Устройства Cisco IPS серии 4300

Поскольку пользователи и данные выходят за границы корпоративной сети, и уровень сетевого доступа становится более уязвимым, использование продуктов, в которых угрозы выявляются только на основе сигнатур, ведет к неэффективной защите. Только Cisco использует широкий сетевой контекст на каждом этапе анализа, включая уязвимые ОС, методики обхода, состояние атаки по разным сигнатурам, а также (впервые в отрасли) идентификационные данные и поведение злоумышленника.

Сенсор для предотвращения вторжений Cisco® (IPS) 4300 Series допускает масштабирование в соответствии с потребностями широкого диапазона сценариев развертывания, от небольших офисов и филиалов до архитектур корпоративных центров обработки данных. Благодаря скоростям передачи данных, варьирующимся в диапазоне от 1 Гбит/с до 10 Гбит/с, каждая модель IPS серии 4300 обеспечивает высокий уровень защиты. Устройство Cisco IPS серии 4300 обеспечивает инспекцию с аппаратным ускорением, производительность, соответствующую реальным условиям эксплуатации, высокую плотность портов и энерго-эффективность в форм-факторе 1-RU (рис. 1). Благодаря эффективной готовой системе защиты и автоматическим управлением угрозами защита критически важных активов обеспечивается за считанные минуты.

Рис. 1. Сенсоры Cisco IPS 4345 и 4360

Расширенная защита от угроз

Решения Cisco для IPS предоставляют:

- Широкую и глубокую систему защиты с более чем 5500 сигнатурами
- Запатентованную технологию предотвращения обходов для защиты от червей, вирусов, троянских программ, разведывательных атак, шпионских программ, ботнетов, нежелательных приложений и вредоносного ПО
- Анализ протокола и поведения для окончательного выявления угрозы
- Глобальную корреляцию Cisco для поддержки идентификации источника атаки типа «отказ в обслуживании» (DoS), распределенных атак типа «отказ в обслуживании» (DDoS), SYN flood, а также зашифрованных атак, что позволяет блокировать их
- Специфическую защиту для Unified Communications, WLAN, маршрутизации и коммутации, помогающую охранять безопасность инфраструктуры Cisco

Обеспечение совместимости

Решения Cisco IPS помогают клиентам повышать уровень совместимости со следующими нормативными требованиями в отношении конфиденциальности и защите данных:

- Стандарт отрасли платежных карт (PCI)
- Правила обеспечения конфиденциальности, принятые в ЕС
- Закон Сарбейна-Оксли (SOX), США
- Закон Грэмма-Лича-Блайли (GLBA), США
- Обеспечение безопасности ключевой инфраструктуры NERC (CIP)
- Акт о передаче и защите данных учреждений здравоохранения (HIPAA)

Простая сетевая интеграция

Технология Cisco IPS обеспечивает самый широкий в отрасли учет особенностей сети. При обеспечении безопасности центра обработки данных, ядра или границы решения Cisco IPS предоставляют защиту от угроз вплоть до прикладного уровня. Для снижения капиталовложений решения Cisco IPS строятся на стандартной архитектуре ПО и на специальных аппаратных платформах, что позволяет осуществлять развертывание в любом месте сети Cisco, включая платформы маршрутизации, коммутации и межсетевого экрана. Согласованная структура политик и операций помогает соблюдать нормативные требования и управлять рисками при более низких текущих расходах.

Беспрецедентное глобальное сопоставление

По мере развития APT, ботнетов и других смешанных угроз проверка трафика только с учетом сигнатур становится недостаточной. Cisco IPS, использующая 10-летний опыт применения технологии веб-репутаций, является единственной системой IPS, которая нейтрализует выявленные атаки, основываясь на репутации источника, а не только на срабатывании сигнатур. Благодаря технологии глобальной корреляции, поддержанной системой Cisco® SIO, решение Cisco IPS обеспечивает прозрачность на основе сотен дополнительных параметров безопасности, миллионов правил обнаружения и 8 Тб данных телеметрии угроз в сутки, ежедневно предоставляемую ведущими отраслевыми почтовыми и веб-клиентами, межсетевыми экранами и устройствами IPS.

Функции, готовые для работы в сети

Чтобы удовлетворить потребности сетей с самыми жесткими требованиями к безопасности, технология Cisco IPS непосредственно встраивается в межсетевой экран, чтобы обеспечить производительность на уровне нескольких Гбит/с, низкую задержку, а также реализовать функции, обеспечивающие высокую доступность. Используя глубокий анализ пакетов с аппаратным ускорением, Cisco IPS серии 4300 обеспечивает производительность в диапазоне от 750 Мбит/с до 1,25 Гбит/с для поддержки широкого спектра приложений и вариантов развертывания. Подробности об уникальной методике, которую Cisco применяет для расчета производительности IPS, см. в документе «Производительность сенсоров Cisco IPS серии 4500 и 4300». Гибкие и высокодоступные варианты развертывания включают конфигурации «активный-активный» и «активный-резервный», режимы «сбой/открытие» и «сбой/закрытие»; режимы IDS и IPS; а также резервные блоки питания. IPS серии 4300 также позволяет анализировать инкапсулированный трафик, включая GRE, MPLS, 802.1q, IPv4 в IPv4, IPv4 в IPv6, а также Q-in-Q double VLAN.

Проверенная система предотвращения угроз

Благодаря более чем 100 млн. долларов инвестиций в исследования в сфере безопасности, усилиям 500 аналитиков угроз и терабайтам данных об угрозах, поступающих в систему Cisco SensorBase™ каждый день, Cisco дает клиентам уверенность в безопасности их сетей. Поэтому технология Cisco IPS является самой распространенной в мире коммерческой технологией IPS. И именно по этой причине независимые тестовые организации также рекомендуют Cisco IPS.

Полный контроль и прозрачность в режиме реального времени

Cisco предоставляет решения по управлению для небольших развертываний, а также решения корпоративного класса. Cisco IPS Manager Express представляет собой полнофункциональное приложение для управления системами IPS и формирования отчетов по этим системам, поддерживающее до 10 устройств. Cisco Security Manager представляет собой решение по управлению безопасностью корпоративного класса с тысячами реальных развертываний.

Оба решения поддерживают устройства Cisco IPS серии 4300, а также другие сенсоры Cisco, маршрутизаторы Cisco с интегрированными сервисами (ISR), а также сервисные модули обнаружения вторжений Cisco (IDSM).

Cisco IPS Manager Express предоставляет следующие функции:

- Подготовку, мониторинг и устранение неполадок
- Перетаскиваемые устройства панели мониторинга для простоты настройки; персонализированные области просмотра, которые запоминают параметры пользователя, чтобы минимизировать время настройки и управления
- Гибкое средство создания отчетов, которое позволяет создавать настраиваемые отчеты и отчеты по соответствию нормативным требованиям в течение секунд

Cisco Security Manager 4.x предоставляет следующие функции:

- Гибкие процессы для поэтапной поставки новых и обновленных сигнатур, а также создания политик для IPS относительно этих сигнатур с последующим распространением политик на другие устройства
- Поддержка расширенной отчетности и управления событиями для новейших функций IPS Cisco, включая глобальную корреляцию Cisco IPS
- Контроль доступа на основе ролей (RBAC) и рабочие процессы для безошибочных развертываний и соответствия требованиям к процессам

В таблицах 1 и 2 приведены характеристики сенсоров Cisco IPS серии 4300.

Таблица 1. Характеристики сенсора Cisco IPS 4300

Характеристика	Cisco IPS 4345	Cisco IPS 4360
Средняя пропускная способность проверки	750 Мбит/с	1.25 Гбит/с
Максимальная пропускная способность проверки	1.8 Гбит/с	2.4 Гбит/с
Максимальное количество подключений	750 000	1 700 000
Кол-во соединений в секунду	30 000	45 000
Среднее время задержки	<150 мкс	<150 мкс
Защита от угроз	Более 25 000 угроз	Более 25 000 угроз
Защита от аномалий протокола	Да	Да
Выявление и нейтрализация методик обходов IPS	Да	Да
Защита от аномалий приложений	Да	Да
Пассивный контроль признаков ОС	Да	Да
Глобальная корреляция	Да	Да
Предварительные черные списки репутаций	Да	Да
Выбор способа нейтрализации на базе репутации	Да	Да
Комплексный анализ сигнатур (разнородные оповещения объединяются в идентификатор угрозы более высокого уровня)	Да	Да
Настраиваемые рейтинги сигнатур: Степень серьезности, точность	Да	Да
Поддержка настраиваемых сигнатур	Да	Да

Таблица 2. Характеристики Cisco IPS

Характеристика	Cisco IPS 4345	Cisco IPS 4360
Интерфейс управления и мониторинга	1 порт Ethernet 10/100	1 порт Ethernet 10/100
ЦП	Многоядерный	Многоядерный
Память	8 Гб	16 Гб
Порты данных	8 x 11GE	8 x 11GE
Минимальный объем флэш-памяти	8 Гб	8 Гб
Температура	от -4 до 45 °C	от -4 до 45 °C
Относительная влажность (при эксплуатации)	от 10 до 90 % (без конденсации)	от 10 до 90 % (без конденсации)
Высота над уровнем моря (при эксплуатации)	от 0 до 3 024 м	от 0 до 3 024 м
Макс. пиковая мощность	Макс. 30 Вт	Макс. 90 Вт
Среднее время бесперебойной работы (MTBF)	874 070 часов (100 лет)	299 588 часов (31 год)
Размеры (ВхШхГ)	1,67 x 16,9 x 15,5 дюйма (4,24 x 42,9 x 39,5 см)	1,67 x 16,7 x 19,1 дюйма (4,24 x 42,9 x 48,4 см)
Масса	6,77 кг	7,63 кг
Безопасность	UL 1950, CSA C22.2 No. 950, EN 60950 IEC 60950, AS/NZS3260, TS001	UL 1950, CSA C22.2 No. 950, EN 60950 IEC 60950, AS/NZS3260, TS001
Электромагнитная совместимость (ЭМС)	Соответствие стандартам EC, FCC часть 15 класс A, AS/NZS 3548 класс A, VCCI класс A, EN55022 класс A, CISPR22 класс A, EN61000-3-2, EN61000-3-3	Соответствие стандартам EC, FCC часть 15 класс A, AS/NZS 3548 класс A, VCCI класс A, EN55022 класс A, CISPR22 класс A, EN61000-3-2, EN61000-3-3

Информация для заказа

Для оформления заказа перейдите на главную страницу заказов Cisco. Информацию для оформления заказа см. в таблице 3.

Таблица 3. Информация для заказа

Наименование продукта	Номер по каталогу
Устройства Cisco IPS серии 4300	
Сенсор Cisco IPS 4345	IPS-4345-K9
Сенсор Cisco IPS 4360	IPS-4360-K9
Сенсор Cisco IPS 4345 (версия с питанием постоянного тока)	IPS-4345-DC-K9
Сенсор Cisco IPS 4360 (версия с питанием постоянного тока)	IPS-4360-DC-K9

Обслуживание и техническая поддержка

Компания Cisco предлагает широкий диапазон программ по обслуживанию и поддержке, которые призваны содействовать успеху в работе клиентов. Эти инновационные программы реализуются благодаря уникальному сочетанию человеческих ресурсов, процессов, инструментов и партнеров, что позволяет полностью удовлетворять запросы клиентов. Сервисы Cisco помогают защитить ваши инвестиции в организацию сетей, оптимизировать работу сетей и подготовить их для реализации новых приложений, расширяющих интеллектуальные функции сетей и повышающих эффективность вашего бизнеса. Дополнительные сведения об услугах Cisco см. по адресу http://www.cisco.com/go/services/security.

Сервисы Cisco для IPS

Сервисы Cisco для IPS представляют собой неотъемлемую часть решения Cisco IPS серии 4300 и позволяют потребителям получать критические по времени обновления файлов сигнатур и уведомления. Будучи частью портфеля Cisco Technical Support Services (услуг технической поддержки Cisco), сервисы Cisco IPS позволяют поддерживать сенсоры Cisco IPS серии 4300 в актуальном состоянии для борьбы с самыми последними угрозами благодаря точной идентификации, классификации и блокировке злонамеренного или вредоносного трафика. Сервисы Cisco для IPS включают:

- Обновления файлов сигнатур и уведомления
- Репутационные веб-каналы для глобальной корреляции угроз
- Доступ зарегистрированных пользователей на сайт Cisco.com для использования интерактивных инструментов и технической помощи
- Доступ к центру технической поддержки Cisco.
- Обновления программного обеспечения Cisco IPS
- Заблаговременная замена неисправного оборудования

Для получения дополнительных сведений об услугах Cisco для IPS, посетите веб-сайт http://www.cisco.com/en/US/products/ps6076/serv_group_home.html.

Замечания относительно экспорта

Продукты Cisco IPS серии 4300 являются объектом экспортного контроля. Дополнительные сведения см. на интернет-сайте, посвященном нормативным требованиям к экспорту, расположенном по адресу http://www.cisco.com/wwl/export/crypto/. Специальные вопросы относительно экспорта можно направить по электронной почте на адрес rus-import@cisco.com.

Дополнительная информация

Для получения дополнительной информации перейдите по следующим ссылкам.

- Системы предотвращения вторжений Cisco: http://www.cisco.com/go/ips
- Модули Cisco IDS и сенсоры IPS, а также версии ПО, которые уже сняты с продаж: http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_eol_notices_list.html
- Cisco Security Manager: http://www.cisco.com/go/csmanager
- Cisco IPS Manager Express: http://www.cisco.com/go/ime

Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауэрс»,
Космодамианская наб., д. 52, стр. 1, 4 этаж
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. 15, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru

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-й этаж
Телефон: +994-12-437-48-20, 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