

# Защита серверов электронной почты

# Защита серверов электронной почты

Этапы развертывания и безопасной настройки серверов электронной почты:

- ❑ **Планирование развертывания почтового сервера**
- ❑ **Выбор местоположения почтового сервера в сети**
- ❑ **Обеспечение сетевой безопасности почтового сервера**
- ❑ **Безопасное конфигурирование ОС сервера**
- ❑ **Безопасная установка и настройка почтового сервера**
- ❑ **Администрирование почтового сервера**

# Защита серверов электронной почты

## Планирование установки и развертывания почтового сервера

Для снижения затрат и достижения максимального уровня защищенности необходимо, чтобы требования по безопасности вырабатывались и предъявлялись, начиная с самых ранних этапов построения системы.

Гораздо сложнее и дороже обходится обеспечение безопасности почтового сервера, если о безопасности начинают думать, когда сервер уже развернут и работает.



# Планирование развертывания почтового сервера

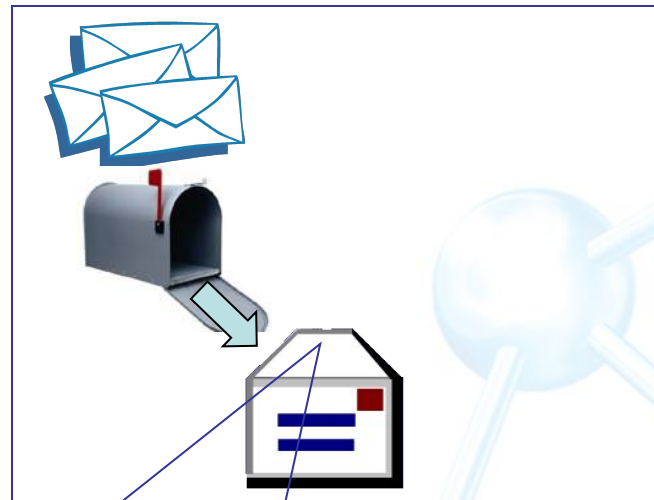
На этапе планирования необходимо:

- **определить цель (цели) использования почтового сервера:**
  - информация каких категорий будет обрабатываться или пересылаться через почтовый сервер;
  - каковы требования к обеспечению безопасности данной информации;
  - какие дополнительные услуги будут предоставляться почтовым сервером (будет ли этот компьютер использоваться только для почтового сервера – наиболее безопасный вариант - или на нем будут развернуты еще какие-то службы);
  - каковы требования к безопасности этих дополнительных служб;
  - где в (какой зоне) сети будет размещаться почтовый сервер.

# Планирование развертывания почтового сервера

На этапе планирования необходимо:

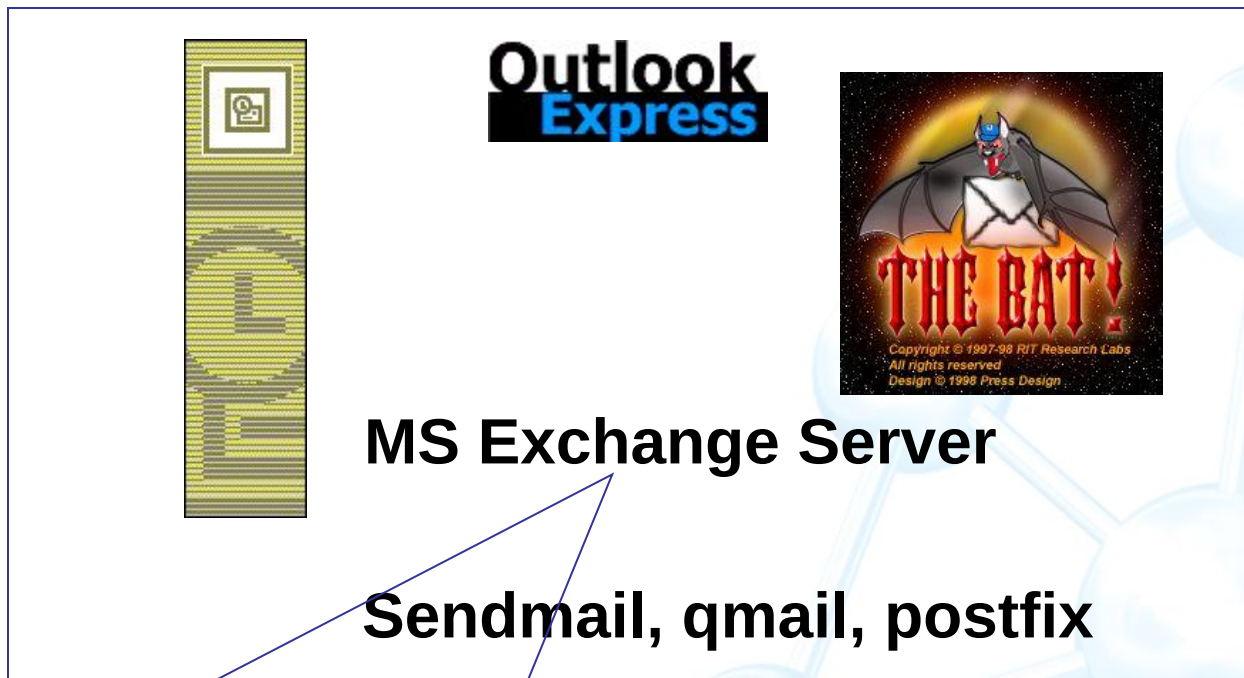
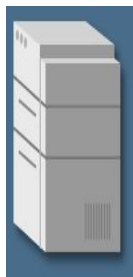
- ❑ **определить сетевые службы, которые будут развернуты на почтовом сервере и используемые ими протоколы, например:**
  - **SMTP**
  - **POP**
  - **IMAP**



# Планирование развертывания почтового сервера

На этапе планирования необходимо:

- определить какое серверное и клиентское программное обеспечение будет использоваться на почтовом сервере и других поддерживаемых серверах;



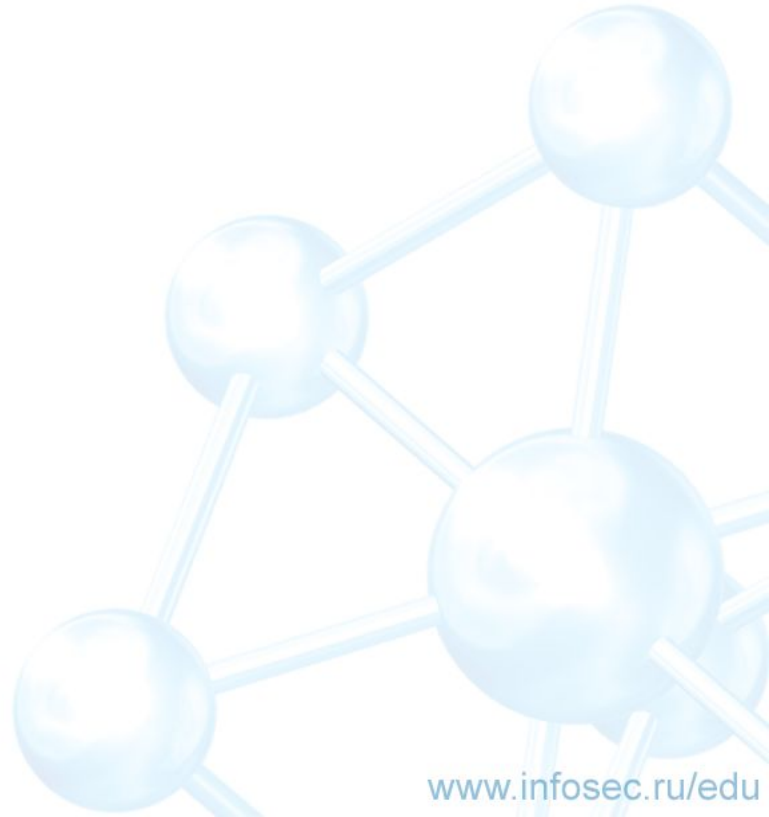
MS Exchange Server

Sendmail, qmail, postfix

# Планирование развертывания почтового сервера

На этапе планирования необходимо:

- **определить пользователей или категории пользователей почтового сервера и других обеспечивающих серверов;**

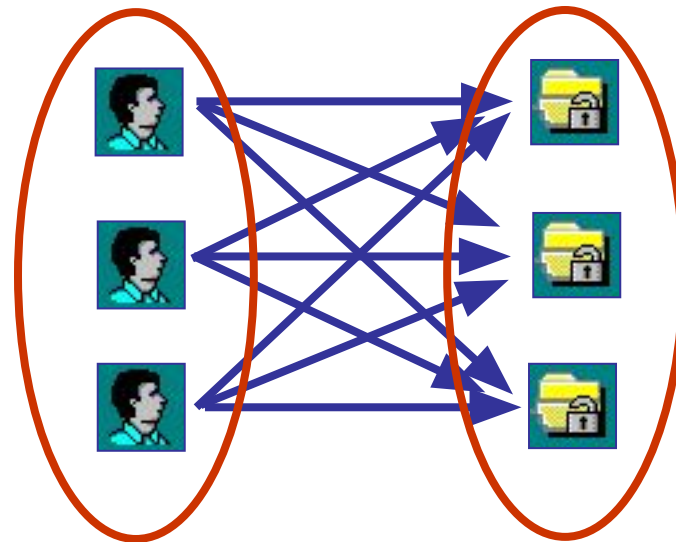




# Планирование развертывания почтового сервера

На этапе планирования необходимо:

- **определить привилегии (права доступа к ресурсам) для каждой категории пользователей на почтовом сервере и на других обеспечивающих серверах;**

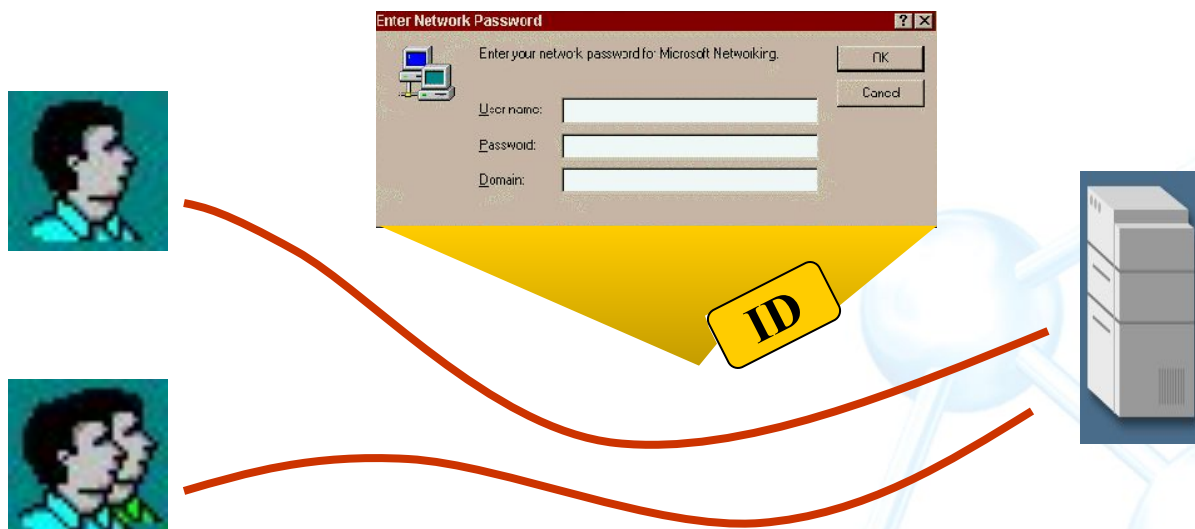




# Планирование развертывания почтового сервера

На этапе планирования необходимо:

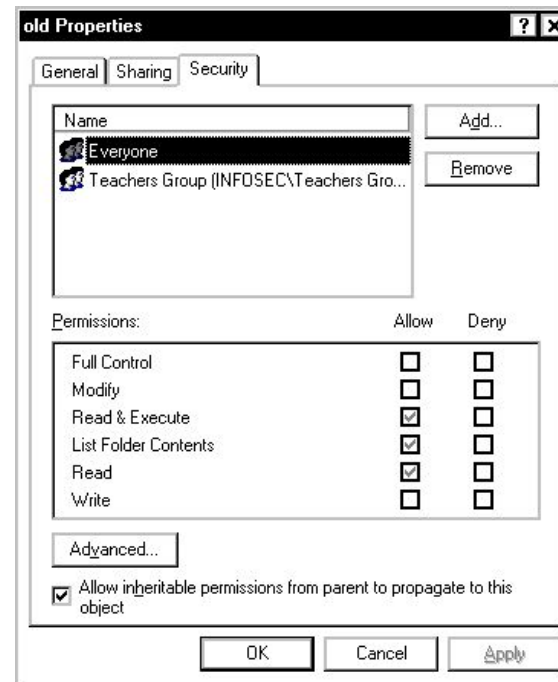
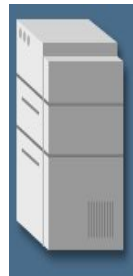
- ❑ решить, будут ли (и если будут, то как) пользователи аутентифицироваться, и как данные аутентификации (имена и пароли) будут защищаться;



# Планирование развертывания почтового сервера

На этапе планирования необходимо:

- **определить какими средствами будут реализовываться заданные правила разграничения доступа к информационным ресурсам.**

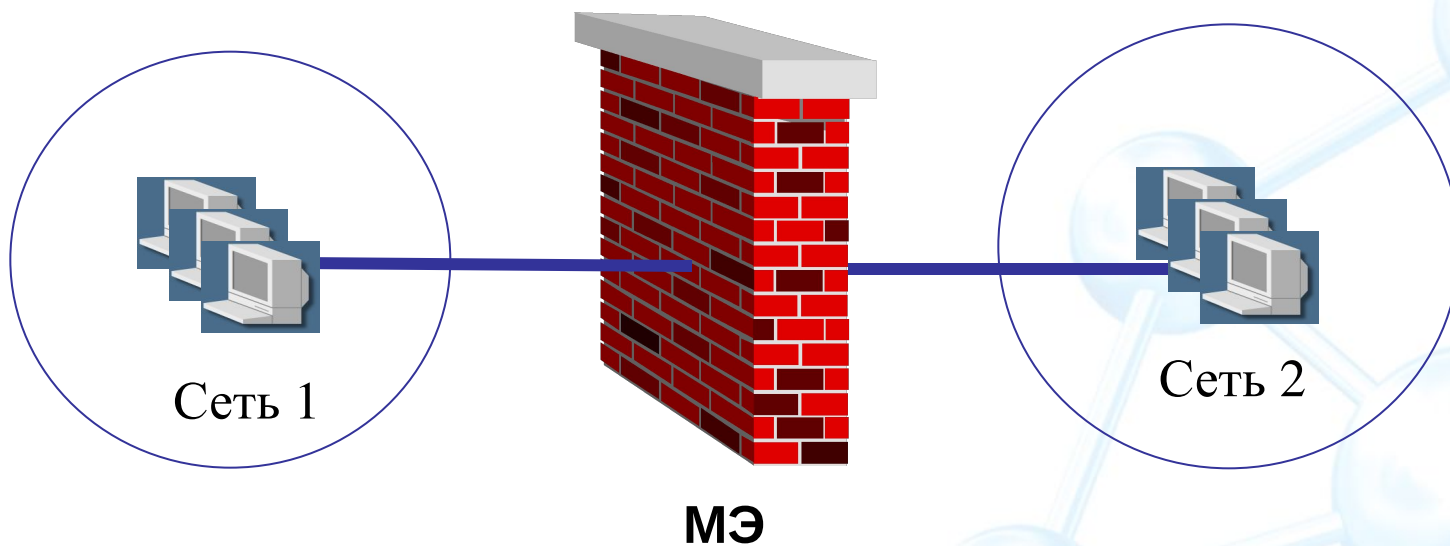


# Выбор местоположения почтового сервера в сети

# Что такое межсетевой экран?

## Межсетевой экран -

это специализированное программное или аппаратное обеспечение, позволяющее разделить сеть на две или более частей с различными требованиями к безопасности и реализовать набор правил, определяющих условия прохождения сетевых пакетов из одной части в другую



# Ограничение доступа к почтовому серверу

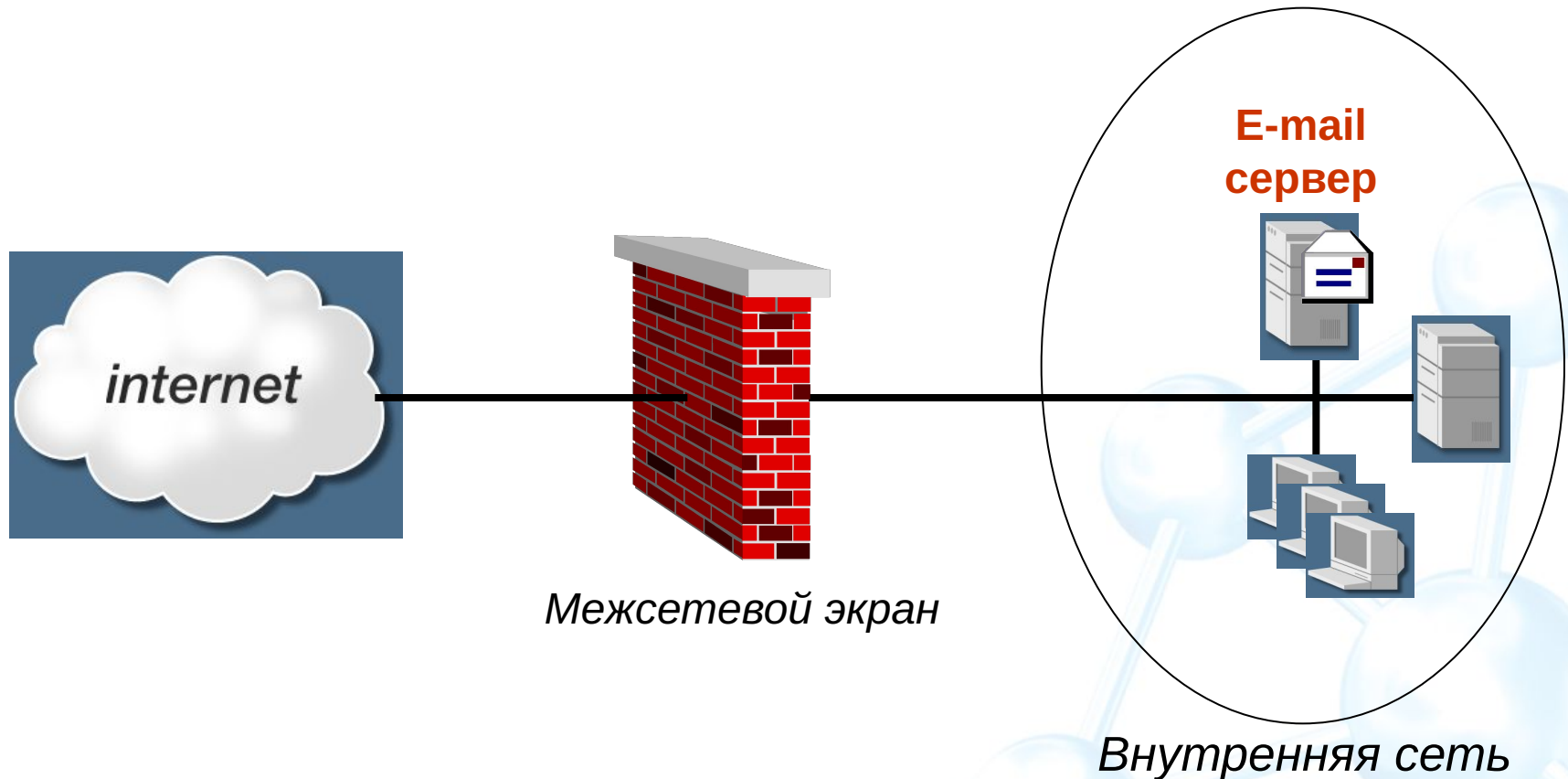
**Межсетевой экран** позволяет ограничить доступ к компьютеру с установленным на нем почтовым сервером только разрешенными почтовыми протоколами



- ✓ Это не позволит внешнему злоумышленнику использовать для атаки на сервер неразрешенные сервисы
- ✓ Если для атаки использовалось ПО самого почтового сервера, то после атаки затруднительно будет использовать машину в качестве плацдарма для атаки на внутреннюю сеть

# Варианты размещения почтовых серверов

## Размещение почтового сервера во внутренней сети



# Варианты размещения почтовых серверов

## Размещение почтового сервера во внутренней сети

### Преимущества с точки зрения безопасности:

- почтовый сервер может быть защищен межсетевым экраном;
- проще администрировать почтовый сервер.

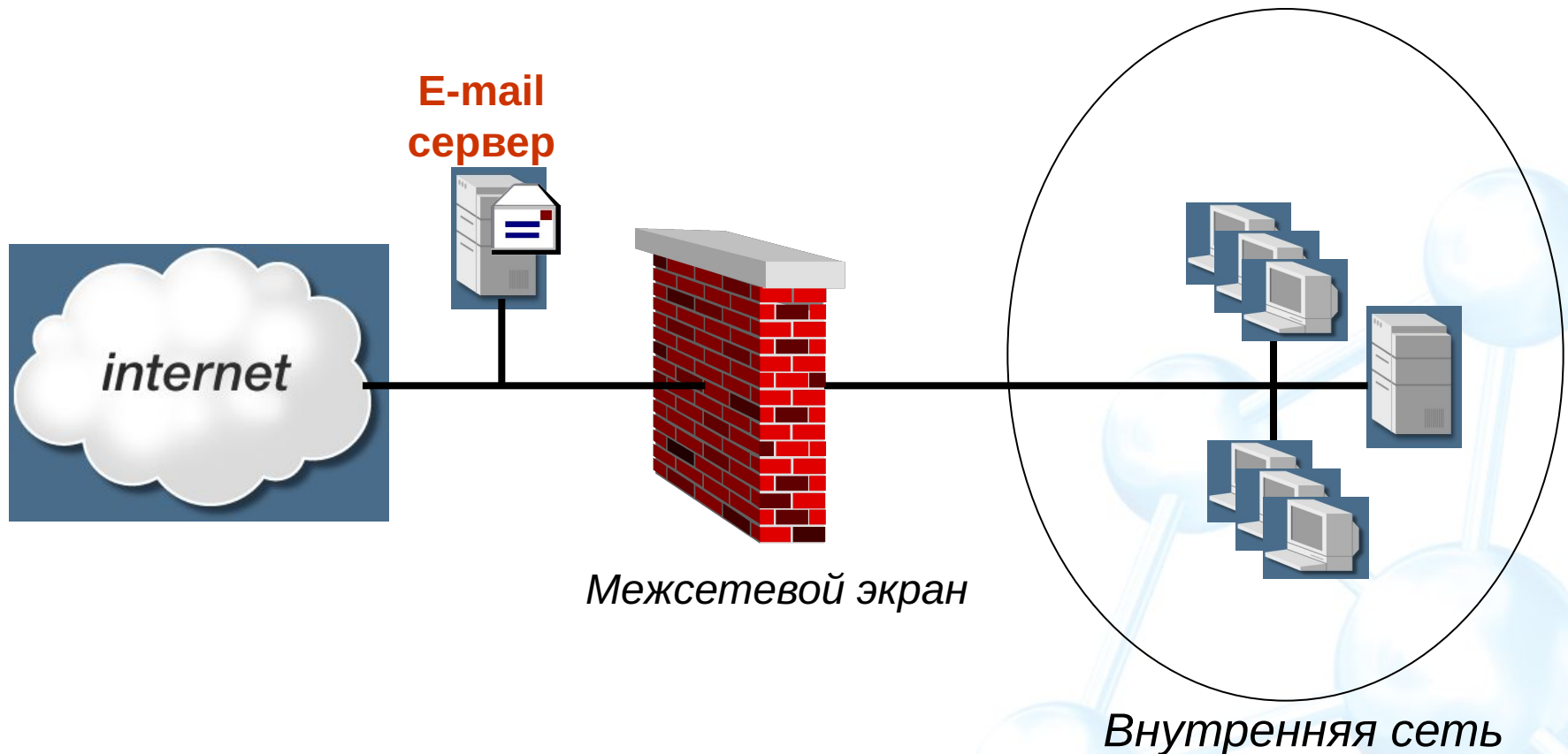
### Недостатки:

- компрометация почтового сервера непосредственно угрожает безопасности всей внутренней сети.



# Варианты размещения почтовых серверов

## Размещение почтового сервера во внешней сети



# Варианты размещения почтовых серверов

## Размещение почтового сервера во внешней сети

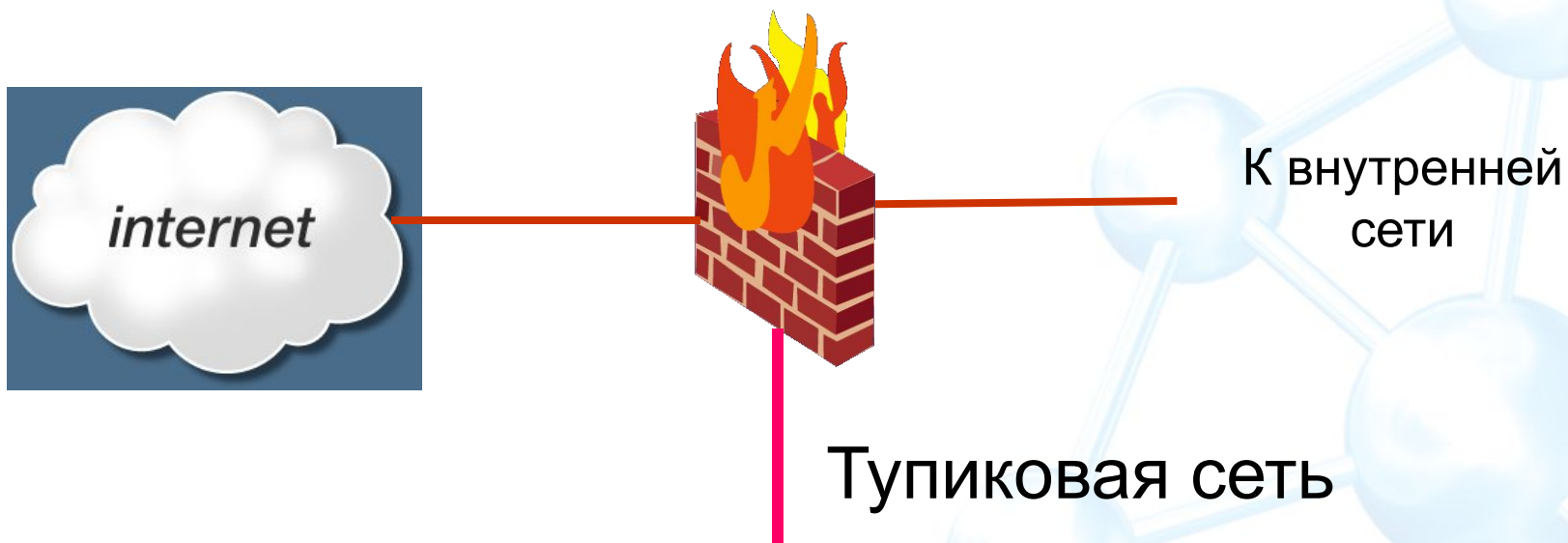
### Преимущества с точки зрения безопасности:

- ❑ компрометация почтового сервера безопасности всей внутренней сети непосредственно не угрожает;
- ❑ DoS атаки на почтовый сервер не влияют (кроме как на почту) на работу узлов внутренней сети.

### Недостатки:

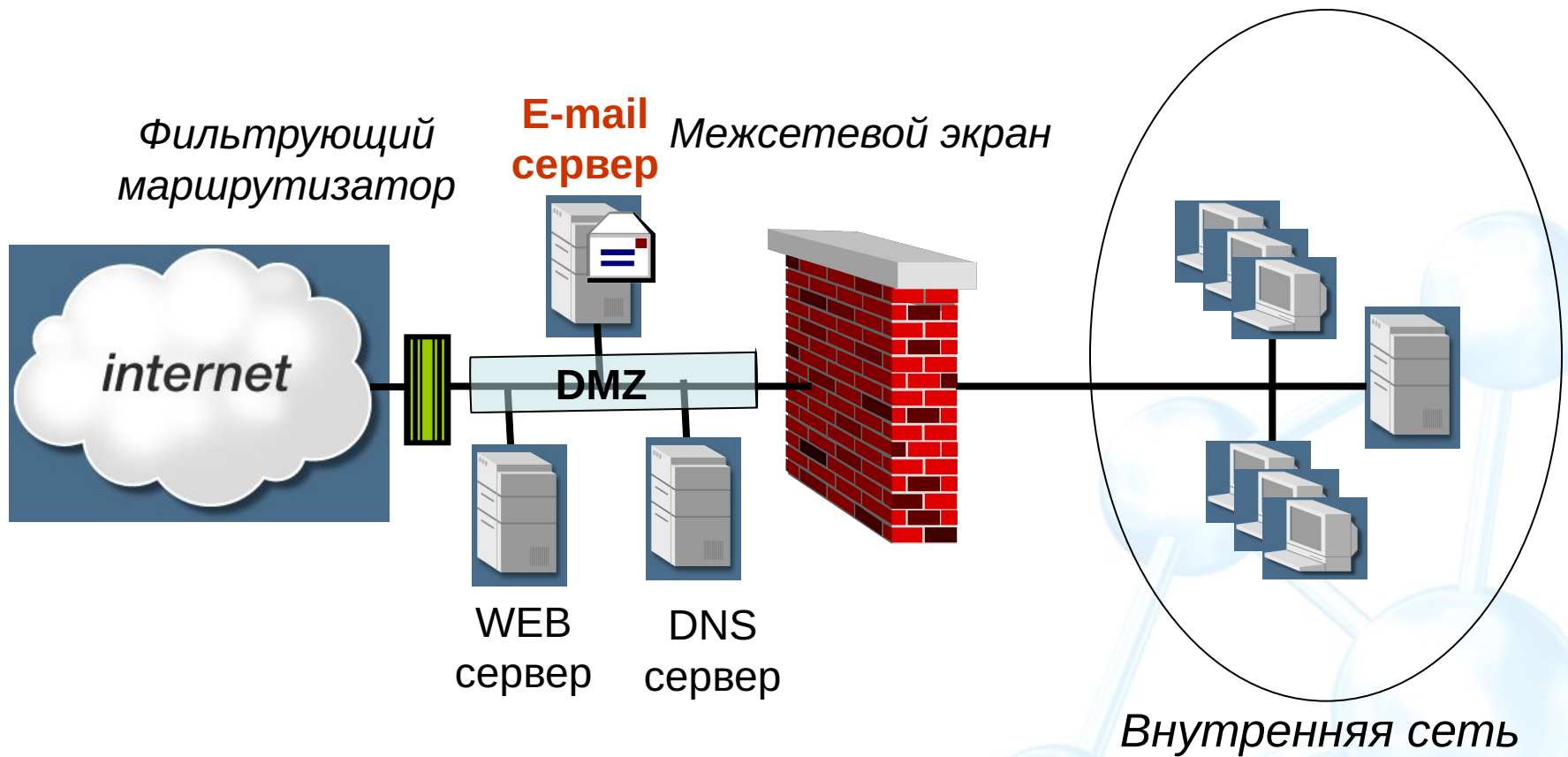
- ❑ почтовый сервер не может быть защищен межсетевым экраном;
- ❑ почтовый сервер и операционная система его компьютера должны быть очень хорошо настроены для обеспечения безопасности;
- ❑ сложно обеспечить безопасность удаленного администрирования почтового сервера;
- ❑ сложно осуществлять мониторинг входящего и исходящего трафика почтового сервера.

# Демилитаризованная зона (ДМЗ)



# Варианты размещения почтовых серверов

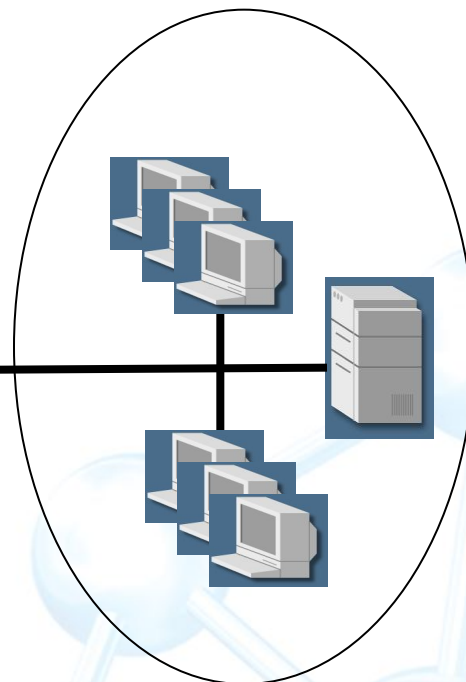
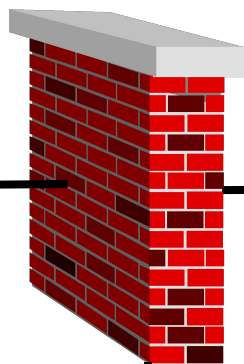
## Размещение почтового сервера в ДМЗ (вариант 1)



# Варианты размещения почтовых серверов

## Размещение почтового сервера в ДМЗ (вариант 2)

*Межсетевой экран*



*Внутренняя сеть*

**DMZ**



**WEB**  
сервер



**E-mail**  
сервер



**DNS**  
сервер

# Варианты размещения почтовых серверов

## Размещение почтового сервера в ДМЗ

### Преимущества с точки зрения безопасности:

- ❑ возможна защита почтового сервера и мониторинг всего трафика к нему и от него;
- ❑ компрометация почтового сервера не угрожает непосредственно ресурсам внутренней сети;
- ❑ больше возможностей по управлению безопасностью почтового сервера;
- ❑ проще администрировать почтовый сервер;
- ❑ конфигурацию DMZ можно оптимизировать с позиций производительности сети и защищенности почтового сервера.



# Варианты размещения почтовых серверов

## Размещение почтового сервера в ДМЗ

### Недостатки с точки зрения безопасности :

- ❑ DoS атаки, нацеленные на почтовый сервер, могут сказываться и на трафике внутренней сети;
- ❑ в зависимости от разрешенных видов трафика между DMZ и внутренней сетью, возможно использование почтового сервера для атаки и компрометации узлов внутренней сети.

Во втором варианте конфигурации ДМЗ МЭ подвергается повышенному риску снижения пропускной способности при осуществлении DoS атак на почтовый сервер.



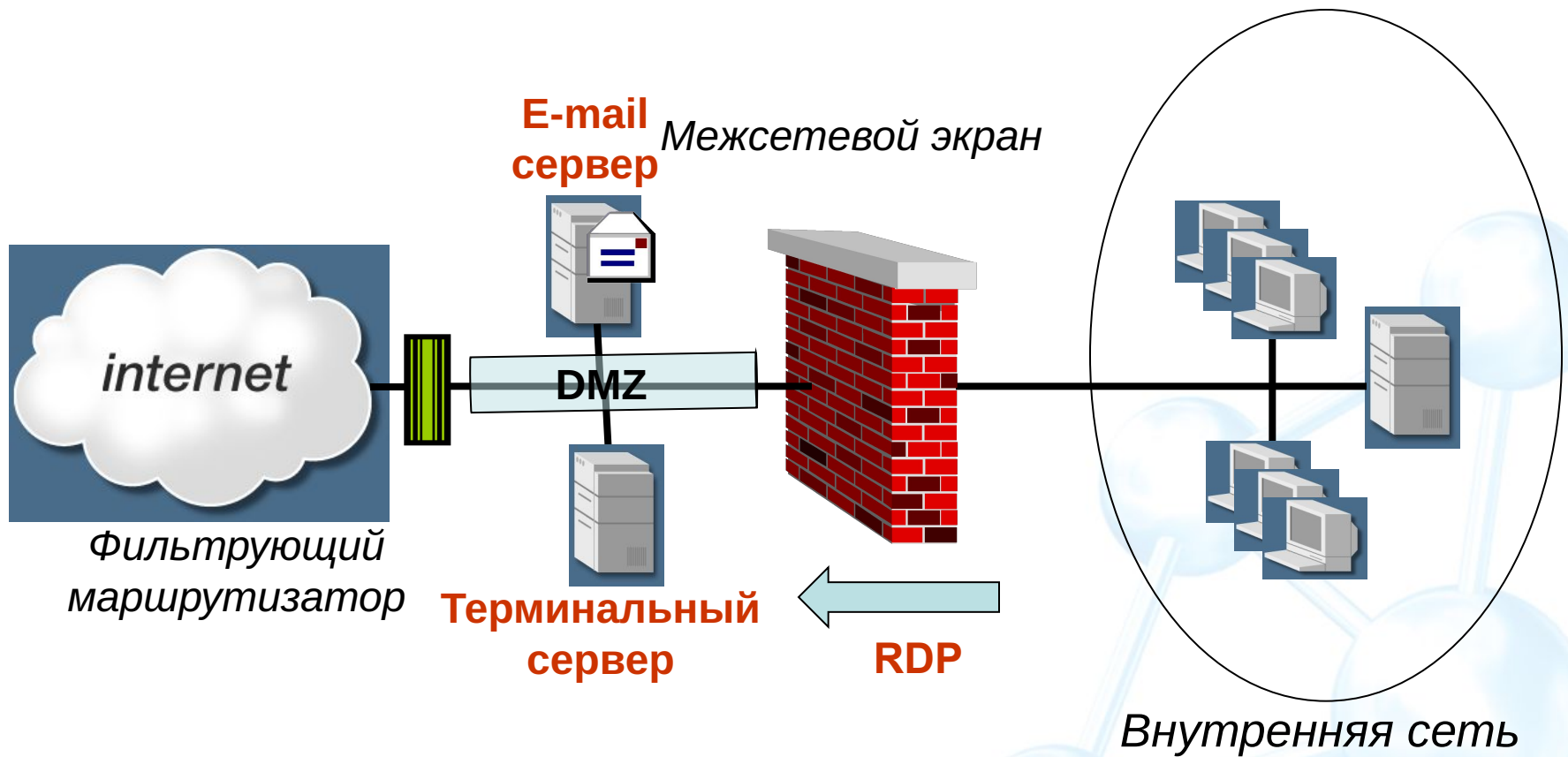
# Варианты размещения почтовых серверов

Размещение почтового сервера  
во внутренней сети  
с использованием дополнительного  
почтового шлюза в ДМЗ



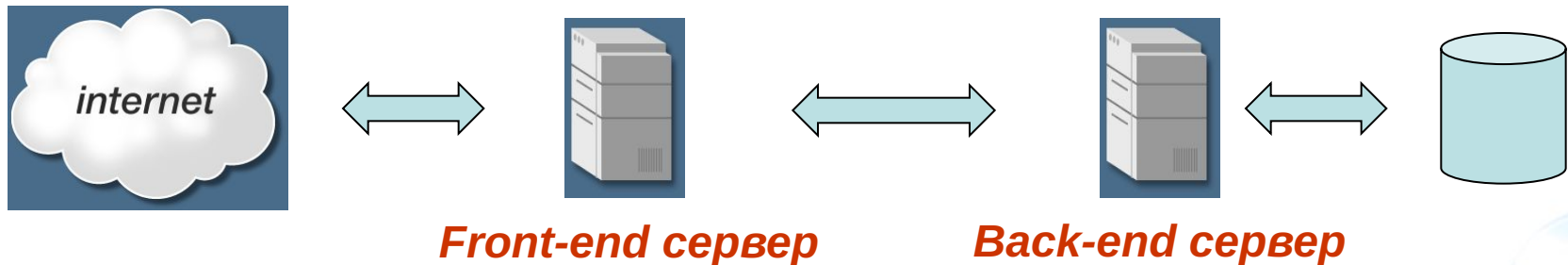
# Варианты размещения почтовых серверов

Размещение почтового сервера и терминального сервера в ДМЗ



# Варианты размещения почтовых серверов

## Использование конфигурации с двумя почтовыми серверами



Такой вариант конфигурации позволяет разделить роли между почтовыми серверами:

- ✓ **Front-end сервер** будет отвечать за обмен информацией со внешним миром
- ✓ **Back-end сервер** будет заниматься хранением баз данных и обработкой запросов внутренних пользователей

# Обеспечение сетевой безопасности почтового сервера



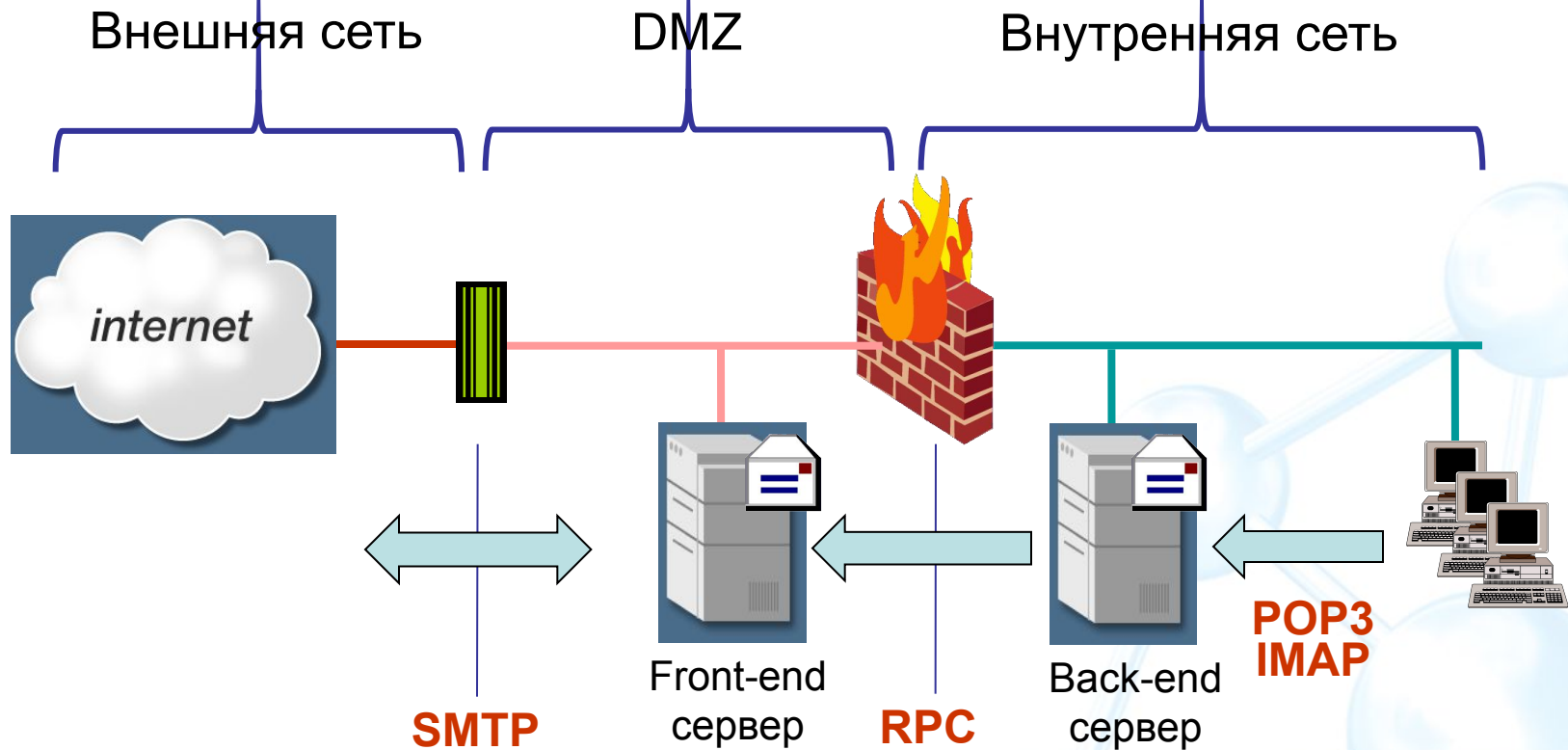
# Обеспечение сетевой безопасности

Элементы сетевой инфраструктуры, влияющие на безопасность почтового сервера:

- ❑ межсетевые экраны (firewalls)
- ❑ маршрутизаторы (routers)
- ❑ сетевые коммутаторы (switches)
- ❑ системы обнаружения атак (IDS)

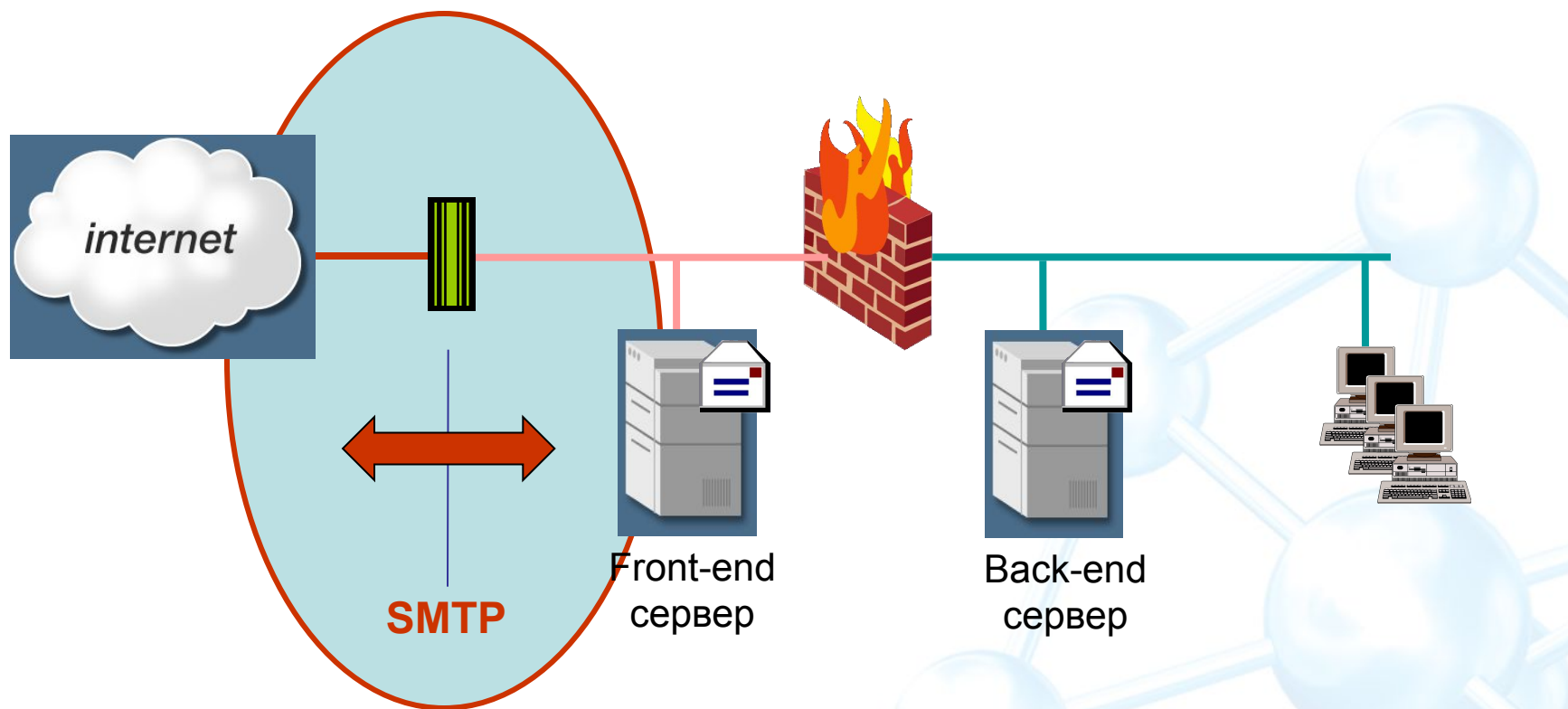
# Конфигурирование межсетевых экранов

Для варианта конфигурации с двумя почтовыми серверами



# Настройка фильтрующего маршрутизатора

Отправка почты при помощи SMTP  
получение почты при помощи SMTP





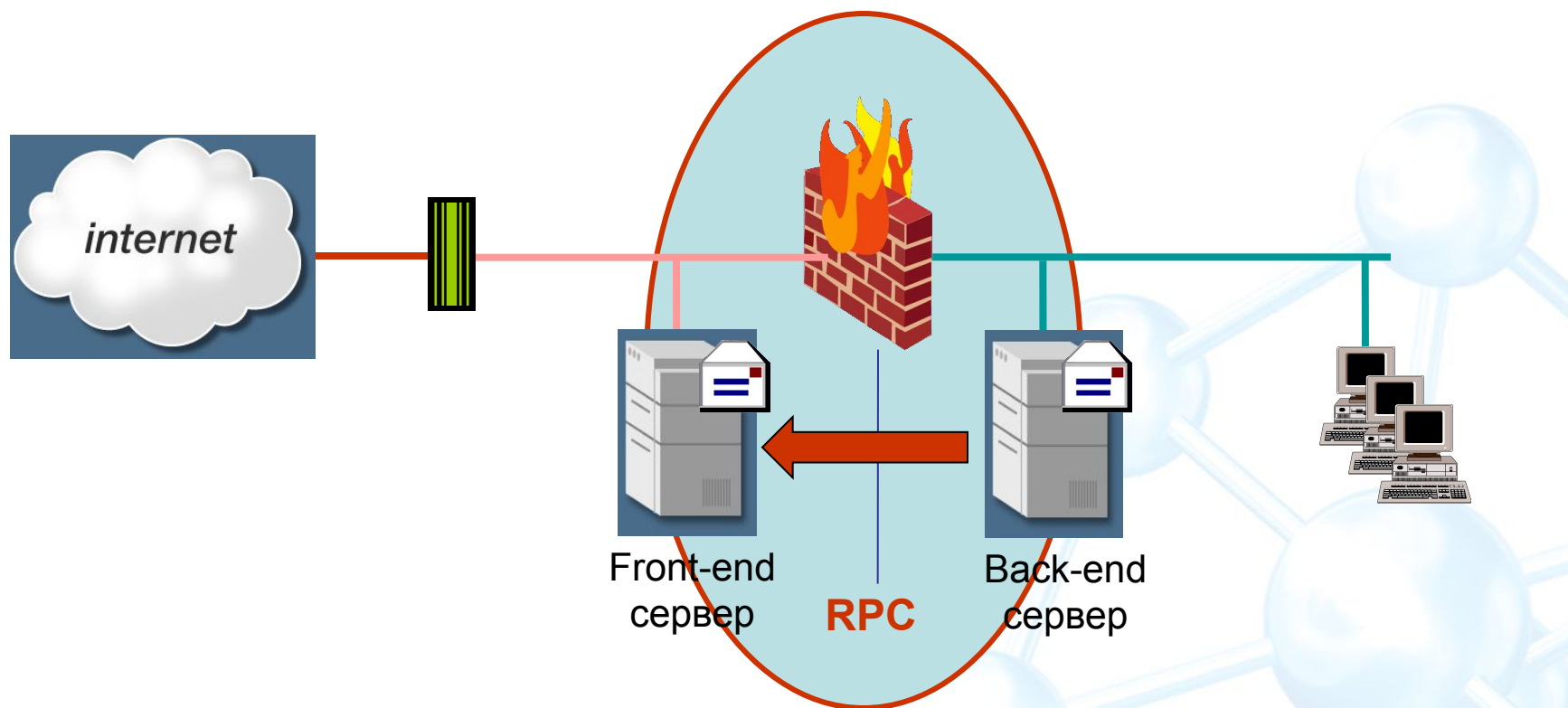
# Настройка фильтрующего маршрутизатора

## Правила фильтрации

№	Действие	Узел-источник	Порт	Узел-получатель	Порт	Флаги TCP Опции IP	Комментарий
1	Разрешить	*	1024-65535	Front-end сервер	25	TCP	
2	Разрешить	Front-end сервер	25	*	1024-65535	TCP ACK=1	
3	Разрешить	Front-end сервер	1024-65535	*	25	TCP	
4	Разрешить	*	25	Front-end сервер	1024-65535	TCP ACK=1	

# Настройка межсетевого экрана

## Отправка почты при помощи RPC



# Настройка межсетевого экрана

## Правила фильтрации

№	Действие	Узел-источник	Порт	Узел-получатель	Порт	Флаги TCP Опции IP	Комментарий
1	Разрешить	Back-end сервер	1024-65535	Front-end сервер	RPC	TCP	
2	Разрешить	Front-end сервер	RPC	Back-end сервер	1024-65535	TCP ACK=1	
3	Разрешить	Front-end сервер	1024-65535	Back-end сервер	RPC	TCP	
4	Разрешить	Back-end сервер	RPC	Front-end сервер	1024-65535	TCP ACK=1	

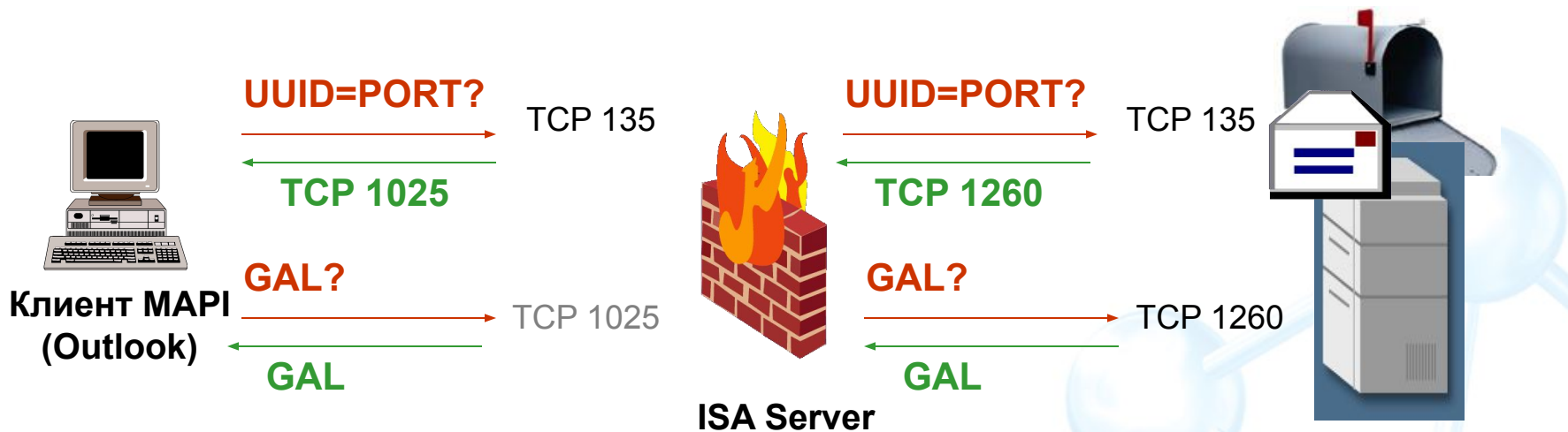
# Настройка межсетевого экрана

## Клиентский доступ

<b>Порт</b>	<b>Служба</b>
25	SMTP
80	HTTP
110	POP3
143	IMAP4
443	HTTPS
636	LDAP over SSL

# Настройка межсетевого экрана

## ISA RPC Application Filter



UUID	PortInt	PortExt
XXXX	1260	1025

# Настройка межсетевого экрана

## ISA RPC Application Filter

### Не «слушает» на портах RPC

```
+ [public IP address of ISA server]
|___ 21  File Transfer Protocol [Control]
|___ 25  Simple Mail Transfer
|___ 53  Domain Name Server
|___ 135 DCE endpoint resolution
|___ 3389
```

### Не публикует сервисы RPC

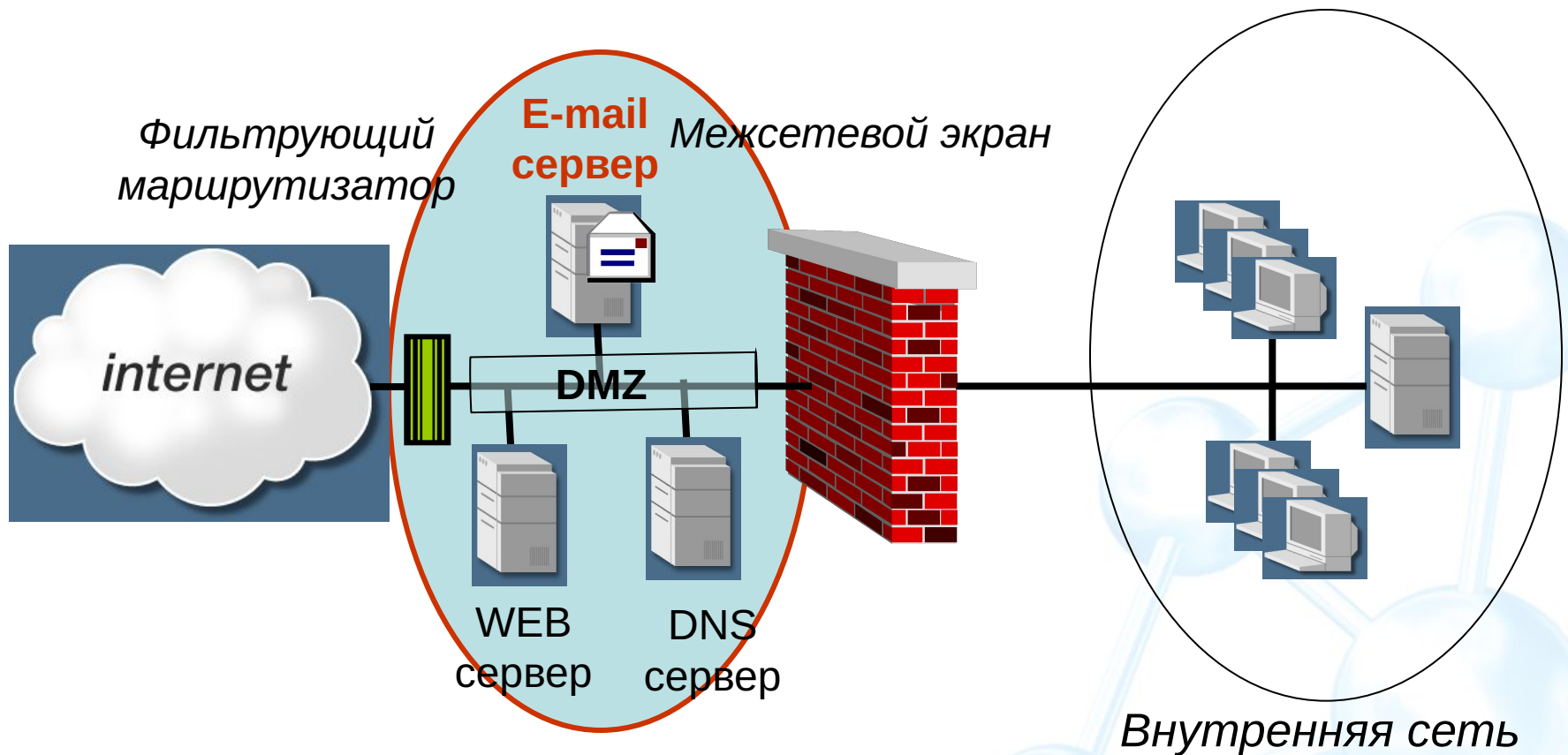
```
Querying Endpoint Mapper Database...
RpcMgmtEpEltnqNext:(The remote procedure call failed. ).
rpcdump failed after 1 seconds
```

### Не подвержен атакам на EndPoint Mapper

### Аутентификация средствами ОС

# Применение коммутатора (switch)

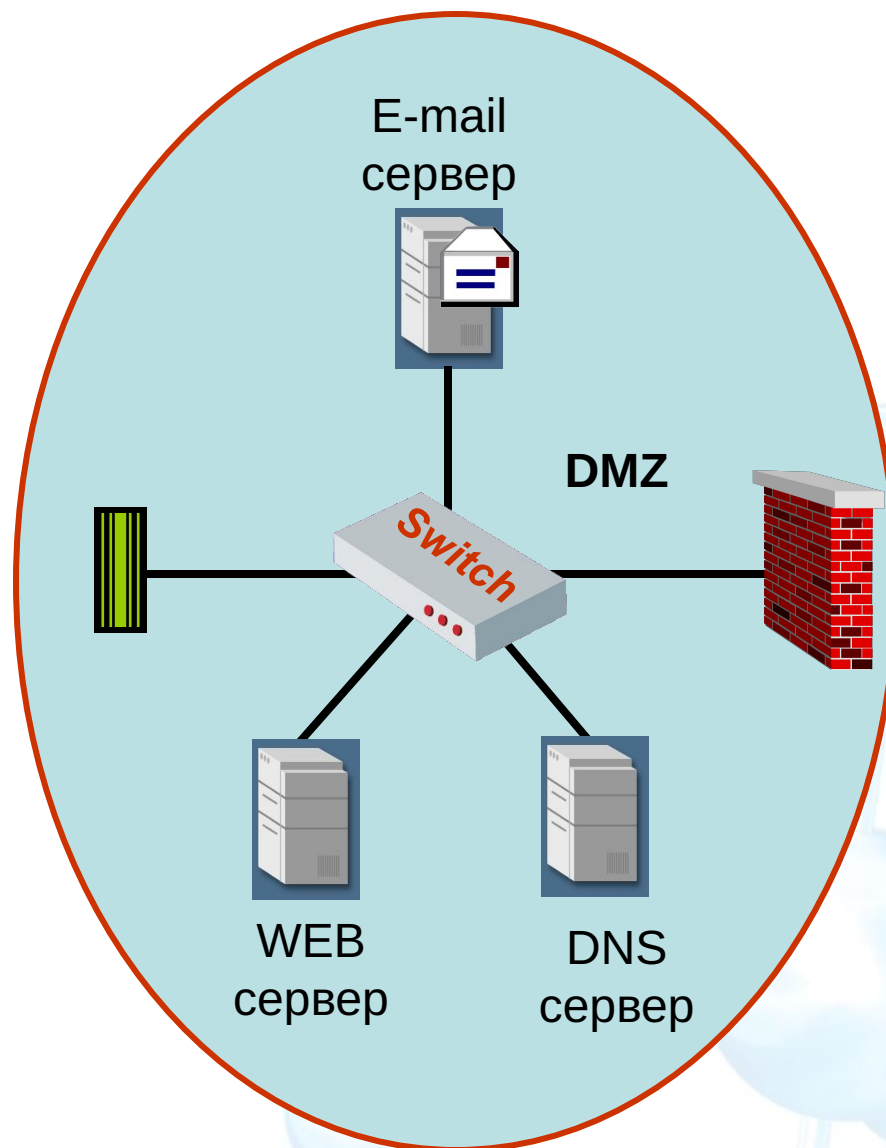
при организации демилитаризованной зоны





# Применение коммутатора (switch)

**Преимущество использования коммутаторов (switch) вместо концентраторов (hub) в сети с точки зрения безопасности состоит в том, что нарушителю становится намного сложнее перехватить (подслушать) трафик между другими компьютерами в том же сегменте сети**

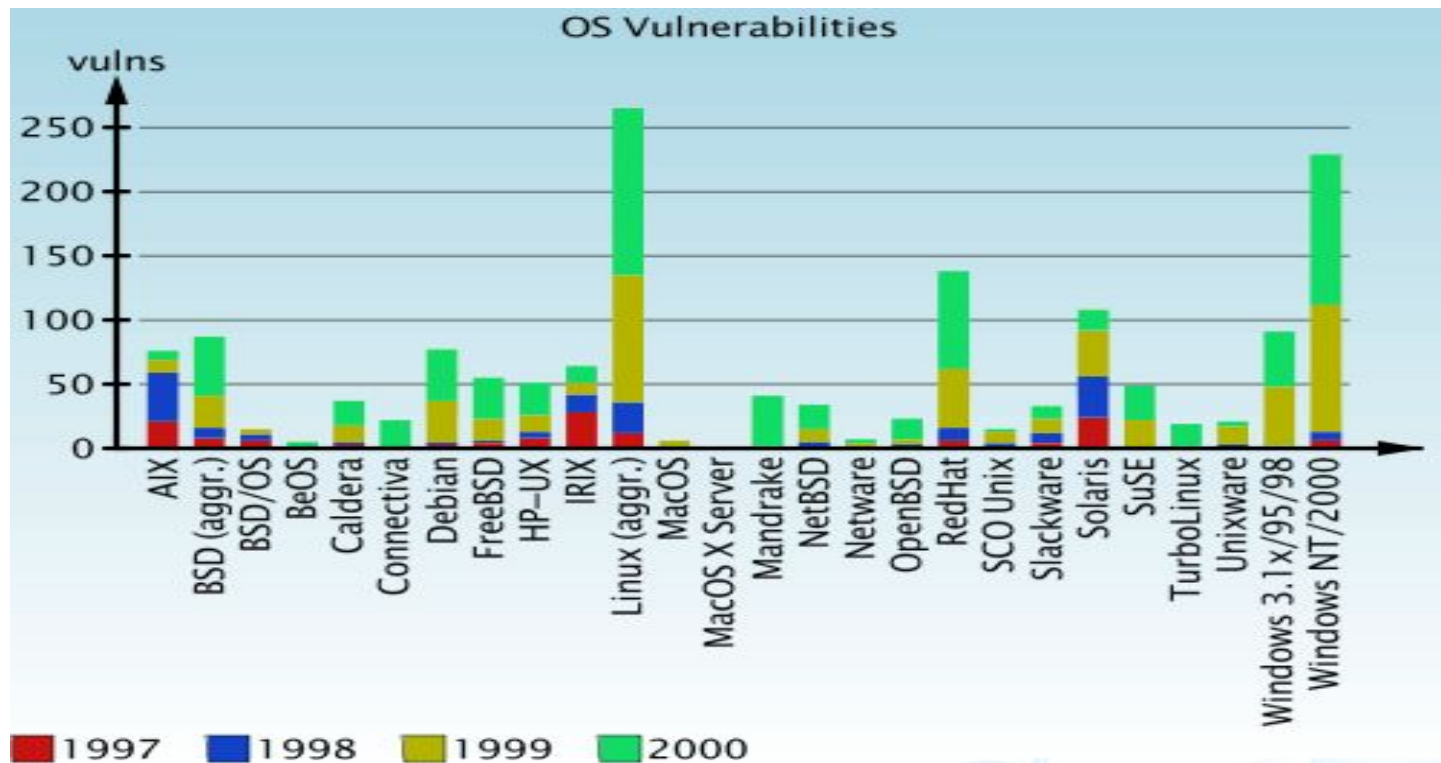


# Безопасное конфигурирование ОС почтового сервера

# Выбор ОС для почтового сервера

ОС должна удовлетворять следующим требованиям:

- минимальная уязвимость и подверженность воздействиям (все операционные системы уязвимы!);



# Выбор ОС для почтового сервера

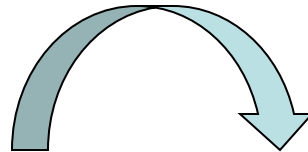
ОС должна удовлетворять следующим требованиям:

- ❑ возможность назначения административных прав и максимальных полномочий только авторизованным пользователям;
- ❑ возможность запрета доступа к информационным ресурсам сервера, которые не нужны почтовому серверу для работы;
- ❑ возможность запрета ненужных встроенных в ОС сетевых сервисов (служб);
- ❑ возможность регистрации в журналах сервера событий, полезных для обнаружения попыток вторжения.

# Безопасное конфигурирование ОС

Для обеспечения базового уровня безопасности ОС необходимо выполнять следующие четыре шага:

1. **планирование инсталляции и развертывания операционной системы и других необходимых базовых компонент на компьютере для почтового сервера;**



# Безопасное конфигурирование ОС

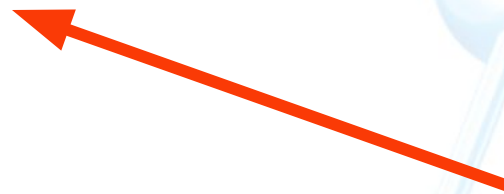
Для обеспечения базового уровня безопасности ОС необходимо выполнять следующие четыре шага:

2. **конфигурирование операционной системы компьютера в соответствии с существующими требованиями безопасности;**
3. **установка необходимых пакетов обновлений и «заплаток» ПО для ОС;**

# Безопасное конфигурирование ОС

Для обеспечения базового уровня безопасности ОС необходимо выполнять следующие четыре шага:

4. **тестирование операционной системы компьютера для проверки реализации предыдущими действиями адекватного требованиям уровня безопасности.**



Сканер  
безопасности

# Безопасное конфигурирование ОС

Удаление или отключение ненужных служб повышает безопасность почтового сервера следующим образом:

- ❑ Другие службы могут быть скомпрометированы и использованы для атак на хост или для ухудшения работы почтовых служб.
- ❑ Безопасность компьютера при наличии на нем отдельной службы можно обеспечить (настроить) гораздо лучше.
- ❑ Уменьшение числа служб приводит к уменьшению числа записей в журналах регистрации событий



# Безопасное конфигурирование ОС

Список некоторых сервисов и приложений, которые требуется запретить (не устанавливать):

- доступ по сети к файлам и принтерам в Windows NetBIOS;
- сетевые файловые системы в UNIX (NFS);
- Telnet;
- SNMP;
- FTP;
- трансляторы (компиляторы) и библиотеки;
- средства разработки и отладки программ;
- сетевые средства управления и утилиты.

# Безопасное конфигурирование ОС

## Настройка аутентификации пользователей в ОС:

- ❑ Удалить или запретить учетные записи (пользователей) и группы, установленные по умолчанию.
- ❑ Запретить неинтерактивные учетные записи.
- ❑ Создать группы пользователей.
- ❑ Создать учетные записи пользователей.
- ❑ Проверить исполнение требований политики организации относительно паролей (длина, сложность, время действия, повторяемость, аутентификация)
- ❑ Включить блокировку учетных записей после нескольких неудачных попыток входа.

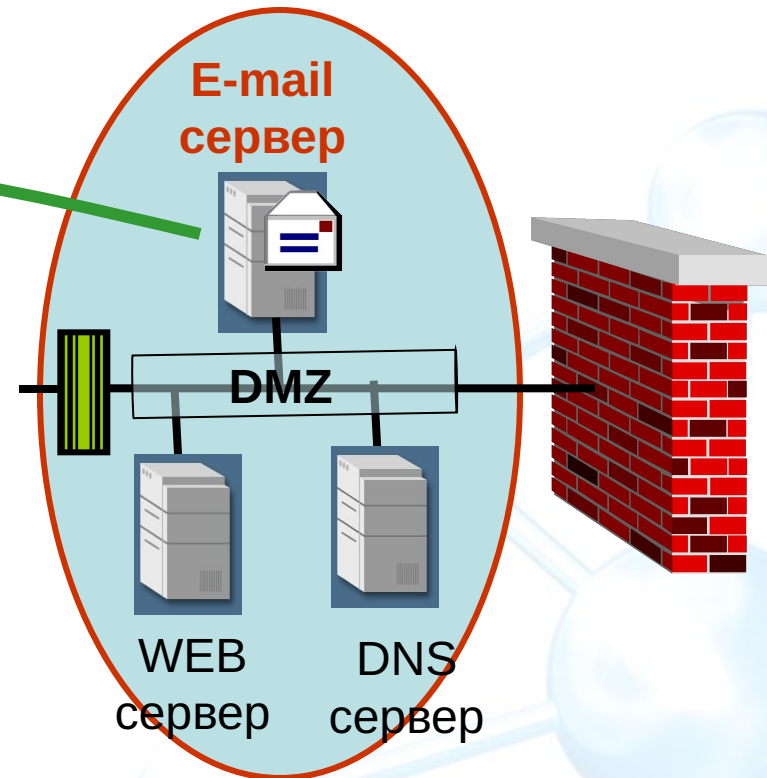
# Безопасная установка и настройка почтового сервера



# Безопасная установка почтового сервера

Целесообразно выполнять следующие рекомендации:

- устанавливать программное обеспечение сервера на отдельный (выделенный) компьютер (хост);

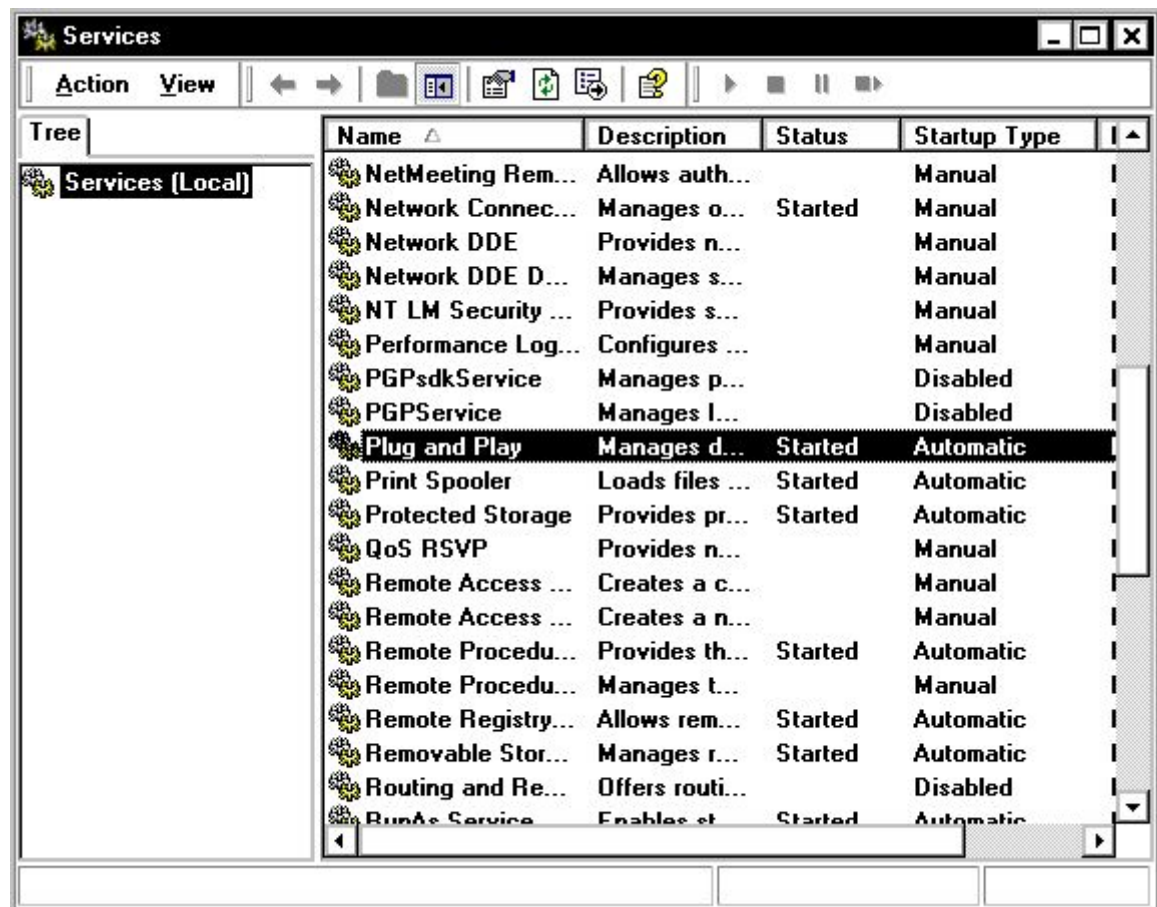


# Безопасная установка почтового сервера

Целесообразно выполнять следующие рекомендации:

- устанавливать минимум служб (только необходимые службы);

E-mail  
сервер



# Безопасная установка почтового сервера

Целесообразно выполнять следующие рекомендации:

- **применять (устанавливать) патчи и обновления для устранения всех известных уязвимостей;**



**E-mail сервер**

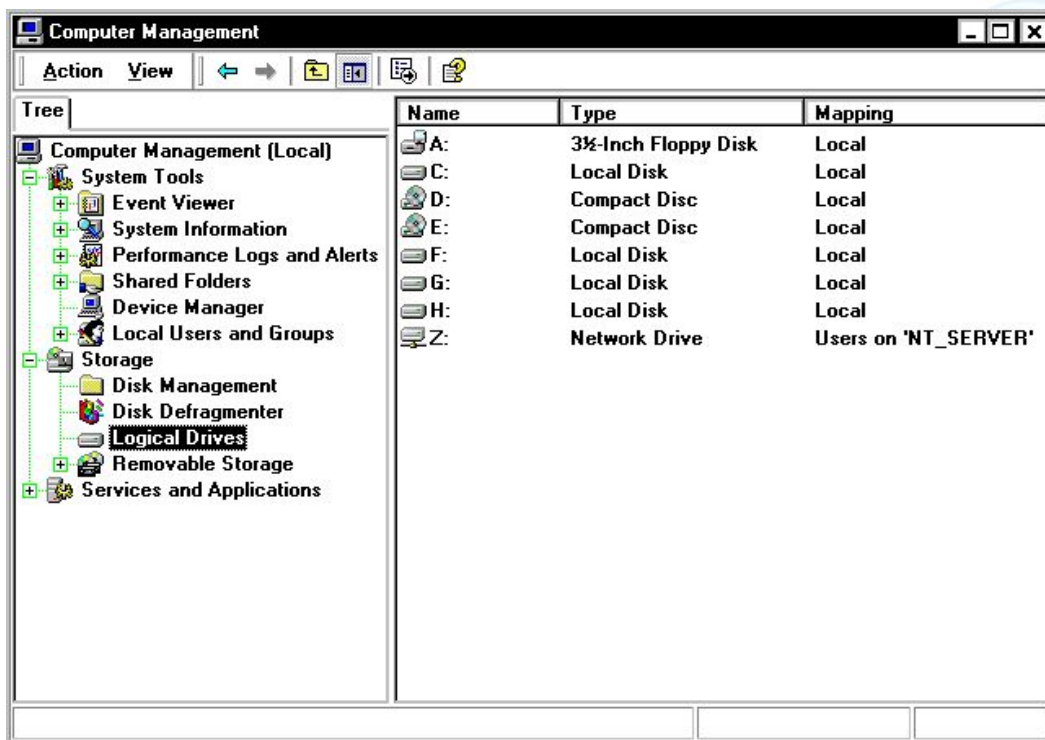




# Безопасная установка почтового сервера

Целесообразно выполнять следующие рекомендации:

- использовать отдельный физический диск или отдельный логический раздел (раздельный с операционной системой и программным обеспечением почтового сервера) для почтовых ящиков пользователей;





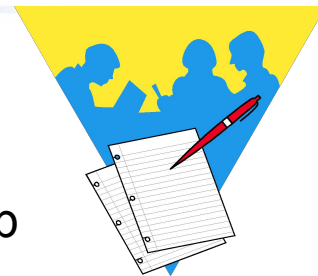
# Безопасная установка почтового сервера

Целесообразно выполнять следующие рекомендации:

- ❑ удалять или запрещать работу всех ненужных, но установленных при инсталляции служб почтового сервера (например, Web-доступ к почте, FTP, удаленное администрирование и т.п.);
- ❑ удалять с сервера всю документацию разработчика;
- ❑ применять подходящие настройки средств безопасности почтового сервера;
- ❑ изменять баннеры (выдаваемые при обращении заголовки) служб SMTP, POP, IMAP и других, чтобы по ним нельзя было установить тип и версию используемой операционной системы и почтового сервера.

# Установка сервера Exchange 2000

## Практическая работа 7



Работа выполняется в паре. Один из узлов пары – контроллер домена с установленной Active Directory (DC-AD), Второй узел – сервер Exchange (ExchSrv).

**TREExx.EDU**



**DC-AD**

Active Directory  
Microsoft Outlook



**ExchSrv**

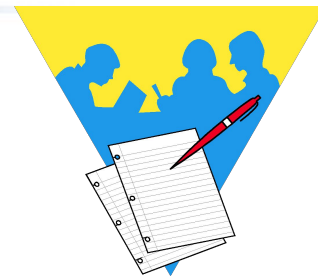
сервер  
Exchange  
Microsoft Outlook

**EXxx**

1. Загрузить ОС Windows 2000 Server (с Active Directory) на одном из узлов пары (DC-AD)
2. Загрузить ОС Windows 2000 Server (без Active Directory) на другом узле пары (на нём будет установлен сервер Exchange)

# Установка сервера Exchange 2000

## Действия на DC-AD:



3. Создать глобальную группу, в которую будут включены администраторы сервера Exchange:

Имя: **Exchange Admins**

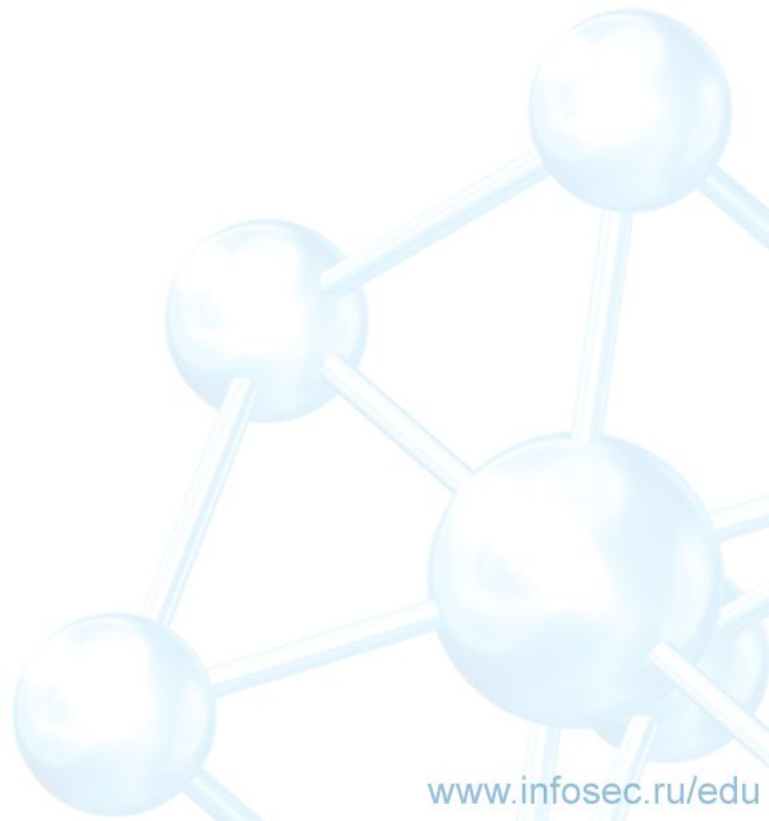
4. Создать учётную запись, которая будет использоваться для администрирования сервера Exchange

Имя: **Eadmin**

Пароль: **1111**

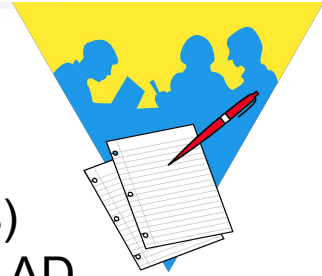
5. Включить учётную запись в группы:

Enterprise Admins,  
Domain Admins,  
Schema Admins,  
Exchange Admins



# Установка сервера Exchange 2000

## Действия на сервере Exchange (ExchSrv):



6. Войти локальным администратором и включить (проверить) узел **ExchSrv** в Active Directory на контроллере домена DC-AD
  - Войти с использованием учётной записи **Eadmin**
  - Запустить процедуру установки с ключом **/ForestPrep**
  - Запустить процедуру установки с ключом **/DomainPrep**
  - Выполнить процедуру установки **Exchange 2000** обычным образом
  - Установить **Service Pack 3** for Exchange 2000
  - Создать пользователей **user##** и **user##** с почтовыми адресами и ящиками (номера **##** должны соответствовать номерам компьютеров пары в классе)

# Вопросы ?