Н. Е. Бриль, А. М. Шабалин
Тюменский государственный университет, г. Тюмень
УДК 004.732

ОРГАНИЗАЦИЯ ЗАЩИТЫ СЕТИ ПРЕДПРИЯТИЯ СРЕДСТВАМИ МЕЖСЕТЕВОГО ЭКРАНА НОВОГО ПОКОЛЕНИЯ

Аннотация. *В статье рассмотрены способы организации защиты сети предприятия средствами межсетевых экранов нового поколения, а также — проанализированы современные мировые производители данного класса телекоммуникационного оборудования. Результатом работы стала модель компьютерной сети предприятия с применением защиты периметра компьютерной сети предприятия.*
Ключевые слова: *NGFW, UTM, Huawei, eNSP.*

Введение. С развитием технологий построения компьютерных сетей растет также и количество всевозможных уязвимостей, которые могут эксплуатировать злоумышленники для нарушения конфиденциальности информации, передаваемой между компьютерами, поэтому вопрос обеспечения безопасности сетей предприятий с каждым днем становится все актуальнее.

В современных условиях данный вопрос решается разными способами: разработкой средств обеспечения безопасности на основе операционных систем семейства Windows [1] или использованием технологии частных виртуальных систем (Virtual Private Network, VPN) [2]. Также основной упор делается на защиту корпоративной сети при администрировании операционных систем семейства Linux [3]. Однако ни один из предложенных подходов не позволяет достичь должного уровня безопасности от современных угроз компьютерной сети, возникающих на ее периметре — точке подключения к сети Интернет.

Проблема исследования. Защита периметра компьютерной сети средствами современными межсетевыми экранами (Next-Generation Firewall, NGFW) является достаточно сложным и комплексным процессом, поэтому были выделены несколько задач:

1) изучить функциональные особенности NGFW;

2) сравнить NGFW с другими средствами обеспечения сетевой безопасности;

3) проанализировать возможности NGFW от различных мировых производителей;

4) смоделировать компьютерную сеть организации, использующую NGFW, в программном эмуляторе.

Материалы и методы. Методами данного исследования стали: наблюдение, сравнение, эксперимент, измерение и абстрагирование. Для эмуляции компьютерной сети было выбрано программное средство Huawei eNSP 1.3.00.100.

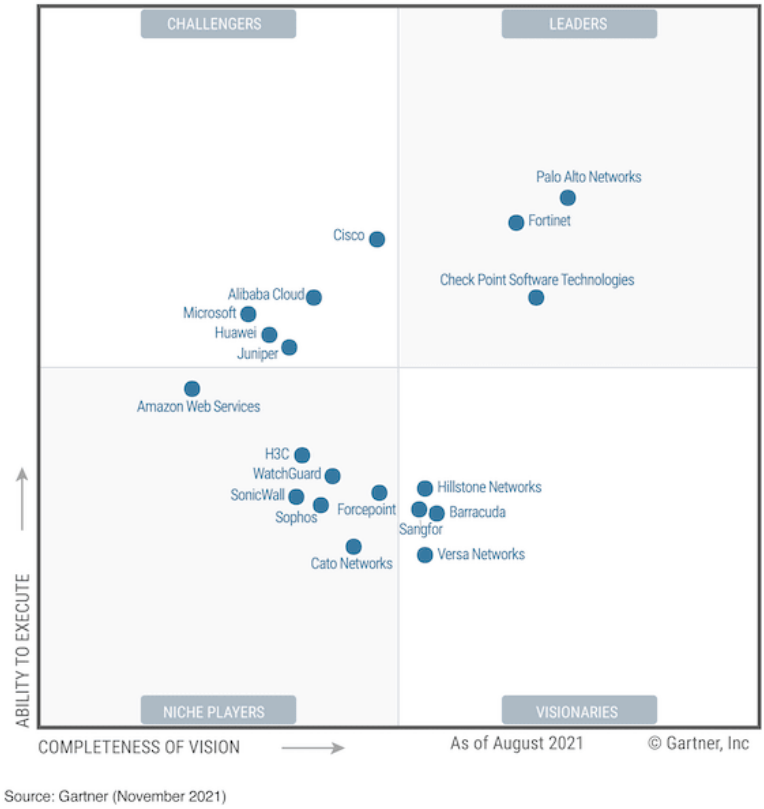
Результаты. Межсетевой экран (МСЭ, файрволл, брандмауэр) — это устройство сетевой безопасности, которое позволяет отслеживать трафик на разных участках сети и принимать решения о его разрешении или блокировке, основываясь на заранее созданных на нем политик безопасности [4]. На протяжении долгого времени МСЭ являются базовыми компонентами обеспечения сетевой безопасности, а также — барьерами между контролируемыми внутренними (доверенными) сетями и ненадежными внешними сетями типа Internet.

NGFW помимо указанных функций расширилось за счет ряда нововведений: глубокая проверка пакетов (Deep Packet Inspection, DPI), идентификация приложений, а также систем обнаружения и предотвращения вторжений (Intrusion Prevention Detection System, IPDS) [5].

Универсальный шлюз безопасности (Unified Threat Management, UTM) представляет собой многофункциональное средство, созданное на основе традиционного МСЭ, но включающее в себя функции IPDS, VPN и других сервисов безопасности. Фактически, система UTM имеет схожую функциональность с NGFW, но обладает в свою очередь такими недостатками, как довольно низкая производительность, а также то, что малейший сбой в работе может привести к отказу сразу всех защитных сервисов, работающих на устройстве. Таким образом, NGFW являются наиболее приоритетным вариантом сетевого оборудования, для организации защиты сети.

Для сравнения мировых производителей, поставляющих NGFW, был рассмотрен так называемый магический квадрант Гартнера для МСЭ (рис. 1) [6].

Figure 1: Magic Quadrant for Network Firewalls



Source: Gartner (November 2021)

Рис. 1. Магический квадрант Гартнера для МСЭ

Из данного квадранта видно, что лидерами и претендентами являются такие компании, как Cisco, Huawei, Fortinet, Check Point, Palo Alto и другие. Исходя из этого была составлена сравнительная таблица крупнейших поставщиков NGFW, основные различия которых представлены в табл. 1.

Таблица 1

Сравнение мировых производителей NGFW

	Cisco Systems	*Check Point Software Technologies*	*Fortinet*	*Huawei Technologies*	*Palo Alto Networks*
Сертификат ФСТЭК	Есть	Есть	Есть	Есть	Нет
Алгоритмы симметричного шифрования семейства *ES	+	+ NSA	+ SEED, ARIA	+ SM1, SM4	+
Поддержка L2TP	Нет	Есть	Есть	Есть	Нет
Проприетарные технологии VPN	Нет	Нет	Нет	Есть	Есть
Маршрутизация	BGP, OSPF, IS-IS, EIGRP, PIM-SM	RIP, RIPng, OSPF, BGP, OSPFv3, IGMP, PIMv4/v6	RIPv1/v2, RIPng, OSPF, OSPFv3, IS-IS, BGP-4	RIP, RIPng, OSPF, BGP, OSPFv3, IGMP, EVPN, L3 VPN	OSPFv2/v3, RIP, BGP
DNS-прокси	Есть	Нет	Есть	Есть	Есть
HTTP-прокси	Нет	Есть	Есть	Есть	Нет
Количество контролируемых сетевых приложений	5000	8000	3000	6000	3145
Количество категорий URL-адресов	80	114	75	138	75

Исходя из представленных результатов, а также опираясь на условия нынешней ситуации, когда многие зарубежные компании уходят с рынка России, мы остановили свой выбор на компании Huawei, сетевые устройства которых хорошо эмулируются с помощью программного средства eNSP.

Для реализации базовых настроек NGFW была спроектирована упрощенная топология сети малого предприятия, включающая в себя устройства, находящиеся в доверенной (trust), недоверенной (untrust) и демилитаризованной (DMZ) зонах (рис. 2).

На рис. 2 представлен NGFW, названный FW1, на котором были произведены следующие базовые настройки: зоны безопасности (trust, untrust и DMZ), политики безопасности и NAT (Network Address Translation). Результат функционирования NGFW представлен на рис. 3.

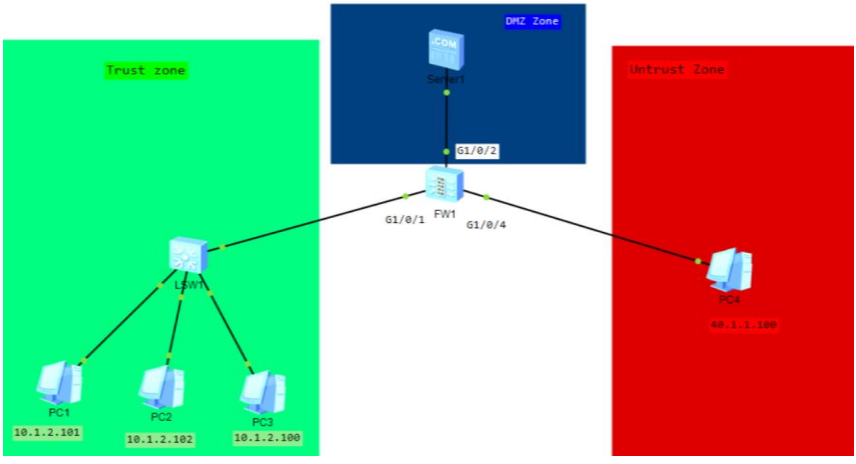


Рис. 2. Упрощенная топология сети малого предприятия

```
[NGFW-policy-nat]display firewall session table
2022-05-19 11:32:56.800
 Current Total Sessions : 5
 icmp  VPN: public --> public  10.1.2.101:15155[1.1.1.2:2049] --> 4.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.101:14899[1.1.1.2:2048] --> 4.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.101:15411[1.1.1.2:2050] --> 4.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.101:15667[1.1.1.2:2051] --> 4.1.1.100:2048
 icmp  VPN: public --> public  10.1.2.101:15923[1.1.1.2:2052] --> 4.1.1.100:2048
```

Рис. 3. Таблица сессий NGFW Huawei

Заключение. В результате проведенной работы была смоделирована защита периметра сети предприятия средствами NGFW. Также в статье были проанализированы теоретические особенности функционирования NGFW и современные поддерживаемые технологии от различных мировых производителей. В статье рассматриваются базовые методы защиты сети предприятия средствами NGFW, которые и были реализованы в среде эмуляции.

СПИСОК ЛИТЕРАТУРЫ

1. Ларсанова З. М. Разработка средств обеспечения безопасности сети предприятия на базе ОС WINDOWS / З. М. Ларсанова, А. В. Юсупова. — Текст : электронный // Современная математика и ее приложения — 2021. — № 1. — URL: elibrary_48030384_12718789.pdf (дата обращения: 28.04.2022).
2. Копырулина О. А. Технология обеспечения информационной безопасности в корпоративных сетях / О. А. Копырулина, Е. В. Устюжанин. — Текст : электронный // Лучшая студенческая статья. — 2018. — № 1. — URL: elibrary_36616488_89071023.pdf (дата обращения: 04.05.2022).
3. Селецкая Л. С. Информационная безопасность в локальных вычислительных сетях / Л. С. Селецкая, С. С. Соколов, Н. В. Черкасова. — Текст : электронный // Новая наука: современное состояние и пути развития. — 2015. — № 6-2. — URL: elibrary_25023325_ 10326516.pdf (дата обращения: 07.05.2022).
4. Межсетевой экран (Firewall). — Текст : электронный // https://www.tadviser.ru : портал выбора технологий и поставщиков. — 2020. — URL: https:://www.tadviser.ru/index.php/Статья:Межсетевой _экран_ (Firewall) (дата обращения: 07.05.2022).
5. Межсетевые экраны нового поколения (Next-Generation Firewall). — Текст : электронный // https://www.tadviser.ru : портал выбора технологий и поставщиков. — 2020. — URL: https://www.tadviser.ru/ index.php (дата обращения: 08.05.2022).
6. Gartner 2021 Magic Quadrant | Network Firewall | Fortinet. — URL: https://www.fortinet.com/ru/solutions/gartner-network-firewalls (date of the application: 10.05.2022). — Text : electronic.