МОЩНАЯ ЗАЩИТА ОТ ВРЕДОНОСНЫХ ПРОГРАММ В СОСТАВЕ САМОГО ПОЛНОГО СРЕДСТВА БЕЗОПАСНОСТИ ПЕРИМЕТРА СЕТИ

Устройства безопасности Web IronPort S-Series

ОБЗОР

ОБЕЗОПАСЬТЕ И КОНТРОЛИРУЙТЕ WEB-ТРАФИК С ПОМОЩЬЮ ВЕДУЩЕГО УСТРОЙСТВА БЕЗОПАСНОСТИ WEB

Web-трафик стал главным каналом распространения угроз с очевидным риском. Существующие средства защиты на шлюзах оказались неспособными справиться с множеством вредоносного ПО, тем самым оставляя корпоративную сеть в опасности. По статистике, в среднем 75% корпоративных ПК заражены, и все равно только 10% корпораций установили защиту от вредоносного ПО на периметре. Скорость, многообразие и разрушительное действие Web-атак акцентируют внимание на важности жесткой, безопасной платформы, способной защитить периметр сети от таких угроз.

Существующие средства защиты на шлюзах оказались неспособными справиться с множеством вредоносного ПО. Только устройство безопасности Web IronPort S-Series предоставляет единое решение для мощной защиты и контроля.

Вдобавок к угрозам безопасности, вызванными вредоносным ПО, неконтролируемый Web-трафик также угрожает продуктивности сотрудников предприятия и соответствию правовым требованиям в случаях использования Web сотрудниками не по назначению.

Устройство Web-безопасности *IronPort S-Series* – это первое среди конкурентов решение, объединяющее традиционную фильтрацию URL, репутационную фильтрацию и фильтрацию вредоносного ПО. Объединив в себе эти инновационные технологии, *IronPort S-Series* помогает организациям справляться с задачами защиты и контроля Web-трафика.

Клиентам нравится низкая Общая Стоимость Владения (TCO), потому что эти мощные приложения интегрированы в одно устройство и управляются вместе. Жесткое управление и средства отчетности предоставляют простоту администрирования, гибкость и контроль, полное видение действий пользователей по отношению к политикам доступа и угрозам.

ИННОВАЦИОННАЯ ПЛАТФОРМА БЕЗОПАСНОСТИ, ПРЕДОСТАВЛЯЮЩАЯ НЕПРЕВЗОЙДЕННЫЕ ПРОИЗВОДИТЕЛЬНОСТЬ И ТОЧНОСТЬ

Устройства *IronPort S-Series* помогают предприятиям защитить и контролировать Web-трафик, объединяя в себе безопасный прокси уровня приложений для Web-трафика, Монитор трафика четвертого уровня (L4), и *IronPort Dynamic Vectoring and Streaming (DVS) Engine*™ - изощренную систему сканирования и векторизации, созданную изначально для решения задач, связанных со сканированием Web-трансакций и объектов. Это предоставляет мощную платформу Web-безопасности, оптимизированную для производительности и эффективности.

Быстрый Web-прокси предоставляет контроль за всем Web-трафиком и возможность глубокого анализа контента, что является критическим для точного обнаружения хитрого вредоносного ПО. Первое в индустрии внедрение кэширования, основанного на репутации, позволяет организовать быструю доставку безопасных объектов и контента конечному пользователю. Основанный на *AsyncOS*™ - операционной системе IronPort, Web-прокси легко обеспечивает высокую производительность и пропускную способность в самых больших сетях.

Интегрированный L4 Traffic Monitor (Монитор трафика четвертого уровня) сканирует все порты, обнаруживая и блокируя подозрительную активность. Следя за всеми 65,535 сетевыми портами, *L4 Traffic Monitor* эффективно блокирует вредоносное ПО, которое пытается достучаться в Интернет через порт 80, а также обнаруживает P2P- и IRC-активность.

Система IronPort DVS использует разносторонние технологии обработки объектов и векторизации вместе со сканированием потока и кэшированием вердиктов, что выливается в десятикратном преимуществе в пропускной способности по сравнению с решениями первых поколений.

МНОГОУРОВНЕВАЯ, МУЛЬТИВЕНДОРНАЯ ГЛУБОКАЯ ЗАЩИТА

IronPort URL Filters™ (Фильтры URL) предоставляют крупнейшую базу и высочайшую точность в контроле Web-контента. Эти фильтры сравнивают Web-запросы пользователя с установленными администратором политиками для 52-х заготовленных (и неограниченного числа настраиваемых) категорий.

С базой данных, содержащей более 20-ти миллионов сайтов (более 3-х миллиардов Web-страниц) на семидесяти языках в двухстах странах, *IronPort URL Filters* предоставляют непревзойденное покрытие и точность проверки Web-запросов.

Первые в истории Web reputation filters (фильтры репутации Web) обеспечивают мощный внешний слой защиты. Используя *SenderBase®*, *IronPort Web Reputation Filters*™ анализируют более 50-ти различных параметров, связанных с Web-трафиком и сетевой активностью, для точного определения надежности сайта. Изощренные технологии моделирования безопасности используются для взвешивания каждого параметра и генерации единого рейтинга в интервале от -10 до +10. Политики, созданные администратором автоматически применяются, основываясь на репутации.

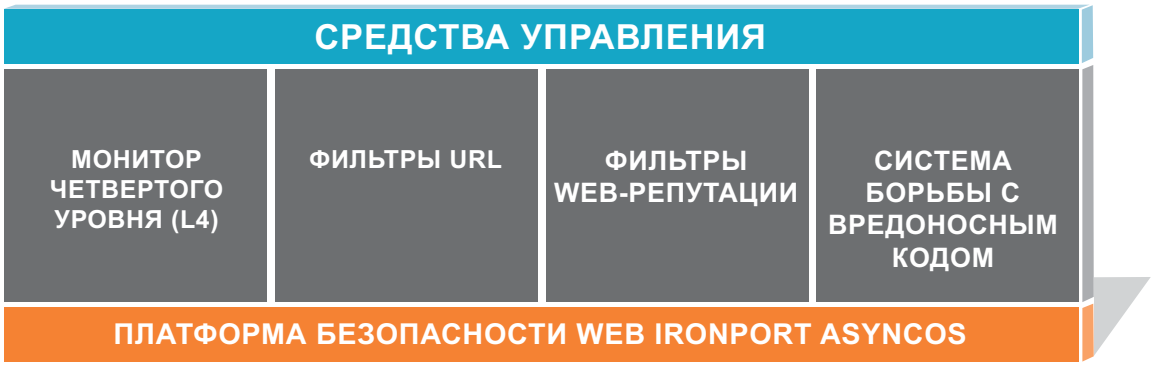
Ведущая антивирусная система IronPort Anti-Malware System™ использует систему *IronPort DVS* и различные системы сканирования (первая - Webroot) для обеспечения надежной защиты от широчайшего спектра угроз из Web. Эти угрозы включают все - от рекламных приложений, фишинговых и фарминговых атак до более вредных угроз, таких как трояны, черви, мониторы и килогеры.

Система IronPort DVS была создана, чтобы обеспечить интегрированное в одном устройстве решение, использующее множество типов сигнатур от разных разработчиков. Первый набор идет от Webroot - лидера в индустрии борьбы с вредоносным ПО. Команда Webroot Threat Research поддерживается Phileas – первой автоматизированной системой обнаружения шпионских программ, которая идентифицирует известные и новые угрозы, сканируя миллионы сайтов ежедневно. Устройства *IronPort S-Series* первыми включили передовую технологию Webroot на периметре шлюза для того, чтобы оградить сеть от проникновения этих угроз.

МОЩНЫЕ СРЕДСТВА УПРАВЛЕНИЯ И ОТЧЕТНОСТИ

IronPort Web Security Manager™ позволяет создавать унифицированные политики для всех фильтров и предоставляет гранулированные опции для организаций, основываясь на аутентифицированных или неаутентифицированных пользователях.

Мощь на периметре: IronPort S-Series комбинирует революционные технологии для обеспечения многоуровневой защиты Web в одном устройстве.



Администраторы управляют всеми политиками Web-доступа (включая URL-фильтрацию, репутационную фильтрацию и фильтрацию вредоносного ПО) из единого места. Администраторы создают и управляют группами и пользователями для всех служб фильтрации на устройстве.

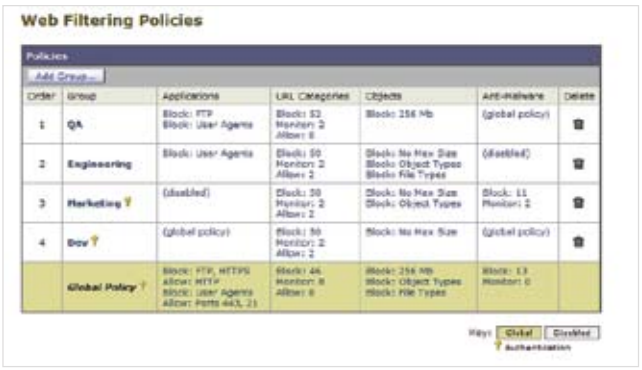
IronPort Web Security Monitor™ предоставляет ценные данные как о Web-активности в целом, так и отдельно об обнаружении и предотвращении угроз в сети. Эти отчеты разработаны для предоставления как актуальной, так и исторической информации. Продвинутые средства отчетности дают обзор нарушений политик и безопасности.

Различные сценарии подключения предоставляют гибкость для сети предприятия. Режимы внедрения включают: прямой прокси, прозрачное включение вне свича L4 или роутера WCCP внутри сети. Устройство *IronPort S-Series* может быть настроено в качестве отдельного прокси или сосуществовать с другими прокси.

MIB для SNMP позволяет предприятиям осуществлять мониторинг и оповещения для ключевых системных параметров, таких как состояние оборудования, производительность и доступность. Система оповещений обеспечивает слежение за всеми системными параметрами – оборудованием, безопасностью, производительностью и доступностью.

Интегрированная аутентификация через стандартные директории (такие, как LDAP или Active Directory) и возможность внедрения множества схем аутентификации (таких как NTLM или Basic) дает организациям легкость при установке *IronPort S-Series*, позволяя использовать существующие схемы аутентификации и контроль политик.

Расширенное журналирование позволяет организациям следить за всем Web-трафиком, как хорошим, так и вредоносным. Стандартные форматы логов включают Apache, Squid или Squid-detailed – вместе с возможностью создания своих форматов логов. Администраторы могут включать или выключать журналирование, устанавливать ограничения на размеры файлов и другое.



Группировка по LDAP, AD, сетям

- Блокировать FTP
- Разрешить Media
- Разрешить все категории URL

Маркетинг

- Блокировать исполняемые файлы
- Блокировать игровые сайты
- Блокировать вредоносный код

Продажи

- Разрешить скайп
- Отслеживать весь трафик
- Разрешить исполняемые файлы
- Разрешить все приложения

IT

ЛИНЕЙКА ПРОДУКТОВ

ВЫБОР РЕШЕНИЯ БЕЗОПАСНОСТИ WEB ДЛЯ ВАС

IronPort Systems предлагает ведущие устройства защиты Web для организаций всех размеров.

IronPort S650	Создана для самых требовательных сетей в мире. Рекомендуется организациям с более 5000 сотрудников.
IronPort S350	Рекомендуется организациям с менее 5000 сотрудников.

СПЕЦИФИКАЦИИ

СИСТЕМА / ПРОЦЕССОР	
Форм-фактор	Стоечный корпус 19”, 2U
Размеры	3.5” (h) x 19” (w) x 29” (d)
Процессор	2x Dual Core Intel Xeon 5140, 4 MB Cache
Память	4 GB
Питание	С горячей заменой, 750 watts, 100/240 volts
ХРАНЕНИЕ	
RAID	RAID 10, 256MB cache с автономным питанием
Диски	Шесть дисков с горячей заменой, 146 GB SAS, всего 876 GB
ПОДКЛЮЧЕНИЯ	
Ethernet	6x Gigabit NICs, RJ-45
Serial	1x RS-232 (DB-9) Serial Port
ИНТЕРЙЕЙСЫ/НАСТРОЙКА	
Web-интерфейс	Доступ через HTTP или HTTPS
Командная строка	Доступ через SSH или Telnet; Configuration Wizard or command-based
Передача файлов	SCP, FTP или SYSLOG
Файлы настроек	Файлы конфигурации в XML

Представитель в странах СНГ и Балтии.

headtechnology it-security

www.headtechnology.ru
www.headtechnology.com.ua
www.headtechnology.kz
www.headtechnology.lv

IRONPORT S-SERIES

IRONPORT

IronPort Systems, Inc.
950 Elm Avenue, San Bruno, California 94066
TEL 650.989.6500 **FAX** 650.989.6543
EMAIL info@ironport.com **WEB** www.ironport.com

IronPort Systems, a Cisco business unit, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world’s largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company’s network infrastructure.

IronPort is now part of Cisco.

CISCO