ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
СПбГУТ))) Декабрь 2017 Том 5 № 4 ISSN 2307-1303 http://www.itt.sut.ru
TELECOM IT
December 2017 Vol. 5 Iss. 4 ISSN 2307-1303 http://www.itt.sut.ru

CISCO TRUSTSEC

А. И. Катасонов[1*], А. Ю. Цветков[1], В. И. Андрианов[1]

[1] СПбГУТ, Санкт-Петербург, 193232, Российская Федерация
* Адрес для переписки: ksasha716@yandex.ru

Аннотация
В наше время технологии непрерывно развиваются. С каждым днем появляются новые протоколы для функционирования сети, знания о работе которых необходимы для обеспечения корректной работы сети. **Предмет исследования.** Статья посвящена протоколу обеспечения безопасности в сети, его принципу работы, архитектуре, возможностям, а также сходствам и различиям данного протокола от его аналогов. **Метод.** Рассмотрена структура, принцип работы возможности данного протокола, выявлены его характерные черты, а также проведен сравнительный анализ с протоколом IPSec, показывающий положительные и отрицательные стороны исследуемого протокола. **Основные результаты.** Проанализирована работа протокола TrustSec, выявлены особенности данного протокола, а также описан принцип работы, архитектура, возможности и характерные черты данного протокола. Составлен материал для изучения и получения необходимых знаний для использования протокола TrustSec. **Практическая значимость.** Разработанная нами статья может быть использована преподавателями для обучения, а также помогает администраторам сети настроить работу данного протокола.
Ключевые слова
TrustSec, безопасность, сеть, шифрование, Cisco, MACsec.

Информация о статье
УДК 004.057.4
Язык статьи – русский.
Поступила в редакцию 31.10.17, принята к печати 01.12.17.

Ссылка для цитирования: Катасонов А. И., Цветков А. Ю., Андрианов В. И. Cisco TrustSec // Информационные технологии и телекоммуникации. 2017. Том 5. № 4. С. 85–95.

CISCO TRUSTSEC

A. Katasonov[1*], A. Tsvetkov[1], V. Andrianov[1]

[1] SPbSUT, St. Petersburg, 193232, Russian Federation
* Corresponding author: ksasha716@yandex.ru

Abstract—In our time, technology is continuously evolving. Each day, new protocols for networking, knowledge of the work necessary to ensure the proper functioning of the network. **Research subject.** The article is devoted to the security protocol in the network, TrustSec, its operation principle, architec-

ture, capabilities, and similarities and differences of this protocol from its analogues. **Method.** The structure, operating principle, available protocol and characteristic features are revealed, and a comparative analysis was carried with the IPSec protocol, showing the positive and negative aspects of the explored protocol. **Core results.** The work of the protocol of TrustSec, the revealed features of this protocol, as well as the described operating principles, architecture, capabilities and characteristics of this protocol are analyzed. Material is prepared for studying and obtaining the necessary knowledge to use the TrustSec protocol. **Practical relevance.** The article developed by us can be filled by teachers for teaching students, help network administrators configure the operation of this protocol.

Keywords—TrustSec, Security, network, encryption, Cisco, MACsec.

Article info
Article in Russian.
Received 31.10.17, accepted 01.12.17.

For citation: Katasonov A., Tsvetkov A., Andrianov V.: Cisco TrustSec // Telecom IT. 2017. Vol. 5. Iss. 4. pp. 85–95 (in Russian).

Введение

Архитектура Cisco TrustSec – это система управления безопасностью сети с помощью меток безопасности Secure Group Tag (SGT), которые по своему потенциалу несут более глубокий и продвинутый подход к формированию политик доступа в сеть с возможностью их детализации и применения.

Ключевыми элементами данной системы являются системы политик, а именно система контроля и учета доступа в сеть – Cisco Identity Services Engine (ISE), MACsec и SGT. Рассмотрим архитектуру TrustSec и всех её частей по отдельности.

Модель работы TrustSec

Классификация, транспорт и политика обеспечения безопасности Cisco TrustSec встроены в коммутаторы, маршрутизаторы, беспроводные локальные сети и продукты брандмауэра компании Cisco. Трафик классифицируется на основе контекстной идентичности конечной точки с ее IP-адресом, Cisco TrustSec предлагает более гибкие средства управления доступом для динамических сетевых сред и центров обработки данных. Особенности, связанные с SGT *(Secure Group Tag*) на сетевых устройствах, можно разбить на три категории: Классификация, Транспорт и Исполнение.

- *Классификация:* Классификация – это присвоение SGT IP-адресу. Он может быть либо динамический, либо статический. Динамическая классификация использует богатые контекстные данные, доступные для Cisco Identity Services Engine (ISE) для создания политических решений, может быть выполнена с использованием 802.1X, аутентификации MAC, *Bypass* (Запасной путь) или веб-аутентификации. Статическая классификация обычно настраивается на коммутаторе, к которым подключены серверы. Варианты статической классификации включают отображение IP-адресов, VLAN или порт SGT.
- *Транспорт:* таблица прав доступа следует за трафиком через сеть. Это может быть выполнено посредством встроенной маркировки или протокола SGT *eXchange* (SXP). В первом варианте SGT встраивается в заголовок кадра Ethernet. Стоит отметить, что не все сетевые устройства поддерживают встроенные теги.

- *Исполнение:* Исполнение осуществляет разрешение или отклоняет политическое решение, основанное на источнике и назначения SGT. Это может быть выполнено с помощью SGACL (*Security group access control list* – контрольный лист безопасности прав доступа) при переключении платформ и SGFW (*Secure Group Firewall* – Брандмауэр групп доступа).

MACsec обеспечивает безопасную связь в проводных локальных сетях. Когда MACsec используется для защиты связи между конечными точками в локальной сети, каждый пакет на проводе шифруется с использованием симметричной криптографии ключа, так что связь не может быть просмотрена или изменена во время передачи. Когда MACsec используется в сочетании с тегами группы безопасности, он обеспечивает защиту для тега вместе с данными, содержащимися в полезной нагрузке кадра.

В точке доступа к сети, группой политик Cisco TrustSec, называемых SGT, присваивается конечная точка. Это делается с учетом любого из множества наборов атрибутов, включая пользователя конечной точки, тип устройства, статус и атрибуты местоположения. SGT показывает есть ли у конечной точки право доступа. Важно понимать, что весь трафик несет в себе информацию SGT. SGT охватывает определенную физическую область и не зависит от IP-адреса, подсети или VLAN.

Вместо управления доступом к большому количеству префиксных IP-адресов управление доступом регулируется через относительно небольшое количество соответствующих классификаций групп безопасности. SGACL определяет, какие услуги доступны между двумя группами безопасности. Простая матрица присваивает все SGACL для исходных и целевых пар SGT. Одна матрица обеспечивает всю политику для всего Домена TrustSec.

Сравним TrustSec с традиционной политикой контроля доступа, которая реализуется со статическими ACL (*Access Control List*), развернутые в стратегических пунктах обеспечения безопасности SGA. Преимущества TrustSec заключаются в намного более простых процедурах обслуживания. Традиционные списки ACL имеют повторяющиеся записи, которые охватывают различные IP-адреса источника и назначения. Когда предоставляется новая беспроводная подсеть или запускается новый веб-сервер, все связанные списки управления доступом должны быть обновлены. На крупном предприятии, эти списки ACL могут быть длинными и очень сложными. На рис. 1 изображен пример увеличения архитектуры сети, который потребует значительного ACL пересмотра в традиционной реализации. Подобные изменения необходимы, когда часть сети выведена из эксплуатации. Эти события намного проще администрировать при помощи TrustSec. С TrustSec недавно созданный ресурс просто нуждается в настройке классификации при входе, чтобы должным образом поддерживать существующую политику SGACL. В этом случае необходимо ввести новые группы безопасности, тогда новая строка и столбец будут добавлены к матрице. Эта матрица обновляется централизованно на Cisco ISE и динамически распространяется через домены TrustSec.

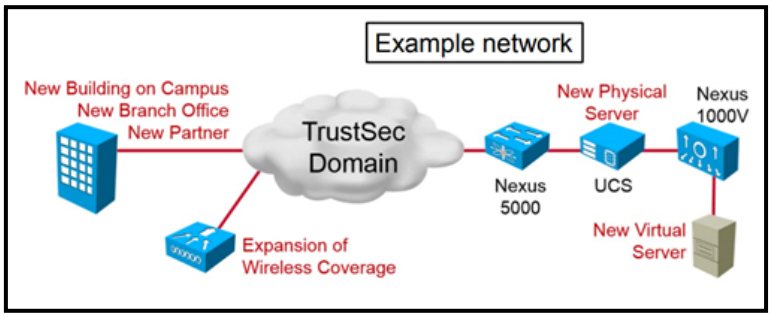

Рис. 1. Пример увеличения архитектуры сети

Cisco Security Group Access (SGA) устанавливает облака доверенных сетевых устройств для создания безопасных сетей.

SGA решает использовать информацию об идентификаторе устройства и пользователе, которую он получает во время аутентификации для классификации пакетов при их входе в сеть. Эта классификация, поддерживается путем маркировки пакетов при входе в сеть SGA. Она допускает в сеть пакеты, которые поддерживаются политикой безопасности как во время передачи информации, так и при выходе её в сеть. Тег, также называемый тегом группы безопасности (SGT – *Security Group Tag*), распространен по всей сети как часть кадра Ethernet. Выходное устройство может фильтровать трафик на основе исходного SGT и SGT, который связан с целевым устройством [1].

Основное преимущество решения SGA заключается в увеличении масштабируемости определения политики. SGA абстрагирует топологию сети от политики, которую необходимо настроить на Cisco ISE.

Более конкретно, SGA даёт следующие преимущества:

- Контроль доступа упрощается благодаря использованию ACL групп безопасности (SGACL);
- Контроль доступа основан на идентификационных группах независимо от физического местоположения, метода передачи (проводной, беспроводной, VPN и т. д.) и IP-адреса;
- Сеть автоматизирует выравнивание пользователей и серверов с группами;
- Администратор управляет всеми отношениями между исходной группой и назначением;
- Философия SGA значительно уменьшают количество правил политики, которые должны быть определены на Cisco ISE.

Кадры, которые входят в домен Cisco TrustSec, отмечены уникальным 16-битным тегом, который представляет собой уникальную роль источника трафика в сети. Тег можно рассматривать как идентификатор привилегии исходного пользователя, устройства или объекта.

Когда кадры поступают на выходное устройство домена Cisco TrustSec, они фильтруются в исходящих портах с использованием SGACL. Конфигурация SGACL не использует какой-либо конкретный IP-адрес. Он распространяется Cisco ISE и содержит ссылки на тэги входа и выхода. Cisco ISE отвечает за предоставление политики тегирования входа и выхода ACL для сетевых устройств в домене Cisco TrustSec.

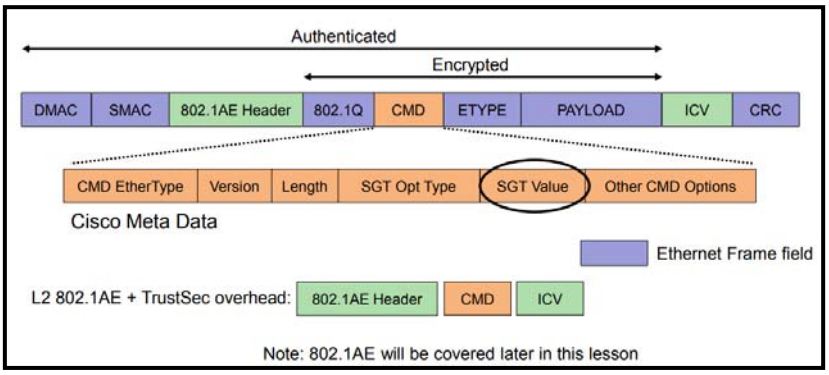

Рис. 2. Состав кадра

Кадры, которые пересекают домен Cisco TrustSec, изменяются во входящем доступе, чтобы поддерживать теги и криптографические функции, предлагаемые решением Cisco TrustSec. Инкапсуляция включает в себя заголовок 802.1AE, заголовок метаданных Cisco и поле Integrity Check Value (ICV – Значение проверки целостности) (рис. 2).

Заголовок метаданных Cisco включает SGT, 16-разрядное число, которое идентифицирует источник трафика.

Операция тегирования на входном устройстве выполняется перед другими службами уровня 2, такими как обработка качества обслуживания (QoS – *Quality of Service*), увеличение максимального размера блока передачи (MTU – *Maximum Transmission Unit*), которое получается из-за служебных данных 802.1AE и Cisco TrustSec, объем которых составляет приблизительно 40 байт.

Не все устройства Cisco, а также сетевые устройства от других поставщиков способны использовать встроенный SGT-транспорт. SXP позволяет распространять IP на SGT обходя все границы. Основная цель – получить данные SGT от устройств, которые выполняли классификацию подключаемых конечных точек на восходящих устройствах, которые будут выполнять принудительное выполнение Cisco TrustSec на основе информации SGT.

Соединения SXP являются двухточечными и используют TCP в качестве базового транспортного протокола, используя 64999 порт. При настройке SXP-соединения с одноранговым узлом необходимо назначить каждое устройство в качестве источника или приёмника. Режим источника позволяет устройству пересылать все активные IP-адреса в SGT вышестоящим устройствам для соблюдения политики. Режим приёмника позволяет устройству получать IP-адреса SGT от последующих устройств и использовать эту информацию при принятии политических решений.

Если один конец SXP-соединения настроен как источник, другой конец должен быть настроен как приёмник, и наоборот [2]. Если оба устройства на каждом конце SXP-соединения сконфигурированы с одинаковой ролью, SXP-соединение не удастся. Необходимо соблюдать осторожность при настройке соединений SXP, чтобы избежать создания циклов, если не используется развертывание SXP версии 4 или выше. Ниже перечислены возможности SXP версий с 1 по 4:

- *Версия 1:* Исходная версия. Поддержка распространения привязки IPv4.
- *Версия 2:* Добавлено распространение привязки IPv6 и согласование версий.

- *Версия 3:* Добавлена поддержка подсетей для привязок SGT. Если вы говорите со слушателем более низкой версии, динамик расширит подсеть.
- *Версия 4:* добавлено обнаружение и предотвращение циклов, обмен возможностями и встроенный механизм поддержания активности.

Используя SGACL, вы можете управлять политиками доступа на основе тегов группы безопасности источника и получателя. Применение политики в домене Cisco TrustSec представлено матрицей разрешений с номерами групп безопасности на одной оси и номерами групп безопасности назначения на другой оси. Каждая ячейка в теле матрицы может содержать упорядоченный список SGACL. Каждый SGACL указывает разрешения, которые должны применяться к пакетам, исходящим из исходной группы безопасности и предназначенным для целевой группы безопасности. Важно отметить, что источник и адресаты указаны в матрице политики, а не в SGACL. Спецификация тегов исходной или целевой группы в SGACL отсутствует, так как есть приложение SGACL в матрице разрешений, определяющее группы безопасности источника и назначения. Также важно понимать, что один и тот же SGACL может применяться к нескольким парам пар и групп безопасности источника и получателя в матрице разрешений.

Применяя контроль доступа между парами групп безопасности, Cisco TrustSec обеспечивает поддержку на основе ролей, не зависящую от топологии в сети. Изменения в топологии сети обычно не требуют изменения политики безопасности на основе SGACL. Если изменения требуют создания новой группы безопасности, то матрица разрешений будет увеличиваться в размере на одну строку и один столбец. Политика для новых ячеек определяется централизованно в Cisco ISE и динамически развертывается во всех точках безопасности SGACL.

Использование ролевых разрешений значительно уменьшает размер списков ACL и упрощает их обслуживание. С Cisco TrustSec количество настроенных ACE (*Access control entitles* – объекты контроля доступа) определяется количеством указанных разрешений, что приводит к значительно меньшему количеству ACE, чем в традиционной IP-сети. Кроме того, только одна копия SGACL должна находиться в TCAM устройства (*Ternary Content Addressable Memory* – Адресная память с троичными данными), независимо от того, сколько раз используется SGACL. Использование SGACL в Cisco TrustSec обычно приводит к более эффективному использованию ресурсов TCAM по сравнению с традиционными списками ACL [3].

Вместо SGACL адаптивное устройство безопасности Cisco и подходящая платформа маршрутизации применяют политику TrustSec, используя функции SGFW (*Secure Group Firewall* – Брандмауэр групп доступа). Когда политика SGACL централизованно управляется из *Cisco Identity Services Engine* (Сервис идентификации), политика SGFW управляется независимо от конфигурации устройства. Возможности SGFW были интегрированы в политику правил ASA (*Adaptive Security Appliance* – серия аппаратных межсетевых экранов, разработанных компанией Cisco Systems) в версии 9.0 и в функцию брандмауэра на основе зон IOS в версии 15.2. На рис. 3 показано использование данных группы безопасности в записи управления доступом в ASA, как из ASDM (*Adaptive Security Device Manager*), так и из CLI (*Command Line Interface* – интерфейс командной строки). В брандмауэре на основе зон IOS можно сопоставлять утверждения группы безопасности в определениях классовой карты. В обоих случаях информация группы

безопасности может использоваться в сочетании с другими механизмами спецификации трафика, такими как IP-адрес источника и получателя, номера протоколов и портов.

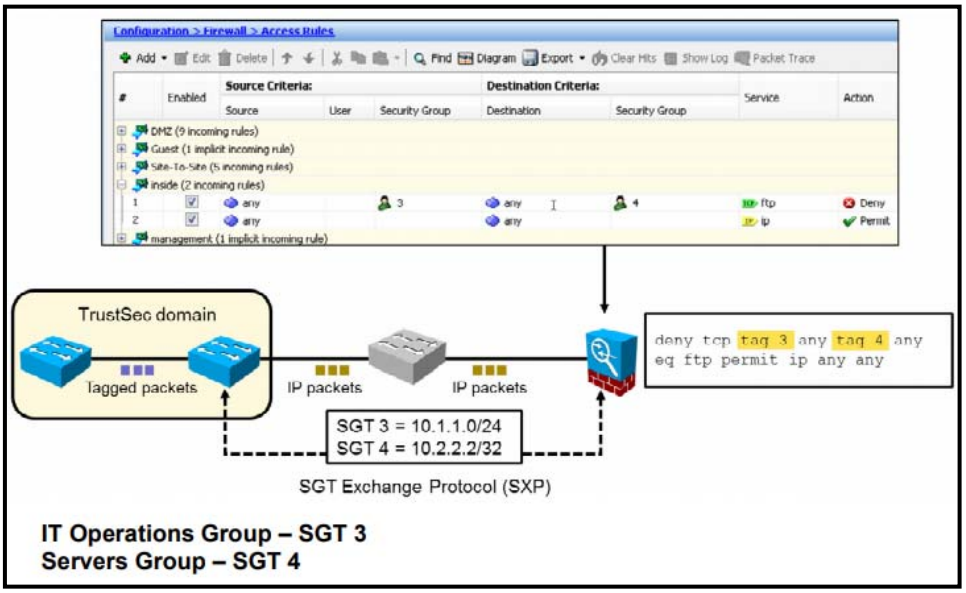

Рис. 3. Использование брэндмауэра группы безопасность

Политика безопасности ASA настраивается с помощью списков ACL. Можно создавать списки управления доступом в ASA, содержащие SGT или имена групп безопасности. ASA будет применять политики на основе SGT-групп безопасности, если ASA имеет таблицу групп безопасности для сопоставления имен групп безопасности SGT и, если существует сопоставление SGT с IP.

MACsec 802.1AE

IEEE 802.1AE MACsec предназначена для осуществления безопасности в проводной сети *Ethernet* от таких атак, как пассивная переадресация, «перехват сообщения во время передачи» и некоторые атаки типа «отказ в обслуживании».

MACsec помогает обеспечить непрерывные сетевые операции путем идентификации несанкционированных станций в локальной сети и предотвращения связи с ними. Он защищает протоколы управления и другие данные с помощью криптографических методов, которые аутентифицируют начало данных, защищают целостность сообщений и обеспечивают защиту и конфиденциальность воспроизведения.

Для стандарта 802.1AE требуются протоколы для управления ключами, аутентификацией и авторизацией. Для реализации этого, Институт инженеров электротехники и электроники предложил дополнительный стандарт 802.1af MAC Key Agreement (802.1X-2010/MKA). Расширение 802.1X, которое управляет сеансовыми ключами, короткого времени действия, которые используются для кодирования и декодирования сообщений. Стандарт 802.1X-2010/MKA поддерживает политику безопасности для каждого устройства с общей средой.

MACsec – это алгоритм шифрования и целостности уровня 2, основанный на 128-битном шифровом ключе стандарта шифрования AES-GCM. Коммутаторы

Cisco, которые поддерживают MACsec, используют специализированную интегральную схему (ASIC) для обеспечения шифрования и дешифрования в режиме реального времени и обеспечивают защиту воспроизведения для каждого кадра. Стандарт MACsec предлагает шифрование полезной нагрузки кадра, метаданных Cisco, которые содержат SGT, и заголовок 802.1Q [6].

Когда кадр поступает на станцию MACsec, объект безопасности MACsec дешифрует его, если необходимо, вычисляет ICV в кадре и сравнивает его с ICV, включенным в кадр. Если они совпадают, станция обрабатывает кадр как обычно. Если они не совпадают, порт обрабатывает кадр в соответствии с заданной политикой, например, отбрасывая его.

Политика MACsec нисходящей линии настроена как элемент профиля авторизации в Cisco ISE. Чтобы указать политику MACsec для конечных точек, необходимо включить политику MACsec, а затем выбрать параметр политики (*must-not-secure, must-secure,* и *should-secure*). Это заполняет значение атрибута *linksec-policy*, пару Cisco AV (атрибут-значение), отправленную на устройство доступа к сети, как часть сообщения о доступе к RADIUS (*Remote Authentication Dial-In User Service* – Служба удаленного доступа к удаленной аутентификации).

Политика MACsec, определенная в ISE, будет взаимодействовать с установленными политиками и возможностями как NAD, так и с тем, кто производит запрос. Например, если политика ISE must-secure, и либо запрашивающий, либо коммутатор не способны работать с MACsec, тогда доступ будет отклонен. При работе опции Should-secure трафик будет защищен, если все компоненты будут настроены для работы с MACSec, но позволят обеспечить незащищенный доступ, если компонент не поддерживает MACsec или если работает опции must-not-secure.

Чтобы включить MACsec на адресе нисходящей линии связи в диспетчере сетевого доступа Cisco AnyConnect, необходимо создать профиль и настроить его на использование MKA (*MACsec Key Agreement)* в качестве метода управления ключами и установить алгоритм шифрования для MACsec: AES-GCM-128.

На рис. 4 показана конфигурация функции MACsec на порту коммутатора. Помимо включения MACsec, необходимо включить политику MKA с помощью команды mka. Команда *authentication* linksec policy позволяет выбрать один из трех вариантов: must-secure, must-not-secure и must-secure. По умолчанию включена опция should-secure.

```
HQ-Sw(config)#
interface GigabitEthernet0/1
macsec
mka default-policy
authentication linksec policy should-secure
```

Рис. 4. Настройка MACsec на коммутаторе

Команда show authentication sessions interface может использоваться для проверки политики MACsec, которая была согласована для порта коммутатора, а также текущего состояния MACsec на порту [4, 5]. Можно дополнительно изучить криптографические данные, используя команду show macsec interface (рис. 5).

```
HQ-Sw# show authentication sessions interface gigabitEthernet 0/1
            ...
            User-Name:  it1
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Secured
       Oper host mode:  single-host
<output omitted>
```

```
HQ-Sw# show macsec interface gigabitEthernet 0/1
 MACsec is enabled
  Replay protect : enabled
  Replay window : 0
  Include SCI : yes
  Cipher : GCM-AES-128
  Confidentiality Offset : 0
 Capabilities
  Max. Rx SA : 16
  Max. Tx SA : 16
  Validate Frames : strict
  PN threshold notification support : Yes
  Ciphers supported : GCM-AES-128
 <output omitted>
```

Рис. 5. Проверка настроек MACsec

Заключение

Обобщая вышесказанное, можно выделить основные моменты работы TrustSec. Они заключаются в следующем:

1. Cisco TrustSec включает SGT и MACsec.

2. В SGA управление доступом упрощается благодаря использованию ACL групп безопасности (SGACL), которые определяют разрешенные службы. Местоположение источника и получателя динамически добавляются в виде тэгов в заголовок кадра.

3. MACsec помогает обеспечить непрерывные сетевые операции путем идентификации несанкционированных станций в локальной сети и предотвращения связи с ними. Он защищает протоколы управления и другие данные с помощью криптографических методов, которые аутентифицируют начало данных, защищают целостность сообщений и обеспечивают защиту и конфиденциальность воспроизведения.

4. Cisco TrustSec – протокол безопасности нового поколения, однако и он мог бы быть лучше, если бы он перенял некоторые плюсы от других протоколов, таких как IPSec, AAA и др. Однако и без этого данный протокол широко используется многими известными компаниями и еще долго прослужит им для защиты корпоративных сетей.

Литература

1. Ковалев Д. TrustSec на защите корпоративных сетей // Век качества. 2010. № 4. С. 44–45.

2. Десницкий В. А., Котенко И. В. Проектирование защищенных встроенных устройств на основе конфигурирования // Проблемы информационной безопасности. Компьютерные системы. 2013. № 1. С. 44–54.

3. Орлов С. Шлюзы безопасности: Новая волна // Журнал сетевых решений/LAN. 2010. № 9. С. 50–57.

4. Красов А. В., Левин М. В., Штеренберг С. И., Исаченков П. А. Модель управления потоками трафика в программно-определяемой сети с изменяющейся нагрузкой // Наукоемкие технологии в космических исследованиях Земли. 2016. Т. 8. № 4. С. 70–74.

5. Красов А. В., Левин М. В., Штеренберг С. И., Исаченков П. А. Методология управления потоками трафика в программно-определяемой адаптивной сети // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2016. № 4. С. 3–8.

6. Красов А. В., Левин М. В. Возможности управления трафиком в рамках концепции SDN // Актуальные проблемы инфотелекоммуникаций в науке и образовании. IV Международная научно-техническая и научно-методическая конференция. 2015. С. 350–354.

7. Красов А. В., Верещагин А. С., Цветков А. Ю. Аутентификация программного обеспечения при помощи вложения цифровых водяных знаков в исполняемый код // Телекоммуникации. 2013. № S7. С. 27–29.

8. Василишин Н. С., Ушаков И. А., Котенко И. В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // 9-я конференции по проблемам управления «Информационные технологии в управлении» (ИТУ). 2016. С. 670–675.

9. Кузьмин Н. Н., Красов А. В., Ушаков И. А. Разработка инструментария верификации процесса проектирования УМК на основе лингвистического подхода // Известия СПбГЭТУ ЛЭТИ. 2013. № 3. С. 26–32.

10. Красов А. В., Ушаков И. А. Подготовка специалистов в области информационной безопасности в Санкт-Петербургском государственном университете телекоммуникаций им. проф. М. А. Бонч-Бруевича // Инновации. 2013. № 7 (177). С. 92–97.

11. Десницкий В. А., Котенко И. В. Модель защиты программного обеспечения на основе механизма «удаленного доверия» // Известия высших учебных заведений. Приборостроение. 2008. Т. 51. № 11. С. 26–31.

12. Десницкий В. А., Котенко И. В., Чечулин А. А. Конфигурирование защищенных систем со встроенными и мобильными устройствами // Вопросы защиты информации. 2012. № 2. С. 20–28.

References

1. Kovalev D. TrustSec on the protection of corporate networks // Vek kachestva. 2010. No. 4. pp. 44–45.

2. Desnitsky V., Kotenko I. Configuration Based Design of Secure Embedded Devices // Information Security Problems. Computer Systems. 2013. Iss. 1. pp. 44–54.

3. Orlov S. Security Gateways: A New Wave // Network Solutions Journal/LAN. 2010. Iss. 9. pp. 50–57.

4. Krasov A., Levin M., Shterenberg S., Isachenkov P. Traffic Flow Management Model in Software-Defined Networks with Unequal Load Metric // H&ES Research. 2016. Vol. 8. Iss. 4. pp. 70–74.

5. Krasov A., Levin M., Shterenberg S., Isachenkov P. Methodology Research on the Efficiency of the Traffic Flow Management Method based on the Information about the Load of Software-Defined Networks with Unequal Route Metric // Vestnik of St. Petersburg State University of Technology and Design. Series 1. Natural and technical science. 2016. Iss. 4. pp. 3–8.

6. Krasov A., Levin M. The possibility of traffic management within the SDN concept // Actual Problems of Education in Science and Education. IV International Scientific-Technical and Scientific-Methodical Conference. 2015. pp. 350–354.

7. Krasov A., Vereschagin A., Tsevtkov A. Software Authentication with Digital Watermarks in Executable Code // Telekommunikatsii. 2013. S7. pp. 27–29.

8. Vasilishin N., Ushakov I., Kotenko I. Investigation of Algorithms for Analyzing Network Traffic using Large Data Technologies for Detecting Computer Attacks // 9 Conference on Management Problems «Information Technologies in Management» (ITM). 2016. pp. 670–675.

9. Kuzmin N., Krasov A., Ushakov I. Development of Toolkit for Verification of TMK Designing Process on the Linguistic Approach Basis // Proceedings of Saint Petersburg Electrotechnical University. 2013. Iss. 3. pp. 26–32.

10. Krasov A., Ushakov I. Future Experts' Preparation in the Field of Information Security at the Bonch-Bruevich Saint-Petersburg State University of Telecommunications // Innovatsii. 2013. Iss. 7 (177). pp. 92–97.

11. Desnitskiy V., Kotenko I. Software Protection Model Based on Remote Entrusting Mechanism // Izvestiya vysshikh uchebnykh zavedeniy. Priborostroenie. 2008. Vol. 51. Iss. 11. pp. 26–31.

12. Desnitskiy V., Kotenko I., Chechulin A. Configuration of Secure Systems with Embedded and Mobile Devices // Voprosy zaschity informacii. 2012. Iss 2. pp. 20–28.

Катасонов Александр Игоревич – студент, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, ksasha716@yandex.ru

Цветков Александр Юрьевич – старший преподаватель, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, alexander.tsvetkov89@gmail.com

Андрианов Владимир Игоревич – кандидат технических наук, доцент, СПбГУТ, Санкт-Петербург, 193232, Российская Федерация, vladimir.i.andrianov@gmail.com

Katasonov Alexandr – Student, SPbSUT, St. Petersburg, 193232, Russian Federation, ksasha716@yandex.ru

Tsvetkov Alexandr – Senior Lecturer, SPbSUT, St. Petersburg, 193232, Russian Federation, alexander.tsvetkov89@gmail.com

Andrianov Vladimir – Candidate of Engineering Sciences, Associate Professor, SPbSUT, St. Petersburg, 193232, Russian Federation, vladimir.i.andrianov@gmail.com