

Безопасность корпоративного класса для SMB



NETGEAR STM — это сочетание лучших функций безопасности и запатентованной технологии Stream Scanning, обеспечивающей для SMB эффективную, но в то же время простую и доступную по цене защиту Web и Email от исходящих из Интернета угроз. Вредоносное ПО, шпионское ПО, черви, спам и фишинг распространяются с помощью протоколов Web и Email. Они становятся все более опасными и изощренными, атакуя по нескольким направлениям и тщательно маскируясь.

Сегодня атаки через Web и электронную почту осуществляются сразу по нескольким направлениям и используют комбинацию вредоносных программ. Такие массовые атаки приводят к блокированию или захвату компьютерных ресурсов и информации. Злоумышленники пытаются проникнуть не только с помощью зараженных писем, но и все чаще через Интернет-трафик реального времени, который трудно сканировать из-за необходимости свести задержки к минимуму.

Безопасность корпоративного класса

Главные преимущества STM

Защита в реальном времени

- Запатентованная технология Stream Scanning Technology обеспечивает масштабируемое сканирование Web-трафика в реальном времени для защиты от замаскированного под обычные данные опасного программного кода. Вредоносное ПО блокируется на шлюзе, но это не мешает доступу к Интернету.

Комплексная защита

- Обеспечивает безопасность для работы в Web и электронной почты, сканируя трафик, который передается по шести основным сетевым протоколам - HTTP, HTTPS, FTP, SMTP, POP3 и IMAP. Продукты STM используют механизмы сканирования корпоративного класса с обнаружением с помощью баз сигнатур и эвристического подхода, что позволяет блокировать как известные, так и неизвестные угрозы. База данных вредоносного ПО содержит более полутора миллиона сигнатур шпионских программ, вирусов и другого вредоносного ПО.

Автоматическое обновление сигнатур

- Сигнатуры вредоносного ПО автоматически обновляются каждый час. Важные новые сигнатуры добавляются за несколько часов до того, как их выпустят ведущие разработчики антивирусных программ.

Идеальное решение

- Развертывается за несколько минут в любом месте сети. Работает автоматически и не тормозит сеть. Устройство, о котором можно забыть после его развертывания.

Мощные возможности управления

- Безопасная и удобная Web-консоль управления. Можно точно настраивать правила и выдачу предупреждений, проверять итоговую статистику и графики, извлекать данные с уровня IP-адреса и интегрировать данные из журнала с такими средствами сетевого управления, как SNMP.

Упрощенное лицензирование

- Продукты STM также используют принципиально новую упрощенную схему лицензирования — покупателю не нужно лицензировать дополнительные опции либо приобретать лицензию по числу пользователей. Предлагаются только три лицензии - на Web, Email и Maintenance and Support без каких-либо ограничений на число пользователей. Кроме того, лицензия Maintenance and Support стандартно предусматривает круглосуточную поддержку и расширенные возможности замены.

Компании SMB сталкиваются с теми же рисками безопасности ИТ, что и крупные предприятия, поэтому им требуется защита корпоративного уровня. Многие вендоры предлагают SMB для защиты от вредоносного ПО «облегченные» версии коммерческих программ либо утилиты на основе open source. Эти инструменты используют сокращенную базу сигнатур, ненадежные алгоритмы обнаружения, медленно реагирующие на новые угрозы и неспособные в реальном времени обрабатывать трафик из web. В отличие от этих дешевых средств технологии корпоративного класса защищают не от отдельных угроз, а от всего спектра угроз. Однако они очень сильно загружают процессоры, поэтому для их применения требуется дорогое оборудование.

Продукты STM построены на основе запатентованной и оптимизированной для Web архитектуры Stream Scanning. NETGEAR STM Stream Scanning Technology позволяет использовать технологии корпоративного класса и в то же время обеспечивает высокую пропускную способность. NETGEAR совместно с лидерами индустрии «Лабораторией Касперского» и Commtouch перенесла на платформу STM лучшие механизмы сканирования Web-трафика и электронной почты. Функционируя поверх платформы Stream Scanning, эти механизмы работают параллельно с механизмом эвристического анализа NETGEAR, выявляя известные и неизвестные угрозы.

В NETGEAR STM встроены несколько технологий корпоративного класса

• Инструмент корпоративного класса для защиты от вредоносного ПО

В продуктах STM встроены инструменты корпоративного класса для защиты от вредоносного ПО на основе мощных алгоритмов сканирования и базы данных с сотнями тысяч сигнатур. По сравнению с конкурирующими продуктами, которые из соображений производительности используют сокращенную базу сигнатур, насчитывающую тысячи записей, покрытие улучшается на два порядка. Вирусы, шпионское ПО и другое вредоносное ПО обнаруживается и блокируется. Продукты STM также блокируют функцию загрузки phone home шпионского ПО, предотвращая дальнейшее заражение и защищая важную информацию пользователя.

• Защита в реальном времени (Zero Hour Threat Protection)

Продукты NETGEAR STM идентифицируют новые угрозы сразу же после их появления в Интернете и еще до того, как они проникли в сеть компании. Угрозы такого типа, которые идентифицируются по мере их появления в Интернете, называются zero hour threats. С помощью этой функции продукты STM проактивно блокируют новое вредоносное ПО, фишинговые атаки, спам, подозрительные URL и атаки зомби/ботов еще до того, как они дойдут до сети. Она каждый день проверяет два миллиарда транзакций и выявляет в них признаки вредоносного ПО zero hour, фишинга, попыток анализа уязвимостей защиты, IP reputation, спама и данных зомби.

• Лучший в индустрии инструмент защиты от спама

Инструмент защиты от спама NETGEAR использует архитектуру Distributed Spam Analysis на базе «облачного» подхода, что позволяет оперативно передать на устройство информацию о новом спае, который начал распространяться в Интернете. В результате обеспечивается самый высокий в индустрии процент обнаружения спама и самый низкий процент ложных срабатываний. В отличие от фильтров на основе open source и других традиционных фильтров Distributed Spam Analysis великолепно адаптируется к новому спаю, одинаково хорошо отражает спам на разных языках и не требует периода обучения — новый спам идентифицируется и классифицируется через несколько секунд после его появления в Интернете.



• Фильтр URL корпоративного класса

URL-фильтр STM использует технологию фильтрации web корпоративного класса, которая классифицирует адреса URL по 64 категориям для специального и целевого администрирования. Используя базу данных с более чем 100 миллионов URL, URL-фильтр NETGEAR STM с помощью HTTP-коннекторов, размещенных в «облаке» у сервис-провайдеров по всему миру классифицирует и обновляет записи URL в реальном времени. Кроме того, URL-фильтр NETGEAR STM автоматически адаптируется и классифицирует новые прежде неизвестные URL в отличие от других менее эффективных подходов, при использовании которых администратор должен вручную вносить в базу новые URL. URL-фильтр не только блокирует доступ к опасным сайтам, но и к тем сайтам, которые содержат шпионское ПО.

• IM, P2P, Toolbar Application Control**

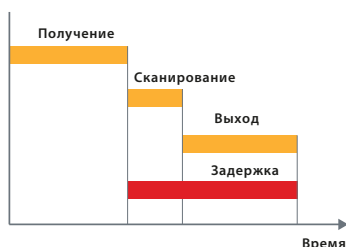
Вводит в действие для корпоративной сети правила контроля приложений STM. Для повышения продуктивности работы сотрудников блокирует доступ к таким общедоступным клиентам IM, как AIM®, Yahoo!® Messenger, ICQ, и MSN® Messenger, экономит полосу пропускания за счет блокирования таких приложений для потокового воспроизведения аудио и видео RealPlayer®, iTunes® и Winamp. Блокирует загрузку и открытие всплывающих окон в Web-браузере.

Выпустив STM, NETGEAR впервые предоставила SMB функции, которые раньше использовали только крупные предприятия.

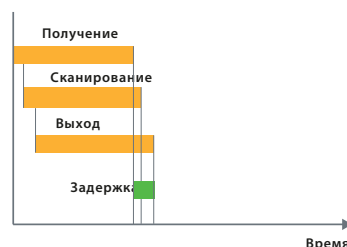
Революционная платформа сканирования

Большинство самых совершенных программ сканирования сильно загружают процессор и память. Поскольку для сканирования чувствительного к задержкам Web-трафика нужна высокая производительность, то до сих пор не было доступных для SMB продуктов, в которых использовались технологии безопасности корпоративного класса. NETGEAR STM использует запатентованную Stream Scanning Technology, которая анализирует потоки данные при их поступлении в сеть. NETGEAR Stream Scanning работает намного быстрее традиционных методов сканирования, которые сначала загружают входящий файл в буфер и из-за этого вносят задержки в сеть. Хотя такие задержки допустимы для электронной почты, при загрузки из Web больших объемов HTTP-трафика они сильно тормозят просмотр Web-сайтов. Для решения этой проблемы применяются прокси, сканирование ограничивается определенными типами файлов и несколько устройств объединяются в кластер. Однако эти решения может сконфигурировать и установить только высококвалифицированный специалист, они очень дороги, часто снижают уровень безопасности и всё равно работают медленнее, чем Stream Scanning Technology. Архитектура StreamScanning - это фундамент для STM

Традиционное сканирование потока данных



Stream Scanning



Простая настройка и управление

STM разворачивается за несколько минут в любом месте сети. Она работает автоматически и не тормозит сеть. В отличие от традиционных решений на базе прокси не нужно заново конфигурировать сеть. Это устройство, о котором можно забыть после его разворачивания. Для администрирования используется удобный Web-интерфейс. Можно точно настраивать правила и выдачу предупреждений, проверять итоговую статистику и графики, извлекать данные с уровня IP-адреса и интегрировать данные из журнала с такими средствами сетевого управления, как SNMP.

Для многих администраторов и ИТ-специалистов главная «головная боль» - управление индивидуальными лицензиями или рабочими местами. Приобретение дополнительных лицензий по мере добавления в сеть компьютеров и пользователей — это процесс, связанный с существенными расходами и затратами рабочего времени. NETGEAR предлагает лицензирование для защиты Web и электронной почты без учета числа рабочих мест.



СВОДНАЯ ТАБЛИЦА ХАРАКТЕРИСТИК STM SERIES

МОДЕЛЬ	STM150	STM300	STM600
РЕКОМЕНДАЦИИ ПО ВЫБОРУ МОДЕЛИ			
Тип заказчика	Небольшая сеть	Средняя сеть	Средняя сеть
Рекомендуемое число пользователей	20 - 150	До 300	До 600
Одновременно сканируемые соединения HTTP	1,000	2,000	4,000
Пропускная способность HTTP (Мбайт/сек)	43	148	239
Пропускная способность SMTP (писем/час)	139,000	420,000	960,000
БЕЗОПАСНОСТЬ КОНТЕНТА			
Защита сети от вредоносного ПО			
Web (HTTP, HTTPS, FTP)	●	●	●
Email (SMTP, POP3, IMAP)	●	●	●
Потоковое сканирование	●	●	●
Проверка входящего и исходящего трафика	●	●	●
Защита Zero Hour	●	●	●
Автоматическое обновление сигнатур	Каждый час	Каждый час	Каждый час
Распределенный анализ спама	●	●	●
Карантин для почты	●*	●	●
Фильтрация URL-контента по 64 категориям	●	●	●
Число пользователей	Неограниченное	Неограниченное	Неограниченное
РАЗВЕРТЫВАНИЕ			
Plug and Play	●	●	●
Inline Transparent Bridge	●	●	●
Поддержка VLAN	●	●	●
Fail-open		●	●
ОБОРУДОВАНИЕ			
Портов Gigabit RJ-45	5	3	5
Портов Gigabit RJ-45 с Failure Bypass	0	2	4
Выделенные порты RJ45 для управления VLAN	0	1	1
Порт консоли администратора	RS232	RS232	RS232
Форм-фактор	1U	1U	1U
Размеры (H x L x W)	дюймы	1.7 x 10.2 x 17.3	1.75 x 19.7 x 16.8
	мм	43.5 x 258 x 440	44.4 x 500 x 426
Вес	фунты	8.1	18.1
	кг	3.68	8.2

Технические спецификации**• Функции безопасности****Защита от вредоносного ПО**

- Механизм защиты корпоративного уровня с сотнями тысяч сигнатур
- Защита Cloud Zero Hour Threat
- Блокирование загрузки шпионского ПО
- Блокирование сайтов со шпионским ПО
- Блокирование атак фишинга
- Настоящее сканирование трафика HTTP

Защита от спама

- Фильтр спама корпоративного класса с использованием архитектуры Distributed Spam Analysis

- Превентивное блокирование распространения вирусов
- Блокирование спама, передаваемого через SMTP и POP3

Обслуживаемые протоколы

- Web (HTTP, HTTPS, FTP)
- Электронная почта (SMTP, POP3, IMAP)

Фильтрация контента

- Фильтр URL корпоративного уровня
- 64 категорий
- Задаваемый список разрешенных URL
- Задаваемый список запрещенных URL
- Блокирование заданных пользователем типов файлов

- Блокирование почтовых вложений, защищенных паролем
- Блокирование ActiveX
- Блокирование Flash
- Контроль Javascript
- Блокирование писем в зависимости от их темы

Расширенные возможности задания правил**

- Интеграция с сервером каталога LDAP
- Правила в зависимости от времени суток
- Правила для отдельных пользователей
- Интеграция с контроллером домена Windows
- Правила для пользователей и групп

Контроль приложений**

- Протоколы мгновенных сообщений
- Поточковая передача мультимедиа
- Блокирование всплывающих окон

• Функции управления**Интерфейс администрирования**

- Защищенная консоль администратора
- Поддержка SNMP
- Автоматическое онлайн-обновление
- Опции гранулярных политик
- Лицензии для неограниченного числа пользователей

Регистрация событий

- Гранулярные запросы к журналу
- Поддержка syslog
- Пересылка журнала по электронной почте

Отчеты

- Суммарная статистика
- Графические отчеты
- Автоматическое оповещение об угрозах
- Оповещение о вредоносном ПО

• Функции развертывания

- Plug and play
- Inline transparent bridge
- Поддержка VLAN

• Требования к системе

- Доступ к Интернету
- Internet Explorer® 5.0 или более поздний
- Mozilla Firefox® 1.0 или более поздний

• Контракты**Support & Maintenance**

- Поддержка 24x7
- Обслуживание и обновление ПО
- Расширенные возможности замены

Защита от Web-угроз

- Для HTTP, HTTPS и FTP
- Правила обработки шпионского ПО с обновлением определений каждый час
- Обновление базы вирусов каждый час
- Обновление в реальном времени базы данных фильтра контента

Защита от угроз электронной почты

- Для IMAP, POP3 и SMTP
- Правила обработки шпионского ПО с обновлением определений каждый час
- Обновление базы вирусов каждый час
- Обновление в реальном времени Distributed Spam Analysis

• Условия эксплуатации и хранения

- Температура при эксплуатации: 0° — 40°C
- Температура при хранении: -20° — +70°C
- Влажность при хранении: 5% — 95%

• Электрические характеристики

- 100 — 240 В перем. тока
- 50 — 60 Гц — Универсальный вход
- Ток максимум 1.5 А

• Электромагнитное излучение

- CE mark, коммерческое оборудование
- FCC Part 15 Class A
- VCCI Class A

• Безопасность

- UL listed
- C-Tick

• Защита окружающей среды

- RoHS

Гарантия

- Три года на оборудование

Состав пакета поставки

- ProSecure STM150, STM300 или STM600
- Кабель Ethernet
- Силовой кабель
- Резиновые ножки
- Гарантийный талон
- Руководство по эксплуатации
- Лицензионное соглашение
- Документ CE
- Извещение GPL
- Талон подписки (только для bundle)

Информация для заказа**• Оборудование
требуется лицензия Web и/или Email**

- STM150-100EUS
- STM300-100EUS
- STM600-100EUS

**• Bundle
Оборудование вместе с лицензиями
на 1 год Web, Email и Software
Maintenance & Upgrades, поддержку
24/7 и Advanced Replacement**

- STM150EW-100EUS
- STM300EW-100EUS
- STM600EW-100EUS

**• Web Threat Management
лицензия на 1 год**

- STM150W-10000S
- STM300W-10000S
- STM600W-10000S

**• Web Threat Management
лицензия на 3 года**

- STM150W3-10000S
- STM300W3-10000S
- STM600W3-10000S

**• Email Threat Management
лицензия на 1 год**

- STM150E-10000S
- STM300E-10000S
- STM600E-10000S

**• Email Threat Management
лицензия на 3 года**

- STM150E3-10000S
- STM300E3-10000S
- STM600E3-10000S

**• Software Maintenance & Upgrades,
24/7 Support, & Advanced Replacement
лицензия на 1 год**

- STM150M-10000S
- STM300M-10000S
- STM600M-10000S

**• Software Maintenance & Upgrades,
24/7 Support, & Advanced Replacement
лицензия на 3 года**

- STM150M3-10000S
- STM300M3-10000S
- STM600M3-10000S

NETGEAR®

103045, Москва
ул. Трубная, д.12, офис 5F
Бизнес-центр Millennium House
Тел.: +7 (495) 799-5610
Факс: +7 (495) 799-5610

© 2009 NETGEAR, Inc. NETGEAR, логотип NETGEAR, NETGEAR Digital Entertainer Logo, Connect with Innovation, FrontView, IntelliFi, PowerShift, ProSafe, ProSecure, RAIDar, RAIDiator, X-RAID, RangeMax, ReadyNAS и Smart Wizard являются торговыми марками NETGEAR, Inc. в США и/или других странах. Другие используемые для идентификации названия брендов могут быть торговыми марками соответствующих компаний. Информация может быть изменена без предварительного уведомления. Все права защищены.

* На основе исследований Osterman Research

** Будет доступно в третьем квартале 2009 года

† Максимальная скорость беспроводной сети приведена в соответствии со спецификацией стандарта IEEE 802.11. В реальных условиях скорость может быть меньше из-за состояния сети и внешних факторов, включая объем сетевого трафика, материалы и конструкции здания, накладные расходы при передаче в сети. Использование некоторых функций зависит от конкретной модели MSO заказчика.