ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27033-4— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность сетей

Часть 4

Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности

(ISO/IEC 27033-4:2014, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Акционерным обществом «Научно-технический и сертификационный центр по комплексной защите информации» (АО Центр «Атомзащитаинформ») ГК «Росатом» и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 19 мая 2021 г. № 391-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27033-4:2014 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 4. Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности» (ISO/IEC 27033-4:2014 «Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways», IDT).

ИСО/МЭК 27033-4 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА.

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Большинство как коммерческих, так и государственных организаций владеют информационными системами, соединенными сетями, причем сетевые соединения могут быть одним или несколькими вариантами из следующих:

- внутри организации;
- между разными организациями;
- между организацией и общедоступными сетями.

Кроме того, в связи с быстрым развитием общедоступных сетевых технологий (в частности, сети Интернет), предоставляющих широкие возможности для бизнеса, организации все чаще ведут электронный бизнес в глобальном масштабе и предоставляют общедоступные онлайн-услуги. Такие возможности включают в себя различные услуги — от простой поддержки более дешевой передачи данных с использованием сети Интернет в качестве глобальной среды связи до более сложных услуг, предоставляемых поставщиками Интернет-услуг (ISP). Это может означать использование как недорогих локальных точек подключения на каждом конце канала, так и полнофункциональных систем электронной онлайн-торговли и предоставления услуг с использованием веб-приложений и услуг. Также новые технологии (включая интеграцию данных, голоса и видео) расширяют возможности удаленной работы. Работники, работающие в режиме удаленного доступа, могут обеспечить связь путем применения средств удаленного доступа к сетям организаций и сообществ, а также к соответствующей информации и сервисам поддержки бизнеса.

Эта среда действительно обеспечивает бизнесу значительные преимущества, но также порождает необходимость управлять новыми угрозами безопасности. Поскольку для ведения бизнеса организации в значительной степени полагаются на использование информации и соответствующих сетей, потеря конфиденциальности, целостности и доступности информации и услуг может оказать существенное неблагоприятное воздействие на бизнес-процессы. Таким образом, существует большая потребность в надлежащей защите сетей и связанных с ними информационных систем и информации. Другими словами, реализация и поддержание адекватной безопасности сетей имеет решающее значение для успеха бизнес-процессов каждой организации.

В этом контексте отрасли телекоммуникаций и информационных технологий стремятся к экономически эффективным комплексным решениям обеспечения безопасности, предназначенным для защиты сетей от целевых атак и непреднамеренных ошибочных действий, тем самым удовлетворяя бизнес-требования по обеспечению конфиденциальности, целостности и доступности информации и услуг. Защита сети важна и для точного выставления счетов за использование сетей. Возможности защиты в продуктах имеют решающее значение для общей безопасности сети (включая приложения и услуги). Однако по мере того, как все больше продуктов объединяется для создания комплексных решений, их способность к взаимодействию или ее отсутствие будут определять успех этого решения. Безопасность должна быть не только предметом рассмотрения для каждого продукта или услуги, но и должна разрабатываться таким образом, чтобы способствовать объединению возможностей защиты в общее решение обеспечения безопасности.

Цель настоящего стандарта заключается в том, чтобы предоставить руководство по идентификации и анализу угроз безопасности сетей, связанных со шлюзами безопасности, определить требования по обеспечению безопасности сетей для шлюзов безопасности на основе анализа угроз, представить методы разработки для создания сетевой архитектуры технической безопасности для устранения угроз и решения вопросов управления для типовых схем построения сетей, а также для решения проблем, связанных с внедрением, эксплуатацией, мониторингом и проверкой мер обеспечения информационной безопасности (ИБ) с помощью шлюзов безопасности.

Следует подчеркнуть, что настоящий стандарт может быть использован всем персоналом, который участвует в детальном планировании, проектировании и внедрении шлюзов безопасности (например, архитекторов и проектировщиков сетей, администраторов сетей и сотрудников службы безопасности сетей)[1)].

[1)] *Положения настоящего стандарта должны рассматриваться с учетом требований национальных нормативных правовых актов и стандартов Российской Федерации в области защиты информации.*

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность сетей

Часть 4

Обеспечение безопасности межсетевого взаимодействия с использованием шлюзов безопасности

Information technology. Security techniques. Network security.
Part 4. Securing communications between networks using security gateways

Дата введения — 2021—11—30

1 Область применения

В настоящем стандарте содержится руководство по обеспечению безопасности межсетевого взаимодействия с использованием шлюзов безопасности (межсетевых экранов, межсетевых экранов уровня приложений, систем предотвращения вторжений и т. д.) в соответствии с документированной политикой информационной безопасности (ИБ) для шлюзов безопасности, включающее в себя:

a) выявление и анализ угроз безопасности сети, связанных со шлюзами безопасности;

b) определение требований по обеспечению безопасности сетей для шлюзов безопасности на основе анализа угроз;

c) использование методов проектирования и реализации для устранения угроз и решения вопросов управления для типовых схем построения сетей;

d) решение проблем, связанных с внедрением, эксплуатацией, мониторингом и проверкой шлюзов безопасности сети.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения).

ISO/IEC 27033-1, Information technology — Security techniques — Network security — Part 1: Overview and concepts (Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и понятия)

3 Термины и определения

Для целей настоящего стандарта применены термины и определения, приведенные в ИСО/МЭК 27033-1, а также следующие термины с соответствующими определениями:

3.1 **узел-бастион (**bastion host): Конкретный узел с усиленной операционной системой, который используется для перехвата пакетов, входящих или выходящих из сети или системы, к которому долж-

Издание официальное

ны подключаться все внешние пользователи для получения доступа к услуге или системе, которая находится под защитой межсетевого экрана организации.

3.2 **оконечный программный межсетевой экран** (end-point software-based firewall): Программное приложение, работающее на одном компьютере, защищающее сетевой трафик, входящий и исходящий из этого компьютера, с целью разрешить или запретить обмен данными на основе политики безопасности, определенной конечным пользователем.

3.3 **усиленная операционная система** (hardened operating system): Операционная система, которая была сконфигурирована или разработана специально для минимизации возможности компрометации или атаки.

Примечание — Это может быть обычная операционная система (ОС), такая как Linux, настроенная для этой среды, или более специализированное решение.

3.4 **Интернет-шлюз** (Internet gateway): Точка входа в сеть Интернет.

3.5 **пакет** (packet): Объект, содержащий четко определенный блок байтов, состоящий из заголовка, данных и необязательного концевика, который может передаваться по сетям или телефонным линиям.

Примечание — Формат пакета зависит от протокола, согласно которому он создан. Для мониторинга и управления сеансом связи различные стандарты связи и протоколы используют пакеты специального назначения. Например, стандарт X.25 использует пакеты диагностики, очистки вызова и сброса пакетов (среди прочих), а также пакеты данных/блок данных, которые передаются по сети.

3.6 **сеть периметра** (perimeter network): Физическая или логическая подсеть, которая содержит и предоставляет услуги организации для внешних пользователей.

3.7 **удаленный офис/филиал** (remote office, branch office): Офис, удаленно подключенный к головному офису организации с использованием каналов связи, для предоставления пользователям услуг (например, службы файлов, печати и других служб), необходимых для поддержания их повседневной работы.

3.8 **единая точка отказа** (single point of failure): Тип отказа, при котором если какой-либо элемент системы выходит из строя, то и вся система перестает работать.

3.9 **шлюз протокола инициализации сеанса** (SIP gateway): Устройство периметра, которое находится между внутренней VoIP-сетью (сетью передачи голоса по IP-сети, Voice-over-IP) и внешней сетью, такой как телефонная сеть общего пользования.

Примечание — Часто для выполнения этой роли используется маршрутизатор. В тех случаях, когда VoIP используется для внешних IP-сетей, важно обеспечить, чтобы шлюз содержал достаточные защитные меры, особенно для того, чтобы все динамические изменения базы правил для всех настроек вызовов выполнялись безопасным образом.

4 Сокращения

ACL — список управления доступом (access control list);

API — интерфейс прикладного программирования (application programming interface);

ASIC — специализированная интегральная схема (application specific integrated circuit);

BGP — протокол граничного шлюза (border gateway protocol);

DDoS — распределенный отказ в обслуживании (distributed denial-of-service);

DLL — библиотека динамических ссылок (dynamic link library);

DNS — система доменных имен (domain name system);

DoS — отказ в обслуживании (denial-of-service);

FTP — протокол передачи файлов (file transfer protocol);

HTTP — протокол передачи гипертекста (hypertext transfer protocol);

HTTPS — протокол передачи гипертекста через уровень защищенных сокетов (hypertext transfer protocol over secure socket layer);

ICMP — интернет-протокол управления сообщениями (internet control message protocol);

IP — интернет-протокол (internet protocol);

MIME — многоцелевые расширения Интернет-почты (multipurpose internet mail extensions);

NAT — трансляция сетевых адресов (network address translation);

NFS — сетевая файловая система (network file system);

NIS — сетевая информационная система (network information system);

NNTP — сетевой транспортный протокол новостей (network news transport protocol);

NTP — сетевой протокол времени (network time protocol);

OSI — взаимосвязь открытых систем (open system interconnection);

OSPF — протокол нахождения кратчайшего пути (open shortest path first);

RIP — протокол информации о маршрутизации (routing information protocol);

RPC — удаленный вызов процедур (remote procedure call);

SIP — протокол инициализации сеанса (session initiation protocol);

SMS — служба коротких сообщений (short message service);

S/MIME — безопасные многоцелевые расширения Интернет-почты (secure/multipurpose internet mail extensions);

SMTP — простой протокол пересылки почты (simple mail transfer protocol);

SOAP — простой протокол доступа к объектам (simple object access protocol);

SPA — анализатор коммутируемых портов (switched port analyzer);

SPOF — единая точка отказа (single point of failure);

SQL — язык структурированных запросов (structured query language);

SSL — протокол уровня защищенных сокетов (secure sockets layer protocol);

SYN — синхронный (одновременный) (synchronous);

TCP — протокол управления передачей (transmission control protocol);

TLS — протокол безопасности транспортного уровня (transport layer security);

UDP — протокол пользовательских датаграмм (user datagram protocol);

VLAN — виртуальная локальная сеть (virtual local area network);

VoIP — передача голоса [голосового трафика] по IP-сетям (voice over internet protocol);

VPN — виртуальная частная сеть (virtual private network);

WAIS — информационные серверы или службы глобальной сети (wide-area information servers or service);

WLAN — беспроводная локальная сеть (wireless local area network);

XML — расширяемый язык разметки (extensible markup language);

ВМ — виртуальная машина (virtual machine, VM);

ДМЗ — демилитаризованная зона (demilitarized zone, DMZ);

ОС — операционная система (operating system, OS);

СОВ — система обнаружения вторжений (intrusion detection system, IDS);

СПВ — система предотвращения вторжений (intrusion prevention system, IPS);

ЦП — центральный процессор (central processing unit, CPU).

5 Структура документа

Настоящий стандарт содержит следующие разделы и подразделы:

- обзор шлюза безопасности (VPN) (раздел 6);
- описание угроз безопасности, связанных с шлюзом безопасности (раздел 7);
- описание требований по обеспечению безопасности, основанных на анализе шлюзов безопасности (раздел 8);
- описание мер обеспечения ИБ, связанных с типовыми схемами построения сетей и областями сетевых технологий, использующих шлюз безопасности (раздел 9);
- описание методов проектирования шлюзов безопасности (раздел 10);
- рекомендации по выбору продукта (раздел 11).

6 Обзор

Шлюз безопасности размещается на границе между двумя или более сегментами сети, например между внутренней сетью организации и общедоступной сетью, для фильтрации трафика, проходящего через границу, в соответствии с задокументированной политикой доступа к функциям шлюза безопасности для этой границы. Другое использование шлюзов безопасности — это разделение сегментов сети при использовании услуг, которые могут иметь несколько арендаторов; например, при использовании служб облачных вычислений шлюз безопасности будет защищать информацию организации, применяя политику безопасности организации.

Пример сетевого окружения показан на рисунке 1, который в данном обзоре используется только для иллюстрации. ДМЗ, называемая сетью периметра, представляет собой физическую или логическую подсеть, которая содержит и предоставляет внешние услуги организации для общедоступной сети, обычно сети Интернет. Целью ДМЗ является добавление дополнительного уровня безопасности к внутренней сети организации; внешний злоумышленник имеет доступ только к услугам в ДМЗ, а не к какой-либо другой части внутренней сети. Все внешние подключения к сетевым услугам должны завершаться внутри систем ДМЗ, а системы ДМЗ должны иметь ограниченный доступ или вообще не иметь доступа к внутренним системам. Проектирование сети таким способом не устраняет риск компрометации внутренней сети, а только усложняет ее. Злоумышленник, преодолевший защиту периметра внутренней сети, затем сможет использовать другую уязвимость для развития атаки на ресурсы внутренней сети. По этой причине, среди прочих, внутренняя сеть должна быть максимально защищенной.

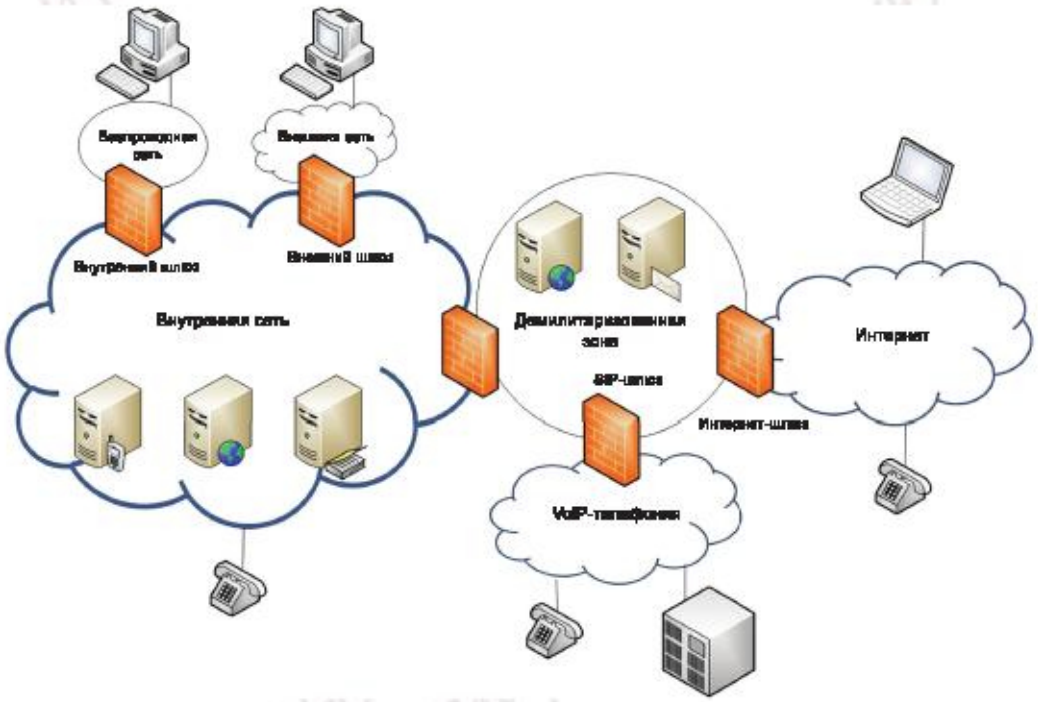

Рисунок 1 — Пример сетевого окружения

Большинство организаций может иметь несколько «зон» или областей ДМЗ для уровней веб, приложений и баз данных и для выполнения некоторых нормативных требований или требований политики безопасности организации.

В настоящее время существуют «гибридные» решения, применимые в нескольких функциональных областях. Существующие межсетевые экраны с фильтрацией пакетов содержат в себе прокси-

сервер для определенных служб и включают больше мер обеспечения ИБ для такого контекста, как, например, роль, время суток и т. д.

Сетевая структура организации, называемая интранетом, управляется и поддерживается уполномоченными этой организации. Каждая организация независимо от размера должна иметь отдельные сегменты сети, между которыми потоки трафика будут контролироваться внутренними шлюзами безопасности. Для специальных целей в интранете может быть создана отдельная инфраструктура. Например, если WLAN используется как часть интранета, то она должна быть изолированной и требовать дополнительной аутентификации, поскольку это создает дополнительные риски. Для защиты активов организации от атак при такой сегментации может использоваться внутренний шлюз безопасности.

Организация обменивается данными с доверенными третьими сторонами, расширяя интранет в сторону сети партнеров, что называется экстранетом. Для устранения угроз, создаваемых этим расширением, может применяться шлюз безопасности экстранета. При использовании таких услуг, как облачные вычисления, шлюз безопасности ограничивает доступ пользователей к ним, применяя политики безопасности организации к логическим сетям. Деятельность организации требует коммуникаций и обмена данными с деловыми партнерами, клиентами и широкой общественностью через общедоступную сеть, примером которой является сеть Интернет. Поскольку уровень доверия к общедоступной сети относительно низок, для устранения рисков, вызванных ею, необходимы шлюзы безопасности, называемые Интернет-шлюзами.

7 Угрозы безопасности

В обозримом будущем организации могут ожидать все более изощренные атаки на свои системы. Попытки несанкционированного доступа (НСД) могут быть злонамеренными, например, привести к атаке типа «отказ в обслуживании» (DoS), злоупотреблению ресурсами или НСД к ценной информации. Организации должны защищать свою внутреннюю сеть или активы от различных угроз, таких как преднамеренное злоупотребление активами, неправильная конфигурация систем, несанкционированная передача трафика из разных доверенных сетевых сегментов в организации или другие угрозы со стороны служб Интернет-приложений.

Шлюз безопасности должен защищать организацию от вторжений со стороны неавторизованных пользователей, получающих доступ к сетевым ресурсам из внутренней сети, сети Интернет или иных сетей. Неконтролируемый контент, исходящий из организации, может привести к юридическим проблемам и потенциальной потере интеллектуальной собственности. Кроме того, поскольку все больше организаций подключаются к Интернету для удовлетворения своих требований, они сталкиваются с необходимостью контролировать доступ к неподходящим или нежелательным веб-сайтам или веб-приложениям и услугам. Без контроля доступа перед организациями встает угроза потери производительности, ответственности и неправильного распределения полосы пропускания из-за непродуктивного веб-серфинга. Таким образом, ключевые угрозы безопасности, которые необходимо устранить, бывают следующими:

- отказ в обслуживании авторизованным пользователям;
- несанкционированное изменение данных;
- несанкционированное разглашение информации;
- несанкционированная реконфигурация системы;
- несанкционированное использование ресурсов и активов организации;
- искажение контента в результате воздействия вируса или вредоносного ПО;
- нарушение виртуализации;
- DoS- и DDoS-атаки, нацеленные на шлюз безопасности.

8 Требования к обеспечению безопасности

Шлюзы безопасности управляют доступом к сети (уровни 2, 3 и 4 модели OSI) или приложению (уровни 5—7 модели OSI), что показано на рисунке 2.

Шлюзы безопасности используются для выполнения следующих требований по обеспечению безопасности:

- обеспечивать логическую сегментацию сети;
- ограничивать и анализировать трафик, проходящий между логическими сетями;

- контролировать доступ к сети организации и обратно путем проверки подключений или работы прокси-сервера для выбранных приложений;
- применять политику безопасности для сети организации;
- регистрировать трафик для последующего аудита;
- скрывать архитектуру внутренней сети, узла и приложения;
- предоставлять возможность для упрощения выполнения действий по управлению сетью, например смягчение последствий DoS- или DDoS-атак.

Рисунок 2 — Семь уровней модели OSI

Таблица 1 иллюстрирует взаимосвязь между угрозами из раздела 7 и требованиями по обеспечению безопасности данного раздела.

Таблица 1 — Связь между угрозами и требованиями по обеспечению безопасности

Угрозы	Требования						
	Обеспечить логическую сегментацию сети	Ограничивать и анализировать трафик, который проходит между логическими сетями	Контролировать доступ к сети организации и из нее, проверяя соединения или работу прокси-сервера в выбранных приложениях	Обеспечить соблюдение политики безопасности для сети организации	Регистрировать трафик для последующего анализа	Скрыть архитектуру внутренней сети, узла и приложения	Предоставить возможность облегчения функций управления сетью
Отказ в обслуживании авторизованным пользователям		X		X	X		X
Неавторизованное изменение данных	X	X	X	X	X		X
Неавторизованное разглашение информации	X	X	X	X	X		X
Неавторизованная реконфигурация системы			X	X	X	X	X

Окончание таблицы 1

Угрозы	Требования						
	Обеспечить логическую сегментацию сети	Ограничивать и анализировать трафик, который проходит между логическими сетями	Контролировать доступ к сети организации и из нее, проверяя соединения или работу прокси-сервера в выбранных приложениях	Обеспечить соблюдение политики безопасности для сети организации	Регистрировать трафик для последующего анализа	Скрыть архитектуру внутренней сети, узла и приложения	Предоставить возможность облегчения функций управления сетью
Несанкционированное использование ресурсов и активов организации	X	X	X	X	X	X	X
Искажение контента в результате воздействия вируса или вредоносного ПО	X	X	X	X	X	X	X
Нарушение виртуализации	X	X	X	X	X		X
DoS- и DDoS- атаки, нацеленные на шлюз безопасности		X		X	X		X

9 Меры обеспечения информационной безопасности

9.1 Обзор

Для каждого шлюза безопасности должен быть разработан отдельный документ «Политика (безопасности) доступа к услугам» (далее — политика), в содержании которого должно быть отражено, что для прохождения разрешен только авторизированный трафик. Этот документ должен содержать подробную информацию о наборе правил, который требуется для администрирования шлюза, а также о конфигурации шлюза. Иерархию политик необходимо ввести в действие: организация, независимо от размера, вероятно, будет иметь общую политику для всей организации, возможно, дополненную общей политикой в отношении целого класса устройств безопасности, возможно, дополнительно усиленную отдельной политикой для конкретного устройства. Таким образом, для гарантии того, что подключаются только санкционированные пользователи и передается только санкционированный трафик, политика должна определять и подробно фиксировать ограничения и правила, применяемые к трафику, приходящему в шлюз безопасности и исходящему из него, а также параметры для его администрирования и конфигурирования. Для всех шлюзов безопасности необходимо надлежащим образом использовать имеющиеся средства идентификации и аутентификации, логического контроля доступа и аудита. Кроме того, их следует регулярно проверять на наличие неавторизованного ПО и/или данных, и если таковые обнаружены, то составлять отчеты об инцидентах в соответствии с планом управления инцидентами ИБ организации и/или сообщества (ИСО/МЭК 27035). Обновление безопасности — это изменение, применяемое к шлюзу безопасности для исправления недостатка, называемого уязвимостью, с целью предотвращения его успешной эксплуатации и устранения или ослабления последствий реализации угрозы в шлюзе. Следовательно, для шлюза безопасности должны регулярно устанавливаться последние обновления и версии ПО, что гарантирует их защищенность от недавно выявленных уязвимостей.

Шлюз безопасности не должен быть подключен к сети организации, пока не будет установлено, что его конфигурация удовлетворяет требованиям политик его администрирования.

Межсетевой экран (МЭ) является хорошим примером шлюза безопасности. МЭ обычно должен гарантировать соответствующую защиту, соизмеримую с оцененными угрозами, за счет стандартного набора правил, безоговорочно запрещающего все для всего трафика между сетями и добавляющего явные правила только для необходимых каналов связи.

Политики, управляющие шлюзом безопасности, используемым для защиты удаленной системы, могут не требовать затрат и специальных навыков для поддержки указанного аппаратного устройства. Можно использовать оконечный программный МЭ, так называемый персональный МЭ, который управляет потоком трафика между удаленным компьютером и сетью, к которой он подключен. Как и в случае всех шлюзов безопасности, организация должна быть уверена в том, что конфигурация набора правил в оконечном программном МЭ соответствует требованиям политик управления.

Существуют различные типы шлюзов безопасности, включая пакетные фильтры, МЭ с прокси-сервером, МЭ с отслеживанием состояния пакетов, фильтры контента, МЭ уровня приложений. Описания для каждого типа шлюза безопасности будут даны в следующих подразделах.

Для реализации необходимых функций шлюз безопасности может использовать технологию виртуализации. ВМ должны быть хорошо изолированы при совместном использовании памяти, ЦП и хранилищ.

Гипервизор, также называемый диспетчером ВМ, должен обеспечивать собственную защиту и защиту размещенных ВМ, например, путем перемещения работы антивирусного ПО и антиспама с ВМ на гипервизоры.

Безопасность виртуализации защищает как гипервизор, так и его ВМ. Это защищает гипервизор от атак и обеспечивает изоляцию ВМ. Данная функция также включает защиту образов ВМ и приостановленных экземпляров ВМ в хранилище и во время миграции, а также общее управление жизненным циклом безопасности ВМ.

9.2 Фильтрация пакетов без отслеживания состояния

Пакетный фильтр оценивает каждый пакет отдельно от всех других пакетов. Решение о том, разрешить или запретить его прохождение, основано только на данных самого пакета. Попытка связать пакет с любыми предыдущими пакетами, которые были проанализированы пакетным фильтром, не осуществляется. Поэтому решение основывается на анализе таких данных, как следующие:

- IP-адрес источника и/или назначения;
- полезная нагрузка, которую несет пакет (например, TCP, UDP, ICMP);
- порт источника и/или назначения для полезной нагрузки TCP или UDP;
- время/дата получения/отправления пакета;
- карта сетевого интерфейса прибытия/отправления.

Шлюзы фильтрации пакетов работают быстро, но не отслеживают значимость какого-либо пакета в общем потоке связи.

9.3 Проверка пакетов с отслеживанием состояния

Проверка пакетов с отслеживанием состояния расширяет фильтрацию пакетов, регистрируя ключевые события в жизненном цикле обмена сообщениями, обычно отслеживая состояние протоколов транспортного уровня. Основанный на технологии фильтрации пакетов, реализованный в некоторых МЭ подход с отслеживанием состояния пакетов подразумевает больше проверок безопасности, имитируя проверки безопасности МЭ уровня приложений с прокси-сервером. Вместо простого просмотра адреса каждого входящего пакета МЭ с проверкой пакетов с отслеживанием состояния перехватывает входящие пакеты на сетевом уровне до тех пор, пока у него не будет достаточно информации для определения состояния попытки соединения на верхних уровнях. При принятии решения по пакету пакетный фильтр с сохранением состояния анализирует пакет в контексте других пакетов, которые он уже анализировал. Это позволяет фильтру, например, различать пакет, который является частью установленного TCP-соединения, и аналогичный пакет, который поступил один раз. Пакетный фильтр с отслеживанием состояния может принимать более «тонкие» решения, чем пакетный фильтр без отслеживания состояния. Однако для достижения той же пропускной способности это требует больше ресурсов (памяти и вычислительной мощности).

9.4 Межсетевой экран уровня приложений

МЭ уровня приложений анализирует обмен данными по протоколу прикладного уровня. Например, МЭ уровня веб-приложений будет содержать правила, которые представляют корректную работу HTTP. Решение о том, разрешить ли HTTP-запрос или HTTP-ответ, может основываться как на состоянии HTTP-разговора (например, подходит ли этот ответ для ранее увиденного запроса?), так и на некотором конкретном шаблоне данных (например, присутствуют ли символы, характерные для атаки типа «SQL-инъекция»?).

Если МЭ уровня приложений должен функционировать при зашифрованной связи, такими средствами как SSL/TLS, то на МЭ уровня приложений должно быть исключено сквозное шифрование, чтобы он мог фильтровать данные приложения в открытом виде. Тогда МЭ уровня приложений должен управлять парой зашифрованных каналов связи между источником и получателем. Если целостность такого МЭ уровня приложений будет нарушена, то при доверии пользователей к защите на основе сквозного шифрования последствия будут особенно серьезными.

МЭ устраняют некоторые из угроз, описанных в разделе 7, например, несанкционированное использование ресурсов и активов организации, ограничивая доступ к приложению или компьютеру конечным набором определенных задач внутри самого прокси-сервера.

Использование МЭ уровня приложений поддерживает качественный контроль безопасности, поскольку обеспечивает осведомленность на уровне приложений о попытках соединения, проверяя все на самом высоком уровне стека протоколов. МЭ уровня приложений может быть реализован в составе прокси-сервера приложений, что может ускорить отклик и уменьшить дублирование трафика. Служба прокси-сервера приложений имеет полную видимость на уровне приложений и, соответственно, может заранее просматривать подробные сведения о каждом ранее предпринятом соединении и соответствующим образом реализовывать политики безопасности. Службы прокси-сервера приложений также имеют встроенную прокси-функцию — завершение клиентского соединения на шлюзе приложений и инициирование нового соединения с внутренней защищенной сетью. Работа прокси-сервера обеспечивает дополнительную безопасность, поскольку он разделяет внешнюю и внутреннюю системы и затрудняет использование уязвимостей внутренних систем организации злоумышленникам извне. Зашифрованные сквозные соединения не могут напрямую проходить через МЭ уровня приложений, но в МЭ уровня приложений они существуют в виде двух зашифрованных потоков с сообщением в открытом виде. Это делает МЭ уровня приложений особенно привлекательным в качестве цели атаки, с которой можно запускать атаки типа «человек посередине» на зашифрованные соединения.

Во многие МЭ уровня приложений встроены как традиционные службы прокси-сервера, так и возможности прокси-сервера, часто называемые «глубокой проверкой пакетов» или «контролем приложений». Они осведомлены о приложении и могут разрешать только определенные функции в приложении или применять дополнительные меры обеспечения ИБ (например, антивирусное сканирование файлов, передаваемых в приложении, или блокирование видеовызова в клиентах службы мгновенных сообщений).

Защищенные шлюзы, использующие прокси-сервер приложений, обеспечивают максимальную безопасность с единственным недостатком, заключающимся в том, что дополнительные средства защиты могут отрицательно влиять на производительность. Кроме того, для новых служб часто требуется время, прежде чем прокси-сервер станет доступным для них.

9.5 Фильтрация контента

Шлюзы безопасности с прокси-сервером приложений часто реализуют фильтрацию контента. Фильтрация контента является основной защитой от вредоносного или неподходящего кода. Она может помочь защититься от угроз, доставляемых при загрузке приложений или выполняемых в браузере. Примеры разнообразны: от троянских коней до неуместных элементов управления ActiveX. Поскольку большая часть этого вредоносного кода распространяется через сеть Интернет по электронной почте или HTTP-соединениям (например, загрузка с веб- или FTP-сайта), защита должна начинаться в точке взаимодействия шлюза безопасности с сетью Интернет. Таким образом, в экранированную подсеть или ДМЗ добавляется сканер вирусов или, в более общем смысле, сканер контента. В большинстве конфигураций сканер контента напрямую связан с МЭ с помощью сетевого интерфейса, так что такие службы, как трафик электронной почты на основе SMTP и связь на основе HTTP, маршрутизируются на сканер фильтрации контента.

Преобладающими технологиями анализа контента являются следующие:

- анализ протоколов;
- сканирование на основе сигнатур (поиск известных шаблонов);
- исследовательский анализ (анализ кода на наличие функций и поведения, о которых известно, что они связаны с вредоносным кодом);
- технология «песочницы» (по сути, программа мониторинга контента, которая помещает подозрительный код в «песочницу»).

Поскольку разница между сканированием контента и обнаружением вторжений невелика, особенно в том, что касается обнаружения сетевых вторжений, СОВ можно также объединить с МЭ, установив агент СОВ на устройстве МЭ (см. ISO/IEC TR 15947).

Примечание — Выбор, развертывание и эксплуатация систем обнаружения или предотвращения вторжений являются предметом ИСО/МЭК 27039.

Технология фильтрации контента также имеет некоторые ограничения. Если данные зашифрованы на транспортном или прикладном уровне (например, с помощью SSL/TLS или S/MIME), проверка контента далее невозможна, пока зашифрованные данные не будут расшифрованы и потом повторно зашифрованы на МЭ. Это может создавать угрозы безопасности, такие как атаки «человек посередине».

В отношении сканирования и фильтрации контента могут возникнуть юридические последствия, особенно в тех случаях, когда действует строгое законодательство о защите данных. Тогда может быть разрешено только автоматическое сканирование на наличие вредоносного кода, но не сканирование на конкретный контент электронной почты, поскольку это может нарушить приватность отправителя и получателя.

9.6 Системы предотвращения и системы обнаружения вторжений

Вторжение — это НСД к сети или системе, подключенной к сети, то есть преднамеренный или случайный НСД к информационной системе (ИС), злонамеренная деятельность в отношении ИС или несанкционированное использование ресурсов в ИС. Предотвращение вторжений — это формальный процесс активного реагирования для предотвращения вторжений. СПВ представляет собой вариант СОВ, которая специально разработана для обеспечения возможности активного реагирования, тогда как СОВ просто обнаруживают возможные вторжения, которые были предприняты, происходят или произошли, и, возможно, уведомляют администраторов о вторжениях.

9.7 Интерфейс прикладного программирования для управления безопасностью

Функция централизованного управления позволяет правильно и эффективно управлять шлюзами безопасности, развернутыми в сети организации.

В организации для удаленного централизованного управления шлюзом безопасности должен предоставляться интерфейс прикладного программирования (API) для управления безопасностью. Эта функция централизованного управления должна помочь при удаленном управлении шлюзами безопасности в их эксплуатации и конфигурировании.

Удаленный доступ администратора должен быть идентифицирован и аутентифицирован шлюзом безопасности. Этот API удаленного управления должен предоставлять сетевому администратору инструменты для администрирования, мониторинга и устранения неполадок в шлюзе безопасности.

10 Методы проектирования

10.1 Компоненты шлюзов безопасности

10.1.1 Коммутаторы

Коммутаторы используются для поддержки высокоскоростной связи, обеспечивающей полную пропускную способность сети для каждого физического порта. Обычно коммутаторы — это устройства уровня 2, которые широко используются для сегментирования локальных сетей. Кроме того, они могут обеспечить изоляцию подсети при реализации VLAN. Трафик между коммутатором и узлами, подключенными к этому коммутатору, можно контролировать с помощью ACL. Они могут быть применены на уровнях 2, 3 и 4 модели OSI. Функция управления доступом, предоставляемая коммутаторами, делает их полезными для включения в качестве компонентов архитектуры шлюза безопасности, особенно для реализации и структурирования любых ДМЗ с экранированными подсетями. Коммутаторы, используемые в среде шлюза безопасности, не должны быть подключены напрямую к общедоступной сети из-за различных угроз, например DoS-атак, которые могут привести к тому, что незащищенный коммутатор «наводнит» подключенные сети пакетами.

Известны коммутаторы с балансировкой нагрузки, работающие на уровне 7. Они используются для обеспечения доступности как МЭ, так и серверов (хотя обычно это не уровень 7 для МЭ).

10.1.2 Маршрутизаторы

Маршрутизаторы, как правило, предназначены для подключения к различным сетям путем поддержки нескольких сетевых протоколов и для оптимизации сетевого трафика и маршрутов между взаимодействующими узлами. Кроме того, маршрутизаторы могут использоваться в качестве компонентов шлюзов безопасности, поскольку они могут фильтровать соответствующие пакеты данных для передачи данных на основе методов фильтрации пакетов. Маршрутизатор, который использует такую проверку пакетной информации для управления сетевым трафиком, часто называют экранирующим маршрутизатором. Маршрутизаторы обычно работают на уровне 3 модели OSI (сетевой уровень). На этом уровне можно анализировать только информацию уровня пакета, такую как порты источника и назначения. Маршрутизаторы могут выполнять трансляцию сетевых адресов (NAT) и фильтрацию пакетов.

Известны маршрутизаторы с балансировкой нагрузки, которые работают на уровне 7. Они используются для обеспечения доступности как МЭ, так и серверов (но обычно не уровня 7 для МЭ).

10.1.3 Шлюзы уровня приложений

Шлюз уровня приложений — это аппаратно-программное устройство или набор устройств. Шлюзы уровня приложений специально предназначены для ограничения доступа между двумя отдельными сетями. В первую очередь для реализации шлюзов уровня приложений используются два метода:

- проверка пакетов с отслеживанием состояния;
- прокси-сервер приложений.

Также могут использоваться комбинации и вариации (например, МЭ уровня канала) этих методов. Кроме того, шлюзами уровня приложений может выполняться NAT. Шлюз уровня приложений «понимает» приложения и протоколы, используемые приложениями, для того, чтобы иметь возможность определить, являются ли запросы законными. Например, чтобы разрешить соответствующую информацию между соединениями при использовании таких приложений, как VoIP, шлюз уровня приложений должен «понимать» SIP.

При использовании технологии VoIP для предоставления телефонного обслуживания сеть организации должна быть защищена от атак на SIP так называемым МЭ с поддержкой SIP — типовой пример шлюза уровня приложений.

10.1.4 Устройства безопасности

Сетевые устройства (маршрутизаторы, коммутаторы, модемы и т. д.), оснащенные усиленными ОС, предназначенными для обеспечения безопасности, называются устройствами безопасности. На эти устройства может устанавливаться ПО безопасности (МЭ, СОВ/СПВ, антивирусная защита и т. д.). Для удовлетворения разнообразных требований по обеспечению безопасности устройства безопасности предлагаются для различных платформ — от самых маленьких удаленных локаций до крупных корпоративных сетей и центров обработки данных. Устройство, предназначенное для одного компьютера, которое называется персональным МЭ, представляет собой программное приложение, работающее на этом компьютере для защиты входящего и исходящего с этого компьютера трафика. Устройство, предназначенное для защиты удаленной локации, называется устройством безопасности филиала/домашнего офиса или удаленного офиса и филиала. Устройство безопасности удаленного офиса и филиала обычно защищает трафик в удаленный офис/филиал или домашний офис и обратно. Все случаи, упомянутые в разделе 9, могут быть реализованы при использовании устройств безопасности.

10.1.5 Функция мониторинга

Централизованная функция мониторинга/аудита позволяет правильно и эффективно проводить аудит и/или мониторинг шлюзов безопасности, развернутых в сети организации. Соединение между функцией мониторинга/аудита и шлюзом безопасности должно быть защищено, что используется для обмена необходимой информацией для правильного выполнения функции аудита и мониторинга.

Кроме того, каждый шлюз безопасности должен поддерживать интерфейс для связи с централизованной функцией мониторинга/аудита. Эта централизованная функция мониторинга/аудита может помочь отследить каждое ненормальное состояние шлюзов безопасности и/или любые попытки и действия, которые могут вызвать нарушение безопасности шлюзов и/или внутренних систем, а также отследить ответственность пользователей за выполненные действия и зафиксировать нарушения политики безопасности.

Комплексная функция мониторинга/аудита облегчает всесторонний мониторинг работы шлюза безопасности и журналов регистрации событий. Кроме того, он может предложить наглядную, эффективную и доступную информационную панель для принятия управленческих решений.

10.2 Развертывание элементов управления шлюза безопасности

10.2.1 Архитектура межсетевого экрана с фильтрацией пакетов

Существует два типа МЭ с фильтрами пакетов: с отслеживанием или без отслеживания состояния. МЭ без отслеживания состояния подходит для удаления искаженных пакетов и пакетов, поступающих из «неправильного» источника или направляющихся к «неправильному» назначению. Источник или назначение могут быть идентифицированы по направлению потока через МЭ, сетевому адресу пакета или порту содержимого транспортного уровня пакета. Каждый пакет рассматривается изолированно от всех других пакетов. МЭ с фильтрацией пакетов не разрывает сквозного подключения. Самый базовый тип архитектуры МЭ называется МЭ с фильтрацией пакетов, изображенным на рисунке 3. МЭ с фильтрацией пакетов — это, по сути, устройства маршрутизации, которые включают в себя функции контроля доступа для сетевых адресов и сеансов связи. Их часто называют экранирующими маршрутизаторами. В своей базовой форме МЭ с фильтрацией пакетов работают на уровне 3 модели OSI.

Рисунок 3 — МЭ с фильтрацией пакетов/экранирующий маршрутизатор

Функция управления доступом МЭ с фильтрацией пакетов управляется набором директив, совместно именуемых набором правил. Наборы правил обычно называются ACL. Они обеспечивают управление доступом к сети и могут, например, быть основаны на адресе источника пакета, адресе получателя пакета, типе трафика, некоторых характеристиках связи уровня 4, таких как порты источника и получателя, а также на информации, относящейся к тому интерфейсу маршрутизатора, с которого поступил пакет, и какому интерфейсу маршрутизатора предназначен пакет.

МЭ с фильтрацией пакетов имеют два основных преимущества: скорость и гибкость. Поскольку пакетные фильтры обычно не исследуют данные выше уровня 4 модели OSI, они могут работать очень быстро. Эта простота позволяет развертывать МЭ с фильтрацией пакетов как внешний маршрутизатор перед экранированным узлом или экранированной подсетью. Причиной такого размещения является их способность блокировать «отказ в обслуживании» и связанные с ним атаки. Экранирующие маршрутизаторы не могут предотвратить атаки, в которых используются специфичные для приложений уязвимости или функции, поскольку они не проверяют данные верхнего уровня (уровень 5—7). Ограниченная информация, доступная МЭ, приводит к ограниченной функциональности регистрации в МЭ с фильтрацией пакетов. Из-за большого количества переменных, используемых в решениях по управлению доступом, они подвержены нарушениям безопасности, вызванным неправильными конфигурациями.

10.2.2 Архитектура двудомного шлюза

Двудомный шлюз — это прокси-сервер приложений/шлюз уровня приложений, который разрывает сквозное соединение. Двудомный шлюз, показанный на рисунке 4, состоит из узла с двумя сетевыми интерфейсами A и B и с отключенной возможностью пересылки IP-адресов внутри узла. Таким образом, IP-пакеты из одной сети (например, сети Интернет) не направляются напрямую в другую сеть (например, во внутреннюю сеть). Системы внутренней сети могут взаимодействовать с двудомным узлом, и системы за МЭ во внешних сетях могут взаимодействовать с двудомным узлом, но эти системы не могут напрямую взаимодействовать друг с другом.

Если узел оснащен несколькими сетевыми картами, то существуют варианты конфигурации, например для отдельных подключений к сети Интернет, к поставщикам Интернет-услуг или к внутренней

сети с различными серверами, такими как серверы электронной почты или серверы регистрации событий. В этом случае он называется мультидомным шлюзом.

При необходимости маршрутизатор, действующий в качестве пакетного фильтра, может быть подключен к внешним сетям для обеспечения дополнительной защиты путем фильтрации сетевых пакетов. Двудомный шлюз блокирует весь прямой IP-трафик между внешними сетями и защищенным узлом сети. Доступ предоставляется службами прокси-сервера приложений на МЭ.

Рисунок 4 — Двудомный шлюз

Двудомный шлюз представляет собой более «квалифицированный» тип шлюза безопасности, поскольку он скрывает внутренние IP-адреса от систем внешних сетей и обеспечивает возможность регистрации, которая может использоваться в сочетании с СОВ для обнаружения возможных действий злоумышленника. Ограниченная гибкость — это возможность передачи только таких служб, для которых существует прокси-сервер; ограниченная гибкость может быть недостатком для некоторых узлов сети.

Эту проблему может решить дополнительный маршрутизатор, если в этом случае может быть установлено надежное соединение в обход шлюза безопасности. Безопасность узла, используемого для МЭ, имеет решающее значение для общей защиты, потому что, если МЭ скомпрометирован, то злоумышленник может получить доступ к внутренним системам.

10.2.3 Архитектура экранированного узла

Архитектура экранированного узла, показанная на рисунке 5, объединяет маршрутизатор с фильтрацией пакетов с узлом-бастионом, используя прокси-сервер приложений. Узел-бастион находится в защищенной части подсети маршрутизатора. В этой архитектуре первичная защита обеспечивается маршрутизатором с фильтрацией пакетов, например, чтобы пользователи не могли обходить прокси-серверы для установления прямых соединений с внутренней сетью.

Рисунок 5 — Экранированный узел

Фильтрация пакетов на экранирующем маршрутизаторе настроена таким образом, что узел-бастион является единственной системой, с которой узлы внешних сетей могут открывать соединения.

Такой узел-бастион, как МЭ уровня приложений, состоит из служб прокси-сервера, которые пропускают или блокируют службы в соответствии с политикой узла. Маршрутизатор отфильтровывает потенциально опасные протоколы до передачи их в узел-бастион.

Трафик приложений из внешних сетей на узел-бастион маршрутизируется; весь другой трафик от внешних сайтов отклоняется. Маршрутизатор отклоняет весь трафик приложения, исходящий из внутренних сетей, если только он не пришел с узла-бастиона.

10.2.4 Архитектура экранированной подсети

Архитектура экранированной подсети, изображенная на рисунке 6, представляет собой вариант архитектур с двудомным шлюзом и экранированным узлом. Это добавляет дополнительный уровень защиты к архитектуре экранированного узла, присоединяя сеть периметра, что далее изолирует внутреннюю сеть от внешних сетей, таких как сеть Интернет.

Рисунок 6 — Архитектура экранированной подсети

Для создания внутренней экранированной подсети используются два маршрутизатора. В этой подсети, иногда называемой ДМЗ или сетью периметра, размещается узел-бастион или МЭ уровня приложений, однако в ней также могут размещаться веб-сервер(ы), сервер(ы) электронной почты или DNS-сервер(ы) и другие системы, требующие тщательно контролируемого доступа. Внешний маршрутизатор ограничивает доступ из внешних сетей к конкретным системам в экранированной подсети (например, маршрутизация трафика электронной почты с узлов сети Интернет на сервер электронной почты) и блокирует весь другой трафик во внешние сети, исходящий из систем, которые не должны создавать соединения (например, монтирование файловой системы на внешние системы). Внутренний маршрутизатор передает трафик в и из систем в экранированной подсети в соответствии с существующими правилами (например, маршрутизация трафика электронной почты от систем узла сети к серверу электронной почты и наоборот).

Для двудомного и часто многодомного шлюза важно, чтобы ни одна внутренняя система не была напрямую доступна из внешних сетей и наоборот. Благодаря экранированной архитектуре подсети нет необходимости в реализации соответствующего узла-бастиона шлюза уровня приложений в качестве двудомной системы. С архитектурой экранированной подсети нет абсолютной необходимости для реализации соответствующего базового узла шлюза уровня приложений в качестве системы с двойным интерфейсом.

Экранированная архитектура подсети может больше подходить для узлов с большим объемом трафика или узлов, которым требуется обеспечить высокоскоростной трафик.

11 Рекомендации по выбору продукта

11.1 Обзор

Предполагается, что если организация подключена к сети Интернет, то ее сети уже защищены каким-либо МЭ с фильтрацией пакетов. Если это не так, то на периметре необходимо незамедлительно разместить МЭ и настроить его в соответствии с политикой безопасности, установленной организацией.

Предполагается, что узлы в одной подсети имеют одинаковые уровни доверия. Например, предполагается, что внешние серверы организации (веб, электронная почта, DNS и т. д.) выделены в свою собственную подсеть, отличную от подсети для внутренних узлов организации. Если узлы с существенно разными уровнями доверия находятся в одной подсети, то требуется пересмотреть проект сети так, чтобы границы между различными областями доверия были четкими. Именно на этих границах будут расположены устройства шлюза сетевой безопасности.

Для обеспечения выполнения требований, изложенных в разделе 8, необходим структурированный подход для выбора и конфигурирования шлюзов безопасности. В данном разделе для этого процесса даны некоторые рекомендации, особенно по следующим вопросам:

- выбор архитектуры шлюза безопасности и соответствующих компонентов;
- выбор аппаратной и программной платформ;
- конфигурирование;
- функции и настройки безопасности;
- администрирование;
- регистрация;
- аудит;
- обучение/образование.

В качестве общего руководства следует применять следующие принципы:

- обратить внимание на все возможные угрозы, особенно на внутренние;
- обратить внимание на человеческий фактор, например, с точки зрения управления и обучения;
- делать все как можно проще, хотя более высокие требования по обеспечению безопасности обычно подразумевают и более сложные архитектуры;
- использовать компоненты или устройства в соответствии с их назначением и конфигурацией.

11.2 Выбор архитектуры шлюза безопасности и соответствующих компонентов

Исходя из требований бизнеса и требований по обеспечению безопасности для шлюза безопасности (для получения дополнительной информации см. раздел 8) следует выбрать и адаптировать соответствующую архитектуру шлюза безопасности (обзор возможных архитектур шлюза безопасности см. в 10.2).

Как только архитектура определена, далее должен быть определен каждый компонент этой архитектуры, а их функции должны быть оценены (обзор возможных компонентов см. в 10.2 и подробное описание предоставляемых функций см. в 10.1). На практике часто используются несколько уровней шлюзов.

Следующие подразделы дают некоторые дополнительные рекомендации по выбору правильных компонентов для соответствующих архитектур.

11.3 Программная и аппаратная платформы

При выборе аппаратной платформы следует особенно учитывать производительность, эффективность, надежность и применимость; например, если платформа имеет только Ethernet-интерфейсы, но требуется ретрансляция кадров на V.35, то эта платформа непригодна для использования. Далее следует рассмотреть ОС аппаратного устройства. В целях обеспечения безопасности следует использовать усиленную ОС. Рекомендуется также проверить ее на наличие известных уязвимостей. Программная платформа также должна быть проверена на ее производительность и надежность; например, маршрутизатор с интерфейсом 10BaseT Ethernet не может обеспечить гигабитную пропускную способность в секунду.

11.4 Конфигурирование

В процессе конфигурирования должны учитываться следующие рекомендуемые настройки для сетевых устройств шлюза безопасности:

- настроить коммутируемую сеть для архитектуры экранированной подсети для ДМЗ;
- настроить статическую маршрутизацию между маршрутизатором(ами) и шлюзом безопасности;
- не принимать информацию о маршрутизации от источника;
- на шлюзе безопасности установить только те ПО/программы, которые абсолютно необходимы для работы (так называемое «усиление платформы»);
- убедиться, что порты не открыты по умолчанию;
- убедиться, что порты анализатора коммутируемых портов (SPA) не открыты, если не требуется использование СОВ;
- убедиться, что на интерфейсах устройства заданы пароли;
- настроить отклонение сообщения «Свободная маршрутизация от источника» RIP;
- настроить NAT в случае необходимости;
- настроить прозрачную работу шлюза безопасности;
- настроить контроль доступа на шлюзе безопасности (идентификация, аутентификация);
- в случае сбоя шлюза безопасности исполнять только задачи администрирования;
- обеспечить регистрацию всех событий администрирования и всего трафика;
- настроить усиление платформы в отношении ОС.

11.5 Функции и настройки безопасности

МЭ уровня приложений должен обеспечивать, как минимум, следующее:
- поддержку основных Интернет-служб (HTTP, FTP, Telnet, SMTP, NNTP);
- поддержку других Интернет-служб;
- поддержку универсальных прокси-серверов (для новых протоколов или служб);
- HTTP-прокси-сервер должен правильно обрабатывать HTTPS;
- отклонение уведомления сообщения BGP (например, посредством общего прокси-сервера);
- поддержку протоколов динамической маршрутизации;
- поддержку веб-служб (например, SOAP/XML);
- поддержку прокси-сервера для заархивированных корпоративных приложений или других бизнес-приложений;
- поддержку идентификации приложений, работающих в потоке протоколов (офисных приложений для повышения производительности, встроенного видео, обмена мгновенными сообщениями и т. д.);
- поддержку фильтрации входящего трафика на наличие вредоносных программ и т. д. в случае VPN-соединения;
- возможность разрешения, запрета или сброса соединений или пакетов.

Устройство фильтрации пакетов должно, как минимум, иметь возможность:
- поддержки фильтрации пакетов на основе:
- IP-адреса источника и назначения;
- порта источника и назначения (для TCP, UDP);
- направления соединения (входящее, исходящее).

И устройство фильтрации пакетов и устройство фильтрации с отслеживанием состояния должны, как минимум, иметь возможность:
- сохранять согласованные правила фильтрации;
- фильтровать пакеты для каждого сетевого интерфейса отдельно;
- поддерживать многоадресные пакеты, если необходима кластеризация устройств;
- сохранять порядок правил фильтрации на шлюзе безопасности;
- ограничивать длину фрагментов IP-пакетов и определять минимальное смещение фрагмента;
- фильтровать ICMP-сообщения «назначение недоступно» и «перенаправление»;
- предотвращать подделку внутренних IP-адресов, если они приходят из сети Интернет (противодействие атаке типа «IP Spoofing»).

Кроме того, фильтрующее устройство с отслеживанием состояния должно, как минимум, быть способно:
- поддерживать службы NFS, NIS, RPC, RIP, OSPF, DNS, WAIS путем адекватной защиты на основе динамических пакетных фильтров;
- обнаруживать определенные атаки типа «отказ в обслуживании», такие как атака типа «TCP-SYN flooding»;
- предотвращать угадывание порядкового номера TCP;

- противостоять атакам типа «ping-of-death» (вид атаки типа «отказ в обслуживании»);
- совместно использовать команды FTP с определенными правами доступа;
- разрешать сохранение контекстной информации, например проверять динамически назначенные номера портов;
- фильтровать другие сетевые объекты (домены, группы, объекты VPN и т. д.);
- предотвращать определенные атаки перехвата сеансов (атаки типа «hijacking»).

Рекомендуется проверить другие различные функции или настройки, например:

- создание оповещений при обнаружении вторжения либо на основе регистрации, либо с помощью сенсора обнаружения вторжения;
- следует отметить, что приложения, использующие средства связи SOAP, могут не обнаруживаться МЭ с отслеживанием состояний и МЭ с прокси-сервером уровня приложений. Это дает возможность обойти прокси-сервер приложений и другие политики МЭ. Особое внимание следует уделять обстоятельствам, когда приложениям на основе SOAP требуются соединения, проходящие через шлюзы безопасности: например, некоторые приложения на основе SOAP могут быть защищены с помощью специальных фильтров контента для приложений (в МЭ для XML, который позволяет программировать подходящие фильтры для XML) и/или путем применения политики, которая позволяет приложениям на основе SOAP обмениваться данными через шлюз безопасности, только если он защищен сквозной VPN.

11.6 Возможности администрирования

Для поддержания адекватного уровня безопасности процесс администрирования является одной из наиболее важных задач. Следует обратить особое внимание на следующие функции шлюзов безопасности:

- идентификация и аутентификация администраторов шлюзов безопасности;
- надежный канал связи при выполнении задач администрирования (например, консоль, зашифрованная связь, отдельная сеть);
- удаленное администрирование только со строгой аутентификацией и шифрованием;
- возможность централизованного администрирования в случае развертывания нескольких шлюзов безопасности;
- проверка целостности программ и файлов, используемых шлюзом безопасности;
- способность журналов регистрации шлюза безопасности отправлять оповещения на внешний узел;
- отправка оповещений администратору по определенному защищенному каналу, например по электронной почте, SMS;
- детальные разрешения доступа, например, чтобы можно было проводить аудит политик и мер обеспечения ИБ из учетной записи только для чтения, должны существовать учетные записи «admin» и «только для чтения»;
- простое администрирование.

11.7 Возможности регистрации

Процесс регистрации очень важен, когда необходимо отслеживать потоки данных, например, для аварийного восстановления, судебных расследований и т. д., включая:

- возможность регистрации (идентификация пользователя, IP-адрес источника и назначения, номер порта, время, дата), поскольку чем больше информации хранится, тем качественнее обработка инцидентов;
- возможность синхронизации с NTP-сервером для знания точной даты и времени;
- защита файлов журналов регистрации от вредоносных изменений и НСД.

11.8 Возможности аудита

Шлюз безопасности должен поддерживать возможности аудита для проверки файлов журналов регистрации, следуя при этом базовым понятиям ИБ, таким как конфиденциальность, целостность, доступность, аутентичность, подотчетность и неотказуемость.

11.9 Тренинги и обучение

Основное внимание следует уделять обучению и тренировкам персонала по эксплуатации (использованию) функций шлюза безопасности, включая:

- обеспечение шлюзов безопасности соответствующей документацией и вспомогательными материалами для выполнения установки и внедрения, что поддерживает достаточную защиту сетей и систем;

- разработку учебных материалов для персонала, занимающегося эксплуатацией и обслуживанием;

- персонал, задействованный в эксплуатации и обслуживании шлюза безопасности, должен периодически проходить обучение, что гарантирует, что он поддерживает и сохраняет адекватный уровень знаний и компетенций.

11.10 Типы реализации

Обычно существует два типа реализации МЭ: аппаратная (АМЭ) и программная (ПМЭ). Они могут быть разделены на различные подтипы. АМЭ относится в основном к аппаратным решениям, в настоящее время это наиболее распространенные устройства-шлюзы. Они могут быть подразделены на ПО на базе центрального процессора (например, i386/x64) с усиленной ОС и специализированные устройства, которые часто содержат ASIC для выполнения определенных функций, таких как высокоскоростное сетевое экранирование или ускорение VPN. Есть также некоторые реже используемые АМЭ, встроенные в сетевые интерфейсы.

Некоторые АМЭ также имеют возможность создавать виртуальные МЭ, которые хоть и являются частью одного и того же физического оборудования, но логически разделены и имеют собственные интерфейсы, наборы правил и связанные с ними таблицы маршрутизации.

ПМЭ могут представлять собой более традиционный программный пакет, устанавливаемый поверх усиленной ОС, персональные МЭ для систем конечных пользователей или виртуальные образы, которые можно использовать в виртуальных серверных средах.

Некоторые ПМЭ для управления потоком трафика из виртуальных систем располагаются на уровне гипервизора.

11.11 Высокая доступность и режимы работы

В настоящее время для повышения доступности большинство организаций используют какую-либо технологию высокой доступности или кластеризации. Обычно это достигается технологиями производителя, а также использованием коммутаторов с балансировкой нагрузки. Рекомендуется учитывать единую точку отказа шлюза безопасности, которая может повлиять на доступность.

11.12 Дополнительные рекомендации

Рекомендуется проверить другие системы и устройства, которые могут повлиять на общий уровень безопасности, например:

- защита любых подключений удаленного доступа шлюзом безопасности;
- антивирусная проверка;
- фильтрация исполняемого кода, такого как Java, JavaScript, MIME, ActiveX; даже если это включено в передачу данных по FTP;
- использование шлюзов безопасности в контексте VPN;
- интеграция продуктов защиты контента третьих лиц.

Архитектура шлюзов безопасности часто объединяет решения по защите контента, которые включают в себя сканирование и проверку файлов или Интернет-трафика (например, SMTP, FTP, HTTP) на наличие вирусов или вредоносного кода. С одной стороны, существуют подходы с отдельными серверами шлюзов, которые сканируют Интернет-трафик или определенные Интернет-службы на наличие вирусов или вредоносного кода, проходящего через серверы, и предотвращают проникновение опасного кода во внутреннюю сеть. С другой стороны, существуют решения с более тесной интеграцией в МЭ возможностей проверки контента с помощью DLL или API. Часто в подходы к обеспечению безопасности контента также включается проверка или фильтрация URL-адресов;

- интеграция СОВ.

В контексте шлюзов безопасности СОВ расположены в ДМЗ. К таким системам относятся МЭ, а также важные серверы приложений, которые контролируются сенсором СОВ. Дополнительную информацию по этому вопросу можно найти в ISO/IEC TR 15947:2002.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 27033-1	IDT	ГОСТ Р ИСО/МЭК 27033-1—2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- IDT — идентичный стандарт.

Библиография

[1] ISO/IEC TR 15947:2002, Information technology — Security techniques — IT intrusion detection framework

[2] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements

[3] ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls

[4] ISO/IEC 27033-3:2010, Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues

[5] Recommendation ITU-T X.25:1996, Interface between Data Terminal Equipment (DTE) and Data Circuit-terminating Equipment (DCE) for terminals operating in the packet mode and connected to public data networks by dedicated circuit

[6] IEEE 802.3: Defines the MAC layer for bus networks that use CSMA/CD

[7] Bundesamt für Sicherheit in der Informationstechnik (BSI). Gesicherte Verbindung von Computernetzen mit Hilfe einer Firewall. Bonn, 1997

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI Firewall Studie II. Bonn, 2001

[9] Chapman, D.B., & Zwicky, E.D. Building Internet Firewalls. O'Reilly, Cambridge, 2000

[10] Cheswick, W.R., & Bellovin, S.M. Firewall and Internet Security: Repelling the Wily Hacker. Addison-Wesley, Reading, 1994

[11] Ellermann, U. Firewalls: Isolations- und Audittechniken zum Schutz von lokalen, Computer-Netzen. Berlin 1994 (DFN-Bericht Nr. 76)

[12] Siyan, K., & Hare, C. Internet Firewalls and Network Security. New Riders Publishing, Indian apolis, 1995

[13] Wack, J., Cutler, K., Pole, J. Guidelines on Firewalls and Firewall Policy. Recommendations of the National Institute of Standards and Technology, 2001 [National Institute of Standard and Technology (NIST) Special Publication 800-41]

УДК 006.354:004.056.5:006.354 ОКС 35.040

Ключевые слова: методы и средства обеспечения безопасности, безопасность сетей, обмен данными в сетях, шлюзы безопасности, межсетевой экран

Технический редактор *И.Е. Черепкова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 21.05.2021. Подписано в печать 02.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,80.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru

Федеральное агентство
по техническому регулированию
и метрологии
Федеральное агентство
по техническому регулированию
и метрологии

Федеральное агентство
по техническому регулированию
и метрологии
Федеральное агентство
по техническому регулированию
и метрологии