически самым эффективным в отрасли с точки зрения обеспечения безопасности операций в беспроводной сети.

Трудности при защите беспроводной сети

Распространение беспроводных сетей и большое количество новых мобильных вычислительных устройств размыли традиционные границы между доверенными и не доверенными сетями, а также переместили приоритеты безопасности с сетевого периметра на защиту информации и на обеспечение безопасности пользователей.

К числу проблем ИТ-безопасности относятся: нелегальные точки доступа, создающие т. н. «черный ход», DDoS-атаки (distributed denial-of-service), сетевая разведка «по воздуху», подслушивание, взламывание трафика и необходимость демонстрировать соответствие отраслевым требованиям.

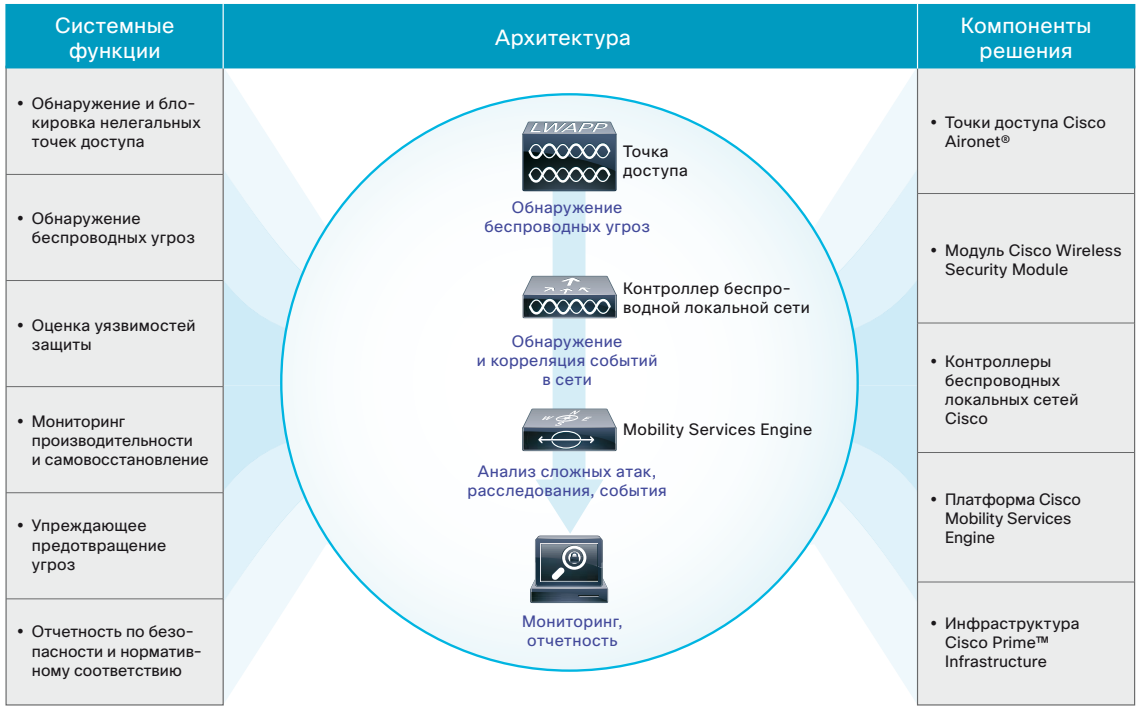
Ценность решения Cisco wIPS

Cisco wIPS – это всеобъемлющее решение по обеспечению беспроводной безопасности, использующее инфраструктуру Cisco Unified Access™ с целью обнаружения, локализации, блокировки и ограничения проводных и беспроводных угроз на сетевых уровнях 1 и 2. Интеграция беспроводной системы предотвращения вторжений в инфраструктуру беспроводной локальной сети (WLAN) обеспечивает экономическую и операционную эффективность благодаря использованию единой инфраструктуры и для сервисов wIPS, и для сервисов WLAN. В состав описываемого решения входят следующие компоненты: стандартные точки доступа Cisco Aironet® с модулями беспроводной безопасности Wireless Security Module, контроллеры беспроводной локальной сети Cisco, платформа Cisco Mobility Services Engine и инфраструктура Cisco Prime™ Infrastructure (рис. 1)

Преимущества решения Cisco wIPS

Решение Cisco wIPS предлагает расширенный набор средств, которые с точки зрения архитектуры невозможно реализовать в случае отдельных, подключаемых решений для предотвращения вторжений в беспроводные сети. Архитектура решения Cisco wIPS, интегрированная в инфраструктуру, позволяет сетевым администраторам сделать следующее:

Рис. 1. Компоненты решения Cisco wIPS



- **Обеспечить всеобъемлющую защиту.** Решение Cisco wIPS идентифицирует и локализует беспроводные атаки на защищаемую им сеть (в т. ч. нелегальные точки доступа, сетевая разведка, взлом аутентификации и шифрования, DoS-атаки, атаки типа man-in-the-middle, попытки заимствования прав, атаки нулевого дня, новые неизвестные атаки), чтобы обеспечить всеобъемлющую защиту во всей беспроводной среде.
- **Видеть полную картину.** Решение Cisco wIPS анализирует сетевой трафик, чтобы обнаружить нестандартную активность и беспроводные атаки в зонах действия точек доступа и контроллеров беспроводной локальной сети. Кроме того, оно отслеживает инвентаризационный перечень устройств, проводит аудиты сетевой конфигурации и осуществляет мониторинг показателей функционирования сетевой среды.
- **Осуществление корректирующих действий.** Решение Cisco wIPS не только обнаруживает угрозы, уязвимости и проблемы производительности; оно уведомляет администраторов о продолжающихся беспроводных угрозах, локализует атакующего, регистрирует релевантные данные для расследования и автоматически инициирует противодействующие меры, если это возможно.
- **Задействовать все ресурсы беспроводной локальной сети.** Решение Cisco wIPS способно использовать все точки доступа защищаемой сети для обнаружения, локализации и блокировки нелегальных устройств. Это повышает точность локализации, снижает количество ложноположительных реакций и ускоряет блокировку.

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Cisco и логотип Cisco являются товарными знаками или зарегистрированными товарными знаками компании Cisco и/или ее аффилированных компаний в США и других странах. Перечень товарных знаков Cisco доступен по адресу: www.cisco.com/go/trademarks. Прочие товарные знаки, упомянутые в настоящем документе, являются собственностью соответствующих владельцев. Использование слова «партнер» не подразумевает наличия партнерских отношений между Cisco и какой-либо другой компанией. (1110R)

- **Предлагать непрерывную актуальную защиту.** Благодаря автоматизированной оценке уязвимостей и актуальной библиотеке угроз администратор беспроводной сети обладает необходимыми знаниями для защиты беспроводной сети, даже не являясь специалистом по безопасности.
- **Воспользоваться гибкими архитектурами для развертывания.** Решение Cisco wIPS может использовать точки доступа для мониторинга на постоянной основе, точки доступа, обслуживающие пользователей беспроводной сети с одновременным обеспечением защиты в канале или выделенный модуль беспроводной безопасности Wireless Security Module, обеспечивающий защиту в диапазонах 2,4 и 5 ГГц. При этом показатели работы радиоустройств, обслуживающих данные, не ухудшаются.
- **Использовать решение корпоративного уровня, обеспечивающее возможности управления.** Инфраструктура Cisco Prime Infrastructure способна управлять сотнями контроллеров беспроводной локальной сети Cisco и до 15000 точек доступа Cisco Aironet. Решение wIPS использует платформу Cisco Mobility Services Engine для локализации беспроводных угроз и корреляции событий безопасности, таких как нелегальные точки доступа, источники помех и активные вторжения.

Характеристики

Решение Cisco wIPS обладает следующими ключевыми характеристиками и преимуществами:

- **Обнаружение, локализация, классификация и блокировка нелегальных точек доступа.** Решение wIPS обнаруживает, автоматически классифицирует на основе настраиваемых правил и блокирует нелегальные точки доступа, клиентов нелегальных точек доступа, ложных клиентов и клиентские ad hoc соединения.
- **Обнаружение беспроводных атак.** Решение wIPS идентифицирует и локализует атаки на беспроводную сеть, в т. ч. нелегальные точки доступа, DoS-атаки на валидных клиентов и сеть, атаки типа man-in-the-middle, попытки использования чужого пароля, атаки нулевого дня и новые неизвестные атаки.
- **Мониторинг уязвимостей защиты.** Решение wIPS самостоятельно выполняет автоматический круглосуточный мониторинг и оценку беспроводных уязвимостей путем упреждающего и постоянного сканирования беспроводной сети на предмет ослабления защиты и конфигураций, несоответствующих политикам.
- **Управление, мониторинг и отчетность.** Решение wIPS полностью интегрировано в инфраструктуру Cisco Prime Infrastructure, что обеспечивает единое унифицированное представление для управления проводной и беспроводной сетью. Инфраструктура Cisco Prime Infrastructure предлагает встроенные отчеты о соответствии отраслевым требованиям (в том числе, обязательные отчеты на соответствие стандартам Payment Card Industry (PCI) 2.0).

Почему именно Cisco?

Только Cisco предоставляет систему предотвращения беспроводных вторжений, которая глубоко интегрирована в инфраструктуру Unified Access. Это обеспечивает превосходное обнаружение вторжений, включая возможности локализации и предотвращения атак, защищающие и проводную, и беспроводную сеть от беспроводных угроз и атак.

Дополнительная информация: http://www.cisco.com/go/wips и www.cisco.com/go/mse.

Россия, 121614, Москва,
ул. Крылатская, д.17, к.4 (Krylatsky Hills)
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru, www.cisco.com

Казахстан, 050059, Алматы, бизнес-центр «Самал Тауэрс»,
ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, «Лэндмарк» здание III, 3 этаж
Телефон: +994 (12) 437 4820, факс: +994 (12) 437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998 (71) 140 4460, факс: +998 (71) 140 4465

© Cisco и/или ее дочерние компании, 2016. Все права защищены. Cisco и логотип Cisco являются товарными знаками или зарегистрированными товарными знаками компании Cisco и/или ее аффилированных компаний в США и других странах. Перечень товарных знаков Cisco доступен по адресу: www.cisco.com/go/trademarks. Прочие товарные знаки, упомянутые в настоящем документе, являются собственностью соответствующих владельцев. Использование слова «партнер» не подразумевает наличия партнерских отношений между Cisco и какой-либо другой компанией.

(1110R) C45-504521-01 10/13