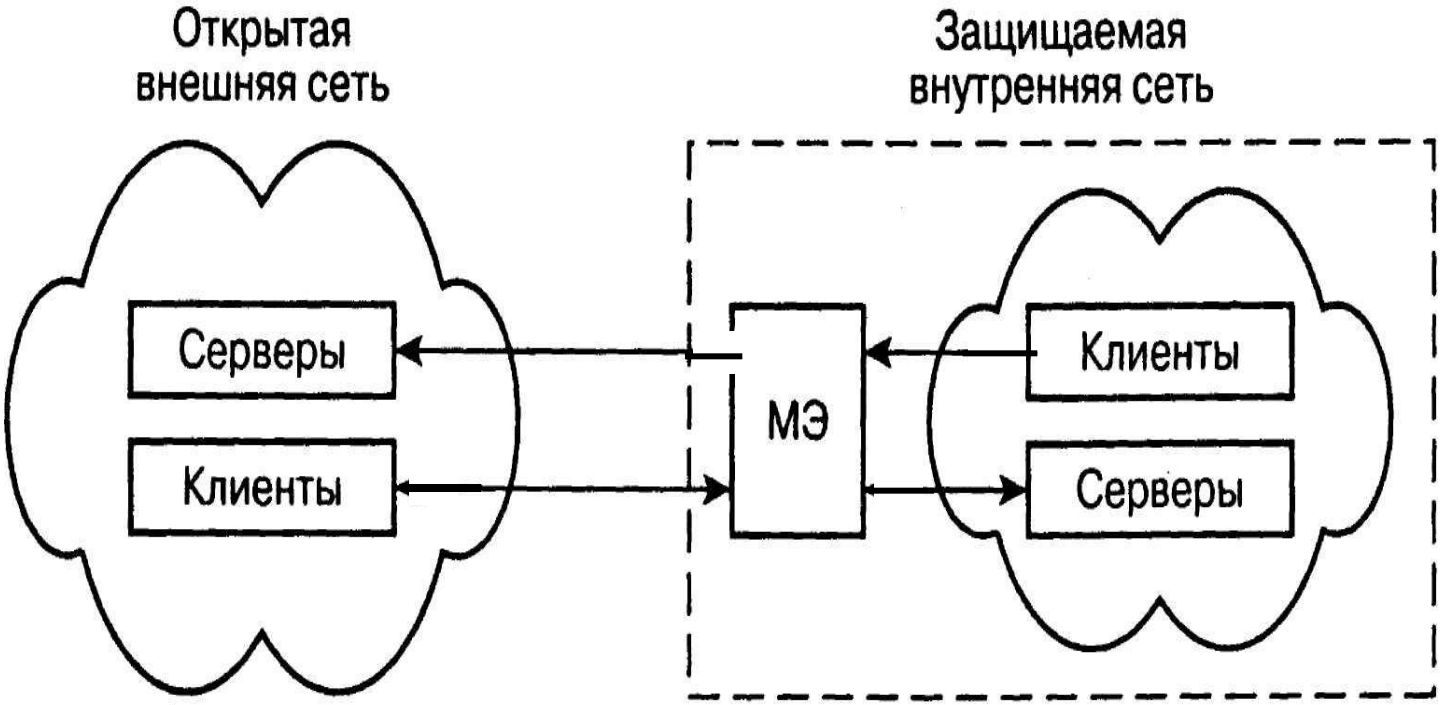
Межсетевые экраны

1.Назначение и классификация межсетевых экранов.
2. Принципы построения и функционирования межсетевых экранов на различных уровнях модели взаимодействия открытых систем.
3. Требования к межсетевым экранам.

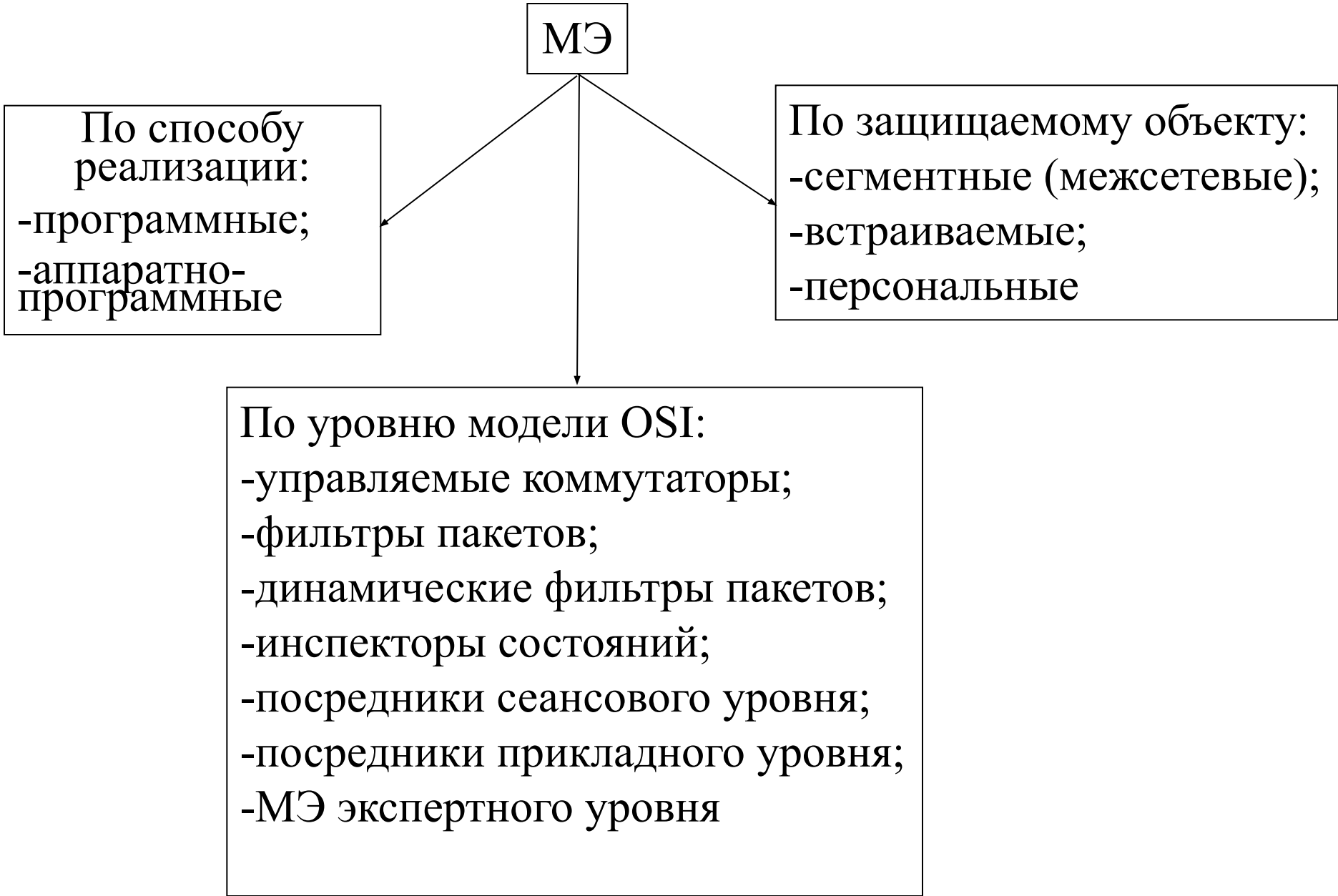
Схема подключения межсетевого экрана



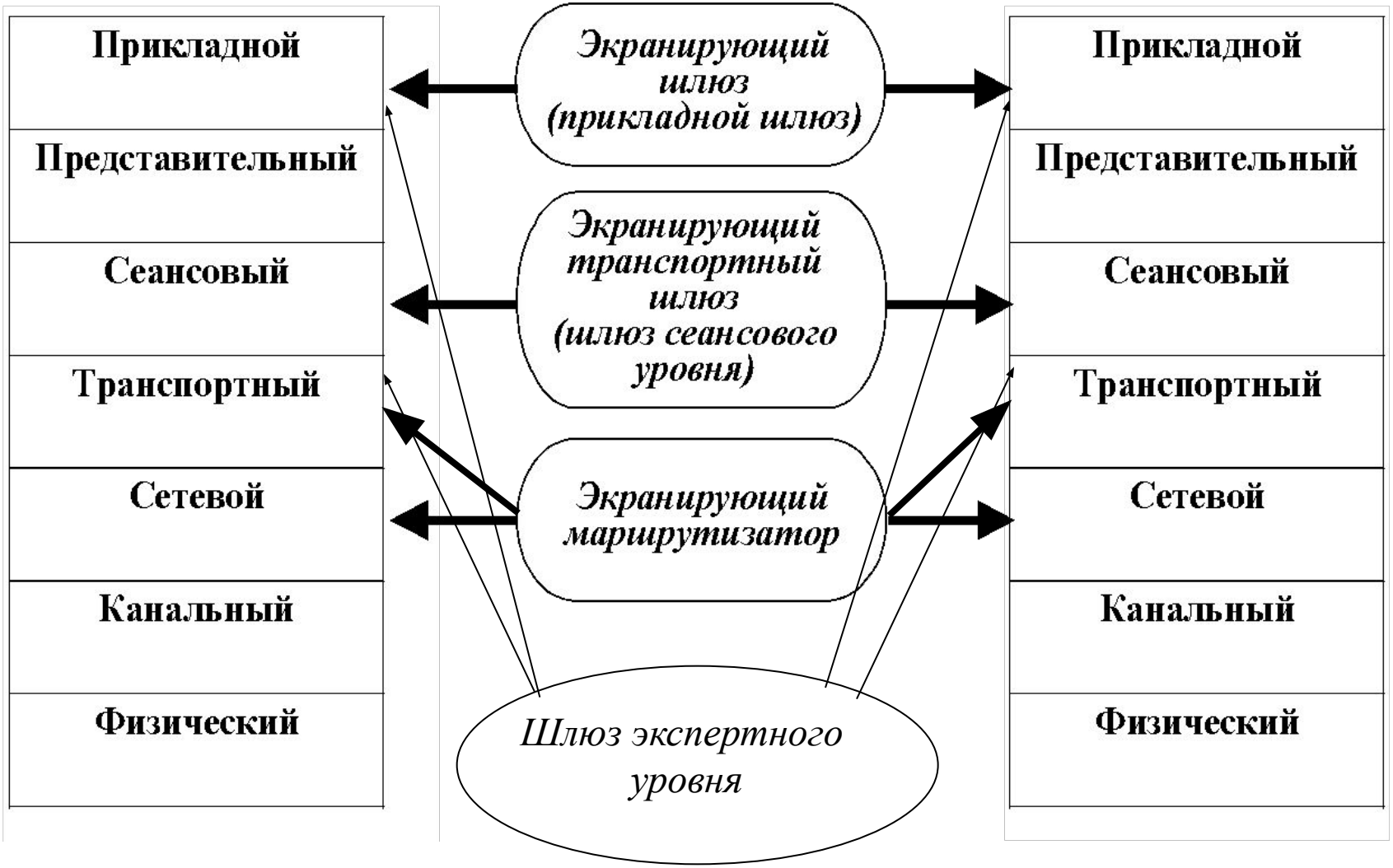
МЭ представляет собой локальное или функционально-распределенное средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС, и обеспечивает защиту АС посредством фильтрации информации.

Брандмауэр, Firewall

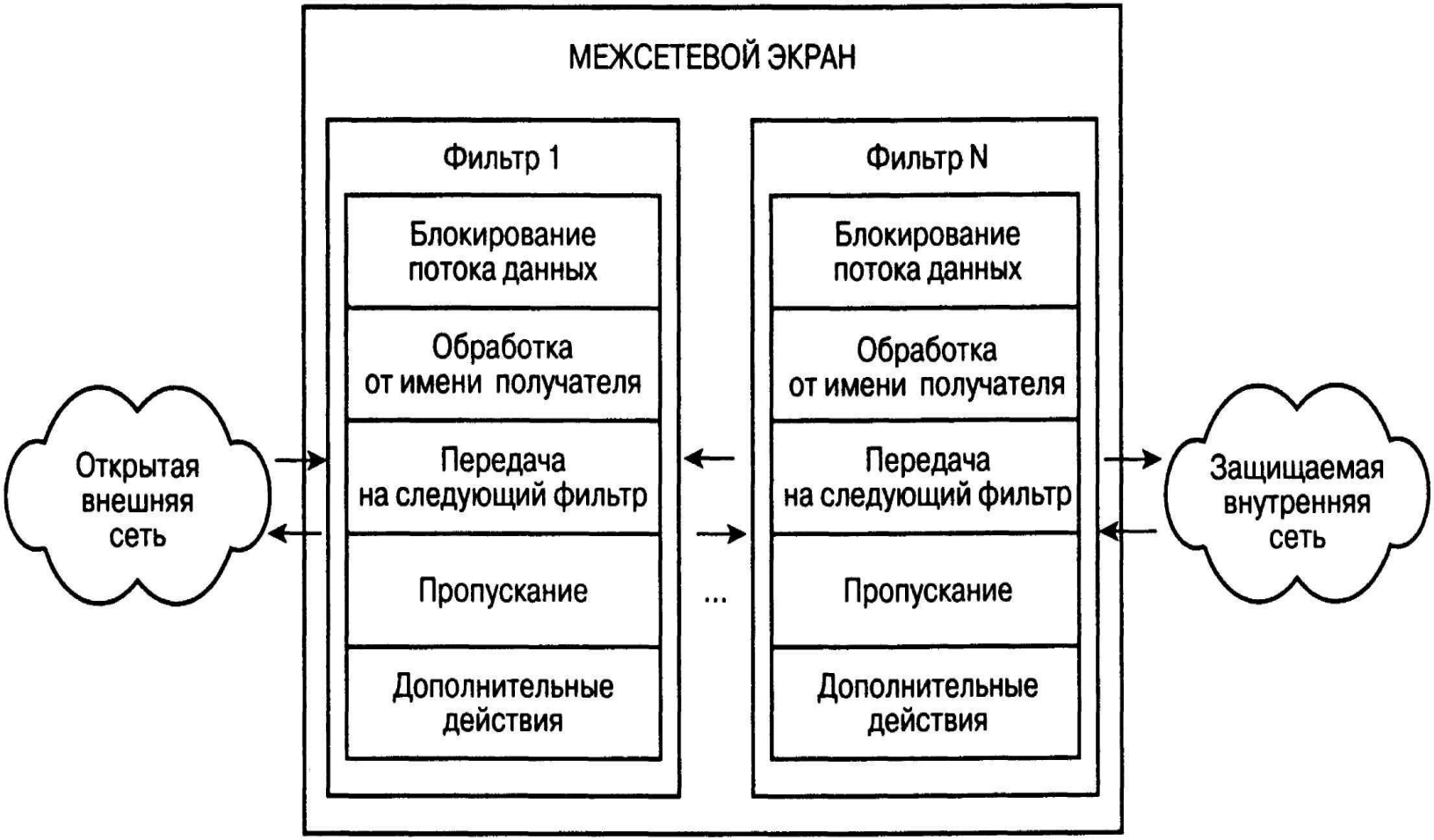
Классификация сетевых экранов



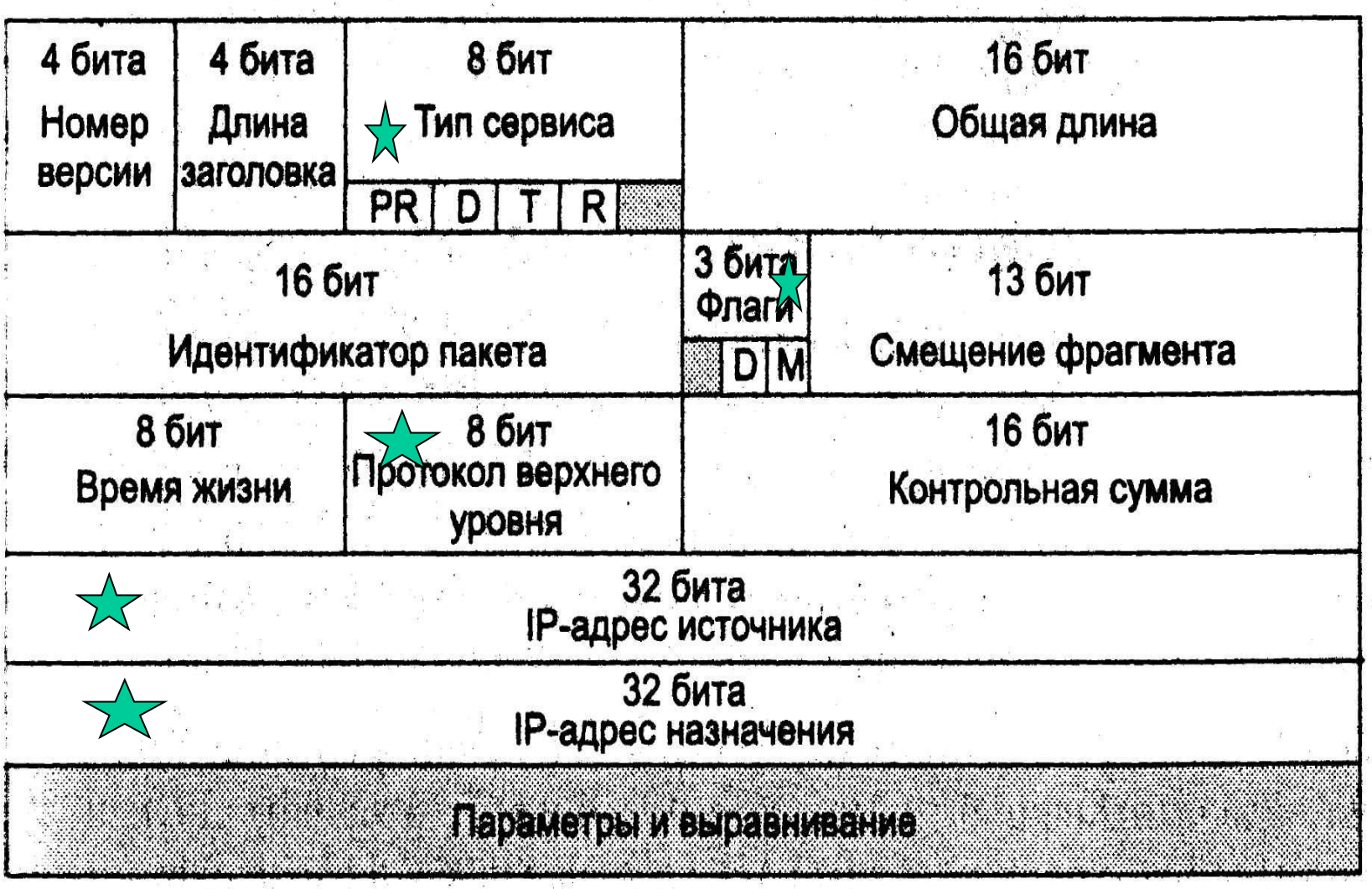
Типы межсетевых экранов



Фильтрация трафика

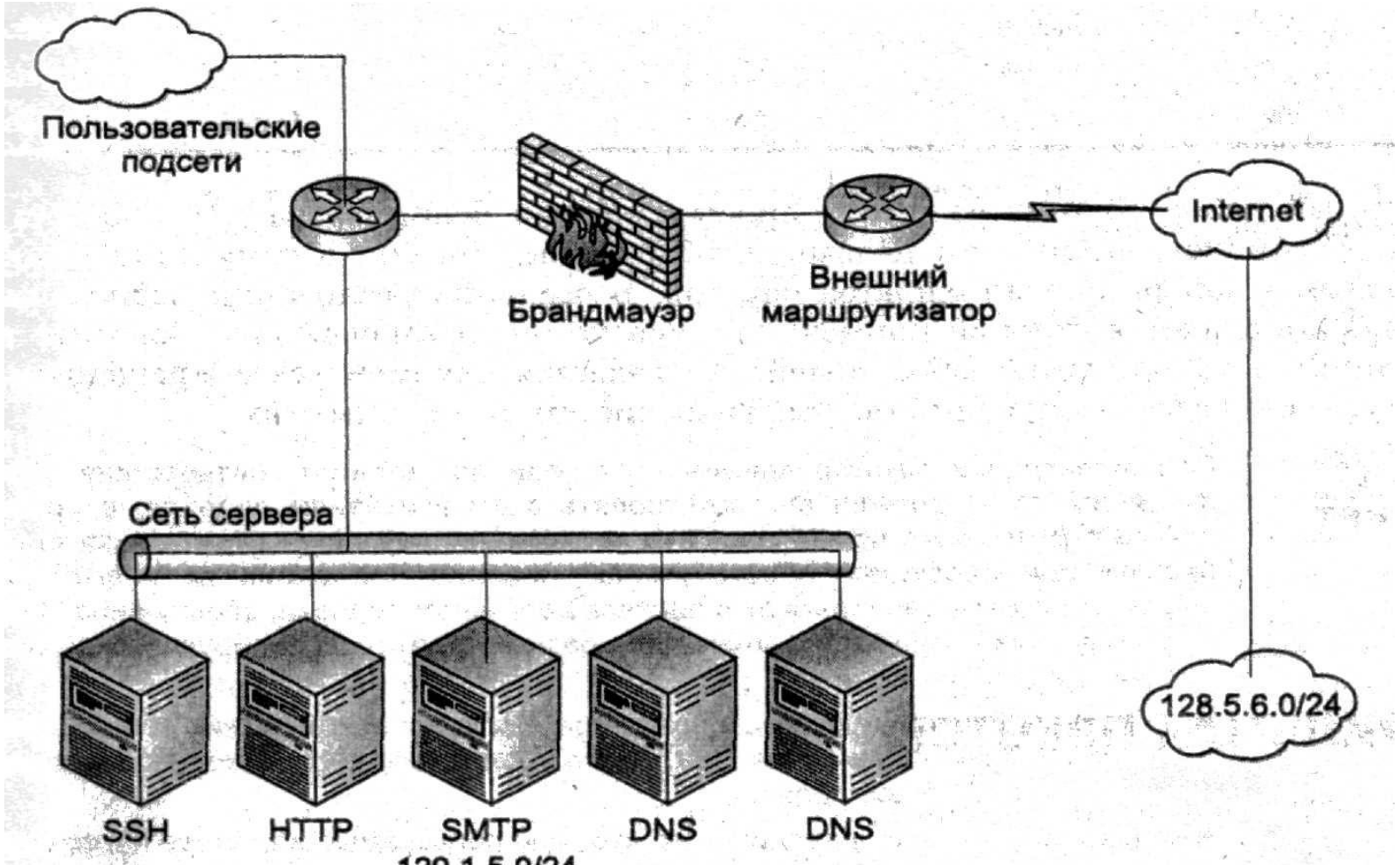


Структура заголовка IP-пакета



Структура TCP-заголовка

Пример топологии сети с фильтрацией пакетов



Типичный набор правил фильтрации входящих пакетов

Правило	Тип протокола	Адрес отправителя	Адрес получателя	Порт отправителя	Порт получателя	Действие
1	TCP	128.5.6.0/24	129.1.5.155	1023	22	Разрешить
2	TCP	Любой	129.1.5.154	1023	80	Разрешить
3	TCP	Любой	129.1.5.150	1023	25	Разрешить
4	UDP	Любой	129.1.5.152	1023	53	Разрешить
5	UDP	Любой	129.1.5.153	1023	53	Разрешить
6	Любой	Любой	Любой	Любой	Любой	Запретить

1. Доступ разрешен для небольшой подсети для удаленного доступа к локальным ресурсам (протокол Telnet).
2. Разрешена передача входящих пакетов для трафика HTTP на Web сервер домена.
3. Разрешен входящий трафик на почтовый сервер SMTP.
4,5. Прием дейтаграмм на два сервера DNS.
6. Запрет всех пакетов, которые не соответствуют критериям правил 1-5.

Достоинства и недостатки МЭ фильтрации пакетов

Достоинства:

- простота реализации;
- Высокая производительность;
- Прозрачность для программных приложений;
- Малая стоимость
- Недостатки:
- Не обеспечивают высокой безопасности, т.к. просматривают только заголовки.
- Не поддерживают функции аутентификации, шифрования и имитозащиты данных:
- Уязвимы к атакам подмены адресов.

Схема функционирования шлюза сеансового уровня

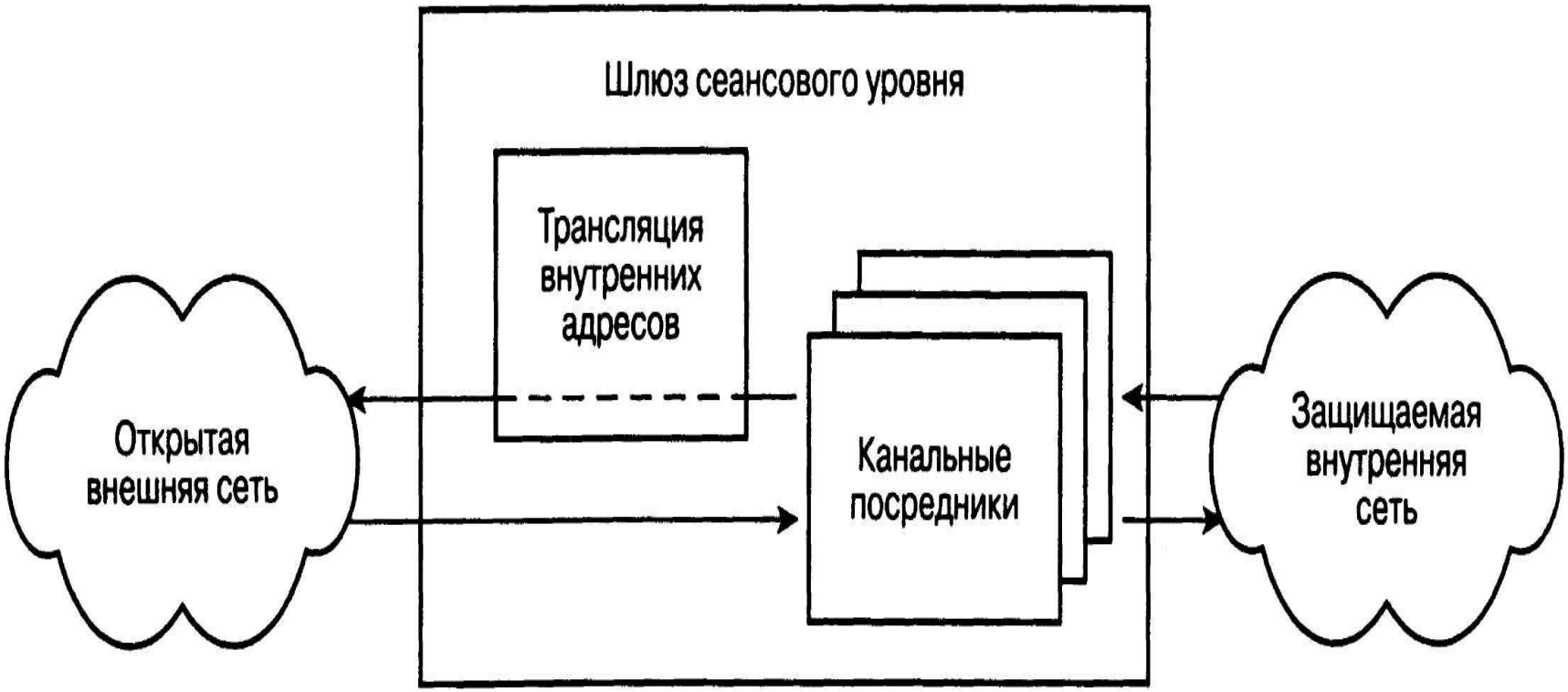
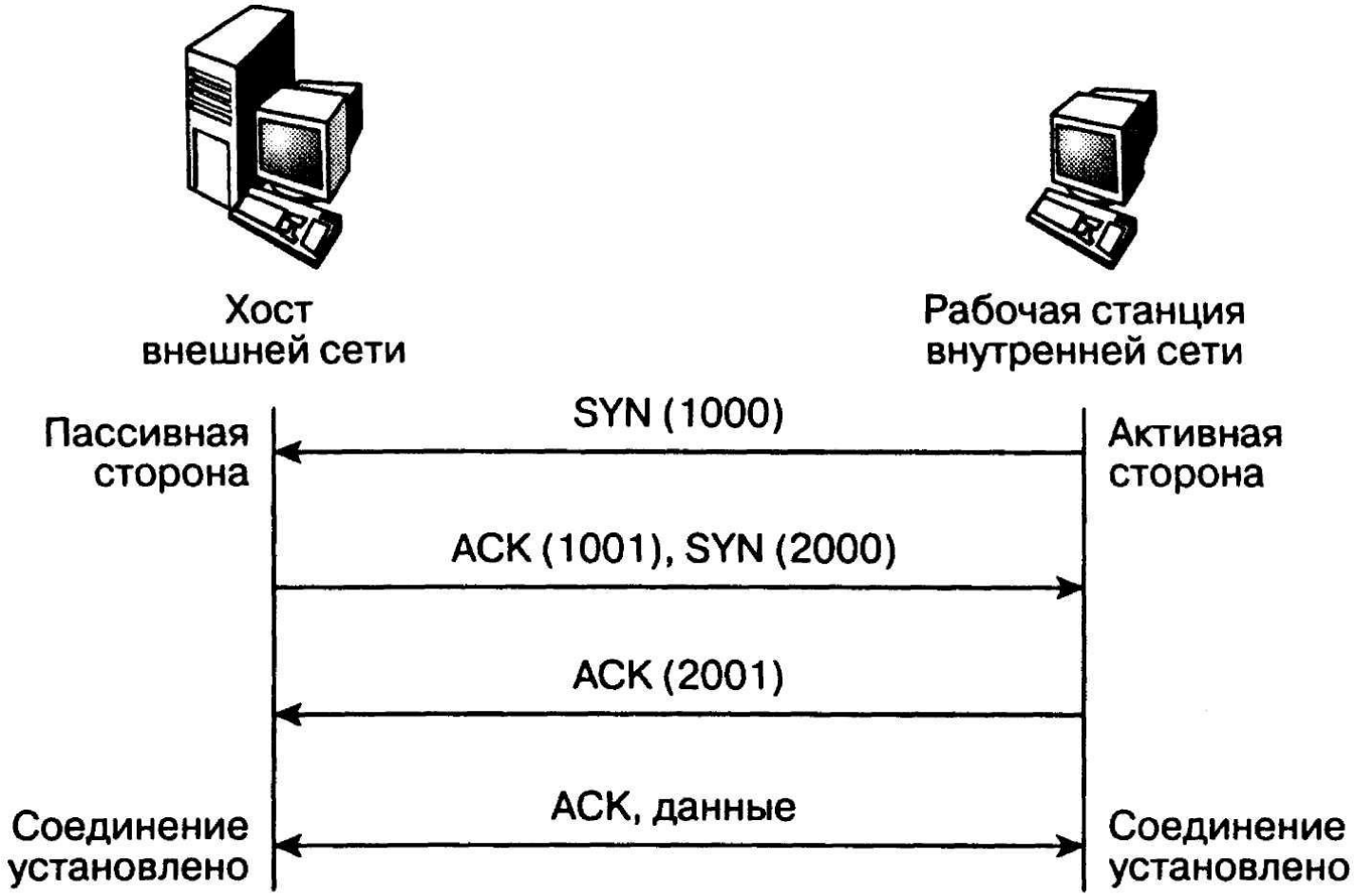
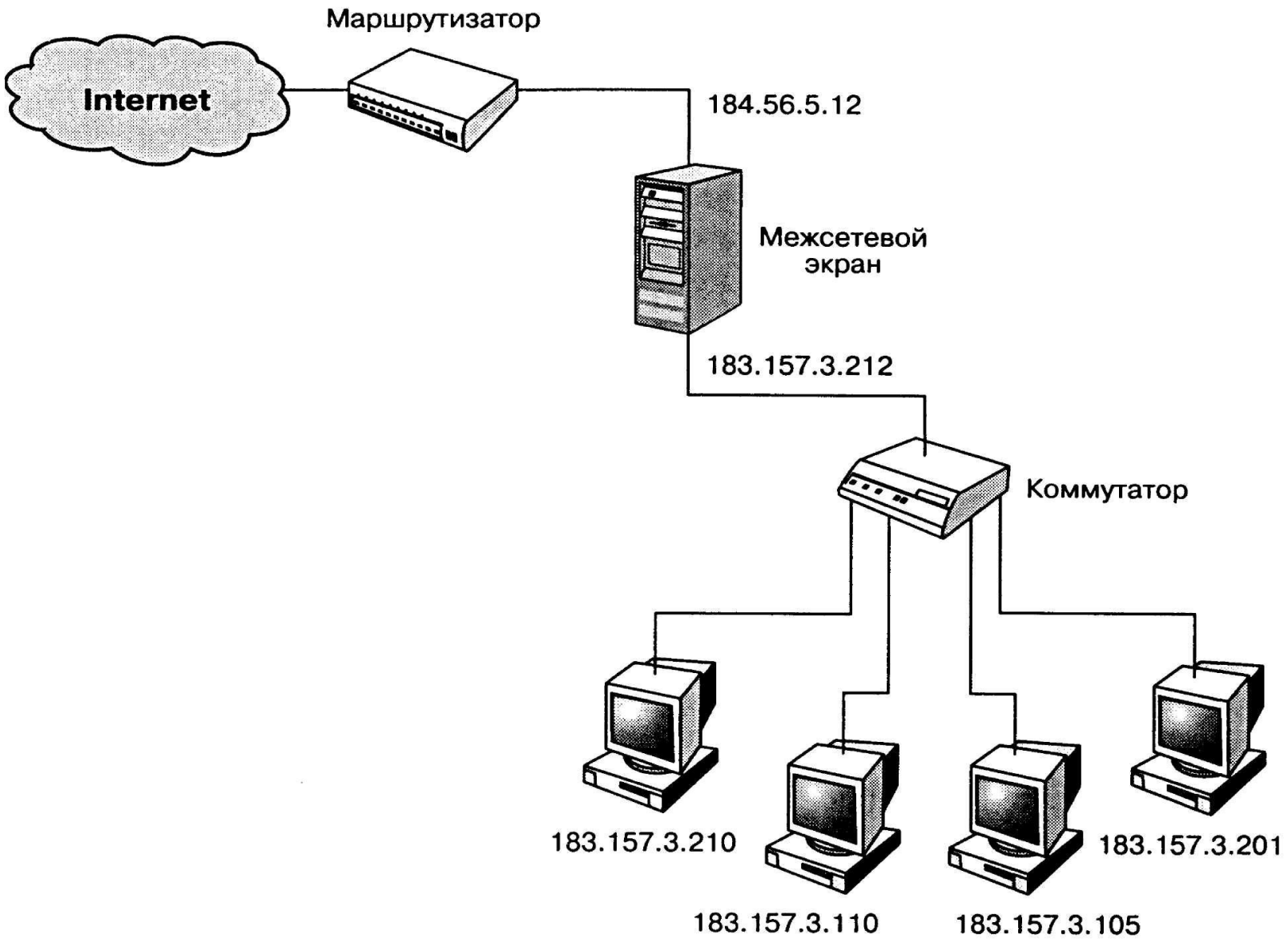


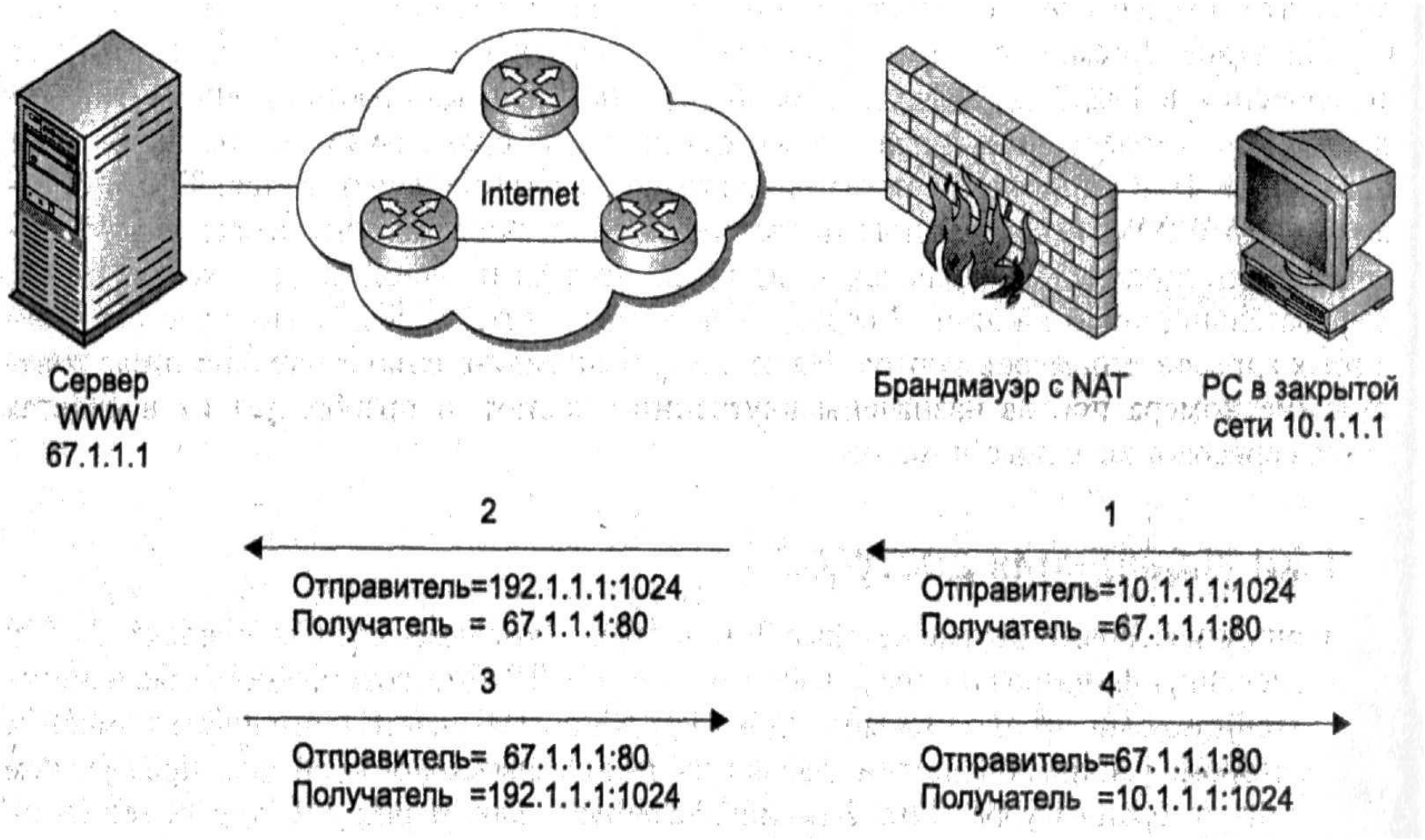
Схема трехэтапного квитирования связи по протоколу TCP



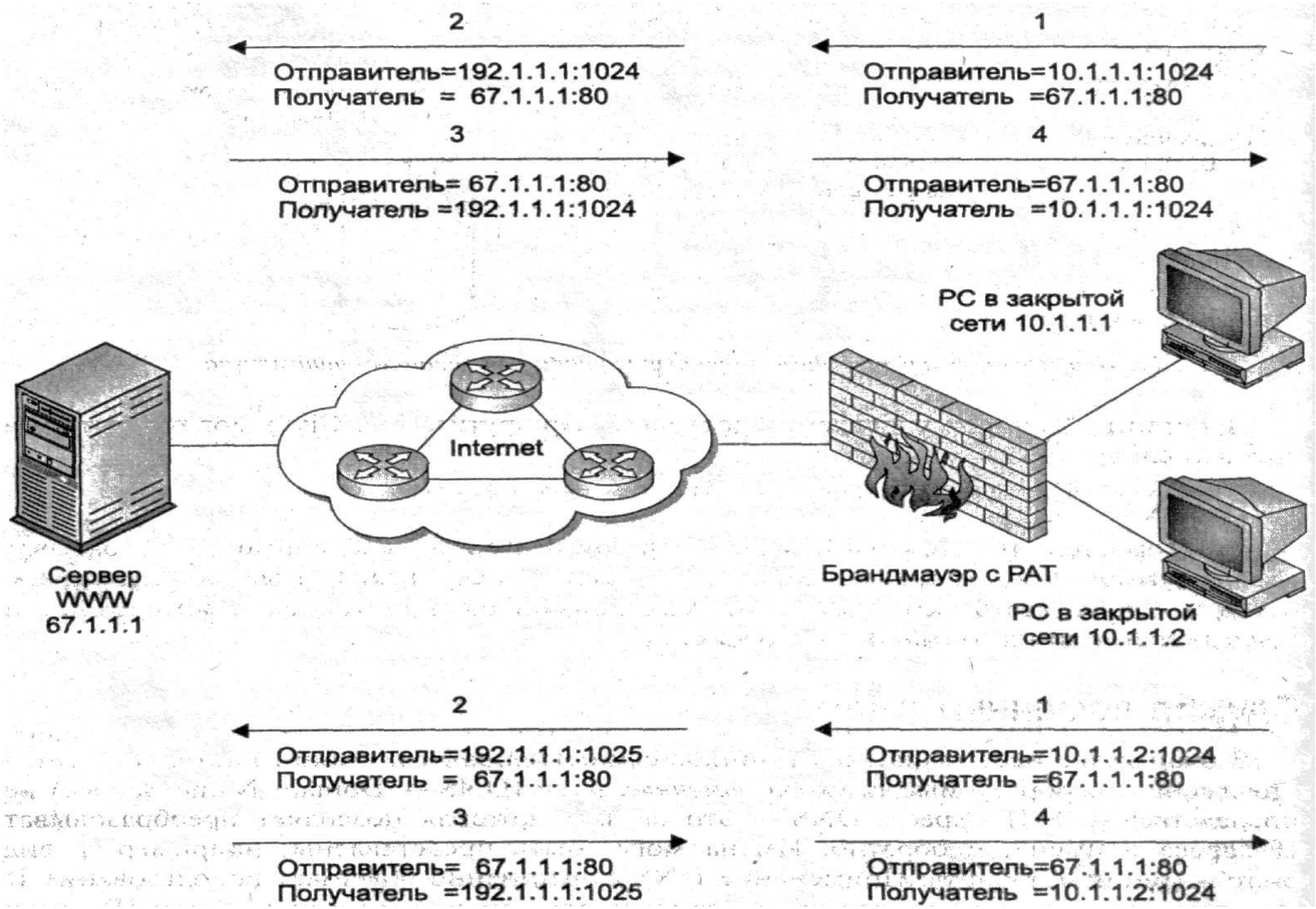
Трансляция сетевых адресов



NAT


Internet
Сервер
WWW
67.1.1.1
Брандмауэр с NAT
PC в закрытой
сети 10.1.1.1
2
Отправитель=192.1.1.1:1024
Получатель = 67.1.1.1:80
1
Отправитель=10.1.1.1:1024
Получатель =67.1.1.1:80
3
Отправитель= 67.1.1.1:80
Получатель =192.1.1.1:1024
4
Отправитель=67.1.1.1:80
Получатель =10.1.1.1:1024

PAT


2
Отправитель=192.1.1.1:1024
Получатель = 67.1.1.1:80
3
Отправитель= 67.1.1.1:80
Получатель =192.1.1.1:1024
1
Отправитель=10.1.1.1:1024
Получатель =67.1.1.1:80
4
Отправитель=67.1.1.1:80
Получатель =10.1.1.1:1024
PC в закрытой сети 10.1.1.1
Internet
Сервер WWW 67.1.1.1
Брандмауэр с PAT
PC в закрытой сети 10.1.1.2
2
Отправитель=192.1.1.1:1025
Получатель = 67.1.1.1:80
3
Отправитель= 67.1.1.1:80
Получатель =192.1.1.1:1025
1
Отправитель=10.1.1.2:1024
Получатель =67.1.1.1:80
4
Отправитель=67.1.1.1:80
Получатель =10.1.1.2:1024

Достоинства и недостатки МЭ сеансового уровня

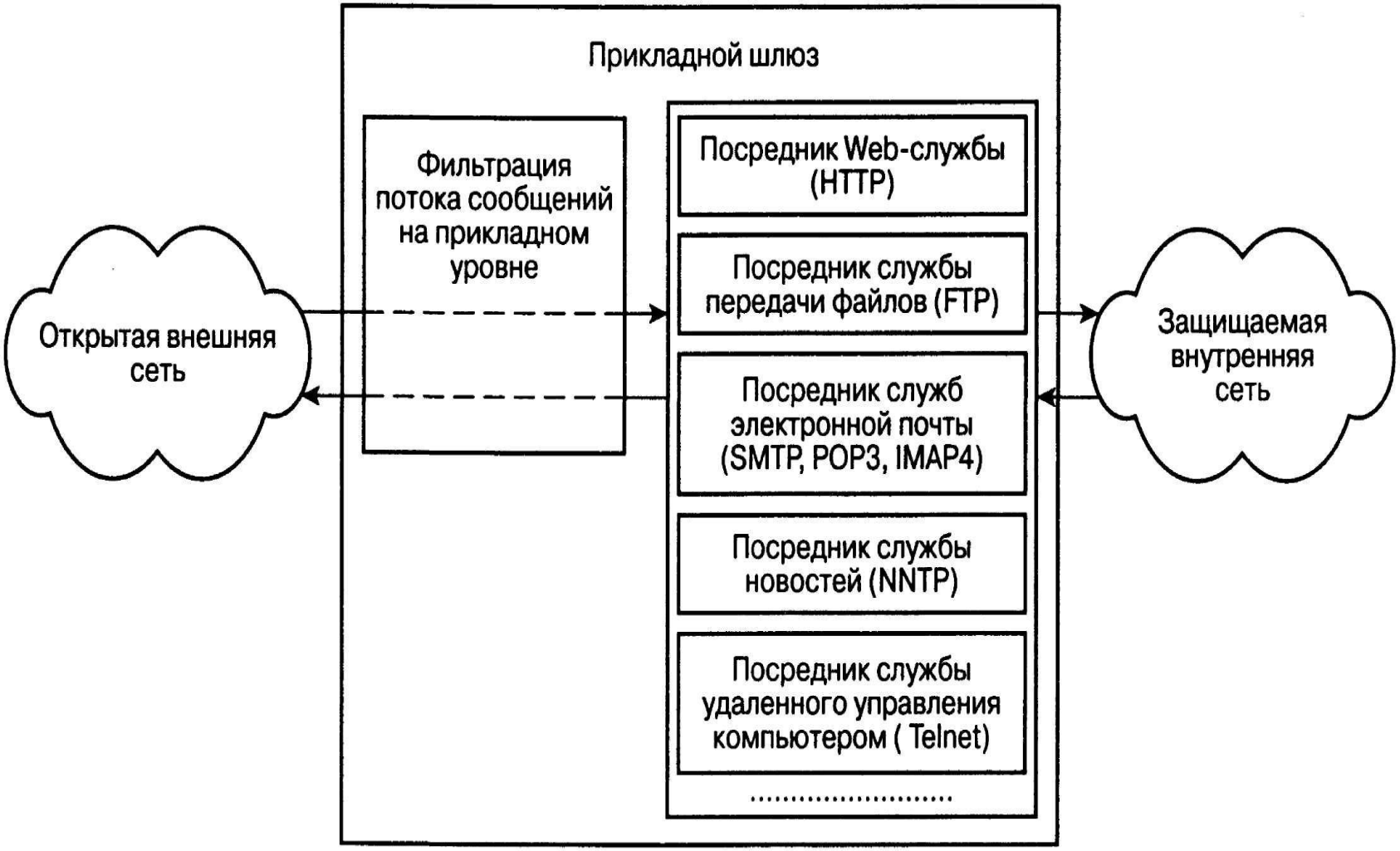
Достоинства:

- Достаточно просты и надежны;
- Высокая производительность;
- Дополняют МЭ фильтрации пакетов функцией контроля виртуального соединения;

Недостатки:

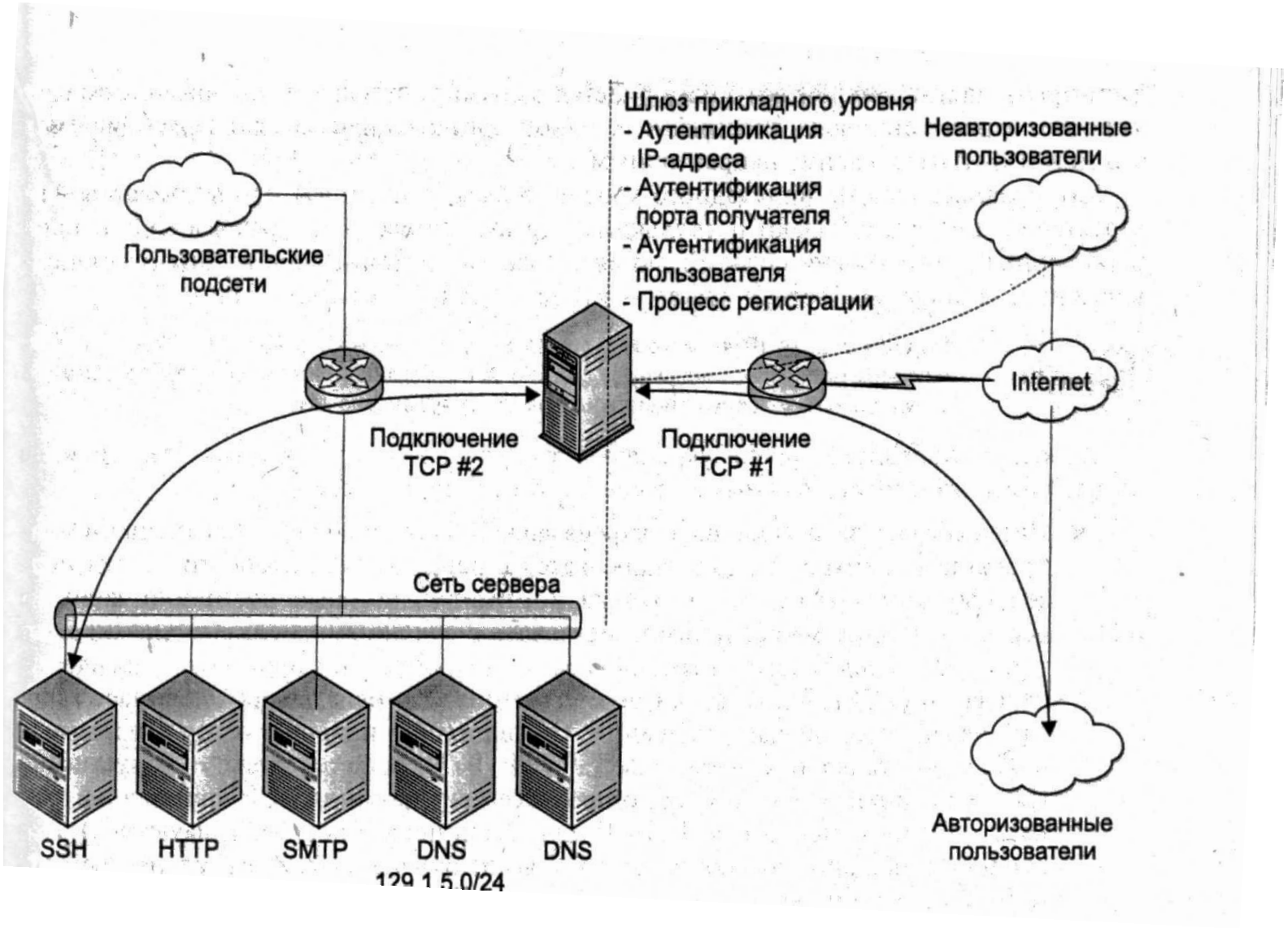
- Не обеспечивают контроль за содержимым пакетов;
- Не поддерживают функции аутентификации пользователей, шифрования и имитозащиты данных:
- При перехвате нарушителем TCP сессии может быть реализована атака даже в рамках защищенной сессии.

Схема функционирования прикладного шлюза



- МЭ прикладного уровня представляет универсальный компьютер, на котором функционируют программы-посредники (экранирующие агенты), по одному для каждого обслуживаемого прикладного протокола (HTTP, FTP, SMTP, NNTP, и др.

Схема виртуального подключения через шлюз прикладного уровня



Достоинства и недостатки МЭ прикладного уровня уровня

Достоинства:

- Высокий уровень защиты, благодаря реализации функции посредничества;
- Возможна реализации дополнительных проверок содержимого пакетов;
- При отказе МЭ блокируется сквозная передача между разделяемыми сетями;

Недостатки:

- Относительно высокая стоимость;
- Большая сложность самого МЭ, процедур его установки и конфигурирования;
- Отсутствие прозрачности для пользователей.
- Снижение пропускной способности линии между межсетевого взаимодействия

Требования к межсетевым экранам

Показатели защищенности	**5**	**4**	**3**	**2**	**1**
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	-	-	+	=	+
Регистрация	-	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	-	-	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	=
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

Основные характеристики межсетевых экранов

Характеристика \ Средство	"Континент-К" НИП "ИНФОРМЗАЩИТА"	"Застава-Джет" компании "Инфосистемы Джет"	VPNet Office Firewall компании "Инфотекс"	Secure PIX Firewall 520 компании Cisco System	FireWall-1 компании Check Point	Symantec Enterprise Firewall компании Symantec
Наличие аппаратной реализации	+	+	+	+	+	+
Наличие программной реализации:		+	+		+	+
• **для ОС Windows NT / 2000**			+		+	+
• **для ОС Solaris**					+	
• **для ОС Linux**					+	
Технология функционирования:						
• **пакетная фильтрация**	+	+	+	+	+	+
• **использование посредников (proxy)**		+			+	+
• **контекстная проверка (Stateful Inspector)**				+	+	
Аутентификация:						
• **аутентификация администратора**	+	+	+	+	+	+
• **аутентификация пользователей**		+		+	+	+
• **интеграция с базой учетных записей**					+	+

Основные характеристики межсетевых экранов

Трансляция IP адресов (NAT)	+	+		+	+	+
Поддержка шифрования (VPN):						
• **между брандмауэрами**	+		+	+	+	+
• **между клиентом и брандмауэром**	+		+	+	+	+
Защита от типовых атак (IP-spoofing, Denial of Service и др.)	+	+	+	+	+	+
Обнаружение сканирования портов		+			+	
Аудит и сигнализация:						
• **регистрация событий**	+	+	+	+	+	+
• **сигнализация (включая e-mail)**		+		+	+	+
Наличие сертификатов:	+	+	+	+	+	+
Гостехкомиссии России	+	+	+	+	+	+
ICSA				+	+	+

Наименование продукта	Cisco PIX 520 (506, 525, 535)	Check Point FireWall-1	ЗАСТАВА	Raptor Symantec-AXENT	CyberWall-Plus
Поставщик-производитель	Cisco Systems	Check Point	ЭЛВИС+	Symantec-AXENT	Network-1
Класс Гостехкомиссии РФ	3, разовая сертификация (для Cisco PIX 520)	3 (сертификат на серию)	3 (сертификат на серию)	Нет	Готовится к сертификации по 4
Используемая ОС (платформа)	ОС собственной разработки	Solaris (Sparc), NT (x86), HP-UX (HP)	Solaris (Sparc)	Solaris (Sparc), NT (x86), HP-UX (HP)	NT/2000 (x86)
Уровень фильтрации	Сеансовый, сетевой	Прикладной, сеансовый, сетевой	Прикладной, сеансовый, сетевой	Прикладной, сеансовый, сетевой	Прикладной, сеансовый, сетевой
Прозрачность для приложений	Прозрачен	Прозрачен	Прозрачен	Прозрачен	Прозрачен
Proxy	Нет	Нет	Нет	HTTP, FTP, Telnet, Rlogin, RSH, SMTP, POP3, Gopher, SSL, X11, SQL, LP, NNTP, RealAudio, RealVideo, StreamWorks, VDOlive, NetShow, LDAP	HTTP, FTP, RealAudio
Поддержка протокола для фильтрации	FTP, SMTP, Archie, Gopher, Telnet, H.323, NetMeeting, InternetPhone, RealAudio	FTP, RPC, H.323, NetMeeting, DVOlive, NetShow, CU-SeeMe, MS Exchange, RealAudio, SQL Net, Vosaic, WebTheater, WinFrame	RSH, SMTP, SNMP, POP3, Gopher, SSL, X11, SQL, LP, NNTP, RealAudio, RealVideo, StreamWork, VDOlive, NetShow, LDAP	FTP, RPC, H.323, NetMeeting, DVOlive, NetShow, CU-SeeMe, MS Exchange, RealAudio, SQL Net, Vosaic, WebTheater, WinFrame	Более 1000 протоколов
Трансляция сетевых адресов	Есть	Есть	Есть	Есть	Есть

Наименование продукта	Cisco PIX 520 (506, 525, 535)	Check Point FireWall-1	ЗАСТАВА	Raptor Symantec-AXENT	CyberWall-Plus
Аутентификация пользователей	Secure, RADIUS, TACACS+, AXENT, CryptoCard	S/Key, SecurID, RADIUS, TACACS, TACACS+, Defender, OSPassword	RADIUS	S/Key, SecurID, RADIUS, TACACS, TACACS+, Defender, OSPassword	S/Key, SecurID, RADIUS
Генерация отчетов	Текст	Бинарный формат	Текст	Текст	Текст, бинарный формат
Аутентифицируемые протоколы	FTP, HTTP, Telnet	Все	POP3	Все	FTP, HTTP, Telnet, Rlogin
Реагирование на попытки НСД	Есть	Есть	Есть	Есть	Есть
Централизованное администрирование	Есть	Есть (отдельная утилита)	Нет	Есть	Есть
Предельная производительность, Мбит/с	1 Гбит/с	100	10	100	100
Контекстный просмотр кода Java/ActiveX	Да	Да	Нет	Да	Да
Поддержка технологии plug-and-play	Есть	Невозможна	Нет	Есть	Есть
Лицензирование	По количеству соединений (64000–256000 и выше)	На 25, 50, 250, 500 клиентов и неограниченно	На 50, 100 IP и неограниченно	На 25, 50, 250, 500 клиентов и неограниченно	На рабочие станции – 10, 100, 250 клиентов. На корпоративные серверы – 1, 5, 10, 15 серверов. На всю сеть – 100, 500 сессий и неограниченно

Варианты исполнения МЭ

Программно-аппаратные 5000-12000$

Программные

стоимость компьютера;
-стоимость лицензионного дистрибутива операционной системы; -
-стоимость сопутствующего программного обеспечения (например, браузера Internet Explorer или СУБД Oracle);
-стоимость затрат на установку и настройку всего комплекса в целом. Обычно эти затраты составляют 20-30% от стоимости составляющих всего комплекса;

-стоимость поддержки всех составляющих комплекса (компьютера и его аппаратных составляющих, операционной системы, дополнительного ПО и т.д.).

Достоинства специализированных программно-аппаратных решений

-простота внедрения в технологию обработки информации. Средства поставляются уже с заранее установленной и настроенной операционной системой и защитными механизмами, поэтому необходимо только подключить их к сети. Время, затрачиваемое на настройку, существенно меньше, чем в случае установки и настройки межсетевого экрана «с нуля»;

простота управления. Данные средства могут управляться с любой рабочей станции Windows или UNIX. Взаимодействие консоли управления с устройством осуществляется либо по стандартным протоколам, например Telnet или SNMP.
отказоустойчивость и высокая доступность. Исполнение в виде специализированного программно-аппаратного комплекса позволяет реализовать механизмы обеспечения не только программной, но и аппаратной отказоустойчивости и высокой доступности.

высокая производительность и надежность. За счет исключения из операционной системы всех ненужных сервисов и подсистем программно-аппаратный комплекс работает более эффективно с точки зрения производительности и надежности;

специализация на защите. Решение только задач обеспечения сетевой безопасности не приводит к затратам ресурсов на выполнение других функций, например маршрутизации и т.п..

Схемы подключения межсетевых экранов

Межсетевой экран – экранирующий маршрутизатор

Схемы подключения МЭ

Схема единой защиты локальной сети

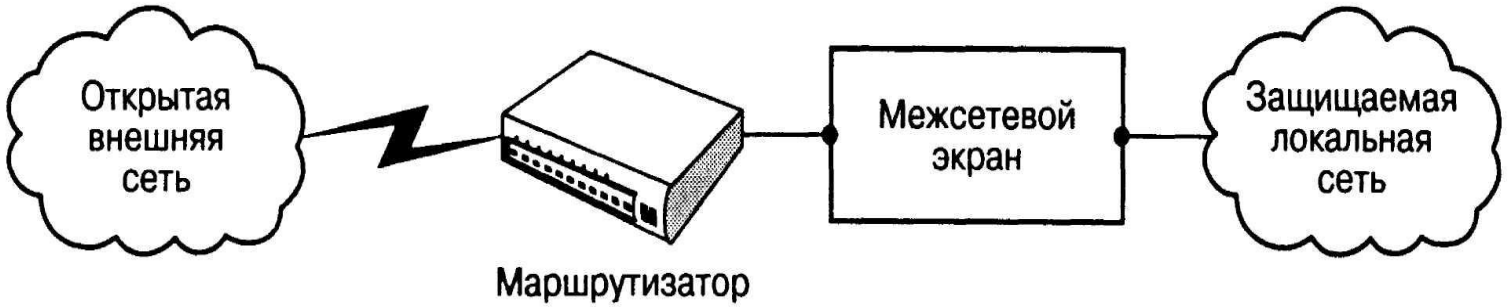
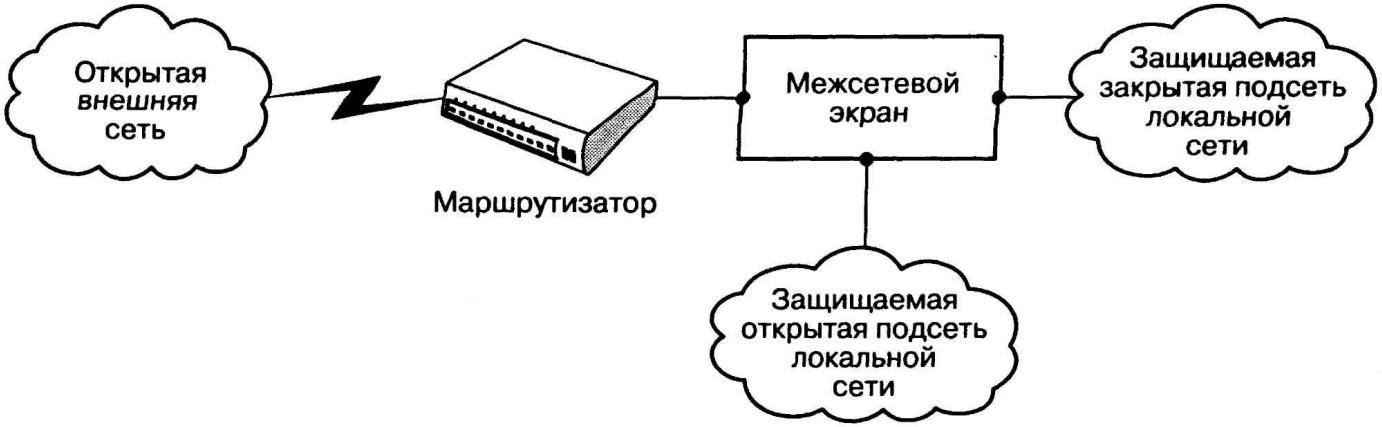


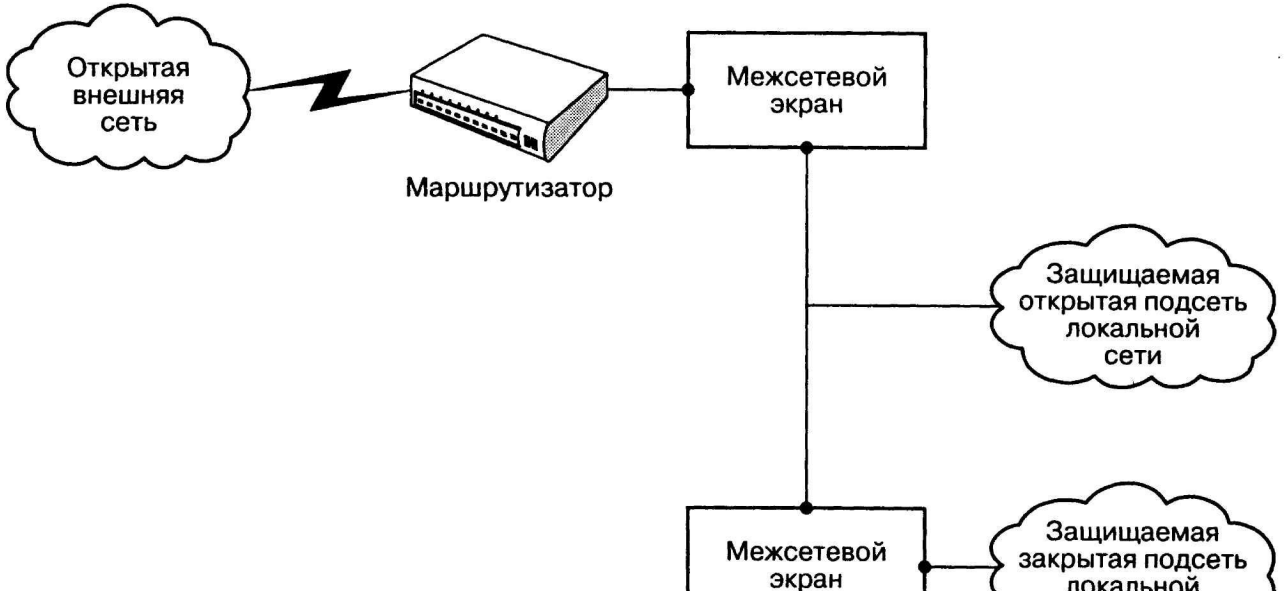
Схема с защищаемой закрытой и незащищаемой открытой подсетями

Схемы с раздельной защитой закрытой и открытой подсетей

На основе одного МЭ с тремя сетевыми интерфейсами



На основе двух МЭ с двумя сетевыми интерфейсами



Сравнительная характеристика VPN продуктов отечественного производства

	ШИП	Застава	ФПСУ-IP	VipNet	Континент-К	Криптон-IP
Производитель	**МО ПНИЭИ**	**Элвис+**	**Амикон**	**Инфо-Текс**	**Информзащита**	**Анкад**
Операц. система	FreeBSD	Win NT/95/98 Sparc/Intel Solaris	Собственная	Win NT/95/98/ ME/2000 Linux	Win NT	MS-DOS 5.0 и выше
Сертификат ГТК или ФАПСИ	Сертиф. ФАПСИ	Класс 3	Класс 3	Класс 1В для АС и класс 3 МЭ	Класс 3	Принят в сертиф.
Использование ГОСТ	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89	ГОСТ 28147-89
Фильтрация с учетом любых значимых полей сетевых пакетов	Да	Да	Да	Да	Да	Н/д
Фильтрация на транспортн. уровне запросов	Да (TCP/ UDP)	Да (TCP/ UDP)	Да (TCP/ UDP)	Да (TCP/ UDP)	Да (TCP/ UDP)	Н/д

Сравнительная характеристика российских VPN-продуктов

Трансляция номеров портов/сетев. адресов	-/+	-/+	-/+	-/+	-/+	Н/д
Аутентифика-ция трафика	Да, хэш-е по ГОСТ Р 34.11-94	Да, хеш ф-ция по алг. MD-5	Да, хэш-е по ГОСТ Р 34.11-94	Нет	Да, реж. ими-вки по ГОСТ 28147-89	Да, односто. аутент. с имитовст.
Базовый протокол	SKIP	SKIP	Собствен ный	Собствен ный	Собствен ный	Собствен ный
Расходы на поддержку туннелей	112 байт на пакет	112 байт на пакет	18-20 байт на пакет	30-80 байт на пакет	26-36 байт на пакет	Н/д
Кол-во одновременно туннелей	Н/д	1400	до1024 на кажд. сет. интерф.	Win. 50, Linux -300	не более 500 на кажд КШ	Н/д
Возможность каскадирован. туннелей	Да	Да	Да	Н/д	Н/д	Н/д
Пропускная способность Мбит/с	8 (P-200)	8 (P-200)	11 (P-200)	9,5 (P-III/450)	17,4 (Cel. 500)	1,2-1,8 (Intel 486)
Цена, долл.	Н/д	2500-3000	1000-1500	Н/д	Н/д	350