Компания Lancope теперь входит в состав корпорации Cisco.

Краткое руководство пользователя для StealthWatch FlowCollector 4000

12 апреля 2016 г.

Корпорация Cisco Systems.

www.cisco.com

Компания Cisco насчитывает более 200 представительств по всему миру.

Адреса, номера телефонов и факсов указаны на веб-сайте Cisco по адресу

www.cisco.com/go/offices.

Номер текстовой части:

Компания Lancope теперь входит в состав корпорации Cisco.

ХАРАКТЕРИСТИКИ И СВЕДЕНИЯ О ПРОДУКТАХ, ПРИВЕДЕННЫЕ В НАСТОЯЩЕМ РУКОВОДСТВЕ, МОГУТ БЫТЬ ИЗМЕНЕНЫ БЕЗ ПРЕДВАРИТЕЛЬНОГО УВЕДОМЛЕНИЯ. ВСЕ ЗАЯВЛЕНИЯ, СВЕДЕНИЯ И РЕКОМЕНДАЦИИ В НАСТОЯЩЕМ РУКОВОДСТВЕ ПРИЗНАЮТСЯ ТОЧНЫМИ, НО НЕ ПРЕДОСТАВЛЯЮТ ГАРАНТИЙ ЛЮБОГО РОДА, КАК ЯВНЫХ, ТАК И КОСВЕННЫХ. ПОЛЬЗОВАТЕЛЬ НЕСЕТ ПОЛНУЮ ОТВЕТСТВЕННОСТЬ ЗА ИСПОЛЬЗОВАНИЕ ЛЮБЫХ ОПИСАННЫХ ПРОДУКТОВ.

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ К ПРОГРАММНОМУ ОБЕСПЕЧЕНИЮ И УСЛОВИЯ ОГРАНИЧЕННОЙ ГАРАНТИИ НА СОПРОВОЖДАЮЩИЙ ПРОДУКТ ИЗЛОЖЕНЫ В ИНФОРМАЦИОННОМ ПАКЕТЕ, ПОСТАВЛЯЕМОМ ВМЕСТЕ С ПРОДУКТОМ И ЯВЛЯЮЩЕМСЯ ЕГО НЕОТЪЕМЛЕМОЙ ЧАСТЬЮ НА ОСНОВАНИИ ДАННОЙ ССЫЛКИ. ПОЛУЧИТЬ ЭКЗЕМПЛЯР ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ ИЛИ УСЛОВИЙ ОГРАНИЧЕННОЙ ГАРАНТИИ В СЛУЧАЕ ИХ ОТСУТСТВИЯ В КОМПЛЕКТЕ МОЖНО У ПРЕДСТАВИТЕЛЯ КОМПАНИИ CISCO.

Сжатие TCP-заголовков в продуктах Cisco реализовано в виде адаптации программы, разработанной в Калифорнийском университете в Беркли (UCB) как часть свободно распространяемой операционной системы UNIX. Все права защищены. © Члены правления Университета Калифорнии, 1981.

НЕСМОТРЯ НА ЛЮБЫЕ ДРУГИЕ ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА, ЗАЯВЛЕННЫЕ В НАСТОЯЩЕМ ДОКУМЕНТЕ, ВСЕ ФАЙЛЫ ДОКУМЕНТОВ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ПРЕДОСТАВЛЯЮТСЯ УКАЗАННЫМИ ПОСТАВЩИКАМИ НА УСЛОВИЯХ «КАК ЕСТЬ» БЕЗ ОБЯЗАТЕЛЬСТВА УСТРАНЕНИЯ ОШИБОК. КОМПАНИЯ CISCO И ВЫШЕНАЗВАННЫЕ ПОСТАВЩИКИ ОТКАЗЫВАЮТСЯ ОТ ВСЕХ ЯВНЫХ И ПОДРАЗУМЕВАЕМЫХ ГАРАНТИЙ, ВКЛЮЧАЯ ГАРАНТИИ ТОВАРНОГО СОСТОЯНИЯ И ПРИГОДНОСТИ ДЛЯ ИСПОЛЬЗОВАНИЯ ПО НАЗНАЧЕНИЮ, И ОТ ГАРАНТИЙ, ВОЗНИКАЮЩИХ В ХОДЕ ДЕЛОВЫХ ОТНОШЕНИЙ, ИСПОЛЬЗОВАНИЯ ИЛИ ТОРГОВОЙ ПРАКТИКИ.

НИ ПРИ КАКИХ УСЛОВИЯХ КОМПАНИЯ CISCO И ЕЕ ПОСТАВЩИКИ НЕ НЕСУТ ОТВЕТСТВЕННОСТИ ЗА ЛЮБЫЕ ВИДЫ КОСВЕННОГО, НАМЕРЕННОГО, ВЫТЕКАЮЩЕГО ИЛИ СЛУЧАЙНО ВОЗНИКШЕГО УЩЕРБА, ВКЛЮЧАЯ ПОТЕРЮ ПРИБЫЛИ И ПОВРЕЖДЕНИЕ ДАННЫХ В РЕЗУЛЬТАТЕ ИСПОЛЬЗОВАНИЯ ИЛИ НЕВОЗМОЖНОСТИ ИСПОЛЬЗОВАНИЯ НАСТОЯЩЕГО РУКОВОДСТВА, ДАЖЕ В ТОМ СЛУЧАЕ, ЕСЛИ КОМПАНИЯ CISCO И (ИЛИ) ЕЕ ПОСТАВЩИКИ ОСВЕДОМЛЕНЫ О ВОЗМОЖНОСТИ ПОДОБНОГО УЩЕРБА.

IP-адреса и номера телефонов, использованные в настоящем документе, не являются реальными адресами и номерами телефонов. Все примеры, текст командной строки, схемы топологии сети и иные изображения в настоящем документе приводятся исключительно в демонстрационных целях. Использование любых, реально существующих IP-адресов или номеров телефонов в наглядных материалах является непреднамеренным и случайным.

Содержание

Характеристики оборудования для StealthWatch FlowCollector Appliance

Функциональные возможности StealthWatch FlowCollector

Устройство StealthWatch FlowCollector для NetFlow позволяет вести сбор данных протоколов NetFlow, cFlow, J-Flow, Packeteer 2, NetStream и IPFIX для обеспечения экономичной защиты сети на основе поведения пользователей. FlowCollector агрегирует высокоскоростные поведенческие данные из нескольких сетей или сегментов сети для обеспечения комплексной защиты и повышения производительности в территориально распределенных сетях. По мере получения данных FlowCollector выявляет известные или неизвестные механизмы атаки, случаи ненадлежащего использования сетевых ресурсов внутри организации или неверно настроенные сетевые устройства независимо от фрагментации или шифрования пакетов данных. Как только StealthWatch выявляет тот или иной механизм злонамеренного поведения, система может выполнять любые настроенные для этого механизма действия.

FlowCollector серии 4000 предоставляет вариант массивно масштабируемой конфигурации для обработки очень больших объемов данных и имеет хранилище данных расширяемой емкости. Устройство обрабатывает данные до 120 000 потоков в секунду и до 2000 модулей экспорта. Устройство располагает хранилищем потоков объемом 4 ТБ (RAID-6, резервирование).

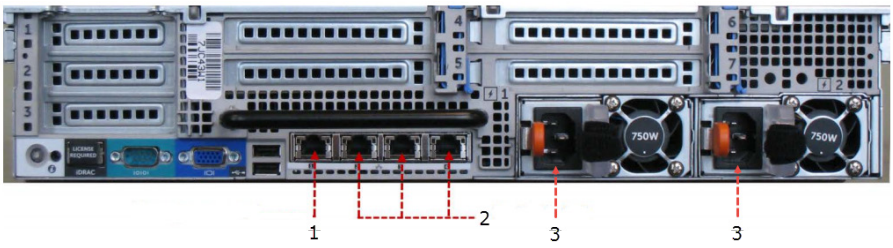
FlowCollector 4000 использует аппаратную платформу R720 и 12-е поколение аппаратного обеспечения. Это устройство оснащено адресным ЗУ объемом 5,4 ТБ.

Передняя панель

На следующем рисунке показана общая конфигурация передней панели устройства FlowCollector. Ваша модель может выглядеть несколько по-другому.

Задняя панель

На следующем рисунке показана общая конфигурация задней панели устройства FlowCollector. Ваша модель может выглядеть несколько по-другому.



Номер	Компонент
1	Порт управления
2	Порты мониторинга
3	Вход для электропитания

Характеристики оборудования

В следующей таблице описаны физические свойства и условия окружающей среды для устройств StealthWatch FlowCollector Appliance.

Технические характеристики FlowCollector серии 4000	
Стоечные модули (монтируемые)	**Вес**
2U Рельсовые направляющие с держателем кабелей	29,2 кг (64,3 фунта)
Габариты	**Сеть**
Высота: 8,7 см (3,4 дюйма) **Ширина:** 48,2 см (19 дюймов) с защелками стойки 44,4 см (17,5 дюйма) без защелок стойки **Глубина:** 75,5 см (29,7 дюйма) с блоком питания и кромкой 74,1 см (29,2 дюйма) без блоков питания и кромки	**Порт управления:** 1; медный 10/100/1000 **Порты мониторинга/прослушивания:** 3

Технические характеристики FlowCollector серии 4000	
Влажность (относительная)	**Высота (над уровнем моря)**
Эксплуатация: 10–80% (без конденсации) с макс. точкой росы 26 °C (78,8 °F) Хранение: 5–95% (без конденсации) с макс. точкой росы 33 °C (91 °F) **Хранение:** 5–95% (без конденсации) с макс. точкой росы 33 °C (91 °F)	**Эксплуатация:** от –15,2 до 3048 м (от –50 до 10 000 футов) **Хранение:** от –15,2 до 12 000 м (от –50 до 39 370 футов)
Питание	**Теплоотдача**
750 Вт пер. тока, 50/60 Гц (с резервированием) Авторегулировка (от 100 В до 240 В)	2891 БТЕ в час максимум
Температурный режим	**Вибрационная нагрузка**
Эксплуатация: 10–35 °C (50–95 °F) при относительной влажности 10–80%, с макс. точкой росы 26 °C (78,8 °F) **Примечание.** Для высоты над уровнем моря выше 900 м (2,952 фута) максимально допустимая температура сухого термометра снижается на -17 °C (1 °F) каждые 167 м (550 футов). **Хранение:** от –40 до 65 °C (от –40 до 149 °F) с максимальным перепадом температуры 20 °C (68 °F) в час	**Максим. при эксплуатации:** 0,26g среднекв. при 5–350 Гц во всех положениях **Максим. при хранении:** 1,87g среднекв. при 10–500 Гц на 15 минут (протестированы все 6 сторон)
Ударная нагрузка	**Нормативные требования**
Максим. при эксплуатации: полусинусоидальный импульс во всех рабочих положениях с ускорением 31g ± 5% и длительностью импульсов 2,6 мс ± 10% **Максим. при хранении:** полусинусоидальный импульс по всем 6 сторонам с ускорением 71g ± 5% и длительностью импульсов 2 мс ± 10%; прямоугольный импульс по всем 6 сторонам с ускорением 27g при изменении скорости в 6 м/с или более.	• FCC (только для США), класс A • DOC (Канада), класс A • Маркировка CE (EN 55022, класс A, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 60950) • VCCI, класс A • UL 1950 • CSA 950 Запросите полный список по телефону.

Способ размещения

Правила и условия монтажа, подключения к сети и введения в эксплуатацию.

Сведения об ограничениях в использовании технического средства с учетом его предназначения для работы в жилых, коммерческих или производственных зонах.

Оборудование предназначено для производственной или иной коммерческой деятельности в зонах без воздействия вредных и опасных производственных факторов. Техническое средство не бытового назначения. Оборудование предназначено для эксплуатации без постоянного присутствия обслуживающего персонала. Оборудование подлежит установке и обслуживанию специалистами, обладающими соответствующей квалификацией, достаточными специальными знаниями и навыками.

Требования обеспечения безопасности

Перед установкой устройства Cisco рекомендуется учесть следующие моменты:

- Размещайте устройство в запираемой стойке в защищенном месте для предотвращения доступа неуполномоченного персонала.
- Разрешить только обученному и квалифицированному персоналу установку, замену, администрирование или обслуживание устройства.
- Подключайте интерфейс управления только к безопасной внутренней сети управления, защищенной от несанкционированного доступа.
- Укажите IP-адреса конкретных рабочих станций, которым можно подключаться к устройствам.

Контроль статического электричества

внимание: Процедуры контроля электростатического разряда (например, использование антистатической манжеты и рассеивающей статическое электричество рабочей поверхности) должны быть применены до распаковки, установки или перемещения устройства. Сильные электростатические разряды могут повредить устройство или нарушить его работу.

Правила и условия безопасной эксплуатации

Продукт класса B

Для обеспечения электромагнитной совместимости, устройство должно быть установлено согласно инструкциям, описанным в руководстве по установке оборудования.

Правила и условия хранения, перевозки, реализации и утилизации

Диапазон температур при хранении (в выключенном состоянии): от -40 до 65 °C

Диапазон относительной влажности воздуха (в выключенном состоянии): от 5 до 95%, без конденсации

Оборудование должно храниться в помещении в заводской упаковке.

Транспортировка оборудования должна производиться в заводской упаковке в крытых транспортных средствах любым видом транспорта.

Температура при перевозке: от -40 до 65 °C.

Правила и условия реализации оборудования определяются условиями договоров, заключаемых компанией Cisco или авторизованными партнерами Cisco с покупателями оборудования.

Утилизация этого изделия по завершении его срока службы должна выполняться в соответствии с требованиями всех государственных нормативов и законов.

Общие указания

Оборудование предназначено для производственной или иной коммерческой деятельности в зонах без воздействия вредных и опасных производственных факторов. Техническое средство не бытового назначения. Оборудование предназначено для эксплуатации без постоянного присутствия обслуживающего персонала. Оборудование подлежит установке и обслуживанию специалистами, обладающими соответствующей квалификацией, достаточными специальными знаниями и навыками.

Информация о мерах, которые следует принять при обнаружении неисправности технического средства

В случае обнаружения неисправности технического средства, а также для принятия претензий к качеству оборудования обратитесь в компанию, у которой приобретен данный продукт.

Кроме того, информацию о технической поддержке Cisco можно получить на официальном веб-сайте Cisco:

http://www.cisco.com/cisco/web/RU/support/index.html

Вы также можете воспользоваться автоматической программой для поиска наиболее подходящего контакта в компании Cisco:

http://www.cisco.com/cisco/web/siteassets/contacts/index.html?locale=ru_RU

Общий многоканальный телефон:

+7 495 961 13 82 (Москва), (8 800) 700 05 22 (Россия)

Беларусь: 800 721 7549;

Казахстан: 8 800 121 4321 (наберите 8, подождите до 2-го сигнала, затем наберите остальные цифры; наберите PIN 800 721 7549).

При наличии действующего контракта на сервисную поддержку в Службе поддержки Cisco Technical Assistance Center (TAC), обратитесь в службу технической поддержки по телефону:

+7 495 961 13 82 (Москва), (8 800) 700 05 22 (Россия) — меню «Технические услуги».

Подробная информация об услугах технической поддержки доступна на сайте:

http://www.cisco.com/cisco/web/support/RU/tac_overview.html

http://www.cisco.com/cisco/web/RU/support/index.html

Изготовитель гарантирует соответствие основных технических характеристик оборудования техническим характеристикам, приведенным на этикетке, при соблюдении условий и правил хранения, транспортирования, монтажа и эксплуатации, установленных технической документацией.

Гарантия и сервисная поддержка не распространяются на оборудование в следующих случаях:

- при изменении, модификации, неправильном обращении, уничтожении или повреждении, вызванном следующими причинами: (i) естественными причинами; (ii) воздействием окружающей среды; (iii) отказом принять любые необходимые меры; (iv) небрежным или преднамеренным действием или бездействием или использованием в целях, отличных от тех, которые определены в применимой документации; (v) действием или бездействием третьего лица;
- при признаках воздействия огня; воды; химических веществ, включая нанесение краски, покрытие иными веществами, но не ограничиваясь этим; неправильной эксплуатации; самостоятельного ремонта; изменения внутреннего устройства; при наличии механических повреждений; при наличии признаков, вызванных попаданием внутрь посторонних предметов, жидкостей, насекомых; при повреждениях, вызванных несоответствием действующим Техническим регламентам, Государственным стандартам, НПА по вопросам применения на сети связи общего пользования и другим применимым официальным требованиям параметров питающих, телекоммуникационных, кабельных сетей и других подобных внешних факторов.

В таблице ниже поясняется, как узнать дату производства для каждой модели.

Модели	Дата производства
StealthWatch FlowCollector Appliance	Неделя производства зашифрована в стандартном серийном номере Cisco из 11 цифр в формате LLLYYWWSSSS, где: LLL — буквенно-цифровое местоположение поставщика в системе счисления с основанием 34; YYWW — числовое выражение года и недели в десятичной системе; SSSS — буквенно-цифровой последовательный серийный номер в системе счисления с основанием 34.

Дополнительная информация

См. руководство по установке и настройке аппаратного обеспечения в библиотеке документов в разделе справки консоли управления StealthWatch.

Техническая поддержка

Дополнительная информация, руководства и правила обращения с продуктом, а также возможность загрузки ПО доступны в разделе Product/Technology Support на официальном веб-сайте Cisco:

http://www.cisco.com/cisco/web/psa/default.html

Сохраните упаковку и этикетку. В случае если упаковка утрачена, повреждена или на ней отсутствует информация об импортере или стране, где изготовлено техническое средство, для получения информации об импортере обратитесь, пожалуйста, в компанию, у которой приобретено техническое средство. Информация о стране производства (на английском языке) указана на продукте. Также для получения информации о стране производства можно использовать веб-приложение Trade Tool на сайте cisco.com (на английском языке, требуется серийный номер устройства и регистрация на сайте cisco.com):

http://tools.cisco.com/FinAdm/GCTA/servlet/ControllerServlet?action=QueryForm

Компания-изготовитель оставляет за собой право изменять настоящий документ без предварительного уведомления.

Наименование и местонахождение уполномоченного изготовителем лица.

Уполномоченное изготовителем лицо на территории стран Таможенного союза: ООО «Сиско Системс»

Адрес местонахождения: 115054, г. Москва, Космодамианская наб., 52, стр. 1. Телефон: (495) 961-14-10. E-mail: rus-cert@cisco.com

Офис в Республике Беларусь:

Республика Беларусь, 220034, Минск, бизнес-центр «Виктория Плаза» ул. Платонова, д. 1Б, 3-й подъезд, 2-й этаж

Телефон: +375-17-2691691; факс: +375-17-2691699; www.cisco.ru

Офис в Республике Казахстан:

Казахстан, 050059, Алматы, бизнес-центр «Самал Тауэрс»,

ул. О. Жолдасбекова, 97, блок А2, 14-й этаж

Телефон: +7-727-244-2101; факс +7-727-244-2102; www.cisco.ru

Россия, 115054, Москва, Космодамианская набережная, 52, стр.1 (Riverside Towers), 4-й этаж

Телефон: 7-495-961-1410; факс: 7-495-961-1469; www.cisco.ru

Штаб-квартира в США:

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706 USA (США) www.cisco.com