Системы предотвращения атак серии N

Информация о продукте

Обзор продукта

Системы предотвращения атак серии N обеспечивают новый уровень безопасности и защиту в реальном времени, предоставляя средства для проактивной защиты трафика сети и центра обработки данных сегодня и в будущем. Архитектура платформы IPS нового поколения предлагает широкие возможности для глубокого анализа трафика, а модульная структура программного обеспечения позволяет дополнять систему защиты от атак новыми эффективными службами защиты сети. Эта аппаратная платформа представляет собой новый этап в развитии решений для защиты от атак, делая их основой системы комплексной защиты сети.

Основные возможности

- Доказавшие свое превосходство в своевременном блокировании атак средства защиты.
- Многоцелевая современная система с широкими возможностями IPS.
- Лучшая в отрасли группа исследователей в области безопасности — DVLabs.
- Снижение расходов и сложности системы безопасности.
- Лучшее средство для обеспечения сетевой безопасности.

Возможности и преимущества

Технические возможности

- **Система защиты от вторжений (IPS).** Системы IPS серии N обеспечивают новый уровень безопасности и защиту в реальном времени, предоставляя средства для проактивной защиты трафика сети и центра обработки данных сегодня и в будущем. Архитектура этих систем предоставляет широкие возможности для глубокой инспекции трафика, а модульная структура программного обеспечения позволяет добавлять новые компоненты защиты.
- **Надежная и оперативная защита.** С 2001 г. нашей главной целью было создание решений IPS, обеспечивающих проактивную и оперативную защиту в сочетании с высокой производительностью и доступностью сети. Полноценное решение по обеспечению безопасности сети не должно приводить к снижению ее производительности и работоспособности. Согласно исследованию, проведенному компанией Infonetics Research в 2008 году, большинство корпоративных заказчиков используют наши решения IPS.
- **Новая расширяемая инфраструктура безопасности с высокой масштабируемостью.** Платформа IPS включает в себя расширяемую инфраструктуру защиты с модульной структурой программного обеспечения, которая поддерживает быструю разработку и развертывание новых комплектов фильтров IPS, служб безопасности и решений сторонних производителей.
- **Новые модули защиты для систем IPS.** Системы IPS серии N позволяют интегрировать новые модули защиты, в том числе определяемые заказчиком данные о репутации IP и DNS, Reputation Digital Vaccine Service, Web Application Digital Vaccine (DV) Service, политики на основе местоположения IPS (периметр, ядро и т. д.) и настраиваемые заказчиком защитные фильтры.
- **Модульная конструкция для интеграции решений.** Модульная конструкция платформы IPS обеспечивает интеграцию с решениями по обеспечению безопасности от сторонних производителей, включая продукты для оценки и управления уязвимостями (VA/VM), решения для криминалистического анализа, системы управления информацией о безопасности (SIM) и продукты для обнаружения сетевых аномалий (NBAD).
- **Поддержка различных типов трафика.** Платформа IPS поддерживает множество типов трафика и протоколов. Она обеспечивает превосходную одновременную проверку протоколов IPv6 и IPv4 и поддерживает туннелирование (4in6, 6in4 и 6in6). Кроме того, она поддерживает проверку трафика IPv6 и IPv4 с тегами VLAN и MPLS, мобильного трафика IPv4, GRE и GTP (туннелирование GPRS), а также кадров крупных размеров, благодаря чему ИТ-администраторы получают гибкость и могут развертывать средства защиты IPS в любом месте сети.
- **Новый механизм блокирования атак (TSE).** Платформа IPS использует новый механизм блокирования атак (TSE), чтобы справляться с быстро изменяющимися угрозами и требованиями сетей и центров обработки данных современных предприятий. Архитектура TSE применяет специализированные модули ASIC и высокопроизводительные сетевые процессоры для полной проверки потоков пакетов на уровнях 2 – 7, обеспечивая для каждого потока тысячи параллельных проверок и предоставляя широкие возможности глубокой инспекции трафика для новых и будущих модулей защиты.
- **Проверенная надежность и резервирование.** Платформа IPS обеспечивает непревзойденный уровень доступности сети. Она помогает поддерживать высокую скорость передачи данных даже в случае сбоя в работе сети, неисправности внутреннего устройства или отключения электроэнергии. Существует два взаимодополняющих режима высокой доступности (гарантирование того, что трафик не будет задержан внутри устройства и дублирование сегментов внешней сети с сохранением состояния соединений), которые обеспечивают высочайшее время бесперебойной работы и доступность для платформы IPS и устройств SMS.
- **Встроенные функции высокой доступности.** Платформа IPS имеет несколько функций для режима внутренней высокой доступности, в том числе два блока питания горячей замены, аппаратные таймеры системы безопасности для непрерывного мониторинга механизмов безопасности и управления, благодаря которым при внутренней ошибке система IPS может автоматически переключаться на резервные ресурсы, а также средства высокой доступности при выключении питания (ZPHA), обеспечивающие прохождение всего трафика даже при сбоях питания за счет переключения интерфейсов IPS на ретранслятор пакетов, работающий при выключенном питании ZPHA.
- **Возможности резервирования.** Две платформы IPS могут быть развернуты с использованием резервных соединений в прозрачном режиме высокой доступности «активный – активный» или «активный – пассивный». Поскольку платформа IPS действует независимо от общей инфраструктуры, не имеет IP-адреса и не участвует в протоколах маршрутизации, ее можно развертывать в существующих сетях без изменения конфигурации, в том числе при использовании протоколов маршрутизации высокой доступности, таких как VRRP, OSPF и HSRP, которые прозрачно поддерживаются системой IPS.
- **Поддержка высоких скоростей для центров обработки данных и ядра сети.** Системы IPS серии N предназначены для защиты центров обработки данных и ядра сети. В этих критически важных областях сети контроллер HP для ядра сети в сочетании с пулом платформ IPS обеспечивает автоматизированную проверку со скоростью до 20 Гбит/с для надежной защиты сетевых устройств, программного обеспечения виртуализации, операционных систем и приложений от атак без снижения производительности.

- **Короткая задержка пакетов в устройстве, повышающая удобство для пользователей.** Уникальная архитектура платформы IPS обеспечивает полную проверку потоков пакетов и надежную передачу внутри платформы с задержкой менее 80 микросекунд независимо от количества используемых фильтров и модулей защиты. Благодаря этому пользователь не замечает изменений в производительности приложений.
- **Высочайшая точность фильтров предотвращает блокировку безопасного трафика.** Для обеспечения точности фильтров мы используем два простых правила — не должно быть ложных положительных срабатываний и не должно быть ложных отрицательных срабатываний. Именно поэтому наша группа исследователей безопасности DVLabs концентрируется на создании фильтров для защиты всех уязвимостей, а не только предотвращения известных угроз. Фильтры уязвимостей блокируют все возможности использования слабых мест ПО и обеспечивают высочайший уровень точности, благодаря чему системы IPS не блокируют безопасный трафик при защите сети.
- **Применение виртуальных исправлений для защиты систем без исправлений.** Специалисты DVLabs создают фильтры уязвимостей, которые блокируют все возможности использования определенной уязвимости за счет предоставления так называемой защиты Virtual Patch. Эти фильтры защищают уязвимости в программном обеспечении виртуализации, операционных системах и приложениях и не связаны с конкретными известными атаками. Они фильтруют атаки на хосты и приложения, у которых не установлены обновления. И у атакующего создается впечатление, как будто бы обновления уже установлены. Поэтому эти обновления называются виртуальными.
- **Специализированное оборудование и программное обеспечение.** Для блокировки кибератак на скорости в несколько гигабит с чрезвычайно низкими задержками требуется специализированное оборудование и программное обеспечение. Решения других поставщиков используют оборудование и процессоры общего назначения, которые не способны выполнять проверку без снижения производительности сети, однако наша платформа IPS обеспечивает надежную защиту от угроз на высоких скоростях с очень низкой задержкой.
- **Ведущая группа исследователей в области безопасности — Digital Vaccine Labs (DVLabs).** DVLabs — это лучшая группа исследователей в области безопасности, осуществляющая выявление уязвимостей. В состав группы входят признанные в отрасли исследователи, которые применяют в своей работе самые передовые средства инжиниринга и анализа. DVLabs является лидером по количеству ежегодно обнаруживаемых уязвимостей. Исследователи создают фильтры уязвимостей, которые доставляются на платформы IPS заказчиков с помощью службы Digital Vaccine Service.
- **Портал безопасности ThreatLinQ.** ThreatLinQ — это служба, которая позволяет нашим пользователям IPS получать сведения о новейших угрозах по всему миру на основе данных, собираемых с глобальной сети устройств мониторинга Lighthouse и тысяч платформ IPS, используемых заказчиками. Служба ThreatLinQ доступна всем нашим заказчикам и предоставляет ценную информацию, с помощью которой компании могут научиться более эффективно настраивать сетевые политики безопасности в соответствии с существующими тенденциями в области угроз и смотреть, как настраивают свои политики безопасности другие.
- **Самые быстрые в отрасли средства защиты от угроз для надежной защиты.** Наша служба Digital Vaccine Service обеспечивает постоянную (непрерывно обновляемую) защиту от новых угроз. Обновления Digital Vaccine доставляются заказчикам два раза в неделю или мгновенно при обнаружении критических уязвимостей и могут развертываться автоматически без участия ИТ-специалистов. Эти обновления гарантируют защиту от конкретных атак и их потенциальных разновидностей, предотвращая угрозы атак нулевого дня.
- **Программа Zero-Day Initiative (ZDI) обеспечивает лучшую защиту от атак нулевого дня.** Группа DVLabs управляет программой ZDI, в рамках которой поощряются исследователи по всему миру за предоставление сведений об обнаруженных уязвимостях. DVLabs передает сведения обо всех известных уязвимостях, полученные в результате внутренних исследований DVLabs или по программе ZDI, поставщикам соответствующего программного обеспечения и создает фильтры IPS для защиты заказчиков от потенциальных атак нулевого дня, прежде чем об уязвимости станет широко известно.
- **Комплексная защита IPS от угроз и уязвимостей для обеспечения максимальной безопасности.** Благодаря талантливым специалистам, исследовательским возможностям и аналитике в области безопасности от исследовательской группы DVLabs мирового класса, более 1200 исследователей в рамках программы ZDI, глобальному мониторингу угроз ThreatLinQ от тысяч заказчиков, а также партнерству с участниками сообщества по безопасности, такими как Институт SANS, CERT и NIST, мы обеспечиваем защиту от широчайшего спектра угроз и уязвимостей для достижения максимальной безопасности.
- **Защита от угроз во всех областях.** Системы HP IPS серии N обеспечивают исключительный охват уязвимостей и защищают все элементы, в том числе сетевые устройства, ПО виртуализации, операционные системы, корпоративные и веб-приложения, а также сети системы промышленного управления SCADA (УСУТП). Решения HP TippingPoint, охватывающие ОС Microsoft®, системы SCADA, фильтры VoIP и многое другое, обеспечивают действительно высокий уровень сетевой защиты для современных сложных корпоративных ИТ-сред.

- **Reputation DV Service исключает заведомо нежелательный трафик.** Дополнительная служба Reputation Digital Vaccine (Rep DV) Service предоставляет данные о небезопасных адресах IPv4, IPv6 и DNS из глобальной репутационной базы данных DVLabs, позволяющие заказчикам активно применять и управлять репутационными политиками безопасности с помощью платформы IPS, которая выступает в качестве точки применения. Платформа проверяет трафик в реальном времени, выявляет заведомо нежелательный трафик и применяет политики безопасности Rep DV.
- **Автоматизированная, проактивная защита IPS исключает большинство трудоемких ручных задач при возникновении событий.** Автоматизированное применение политик практически полностью устраняет необходимость реагировать на множество оповещений (как реальных, так и ложных) и выполнять очистку после кибератак на сетевые ресурсы. Поскольку не требуется применять исправления сразу же и реагировать на оповещения, расходы на обеспечение безопасности ИТ значительно снижаются, а благодаря уменьшению нагрузки на пропускную способность и защите критически важных приложений возрастает продуктивность ИТ и прибыльность.
- **Устранение необходимости применять исправления в аварийном режиме и защита систем от атак нулевого дня.** Наши фильтры уязвимостей практически полностью устраняют необходимость устанавливать исправления вручную или в аварийном режиме. Благодаря защите уязвимостей программного обеспечения ИТ-специалисты могут внедрять исправления с помощью регулярного, запланированного процесса вместо использования дорогостоящих аварийных процедур. Системы IPS серии N блокируют атаки и позволяют ИТ-персоналу тестировать исправления безопасности перед развертыванием.
- **Улучшенный контроль за компьютерами пользователей.** Большинство ИТ-отделов не может адекватно контролировать компьютеры пользователей. В недавно выпущенном отчете указывается на то, что исправлениями клиентских приложений становится все сложнее управлять вследствие растущего числа уязвимостей. Платформа IPS улучшает ИТ-контроль благодаря защите уязвимостей в системах без исправлений, сегментации сети для блокировки вредоносного трафика с зараженных пользовательских компьютеров и уведомления администратора об источнике атак.
- **Повышение производительности сети за счет перераспределения неиспользуемой пропускной способности.** Системы IPS серии N имеют возможности управления пропускной способностью, позволяющие ограничивать нагрузку на сеть от несанкционированных приложений (таких как пиринговые сети и потоковое мультимедиа). Благодаря непрерывной очистке сети от вредоносного и нежелательного трафика можно обеспечить максимальную производительность сети для критически важных приложений, а ограничение нагрузки от несанкционированных приложений позволяет значительно повысить доступность пропускной способности, иногда на 40 – 70%.
- **Удобная установка за несколько минут позволяет снять нагрузку с ИТ-персонала.** Платформа IPS значительно сокращает время и ресурсы, необходимые для обеспечения высокой работоспособности сети. IPS и система управления безопасностью (SMS) легко устанавливаются в сети (процедура обычно занимает от 30 минут до двух часов). Система IPS не требует изменений существующей сети и легко развертывается без IP- и MAC-адреса, благодаря чему сразу начинает фильтрацию вредоносного и нежелательного трафика.
- **Удобные в управлении решения уменьшают нагрузку на ИТ-персонал.** Средство SMS легко обнаруживает, осуществляет мониторинг, настраивает, выполняет диагностику и создает отчеты от нескольких устройств IPS. Оно имеет простой, современный, безопасный клиентский интерфейс, который обеспечивает анализ общей ситуации с помощью отчетов о тенденциях, корреляций и графиков реального времени о статистике трафика, отфильтрованных атаках, сетевых хостах и службах, а также ресурсах и состоянии IPS. Администрирование возможно из Windows, Lunux и Mac OS.
- **Гибкие возможности локального управления.** Каждый модуль IPS также имеет встроенный локальный веб-интерфейс управления (LSM) и интерфейс командной строки (CLI). LSM — это управляющее приложение с защищенным веб-интерфейсом, предоставляющее возможности администрирования, настройки и отчетности.
- **Обновления Automated Digital Vaccine сокращают время, затрачиваемое на текущее управление.** Возможности автоматической загрузки и распространения Automated Digital Vaccine (DV) уменьшают время, необходимое для управления платформой IPS. SMS поддерживает ручную загрузку и распространение DV или автоматическую загрузку и ручное распространение DV.
- **Простые, но мощные политики безопасности.** Системы IPS серии N позволяют администраторам безопасности настраивать мельчайшие аспекты политики безопасности. Администраторы могут установить определенные сетевые политики безопасности для сегмента сети, VLAN или подсети (CIDR). Кроме того, с помощью репутационных возможностей платформы IPS и службы Reputation Digital Vaccine заказчики теперь могут внедрить информацию о вредоносных IP-адресах и именах DNS в систему управления политиками безопасности.
- **Автоматизированное применение политик безопасности для обеспечения соответствия.** Системы IPS серии N могут быть критически важным компонентом любой программы обеспечения соответствия ИТ. Они решают многие задачи, связанные с обеспечением соответствия законодательству и нормативным актам, в том числе осуществляют управление уязвимостями с помощью Digital Vaccine Service и сетевой мониторинг с помощью системы управления безопасностью. Кроме того, IPS может выполнять компенсирующий контроль, когда требования невозможно удовлетворить другими процессами или решениями.

- **Широкие возможности отчетности о безопасности позволяют получить сведения для аудита.** Благодаря возможностям создания отчетов IPS и SMS администраторы могут демонстрировать внутренним и внешним аудиторам, как сеть защищена от современных угроз. Наряду с удовлетворением нормативных и внутренних требований организации могут использовать лучшие средства применения функций безопасности в своих сетях.

Гарантия и поддержка

- **Гарантия 1 год.** Гарантийная замена и доставка в течение 30 календарных дней (доступно в большинстве стран).
- **Поддержка с помощью электронных средств и по телефону.** HP предоставляет ограниченную поддержку с помощью электронных средств и по телефону; подробные сведения о порядке и сроках предоставления поддержки см. по адресу: www.hp.com/networking/warranty.
- **Выпуски программного обеспечения.** Подробные сведения о выпусках программного обеспечения и сроках их доступности для продуктов см. по адресу: www.hp.com/networking/warranty.

Системы HP S Intrusion Prevention System (IPS) серии N

Технические характеристики

	 **HP S660N 750 Mbps 5 Gig-T/5 1Gb Fiber Segments IPS (JC019A)**	 **HP S1400N 1.5 Gbps 5 Gig-T/5 1Gb Fiber Segments IPS (JC020A)**	 **HP S2500N 3Gbps 5 Gig-T/1 10GbE/5 1GbE Fiber Segments IPS (JC021A)**
Порты	10 портов 10/100/1000 с автоматическим определением скорости RJ-45 (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); дуплексная связь: 10BASE-T/100BASE-TX — полудуплексная или дуплексная, 1000BASE-T — только дуплексная 10 встроенных портов Gigabit Ethernet SFP	10 портов 10/100/1000 с автоматическим определением скорости RJ-45 (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); дуплексная связь: 10BASE-T/100BASE-TX — полудуплексная или дуплексная, 1000BASE-T — только дуплексная 10 встроенных портов Gigabit Ethernet SFP	10 портов 10/100/1000 с автоматическим определением скорости RJ-45 (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); дуплексная связь: 10BASE-T/100BASE-TX — полудуплексная или дуплексная, 1000BASE-T — только дуплексная 10 встроенных портов Gigabit Ethernet SFP 2 порта XFP 10-GbE (IEEE 802.3ae Type 10GBASE-LR); дуплексная связь: только дуплексная
Физические характеристики			
Размеры	60,96 (г) x 42,86 (ш) x 8,69 см (в) (высота 2U)	60,96 (г) x 42,67 (ш) x 8,69 см (в) (высота 2U)	60,96 (г) x 42,88 (ш) x 8,69 см (в) (высота 2U)
Масса	13,2 кг	13,2 кг	14,29 кг
Монтаж	Прилагаются скобы 19" и 23" для монтажа в стойке	Прилагаются скобы 19" и 23" для монтажа в стойке	Прилагаются скобы 19" и 23" для монтажа в стойке
Производительность			
Задержка	< 80 мкс	< 80 мкс	< 80 мкс
Пропускная способность IPS/IDS	750 Мбит/с	1,5 Гбит/с	3 Гбит/с
Пропускная способность сети	750 Мбит/с	1,5 Гбит/с	15 Гбит/с
Контексты обеспечения безопасности	1 200 000	1 200 000	2 600 000
Соединения в секунду	115 000	115 000	230 000
Одновременные сеансы	6 500 000	6 500 000	10 000 000
Условия окружающей среды			
Рабочая температура	0 °C ... 40 °C	0 °C ... 40 °C	0 °C ... 40 °C
Рабочая относительная влажность	5 ... 95% без конденсации	5 ... 95% без конденсации	5 ... 95% без конденсации
Температура хранения	-20 °C ... 70 °C	-20 °C ... 70 °C	-20 °C ... 70 °C
Относительная влажность при хранении	5 ... 95% без конденсации	5 ... 95% без конденсации	5 ... 95% без конденсации
Электрические характеристики			
Напряжение	100 – 240 В переменного тока	100 – 240 В переменного тока	100 – 240 В переменного тока
Сила тока	8/5 A	8/5 A	8/5 A
Частота	50/60 Гц	50/60 Гц	50/60 Гц
Безопасность	UL 60950-1; EN 60825-1 , безопасность лазерных устройств — часть 1; EN 60825-2 , безопасность лазерных устройств — часть 2; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; соответствие ROHS	UL 60950-1; EN 60825-1, безопасность лазерных устройств — часть 1; EN 60825-2 , безопасность лазерных устройств — часть 2; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; соответствие ROHS	UL 60950-1; EN 60825-1 , безопасность лазерных устройств — часть 1; EN 60825-2 , безопасность лазерных устройств — часть 2; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; соответствие ROHS
Излучение	FCC класса A; VCCI класса A; EN 55022 класса A; AS/NZS 3548 класса A; ICES-003 класса A	FCC класса A; VCCI класса A; EN 55022 класса A; AS/NZS 3548 класса A; ICES-003 класса A	FCC класса A; VCCI класса A; EN 55022 класса A; AS/NZS 3548 класса A; ICES-003 класса A
Защищенность			
Электростатический разряд (ESD)	EN 61000-4-2	EN 61000-4-2	EN 61000-4-2
Радиационная стойкость	EN 61000-4-3	EN 61000-4-3	EN 61000-4-3
EFT/импульсные помехи	EN 61000-4-4	EN 61000-4-4	EN 61000-4-4
Импульсная перегрузка	EN 61000-4-5	EN 61000-4-5	EN 61000-4-5
Кондуктивные помехи	EN 61000-4-6	EN 61000-4-6	EN 61000-4-6
Кратковременные перебои напряжения	EN 61000-4-11	EN 61000-4-11	EN 61000-4-11
Гармоники	EN 61000-3-2	EN 61000-3-2	EN 61000-3-2
Мерцание	EN 61000-3-3	EN 61000-3-3	EN 61000-3-3
Управление	Security Management Server (SMS); интерфейс командной строки; веб-браузер; HP TippingPoint IPS MIB	Security Management Server (SMS); интерфейс командной строки; веб-браузер; HP TippingPoint IPS MIB	Security Management Server (SMS); интерфейс командной строки; веб-браузер; HP TippingPoint IPS MIB

Системы HP S Intrusion Prevention System (IPS) серии N

Технические характеристики (продолжение)

	HP S660N 750 Mbps 5 Gig-T/5 1Gb Fiber Segments IPS (JC019A)	HP S1400N 1.5 Gbps 5 Gig-T/5 1Gb Fiber Segments IPS (JC020A)	HP S2500N 3Gbps 5 Gig-T/1 10GbE/5 1GbE Fiber Segments IPS (JC021A)
Примечания	Заметки о производительности. • Пропускная способность IPS/IDS представляет собой показатели пропускной способности, полученные в результате испытаний с применением рекомендуемых профилей безопасности. • Пропускная способность сети представляет собой максимальные показатели пропускной способности при ретрансляции трафика без проверки. • Стандартное время задержки получено в результате измерений с использованием пакетов размером до 1518 байтов. • Число одновременных сетевых сеансов представляет собой максимальное количество одновременных сетевых сеансов, поддерживаемое системой IPS. • Контексты безопасности представляют собой максимальное количество сеансов в защищенном режиме, поддерживаемое системой IPS.	Заметки о производительности. • Пропускная способность IPS/IDS представляет собой показатели пропускной способности, полученные в результате испытаний с применением рекомендуемых профилей безопасности. • Пропускная способность сети представляет собой максимальные показатели пропускной способности при ретрансляции трафика без проверки. • Стандартное время задержки получено в результате измерений с использованием пакетов размером до 1518 байтов. • Число одновременных сетевых сеансов представляет собой максимальное количество одновременных сетевых сеансов, поддерживаемое системой IPS. • Контексты безопасности представляют собой максимальное количество сеансов в защищенном режиме, поддерживаемое системой IPS.	Заметки о производительности. • Пропускная способность IPS/IDS представляет собой показатели пропускной способности, полученные в результате испытаний с применением рекомендуемых профилей безопасности. • Пропускная способность сети представляет собой максимальные показатели пропускной способности при ретрансляции трафика без проверки. • Стандартное время задержки получено в результате измерений с использованием пакетов размером до 1518 байтов. • Число одновременных сетевых сеансов представляет собой максимальное количество одновременных сетевых сеансов, поддержи-ваемое системой IPS. Измеренное значение ограничено возможностями доступного тестового оборудования. • Контексты безопасности представляют собой максимальное количество сеансов в защищенном режиме, поддерживаемое системой IPS.
Услуги	Обозначения и описание уровней обслуживания см. на веб-сайте HP по адресу: www.hp.com/networking/services. Для получения информации об услугах и времени реакции в вашем регионе обратитесь в ближайшее торговое представительство HP.	Обозначения и описание уровней обслуживания см. на веб-сайте HP по адресу: www.hp.com/networking/services. Для получения информации об услугах и времени реакции в вашем регионе обратитесь в ближайшее торговое представительство HP.	Обозначения и описание уровней обслуживания см. на веб-сайте HP по адресу: www.hp.com/networking/services. Для получения информации об услугах и времени реакции в вашем регионе обратитесь в ближайшее торговое представительство HP.

Системы HP S Intrusion Prevention System (IPS) серии N

Технические характеристики (продолжение)

	HP S5100N 5Gbps 5 GigT/1 10GbE/5 1GbE Fiber Segments IPS (JC022A)	HP S6100N 8Gbps IPS (JC577A)
Порты	10 портов 10/100/1000 с автоматическим определением скорости RJ-45 (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); дуплексная связь: 10BASE-T/100BASE-TX — полудуплексная или дуплексная, 1000BASE-T — только дуплексная 10 встроенных портов Gigabit Ethernet SFP 2 порта XFP 10-GbE (IEEE 802.3ae Type 10GBASE-LR); дуплексная связь: только дуплексная	10 портов 10/100/1000 с автоматическим определением скорости RJ-45 (IEEE 802.3 Type 10BASE-T, IEEE 802.3u Type 100BASE-TX, IEEE 802.3ab Type 1000BASE-T); дуплексная связь: 10BASE-T/100BASE-TX — полудуплексная или дуплексная, 1000BASE-T — только дуплексная 10 встроенных портов Gigabit Ethernet SFP 2 порта XFP 10-GbE (IEEE 802.3ae Type 10GBASE-LR); дуплексная связь: только дуплексная
Физические характеристики		
Размеры	60,96 (г) x 42,88 (ш) x 8,69 см (в) (высота 2U)	60,96 (г) x 42,88 (ш) x 8,69 см (в) (высота 2U)
Масса	14,29 кг	14,29 кг
Монтаж	Прилагаются скобы 19" или 23" для монтажа в стойке	Прилагаются скобы 19" или 23" для монтажа в стойке
Производительность		
Задержка	< 80 мкс	< 80 мкс
Пропускная способность IPS/IDS	5 Гбит/с	8 Гбит/с*
Пропускная способность сети	15 Гбит/с	15 Гбит/с
Контексты обеспечения безопасности	2 600 000	2 600 000
Соединения в секунду	230 000	230 000
Одновременные сеансы	10 000 000	10 000 000
Условия окружающей среды		
Рабочая температура	0 °C ... 40 °C	0 °C ... 40 °C
Рабочая относительная влажность	5 ... 95% без конденсации	5 ... 95% без конденсации
Температура хранения	-20 °C ... 70 °C	-20 °C ... 70 °C
Относительная влажность при хранении	5 ... 95% без конденсации	5 ... 95% без конденсации
Электрические характеристики		
Напряжение переменного тока	100 – 240 В	100 – 240 В
Сила тока	8/5 А	8/5 А
Частота	50/60 Гц	50/60 Гц
Безопасность	UL 60950-1; EN 60825-1 , безопасность лазерных устройств — часть 1; EN 60825-2 , безопасность лазерных устройств — часть 2; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; соответствие ROHS	UL 60950-1; EN 60825-1 , безопасность лазерных устройств — часть 1; EN 60825-2 , безопасность лазерных устройств — часть 2; IEC 60950-1; EN 60950-1; CSA 22.2 60950-1; соответствие ROHS
Излучение	FCC класса A; VCCI класса A; EN 55022 класса A; AS/NZS 3548 класса A; ICES-003 класса A	FCC класса A; VCCI класса A; EN 55022 класса A; AS/NZS 3548 класса A; ICES-003 класса A
Защищенность		
Электростатический разряд (ESD)	EN 61000-4-2	EN 61000-4-2
Радиационная стойкость	EN 61000-4-3	EN 61000-4-3
EFT/импульсные помехи	EN 61000-4-4	EN 61000-4-4
Импульсная перегрузка	EN 61000-4-5	EN 61000-4-5
Кондуктивные помехи	EN 61000-4-6	EN 61000-4-6
Кратковременные перебои напряжения	EN 61000-4-11	EN 61000-4-11
Гармоники	EN 61000-3-2	EN 61000-3-2
Мерцание	EN 61000-3-3	EN 61000-3-3
Управление	Security Management Server (SMS); интерфейс командной строки; веб-браузер; HP TippingPoint IPS MIB	Security Management Server (SMS); интерфейс командной строки; веб-браузер; HP TippingPoint IPS MIB
Примечания	Заметки о производительности. • Пропускная способность IPS/IDS представляет собой показатели пропускной способности, полученные в результате испытаний с применением рекомендуемых профилей безопасности. • Пропускная способность сети представляет собой максимальные показатели пропускной способности при ретрансляции трафика без проверки. • Стандартное время задержки получено в результате измерений с использованием пакетов размером до 1518 байтов. • Число одновременных сетевых сеансов представляет собой максимальное количество одновременных сетевых сеансов, поддерживаемое системой IPS. Измеренное значение ограничено возможностями доступного тестового оборудования. • Контексты безопасности представляют собой максимальное количество сеансов в защищенном режиме, поддерживаемое системой IPS.	Заметки о производительности. • *Пропускная способность IPS/IDS представляет собой показатели пропускной способности, полученные в результате испытаний с применением рекомендуемых профилей безопасности. S6100N IPS обеспечивает проверку с пропускной способностью до 9,5 Гбит/с. • Пропускная способность сети представляет собой максимальные показатели пропускной способности при ретрансляции трафика без проверки. • Стандартное время задержки получено в результате измерений с использованием пакетов размером до 1518 байтов. • Число одновременных сетевых сеансов представляет собой максимальное количество одновременных сетевых сеансов, поддерживаемое системой IPS. Измеренное значение ограничено возможностями доступного тестового оборудования. • Контексты безопасности представляют собой максимальное количество сеансов в защищенном режиме, поддерживаемое системой IPS.
Услуги	Обозначения и описание уровней обслуживания см. на веб-сайте HP по адресу: www.hp.com/networking/services. Для получения информации об услугах и времени реакции в вашем регионе обратитесь в ближайшее торговое представительство HP.	Обозначения и описание уровней обслуживания см. на веб-сайте HP по адресу: www.hp.com/networking/services. Для получения информации об услугах и времени реакции в вашем регионе обратитесь в ближайшее торговое представительство HP.

Аксессуары для систем HP S Intrusion Prevention System (IPS) серии N

Комплект для монтажа

Комплект HP Slide Kit Quick Release (JC017A)

Более подробную информацию см. по адресу: www.hp.com/networking

4AA3-0819RUE, создано: август 2010 г., обновлено: март 2011 г., версия 1