Международный союз электросвязи

МСЭ-Т

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

X.1042

(01/2019)

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность информации и сетей –
Безопасность сетей

Службы безопасности, использующие сети с программируемыми параметрами

Рекомендация МСЭ-Т X.1042

Международный союз электросвязи

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	**X.1030–X.1049**
Управление безопасностью	X.1050–X.1069
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность "умных" электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1360–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1389
Безопасность технологии распределенного реестра	X.1400–X.1429
Безопасность технологии распределенного реестра	X.1430–X.1449
Протоколы безопасности (2)	X.1450–X.1459
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

Рекомендация МСЭ-Т X.1042

Службы безопасности, использующие сети с программируемыми параметрами

Резюме

Рекомендация МСЭ-Т X.1042 касается защиты ресурсов сети с использованием служб безопасности на основе сетей с программируемыми параметрами (SDN). В настоящей Рекомендации сетевые ресурсы служб безопасности на основе SDN сначала классифицируются по следующим категориям: SDN-приложение, SDN-контроллер, SDN-коммутатор и диспетчер безопасности (SM). Затем в Рекомендации МСЭ-Т X.1042 дается определение конкретных служб безопасности на основе SDN.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1042	30.01.2019 года	17-я	11.1002/1000/13803

Ключевые слова

Управление доступом, DDoS-атака, межсетевой экран, ловушка, сети с программируемыми параметрами (SDN), сценарии обеспечения безопасности

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL: http://handle.itu.int/, после которого следует уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу http://www.itu.int/ITU-T/ipr/.

Содержание

Рекомендация МСЭ-Т X.1042

Службы безопасности, использующие сети с программируемыми параметрами

1 Сфера применения

Настоящая Рекомендация касается защиты сетевых ресурсов с использованием служб безопасности на основе сетей с программируемыми параметрами (SDN). Настоящая Рекомендация охватывает следующие вопросы:

– классификация сетевых ресурсов, которые могут быть защищены службами безопасности на основе SDN;

– определение служб безопасности на основе SDN;

– описание способов реализации служб безопасности на основе SDN.

Защита сетевых ресурсов (например, маршрутизаторов, коммутаторов, межсетевых экранов, систем обнаружения вторжений) с помощью служб безопасности на основе SDN предусматривает следующее:

– быстрая реакция на новые сетевые атаки [например, черви и распределенные атаки типа отказ в обслуживании (DDoS-атаки)];

– создание частных сетей для отражения изощренных сетевых атак;

– автоматическая защита от сетевых атак без вмешательства администраторов сети;

– динамическое распределение ресурсов в зависимости от нагрузки на сеть.

2 Справочные документы

Указанные ниже Рекомендации МСЭ-Т и другие источники содержат положения, которые путем ссылки на них в данном тексте составляют положения настоящей Рекомендации. На момент публикации указанные издания были действующими. Все Рекомендации и другие источники могут подвергаться пересмотру; поэтому пользователям данной Рекомендации предлагается изучить возможность применения последнего издания Рекомендаций и других источников, перечисленных ниже. Список действующих в настоящее время Рекомендаций МСЭ-Т регулярно публикуется. Ссылка на документ, приведенный в настоящей Рекомендации, не придает ему как отдельному документу статуса Рекомендации.

[ITU-T Y.3300] Recommendation ITU-T Y.3300 (2014), *Framework of software-defined networking*

[ITU-T Y.3301] Recommendation ITU-T Y.3301 (2016), *Functional requirements of software-defined networking*

[ITU-T Y.3302] Recommendation ITU-T Y.3302 (2017), *Functional architecture of software-defined networking*

3 Определения

3.1 Термины, определенные в других документах

В настоящей Рекомендации используются следующие термины, определенные в других документах.

3.1.1 сети с программируемыми параметрами (software-defined networking) [ITU-T Y.3300]: набор методов, который позволяет напрямую программировать, организовывать, контролировать сетевые ресурсы и управлять ими, что облегчает проектирование, доставку и эксплуатацию сетевых служб динамичным и масштабируемым образом.

3.1.2 управление доступом; контроль доступа (access control) [b-ITU-T X.1252]: процедура, применяемая для определения того, следует ли предоставлять тому или иному объекту доступ к ресурсам, устройствам, услугам или информации, на основе заранее установленных правил и конкретных прав или полномочий, связанных с запрашивающей стороной.

3.1.3 политика управления доступом (access control policy) [b-ITU-T X.812]: набор правил, определяющих условия, при которых возможен доступ.

3.1.4 правила политики управления доступом (access control policy rules) [b-ITU-T X.812]: правила политики безопасности, относящиеся к предоставлению услуги управления доступом.

3.2 Термины, определенные в настоящей Рекомендации

В настоящей Рекомендации дается определение следующим терминам.

3.2.1 сетевой ресурс (network resource): устройство, выполняющее пересылку пакетов в сетевой системе.

ПРИМЕЧАНИЕ. – К сетевым ресурсам относятся сетевые коммутаторы, маршрутизаторы, шлюзы и точки доступа Wi-Fi.

3.2.2 межсетевой экран (firewall): устройство или служба на стыке двух сегментов сети, проверяющие каждый пакет при попытке пересечь границу. Межсетевой экран не пропускает пакеты, которые бракуются по определенным критериям, таким как наличие запрещенных номеров порта или IP-адресов.

ПРИМЕЧАНИЕ. – Службы межсетевого экрана могут быть отделены от физических устройств и работать как приложение.

3.2.3 ловушка (honeypot): механизм компьютерной безопасности, предназначенный для приманки лиц, совершающих кибератаки. Используется для обнаружения или отражения атак от законной цели и сбора информации об атаках. Термин "ловушка" (буквально – горшок с медом. – *Прим. перевод.*) объясняется образом действия этого устройства, которое привлекает злоумышленников ("пчел") к определенному месту (объекту атаки, или "меду"), то есть используется как западня.

3.2.4 централизованная служба межсетевых экранов (centralized firewall service): служба, способная устанавливать и распространять правила политики управления доступом среди сетевых ресурсов для эффективного управления межсетевыми экранами. Этими правилами можно управлять динамически из центрального сервера. Сети с программируемыми параметрами (SDN) могут работать как централизованная служба межсетевых экранов через стандартный интерфейс между приложениями межсетевого экрана и сетевыми ресурсами.

3.2.5 централизованная служба отражения DDoS-атак (centralized DDoS-attack mitigation service): служба, способная создавать и распространять правила политики управления доступом среди сетевых ресурсов для эффективного отражения распределенных атак типа отказ в обслуживании (DDoS-атак). Этими правилами можно управлять динамически из центрального сервера. Сеть с программируемыми параметрами (SDN) может работать как централизованная служба отражения DDoS-атак через стандартный интерфейс между приложениями по отражению DDoS-атак и сетевыми ресурсами.

3.2.6 централизованная служба ловушек (centralized honeypot service): служба, способная создавать и распространять правила политики управления доступом среди сетевых ресурсов для динамической конфигурации ловушек. Этими правилами можно управлять динамически из центрального сервера. Сети с программируемыми параметрами (SDN) могут работать как централизованная служба ловушек через стандартный интерфейс между приложениями ловушек и сетевыми ресурсами.

3.2.7 централизованная служба управления несанкционированными устройствами (centralized illegal device management service): служба, способная создавать и распространять правила политики управления доступом среди сетевых ресурсов для ведения черного списка несанкционированных устройств. Этими правилами можно управлять динамически и глобально из центрального сервера. Сети с программируемыми параметрами (SDN) могут действовать в качестве сетевой среды управления несанкционированными устройствами через стандартный интерфейс между приложениями управления несанкционированными устройствами и сетевыми ресурсами.

ПРИМЕЧАНИЕ. – Критерий определения несанкционированных устройств выходит за рамки сферы действия настоящей Рекомендации. Примером способа выявления несанкционированных устройств может служить использование глобальной системы уникальных идентификаторов.

3.2.8 служба управления контролем доступа (access control management service): служба, способная устанавливать и распространять политику прав доступа среди сетевых ресурсов для белого списка устройств интернета вещей (IoT). Этой политикой можно управлять динамически и глобально из центрального сервера. Сети с программируемыми параметрами (SDN) могут действовать в качестве сетевой среды управления устройствами IoT через стандартный интерфейс между приложениями управления контролем доступа и сетевыми ресурсами.

ПРИМЕЧАНИЕ. – Спецификация иерархического состава политики доступа выходит за рамки сферы применения настоящей Рекомендации. Эта политика доступа может компоноваться и разделяться в соответствии с уровнем безопасности сетевых ресурсов и распределяться по сетевой системе.

4 Сокращения и акронимы

В настоящей Рекомендации используются следующие сокращения и акронимы.

ACI	Application Control Interface	Интерфейс управления приложениями
ACM	Access Control Management	Управление контролем доступа
AL-MSO	Application Layer Management Support and Orchestration	Поддержка и организация управления прикладным уровнем
ALM	Application Layer Management	Управление прикладным уровнем
BSS	Business Support System	Система поддержки деятельности предприятия
CL-AS	Control Layer Application Support	Поддержка приложений уровня управления
CL-CLS	Control Layer Control Layer Service	Служба управления уровнем управления
CL-MSO	Control Layer Management Support and Orchestration	Поддержка и организация управления уровнем управления
CL-RA	Control Layer Resource Abstraction	Абстрагирование ресурсов уровня управления
CLM	Control Layer Management	Управление уровнем управления
DDoS	Distributed Denial-of-Service	Распределенная атака типа отказ в обслуживании (DDoS-атака)
DNS	Domain Name Service	Служба наименований доменов
DPI	Deep Packet Inspection	Углубленная проверка пакетов
I2NSF	Interface to Network Security Function	Интерфейс к функции защиты сети
IoT	Internet of Things	Интернет вещей
IP	Internet Protocol	Протокол Интернет
MAC	Media Access Control	Управление доступом к среде передачи
MMF	Multi-layer Management Function	Функция управления многоуровневой структурой
MMFA	Multi-layer Management Function Application layer	Прикладной уровень функции управления многоуровневой структурой
MMFC	Multi-layer Management Function Control layer	Уровень управления функции управления многоуровневой структурой
MMFO	Multi-layer Management Function OSS/BSS	Функция управления многоуровневой структурой OSS/BSS
MMFR	Multi-layer Management Function Resource layer	Уровень ресурсов функции управления многоуровневой структурой

NSF	Network Security Function	Функция защиты сети
OSS	Operation Support System	Система эксплуатационной поддержки
RCI	Resource Control Interface	Интерфейс управления ресурсами
RLM	Resource Layer Management	Управление уровнем ресурсов
RL-MS	Resource Layer Management Support	Поддержка управления уровнем ресурсов
SDN	Software-Defined Networking	Сеть с программируемыми параметрами
SDN-AL	Software-Defined Networking – Application Layer	Прикладной уровень сети с программируемыми параметрами
SDN-CL	Software-Defined Networking – Control Layer	Уровень управления сети с программируемыми параметрами
SDN-RL	Software-Defined Networking – Resource Layer	Уровень ресурсов сети с программируемыми параметрами
SIP	Session Initiation Protocol	Протокол инициации сеанса
SM	Security Manager	Диспетчер безопасности
TCP	Transmission Control Protocol	Протокол управления передачей
VoIP	Voice over Internet Protocol	Передача голоса по протоколу Интернет
VoLTE	Voice over Long-Term Evolution	Передача голоса по технологии долгосрочного развития

5 Соглашения по терминологии

В настоящей Рекомендации:

ключевые слова "требуется, чтобы" означают требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации;

ключевое слово "рекомендуется" означает требование, которое рекомендуется, но не является абсолютно необходимым, таким образом для заявления о соответствии настоящей Рекомендации это требование не является обязательным;

ключевое слово "запрещается" означает требование, которому необходимо неукоснительно следовать и отклонение от которого не допускается, если будет сделано заявление о соответствии настоящей Рекомендации;

ключевые слова "может факультативно " означают необязательное требование, которое допустимо, но не имеет рекомендательного значения. Данный термин не подразумевает, что вариант реализации поставщика должен обеспечивать выполнение этой функции и функция может быть активирована по желанию оператора сети/поставщика услуг дополнительно. Это означает лишь, что поставщик может факультативно предоставить эту функцию и по-прежнему заявлять о соответствии настоящей Рекомендации.

6 Обзор функциональной архитектуры SDN

В этом разделе описана эталонная высокоуровневая архитектура служб безопасности (например, межсетевой экран, отражение DDoS-атак) с использованием высокоуровневой архитектуры SDN, описанной в [ITU-T Y.3300], такой как централизованная служба межсетевого экрана и централизованная служба отражения DDoS-атак.

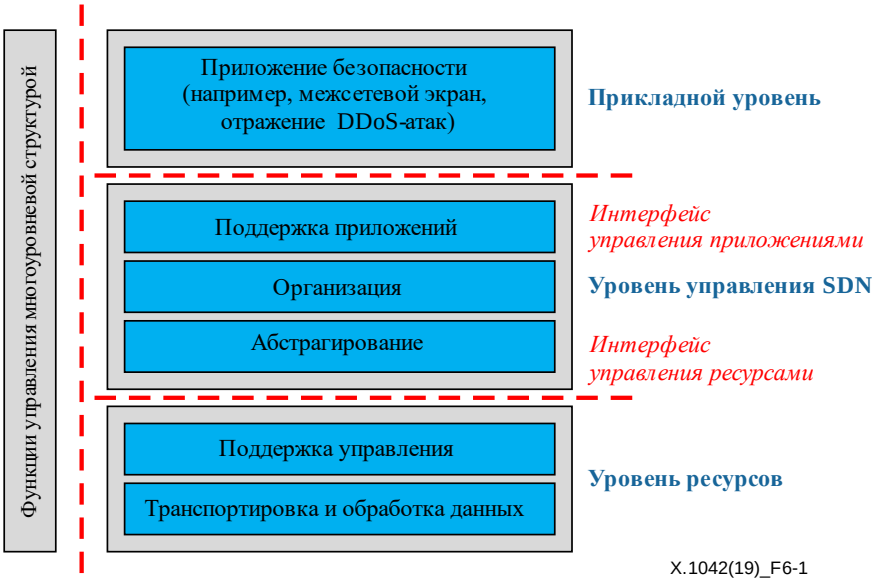

Рисунок 6-1 – Высокоуровневая архитектура служб безопасности на основе SDN

Как показано на рисунке 6-1, приложения для служб безопасности (например, межсетевой экран, отражение DDoS-атак и ловушки) расположены поверх архитектуры SDN. Когда пользователь или администратор (например, управляющий прикладным уровнем (ALM), как показано на рисунке 6-2) применяет политику безопасности к службам безопасности через интерфейс приложений, контроллер SDN автономно и оперативно генерирует соответствующие правила доступа для обеспечения соблюдения такой политики безопасности. Согласно сгенерированным правилам доступа сетевые ресурсы, такие как коммутаторы SDN, принимают меры для отражения сетевых атак, например удаляя пакеты с подозрительной структурой.

На рисунке 6-2 показана описанная в [ITU-T Y.3302] функциональная архитектура SDN, основанная на высокоуровневой архитектуре SDN.

– Прикладной уровень сети с программируемыми параметрами (SDN-AL). SDN-AL состоит из функционального компонента поддержки и организации ALM (AL-MSO) и нескольких прикладных функциональных компонентов SDN [ITU-T Y.3302]. AL-MSO взаимодействует с функциональным компонентом ALM в составе функции управления многоуровневой структурой (MMF) с помощью контрольной точки прикладного уровня функции управления многоуровневой структурой (MMFA) для поддержки управления приложениями SDN и обеспечения возможности совместных операций управления на всех подуровнях SDN. Приложения SDN взаимодействуют с уровнем управления сети с программируемыми параметрами (SDN-CL) через контрольную точку интерфейса управления приложениями (ACI) с помощью запросов SDN-CL для автоматической настройки поведения и свойств сетевых ресурсов. Приложения SDN используют абстрагированное представление и статус сетевых ресурсов, предоставляемые SDN-CL посредством моделей информации и данных, предоставляемых через контрольную точку ACI. В зависимости от вариантов использования SDN (например, внутри центров обработки данных, подвижных сетей, сетей доступа или между ними) могут быть дополнительно определены разные ACI. Предполагается, что ACI используют открытые интерфейсы прикладного программирования.

– SDN-CL. SDN-CL состоит из службы поддержки и организации управления уровнем управления (CL-MSO), службы поддержки приложений уровня управления (CL-AS), службы управления уровнем управления (CL-CLS) и службы абстрагирования ресурсов уровня управления (CL-RA). SDN-CL предоставляет программируемые средства управления поведением ресурсов SDN (например, ресурсов для транспортировки и обработки данных) в соответствии с запросами SDN-AL и политикой MMF. SDN-CL работает на ресурсах, предоставляемых уровнем ресурсов сети с программируемыми параметрами (SDN-RL), и обеспечивает абстрагированное представление сети для SDN-AL. SDN-CL взаимодействует с SDN-RL с использованием контрольной точки интерфейса управления ресурсами (RCI)

и с функциональным компонентом управления уровнем управления (CLM) в MMF с использованием контрольной точки уровня управления функции управления многоуровневой структурой (MMFC). Он также взаимодействует с SDN-AL через контрольную точку ACI. CL-MSO может запросить у MMF делегирование некоторых функций управления. MMF предоставляют средства для управления функциональными возможностями SDN-CL через контрольную точку MMFC.

– SDN-RL. SDN-RL состоит из служб поддержки управления уровнем ресурсов (RL-MS), поддержки контроля уровня ресурсов, обработки данных уровня ресурсов и передачи данных уровня ресурсов. SDN-RL – это уровень, на котором элементы физической или виртуальной сети осуществляют передачу или обработку пакетов данных в соответствии с решениями SDN-CL. Обмен информацией, относящейся к созданию политики (включая информацию о конфигурации), которая возникает в результате принятия решений SDN-CL, а также информацией о сетевых ресурсах осуществляется через контрольную точку RCI. К информации, передаваемой через RCI, относится информация управления, которую SDN-CL предоставляет SDN-RL (например, для настройки сетевых ресурсов или предоставления политики), а также информация, относящаяся к уведомлениям, отправляемым SDN-RL всякий раз, когда обнаруживается изменение сетевых ресурсов (если такая информация имеется). RL-MS предоставляет описание ресурсов, то есть поставщика, версии программного обеспечения и их статуса (например, загрузку центрального процессора, используемый объем оперативной или постоянной памяти). RL-MS может включать агента управления, выполняющего некоторые локальные операции управления, делегированные MMF. MMF предоставляет средства для управления функциональными возможностями SDN-RL через контрольную точку уровня ресурсов функции управления многоуровневой структурой (MMFR).

BSS – система поддержки деятельности предприятия; MMFO – функция управления многоуровневой структурой OSS/BSS; OSS – система эксплуатационной поддержки

Рисунок 6-2 – Функциональная архитектура SDN [ITU-T Y.3302]

7 Классификация сетевых ресурсов

В этом разделе определяются четыре вида сетевых ресурсов для служб безопасности с использованием SDN, как показано на рисунке 6-2.

1) SDN-приложение – служба, которая явным, прямым и программируемым способом передает контроллеру SDN свои требования к сетевым ресурсам и желаемому поведению сети через

интерфейс в восходящем направлении, такой как ACI, показанный на рисунке 6-2. Кроме того, SDN-приложение может использовать абстрагированное представление сети для своих внутренних целей, связанных с принятием решений. Например, в качестве приложений могут выступать службы межсетевого экрана, ловушки, службы отражения DDoS-атак и службы управления несанкционированными устройствами. Эти SDN-приложения должны взаимодействовать с ALM через AL-MSO для управления отказами, конфигурацией, учетом, быстродействием и безопасностью. Поскольку эти приложения создают правила доступа, они также должны взаимодействовать с SDN-CL через ACI для реализации правил доступа.

2) Контроллер SDN – логически централизованный объект, отвечающий: за i) передачу требований из SDN-приложений в коммутаторы SDN; и ii) передачу приложениям абстрактных представлений сети с полезной информацией о сети, такой как статистика трафика и события. Другими словами, контроллер SDN создает записи управления потоком на основе правил доступа, получаемых от SDN-приложений. Таким образом контроллер SDN должен взаимодействовать с CLM, SDN-приложениями и SDN-RL.

3) Коммутатор SDN – программа или устройство, которые пересылают пакеты в среде SDN. Коммутаторы SDN могут хранить правила пересылки пакетов, которыми управляет контроллер SDN через нисходящий интерфейс, такой как RCI, показанный на рисунке 6-2. Таким образом коммутатор SDN должен взаимодействовать со средствами управления уровнем ресурсов (RLM) и SDN-CL.

4) Диспетчер безопасности (SM) – функция ALM, которая передает политику безопасности в SDN-приложение. Таким образом SM должен взаимодействовать с SDN-приложениями через AL-MSO. На рисунке 7-1 показано размещение сетевых ресурсов, представленных на рисунке 6-2. Эти сетевые ресурсы должны соответствовать требованиям [ITU Y.3301].

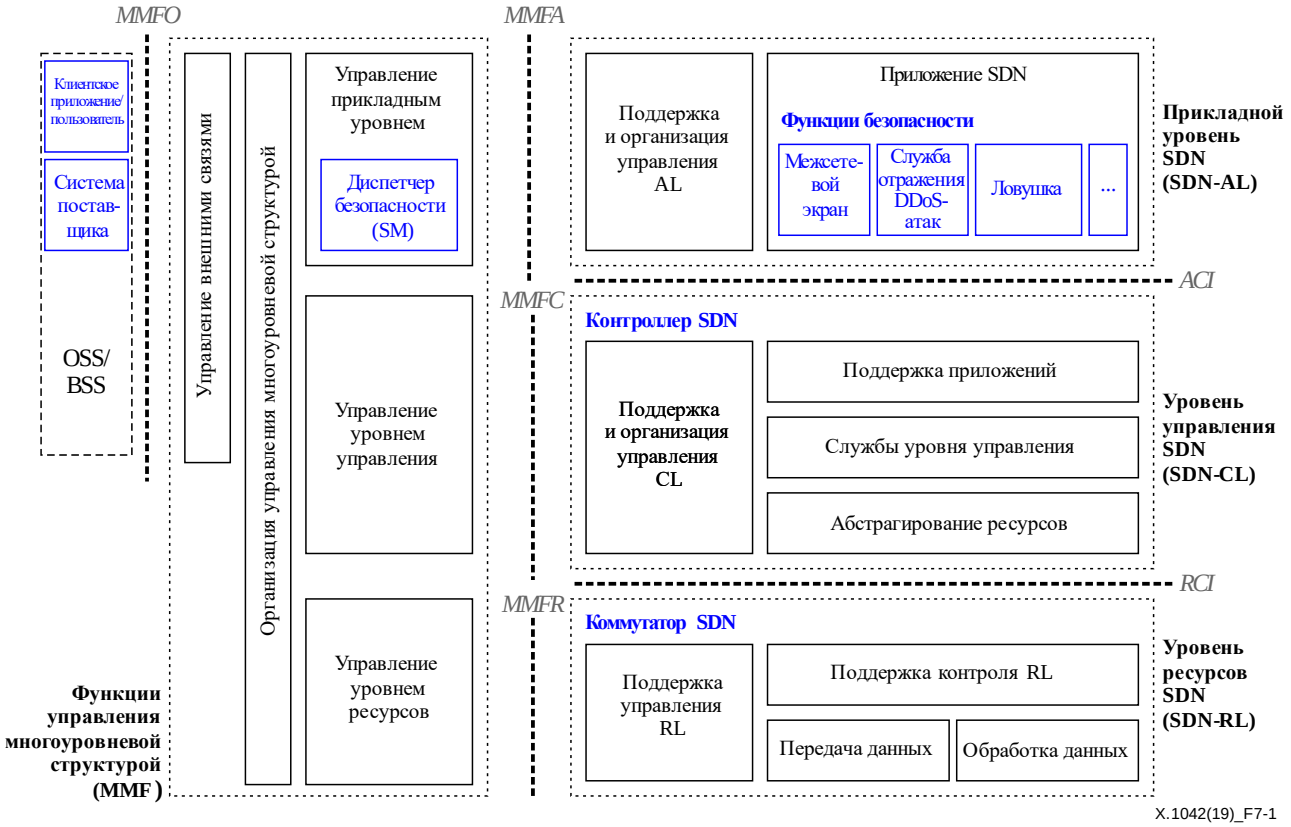

Рисунок 7-1 – Сетевые ресурсы служб безопасности на основе SDN

8 Службы безопасности на основе SDN

В этом разделе представлены службы безопасности, использующие SDN, в двух типах сетей: i) внутридоменные сети, в которых функционируют, например, централизованная служба межсетевого экрана и централизованная служба ловушек; и ii) междоменные сети, в которых функционируют,

например, централизованная служба отражения DDoS-атак и централизованная служба управления несанкционированными устройствами. Под доменом в настоящей Рекомендации понимается группа сетевых ресурсов, которые администрируются в соответствии с общими правилами и процедурами.

8.1 Централизованная служба межсетевого экрана

8.1.1 Основная концепция централизованной службы межсетевого экрана

В этом разделе приводится описание основной концепции централизованной службы межсетевого экрана. Эта служба может управлять сетевыми ресурсами, позволяя гибко управлять правилами межсетевого экрана. Как показано на рисунке 8-1, центральный межсетевой экран управляет коммутаторами SDN, и в них могут быть добавлены новые правила или удалены ненужные.

ПРИМЕЧАНИЕ. – Стратегию фильтрации пакетов, создаваемую приложением межсетевого экрана, легко преобразовать в таблицу управления потоком посредством контроллера. Однако протокол связи между контроллером и коммутаторами (например, протоколы OpenFlow и NETCONF) в настоящее время может соответствовать только уровню протокола управления передачей (TCP) и не имеет поля для идентификационной информации пакетов данных выше уровня TCP. Поэтому невозможно реализовать стратегию идентификации информации выше уровня TCP в межсетевом экране без изменения протокола.

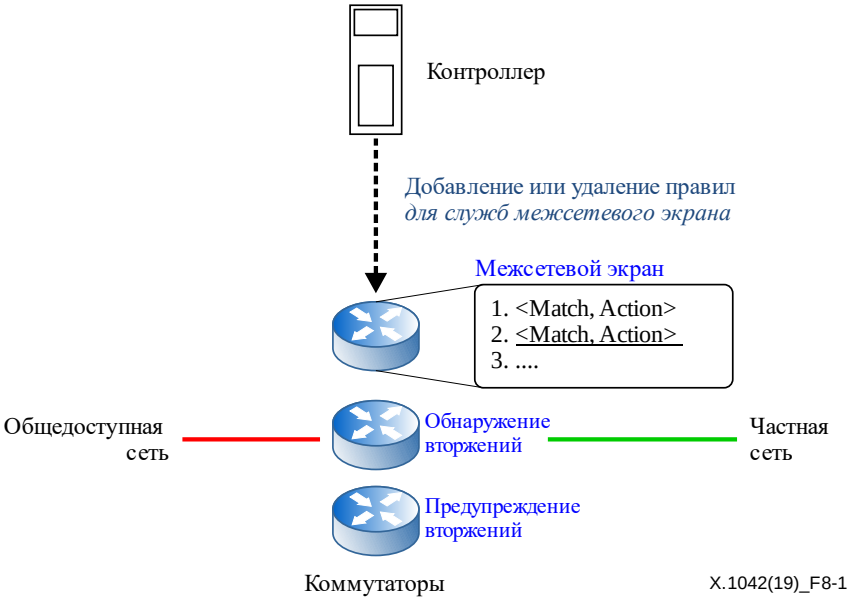

Рисунок 8-1 – Концепция централизованной службы межсетевого экрана

8.1.2 Сценарий централизованной службы межсетевого экрана

На рисунке 8-2 показан пример сценария централизованной службы межсетевого экрана для пресечения распространения червя.

В качестве предварительного условия для этого сценария требуется, чтобы при получении информации о новом черве SM определил новую политику для приложения межсетевого экрана. Для того чтобы предотвратить распространение пакетов с этим червем, пользователь может добавить в приложение межсетевого экрана, работающее поверх контроллера SDN, новую политику (например, удалять пакеты с файлом червя). Также можно организовать централизованное управление, чтобы SM мог определять политику безопасности для приложения межсетевого экрана из единого центра, то есть контроллера SDN.

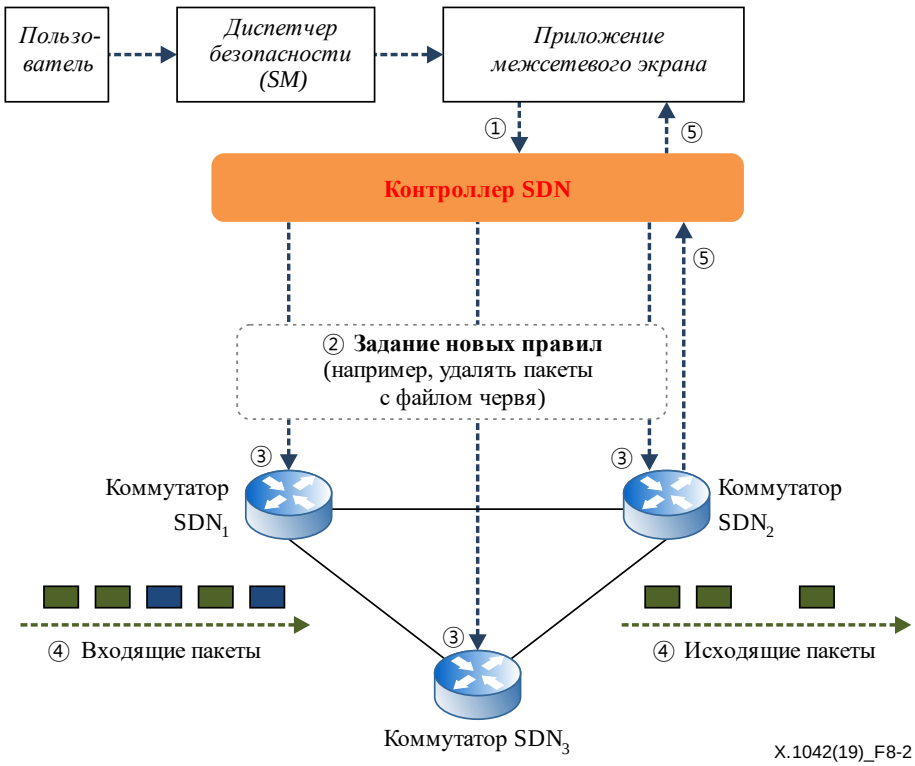

Рисунок 8-2 – Сценарий внутридоменной централизованной службы межсетевого экрана

– Шаг 1. Приложение межсетевого экрана устанавливает новые правила.

  Когда поступает информация о новом черве, приложение межсетевого экрана определяет новое правило. Новое правило (например, удалять пакеты с файлом червя) добавляется в контроллер SDN.

– Шаг 2. Контроллер SDN распространяет новую запись управления потоком во все коммутаторы SDN.

  Создав новую запись управления потоком, контроллер SDN может распространить ее в каждый коммутатор. Таким образом контроллер SDN передает во все коммутаторы SDN команду на добавление записи управления потоком, содержащей правило (например, удалять пакеты с файлом червя).

  Описанный в этом разделе новый червь может быть либо известным, либо вновь выявленным червем. Для известных червей в службе межсетевого экрана уже имеются механизмы обнаружения и защиты, например подписи или отпечатки пальцев. Новых же червей необходимо искать и выявлять, прежде чем применять какие-либо контрмеры для защиты от них. Черви несут в себе вредоносную нагрузку, которая может эксплуатировать уязвимые приложения или службы. Таких червей можно обнаружить путем проверки содержимого пакетов. Пример обнаружения сканирования данных пакетов приведен в Дополнении II.

– Шаг 3. Все коммутаторы SDN вносят новую запись управления потоком в свою таблицу управления потоком.

  Получив команду на добавление записи управления потоком об удалении последующих пакетов с файлом червя, коммутатор SDN добавляет в свою таблицу управления потоком соответствующую запись управления потоком. С этого момента коммутатор SDN будет удалять пакеты, содержащие файл червя.

– Шаг 4. Коммутатор SDN выполняет условия записи управления потоком, предписывающей удалять пакеты, содержащие файлы червя.

  Получая пакеты с файлом червя, коммутатор SDN удаляет их все без исключения. В соответствии с применяемыми правилами не передаются никакие пакеты, содержащие файлы червя.

– Шаг 5. Получив незнакомый пакет, коммутатор SDN сообщает об этом в контроллер.

Получив пакет нового типа, который он еще не обрабатывал, коммутатор SDN удаляет этот пакет и направляет в контроллер отчет о пакете этого типа. Контроллер проводит анализ и определяет, имеет ли место атака. Если это атака, контроллер отправляет сообщение в приложение межсетевого экрана и выполняется шаг 1. В противном случае контроллер сохраняет обычную запись управления потоком, чтобы сообщить коммутаторам, как обрабатывать эту последовательность в последующих пакетах.

8.1.3 Сценарий работы совмещенной службы межсетевого экрана

На рисунке 8-3 показан пример сценария работы приложения межсетевого экрана, совмещенного с приложением углубленной проверки пакетов (DPI) для обеспечения централизованного контроля и управления потоком передачи голоса по протоколу Интернет (VoIP)/передачи голоса по протоколу долгосрочного развития (VoLTE). Этот сценарий показывает, что приложение DPI контролирует каждый коммутатор SDN, управляя потоком вызовов VoIP/VoLTE при помощи правил, которые могут быть динамически добавлены, удалены или изменены. Для защиты службы VoIP/VoLTE это приложение может взаимодействовать с приложением межсетевого экрана. В частности, коммутатор с поддержкой межсетевого экрана выполняет основные проверки безопасности пакетов неизвестных потоков. Если коммутатор обнаруживает пакет неизвестного потока VoIP-вызовов с подозрительной структурой, он запускает контроллер SDN для проведения более специализированного анализа безопасности в отношении этого подозрительного пакета VoIP-вызова.

В качестве предварительного условия для этого сценария требуется, чтобы при распознавании информации о пакете с подозрительной структурой SM определял новую политику для приложения межсетевого экрана и DPI. Для того чтобы предотвратить включение этих структур в пакеты, пользователь добавляет в приложение межсетевого экрана и DPI, работающее поверх контроллера SDN, новую политику (например, удалять пакеты с подозрительной структурой). Также можно организовать централизованное управление, чтобы SM мог определять политику безопасности для приложений из единого центра, то есть контроллера SDN.

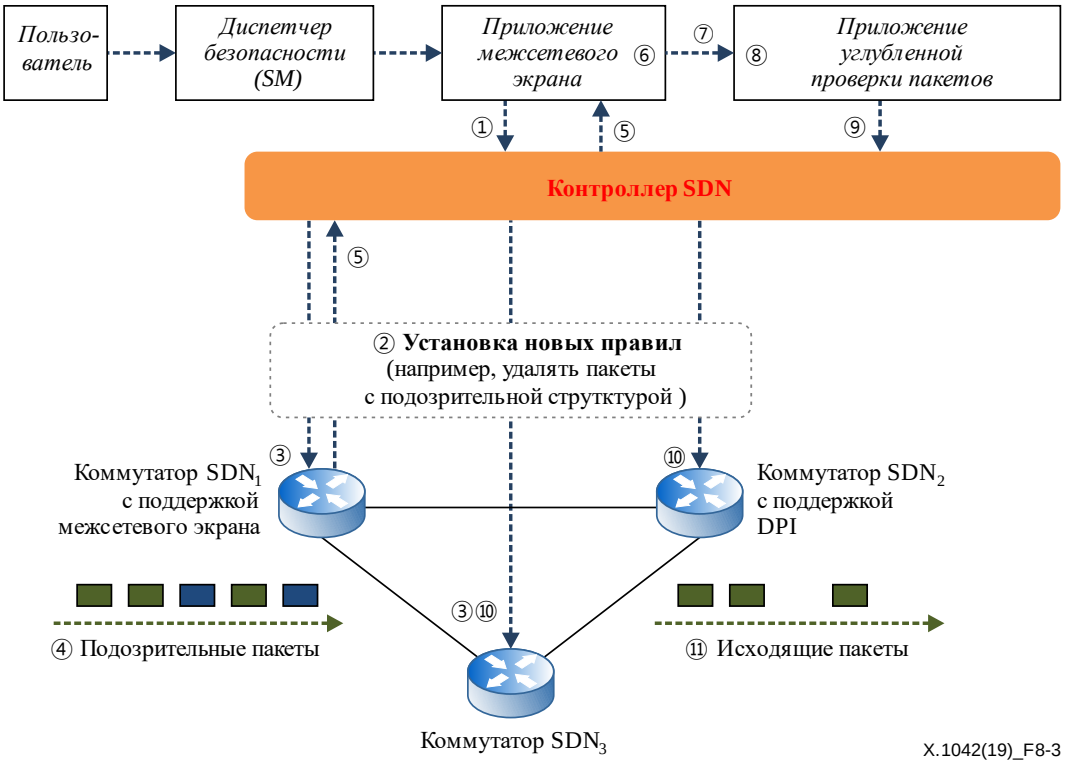

Рисунок 8-3 – Сценарий работы внутридоменной совмещенной службы межсетевого экрана

– Шаг 1. Приложения межсетевого экрана и DPI устанавливают новые правила для известной структуры пакетов.

  Когда поступает информация о новой структуре, приложения межсетевого экрана и DPI определяют новое правило. Это новое правило (например, доставлять пакеты с данной структурой в контроллер SDN) добавляется в контроллер SDN.

– Шаг 2. Контроллер SDN распространяет новую запись управления потоком во все коммутаторы SDN.

  Контроллер SDN может распространить новую запись управления потоком в каждый коммутатор. Таким образом контроллер SDN передает во все коммутаторы SDN команду на добавление записи управления потоком, содержащей правило (например, доставлять пакеты с данной структурой). Если каждый коммутатор имеет свои, отличные от других функции, то контроллер SDN передает в каждый из них разные записи управления потоком. Другими словами, коммутаторы с поддержкой межсетевого экрана не должны получать записи управления потоком, относящиеся к DPI.

– Шаг 3. Все коммутаторы SDN вносят новую запись управления потоком в свои таблицы управления потоком.

  Получив от контроллера SDN команду на добавление записи управления потоком, коммутатор SDN добавляет в свою таблицу управления потоком запись, относящуюся к доставке последующих пакетов с подозрительной структурой.

– Шаг 4. Коммутатор SDN выполняет правила управления потоком, относящиеся к доставке пакетов с подозрительной структурой.

  Коммутатор SDN доставляет полученные пакеты с подозрительной структурой в контроллер SDN. Все пакеты с подозрительной структурой передаются в контроллер SDN в соответствии с применяемыми правилами.

– Шаг 5. По получении любого незнакомого пакета коммутатор SDN со встроенным контроллером пересылает его в приложение межсетевого экрана.

  Когда контроллер SDN получает пакет такого типа, который он никогда ранее не обрабатывал, он пересылает его в приложение межсетевого экрана для базовой проверки на безопасность.

– Шаг 6. Приложение межсетевого экрана анализирует незнакомый пакет.

  Приложение межсетевого экрана анализирует поля заголовка пакета и выясняет, что это сигнальный пакет неизвестного потока VoIP-вызова, например пакет протокола инициации сеанса (SIP), с подозрительной структурой.

– Шаг 7. Приложение межсетевого экрана запускает приложение DPI.

  Приложение межсетевого экрана запускает соответствующее приложение, например приложение DPI, для детального анализа подозрительных сигнальных пакетов на безопасность. После этого он пересылает пакеты в приложение DPI.

– Шаг 8. Приложение DPI анализирует незнакомый пакет.

  Приложение DPI анализирует заголовки и содержимое сигнального пакета, такие как номер вызывающего абонента и заголовки описания сеанса. Если, например, приложение DPI сочтет пакет поддельным хакерским пакетом или сканирующим пакетом, который ищет устройства VoIP/VoLTE, оно удаляет этот пакет.

– Шаг 9. Приложение DPI предписывает контроллеру SDN заблокировать этот пакет.

  Приложение DPI предписывает контроллеру SDN заблокировать этот пакет и блокировать последующие пакеты с тем же идентификатором вызова.

– Шаг 10. Контроллер SDN устанавливает новые правила.

  Контроллер SDN рассылает новую запись управления потоком (например, удалять пакеты) всем коммутаторам SDN, как на шаге 2. С этого момента коммутаторы будут удалять все несанкционированные пакеты.

8.2 Централизованная служба ловушек

8.2.1 Основная концепция централизованной службы ловушек

В этом разделе приводится описание основной концепции централизованной службы ловушек. Централизованная служба ловушек может динамически управлять местами установки ловушек. Как показано на рисунке 8-4, централизованная служба ловушек управляет коммутаторами и новыми маршрутами, заманивая злоумышленников в западню, то есть в ловушку. Ловушка сконфигурирована

как предназначенная для атак мишень и передает собранную информацию об атаках в централизованную службу ловушек.

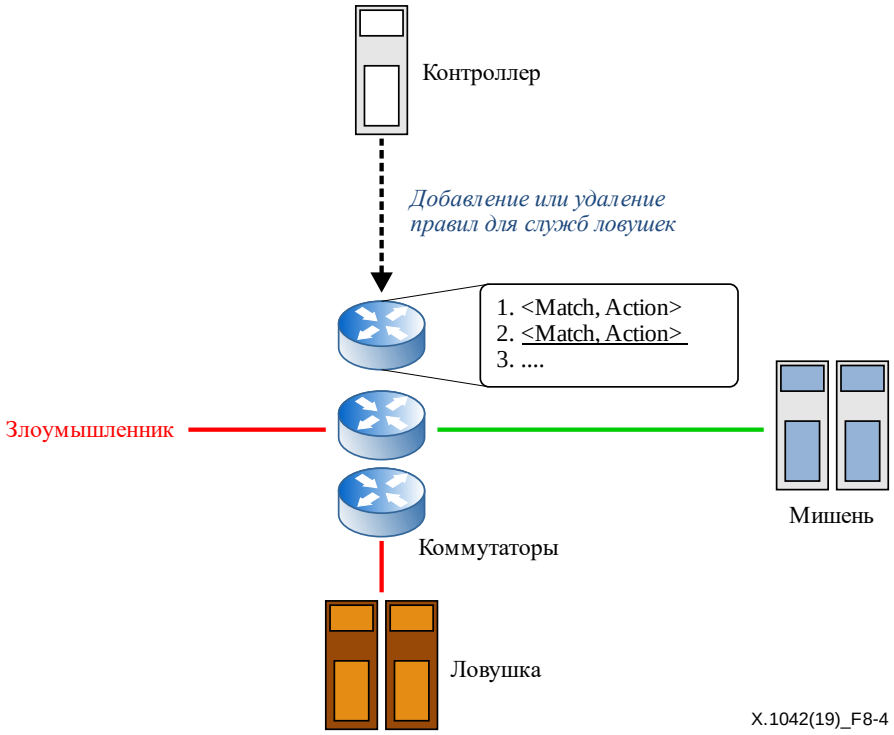

Рисунок 8-4 – Концепция централизованной службы ловушек

8.2.2 Сценарий работы централизованной службы ловушек

На рисунке 8-5 показан пример сценария работы централизованной службы ловушек для добавления в коммутаторы SDN маршрута к ловушке вместо фактической цели.

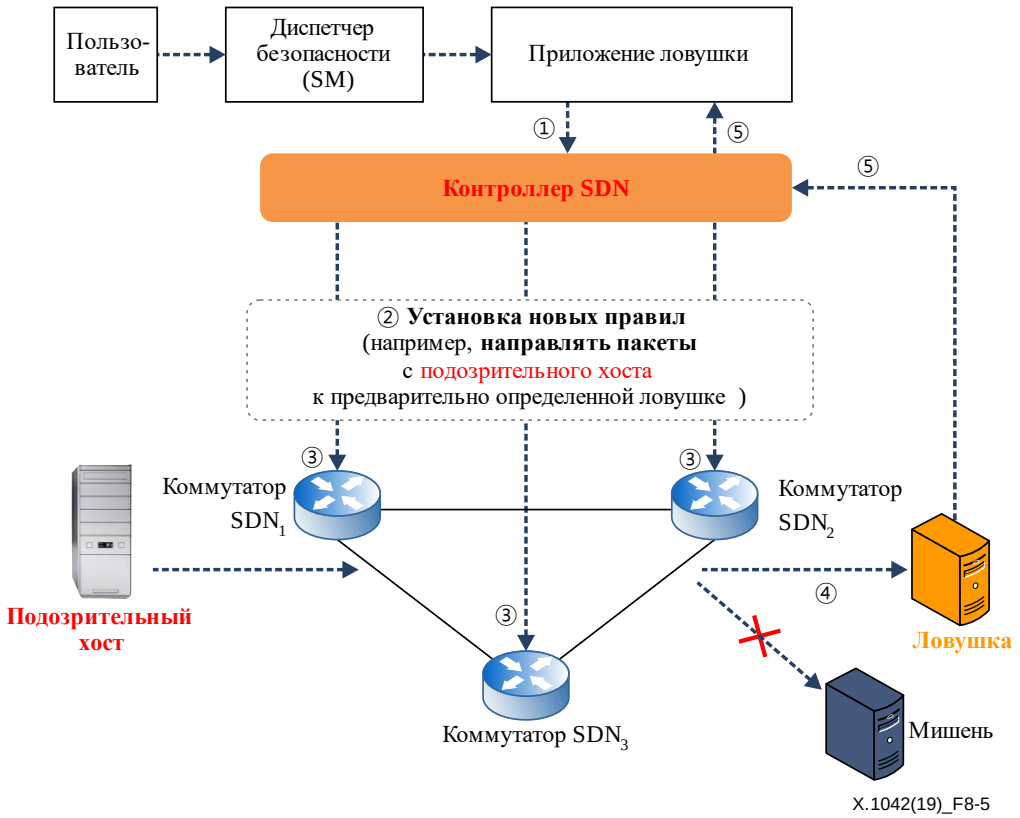

Рисунок 8-5 – Сценарий работы внутридоменной централизованной службы ловушек

– Шаг 1. Приложение ловушки устанавливает новые правила в контроллере SDN.

  Когда появляется информация о подозрительном хосте, приложение ловушки создает новое правило. Приложение ловушки, работающее поверх контроллера SDN, добавляет в контроллер SDN новое правило (например, пересылать пакеты от подозрительного хоста в ловушку), чтобы контролировать трафик, исходящий от подозрительного хоста.

– Шаг 2. Контроллер SDN рассылает новые правила соответствующим коммутаторам SDN.

  Контроллер SDN может разослать вновь установленное правило в каждый коммутатор. Таким образом контроллер SDN отправляет всем коммутаторам SDN команду на добавление записи управления потоком, содержащую правило (например, пересылать пакеты от подозрительного хоста в ловушку). Также можно организовать централизованное управление, с тем чтобы SM мог определять политику безопасности для своей службы из единого центра, то есть контроллера SDN.

– Шаг 3. Все коммутаторы SDN вводят новые правила в свои таблицы управления потоком.

  Получив команду на добавление записи управления потоком в отношении подозрительного хоста, все коммутаторы SDN добавляют в свои таблицы управления потоком запись управления потоком о пересылке последующих пакетов, поступивших от подозрительного хоста, в ловушку. После этого коммутатор SDN пересылает пакеты, поступившие от подозрительного хоста, в ловушку.

– Шаг 4. Коммутатор SDN применяет новые правила для поддержки службы ловушек.

  Получая пакеты от подозрительного хоста, коммутатор SDN пересылает их в ловушку. В соответствии с применяемыми правилами никакие пакеты от подозрительного хоста не могут попасть в коммутатор реального целевого хоста. Пересылаемые пакеты собираются в ловушке.

– Шаг 5. Служба ловушек сообщает контроллеру о подозрительных пакетах.

  Принимая пакеты от подозрительных хостов, служба ловушек обрабатывает их и отправляет в контроллер отчет о пакетах этого вида для анализа пакетов в контроллере.

8.3 Централизованная служба отражения DDoS-атак

8.3.1 Основная концепция централизованной службы отражения DDoS-атак

На рисунке 8-6 показана централизованная служба отражения DDoS-атак. Эта служба добавляет, удаляет или изменяет правила для каждого коммутатора SDN. В отличие от централизованной службы межсетевого экрана, относящейся к внутридоменным службам, эта служба в основном ориентирована на междоменный уровень.

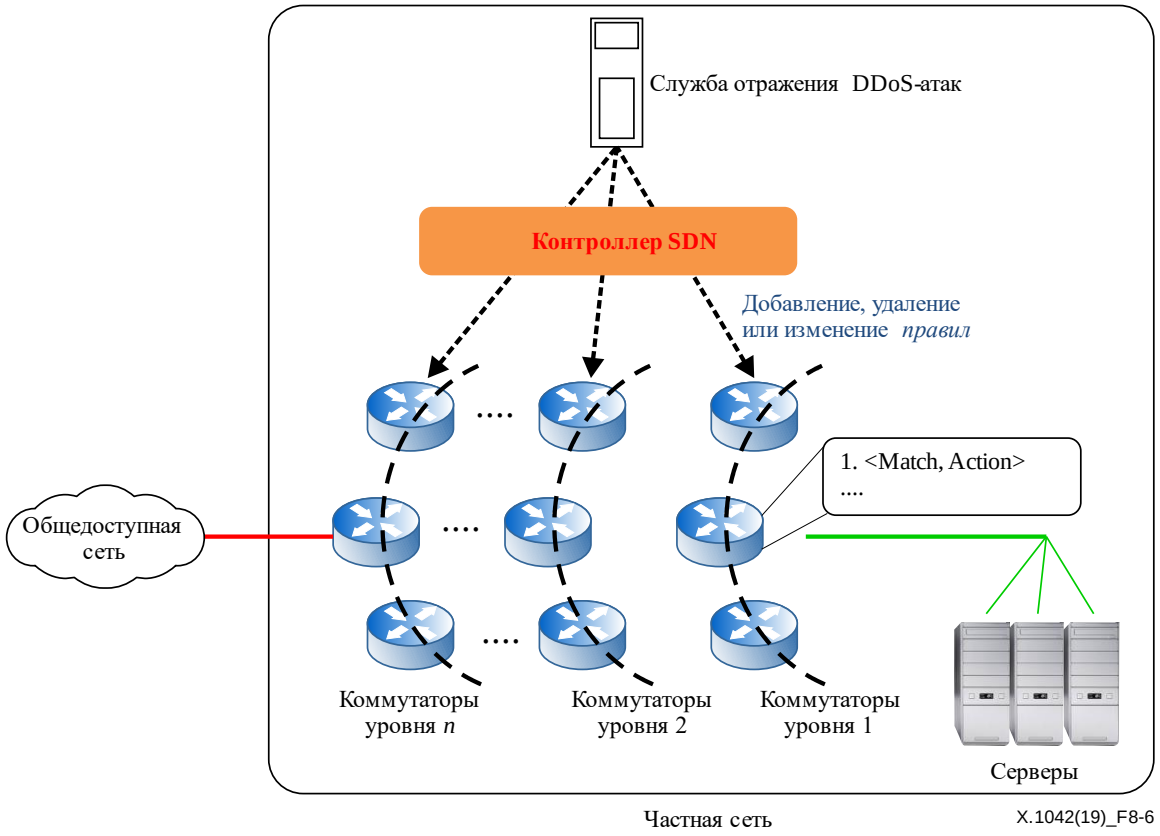

Рисунок 8-6 – Концепция централизованной службы отражения DDoS-атак

8.3.2 Централизованная служба отражения DDoS-атак для серверов, не фиксирующих данные о запросах

На рисунке 8-7 показан пример сценария работы централизованной службы отражения DDoS-атак для серверов службы наименований доменов (DNS), не фиксирующих данные о запросах.

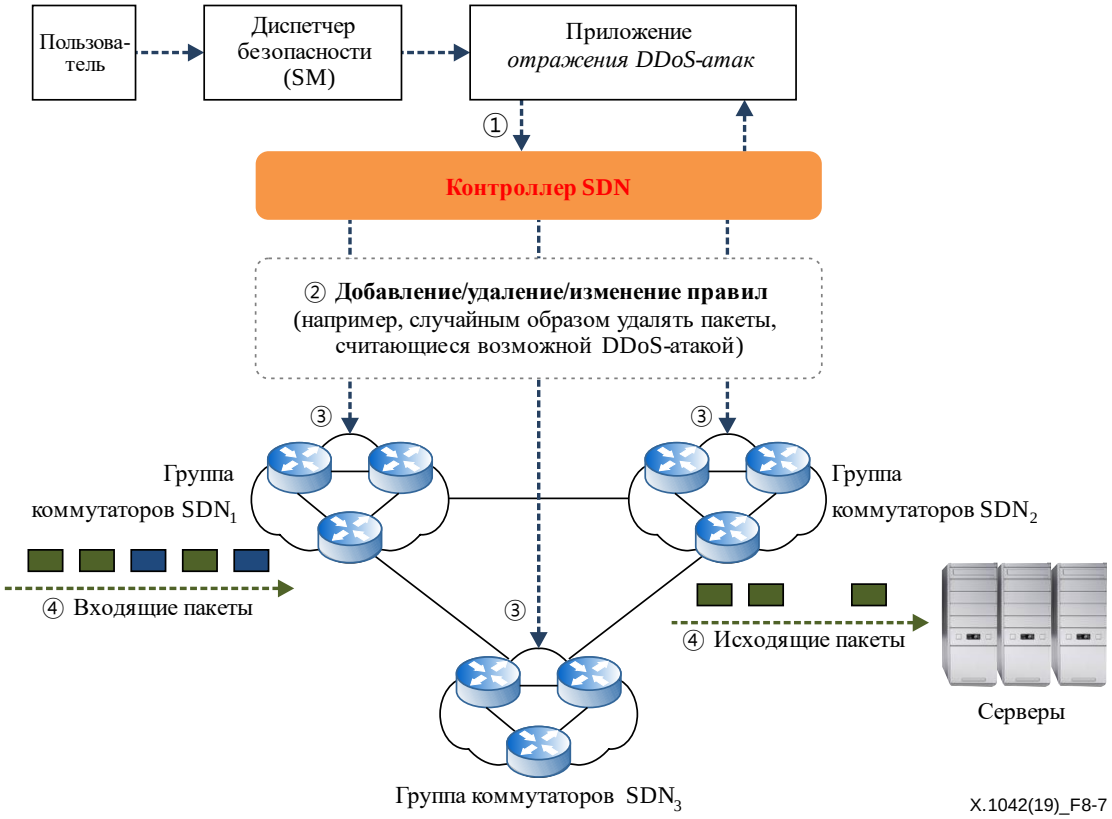

Рисунок 8-7 – Сценарий работы междоменной централизованной службы отражения DDoS-атак для серверов, не фиксирующих данные о запросах

– Шаг 1. Приложение отражения DDoS-атак устанавливает новые правила для контроллера SDN.

Когда от SM становится известно о новой DDoS-атаке, приложение отражения DDoS-атак создает новое правило. Чтобы предотвратить попадание в серверы пакетов и напрасную трату их ресурсов, в контроллер SDN добавляется новое правило (например, удалять пакеты DDoS-атаки случайным образом с некоторой вероятностью). Это добавление правила выполняется приложением отражения DDoS-атак, работающим поверх контроллера SDN.

– Шаг 2. Контроллер SDN рассылает новые правила соответствующим коммутаторам.

Контроллер SDN может разослать вновь установленное правило в каждый коммутатор. Таким образом контроллер SDN направляет во все коммутаторы SDN команду на добавление записи управления потоком, содержащей это правило (например, удалять случайным образом пакеты, считающиеся DDoS-атаками с определенной вероятностью). Также можно организовать централизованное управление, чтобы SM мог определять политику безопасности для своей службы из единого центра, то есть контроллера SDN.

– Шаг 3. Все коммутаторы SDN вводят новые правила в свои таблицы управления потоком.

Получив команду на добавление записи управления потоком для отражения DDoS-атак, все коммутаторы SDN добавляют в свои таблицы управления потоком запись управления потоком, предписывающую удалять последующие пакеты предполагаемой DDoS-атаки. После этого коммутатор SDN внутри домена может удалять пакеты DDoS-атаки с вероятностью, пропорциональной серьезности DDoS-атаки.

– Шаг 4. Коммутатор SDN выполняет новые правила отражения DDoS-атак.

Получая пакеты DDoS-атаки, коммутатор SDN выборочно удаляет их. Пакеты DDoS-атаки удаляются случайным образом в коммутаторах SDN в каждом домене в соответствии с возможностями обработки и функциями доменов. Затем информация о результатах удаления пакетов передается в контроллер SDN.

8.3.3 Централизованная служба отражения DDoS-атак для серверов, фиксирующих данные о запросах

На рисунке 8-8 показан пример сценария работы централизованной службы отражения DDoS-атак для веб-серверов, фиксирующих данные о запросах.

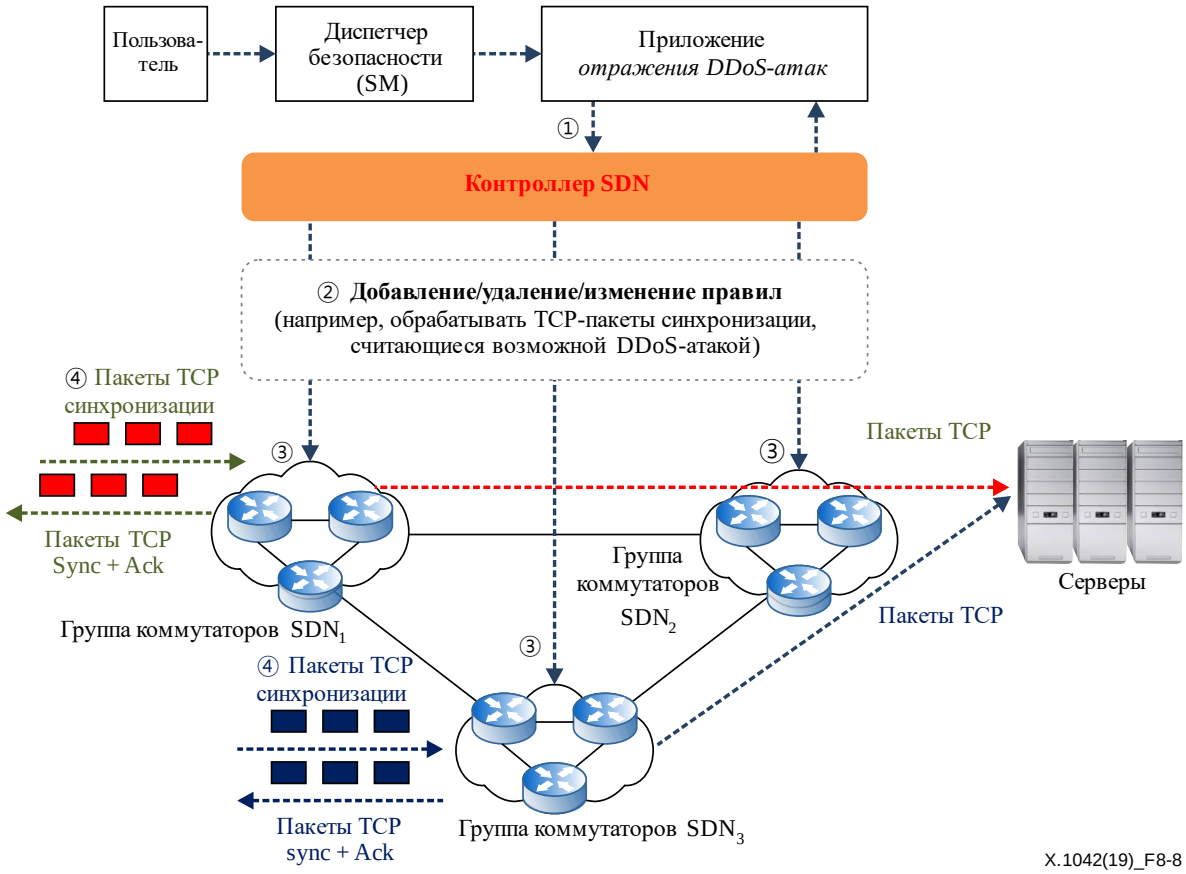

Рисунок 8-8 – Сценарий работы междоменной централизованной службы отражения DDoS-атак для серверов, фиксирующих данные о запросах

– Шаг 1. Приложение устанавливает новые правила для контроллера SDN.

  Приложение отражения DDoS-атак выбирает коммутатор, который будет играть роль прокси-сервера TCP. Добавление нового правила выполняется приложением отражения DDoS-атак, работающим поверх контроллера SDN.

– Шаг 2. Контроллер SDN рассылает новые правила соответствующим коммутаторам.

  После установки нового правила контроллер SDN может разослать его соответствующим коммутаторам для отражения DDoS-атак. В связи с этим контроллер SDN направляет всем коммутаторам SDN команду на добавление записи управления потоком, содержащей это правило (например, генерировать пакеты TCP Sync + Ack для пакетов, считающихся DDoS-атакой). Таким образом в выбранный коммутатор устанавливается новое правило, предписывающее ему генерировать TCP-пакеты Sync-Ack в ответ на запросы TCP Sync. Если одни и те же запросы поступают чаще, чем ожидалось, то контроллер SDN выбирает новый коммутатор для выполнения роли сервера. Для обычных запросов TCP Sync коммутатор передает сеанс TCP соответствующему серверу в частной сети. Также можно организовать централизованное управление, чтобы SM мог определять политику безопасности для своей службы из единого центра, то есть контроллера SDN.

– Шаг 3. Все коммутаторы SDN вводят новые правила в свою таблицу управления потоком.

  Получив команду на добавление записи управления потоком, относящейся к DDoS-атаке, все коммутаторы SDN добавляют в свою таблицу управления потоком запись управления потоком, предписывающую удалять последующие пакеты, считающиеся DDoS-атакой. После

этого коммутатор SDN может генерировать пакеты TCP Sync-Ack с вероятностью, пропорциональной серьезности DDoS-атаки.

– Шаг 4. Коммутатор SDN выполняет новые правила отражения DDoS-атак.

При получении пакетов DDoS-атаки коммутатор SDN в полном объеме реагирует на пакеты TCP Sync от хоста-злоумышленника случайным образом. Вместо реальных серверов запросы DDoS-атаки к серверам, фиксирующим данные о запросах, обрабатывают коммутаторы. Затем информация о результатах работы SDN-коммутатора по отражению DDoS-атаки передается контроллеру SDN.

8.4 Централизованная служба управления несанкционированными устройствами

8.4.1 Основная концепция централизованной службы управления несанкционированными устройствами

В этом разделе приводится описание основной концепции централизованной службы управления несанкционированными устройствами. Как показано на рисунке 8-9, централизованная служба управления несанкционированными устройствами ведет список несанкционированных устройств для предотвращения трафика от этих устройств. Список несанкционированных устройств хранится в базе данных черного списка и может обновляться вручную или автоматически независимыми приложениями. Централизованный диспетчер несанкционированных устройств периодически загружает список несанкционированных устройств из базы данных черного списка и передает эти события в приложение управления несанкционированными устройствами, которое генерирует новые правила безопасности для предотвращения сетевого трафика от этих несанкционированных устройств/к этим устройствам.

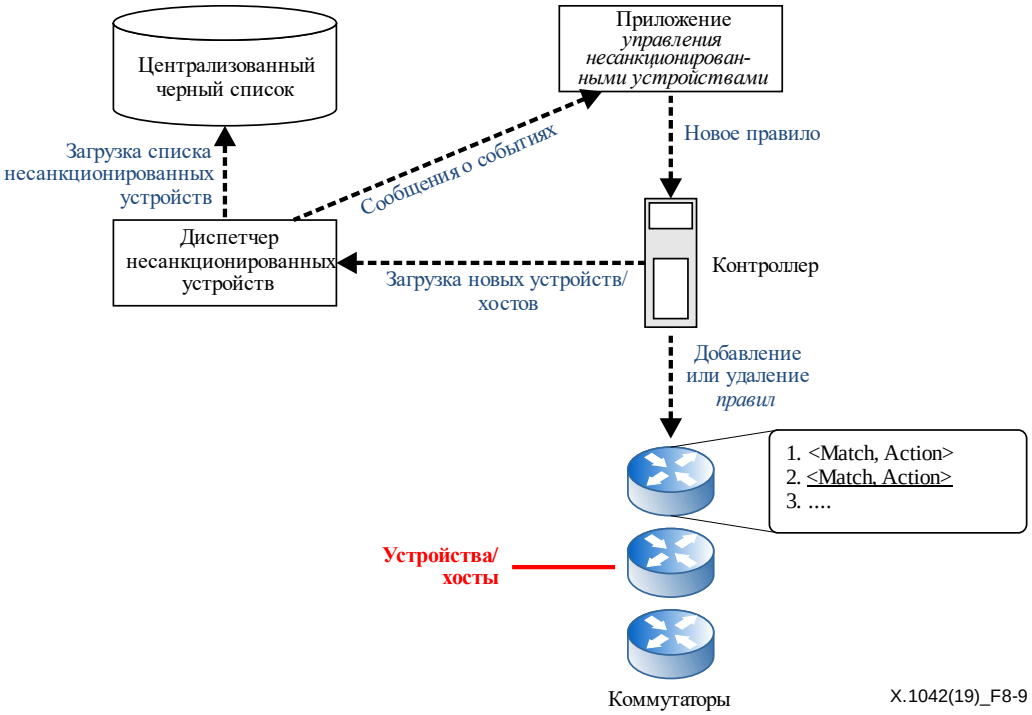

Рисунок 8-9 – Концепция централизованной службы управления несанкционированными устройствами

8.4.2 Сценарий работы централизованной службы управления несанкционированными устройствами

На рисунке 8-10 показан пример сценария работы централизованной службы управления несанкционированными устройствами для предотвращения трафика от украденных мобильных устройств.

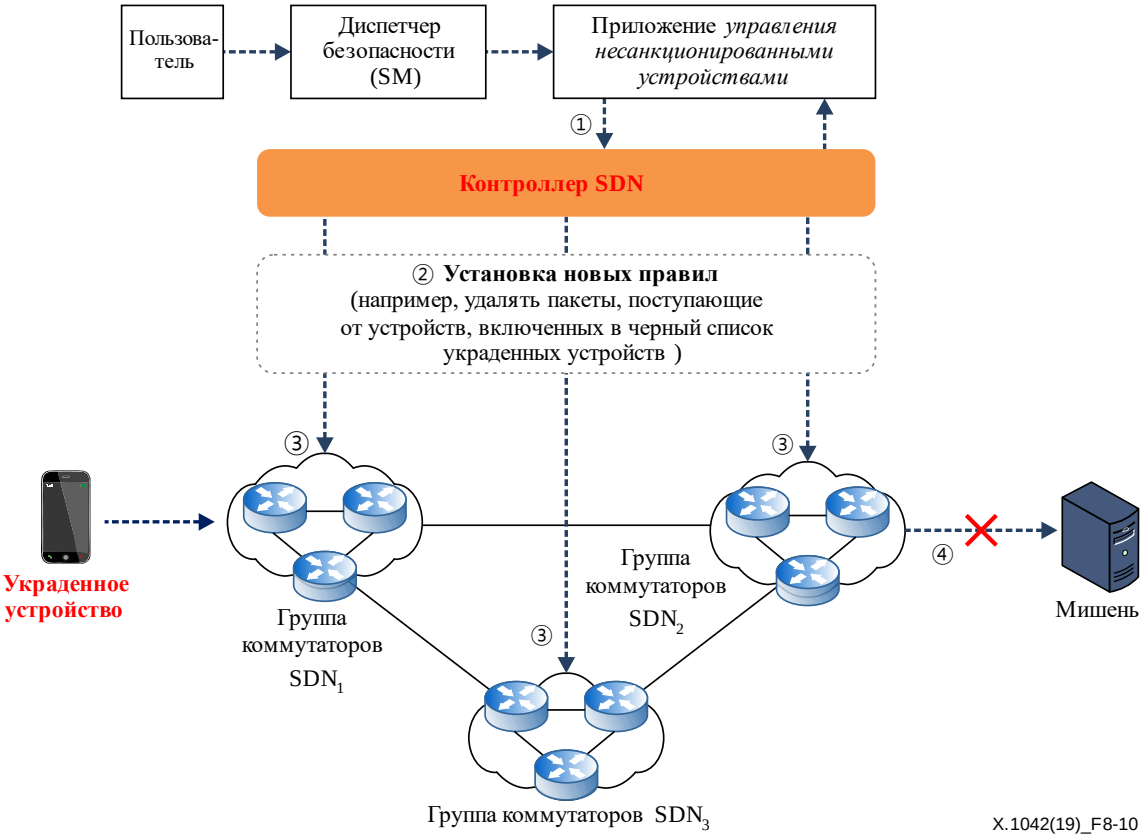

Рисунок 8-10 – Сценарий работы внутридоменной централизованной службы управления несанкционированными устройствами

– Шаг 1. Приложение управления несанкционированными устройствами устанавливает новые правила.

  При поступлении от централизованного диспетчера несанкционированных устройств информации о новых украденных устройствах приложение управления несанкционированными устройствами определяет новое правило. В качестве предварительного шага этого сценария приложение управления несанкционированными устройствами или SM добавляют в контроллер SDN новое правило (например, удалять пакеты, поступающие от устройств, включенных в централизованный черный список украденных устройств).

– Шаг 2. Контроллер SDN распространяет новые правила.

  Контроллер SDN может направить вновь установленное правило в каждый коммутатор. Контроллер SDN передает во все коммутаторы SDN команду добавления записи управления потоком, содержащей правило (например, удалять пакеты, поступающие от новых украденных устройств). Также можно организовать централизованное управление, чтобы центральный диспетчер несанкционированных устройств или SM могли определять политику безопасности для своей службы из единого центра, то есть контроллера SDN.

– Шаг 3. Все коммутаторы SDN добавляют новые правила в свои таблицы управления потоком.

  Получив команду добавления записи управления потоком в отношении украденных устройств, все коммутаторы SDN добавляют в свои таблицы управления потоком новую запись управления потоком, предписывающую удалять последующие пакеты, поступающие от этих устройств.

– Шаг 4. Коммутатор SDN выполняет новые правила.

  Коммутатор SDN полностью удаляет пакеты, поступающие от этих устройств. В соответствии с применяемыми правилами никакие пакеты, поступающие от этих устройств, передаваться не могут. После этого результаты выполнения правила передаются в контроллер SDN.

ПРИМЕЧАНИЕ. – Важно идентифицировать несанкционированные устройства. Для идентификации несанкционированного устройства используется уникальный идентификатор, присваиваемый централизованным

диспетчером несанкционированных устройств. Если контроллер SDN определяет только сетевой адрес, который может динамически изменяться, например адрес протокола Интернет (IP) устройства или адрес управления доступом к среде передачи (MAC), то при каждом изменении сетевого адреса несанкционированного устройства в контроллере SDN устанавливается новое правило, а старое удаляется.

8.5 Служба управления контролем доступа

8.5.1 Основная концепция службы управления контролем доступа

В этом разделе описана основная концепция службы управления контролем доступа (ACM). Модуль ACM с контроллером SDN может иерархически управлять политикой прав доступа. Как показано на рисунке 8-11, модуль ACM управляет правами доступа в целях предотвращения несанкционированного доступа к ресурсам.

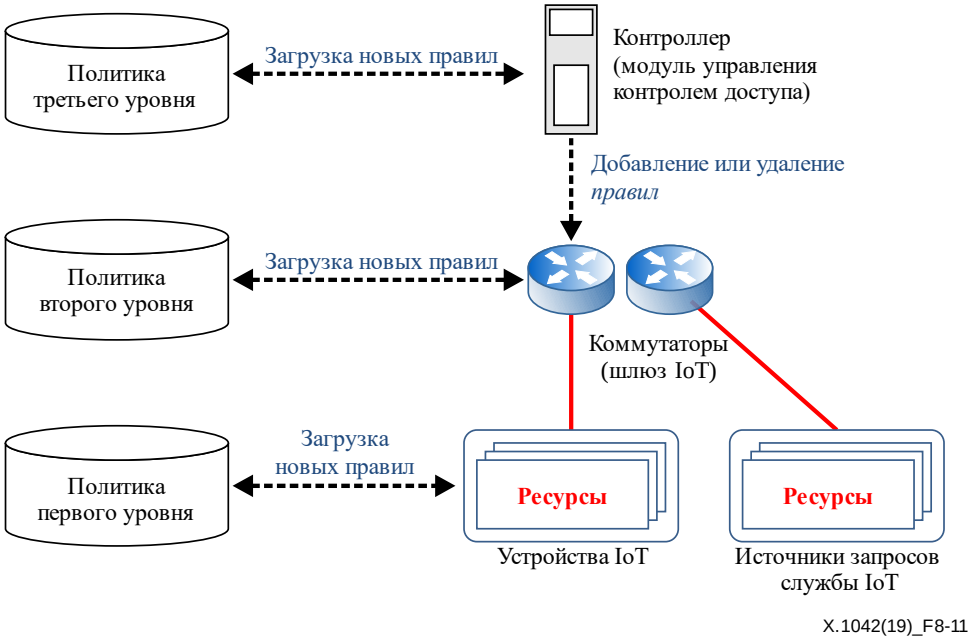

Рисунок 8-11 – Концепция службы управления контролем доступа

8.5.2 Сценарий работы службы управления контролем доступа

На рисунке 8-12 показан пример сценария работы службы ACM под управлением контроллера безопасности. В этом сценарии участвуют контроллер и коммутаторы SDN.

Рисунок 8-12 – Сценарий работы внутридоменной службы управления контролем доступа

– Шаг 1. Приложение ACM устанавливает новую политику от SM.

  Приложение ACM создает новую политику управления доступом к ресурсам в распределенных устройствах, предоставляющих услуги/ресурсы (например, в устройствах IoT). В качестве предварительного шага этого сценария SM уже добавил новую политику в это приложение ACM.

– Шаг 2. Контроллер SDN распространяет новые правила.

  Необходимо сохранить новое правило или правила. Затем контроллер SDN может распространить их в каждый коммутатор. Контроллер SDN может отправить запрос доступа для эксплуатации ресурса (ресурсов) в устройстве, предоставляющем услуги/ресурсы. В этом случае контроллер SDN не получает от коммутаторов SDN никаких запросов в отношении распространения правил. Коммутаторы SDN могут обращаться к контроллеру SDN с запросами на предоставление правил доступа к ресурсам в устройствах, предоставляющих услуги/ресурсы, до отправки контроллеру SDN запросов на распространение правил.

– Шаг 3. Все коммутаторы SDN добавляют новые правила в свою локальную базу данных.

  Все коммутаторы SDN добавляют новые правила в свою локальную базу данных для обработки запросов авторизации доступа к устройствам, предоставляющим услуги/ресурсы.

– Шаг 4. Коммутатор SDN выполняет новые правила.

  Коммутатор SDN может полностью удалять пакеты, поступающие от клиента услуг/ресурсов, в соответствии с правилами доступа. В этом случае каждый домен коммутатора SDN должен иметь возможность использовать разные правила доступа в соответствии со своими характеристиками. В соответствии с применяемыми правилами никакие пакеты от этих клиентов не могут проходить через коммутатор SDN. Приложение ACM должно сообщать обо всех пакетах, для которых отсутствуют правила доступа, контроллеру SDN в целях управления этими пакетами.

Дополнение I

Критерии для служб безопасности на основе SDN

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

В данном Дополнении приводятся критерии для различных служб безопасности.

I.1 Критерии для служб безопасности внутридоменных сетей

I.1.1 Централизованная служба межсетевого экрана

Для традиционных межсетевых экранов характерны проблемы, связанные с их значительной стоимостью, пропускной способностью, управлением контролем доступа, установлением политики и пакетными механизмами доступа. В настоящей Рекомендации представлена структура централизованной службы межсетевого экрана на основе SDN, позволяющая решить эти проблемы. Гибкое управление правилами межсетевого экрана может осуществлять централизованный сервер. Существующие протоколы SDN могут использоваться в стандартных интерфейсах, соединяющих приложения межсетевых экранов с коммутаторами.

– Стоимость

  Стоимость добавления межсетевых экранов к сетевым ресурсам, например к маршрутизаторам, шлюзам и коммутаторам, весьма значительна, поскольку межсетевые экраны необходимо добавлять к каждому сетевому ресурсу. Чтобы решить эту проблему, можно организовать централизованное управление каждым сетевым ресурсом, так чтобы всеми межсетевыми экранами управлял один централизованный сервер.

– Пропускная способность

  Пропускная способность межсетевых экранов часто бывает ниже, чем у соответствующих сетевых интерфейсов. Каждый сетевой ресурс должен проверять правила межсетевого экрана безотносительно состояния сети. В этой структуре межсетевые экраны можно адаптивно развертывать в зависимости от состояния сети.

– Управление контролем доступа

  Поскольку в администрируемой сети могут быть сотни сетевых ресурсов, динамическое управление доступом для служб безопасности, таких как межсетевые экраны, представляет собой проблему. Это связано с необходимостью динамически добавлять в межсетевые экраны правила для отражения новых сетевых атак.

– Установление политики

  Необходимо установить политику для каждого сетевого ресурса. Однако трудно описать, какие потоки разрешены и запрещены в администрируемой сети конкретной организации. Поэтому для определения политики безопасности такой сети может оказаться полезным централизованное представление.

– Пакетный механизм доступа

  На практике пакетного механизма доступа недостаточно, поскольку базовыми элементами контроля доступа обычно являются пользователи или приложения. Таким образом определить правила уровня приложения и добавить их в службу межсетевого экрана должен администратор.

I.1.2 Централизованная служба ловушек

Для традиционных ловушек характерны проблемы, связанные с их значительной стоимостью, пропускной способностью, управлением контролем доступа, установлением политики и пакетными механизмами доступа. В настоящей Рекомендации представлена структура централизованной службы ловушек на основе SDN, позволяющая решить эти проблемы. Местами установки ловушек можно гибко управлять из центрального сервера. Существующие протоколы SDN могут использоваться в стандартных интерфейсах, соединяющих приложения ловушки с коммутаторами.

– Стоимость

Стоимость эксплуатации дополнительных ловушек в сети весьма значительна ввиду необходимости использования для них дополнительных сетевых ресурсов, таких как хосты. Для решения этой проблемы можно организовать гибкое управление местами установки ловушек из центрального сервера.

– Пропускная способность

Пропускная способность ловушек зависит от возможностей хост-машин. Каждая ловушка всегда работает одинаково, независимо от состояния сети или условий атаки. В этой структуре ловушки можно адаптивно развертывать в зависимости от состояния сети или условий атаки.

– Управление контролем доступа

Поскольку в администрируемой сети могут быть сотни сетевых ресурсов, динамическая настройка ловушек представляет собой проблему. Это связано с необходимостью динамически менять места установки ловушек для защиты от новых атак.

– Установление политики

Необходимо установить политику для каждого сетевого ресурса. Однако трудно определить конкретные места установки ловушек для предполагаемых атак в зависимости от состояния сети и условий атаки. Поэтому для динамической корректировки политики безопасности с течением времени может быть полезно централизованное представление.

– Механизм развертывания ловушек

Ловушки должны развертываться в сети надлежащим образом в зависимости от ее состояния и условий атаки. Централизованная служба ловушек на основе SDN определяет оптимальное место для мониторинга и реагирования на атаки в режиме реального времени. Ловушка централизованно настраивается центральным сервером в качестве заданной мишени для атак.

I.2 Критерии для служб безопасности в междоменных сетях

I.2.1 Централизованная служба отражения DDoS-атак

Централизованная служба отражения DDoS-атак защищает серверы от DDoS-атак на частные сети извне, то есть атак, исходящих из сетей общего пользования. Серверы делятся на серверы, не фиксирующие данные о запросах (например, DNS-серверы), и серверы, фиксирующие данные о запросах (например, веб-серверы). На рисунке 8-6 показана конфигурация службы отражения DDoS-атак в частной сети. Коммутаторы в частной сети сконфигурированы в иерархические доменные уровни – коммутаторы уровня 1, коммутаторы уровня 2 и т. д. Коммутаторы уровня *n* образуют динамические линии защиты от различных DDoS-атак.

Для централизованной службы отражения DDoS-атак характерны проблемы, связанные с их значительной стоимостью, пропускной способностью, управлением контролем доступа, установлением политики и пакетными механизмами доступа. В настоящей Рекомендации представлена структура централизованной службы отражения DDoS-атак на основе SDN, позволяющая решить эти проблемы. Гибкое управление правилами отражения DDoS-атак может осуществлять центральный сервер. Можно использовать существующие протоколы SDN через стандартные интерфейсы, соединяющие приложения отражения DDoS-атак с коммутаторами.

– Стоимость

Каждым сетевым ресурсом можно управлять централизованно и гибко с минимальными затратами, так чтобы настройка коммутаторов и управление ими осуществлялись центральным сервером на нескольких уровнях. По мере того как DDoS-атаки на сервер становятся все более серьезными, многоуровневые коммутаторы выборочно удаляют пакеты, ослабляя воздействие DDoS-атак. Другими словами, подозрительные пакеты предполагаемой DDoS-атаки удаляются на раннем этапе в начале маршрута к хосту, являющемуся потенциальным объектом атаки.

– Пропускная способность

Централизованная служба отражения DDoS-атак часто работает медленнее, чем позволяет пропускная способность соответствующих сетевых интерфейсов. В традиционной службе

каждый сетевой ресурс должен проверять правила отражения DDoS-атак безотносительно состояния сети. В этой же структуре приложения для отражения DDoS-атак можно развертывать адаптивно в зависимости от состояния сети.

– Управление контролем доступа

Поскольку в администрируемой сети могут быть сотни сетевых ресурсов, службам безопасности, таким как службы отражения DDoS-атак, трудно динамически управлять доступом. Это связано с необходимостью динамически добавлять правила отражения DDoS-атак для новых DDoS-атак.

– Установление политики

Необходимо устанавливать политику для каждого сетевого ресурса. Однако трудно определить конкретную политику удаления пакетов для отражения DDoS-атак в зависимости от состояния сети. Поэтому для динамической корректировки политики безопасности с течением времени может быть полезно централизованное представление.

– Механизм обнаружения DDoS-атак

Обнаружение DDoS-атак выполняется путем проверки интервала времени, с которым клиентские запросы поступают к службам. Механизм обнаружения DDoS-атак определяет вероятность того, что запросы от клиента представляют собой DDoS-атаку, и удаляет запросы с более высокой частотой, пропорциональной этой вероятности.

I.2.2 Централизованная служба управления несанкционированными устройствами

Для традиционных служб управления несанкционированными устройствами характерны проблемы, связанные с их значительной стоимостью, пропускной способностью, управлением контролем доступа, установлением политики и пакетными механизмами доступа. В настоящей Рекомендации представлена централизованная служба управления несанкционированными устройствами на основе SDN, позволяющая решить эти проблемы. Управление правилами внесения устройств в черный список можно осуществлять глобально. Существующие протоколы SDN могут использоваться через стандартные интерфейсы, соединяющие приложения несанкционированного устройства с коммутаторами.

– Стоимость

Обновление черных списков в сетевых ресурсах, например маршрутизаторах, шлюзах и коммутаторах, связано со значительными расходами из-за необходимости обновлять черные списки в каждом из сетевых ресурсов отдельно. Чтобы решить эту проблему, управление правилами безопасности, относящимися к черным спискам, для каждого сетевого ресурса можно осуществлять централизованно, так чтобы отдельно взятой службой управления несанкционированными устройствами управлял централизованный сервер.

– Пропускная способность

Поскольку в централизованной службе, в отличие от традиционной, пакеты, поступающие от устройств из черного списка, удаляются в начале маршрута, на практике пропускная способность централизованной службы управления несанкционированными устройствами может быть повышена.

– Управление контролем доступа

При локальном управлении черными списками бывает трудно синхронизировать локально распределенные черные списки, поскольку в сети могут быть сотни сетевых ресурсов, расположенных в разных странах. Правила безопасности для новых несанкционированных устройств должны добавляться динамически.

– Установление политики

Необходимо установить политику для каждого сетевого ресурса. Однако трудно описать, какие устройства запрещены в рамках управляемой сети конкретной организации. Для определения политики безопасности такой сети может оказаться полезным централизованное представление.

– Механизм обновления черных списков

Важно поддерживать актуальный черный список несанкционированных устройств. Поэтому для сохранения актуальной информации обо всех несанкционированных устройствах существующие традиционные службы должны регулярно обновлять базу данных черных списков. В централизованной службе управления несанкционированными устройствами черный список ведется центральным сервером как единая логическая база данных.

I.2.3 Служба управления контролем доступа

Для служб ACM характерны некоторые проблемы, связанные со значительной стоимостью, пропускной способностью, управлением контролем доступа, установлением политики и пакетными механизмами доступа. Для решения этих проблем в настоящей Рекомендации представлена централизованная служба ACM на основе SDN. В распределенных сетевых службах (например, контроллеры SDN и коммутаторы) управление правилами внесения устройств в белый список можно осуществлять глобально. Для этого могут использоваться существующие протоколы SDN через стандартные интерфейсы, соединяющие приложения ACM с коммутаторами посредством контроллера SDN.

– Стоимость

  Стоимость обновления белых списков в сетевых ресурсах, например маршрутизаторах, шлюзах и коммутаторах, является значительной из-за необходимости обновлять белые списки в каждом из многочисленных сетевых ресурсов. Для решения этой проблемы управление политикой безопасности, связанной с белыми списками каждого сетевого ресурса, можно осуществлять централизованно, так чтобы службой ACM управлял центральный сервер.

– Пропускная способность

  Поскольку в отличие от традиционной службы пакеты, поступающие от устройств, не имеющих прав доступа, удаляются в начале маршрута, на практике пропускную способность службы ACM можно повысить. Кроме того, информация о правах доступа распределяется и хранится в сетевых ресурсах в соответствии с их уровнем безопасности.

– Управление контролем доступа

  При локальном управлении белыми списками их бывает трудно синхронизировать, поскольку могут быть сотни сетевых ресурсов, находящихся в разных странах. Правила безопасности должны распространяться динамически для передачи сетевым ресурсам новых прав доступа.

– Установление политики

  Для каждого сетевого ресурса необходимо установить политику в соответствии с его уровнем безопасности. Однако трудно описать, какие устройства IoT запрещены в рамках сети конкретной организации, управляемой ACM. Для определения политики безопасности такой сети может оказаться полезным централизованное представление.

– Механизм обновления белых списков

  Важно поддерживать актуальный белый список прав доступа устройств IoT. Поэтому существующие традиционные службы должны регулярно обновлять базу данных белых списков, чтобы в ней содержалась актуальная информация о правах доступа всех устройств IoT. В службе ACM белый список управляется централизованно из центрального сервера как единая логическая база данных. Кроме того, некоторые элементы политики могут быть распределены по сетевым ресурсам.

Дополнение II

Пример обнаружения сканирования данных пакетов

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

Для обнаружения и отражения некоторых атак, таких как файлы червя, необходимо поддерживать обнаружение сканирования подобных пакетов. В целях повышения эффективности администратор настраивает политику на обнаружение лишь некоторых случайным образом выбранных пакетов потока. Одна из возможных схем обнаружения сканирования данных пакетов [b-ICIN SDNSec] предусматривает выбор первых *m* последовательных пакетов из каждого потока. Эту схему можно использовать для всех потоков или только для потоков, удовлетворяющих некоторым условиям, например пакеты с определенным IP-адресом источника или пакеты определенному получателю.

Протокол OpenFlow [b-ONF TS-012] как одну из реализаций нисходящего интерфейса SDN можно расширить для поддержки обнаружения сканирования данных пакетов. В формат записи правила управления потоком можно добавить две дополнительные функции. Эти изменения должны быть отражены как в контроллере, так и в коммутаторах. Одна из этих функций представляет собой схему, которая позволяет обнаруживать сканирование данных пакетов. Другая – это условие с описанием потоков, отвечающих условиям, установленным администратором или приложением. Затем в раздел 5.12 [b-ONF TS-012] добавляется факультативное действие (OFPAT_DETECTION), как указано ниже курсивом: *факультативное действие: действие Detection пересылает пакет в указанный порт OpenFlow, а затем в устройства защиты (например, FW, IDP, DPI и т. д.) для дальнейшего обнаружения сканирования данных.* Это новое действие аналогично действию OFPAT_OUTPUT в протоколе OpenFlow. Наконец, в разделе 7.2.4 [b-ONF TS-012] следует обновить структуры действий, как указано ниже курсивом.

```
enum ofp_action_type {
OFPAT_OUTPUT = 0,                              /* Вывод через порт коммутатора */
OFPAT_DETECTION = XX (заданное число),      /* Вывод через порт коммутатора */
OFPAT_COPY_TTL_OUT = 11,      /* Копирование TTL "вовне" – из следующего за крайним в крайний */
OFPAT_COPY_TTL_IN = 12,       /* Копирование TTL "вовнутрь" – из крайнего в следующий за крайним */
OFPAT_SET_MPLS_TTL = 15,      /* MPLS TTL */
OFPAT_DEC_MPLS_TTL = 16,      /* Уменьшение MPLS TTL */
OFPAT_PUSH_VLAN = 17,         /* Помещение в стек нового тега VLAN */
OFPAT_POP_VLAN = 18,          /* Извлечение из стека крайнего тега VLAN */
OFPAT_PUSH_MPLS = 19          /* Помещение в стек нового тега MPLS */
OFPAT_POP_MPLS = 20,          /* Извлечение из стека крайнего тега MPLS */
OFPAT_SET_QUEUE = 21,         /* Задание идентификатора очереди при выводе через порт */
OFPAT_GROUP = 22,             /* Применение группы */
OFPAT_SET_NW_TTL = 23,        /* IP TTL */
OFPAT_DEC_NW_TTL = 24,        /* Уменьшение IP TTL */
OFPAT_SET_FIELD = 25,         /* Задание поля заголовка с использованием формата OXM TLV */
OFPAT_PUSH_PBB = 26,          /* Помещение в стек нового тега службы PBB (I-TAG) */
OFPAT_POP_PBB = 27,           /* Извлечение из стека крайнего тега службы PBB (I-TAG) */
OFPAT_EXPERIMENTER = 0xffff
};
Для действия Detection используются следующая структура и поля:
/* Структура действия OFPAT_DETECTION, которое передает пакеты из порта */
struct ofp_action_detection {
uint16_t type;                 /* OFPAT_DETECTION */
uint16_t len;                  /* Длина 16 */
uint32_t port;                 /* Выходной порт */
uint16_t schema;               /* Одна из возможных схем: выбирать первые m
                               последовательных пакетов из каждого потока */
uint32_t condition;            /* Одно из возможных условий: пакеты потока в определенный пункт назначения */
};

OFP_ASSERT(sizeof(struct ofp_action_output) == 10);
```

Дополнение III

Архитектура реализации служб безопасности на основе SDN

(Данное Дополнение не является неотъемлемой частью настоящей Рекомендации)

III.1 Структура интерфейса для функций защиты сети с использованием SDN в стандарте IETF

III.1.1 Обзор

В этом разделе представлена структура интерфейса IETF для функции защиты сети (I2NSF) с использованием SDN в облачных службах безопасности, таких как межсетевые экраны, DPI и функции отражения DDoS-атак. SDN позволяет применять некоторые правила фильтрации пакетов в сетевых коммутаторах, управляя их правилами пересылки пакетов. Использование этой функциональной способности SDN позволяет оптимизировать процесс применения службы безопасности в структуре I2NSF.

На рисунке III-1 показана структура I2NSF [b-IETF RFC 8329] с использованием сетей SDN для поддержки сетевых служб безопасности. В этой структуре реализация правил политики безопасности распределена между коммутаторами SDN и функциями сетевой безопасности (NSF). В данном случае используются протокол NETCONF и язык моделирования YANG.

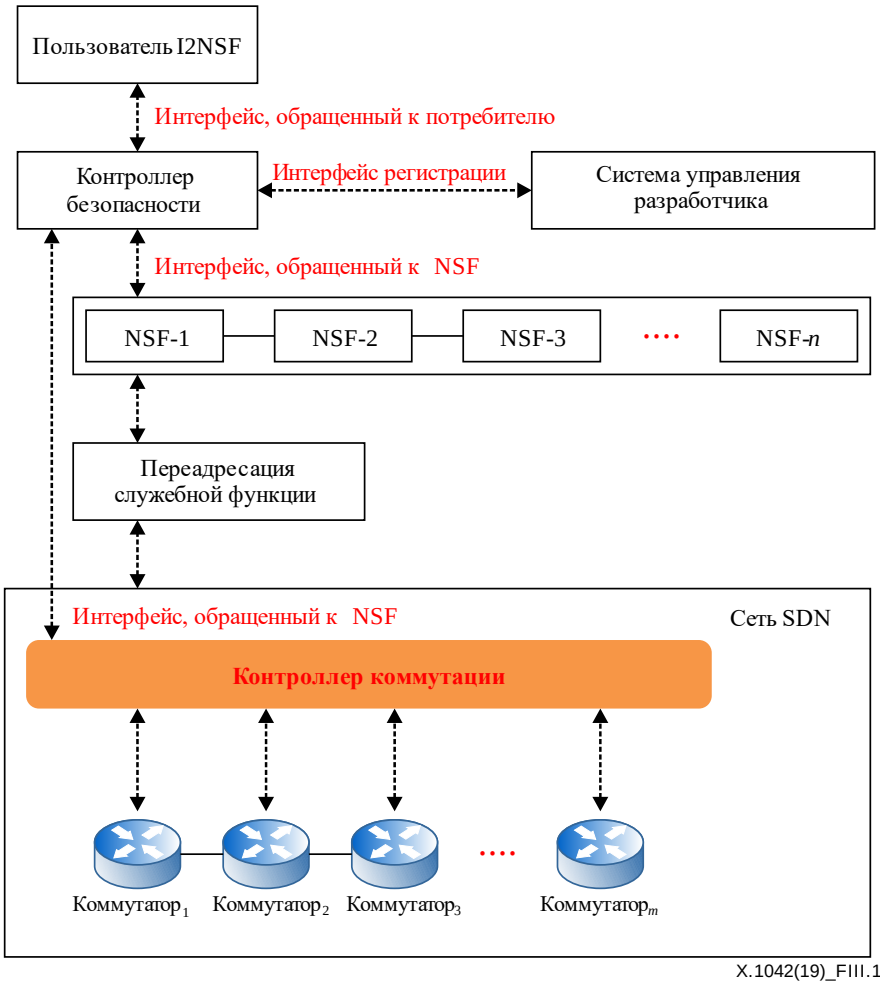

Рисунок III-1 – Структура интерфейса для функций защиты сети в стандарте IETF

III.1.2 Сравнение архитектур, разработанных IETF и МСЭ-Т

На рисунке III-2 приведено сравнение структуры I2NSF с использованием SDN с архитектурой, разработанной МСЭ-Т. Компоненты архитектуры МСЭ-Т показаны синим цветом.

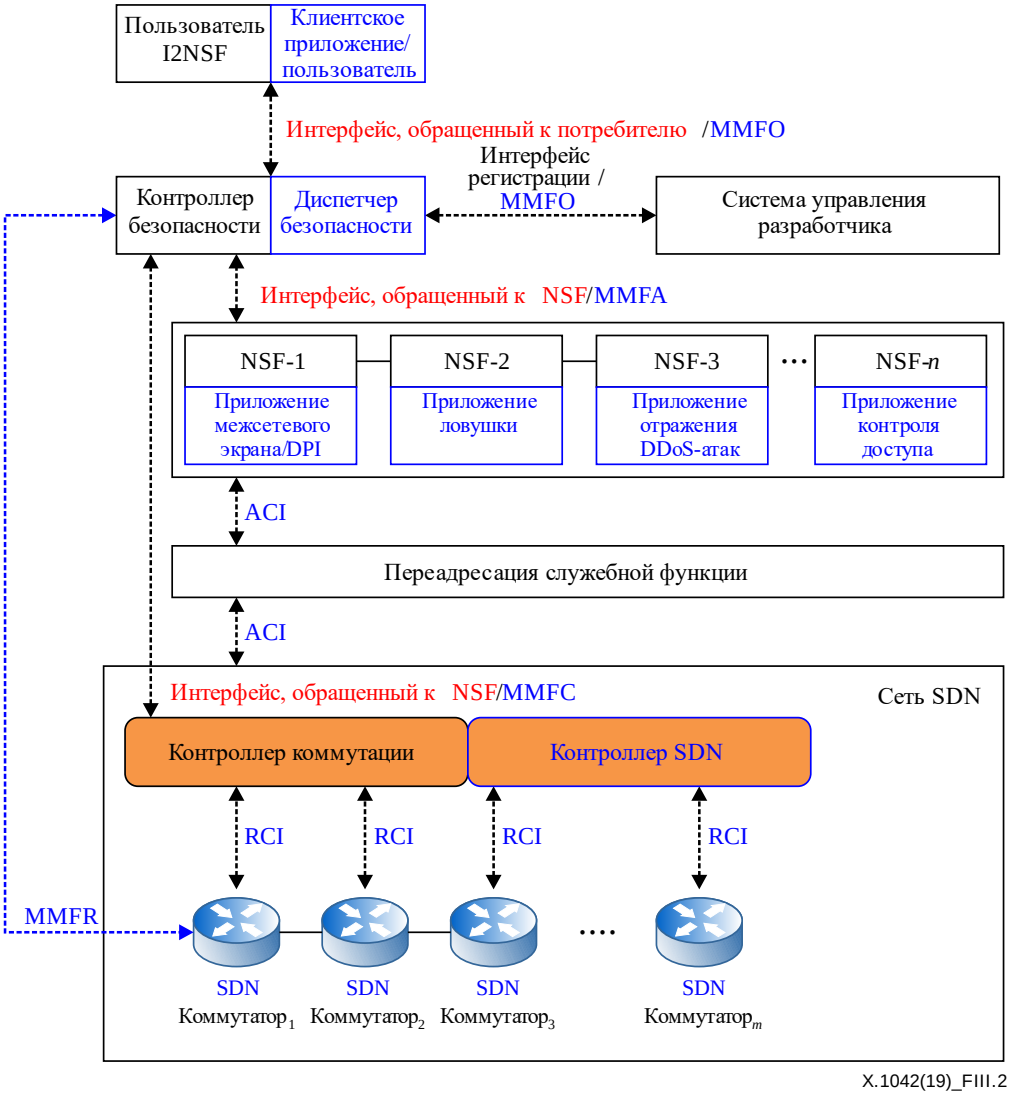

Рисунок III-2 – Сравнение архитектур, разработанных IETF и МСЭ-Т

III.2 Архитектура SDN в стандарте ONF

III.2.1 Обзор

В этом разделе представлена архитектура SDN в стандарте ONF. На рисунке III-3 показана архитектура SDN, предложенная в [b-ONF TR-521]. На рисунке III-3 SDN моделируется как набор отношений клиент–сервер между контроллерами SDN и другими объектами, которые сами могут быть контроллерами SDN. Контроллер SDN в роли сервера может предлагать услуги любому числу клиентов, а контроллер SDN, действующий как клиент, может получать услуги от любого количества серверов. Внутренние детали объектов, которые не являются контроллерами SDN, не включаются в рамки этой архитектуры, если они демонстрируют соответствующее поведение интерфейса. В данном случае используется протокол OpenFlow.

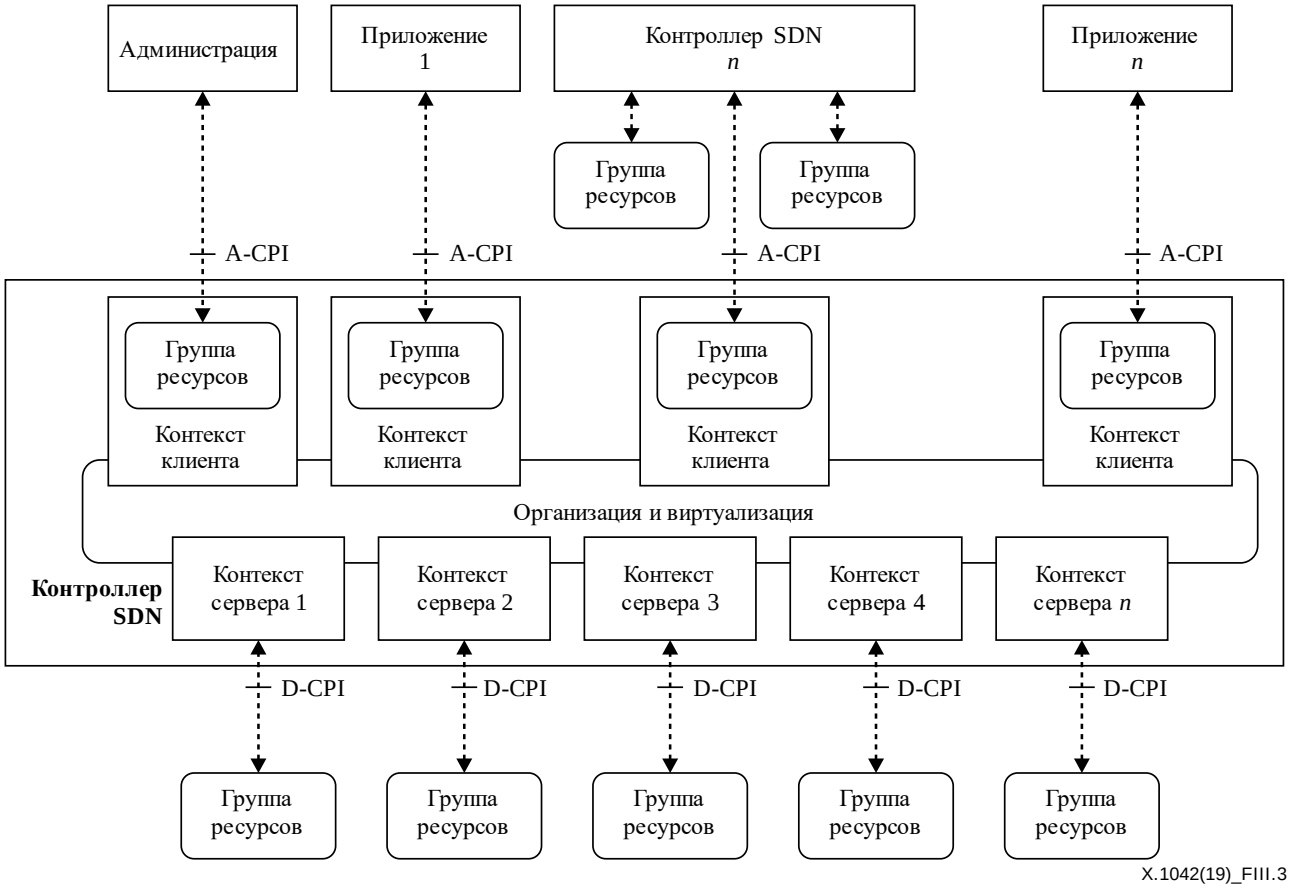

Рисунок III-3 – Архитектура SDN, разработанная ONF

III.2.2 Сравнение архитектур ONF и МСЭ-Т

На рисунке III-4 приведено сравнение архитектур, разработанных ONF и МСЭ-Т. Компоненты архитектуры МСЭ-Т показаны синим цветом.

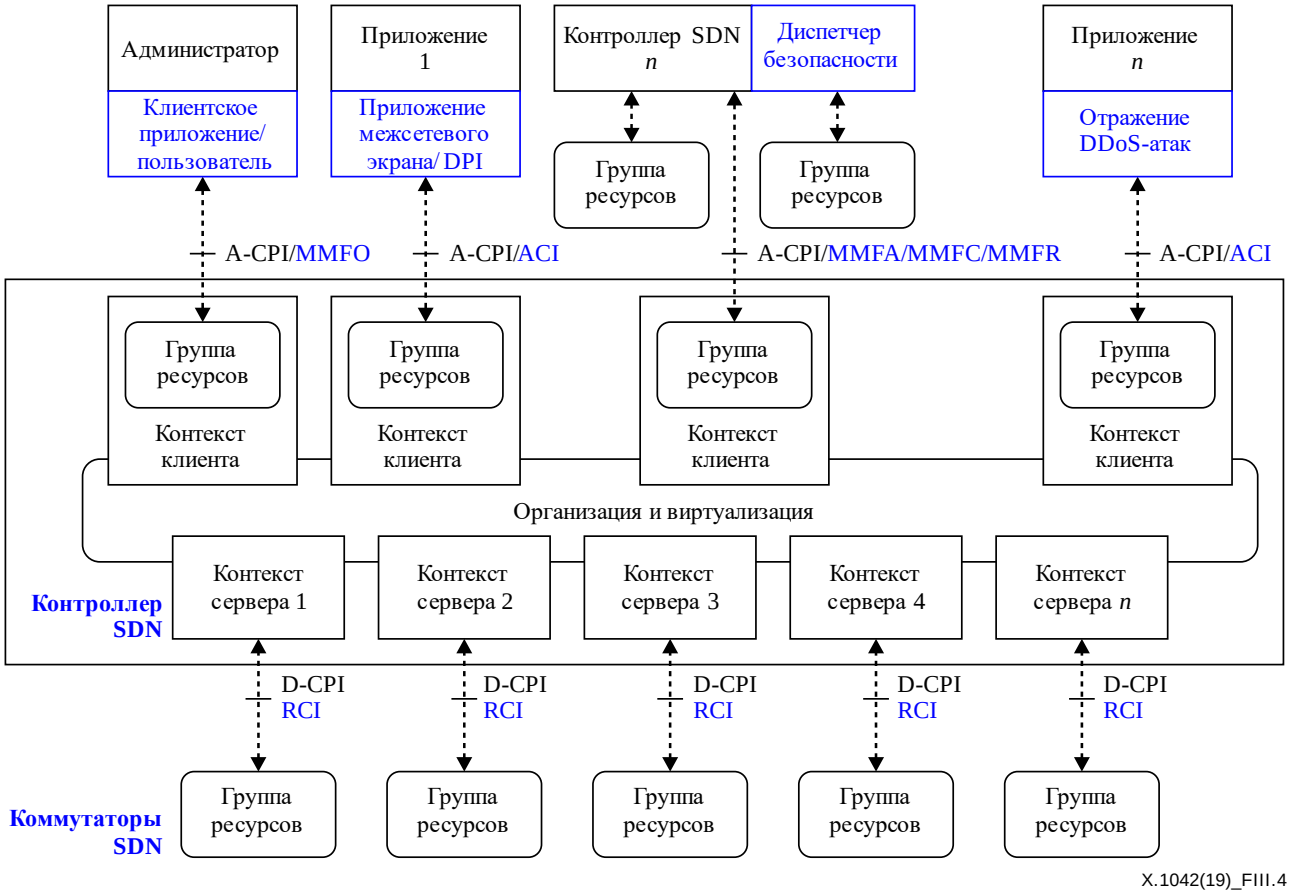

Рисунок III-4 – Сравнение архитектур, разработанных ONF и МСЭ-Т

Библиография

[b-ITU-T X.812] Recommendation ITU-T X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework*

[b-ITU-T X.1252] Рекомендация МСЭ-Т X.1252 (2010 год), *Базовые термины и определения в области управления определением идентичности*

[b-ICIN SDNSec] Hu, Z., Wang, M., Yan, X., Yin, Y., Luo, Z. (2015). A comprehensive security architecture for SDN. См.: *18th International Conference on Intelligence in Next Generation Networks*, pp 30-37. New York, NY: IEEE. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7073803

[b-IETF RFC 8329] IETF RFC 8329 (2018), *Framework for interface to network security functions*. https://tools.ietf.org/html/rfc8329

[b-ONF TR-521] Open Networking Foundation TR-521 (2016), *SDN architecture*. https://www.opennetworking.org/wp-content/uploads/2014/10/TR-521_SDN_Architecture_issue_1.1.pdf

[b-ONF TS-012] Open Networking Foundation TS-012 (2013). *OpenFlow switch specification V.1.4.0*. https://www.opennetworking.org/wp-content/uploads/2014/10/openflow-spec-v1.4.0.pdf

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энегоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и "умные" города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2019 год