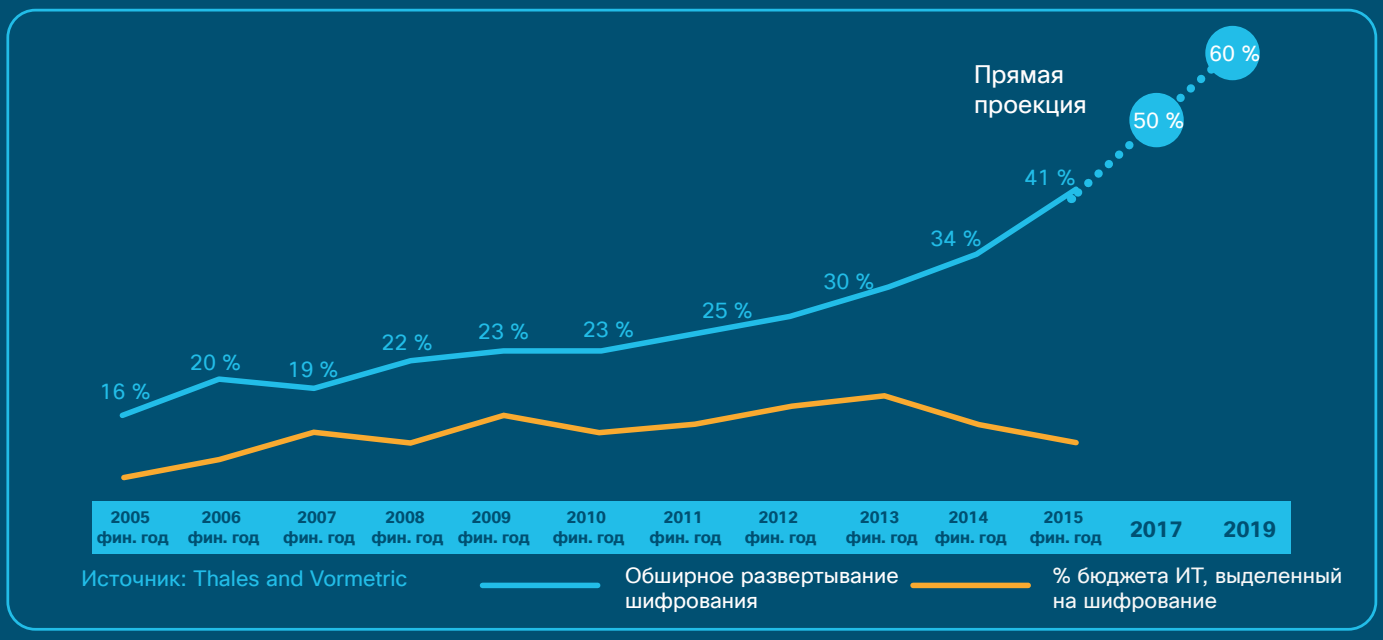
Аналитика зашифрованного трафика

Введение

Быстрый рост объемов зашифрованного трафика меняет ландшафт угроз. Поскольку все больше предприятий переходят на цифровые технологии, значительное число сервисов и приложений используют шифрование в качестве основного метода защиты обмена данными. В частности, объем зашифрованного трафика увеличился более чем на 90 % в годовом исчислении. Более 40 % веб-сайтов использовали шифрование трафика в 2016 году по сравнению с 21 % в 2015 году. По прогнозам Gartner, к 2019 году 80 % веб-трафика будет зашифровано.

Технология шифрования позволила значительно повысить конфиденциальность и безопасность для предприятий, использующих Интернет для связи и бизнеса в Интернете. Мобильные, облачные и веб-приложения используют проверенные реализации механизмов шифрования, использующих для обеспечения безопасности и доверия ключи и сертификаты. Но не только бизнес может выиграть от использования шифрования. Хакеры использовали те же преимущества, чтобы избежать обнаружения и защитить свою вредоносную деятельность. На рис. 1 показаны экономические последствия таких атак.

Шифрование меняет ландшафт угроз.

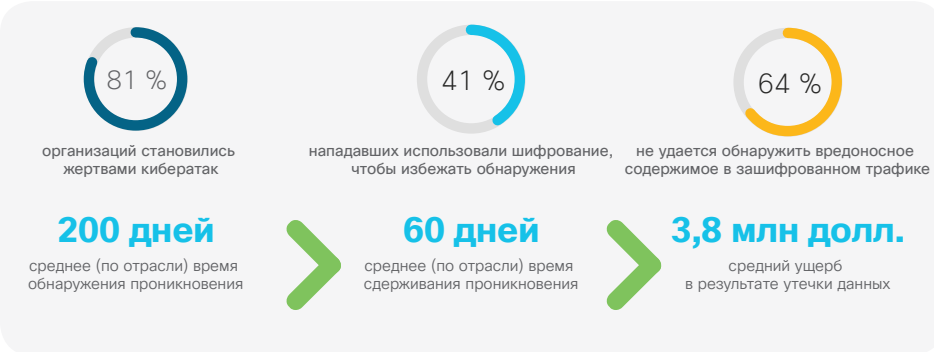


Содержание

Мониторинг всей сети в целом становится все более сложным, и традиционные средства обнаружения не могут предполагать, что какие-либо данные доступны для проверки. Нам необходима возможность одновременно оценить, какая часть нашего цифрового бизнеса защищена, а какая не защищена с помощью шифрования, а также какой трафик является вредоносным, а какой — нет.

По мнению Gartner, половина вредоносных кампаний в 2019 году будет использовать какой-либо тип шифрования для сокрытия доставки вредоносных программ, перехвата управления и кражи данных.

Рис. 1. Экономические последствия хакерских атак



В таблице 1 описаны новые векторы угроз, основанные на природе зашифрованного трафика.

Таблица 1. Новые векторы угроз на основе природы зашифрованного трафика

Непроверяемый зашифрованный трафик	Угрозы
Сотрудники, просматривающие веб-страницы по протоколу HTTPS	▪ Заражение вредоносным ПО ▪ Скрытый канал связи с управляющим сервером ▪ Утечка данных
Сотрудники во внутренней сети, безопасно подключающиеся к серверам периметра сети (ДМЗ)	Горизонтальное распространение с зараженных хостов
Пользователи Интернета, подключающиеся к общедоступным серверам предприятия с помощью зашифрованных протоколов	Ослабление защиты по всей глубине при использовании только одной технологии защиты для проверки входящего трафика

Задачи защиты от угроз в зашифрованном трафике

В большинстве организаций сегодня нет решения для обнаружения вредоносного контента в зашифрованном трафике. Им не хватает средств безопасности и ресурсов для реализации решения, которое могло бы быть развернуто во всей сетевой инфраструктуре без замедления работы сети.

Традиционная проверка на наличие угроз с использованием массовой расшифровки, анализа и повторного шифрования не всегда является практичной или выполнимой из-за снижения производительности и значительной загрузки ресурсов. Однако во многих случаях для идентификации вредоносных потоков для дальнейшей их проверки с использованием методов дешифрования можно использовать передовые аналитические методы.

Никогда точно не известно, какой объем трафика цифрового бизнеса компании зашифрован, а какой нет. Если трафик зашифрован, шифрование обычно выполняется в соответствии с нормативными требованиями, которые определяют конкретные политики безопасности.

Обзор аналитики зашифрованного трафика

Традиционный мониторинг потоков обеспечивает обзорное представление сетевой активности, предоставляя сведения об адресах, портах, количестве байтов и пакетов в потоке. Кроме того, в рамках мониторинга потоков можно собирать, хранить и анализировать метаданные внутри потока, то есть информацию о событиях, происходящих внутри потока. Эти данные особенно ценны, если трафик зашифрован, поскольку глубокая проверка пакетов в этом случае неэффективна. Эти метаданные внутри потока, называемые аналитикой зашифрованного трафика, создаются с использованием новых типов элементов данных или телеметрии, которые не зависят от данных протокола, таких как длина и время прибытия сообщений в потоке. Привлекательность этих элементов данных состоит в том, что они одинаково хорошо подходят как для зашифрованных, так и для незашифрованных потоков.

Используя эти элементы данных или внутрипотоковую телеметрию, технология ETA позволяет идентифицировать вредоносный код в зашифрованном трафике без необходимости его расшифрования (рис. 2). В таблице 2 перечислены преимущества использования аналитики зашифрованного трафика.

Рис. 2. Аналитика зашифрованного трафика – обзор технического решения

Таблица 2. Преимущества использования аналитики зашифрованного трафика

Преимущества
▪ Мониторинг безопасности. Анализ угроз в зашифрованном трафике с использованием аналитики сети. Контекстная аналитика угроз с использованием анализа в режиме реального времени с учетом информации о пользователях и устройствах. ▪ Криптографическая оценка. Соблюдение криптографических протоколов предприятием; мониторинг и информация о том, какой трафик в сети предприятия зашифрован, а какой нет. ▪ Ускорение реагирования. Быстрая изоляция зараженных устройств и пользователей. ▪ Экономия времени и средств. Использование сети как основы для анализа состояния защищенности с извлечением выгоды из инвестиций в безопасность сети.

Аналитика зашифрованного трафика — новые элементы данных для зашифрованного трафика

Аналитика зашифрованного трафика ориентирована на выявление вредоносного кода в зашифрованном трафике посредством пассивного мониторинга, извлечения соответствующих элементов данных и контролируемого машинного обучения с привлечением данных глобального облачного мониторинга.

Transport Layer Security (TLS) — это криптографический протокол, обеспечивающий конфиденциальность приложений. TLS обычно реализуется ниже общих протоколов, таких как HTTP для просмотра веб-страниц или SMTP для электронной почты. HTTPS представляет собой использование протокола TLS для протокола HTTP. Это самый популярный способ защиты обмена данными между веб-сервером и клиентом, который поддерживается большинством основных веб-серверов.

Аналитика зашифрованного трафика извлекает четыре основных элемента данных: последовательность длины и времени пакетов, распределение байтов, специфичные для TLS функции и исходный пакет данных. Созданная Cisco уникальная архитектура специализированных встроенных схем (ASIC) обеспечивает возможность извлечения этих элементов данных без замедления работы сети передачи данных.

- Последовательность длины и времени пакетов (SPLT). SPLT передает длину (количество байтов) прикладных полезных данных каждого пакета для нескольких первых пакетов потока вместе с промежутками времени между прибытием этих пакетов. SPLT можно представить как массив размеров пакетов (в байтах) в сочетании с массивом значений времени (в мс), представляющих время с момента прибытия предыдущего пакета.
- Распределение байтов. Распределение байтов представляет вероятность того, что определенное значение байта появится в полезных данных пакета в потоке. Распределение байтов потока можно рассчитать, используя массив счетчиков. Основные типы данных, связанных с распределением байтов: полное распределение байтов, энтропия байтов и среднее/стандартное отклонение байтов. Например, используя один счетчик для каждого значения байта, запрос GET протокола HTTP, «HTTP/1.1.», можно вычислить, увеличивая значение соответствующего счетчика на 1 для «H», а затем увеличивая другой счетчик дважды для двух последовательных «T» и так далее. Хотя распределение байтов поддерживается как массив счетчиков, его можно легко превратить в правильное распределение, нормализуя по общему количеству байтов.
- Исходный пакет данных (IDP). IDP используется для получения данных пакета из первого пакета в потоке. Это позволяет извлечь необходимые данные, такие как URL-адрес HTTP, имя/адрес DNS-узла и другие элементы данных. Квитирование TLS состоит из нескольких сообщений, содержащих необходимые незашифрованные метаданные, используемые для извлечения элементов данных, таких как комплекты шифров, версии TLS и длина открытого ключа клиента.

В приложении A приведена подробная таблица новых элементов данных.

Расширенные возможности сети как сенсора благодаря аналитике зашифрованного трафика — компоненты

Расширенная технология NetFlow

В архитектуре NetFlow данные передаются от экспортера к коллектору в наборах записей. Каждая запись в наборе данных имеет формат, указанный в его шаблоне. Запись данных состоит из серии информационных элементов NetFlow, или «полей», а для каждого поля назначается определенное значение идентификатора. Значения идентификаторов информационных элементов могут быть определены глобально и заархивированы Администрацией адресного пространства сети Интернет (IANA) либо могут быть специфичными для предприятия и определяться отдельными организациями.

Шаблоны NetFlow используют несколько глобально определенных элементов, администрируемых IANA. Некоторые из глобальных элементов, такие как IP-адреса и номера портов уровня 4, образуют знакомую 5-элементную запись, которая используется как уникальный идентификатор потока (ключ потока). Дополнительные элементы содержат базовую статистику пакета/октета и метки времени.

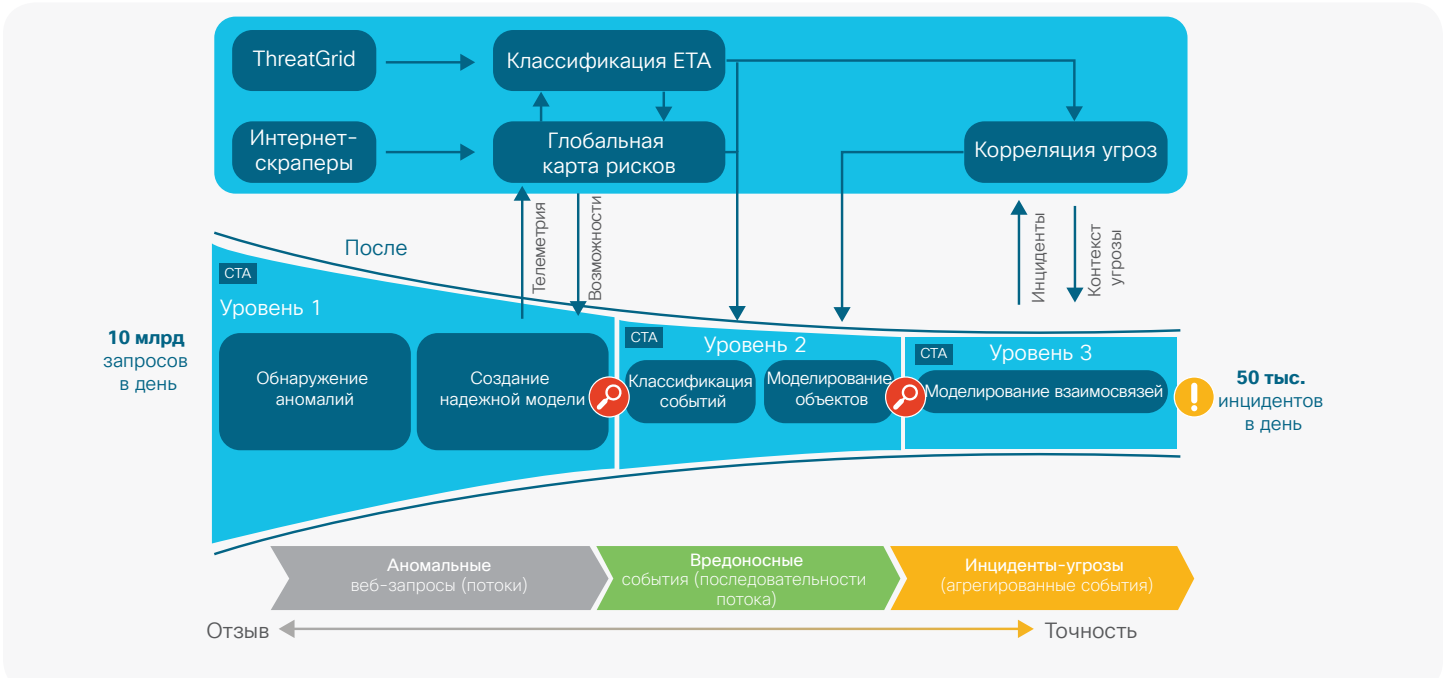
Эти глобально определенные элементы дополняются элементами данных конкретного (ИД поставщика компании Cisco) (описаны ранее и в приложении A). Элементы данных конкретного поставщика предоставляют информацию об угрозах и уязвимостях в зашифрованном трафике с использованием системы Cisco Stealthwatch®.

Stealthwatch с функциями когнитивной аналитики

Система Cisco Stealthwatch использует NetFlow, прокси-серверы, телеметрию оконечных устройств, механизмы политик и доступа, сегментацию трафика и многое другое, чтобы определить базовое нормальное поведение хостов и пользователей в организации. Благодаря интеграции когнитивной аналитики (облачного механизма анализа) система Stealthwatch может сопоставлять трафик с глобальными типами угроз и автоматически идентифицировать зараженные хосты, команды и перехват управления и подозрительный трафик.

Когнитивная аналитика поддерживает глобальную карту рисков — очень широкий профиль поведения серверов в Интернете, идентифицирующий серверы, которые связаны с атаками либо могут быть использованы злонамеренно или в составе атаки в будущем (рис. 3). Это не черный список, а целостная картина с точки зрения безопасности. Механизм когнитивной аналитики анализирует новые элементы данных зашифрованного трафика в расширенной технологии NetFlow, применяя машинное обучение и статистическое моделирование. Глобальная карта рисков и элементы данных аналитики зашифрованного трафика дополняют друг друга в механизме когнитивной аналитики. Вместо того чтобы расшифровывать трафик, система Stealthwatch с механизмом когнитивной аналитики использует алгоритмы машинного обучения для выявления шаблонов вредоносного кода в зашифрованном трафике, чтобы помочь выявлять угрозы и повысить эффективность реагирования на инциденты.

Рис. 3. Механизм когнитивной аналитики



Панель управления анализом безопасности на консоли управления системой Stealthwatch (SMC) предоставляет список пользователей, выявленных с помощью когнитивной аналитики, с сортировкой по типу риска. Расширенная панель управления когнитивной аналитики содержит подробную информацию о распространении угроз с максимальным риском и относительной подверженности угрозам. В таблице 3 перечислены некоторые угрозы, представляющие высокий риск, которые используют зашифрованные команды и элементы управления.

Рис. 4. Панель управления анализом безопасности системы Stealthwatch с когнитивной аналитикой

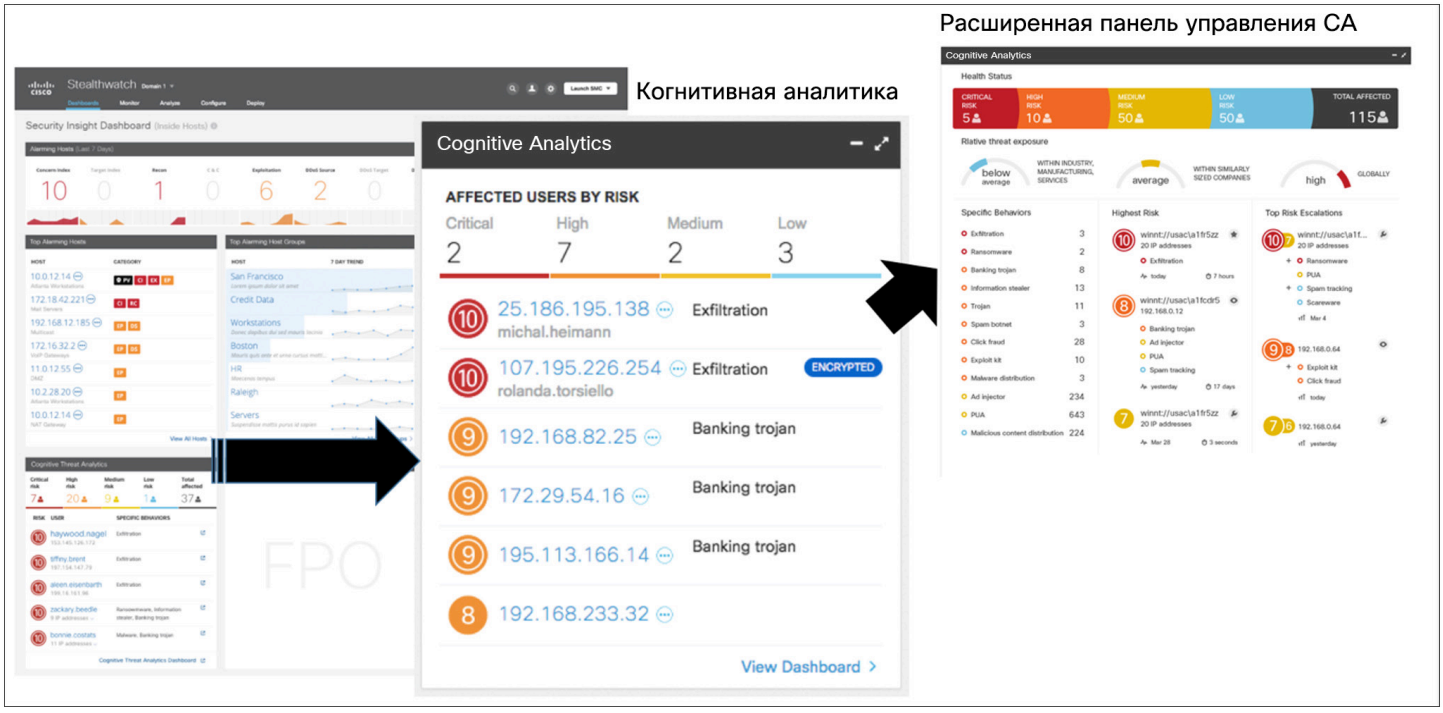


Таблица 3. Примеры угроз с высоким риском с использованием зашифрованных команд и элементов управления

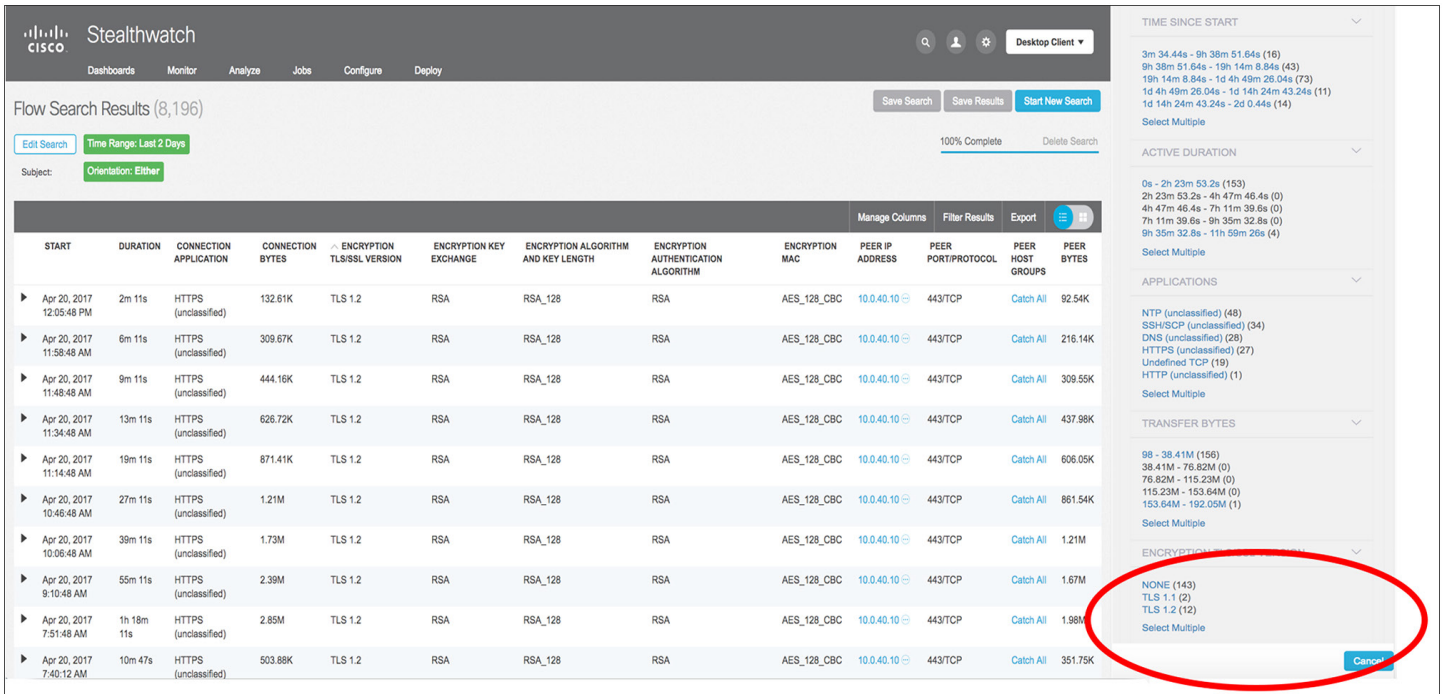
Название	Тип
Gamarue/Andromeda	Модульный ботнет
Sality	Заражает файлы, модульный ботнет
Necurs	Кража информации, инструмент обхода системы защиты, ботнет
Rerdom	Скликивание, ботнет

После обнаружения вредоносный зашифрованный поток может быть заблокирован или помещен в карантин системой Stealthwatch. Действия по восстановлению на основе правил через pxGrid с использованием платформы Cisco Identity Services Engine (ISE) с Cisco TrustSec® и программно определяемым доступом (SDA) упрощают и ускоряют операции обеспечения безопасности сети.

Криптографическая оценка

Аналитика зашифрованного трафика также мгновенно определяет качество шифрования в каждой сетевой цепочке сообщений, обеспечивая мониторинг в соответствии с корпоративными требованиями с использованием криптографических протоколов. Предоставляется информация о том, какой трафик в вашей сети зашифрован, а какой нет, поэтому вы можете с уверенностью утверждать, что ваш цифровой бизнес защищен. Эта криптографическая оценка отображается в системе Stealthwatch и может быть экспортирована через API-интерфейсы в инструменты сторонних производителей для мониторинга и аудита соответствия требованиям к шифрованию (рис. 5).

Рис. 5. Криптографическая оценка



Поддержка функций

Новейшие сетевое оборудование Cisco, начиная с версии Cisco IOS® XE 16.6, будет поддерживать расширенную технологию NetFlow с функциональностью аналитики зашифрованного трафика.

1. Совместимое оборудование Cisco, поддерживающее расширенную технологию NetFlow с аналитикой зашифрованного трафика:

- Коммутаторы: Cisco Catalyst® серии 9300 (начиная с версии Cisco IOS XE 16.6) и серий 9400 и 9500 (начиная с версии Cisco IOS XE 16.8.1)
- Маршрутизаторы: ASR 1001-X, ASR 1002-X, ASR 1001-HX, ASR 1002-HX, ASR 1004, ASR 1006-X, ASR 1009-X, 4221 ISR, 4321 ISR, 4331 ISR, 4351 ISR, 4431 ISR, 4451-X ISR, виртуальный маршрутизатор с интегрированными сервисами (ISRv), включая 5400 Enterprise Network Compute System, маршрутизатор облачных сервисов (CSR) 1000 B (начиная с версии Cisco IOS XE 16.7)

2. Система Stealthwatch дополняется возможностями машинного обучения и статистического моделирования (в версии 6.9.2) для анализа расширенной технологии NetFlow с аналитикой зашифрованного трафика.
3. Stealthwatch Learning Network License (v2.0) на маршрутизаторах может создавать поведенческие профили зашифрованного трафика, позволяя отмечать аномалии, обнаруженные в зашифрованном трафике.

Эффективность и результаты исследований компании Cisco

В экспериментах на основе реальных данных мы смогли достичь точности более 99 % с 0,01 % ложных срабатываний (только 1 неверный положительный сигнал на каждые 10 000 соединений TLS). Исследование было основано на большой выборке реальных сеансов HTTPS, как описано в результатах исследований Cisco.

Заключение

Таким образом, сеть теперь представляет собой очень эффективный сенсор безопасности, способный обнаруживать угрозы в зашифрованном трафике. Инфраструктура с поддержкой архитектуры цифровых сетей Cisco DNA превращает сеть в полноценный сенсор и комплексный регулятор политик, что позволяет обнаруживать, сдерживать и предотвращать самые сложные угрозы безопасности.

Приложение A

Элементы данных, извлеченные аналитикой зашифрованного трафика

Последовательность длины и времени пакетов (SPLT)	Массив значений длины LENGTH, за которым следует массив времени INTERARRIVAL TIME, описывающий первые N пакетов потока, которые несут полезные данные приложений. Каждое значения LENGTH кодируется как 16-разрядное целое число, образуя массив из 20 байтов. Сразу за ним следует значение INTERARRIVAL TIME, которое кодируется в виде 16-разрядного целого значения, формируя другой массив из 20 байтов.
Распределение байтов	Гистограмма, указывающая частоту появления каждого байтового значения (или диапазона значений) в первых N байтах полезных данных приложения в потоке. Каждая частота появления представлена как 16-разрядное целое число.
Исходный пакет данных (IDP)	Содержимое первого пакета этого потока, которое содержит фактические полезные данные, начиная с IP-заголовка.
Записи TLS	Массив значений LENGTH, за которым следует массив значений INTERARRIVAL TIME, затем массив значений CONTENT TYPE и массив значений HANDSHAKE TYPE. Эти массивы описывают первые N записей потока TLS.
Длина записей TLS	Последовательность длин записей для первых N записей в потоке TLS.
Время записей TLS	Последовательность времени между прибытием TLS для первых N записей в потоке TLS.
Типы контента TLS	Последовательность значений ContentType для первых N записей в потоке TLS.
Типы квитирования TLS	Последовательность значений HandshakeType для первых N записей в потоке TLS.
Наборы шифров TLS	Список до N наборов шифров, предложенных клиентом или выбранных сервером в потоке TLS.
Расширения TLS	Массив значений LENGTH, за которым следует массив значений EXTENSION TYPE, описывающих расширения TLS, которые наблюдаются в сообщении Hello для потока TLS.

Имя элемента данных	Описание
Длина расширений TLS	Список длин расширений для первых N расширений TLS, наблюдаемых в сообщении Hello протокола TLS для потока.
Типы расширений TLS	Список типов расширений для первых N расширений TLS, наблюдаемых в сообщении Hello протокола TLS для потока.
Версия TLS	Номер версии протокола TLS, которая наблюдается в сообщении Hello протокола TLS для потока.
Длина ключа TLS	Длина клиентского ключа, который наблюдается в сообщении ClientKeyExchange протокола TLS.
Идентификатор сеанса TLS	Значение идентификатора сеанса, которое наблюдается (если есть) в сообщении Hello протокола TLS для потока.
Случайное значение TLS	Случайное значение, которое наблюдается в сообщении Hello протокола TLS для данного потока.

Справочные материалы

1. Gartner. Директора по информационной безопасности должны обеспечить защиту от угроз, связанных с растущим объемом SSL-трафика
2. Институт Ponemon. Выявление скрытых угроз в зашифрованном трафике, 2016 г.
3. NSS Labs: TLS/SSL. Где мы находимся сегодня? Зашифрованный Интернет. Часть 1. Тенденция роста
4. Выявление зашифрованного трафика вредоносных программ в контекстном потоке данных, Блейк Андерсон (Blake Anderson) и Дэвид Мак-Грю (David McGrew), AISEC '16