УДК 004.7

Оригинальная статья

Обеспечение безопасности корпоративных сетей на основе оборудования D-Link

П. В. Ромасевич[1*], Е. В. Смирнова[2], В. А. Шибанов[3,4]

[1] ФГАОУ ВО «Волгоградский государственный университет», г. Волгоград, Российская Федерация
Адрес: 400062, Российская Федерация, г. Волгоград, пр. Университетский, д. 100

[2] ООО «Д-Линк Трейд», г. Москва, Российская Федерация
Адрес: 129626, Российская Федерация, г. Москва, Графский переулок, д. 14, к. 1

[3] ООО «Д-Линк Трейд», г. Рязань, Российская Федерация
Адрес: 390043, Российская Федерация, г. Рязань, пр-д Шабулина, д. 16

[4] ФГБОУ «Рязанский государственный радиотехнический университет имени В.Ф. Уткина», г. Рязань, Российская Федерация
Адрес: 390005, Российская Федерация, г. Рязань, ул. Гагарина, д. 59/1

[*] promasevich@dlink.ru

Аннотация

На общем фоне атак на корпоративные инфокоммуникации значительную их часть занимают попытки нарушения целостности и доступности информации путем дестабилизации сетевой инфраструктуры. Поскольку злонамеренные действия в этом направлении могут происходить на разных уровнях модели OSI и исходят в основном от «внутренних» нарушителей, в статье делается акцент на комплексное применение функционала обеспечения безопасности сетевой инфраструктуры, встроенного в программное обеспечение активного сетевого оборудования компании D-Link.В работе дана характеристика компонентов функционала безопасности сетевой инфраструктуры и их позиционирование с точки зрения целесообразности использования на уровнях иерархии сети. Функции безопасности уровня магистрали обеспечиваются средствами повышения отказоустойчивости сети при обрывах кабелей, разграничения и фильтрации трафика по различным критериям, защитой коммутаторов от несанкционированного доступа к их ЦПУ, контролем подключения сетевых узлов на основе анализа их связок IP/MAC/порт и их аутентификация на основе портов подключения и MAC-адресов.Средства безопасности уровня шлюза представлены новой линейкой сервисных маршрутизаторов для сектора SMB с отечественным программным обеспечением, что гарантирует независимость от зарубежных разработчиков и своевременное развитие их функционала в соответствии с тенденциями отрасли. Данные устройства совмещают в себе функции маршрутизатора, межсетевого экрана, настраиваемого коммутатора и сервера ряда сетевых протоколов. Новая функция маршрутизаторов по блокировке рекламы позволяет эффективно блокировать рекламные объявления, возникающие при просмотре web-страниц. Сервисные маршрутизаторы D-Link поддерживают работу с российским сервисом контентной фильтрации SkyDNS, который предлагает дополнительные возможности для организации безопасной работы в сети Интернет.

Ключевые слова: корпоративные сети, обеспечение безопасности, коммутаторы, злонамеренные действия, Port Security, Traffic Segmentation, VLAN, IP-MAC-Port Binding, аутентификация, списки управления доступом, Safeguard Engine, CPU Interface Filtering, ERPS, LoopBackDetect, сервисные маршрутизаторы, VPN, средний бизнес, малый бизнес, российское ПО

Конфликт интересов: авторы заявляют об отсутствии конфликта интересов.

Для цитирования: Ромасевич П. В., Смирнова Е. В., Шибанов В. А. Обеспечение безопасности корпоративных сетей на основе оборудования D-Link // Современные информационные технологии и ИТ-образование. 2023. Т. 19, № 2. С. 430-437.

Original article

Ensuring the Security of Corporate Networks Based on D-Link Equipment

P. V. Romasevich[a*], E. V. Smirnova[b], V. A. Shibanov[c,d]
[a] Volgograd State University, Volgograd, Russian Federation
Address: 100 Universitetsky Ave., Volgograd 400062, Russian Federation
[b] D-Link Company, Moscow, Russian Federation
Address: 14-1 Grafskij per., Moscow 129626, Russian Federation
[c] D-Link Company, Ryazan, Russian Federation
Address: 16 Shabulin's pas., Ryazan 390043, Russian Federation
[d] Ryazan State Radio Engineering University named after V.F. Utkin, Ryazan, Russian Federation
Address: 59/1 Gagarin St., Ryazan 390005, Russian Federation
[*] promasevich@dlink.ru

Abstract
Significant part of attacks on corporate information communications is occupied by attempts to violate the integrity and availability of information by destabilizing the network infrastructure. Since malicious actions in this direction can occur at different levels of the OSI model and proceed mainly from "internal" violators, the article focuses on the integrated application of the security functionality of the network infrastructure built into the software of the active network equipment of D-Link. The work describes the components of the security functionality of the network infrastructure and their positioning in terms of the feasibility of using them at the levels of the network hierarchy. The trunk level security functions are provided by means of improving network fault tolerance in case of cable breaks, delimitation and filtering of traffic according to various criteria, protection of switches from unauthorized access and their CPU, control of connection of network nodes based on analysis of their IP/MAC/port and their authentication based on connection ports and MAC addresses. The gateway level security tools are represented by a new line of service routers for the SMB sector with domestic software, which ensures independence from foreign developers and timely development of their functionality in accordance with industry trends. These devices combine the functions of a router, firewall, configurable switch and server of a number of network protocols. The new blocking feature effectively blocks advertisements that occur when browsing the web. D-Link service routers support the Russian content filtering service SkyDNS, which offers additional opportunities to organize secure Internet access.

Keywords: orporate networks, security, switches, malicious activities, Port Security, Traffic Segmentation, VLAN, IP-MAC-Port Binding, authentication, access control lists, Safeguard Engine, CPU Interface Filtering, ERPS, LoopBackDetect, service routers, VPN, medium business, small business, Russian software

Conflict of intersts: The authors declare no conflict of interests.

For citation: Romasevich P.V., Smirnova E.V., Shibanov V.A. Ensuring the Security of Corporate Networks Based on D-Link Equipment. *Modern Information Technologies and IT-Education.* 2023;19(2):430-437.

Актуальность обеспечения информационной безопасности на современном этапе обусловлена возрастающей зависимостью общества от стабильности функционирования инфокоммуникационных сетей. Текущая ситуация характеризуется высокими темпами роста парка компьютеров, мобильных устройств и сервисов, числа пользователей удаленных вычислительных ресурсов, значительным увеличением объемов информации, уязвимостями программного обеспечения, внедрением Интернета вещей в различные сферы жизнедеятельности, а также все более глубоким проникновением сети Интернет в регионы [1-5].При этом темпы развития и внедрения средств информационной безопасности зачастую отстают от темпов роста средств инфокоммуникаций и изощренности инструментария злоумышленников[1] [6].

При разработке концепции информационной безопасности обычно подразумеваются нарушения конфиденциальности и целостности информации и обсуждается защита внешнего и внутреннего периметра сети. Однако целью злоумышленника также может быть полное или частичное нарушение работоспособности сетевой инфраструктуры. Результатом данных действий может быть выход из строя или нестабильная работа ее компонентов, что может повлечь за собой отказы в обслуживании или некорректную работу прикладного программного обеспечения и тем самым нанести ущерб деятельности организации [7, 8]. Важность момента отражает тот факт, что по состоянию на 2021 год в РФ доля средств защиты сетевой инфраструктуры по отношению ко всем категориям защиты инфокоммуникационных систем составила ~45 %[2] .

Корпоративные сети любого масштаба являются объектом атак как со стороны «внешних», так и «внутренних» злоумышленников. Как показывают исследования, большая часть возможных угроз приходится на долю «внутренних» нарушителей, которые имеют доступ к инфраструктуре корпоративной сети: неумышленные действия персонала (~50 %), действия недовольных сотрудников (~10 %) и их корыстные побуждения (~10 %)[3] [9, 10].

Нестабильность сетевой инфраструктуры может выражаться в повреждении кабельной среды передачи данных и нарушении корректной работы активного сетевого оборудования вследствие несанкционированного доступа к нему или определенным сегментам сети [11].

Находясь внутри корпоративной сети, злоумышленник, помимо нарушения физической целостности инфраструктуры, может выполнять действия, направленные на получение контроля над компьютерными системами. К этим действиям относятся прослушивание (sniffing) и подмена (spoofing) сетевой информации, организация переполнения таблиц коммутации, подбор паролей, перехват сеансов, атаки типа «отказ в обслуживании» (DoS), нарушение нормальной работы протоколов канального уровня [12].

Основу современных корпоративных сетей составляют коммутаторы. Современные коммутаторы поддерживают разнообразный функционал обеспечения безопасности сетевой инфраструктуры на первых четырех уровнях модели OSI. Поскольку основными целями обеспечения сетевой безопасности являются конфиденциальность, целостность и доступность информации, то для их реализации в корпоративной сети целесообразно комплексно применять доступные функции безопасности коммутаторов[4] .

Функции обеспечения безопасности активного сетевого оборудования D-Link в целом можно разделить на несколько групп, каждая из которых включает несколько отдельных инструментов[5]:

- защита коммутатора от несанкционированного доступа;
- функции повышения отказоустойчивости сети;
- разграничение трафика;
- фильтрация трафика с помощью списков управления доступом;
- контроль над подключением сетевых узлов к коммутатору;
- защита ЦПУ коммутатора;
- аутентификация клиентов на основе портов подключения и MAC-адресов.

Комплексное решение компании D-Link по обеспечению сетевой безопасности включает:

- безопасность на уровне шлюза;
- безопасность на уровне конечных пользователей;
- безопасность на уровне магистрали сети.

Безопасность на уровне шлюза обеспечивается наличием межсетевого экрана, систем предупреждения и обнаружения вторжений, а также антивирусом шлюза. Безопасность на уровне конечных пользователей предполагает наличие на рабочем месте персонального межсетевого экрана и антивируса. Безопасность на уровне магистрали предполагает наличие средств безопасности не только в устройствах ядра и агрегации, но и в устройствах уровня доступа сети, к которому непосредственно подключаются пользователи [13].На уровнях ядра и агрегации иерархии сети актуальны:

- защита коммутатора от несанкционированного доступа;
- функции повышения отказоустойчивости сети;
- защита ЦПУ коммутатора.

Коммутаторы уровня доступа современных сетей уже не являются лишь устройствами, соединяющими пользователей с сетью, а выполняют ряд интеллектуальных функций:

- контроль над подключением сетевых узлов к коммутатору;
- разграничение трафика;фильтрацию трафика с помощью списков управления доступом;
- аутентификацию клиентов на основе портов подключения и MAC-адресов;
- контроль над полосой пропускания на основе портов и потоков.

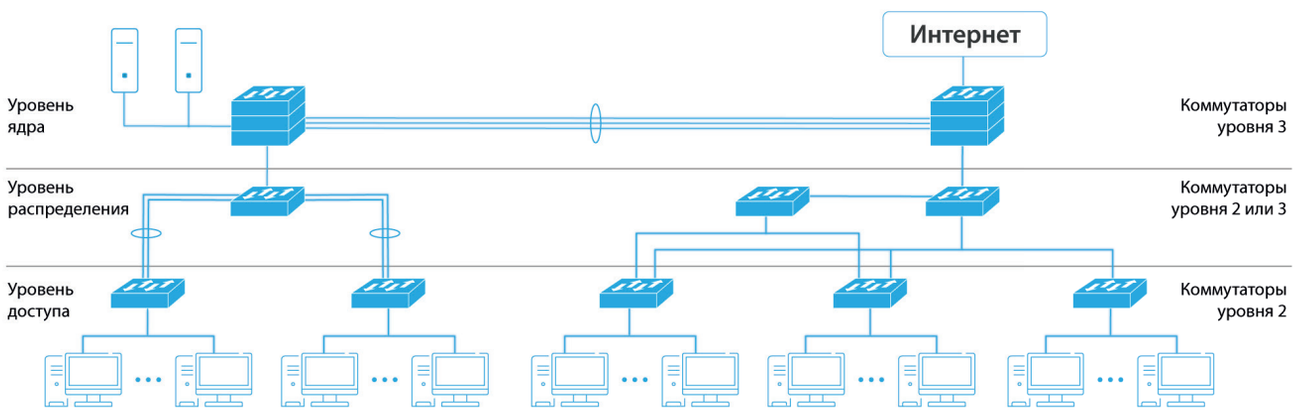
[1] Cybersecurity trends: Looking over the horizon / J. Boehm [et al.] // McKinsey. March 10, 2022. [Электронный ресурс]. URL: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon (дата обращения: 07.02.2023).

[2] Прогноз развития рынка кибербезопасности в Российской Федерации на 2022-2026 годы. М. : Фонд «Центр стратегических разработок», 2022. 14 с. [Электронный ресурс]. URL: https://www.csr.ru/upload/iblock/13f/ufleu9rg5zc3ldu66srqt3a89j0mrve5.pdf (дата обращения: 07.02.2023).

[3] Биячуев Т. А. Безопасность корпоративных сетей : учеб. пособие / Под ред. Л. Г. Осовецкого. СПб. : СПбГУ ИТМО, 2004. 161 с.

[4] Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с англ. Д. А. Беликова. М. : ДМК Пресс, 2020. 326 с.

[5] ООО «Д-Линк Трейд» : официальный сайт [Электронный ресурс]. URL: https://www.dlink.ru (дата обращения: 07.02.2023).



Р и с. 1. Трехуровневая иерархическая модель корпоративной сети

F i g. 1. Three-level hierarchical corporate network model

Компания D-Link предлагает широкую линейку управляемых коммутаторов второго (L2) и третьего (L3) уровня, оптимальных по критерию «цена/функционал», обладающих различной производительностью и развитыми возможностями, комплексное применение которых позволяет обеспечить сетевую безопасность на различных уровнях иерархии сети].

Одним из распространенных методов разграничения доступа к сетевым ресурсам и разделения пользователей на изолированные группы независимо от их места подключения к сети является использование **виртуальных локальных сетей** (VLAN), описанных в стандарте IEEE 802.1Q[6]. Данный подход повышает уровень сетевой безопасности и позволяет локализовать широковещательный трафик внутри групп, что в целом положительно влияет на полезную пропускную способность сети. VLAN 802.1Q ––это широковещательный домен, внутри которого кадры передаются по технологии коммутации. Технология частных VLAN (Private VLAN, PVLAN), определенная в RFC 5517, позволяет увеличить количество VLAN, но при этом эффективно использовать идентификаторы VLAN и IP-адреса, повысить безопасность. Ее можно применять в тех случаях, когда необходимо изолировать трафик разных клиентов или разделить разные типы трафика [14]

Также для разграничения трафика на канальном уровне может использоваться функция **Traffic Segmentation** (сегментация трафика). С помощью программной настройки она позволяет изолировать порты или группы портов коммутатора друг от друга, но в то же время обеспечивает доступ к разделяемым портам, служащим для подключения серверов или магистрали сети. В корпоративной сети функция может использоваться для защиты трафика отделов, работающих с критически важной информацией или для изоляции потенциально опасных отделов от остальной сети [15].

В том случае, если какой-либо порт коммутатора активен, к нему может подключиться злоумышленник и получить несанкционированный доступ к сети: этот пользователь может начать генерировать вредоносный трафик, который создаст проблемы в сети [16, 17]. Для защиты от подобных ситуаций, а также для контроля подключения узлов к портам коммутаторы D-Link предоставляют функции безопасности, которые позволяют указывать MAC- и/или IP -адреса устройств, которым разрешено подключаться к данному порту, и блокировать доступ к сети узлам с неизвестными коммутатору адресами.

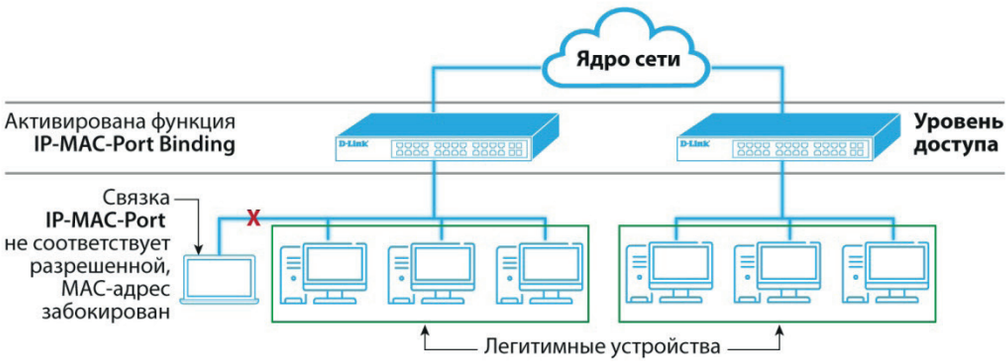
Функция **Port Security** используется для контроля доступа устройств к портам коммутаторов. Для идентификации устройств, которым разрешено подключаться к порту, используются их MAC-адреса. Коммутатор получает информацию о MAC-адресах в результате их динамического изучения портами или ручной настройки администратором [18]. С целью повышения контроля над количеством подключаемых к порту устройст, можно настроить ограничение по количеству изучаемых им MAC-адресов. Функция Port Security служит для борьбы с атаками типа MAC Flooding, MAC Spoofing.

Функция **IP-MAC-Port Binding** (IMPB) позволяет фильтровать пакеты и таким образом контролировать доступ в сеть устройств, подключенных к коммутатору. При настройке функции порт будет проверять, идентичны ли MAC- и IP-адреса источника входящих пакетов параметрам, хранящимся на коммутаторе записей, связывающих MAC- и IP-адреса клиентских устройств с портами, и VLAN подключения:

- если все составляющие (IP/MAC-адреса, порт, VLAN) совпадают, пакеты будут передаваться, и клиенты получат доступ в сеть;
- если все составляющие частично или полностью не совпадают, коммутатор заблокирует MAC-адрес соответствующего узла с занесением его в «черный лист».

Функция IMPB позволяет бороться с атаками типа ARP Spoofing и атаками на протокол DHCP.

[6] IEEE Standard for Local and Metropolitan Area Networks-Bridges and Bridged Networks: IEEE Std 802.1Q-2022 (Revision of IEEE Std 802.1Q-2018. 22 Dec. 2022. 2163 p. https://doi.org/10.1109/IEEESTD.2022.10004498



Р и с. 2. Принцип работы функции IP-MAC-Port Binding
F i g. 2. How the IP-MAC-Port Binding function works

Стандарт IEEE 802.1X осуществляет контроль доступа и не позволяет неавторизованным устройствам подключаться к локальной проводной или беспроводной сети через порты устройства связи[7]

В коммутаторах D-Link реализованы два режима аутентификации IEEE 802.1X:

- аутентификация 802.1X на основе портов: для получения доступа к сети любого компьютера, подключенного к порту, он должен быть авторизован
- аутентификация 802.1X на основе MAC-адресов: аутентификация множества клиентов на одном физическом порту коммутатора. Каждый узел должен проходить аутентификацию индивидуально для доступа к порту.

Списки управления доступом (Access Control List, ACL) осуществляют фильтрацию потоков данных на аппаратном уровне. Они представляют собой упорядоченный набор условий проверки параметров пакетов данных. Когда сообщения поступают на входной порт, коммутатор проверяет параметры пакетов данных на совпадение с критериями фильтрации, определенными в ACL. Результатом проверки является одно из действий над пакетом: Permit (Разрешить) или Deny (Запретить). Фильтрация трафика может быть осуществлена по различным критериям: номеру порта коммутатора, IP или MAC-адресу пользователя, типу кадров Ethernet и протокола вышестоящих уровней, идентификатору VLAN, приоритету пакета и типу приложения [19].

ACL используются для:

- ограничения типов приложений, разрешенных для использования в сети;
- контроля доступа пользователей к сети;
- классификации и маркировки пакетов для реализации требуемой политики QoS.

Следующая группа функций обеспечивает сетевую безопасность путем поддержки работоспособности корпоративной сети при перегрузках ЦПУ коммутаторов и изменении ее топологии

В современных корпоративных сетях передается много различного служебного трафика, который всегда обрабатывается на ЦПУ– административный доступ, включая доступ через Web-интерфейс, SNMP-запросы, пакеты протоколов STP/RSTP/MSTP, IGMP, пакеты с неизвестным IP-адресом назначения и т. д. Весь этот трафик может при определенных условиях перегрузить ЦПУ коммутатора, что фактически означает отказ оборудования. Функция **Safeguard Engine** позволяет сохранить функциональность коммутатора при сканировании сети или вирусных атаках. Принцип ее действия основан на идентификации и приоритизации трафика, направляемого для обработки на ЦПУ [20].

Функция **CPU Interface Filtering** использует программные ACL для фильтрации пакетов, поступающих для обработки на ЦПУ. Программные ACL обладают аналогичными аппаратным ACL принципами работы и конфигурации. Функция CPU Interface Filtering использует для своей работы центральный процессор. В случае сильной атак, его ресурсы будут целиком задействованы для фильтрации вредоносного трафика, что станет причиной снижения производительности коммутатора. С целью минимизации влияния сетевых атак на ЦПУ коммутатора D-Link рекомендуется одновременно настраивать функции Safeguard Engine и CPU Interface Filtering.

Для обеспечения отказоустойчивости сети в случае образования петель коммутации на неуправляемых сегмента, неотъемлемой частью функционала коммутаторов является механизм **LoopBackDetect**, блокирующий порт коммутатора, к которому подключен сегмент с петлей или VLAN, в которой обнаружена петля.

Для распределенных сетей большое значение имеет отказоустойчивость при нарушении целостности кабельной инфраструктуры. Отказоустойчивость достигается за счет резервирования каналов связи, что может привести к образованию петель. Протоколы **STP/RSTP/MSTP** предназначены для устранения образования петель и повышения отказоустойчивости в сетях Ethernet произвольных топологий. Технология **Ethernet Ring Protection Switching** (ERPS) реализует механизмы защиты от петель коммутации в сетях Ethernet с кольцевой топологией, обеспечивая при этом отказоустойчивость сети. По сравнению с протоколами xST, она обладает чрезвычайно малым временем восстановления связи при отказе одной из линий в кольце [21, 22].

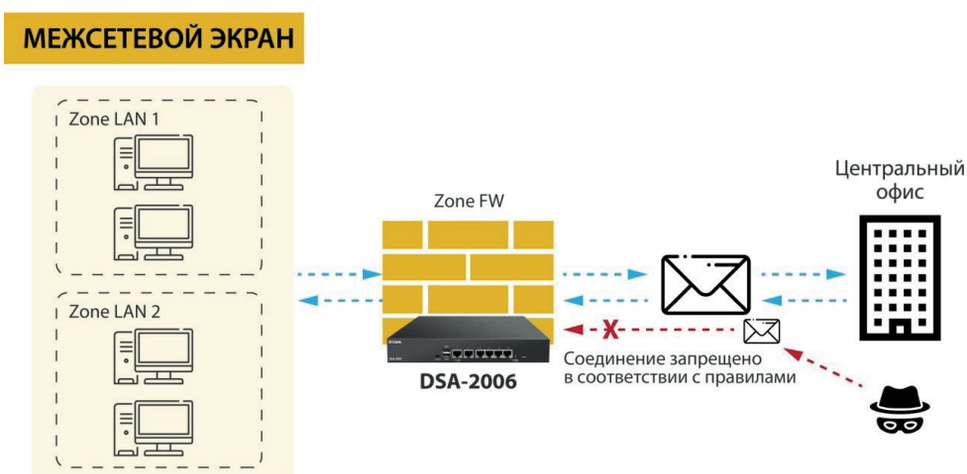
[7] IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control: IEEE Std 802.1X-2004 (Revision of IEEE Std 802.1X-2001). 13 Dec. 2004. 175 p. https://doi.org/10.1109/IEEESTD.2004.96095

Изучить упомянутый функционал безопасности активного сетевого оборудования [23] можно с помощью портала дистанционного обучения D-Link[8] и ряда учебных пособий, изданных с участием компании[9] [24, 21].

Решение задачи обеспечения сетевой безопасности для малого и среднего бизнеса

Все перечисленные проблемы информационной безопасности корпоративных сетей актуальны и для малого и среднего бизнеса. В то же время в малом и среднем бизнесе часто нет возможности применять сложные и многоуровневые средства обеспечения безопасности компьютерных сетей. Компания D-Link предлагает комплексное решение задач информационной безопасности малого и среднего бизнеса — **сервисные маршрутизаторы с настраиваемыми портами D-Link DSA-2003 и D-Link DSA-2006**].

Данные устройства объединяют в себе функции маршрутизатора, межсетевого экрана, настраиваемого коммутатора и сервера ряда сетевых протоколов.



Р и с. 3. Применение сервисного маршрутизатора в сети организации
F i g. 3. Application of a service router in an organization's network

Встроенный межсетевой экран поддерживает разделение сети на **зоны**. **Зоной** называется логическая область сети с одинаковыми уровнями доверия. Поддерживается настройка **политик для взаимодействия зон** и правил фильтрации трафика с широким выбором параметров, что дает большую гибкость при решении задач обеспечения безопасности сети. Правила фильтрации трафика могут применяться по расписанию.

Рассматриваемые нами сервисные маршрутизаторы позволяют настраивать принадлежность Ethernet-портов к сети LAN или WAN. У D-Link DSA-2003 таких портов три, у D-Link DSA-2006 — шесть. Все порты поддерживают скорость передачи данных 1 Гбит/с

Маршрутизаторы позволяют строить территориально распределенные корпоративные сети, устанавливая VPN-соединения с удаленными сетями или отдельными удаленными сетевыми компьютерами на базе протоколов IPsec (IKEv1/IKEv2), L2TP over IPsec, PPTP/L2TP, GRE, IPIP, EoGRE, также поддерживаются неуправляемые L2TPv3-туннели.

Поддержка протокола SSH позволяет выполнять безопасную удаленную настройку и управление маршрутизаторами с шифрованием передаваемого трафика и выполнения безопасной процедуры авторизации.

Маршрутизаторы D-Link DSA-2003 и D-Link DSA-2006 имеют по два порта USB, что позволяет подключать:

- USB-модем стандарта GSM/LTE для подключения корпоративной сети к сети Интернет через сети сотовых операторов связи
- USB-накопитель, для организации внутреннего сетевого хранилища данных, при этом поддерживаются встроенный сервер Samba/FTP/DLNA и учетные записи пользователей для доступа к накопителю
- принте, для организации сетевого доступа к нему.

Маршрутизаторы поддерживают работу с российским сервисом контентной фильтрации SkyDNS], который предлагает больше настроек и возможностей для организации безопасной работы в Интернете как для домашних пользователей

[8] Портал дистанционного обучения D-Link [Электронный ресурс] // ООО «Д-Линк Трейд», 2023. URL: https://learn.dlink.ru (дата обращения: 07.02.2023).

[9] Технологии коммутации и маршрутизации в локальных компьютерных сетях / Е. В. Смирнова, А. В. Пролетарский, Е. А. Ромашкина [и др.]. М. : Изд-во МГТУ им. Н.Э. Баумана, 2013. 392 с. EDN: ZCKZRF; Технологии современных беспроводных сетей Wi-Fi / Е. В. Смирнова, А. В. Пролетарский, Е. А. Ромашкина [и др.]. М. : Изд-во МГТУ им. Н.Э. Баумана, 2016. 448 с. EDN: YQUMUH; Смирнова Е. В., Пролетарский А. В., Ромашкина Е. А. Технологии TCP/IP в современных компьютерных сетях. Вып. 3. М. : Изд-во МГТУ им. Н. Э. Баумана, 2019. 550 с. EDN: MKOZXF; Лапонина О. Р. Основы сетевой безопасности. Часть 1. Межсетевые экраны : учеб. пособие для вузов. М.: ИНТУИТ, 2014. 310 с.; Лапонина О. Р. Основы сетевой безопасности. Часть 2. Технологии туннелирования : учеб. пособие для вузов. М.: ИНТУИТ, 2014. 290 с.

всех возрастных категорий, так и для профессиональной деятельности сотрудников офисов и предприятий.
Новая функция маршрутизаторов по блокировке рекламы поможет эффективно блокировать рекламные объявления, возникающие при просмотре web-страниц.
Программное обеспечение сервисных маршрутизаторов D-Link DSA-2003 и D-Link DSA-2006 полностью **разработано российским офисом** компании D-Link, что исключает зависимость от иностранных поставщиков программного обеспечения.

О компании D-Link

Компания D-Link является ведущим мировым производителем сетевого оборудования, предлагающим широкий набор решений для создания локальных сетей Fast Ethernet/Gigabit Ethernet/10GE/25GE/ 40GE/100GE, построения беспроводных сетей и организации широкополосного доступа, передачи изображений и голоса по IP (VoIP). В РоссиФ офисы компании D-Link открыты в Москве, Санкт-Петербурге, Екатеринбурге, Калининграде, Кемерово, Краснодаре, Красноярске, Новосибирске, Перми, Ростове-на-Дону, Рязани, Самаре, Уфе, Хабаровске и Ярославле. В Брянске, Казани и Челябинске работают региональные представители компании.
Авторизованные учебные центры работают в Москве, Санкт-Петербурге, Екатеринбурге, Ижевске, Кемерово, Магнитогорске, Новосибирске, Омске, Кемерово, Красноярске, Хабаровске, Перми, Ростове-на-Дону, Рязани, Туле и Ярославле[10].

References

[1] Kavak H., Padilla J.J., Vernon-Bido D., Diallo S.Y., Gore R., Shetty S. Simulation for cybersecurity: state of the art and future directions. *Journal of Cybersecurity*. 2021;7(1):tyab005. https://doi.org/10.1093/cybsec/tyab005
[2] Gunduz M.Z., Das R. Cyber-security on smart grid: threats and potential solutions. *Computer Networks*. 2020;169:107094. https://doi.org/10.1016/j.comnet.2019.107094
[3] Kaur J., Ramkumar K.R. The recent trends in cyber security: a review. Journal of King Saud University – *Computer and Information Sciences*. 2022;34(8)B:5766-5781. https://doi.org/10.1016/j.jksuci.2021.01.018
[4] Tonge A.M. Cyber security: challenges for society – literature review. *IOSR Journal of Computer Engineering*. 2013;12(2):67-75. https://doi.org/10.9790/0661-1226775
[5] Rodosek G.D., Golling M. Cyber Security: Challenges and Application Areas. In: Essig M., Hülsmann M., Kern E.M., Klein-Schmeink S. (eds.) Supply Chain Safety Management. *Lecture Notes in Logistics*. Berlin, Heidelberg: Springer; 2013. p. 179-197. https://doi.org/10.1007/978-3-642-32021-7_11
[6] Giannaros A., Karras A., Theodorakopoulos L., Karras C., Kranias P., Schizas N., Kalogeratos G., Tsolis D. Autonomous Vehicles: Sophisticated Attacks, Safety Issues, Challenges, Open Topics, Blockchain, and Future Directions. *Journal of Cybersecurity and Privacy*. 2023;3(3):493-543. https://doi.org/10.3390/jcp3030025
[7] Borky J.M., Bradley T.H. Protecting Information with Cybersecurity. In: Effective Model-Based Systems Engineering. Cham: Springer; 2019. p. 345-404. https://doi.org/10.1007/978-3-319-95669-5_10
[8] Al-Hamami A.H., Al-Saadoon G.M. Security Concepts, Developments, and Future Trends. In: Al-Hamami A.H., Al-Saadoon G.M. (eds.) Handbook of Research on Threat Detection and Countermeasures in Network Security. Hershey, PA: IGI Global, 2015. p. 1-16. https://doi.org/10.4018/978-1-4666-6583-5.ch001
[9] Li Y., Liu Q. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*. 2021;7:8176-8186. https://doi.org/10.1016/j.egyr.2021.08.126
[10] Tariq U., Ahmed I., Bashir A.K., Shaukat K. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*. 2023;23(8):4117. https://doi.org/10.3390/s23084117
[11] Aghmadi A., Hussein H., Polara K.H., Mohammed O. A Comprehensive Review of Architecture, Communication, and Cybersecurity in Networked Microgrid Systems. *Inventions*. 2023;8(4):84. https://doi.org/10.3390/inventions8040084
[12] Funmilola A., Oluwafemi A. Review of Computer Network Security System. *Network and Complex Systems*. 2015;5(5):40-46. Available at: https://iiste.org/Journals/index.php/NCS/article/view/22825 (accessed 07.02.2023).
[13] Ahmad Z., Khan A.S., Shiang C.W., Abdullah J., Ahmad F. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*. 2021;32(1):e4150. https://doi.org/10.1002/ett.4150
[14] Ding P.Q., Holliday J.N., Celik A. Improving the security of wireless LANs by managing 802.1x disassociation. In: First IEEE Consumer Communications and Networking Conference, CCNC 2004. Las Vegas, NV, USA; 2004. p. 53-58. https://doi.org/10.1109/CCNC.2004.1286832
[15] Protect the Data. Ch. 6. In: Andress J., Leary M. (eds.) Building a Practical Information Security Program. Syngress; 2017. p. 103-123. https://doi.org/10.1016/B978-0-12-802042-5.00007-X

[10] Информацию о новинках, решениях и новостях D-Link можно найти на официальном сайте компании, странице «ВКонтакте», а также каналах в YouTube и Telegram. ООО «Д-Линк Трейд» : официальный сайт [Электронный ресурс]. URL: https://www.dlink.ru (дата обращения: 07.02.2023); D-Link Russia [Электронный ресурс] // В Контакте, 2023. URL: https://vk.com/dlink.international (дата обращения: 07.02.2023); D-Link Russia [Электронный ресурс] // YouTube, 2023. URL: https://www.youtube.com/user/DLinkMoscow (дата обращения: 07.02.2023); D-Link Russia [Электронный ресурс] // Telegram, 2023. URL: https://t.me/dlink_ru (дата обращения: 07.02.2023).

[16] Aslan Ö., Aktuğ S.S., Ozkan-Okay M., Yilmaz A.A., Akin E. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*. 2023;12(6):1333. https://doi.org/10.3390/electronics12061333

[17] Mavrommatis K. Confronting and intrusion detection techniques of cyber-attacks in wired and wireless communication networks. In: Proceedings of the 26th Pan-Hellenic Conference on Informatics (PCI '22). New York, NY, USA: Association for Computing Machinery; 2023. p. 290-295. https://doi.org/10.1145/3575879.3576007

[18] Girdler T., Vassilakis V.G. Implementing an intrusion detection and prevention system using Software-Defined Networking: Defending against ARP spoofing attacks and Blacklisted MAC Addresses. *Computers & Electrical Engineering*. 2021;90:106990. https://doi.org/10.1016/j.compeleceng.2021.106990

[19] Frustration Strategies: Technical Controls. Ch. 5. In: Shimeall T.J., Spring J.M. (eds.) Introduction to Information Security: A Strategic-Based Approach. Syngress; 2014. p. 83-106. https://doi.org/10.1016/B978-1-59749-969-9.00005-5

[20] Abu Bakar R., Kijsirikul B. Enhancing Network Visibility and Security with Advanced Port Scanning Techniques. *Sensors*. 2023;23(17): 7541. https://doi.org/10.3390/s23177541

[21] Ryoo J.-d., Long H., Yang Y., Holness M., Ahmad Z., Rhee J.K. Ethernet ring protection for carrier ethernet networks. *IEEE Communications Magazine*. 2008;46(9):136-143. https://doi.org/10.1109/MCOM.2008.4623718

[22] Nakayama Y., Sezaki K. Per-Flow Throughput Fairness in Ring Aggregation Network with Multiple Edge Routers. *Big Data and Cognitive Computing*. 2018;2(3):17. https://doi.org/10.3390/bdcc2030017

[23] Matusa R., Butkus L., Krilavičius T., Man K.L., Liang H. Improving the teaching of Computer Networks through the incorporation of industry based training courses. In: *Proceedings of 2013 IEEE International Conference on Teaching, Assessment and Learning for Engineering (TALE)*. Bali, Indonesia: IEEE Computer Society; 2013. p. 325-328. https://doi.org/10.1109/TALE.2013.6654454

[24] Zakharov P.A., Romasevich P.V., Smirnova E.V., Shibanov V.A. D-Link Comprehensive Training Solution for Networking Professionals. *Modern Information Technologies and IT-Education*. 2020;16(3):776-787. (In Russ., abstract in Eng.) https://doi.org/10.25559/SITITO.16.202003.776-787

[25] Zakharov P.A., Romasevich P.V., Smirnova E.V. D-Link Solutions for Modern Computer Networks and Specialists Education in the Sphere of Network Technologies. *Modern Information Technologies and IT-Education*. 2019;15(4):894-904. (In Russ., abstract in Eng.) https://doi.org/10.25559/SITITO.15.201904.894-904

Поступила 07.02.2023; одобрена после рецензирования 16.04.2023; принята к публикации 20.05.2023.
Submitted 07.02.2023; approved after reviewing 16.04.2023; accepted for publication 20.05.2023.

Об авторах:

Ромасевич Павел Владимирович, доцент кафедры телекоммуникационных систем, ФГАОУ ВО «Волгоградский государственный университет» (400062, Российская Федерация, г. Волгоград, пр. Университетский, д. 100), кандидат технических наук, **ORCID: https://orcid.org/0000-0002-3206-2260**, promasevich@dlink.ru

Смирнова Елена Викторовна, менеджер по образовательным проектам, ООО «Д-Линк Трейд» (129626, Российская Федерация, г. Москва, Графский переулок, д. 14, к. 1), кандидат технических наук, **ORCID**: **https://orcid.org/0000-0001-7823-0701**, esmirnova@dlink.ru

Шибанов Владимир Александрович, консультант по образовательным проектам, ООО «Д-Линк Трейд» (390043, Российская Федерация, г. Рязань, пр-д Шабулина, д. 16), доцент кафедры систем автоматизированного проектирования вычислительных средств, ФГБОУ «Рязанский государственный радиотехнический университет имени В.Ф. Уткина» (390005, Российская Федерация, г. Рязань, ул. Гагарина, д. 59/1), кандидат технических наук, **ORCID: https://orcid.org/0000-0002-2389-4815**, vshibanov@dlink.ru.

Все авторы прочитали и одобрили окончательный вариант рукописи.

About the authors:

Pavel V. Romasevich, Associate professor of Department of "Telecommunication systems" Volgograd State University (100 Universitetsky Ave., Volgograd 400062, Russian Federation), Cand. Sci. (Eng.), **ORCID: https://orcid.org/0000-0002-3206-2260**, promasevich@dlink.ru

Elena V. Smirnova, Education Project Manager, D-Link Company (14-1 Grafskij per., Moscow 129626, Russian Federation), Cand. Sci. (Eng.), **ORCID: https://orcid.org/0000-0001-7823-0701**, esmirnova@dlink.ru

Vladimir A. Shibanov, Education Project Consultant, D-Link Company (16 Shabulin's pas., Ryazan 390043, Russian Federation); associate professor of Department of Systems of Automated Design of Computational Tools, Ryazan State Radio Engineering University (59/1 Gagarina St., Ryazan 390005, Russian Federation), Cand. Sci. (Eng.), **ORCID: https://orcid.org/0000-0002-2389-4815**,uvshibanov@dlink.ru

All authors have read and approved the final manuscript.