ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2023»
XVIII Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XVIII Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2023»

PROCEEDINGS
of the XVIII International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2023»

2023
Астана

УДК 001+37
ББК 72+74
G99

«ǴYLYM JÁNE BILIM – 2023» студенттер мен жас ғалымдардың XVIII Халықаралық ғылыми конференциясы = XVIII Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2023» = The XVIII International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2023». – Астана: – 6865 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-337-871-8

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001+37
ББК 72+74

ISBN 978-601-337-871-8

Қолданылған әдебиеттер тізімі

1. Ahmad, A., Hadgkiss, J., and Ruighaver, A. B. (2012). Incident response teams challenges in supporting the organisational security function.

2. Мандиа Кении, Просис Крис. Защита от вторжений: расследование компьютерных преступлений. М.: Издательство «ЛОРИ», 2005. 476 с.

3. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. К.: ООО «ТИД ДС», 2001. 688 с.

4. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. Спб.: БХВПетербург, 2005. 752 с.

5. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. Горячая Линия – Телеком, 2002. 336 с. 5. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. Питер, 2008. 320 с.

УДК 004.056.5

ОСОБЕННОСТИ ПРИМЕНЕНИЯ АППАРАТНОГО МЕЖСЕТЕВОГО ЭКРАНА

Дауренбеков Нияз Хайнуллович
niyaz_daurenb@mail.ru
Магистрант факультета информационных технологий Евразийского национального университета имени Л.Н. Гумилева, Астана, Казахстан
Научный руководитель - Жүзбаев С.С.

Межсетевой экран, защищающий компьютерную сеть от сетевых атак, имеет определенные технические характеристики. Выбор модели необходимо осуществлять в зависимости от масштабов самой сети, степени конфиденциальности циркулирующей в ней информации, существующей в организации политики доступа в Интернет, подготовленности штатных администраторов и т.п.

Аппаратный межсетевой экран - программно-аппаратное устройство компьютерной сети, предназначенное для проверки на соответствие заданным правилам и дальнейшей фильтрации проходящего сквозь него сетевого трафика. Другие названия: брандмауэр (немецкий «brandmauer» - «противопожарная стена»), файрвол (английский «firewall» - «противопожарная стена»). [4]

Межсетевые экраны используются в корпоративных компьютерных сетях предприятий для защиты всей сети, её сегментов или отдельных компьютеров (серверов) от несанкционированного взлома, нарушения правил доступа, пользуясь уязвимостями в протоколах сетевой модели OSI, TCP/IP или в программном обеспечении, установленном на терминальном оборудовании сети. Межсетевые экраны могут пропускать или запрещать потоки данных, сравнивая его характеристики с настроенными шаблонами.

Значительное разнообразие межсетевых экранов вызывают у потребителя затруднения выбора модели, наиболее адекватно и эффективно решающую задачи по защите конкретной сети. Информация о межсетевых экранах, доступная непосредственно от производителя, чаще всего в рекламных целях преувеличивает достоинства и скрывает недостатки. В данной статье указываются параметры, на которые рекомендуется обращать внимание при подборе модели аппаратного межсетевого экрана предприятия, что поспособствует осознанному выбору продукта, оценивая его достоинства и недостатки.

Первые устройства, выполняющие функцию фильтрации сетевого трафика, появились в конце 1980-х, когда Интернет был новшеством и использовался в локальных, а не в глобальных масштабах. Этими устройствами являлись маршрутизаторы, инспектирующие трафик на основании содержащихся в заголовках протоколов сетевого уровня (например, заголовок IP пакета). Впоследствии, с развитием сетевых технологий, данные устройства получили возможность выполнять фильтрацию трафика, используя данные протоколов более высокого,

транспортного уровня. Маршрутизаторы можно считать первой программно-аппаратной реализацией межсетевого экрана. [4]

На сегодняшний день на рынке существует большое количество аппаратных межсетевых экранов - Cisco Firepower, Cisco ASA, Fortinet FortiGate, Juniper SRX380, Check Point Power и т.д. Выбор конкретной модели (производителя) является достаточно непростой задачей.

Ниже указываются наиболее важные технические характеристики, функциональности и аспекты, которые следовало бы принимать во внимание при выборе модели аппаратного межсетевого экрана.

Месторасположение. Наиболее распространённое место для установки межсетевых экранов - граница периметра локальной сети для защиты внутренних хостов от атак извне. Следует учитывать, что для выхода в Интернет межсетевой экран должен поддерживать трансляцию адресов NAT/PAT, которую также можно рассматривать дополнительной мерой безопасности, позволяющей скрыть адреса конечных хостов. Однако атаки могут начинаться и с внутренних узлов - в этом случае, если атакуемый хост расположен в той же сети, трафик не пересечёт границу сетевого периметра, и межсетевой экран не будет задействован. Поэтому в настоящее время применяются межсетевые экраны пригодные для размещения не только на границе, но и между различными сегментами сети, что обеспечивает дополнительный уровень безопасности. Только для внутреннего контура будет достаточно использовать возможности маршрутизаторов, без необходимости приобретения межсетевого экрана. [5]

Пропускная способность. Межсетевой экран «просматривает» каждый проходящий через него пакет данных на предмет соответствия настроенным фильтрам, в крупных сетях количество пакетов данных может исчисляться миллионами. Как можно догадаться, этот процесс достаточно ресурсоемкий. Способность передавать определённый объем данных принято характеризовать производительностью или пропускной способностью. Современные межсетевые экраны способны обрабатывать десятки Гбит/с информации, однако они очень дорого стоят. Для рационального выбора нужной модели необходимо рассчитывать (измерять) объемов трафика, передаваемого между защищаемыми сегментами сети.

Запоминание состояния сеанса. Межсетевые экраны с запоминанием состояния (stateful) оценивают обмен сетевым трафиком динамически, принимая во внимание предысторию и текущее состояние сеанса, этот режим получил название «stateful packet inspection». Межсетевые экраны с запоминанием состояния для каждого отдельного сеанса, который соответствует настроенному шаблону, выстраивают динамическую структуру сеанса в специальной таблице состояний. После прибытия очередного пакета отслеживаемого сеанса, его состояние обновляется в таблице состояний и принимается решение о выполнении сконфигурированного действия с пакетом - переправлять или отбрасывать. Однако, для малых предприятий, либо имеющих необходимость в разрешении строго определенных служб и сервисов вполне пригодным окажутся недорогие межсетевые экраны без запоминания состояния (stateless). Кроме того, статические правила фильтрации можно настроить на используемых в сети маршрутизаторах, в таком случае приобретение межсетевого экрана становится неактуальным.

IPSec. Для безопасного соединения филиалов или удаленных работников с центром на межсетевых экранах можно настроить «Site-to-Site VPN», на базе протоколов IPSec, позволяющих шифровать и проверять целостность сетевого трафика предприятия, аутентифицировать пользователей. Как правило, стоящий на границе внутренней сети и Интернета межсетевой экран наиболее пригоден для конфигурации шифрованных туннелей с удаленными пользователями [2].

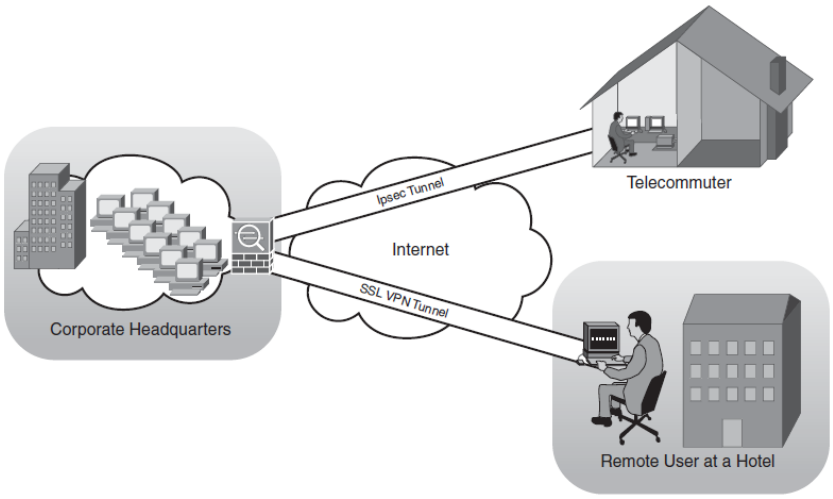

Рисунок 1. Шифрованные VPN-туннели на базе протокола IPSec

Фильтрация трафика на уровне приложений. Функционируя на 7 уровне модели OSI, межсетевые экраны «просматривают» содержимое отправляемого трафика, в их состав входят несколько программ-посредников, каждая из которых обрабатывает свой протокол прикладного уровня. Такой межсетевой экран может «ловить» в передаваемых пакетах и блокировать подозрительные или декларированные последовательности команд, что в подавляющих случаях означает DoS-атаку, либо запрещать действия некоторых команд (например, FTP PUT, которая записывает информацию на FTP сервер). Межсетевой экран как программа-посредник уровня приложений может определять тип передаваемой информации. Например, это позволяет отфильтровать (отбросить) почтовое сообщение, содержащее исполняемый зараженный файл. Посредники прикладного уровня способны проверять подлинность (аутентификация) пользователя, а также определять, что SSL-сертификаты подписаны конкретным удостоверяющим центром. Межсетевые экраны уровня приложений доступны для протоколов HTTP, FTP, почтовые (SMTP, POP, IMAP), Telnet и другие. [1]

Антивирус. Современные межсетевые экраны могут защищать от вирусов, червей и троянов в реальном времени, способны определять, блокировать и уничтожать вредоносные программы на различных платформах, например, способны обнаруживать вложенные в архивы вредоносные коды либо исполняемые файлы. Дополнительно позволяют защитить корпоративных пользователей от фишинговых и подозрительных сайтов. [3]

Одновендорность. Компьютерные сети предприятий зачастую строят свою инфраструктуру на базе оборудования одного производителя. Данный подход обеспечивает совместимость межсетевого экрана с сетевым оборудованием, а также минимизирует затраты на обучение администраторов сети, дистрибьютором как правило в таком случае предоставляются скидки при покупке его оборудования и обучении работников заказчика.

Лицензирование. Политика лицензирования вендоров различного сетевого оборудования в т.ч. и межсетевых экранов неодинаковая. Существуют лицензии на обновление программного обеспечения, расширение производительности, обновления антивирусных баз, для определенного количества пользователей и т.п. Кроме того, лицензии бывают бессрочные и с ограниченным сроком, без продления которых ряд функциональностей межсетевого экрана может быть заблокирована. Очень важно иметь актуальные антивирусные базы для обнаружения новых видов проникающих в сеть вредоносных кодов, зачастую для скачивания таких обновлений на межсетевой экран потребуется периодическая пролонгация или бессрочные лицензии.

Из вышеперечисленных возможностей межсетевых экранов зачастую внедряются не все. Следовательно, выбирать модель (производителя) межсетевого экрана предприятию целесообразно из соотношения финансовых затрат и практической потребности в использовании

конкретных функциональностей, избирательность которых можно определить с помощью данной статьи.

Список использованных источников

1. Олифер В. Г., Олифер Н.А. Безопасность компьютерных сетей. Москва, Горячая линия – Телеком 2017, 644 с.
2. Jazib Frahim, Omar Santos. Cisco ASA All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance. Indianapolis, Cisco Press 2010, p. 1151.
3. Fortinet Inc. FortiOS 7.2.4 Administration Guide. Саннивейл (Калифорния), США, 2023, 3045 с.
4. https://ru.m.wikipedia.org/wiki/Межсетевой_экран
5. https://tcinet.ru/press-centre/glossary/article.php?ELEMENT_ID=5136

ӘОЖ 004.41

КОРПОРАТИВТІК АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІ ИНТЕГРАЦИЯЛАУ МӘСЕЛЕЛЕРІ

Дауренбекова Ажар Жараскановна
zharaskanovna_azhar@mail.ru
Л.Н. Гумилев атындағы Еуразия ұлттық университетінің
4-курс студенті, Астана, Қазақстан
Ғылыми жетекші – Айтқожа Ж.Ж., ф.-м.ғ.к., доцент
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

Аңдатпа. Корпоративтік ақпараттық жүйелерді интеграциялау мәселесі көптеген компаниялар үшін, әсіресе өз қызметінде әртүрлі бағдарламалық шешімдерді қолданатындар үшін өзектілігін жоғалтқан емес. Сондықтан мақалада қарастырылған корпоративтік ақпараттық жүйелерді интеграциялаудағы негізгі мәселелердің ауқымы кең. Осы тақырыпты нақтылау барысында мақалада интеграция ұғымы, интеграция мәселесінің түрлері және оларды шешуге көмектесетін әрекеттер тізбегі сипатталады. Корпоративтік ақпараттық жүйелерді интеграциялау мәселесі күрделі функция және оны шешу компанияның тез өзгеретін нарық пен бәсекелестік ортадағы табысты жұмысы үшін өте маңызды.

Түйін сөздер: корпоративтік ақпараттық жүйелер, интеграция, интеграциялау мәселелері және олардың түрлері.

Қазіргі цифрландыру, диджитализация заманында корпоративтік ақпараттық жүйелердің өзектілігі мен қажеттілігі барша бизнес өкілдеріне мәлім. Сол себепті бұл сала төңірегінде зерттеу жүргізіп дамытқысы келетін жоба авторлары мұны бизнесті сәтті ұйымдастырудың маңызды құралдарының бірі деп санайды. Неге десеңіз, аталған жүйелер, қазіргі экономикалық жағдайды ескере отыра, орта және ірі бизнес процестерді жүйелеу мен автоматтандыруды талап етеді. Қазіргі заманғы компаниялардың қарқынды өсуі және басқару саласында өңдеуге, өзгертуге әрі қайта қолдануға болатын ақпарат көлемінің өсуі компанияларда корпоративтік ақпараттық жүйелерді енгізу және пайдалану мәселесінің өзектілігін одан әрі растайды.

Интеграциялау – бұл ақпарат алмасу және таратылған бизнес-процестерді қолдау мүмкіндігін қамтамасыз ететін ақпараттық жүйелерді біріктірудің стратегиялық тәсілі [1]. Ақпараттық жүйелерді интеграциялау кәсіпорынға бәсекелестік артықшылықтар беретіні сөзсіз, мысалы:

- іс-шаралармен басқарылатын сценарийлерді қолдана отырып, нақты уақыт режимінде бизнес жүргізу;
- сенімді, толық және уақтылы алынған ақпаратқа ие болу.

Жүйелерді интеграциялау жобалық ұйымда қолданылатын екі немесе бірнеше жүйелердегі деректердің сәйкес келмеу мәселелерін шешуді және ұйымның инфрақұрылымын құруды қамтамасыз етеді [2].