СПЕЦИФИКАЦИЯ

Symantec SSL Visibility Appliance

Избавьтесь от «слепых зон», образуемых зашифрованным трафиком

Обзор

Подробная информация о зашифрованном трафике помогает защититься сложных устойчивых угроз

- Автоматическая идентификация всего трафика SSL/TLS вне зависимости от номера порта и приложения.
- Выявление скрытых угроз, использующих SSL для обхода защиты, таких как трояны Dyre и Zeus, Upatre Command and Control (C&C), VMZeus C&C и другие.

Соблюдение конфиденциальности и нормативных требований

- Выборочная расшифровка трафика позволяет соблюсти нормативные требования и сохранить конфиденциальность, где это необходимо.
- Гарантирует соблюдение корпоративных политик в отношении зашифрованного трафика.

Тесная интеграция с имеющейся инфраструктурой безопасности

- Сохранение и улучшение показателей рентабельности инвестиций в инфраструктуру.
- Поддержка нескольких сегментов сети, возможность одновременной передачи данных на активные и пассивные устройства безопасности, а также на ProxySG.

Удобство управления и администрирования

- Подробные журналы и предупреждения позволяют выявлять тенденции и потенциальные проблемы, связанные с использованием SSL.
- Интеграция с Management Center для резервного копирования конфигурации, выполнения задач по расписанию и синхронизации.

Введение

Шифрование помогает обеспечить конфиденциальность и целостность данных, но при этом образуются «слепые зоны», через которые хакеры могут обойти защиту. На сегодняшний день более половины трафика передается в Интернете в зашифрованном виде, а это означает, что «слепые зоны» порождают серьезную уязвимость и создают серьезные риски, в том числе репутационные. Устройство Symantec SSL Visibility Appliance, являющееся ключевым компонентом решения Encrypted Traffic Management, позволяет компаниям устранять «слепые зоны» в корпоративной среде и использовать инвестиции в инфраструктуру безопасности с полной отдачей. Получив контроль за зашифрованным трафиком, организации могут обеспечить соблюдение корпоративных политик, связанных с конфиденциальностью, нормативным соответствием и допустимым использованием шифрования.

Мониторинг зашифрованного трафика

Устройство SSL Visibility Appliance — это один из компонентов корпоративной системы управления трафиком. Оно позволяет контролировать содержимое зашифрованного трафика и диагностировать атаки, которые в противном случае остались бы незамеченными. Устройство идентифицирует и расшифровывает все соединения SSL всех приложений на всех сетевых портах (включая нестандартные). Расшифрованные данные могут использоваться другими компонентами инфраструктуры для выявления и блокирования сложных угроз; принимая на себя ресурсоемкие процессы расшифровки, устройство SSL Visibility Appliance также помогает улучшить производительность корпоративной сети и инфраструктуры безопасности.

Рис. 1. Устройство SSL Visibility Appliance модели SV2800B.

Соблюдение конфиденциальности и нормативных требований

Устройство SSL Visibility Appliance выступает в качестве эффективного средства контроля за соблюдением политик. Оно отслеживает весь SSL-трафик в организации, сокращает риски, связанные с передачей зашифрованных данных, и помогает соблюсти политики, касающиеся конфиденциальности и нормативных требований. Возможность классификации хостов и типов SSL-трафика позволяет быстро создавать и настраивать политики избирательной расшифровки трафика (например: «не расшифровывать исходящий финансовый и банковский трафик»). Кроме того, с помощью политик можно контролировать использование устаревших или ненадежных алгоритмов и стандартов, таких как SSL v3.0.

Таким образом, организации могут сфокусировать внимание на трафике, представляющем наибольший риск, и поддерживать баланс между требованиями безопасности, конфиденциальности и соблюдения нормативов. Также предусмотрена возможность обмена информацией о категориях SSL-хостов, угрозах и вредоносных программах со всемирной аналитической сетью Symantec Global Intelligence Network.

Непревзойденная производительность и масштабируемость

Устройства SSL Visibility Appliance обладают той же пропускной способностью, что и линии, на которых они установлены, поэтому контроль за трафиком и потенциальными угрозами не оказывает негативного влияния на производительность сети и устройств. Отличительные особенности:

- Работа на скорости линии: задержка от порта к порту для незашифрованного трафика составляет менее 40 микросекунд. Устройство поддерживает расшифровку SSL-трафика на скорости до 9 Гбит/с для всех версий SSL/ TLS и более 70 наборов шифров.
- Быстрое создание сеансов и большое число потоков: возможность одновременной проверки до 800 000 сеансов SSL и установления/разрыва до 30 000 сеансов в секунду.
- Высокая доступность: аппаратный режим прямого/открытого соединения, настраиваемый мониторинг состояния канала и поддержка зеркалирования обеспечивают высокую доступность и безопасность сети.

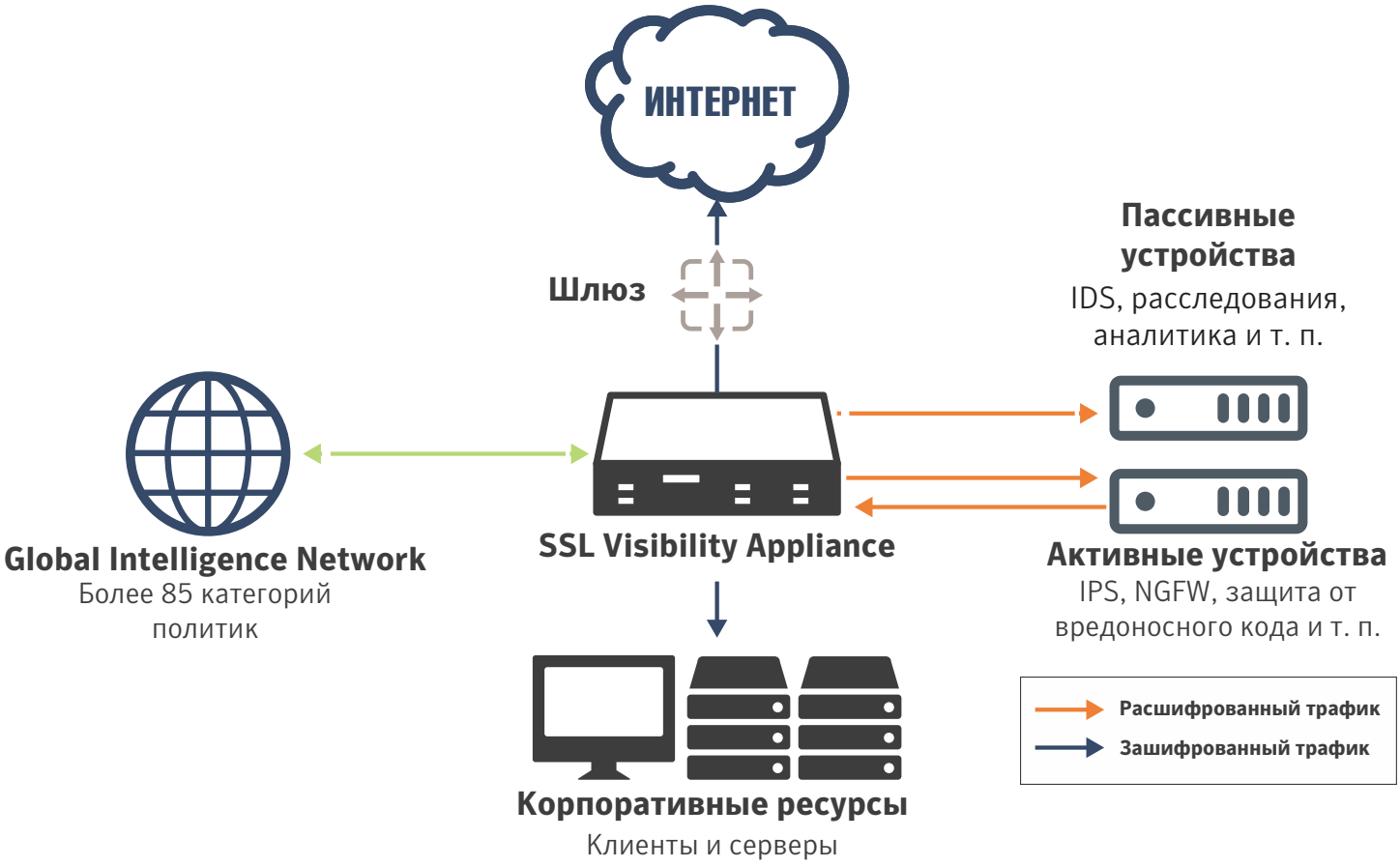
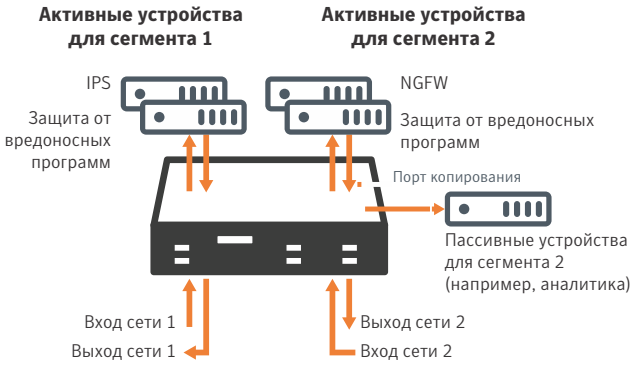


Рис. 2. Symantec SSL Visibility Appliance помогает централизовать управление зашифрованным трафиком.

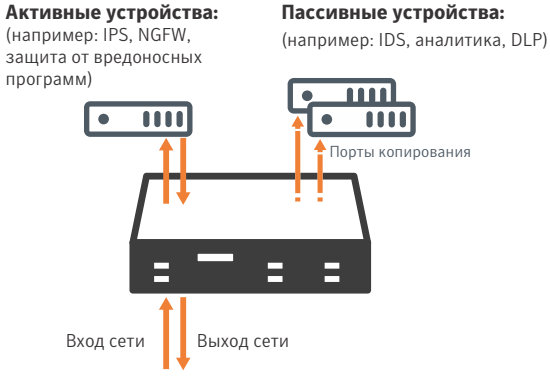
Интеграция в имеющуюся инфраструктуру

Устройства SSL Visibility Appliance идеально вписываются в уже имеющуюся инфраструктуру, не требуя установки дополнительных устройств или изменения сетевой архитектуры. Отличительные особенности:

- Более эффективное использование инфраструктуры: выполняя задачи расшифровки и мониторинга трафика, устройство повышает производительность и расширяет возможности сетевой инфраструктуры и устройств безопасности.
- Прозрачность в сети: устройство SSL Visibility Appliance прозрачно для конечных систем и промежуточных элементов сети. Оно не требует перенастройки сети, изменения IP-адресов или топологии, клиентских настроек IP и конфигурации браузеров.



- Множество вариантов развертывания: установка на линии или на отдельном сегменте, возможность отправки данных на одно или несколько активных или пассивных устройств (поддерживаемое число сегментов зависит от модели устройства).



- Порты копирования: устройство SSL Visibility Appliance может отправлять копии данных на множество устройств через дополнительные порты. Это позволяет передавать весь трафик (расшифрованный и незашифрованный) на дополнительные пассивные устройства.
- Сохранение информации о приложениях: расшифрованные данные, передаваемые на устройства безопасности в виде потока TCP, сохраняют исходные заголовки пакетов. Это позволяет приложениям и устройствам, таким как брандмауэры следующего поколения (NGFW), системы обнаружения/предотвращения вторжений (IDS/IPS), системы предотвращения утечки данных (DLP) и аналитические системы, обеспечивать защиту от угроз, которые ранее были скрыты в зашифрованном трафике. Для работы подключенных систем не требуются специальные программы или функции. При подключении к ProxySG устройство SSL Visibility Appliance должно иметь версию ПО 4.x, а устройство ProxySG — версию не ниже 6.7.2.x.
- Всесторонняя поддержка: полный контроль входящих и исходящих сеансов SSL; поддержка сетей с асимметричной маршрутизацией трафика; поддержка нескольких центров сертификации (CA) повторной подписи при анализе исходящих SSL-соединений; импорт множества пар «ключ сервера/сертификат» для мониторинга входящих SSL-соединений с корпоративными SSL-серверами.
- Консолидация трафика: объединение входящего трафика из нескольких сегментов сети и передача его на анализ в один пассивный сегмент.

Удобство управления и администрирования

Устройства SSL Visibility Appliance отличаются простотой настройки и администрирования:

- Управление одним устройством: мощный и удобный веб-интерфейс настройки и управления, защищенный по стандарту SSL.
- Централизованное управление: администрирование нескольких устройств из Symantec Management Center, включая мониторинг настройки и производительности, контроль работоспособности, резервное копирование конфигурации, выполнение задач по расписанию и синхронизацию конфигураций. Management Center также поддерживает RBAC.
- Уведомление по электронной почте: возможность автоматической генерации предупреждений, которые могут направляться сетевым администраторам незамедлительно или по заданному расписанию.
- Идентификация сеансов SSL: журналы сеансов содержат подробные сведения о всех проверенных и не проверенных соединениях SSL, что позволяет выявлять подозрительные тенденции и схемы использования SSL.
- Передача в формате syslog: поддержка до 8 удаленных серверов syslog позволяет снабжать данными специализированные приложения для составления отчетов и ведения журналов в распределенных средах.
- Поддержка SNMP: обеспечивает возможность мониторинга и управления, осуществляемого сторонними устройствами по протоколу SNMP v3.

	SV800-250M-C	SV800-500M-C	SV1800-C/-F	SV2800B	SV3800B	SV3800B-20
Производительность с ПО серии 3.X						
Общая пропускная способность	8 Гбит/с	8 Гбит/с	8 Гбит/с	20 Гбит/с	40 Гбит/с	40 Гбит/с
Скоросить при проверке SSL	250 Мбит/с	500 Мбит/с	1,5 Гбит/с	2,5 Гбит/с	4 Гбит/с	9 Гбит/с
Задержка при прямой передаче	<40мкс	<40мкс	<40мкс	<40мкс	<40мкс	<40мкс
Число одновременных потоков SSL	20 000	20 000	100 000	200 000	400 000	800 000
Установление соединений RSA (1024 бит)	1 000 в секунду	2 000 в секунду	7 500 в секунду	10 500 в секунду	12 500 в секунду	30 000 в секунду
Установление соединений RSA (2048 бит)	1 000	2 000	3 000	3 000	6 000	6 000
Установление соединений ECDHE256	500	1 000	3 500	6 000	8 000	11 000
Число записей в журнале SSL	32 000 000	32 000 000	32 000 000	32 000 000	32 000 000	32 000 000
Производительность с ПО серии 4.X						
Общая пропускная способность	8 Гбит/с	8 Гбит/с	8 Гбит/с	20 Гбит/с	40 Гбит/с	40 Гбит/с
Проверка классических сегментов	220 Мбит/с	450 Мбит/с	1,3 Гбит/с	2,8 Гбит/с	4,2 Гбит/с	7,3 Гбит/с
Проверка прокси-сегментов	0,2 Гбит/с	0,4 Гбит/с	0,9 Гбит/с	2,6 Гбит/с	3,9 Гбит/с	6,6 Гбит/с
Число одновременных потоков SSL	20 000	20 000	100 000	200 000	400 000	800 000
Установление соединений RSA (1024 бит)	1 000 в секунду	2 000 в секунду	7 300 в секунду	10 500 в секунду	12 500 в секунду	25 000 в секунду
Установление соединений RSA (2048 бит)	1 000	2 000	3 500	4 500	5 700	5 800
Установление соединений SSL ECDHE	450	900	2 800	6 000	8 000	12 000
Число записей в журнале SSL	32 000 000	32 000 000	32 000 000	32 000 000	32 000 000	32 000 000
Характеристики						
Конфигурации	Сетевые интерфейсы: Фикс.: 8 x 1 Гбит/с (витая пара)	Сетевые интерфейсы: Фикс.: 8 x 1 Гбит/с (витая пара)	Сетевые интерфейсы: Фикс.: 8 x 1 Гбит/с (витая пара) или 8 x 1 Гбит/с Fiber SX	Сетевые интерфейсы: 3 разъема Netmod, различные варианты на 1 и 10 Гбит/с	Сетевые интерфейсы: 7 разъемов Netmod, различные варианты на 1 и 10 Гбит/с	
Источники питания	1 x 150 Вт	1 x 150 Вт	Резервир. 1+1 450 Вт	Резервир. 1+1 750 Вт	Резервир. 1+1 750 Вт	
Интерфейсы управления	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45	1 x RJ45	
Стандарты управления	SNMP v1, v2c и v3; поддержка GET и TRAP на нескольких Symantec MIB; поддержка SET только для System Group					
Экран	ЖК 16 x 2 симв.	ЖК 16 x 2 симв.	ЖК 16 x 2 симв.	ЖК 16 x 2 симв.	ЖК 16 x 2 симв.	
Рабочая температура	5 °C – 40 °C	5 °C – 40 °C	5 °C – 40 °C	10 °C – 35 °C	10 °C – 35 °C	
Температура хранения	-10 °C – 60 °C	-10 °C – 60 °C	-10 °C – 60 °C	-10 °C – 60 °C	-10 °C – 60 °C	
Размеры (см.) (В x Ш x Г)	4,45 x 20,32 x 32,39	4,45 x 20,32 x 32,39	4,45 x 43,18 x 50,8	4,45 x 44,45 x 73,66	8,89 x 44,45 x 73,66	
Соответствие нормативным требованиям и стандартам	CE (EN55022, EN55024, EN60950), FCC часть 15 класс A, UL60950-1					
Сертификация	Нет	Нет	FIPS 140-2 уровня 2 для моделей SV180B, SV2800, SV2800B, SV3800, SV3800B и SV3800B-20. Модели также имеют сертификаты Common Criteria NDPP и SOGIS, проводится сертификация EAL3+. Модели также имеют сертификаты UC/APL.			
Режимы работы (в каждом сегменте)	Passive-Tap, Passive-Inline, Active-Inline Fail to Network (FTN) и Fail to Appliance (FTA), сегмент ProxySG (только в 4.x)					
Режимы контроля	Контролируемый клиент (повторная подпись) [на линии], Контролируемый сервер (известный ключ). Полный список см. в руководстве администратора.					
Шифрование	TLS 1.3, TLS 1.2, TLS 1.1, TLS 1.0, SSLv3, частично SSLv2					
Алгоритмы с открытым ключом	RSA, DHE, ECDHE					
Алгоритмы с симметричным ключом	AES, AES-GCM, 3DES, DES, RC4, ChaCha20-Poly1305, Camellia					
Алгоритмы хэширования	MD5, SHA-1, SHA-2, SHA256, SHA384					
Ключи RSA	512 – 4096 бит					
Программное обеспечение						
Лицензирование ПО	Для активации проверки на каждом устройстве необходима лицензия Symantec. См. раздел, посвященный лицензированию, на портале поддержки Symantec. Классификация хостов — дополнительная услуга, требующая отдельной лицензии на каждое устройство.					

Symantec

350 Ellis St., Mountain View, CA 94043 США | +1 (650) 527 8000 | 1 (800) 721 3934 | **www.symantec.com**

SYMC-DS-SSLV-v6