# Система предотвращение вторжений Cisco: Устройства Cisco IPS серии 4500

## Защитите свои центры обработки данных и сетевые точки агрегации с помощью систем предотвращения вторжений с учетом контекста.

Целью для злоумышленников являются данные, используемые широким спектром специальных и коммерческих приложений. Продукты, распознающие только сигнатуры, могут дать лишь одномерный (и иногда некорректный) результат. Только Cisco использует широкий сетевой контекст на каждом этапе анализа, включая пассивный контроль признаков ОС, методики обхода, состояние атаки по разным сигнатурам, а также (впервые в отрасли) идентификационные данные злоумышленника, его местоположение и поведение. Эти современные методы защищают инфраструктуру и приложения от APT угроз и других атак с применением новейших средств, обеспечивая высочайший уровень безопасности.

Устройство Cisco IPS 4500 обеспечивает проверку с аппаратным ускорением, производительность, соответствующую реальным условиям эксплуатации, высокую плотность портов и энергоэффективность в расширяемом шасси, рассчитанном на будущий рост и защиту инвестиций. Его малые размеры и низкое потребление энергии были специально спроектированы для ЦОД, предъявляющих жесткие требования к свободному месту. Благодаря высокоэффективной готовой системе защиты и автоматическому управлению угрозами защита критически важных активов центров обработки данных обеспечивается за считанные минуты.

**Рис 1.** Сенсоры Cisco IPS серии 4500.

## Защита с учетом контекста для критически важных внутренних приложений

На современном предприятии выполняется широкое множество критически важных приложений. Данные в этих приложениях являются ценным объектом для злоумышленников, поскольку доступ к ним имеет первостепенное значение для производительности и успеха предприятия. Необходимо предоставить полный и гибкий доступ авторизованным пользователям и в то же время защитить целостность инфраструктуры и приложений центра обработки данных. Система предотвращения вторжения с учетом контекста чрезвычайно важна для обеспечения полной защиты. Рассмотрим следующие сценарии:

- **Внедрение SQL-кода (SQL_Injection) или инструменты динамических запросов к базе данных?** Если система IPS может выполнить только одно действие при срабатывании сигнатуры внедрения SQL-кода, то ей недостает учета контекста. Технология Cisco IPS может определить уровень действия даже после срабатывания сигнатуры.
- **Вредоносное ПО, сканирующее целевые данные, или работающий сотрудник группы ИТ?** Большое число команд pings отправляется с ноутбука специалиста по продажам, находящегося в командировке. Является ли это результатом деятельности ботнета, ищущего цели, или же сотрудника группы ИТ, старающегося помочь устранить проблемы с доступом к системе управления связями с клиентами (CRM)?
- **Сотрудник, экспериментирующий со скриптом, или целенаправленная атака?** Необходимо ли анализировать действия всех сотрудников или просто регистрировать события в журнале? IPS с учетом контекста знает разницу.

- **Случайные колебания задержки или скрытые атаки?** Некоторые виды скремблирования трафика и деятельности по обходу защиты, как правило, не встречаются в корпоративных сетях. Только Cisco предоставляет непосредственные отчеты по таким действиям и предлагает другие специальные настройки для нейтрализации атак.

## Соответствие нормативным требованиям и предотвращение рисков

Коммерческие группы и правительственные организации имеют юридические обязательства по защите данных от изменения, кражи и несанкционированного доступа. Системы предотвращения вторжения Cisco с учетом контекста обеспечивают защиту приложений, а также непрерывность и безопасность операций в соответствии со следующими нормативными требованиями:

- Розничная торговля и и.п.: Стандарт безопасности в индустрии платежных карт (PCI DSS)
- Открытые акционерные общества в США: Закон Сарбейна-Оксли (SOX), США
- Компании, зарегистрированные в ЕС: Правила обеспечения конфиденциальности, принятые в ЕС
- Электроэнергетика: Обеспечение безопасности ключевой инфраструктуры NERC (CIP)
- Коммерческие организации в США: Акт о передаче и защите данных учреждений здравоохранения (HIPAA)
- ФСТЭК 21/17 382-П ЦБ

## Простая сетевая интеграция

Являясь критически важным компонентом архитектуры Cisco SecureX, Cisco IPS предоставляет самый широкий в отрасли учет особенностей сети. Идет ли речь о защите центра обработки данных, ядра сети или Интернет-периметра, технология Cisco IPS обеспечивает защиту, ориентированную на приложения и инфраструктуру. С целью уменьшения капиталовложений решения Cisco IPS строятся на стандартной архитектуре ПО, 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.

## Беспрецедентная глобальная корреляция

По мере развития APT угроз, ботнетов и других смешанных угроз проверка трафика только с учетом сигнатур становится недостаточной для выявления и нейтрализации угроз. 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. Технология глобальной корреляции Cisco IPS, поддержанная системой Cisco® SIO, собирает информацию по сотне параметров безопасности, миллионам правилам обнаружения и 8 Тб данных телеметрии угроз в сутки, ежедневно предоставляемую ведущими отраслевыми почтовыми и веб-клиентами, межсетевыми экранами и устройствами IPS, что обеспечивает Cisco IPS непревзойденные возможности обнаружения угроз в реальном времени.

## Функции, готовые для работы в сети

Устройство  Cisco IPS серии 4500 обеспечивает низкое время задержки и предоставляет функции, обеспечивающие высокую доступность, чтобы удовлетворить потребности сетей с самыми высокими требованиями. Используя глубокий анализ пакетов с аппаратным ускорением, Cisco IPS серии 4500 обеспечивает производительность в диапазоне нескольких Гбит/с и предоставляет специальное пространство для будущего расширения системы ввода/вывода и повышения производительности. 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»; работу в режиме IDS и IPS; а также резервные блоки питания. Система также может 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 SIO каждый день, Cisco IPS при поддержке Cisco SIO дает клиентам уверенность в безопасности их сетей, осуществляя контекстный анализ срабатывания сигнатур для определения правильной ответной реакции. Cisco является единственным поставщиком коммерческих систем IPS, который публично раскрывает свою базу данных сигнатур, чтобы продемонстрировать лучшую в своем классе защиту активов. Именно поэтому удостоенная наград технология Cisco IPS является самой распространенной в мире коммерческой технологией IPS.

## Полный контроль и прозрачность в режиме реального времени

Cisco предоставляет решения по управлению IPS для развертываний любого размера, от небольших организаций до крупных предприятий. 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 управления безопасностью корпоративного класса с тысячами реальных развертываний. Кроме того, имеется полнофункциональный локальный интерфейс командной строки.

Cisco IPS Manager Express и Cisco Security Manager поддерживают устройства Cisco IPS серии 4500, а также другие сенсоры Cisco IPS.

**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
- Контроль доступа на основе ролей и рабочие процессы для обеспечения безошибочных развертываний и соответствия установленным требованиям.

**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
- Предварительно определенные шаблоны настройки, привязанные к объекту

В таблице 1 приведены спецификации моделей Cisco IPS серии 4500.

**Таблица 1.** Характеристики решения Cisco IPS серии 4500

| Характеристика | Cisco IPS 4510 | Cisco IPS 4520* |
|---|---|---|
| **Средняя пропускная способность проверки (Мбит/с)** | 3 Гбит/с | 5 Гбит/с |
| **Максимальная пропускная способность проверки (Мбит/с)** | 5 Гбит/с | 10 Гбит/с |
| **Максимальное количество подключений** | 3 800 000 | 8 400 000 |
| **Кол-во соединений в секунду** | 72 000 | 100 000 |
| **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 обхода IPS** | Да | Да |
| **Защита от аномалий приложений** | Да | Да |
| **Пассивный контроль признаков ОС** | Да | Да |
| **Глобальная корреляция** | Да | Да |

| Характеристика | Cisco IPS 4510 | Cisco IPS 4520* |
|---|---|---|
| **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 |

* С одним модулем в Cisco IPS 4520; При первой поставке в 4520 поддерживается только один модуль.

В таблице 2 приведены характеристики Cisco IPS.

**Таблица 2.** Характеристики Cisco IPS

| Характеристика | Cisco IPS 4510 | Cisco IPS 4520* |
|---|---|---|
| **Интерфейс управления и мониторинга** | Порт Ethernet 10/100/1000 | Порт Ethernet 10/100/1000 |
| **ЦП** | Двухпроцессорный многоядерный | Двухпроцессорный многоядерный |
| **Память** | 24 Гб | 48 Гб |
| **Порты данных** | 6 портов 10/100/1000, 4 порта 1 или 10 Gigabit Ethernet SFP+ | 6 портов 10/100/1000, 4 порта 1 или 10 Gigabit Ethernet SFP+ |
| **Минимальный объем флэш-памяти** | 2 Гб | 2 Гб |
| **Температура** | При работе: от 0 до 40 °C<br>При хранении: от -40 °C до 70 °C | При работе: от 0 до 40 °C<br>При хранении: от -40 °C до 70 °C |
| **Относительная влажность (при эксплуатации)** | При работе: от 10% до 90%<br>При хранении: от 5% до 95% | При работе: от 10% до 90%<br>При хранении: от 5% до 95% |
| **Высота над уровнем моря (при эксплуатации)** | При работе: от 0 до 3 050 м<br>При хранении: от 0 до 9 144 м | При работе: от 0 до 3 050 м<br>При хранении: от 0 до 9 144 м |
| **Размеры (ВхШхГ)** | 3,47 x 19 x 26,5 дюйма (8,8 x 48,3 x 67,3 см) | 3,47 x 19 x 26,5 дюйма (8,8 x 48,3 x 67,3 см) |
| **Масса** | 22,7 кг с 1 SSP и 1 блоком питания;<br>28,2 кг с SSP, IPS SSP и 2 блоками питания | 22,7 кг с 1 SSP и 1 блоком питания;<br>28,2 кг с SSP, IPS SSP и 2 блоками питания |
| **Безопасность** | UL 60950-1, CAN/CSA-C22.2 No. 60950-1<br>EN 60950-1, IEC 60950-1, AS/NZS 60950-1 | UL 60950-1, CAN/CSA-C22.2 No. 60950-1<br>EN 60950-1, IEC 60950-1, AS/NZS 60950-1 |
| **Электромагнитная совместимость (ЭМС)** | FCC[1] часть 15 (CFR[2] 47) класс A<br>EN55022 класс A с CISPR22 класс A<br>AS/NZS[3] CISPR22 класс A<br>VCCI[4] класс A<br>CISPR 24<br>EN50082-1<br>EN55024<br>EN61000-3-2<br>EN61000-3-3<br>EN61000-6-1<br>KN22 класс A<br>KN24<br>ICES003 класс A | FCC[1] часть 15 (CFR[2] 47) класс A<br>EN55022 класс A с CISPR22 класс A<br>AS/NZS[3] CISPR22 класс A<br>VCCI[4] класс A<br>CISPR 24<br>EN50082-1<br>EN55024<br>EN61000-3-2<br>EN61000-3-3<br>EN61000-6-1<br>KN22 класс A<br>KN24<br>ICES003 класс A |
| | [1] FCC = Федеральная комиссия по связи<br>[2] CFR = Свод федеральных нормативных актов<br>[3] AS/NZS = Стандарты Австралии/Стандарты Новой Зеландии<br>[4] VCCI = Добровольный совет по контролю для оборудования информационных технологий (Япония) | [1] FCC = Федеральная комиссия по связи<br>[2] CFR = Свод федеральных нормативных актов<br>[3] AS/NZS = Стандарты Австралии/Стандарты Новой Зеландии<br>[4] VCCI = Добровольный совет по контролю для оборудования информационных технологий (Япония) |

## 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 4500** | |
| **Cisco IPS 4510** | IPS-4510-K9 |
| **Cisco IPS 4520** | IPS-4520-K9 |
| **Запасные платы** | |
| **Запасная плата Cisco IPS 4510** | IPS-4510-SSP-K9= |
| **Запасная плата Cisco IPS 4520** | IPS-4520-SSP-K9= |

## Обслуживание и техническая поддержка

Компания Cisco предлагает широкий диапазон программ по обслуживанию и поддержке, которые призваны содействовать успеху в работе клиентов. Эти передовые программы обслуживания осуществляются 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 4500 и позволяют пользователям 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 решение Cisco IPS серии 4500 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
- 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

Устройства Cisco IPS серии 4500 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

Дополнительные сведения о решениях Cisco IPS см. по адресу http://www.cisco.com/go/ips.

Чтобы получить информацию о сенсорах Cisco IDS и IPS, а также о версиях ПО, которые уже сняты с продаж, посетите веб-сайт http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_eol_notices_list.html.

Чтобы получить дополнительную информацию о Cisco Security Manager и Cisco IPS Manager Express, посетите сайты:

- http://www.cisco.com/go/csmanager
- 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. 1Б, 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