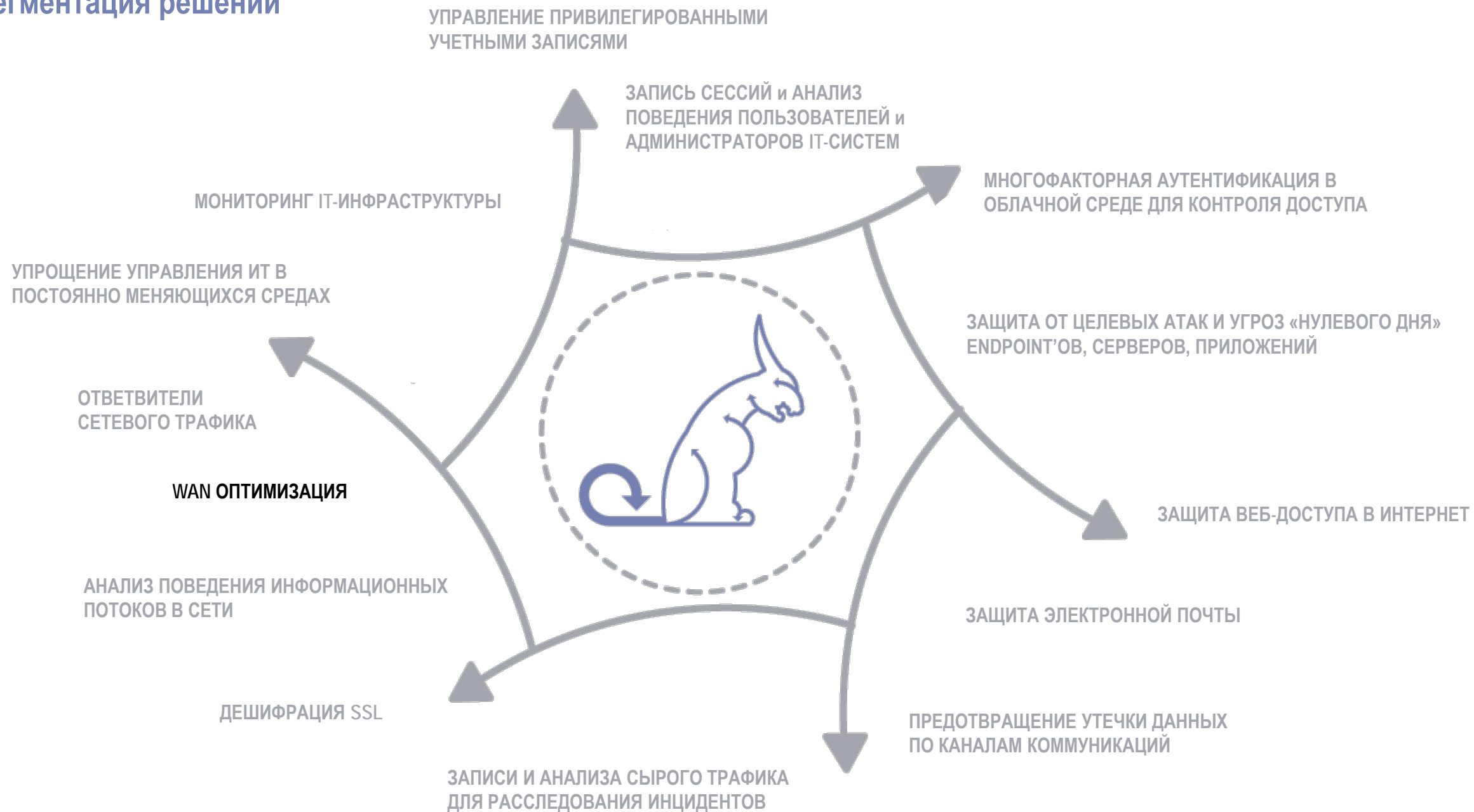


Сегментация решений



ProxySG представляет собой масштабируемую прокси-платформу для обеспечения безопасности взаимодействия с ресурсами сети Интернет (web security) и оптимизации работы бизнес-приложений (WAN optimization). **Устройства NGFW не являются заменителями** прокси-решений в виду ограниченных возможностей разбора веб-трафика.

Преимущества решения ProxySG:

Общее

- Высокопроизводительная фирменная операционная система с возможностью перезагрузки на предыдущую версию.
- Возможность функционирования в качестве прозрачного (transparent) и явного (explicit) прокси одновременно. Применяется для обеспечения защиты внутренних пользователей и сетей от шпионского программного обеспечения и фишинговых атак при веб-доступе в Интернет.
- Возможность функционирования в качестве обратного (reverse) прокси. Применяется в составе организованной сети DMZ для исключения возможности прямого доступа извне к веб-серверам организации. Функционал Web Application Firewall - бесплатный.

Протоколы и аутентификация

- Возможность применения для таких протоколов передачи данных как: HTTP/HTTPS, CIFS, SSL, FTP, FTP-over-HTTP, MAPI, P2P, MMS, RTMP, RTSP, QuickTime, TCP-Tunnel, DNS, WCCP.
- Возможность разграничения прав доступа к ресурсам посредством следующих механизмов аутентификации: на основании локальных списков пользователей; IWA (Basic, NTLM, Microsoft Kerberos), LDAP (Active Directory, eDirectory, SunOne), CA eTrust SiteMinder, Oracle Access Manager, RADIUS; применения сертификатов; поддержка SSO и прозрачной аутентификации, а также последовательной аутентификация в нескольких системах.

SSL

- Аппаратное ускорение SSL-трафика. Контроль параметров SSL-соединений – валидности сертификатов серверов, версий протоколов шифрования SSL/TLS, шифрования и контроля целостности SSL/TLS-соединения (cipher suites).
- Функционал Encrypted TAP позволяет отдать расшифрованный *-over-SSL трафик (HTTPS, IMAPS и т.д.) на анализ во внешнее устройство ИБ (например, “песочницу”) в дешифрованном виде.
- Дешифрация SSL-трафика и SSL off loading

Интеграция

- Поддержка протокола ICAP – для интеграции с DLP или другими системами безопасности.
- Интеграция с другими решениями ИБ позволяет значительно повысить уровень сетевой безопасности.



Решение от Symantec – Secure Web Gateway ProxySG

ЗАЩИТА ВЕБ-ДОСТУПА В ИНТЕРНЕТ КАК ОСНОВНОГО ТРАНСПОРТА ДОСТАВКИ ВРЕДНОСНОГО ПО

<https://www.symantec.com/products/web-and-cloud-security/secure-web-gateway-proxy-sg-and-asg>

Надежность и архитектура

- Работа в режиме Active/Active bridging с поддержкой virtual IP для обеспечения функций резервирования и удаленного управления, встроенный сетевой адаптер passthrough
- Поставляется в виде физических устройств (ProxySG и Advanced Security Gateway) и виртуальных образов (virtual appliance) для ESX/ESXi, Hyper-V или Amazon Web Services

Безопасность

- Контроль действий пользователей в сети Интернет. Позволяет блокировать отдельные приложения и действия в этих приложениях (например, загрузку/выгрузку вложений в веб-почте или отправку писем или сообщений в социальных сетях).
- Возможность выполнения контентной фильтрации и категорирования Интернет-ресурсов – BlueCoat WebFilter или BlueCoat Intelligence Services.

Оптимизация

- Повышение производительности сетевой инфраструктуры, веб приложений и веб-сайтов организации по средствам функционала WAN optimization.
- Возможность кэширования данных с учетом результатов антивирусной проверки.
- Возможность управления сетевыми протоколами и полосой пропускания каналов связи.

Управление и отчетность

- Централизованное управление политиками на всех SWG в сети
- Возможность сбора статистической информации и формирования отчетов в отношении протоколов передачи данных (более 60 контролируемых параметров), а также для определения эффективности и активности рабочих мест пользователей.

Отладка и мониторинг

- Широкие возможности по трассировке и отладке используемых политик безопасности
- Контроль доступности для критичных приложений и услуг
- Поддержка SNMP и Syslog.



Решение от Symantec – PacketShaper

РЕШЕНИЕ ДЛЯ WAN ОПТИМИЗАЦИИ

<https://www.symantec.com/products/web-and-cloud-security/network-performance-optimization/wan-optimization-packetshaper>

PacketShaper позволяет автоматически классифицировать и измерять работу сетевых приложений, обеспечивать для них QoS, с помощью управления трафиком, а также увеличивать пропускные способности WAN при помощи сжатия. Бизнес-критичные приложения должны работать с той же скоростью, с которой происходит деловая активность. Blue Coat PacketShaper предоставляет возможности оптимизации WAN при помощи последовательности модулей: мониторинга, распределения трафика по скорости и сжатия.

- ✓ Возможность распознавать и классифицировать приложения при помощи технологии Layer 7 Plus. Отслеживание производительности в реальном времени, имея необходимую информацию для устранения проблем.
- ✓ Возможность устранять проблемы производительности критичных приложений путем резервирования части полосы пропускания, необходимой для нормальной работы приложений.
- ✓ Возможность получить большую пропускную способность от уже использующихся физических узлов и повысить производительность бизнес-процессов.



Модуль распределения трафика по скорости

Модуль шейпинга, входящий в состав PacketShaper, предоставляет функцию QoS, которая позволяет контролировать трафик таким образом, чтобы критичные для пользователя, чувствительные к задержкам приложения, получали необходимую полосу пропускания, для работы с максимальной производительностью. При помощи запатентованной системы контроля за TCP скоростями, модуль шейпинга может автоматически выставлять нужные скорости передачи данных для компьютеров на удалённых концах сети, что позволяет получить настоящий двунаправленный QoS.

Модуль сжатия

Модуль сжатия, входящий в состав PacketShaper увеличивает пропускную способность WAN, улучшая производительность приложений и время отклика для пользователей. Используя симметричную архитектуру, понимающую приложения, а также множество методов сжатия информации. Модуль сжатия интеллектуально выбирает, какой трафик нужно сжать и какой метод применить, что позволяет увеличить пропускную способность от двух до десяти раз, и в свою очередь, сократить использование полосы пропускания и время отклика WAN.

Модуль мониторинга

Прежде, чем оптимизировать производительность приложения, необходимо получить четкое представление о сетевом трафике. PacketShaper автоматически классифицирует и измеряет сетевые приложения, предоставляя информацию подобно зонду. Модуль мониторинга предоставляет не только данные об использовании сети, приложений и уровне производительности, но и отслеживает, что происходит с каждым отдельным соединением внутри приложения. Модуль Мониторинга также разбирает трафик по приложениям и сайтам на высоком уровне детализации, регистрирует пиковые и средние значения использования, количество переданных байтов, доступность ресурсов, нагрузку от наиболее активных источников и получателей сообщений, производительность сети и многое другое. PacketShaper помогает в диагностике, позволяя отслеживать процент загруженности канала, время отклика критичных приложений для конечного пользователя, а также ключевые параметры. Присутствует возможность целевого захвата пакетов для последующего исследования при помощи инструментов протокольного анализа. Искусственный интеллект в реальном времени отслеживает «Среднюю Оценку» (Mean Opinion Score, MOS), случайные искажения, задержку и потерю сигнала в трафике аудио и видео конференций по протоколу реального времени (RTP).





Решение от Symantec – PacketShaper

РЕШЕНИЕ ДЛЯ WAN ОПТИМИЗАЦИИ

ПРИМЕРЫ РЕШАЕМЫХ ПРОБЛЕМ С ПОМОЩЬЮ SYMANTEC PACKETSHAPER

**Неизвестные проблемы производительности по WAN:
Периодические и хронические проблемы с производительностью ключевых бизнес-приложений, как правило, вызвано полным использованием WANs**

- Symantec дает вам представление в реальном времени обо всех приложениях и веб-контенте в сети и о том, сколько трафика потребляется, а также производительность конечных пользователей
- Позволяет устранять неполадки приложений в режиме реального времени
- Позволяет быстро решить проблемы с помощью advanced QoS и вернуть пропускную способность

Облачные приложения / SaaS: внешне бизнес-приложения могут иметь проблемы с производительностью, особенно при работе с тяжелыми запросами или при управлении документами (например, Salesforce.com)

- Асимметричная оптимизация WAN ускоряет доставку внешних приложений SaaS без развертывания самого устройства / VA в облачной инфраструктуре или маршрутизации трафика через центр обработки данных. Ускорение облачных приложений в 15-25 раз и снижение загрузки канала.
- PacketShaper помогает обеспечить видимость и QoS для облачных приложений, чтобы повысить производительность сети и пользователей. Установите границы потребления полосы пропускания для обеспечения гарантированной пропускной способности для бизнес-критичных приложений SaaS, трафика VPN и т.д.

**Хранение и резервное копирование (аварийное восстановление):
невозможность для филиалов и центров обработки данных проведения резервного копирования и зеркалирования данных рабочих мест по WAN**

- Оптимизация WAN кэшированием байтов, сжатием и оптимизацией протоколов уменьшает нагрузку канала при репликации и резервном копировании данных через WAN на 50-90%
- Оптимизация WAN обеспечивает непрерывность бизнеса и аварийное восстановление (DR) путем ускорения перемещения данных по WAN до 200 раз

ERP, CRM и бизнес-приложения: SAP, Oracle и другие системы (HTTP/SSL) не оправдывают ожиданий по производительности.

- Кэширование объектов (HTTP), сжатие и оптимизация протоколов уменьшают задержки при передаче данных через WAN
- Оптимизация WAN позволяет централизованно развертывать консолидированные корпоративные приложения
- Оптимизация WAN уменьшает нагрузку канала на 40-90% и ускоряет ERP в 2-95 раз, тем самым повышая производительность сотрудников

IP-телефония или видеоконференции: трафик через конвергентную глобальную сеть испытывает проблемы с качеством, невозможно адекватно отслеживать и устранять проблемы с производительностью

- Видимость и QoS обеспечивают производительность голосовых и видеоконференций в глобальной сети. Обеспечьте достаточную пропускную способность для VoIP и видео приложений.
- Отслеживание и контроль качества голоса и видео
- Увеличение пропускной способности сети, чтобы иметь возможность увеличить количество обрабатываемых вызовов и приложений





Наименование	Краткое описание	Самая свежая информация о решении	Принцип лицензирования
Решение от Symantec – PacketShaper	Решение для WAN оптимизации	https://www.symantec.com/products/web-and-cloud-security/network-performance-optimization/wan-optimization-packetshaper	Стоимость решения формируется из следующих составляющих: модель апплайса, объем обрабатываемого трафика, Software Upgrade
Решение от Symantec – Secure Web Gateway	Защита веб-доступа в интернет как основного транспорта доставки вредоносного ПО	https://www.symantec.com/products/web-and-cloud-security/secure-web-gateway-proxy-sg-and-asg	Стоимость решения формируется из следующих составляющих: модель апплайса, кол-во пользователей, модули безопасности, модули управления и отчетности, подписка на модули и доп.оборудование



