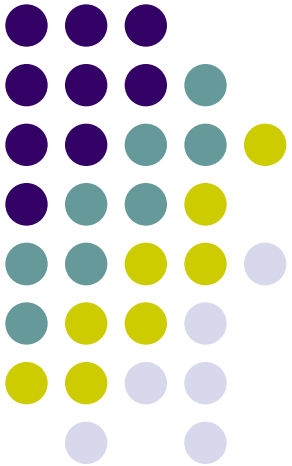
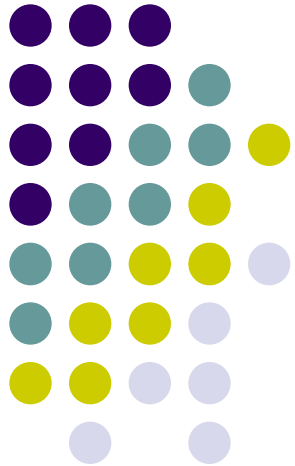
Защита информации в компьютерных сетях

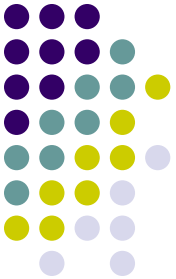
Презентации к курсу лекций



Компьютерные атаки

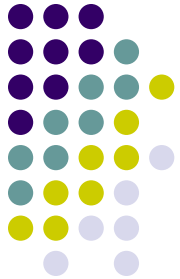


Компьютерная атака



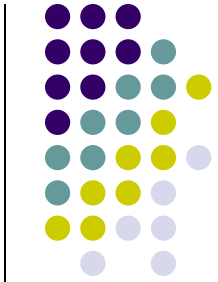
- это целенаправленное воздействие на АИС, осуществляемое программными средствами с целью нарушения конфиденциальности, целостности или доступности информации
- Осуществление компьютерных атак становится возможным благодаря наличию в компьютерной системе *уязвимостей*

Примеры уязвимости КС



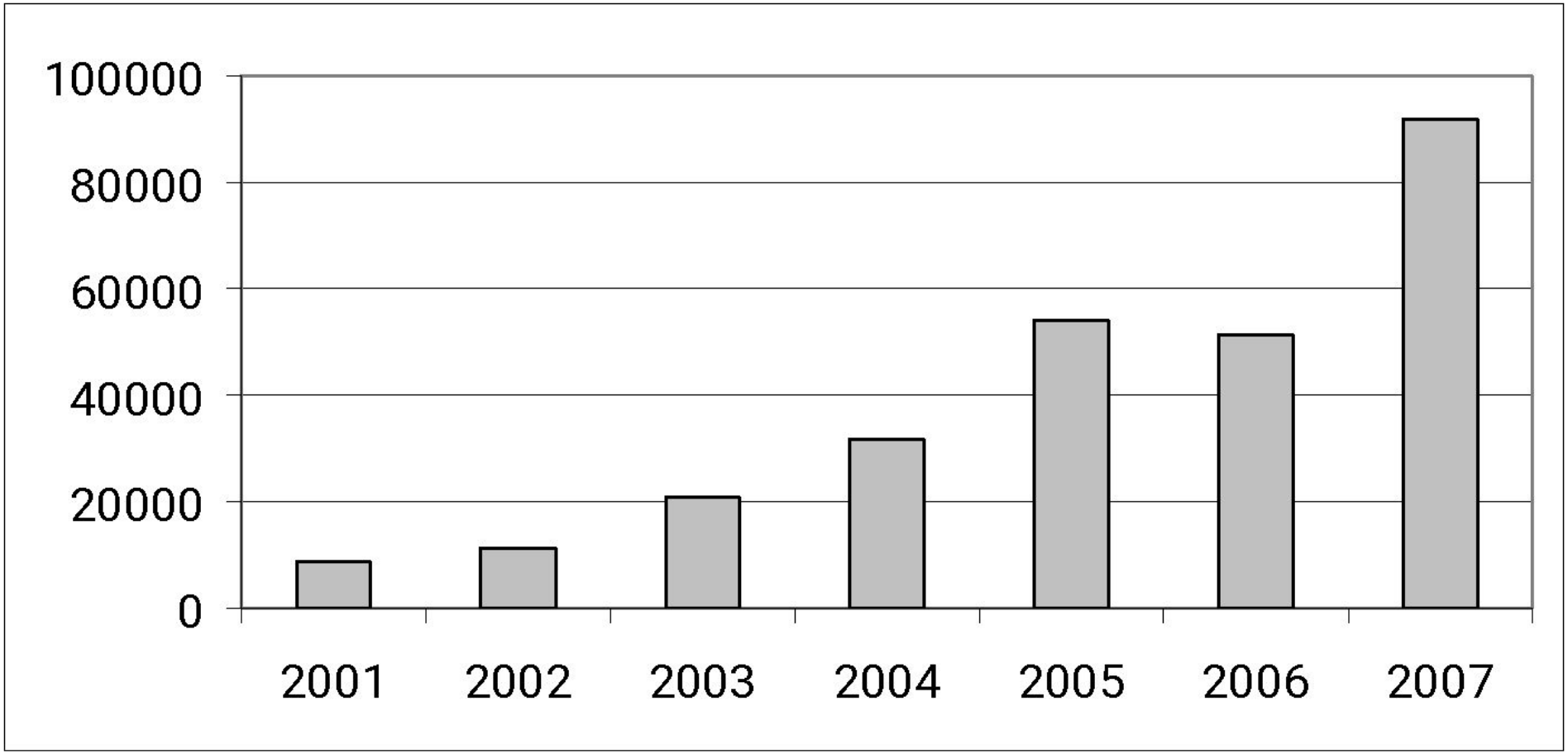
- ошибки, допущенные в ходе разработки ПО или протоколов обмена
  - например, отсутствие механизмов защиты информации от несанкционированного доступа
- ошибки в программном коде, позволяющие тем или иным образом обойти систему защиты
  - (например, ошибки программирования, создающие возможность выполнить атаку на переполнение буфера)
- ошибки конфигурирования и администрирования
  - (неправильная настройка системы защиты, слишком короткий пароль и т. д.).

Классификация компьютерных атак

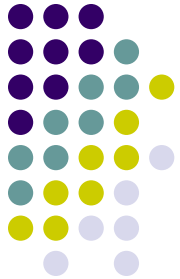


- По типу используемой уязвимости, то есть с позиции атакуемого
- По конечной цели злоумышленника, то есть с позиции атакующего
  - вывод компьютерной системы из строя или ее блокирование (отказ в обслуживании, Denial-of-Service, DoS),
  - копирование или подмена интересующей информации,
  - получение полномочий суперпользователя
- По признакам, позволяющим обнаружить атаку, то есть с позиции наблюдателя
  - наличие в журнале регистрации событий или сетевом трафике определенной информации,
  - подключение к определенной сетевой службе и пр.

Рост обнаруживаемых вредоносных программ

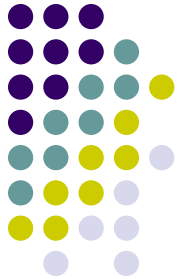


Распределение по ОС



Win32	97100
Linux	123
SunOS	18
Unix	4
DOS	24
SymbianOS	19
Win9x	1

Современные ВП

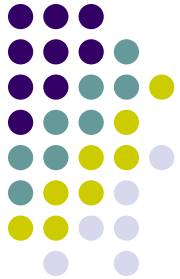


- Лидирует ОС Windows, что говорит главным образом о популярности самой ОС у конечных пользователей
- Технологии распространения
  - с помощью вложений в почтовые сообщения
  - с помощью уязвимостей ОС Windows и ее приложений

Современные ВП

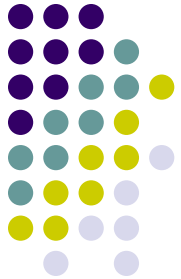
- узлы со старыми системами без обновления уязвимых компонентов, уязвимости «живут» 1-2 года;
- рост числа атак, конечной целью которых является рассылка спама;
- наличие «фонового шума» (15% трафика), вызванного большим количеством bot-сетей, ориентированных на устаревшие уязвимости;
- распространение вредоносных программ через веб-страницы;
- увеличение количества атак, основанных на подборе паролей (bruteforce), направленных на MSSQL, SSH, FTP

Сетевые атаки



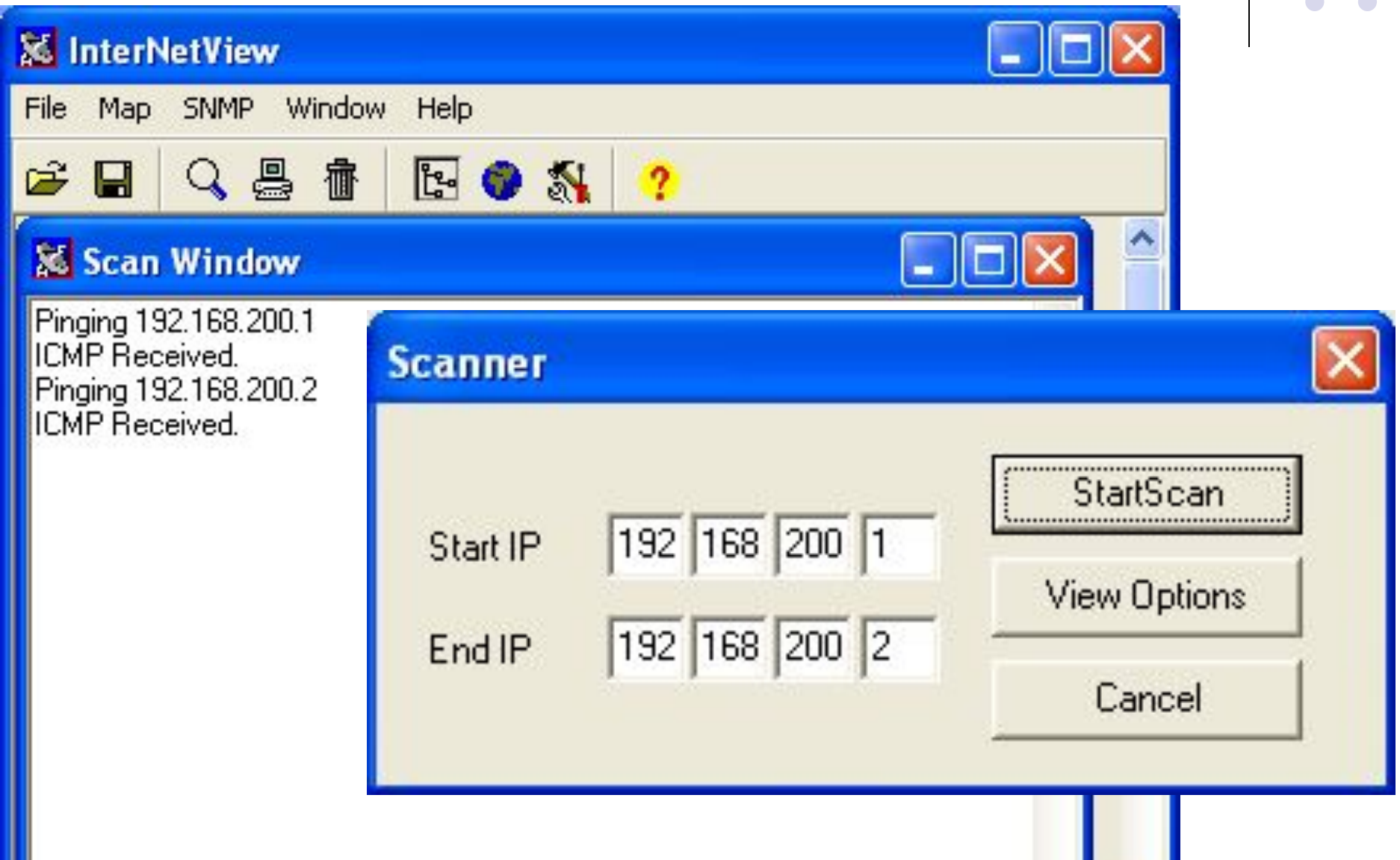
- сбор информации
  - изучение сетевой топологии,
  - определение типа и версии ОС атакуемого узла,
  - доступных сетевых сервисов
- выявление уязвимых мест атакуемой системы
  - анализ наличия уязвимостей в ПО и его настройках
- реализация выбранной атаки
  - отправка сетевых пакетов на определенные сетевые службы
  - SYN Flood, Teardrop, UDP Bomb, подбор паролей

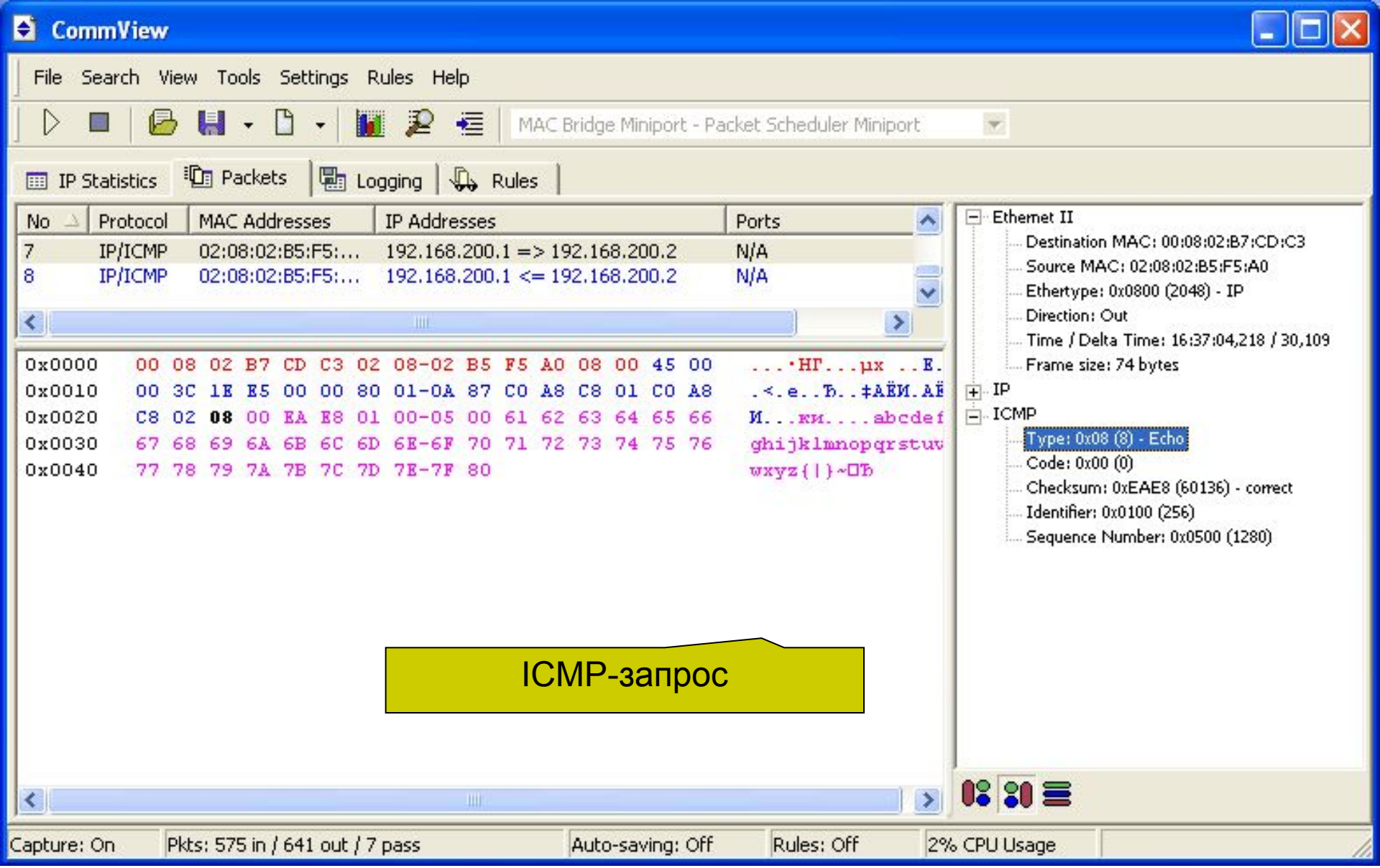
Исследование сетевой топологии

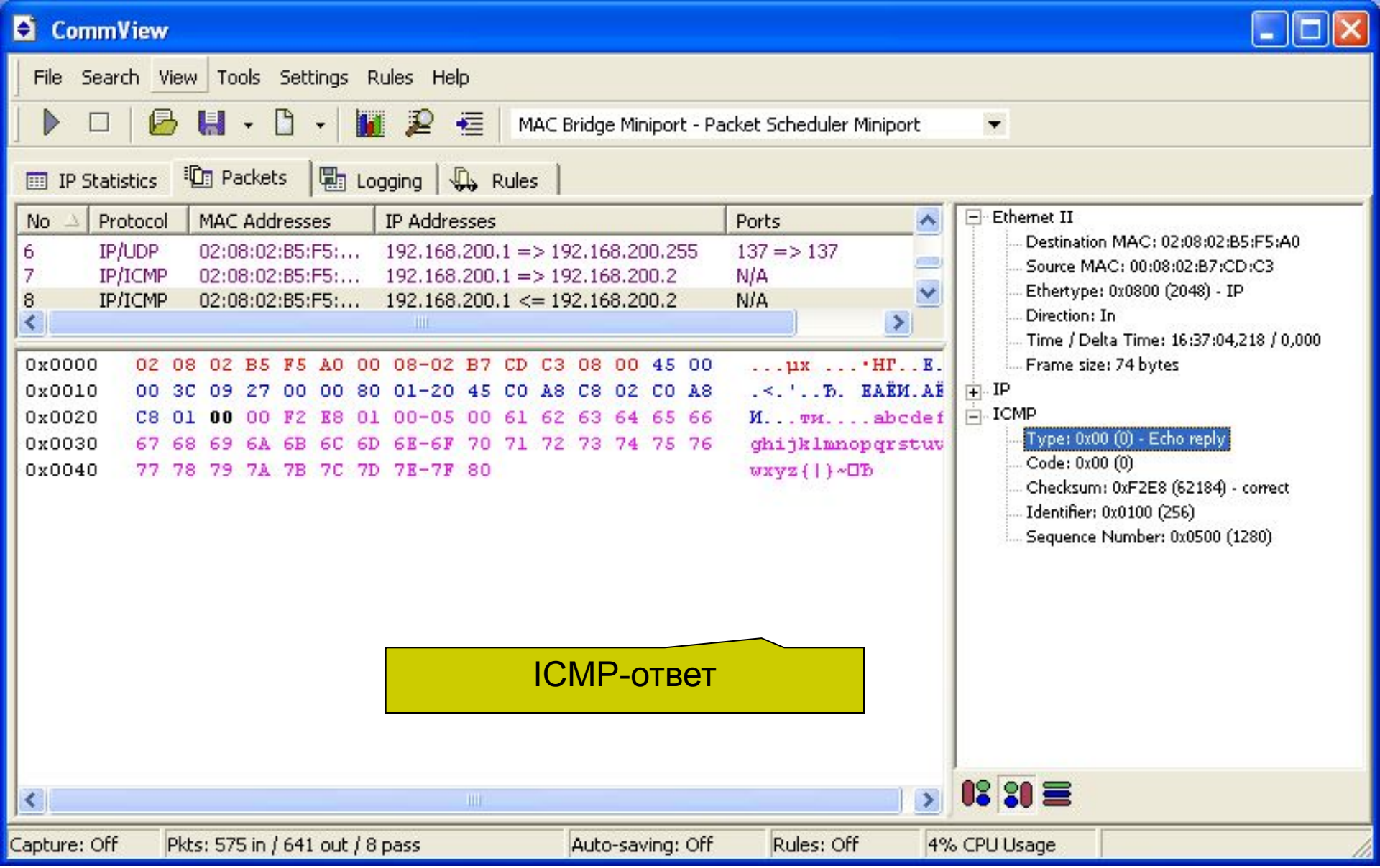


- ICMP-сканирование
  - команда ECHO_REQUEST протокола ICMP
  - ответное сообщение ECHO_REPLY
- TCP-сканирование
  - последовательная установка сетевого соединения по определенному порту с перебором IP-адресов

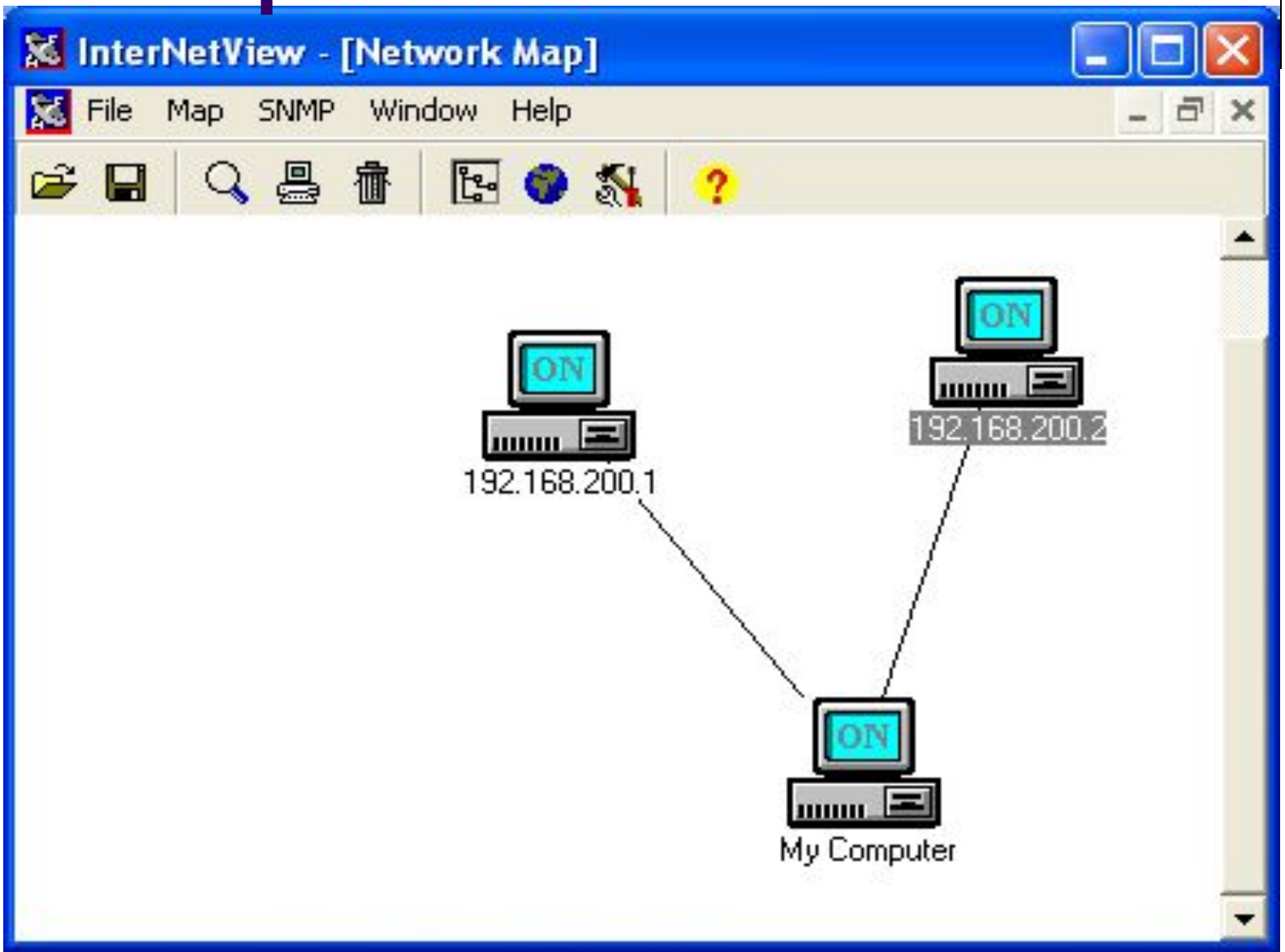
ICMP-сканирование



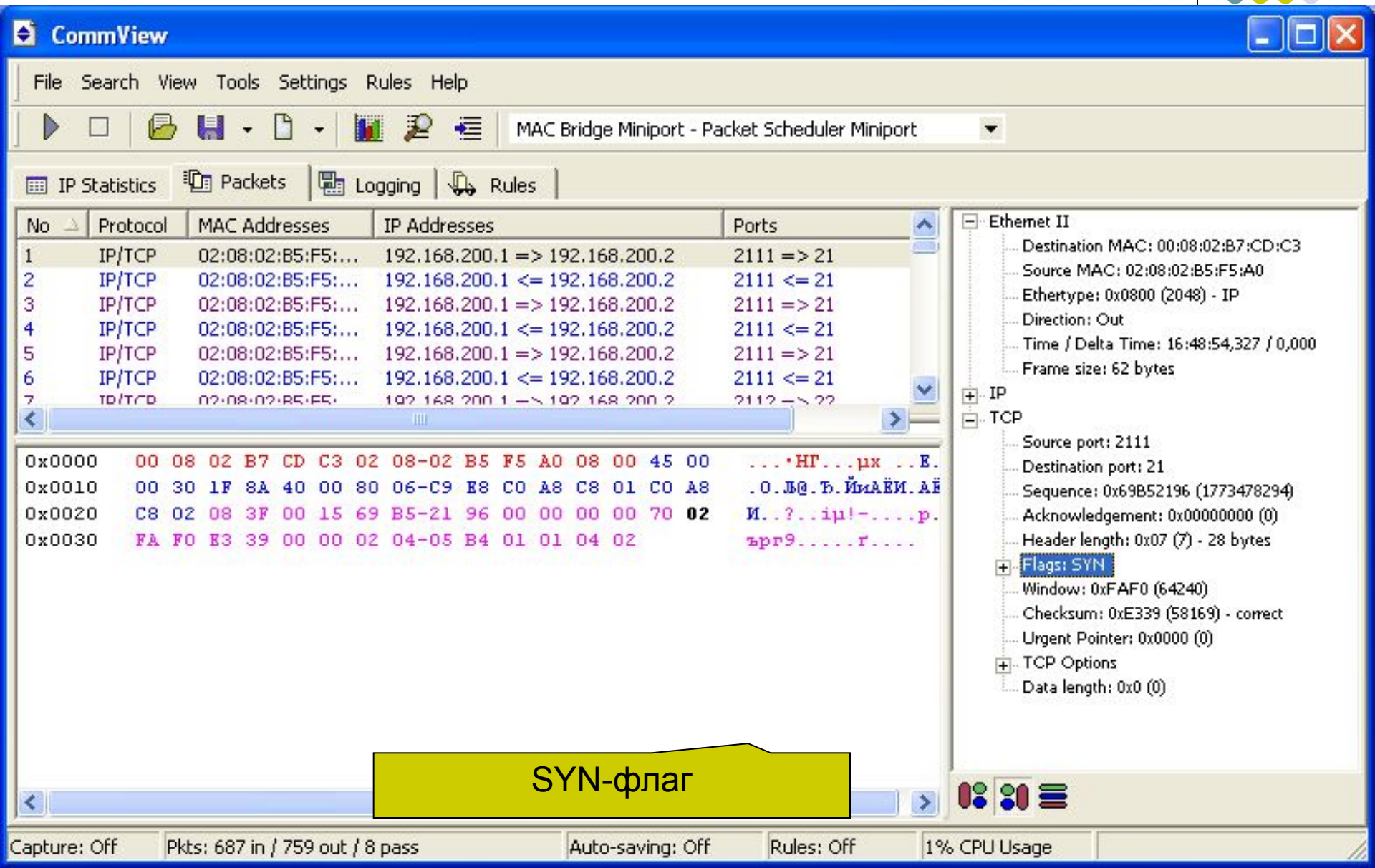

CommView
File Search View Tools Settings Rules Help
MAC Bridge Miniport - Packet Scheduler Miniport
IP Statistics
Packets
Logging
Rules
No Protocol MAC Addresses IP Addresses Ports
7 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 => 192.168.200.2 N/A
8 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 <= 192.168.200.2 N/A
0x0000 00 08 02 B7 CD C3 02 08-02 B5 F5 A0 08 00 45 00
0x0010 00 3C 1E E5 00 00 80 01-0A 87 C0 A8 C8 01 C0 A8
0x0020 C8 02 08 00 EA E8 01 00-05 00 61 62 63 64 65 66
0x0030 67 68 69 6A 6B 6C 6D 6E-6F 70 71 72 73 74 75 76
0x0040 77 78 79 7A 7B 7C 7D 7E-7F 80
Ethernet II
Destination MAC: 00:08:02:B7:CD:C3
Source MAC: 02:08:02:B5:F5:A0
Ethertype: 0x0800 (2048) - IP
Direction: Out
Time / Delta Time: 16:37:04,218 / 30,109
Frame size: 74 bytes
IP
ICMP
Type: 0x08 (8) - Echo
Code: 0x00 (0)
Checksum: 0xEAE8 (60136) - correct
Identifier: 0x0100 (256)
Sequence Number: 0x0500 (1280)
ICMP-запрос
Capture: On
Pkts: 575 in / 641 out / 7 pass
Auto-saving: Off
Rules: Off
2% CPU Usage


CommView
File Search View Tools Settings Rules Help
MAC Bridge Miniport - Packet Scheduler Miniport
IP Statistics Packets Logging Rules
No Protocol MAC Addresses IP Addresses Ports
6 IP/UDP 02:08:02:B5:F5:... 192.168.200.1 => 192.168.200.255 137 => 137
7 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 => 192.168.200.2 N/A
8 IP/ICMP 02:08:02:B5:F5:... 192.168.200.1 <= 192.168.200.2 N/A
0x0000 02 08 02 B5 F5 A0 00 08-02 B7 CD C3 08 00 45 00
0x0010 00 3C 09 27 00 00 80 01-20 45 C0 A8 C8 02 C0 A8
0x0020 C8 01 00 00 F2 E8 01 00-05 00 61 62 63 64 65 66
0x0030 67 68 69 6A 6B 6C 6D 6E-6F 70 71 72 73 74 75 76
0x0040 77 78 79 7A 7B 7C 7D 7E-7F 80
Ethernet II
Destination MAC: 02:08:02:B5:F5:A0
Source MAC: 00:08:02:B7:CD:C3
Ethertype: 0x0800 (2048) - IP
Direction: In
Time / Delta Time: 16:37:04,218 / 0,000
Frame size: 74 bytes
IP
ICMP
Type: 0x00 (0) - Echo reply
Code: 0x00 (0)
Checksum: 0xF2E8 (62184) - correct
Identifier: 0x0100 (256)
Sequence Number: 0x0500 (1280)
ICMP-ответ
Capture: Off
Pkts: 575 in / 641 out / 8 pass
Auto-saving: Off
Rules: Off
4% CPU Usage

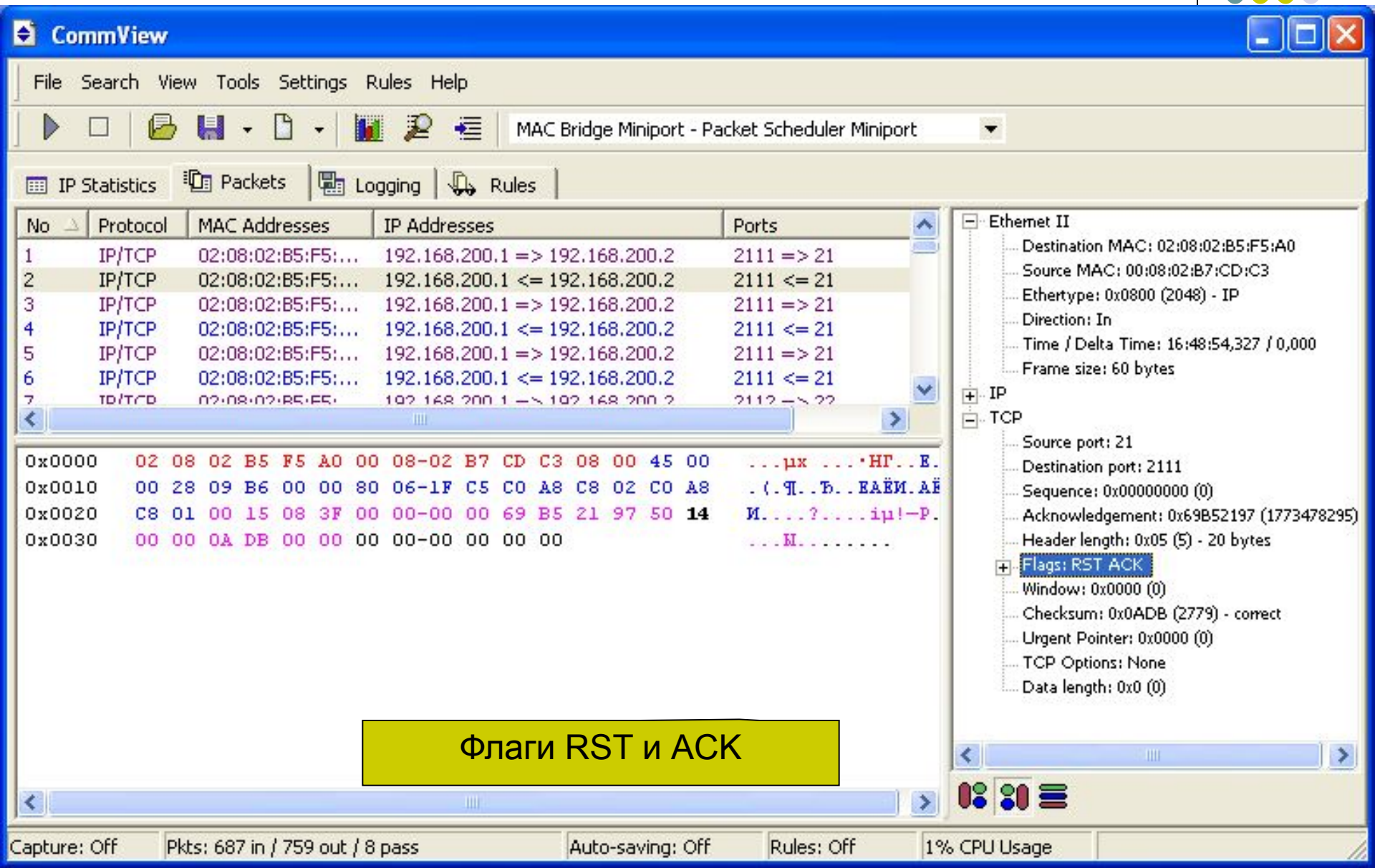
Результат ICMP-сканирования



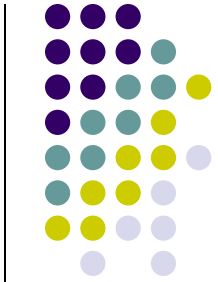
TCP-сканирование



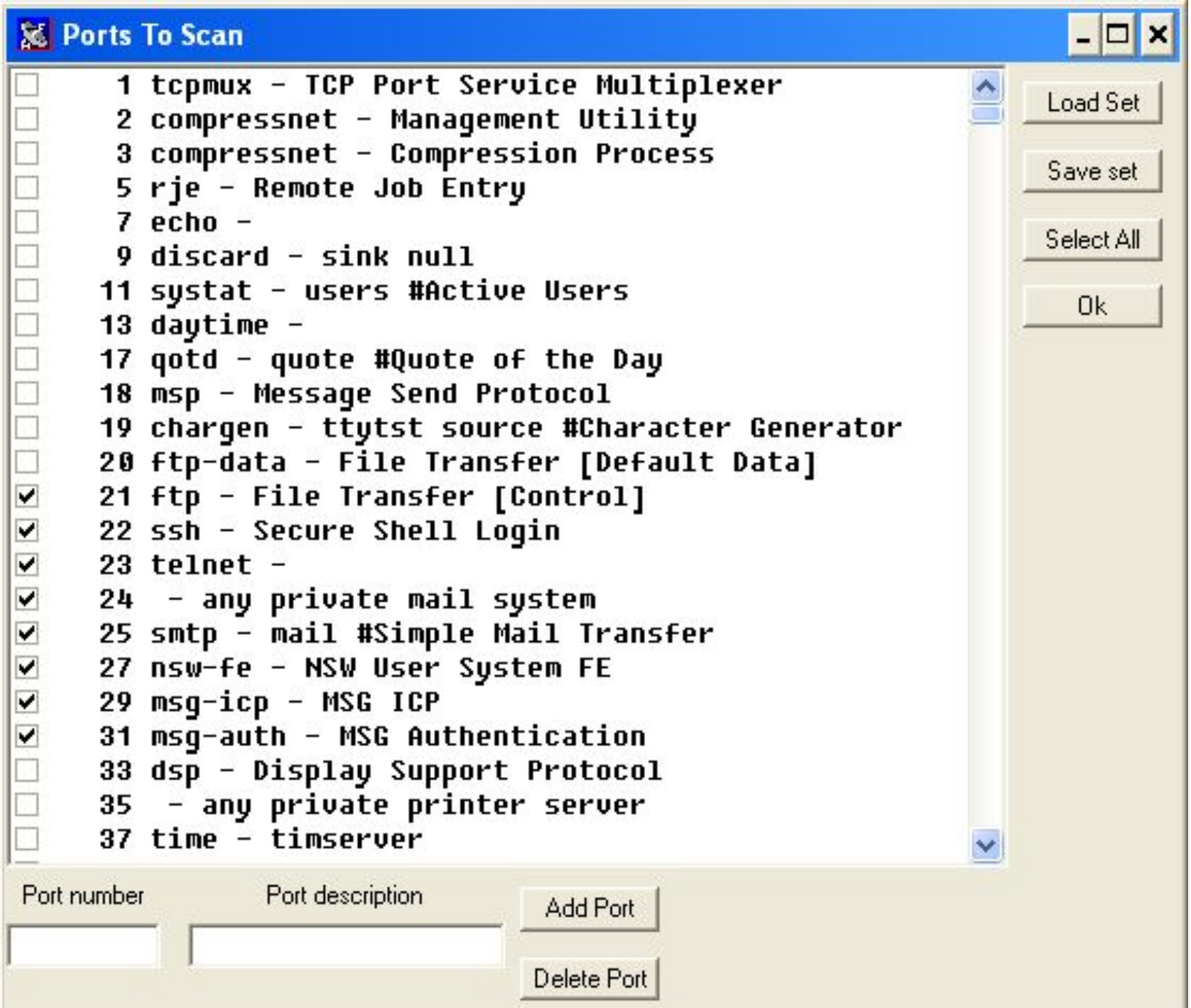
Искомый узел присутствует

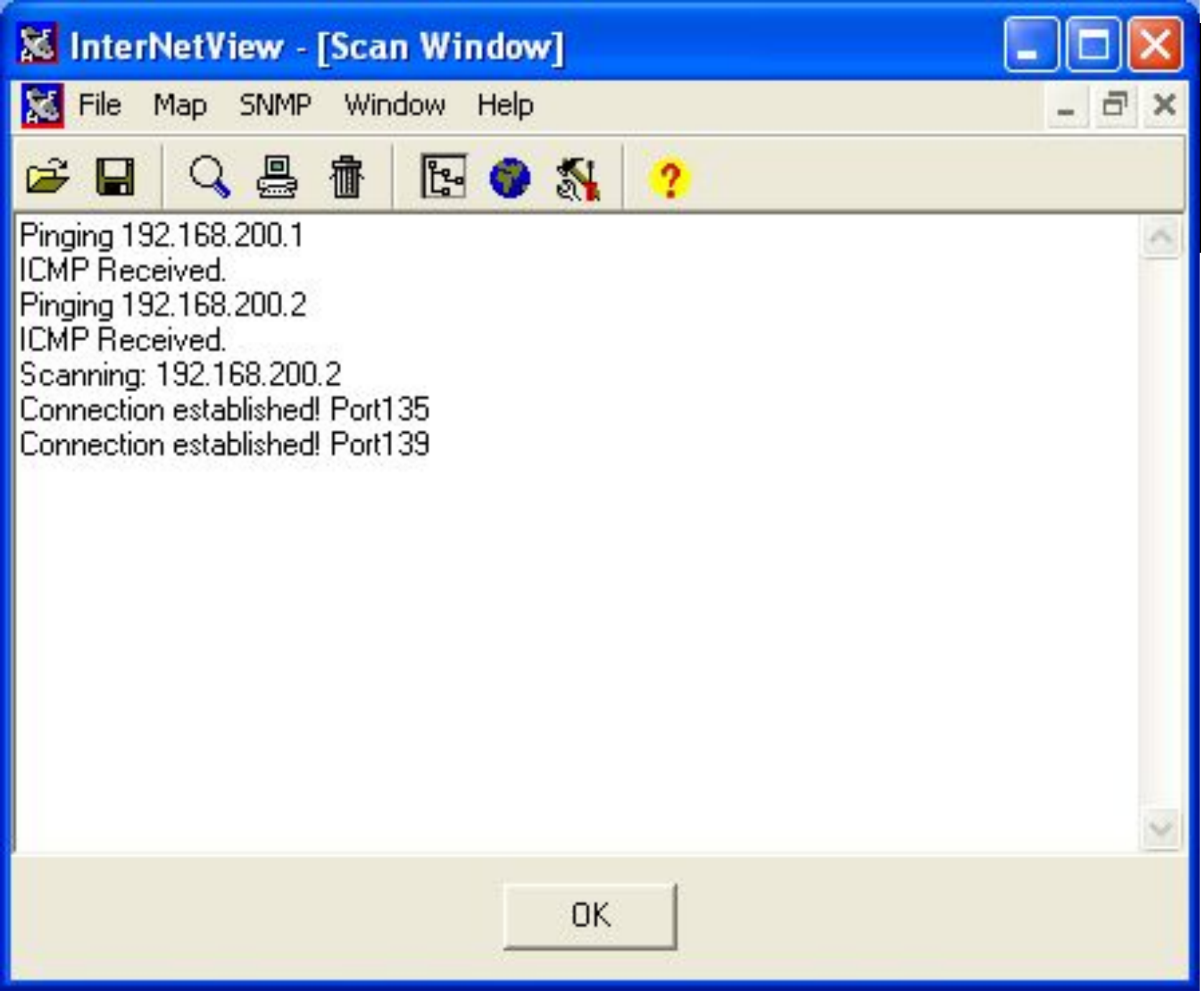


Сканирование портов

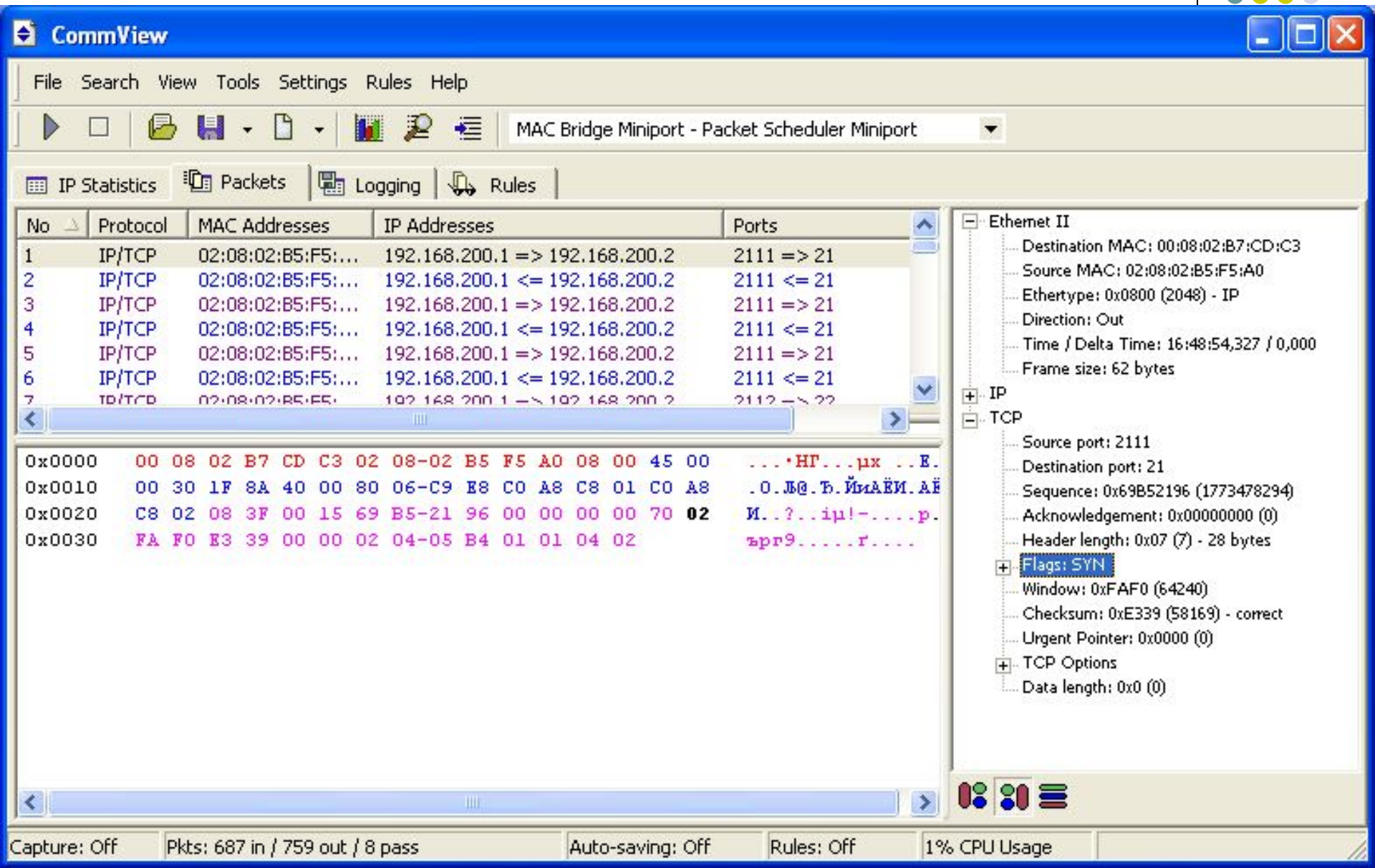


- Определение функционирующих сетевых служб
  - TCP-21- ftp
  - TCP- 23- telnet
  - TCP- 25- smtp
  - TCP- 80- http
  - TCP- 110- pop3
  - TCP- 135- RPC
  - TCP- 139- NetBIOS
  - TCP- 445- RPC, DFS

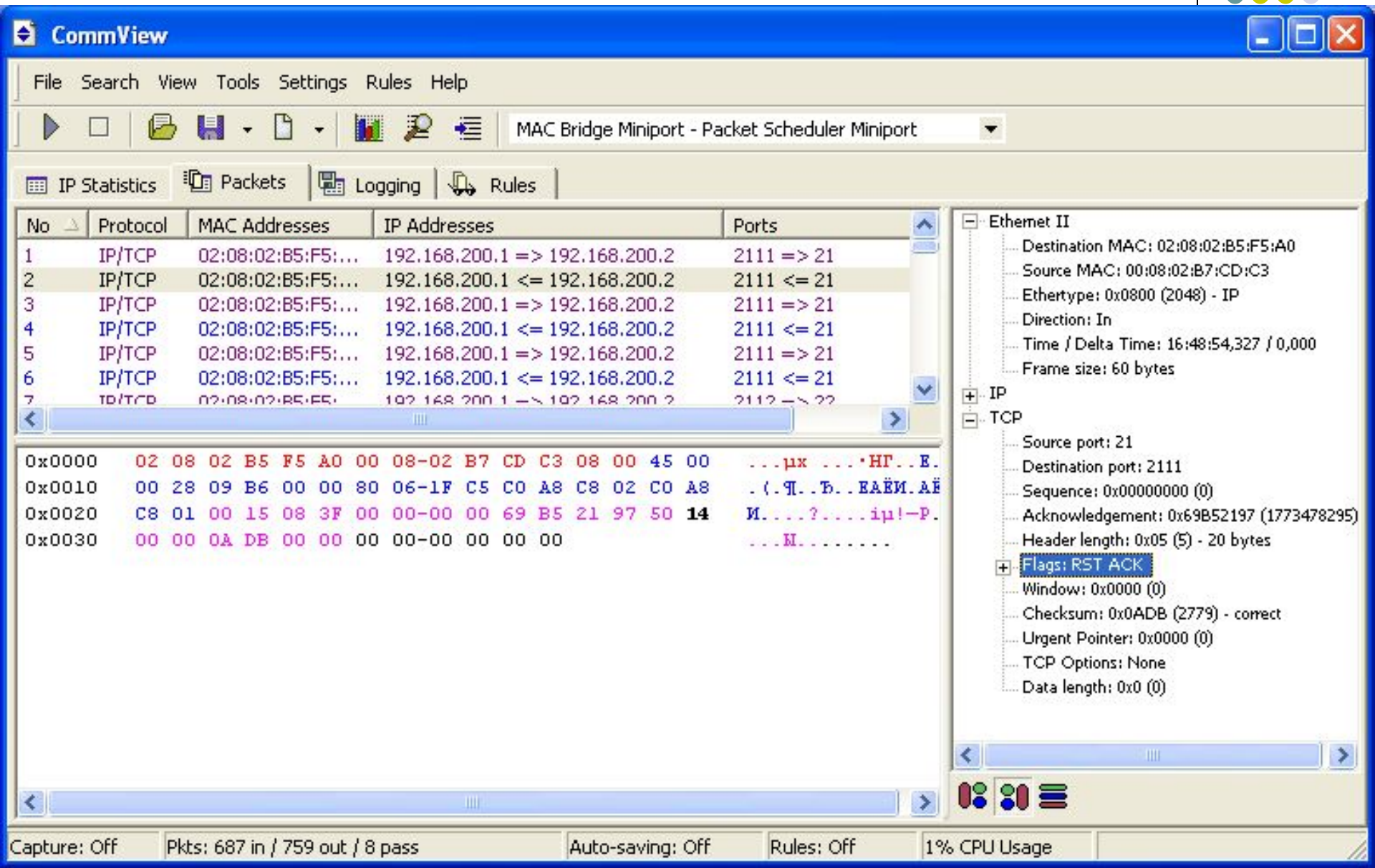

Ports To Scan
1 tcpmux - TCP Port Service Multiplexer
2 compressnet - Management Utility
3 compressnet - Compression Process
5 rje - Remote Job Entry
7 echo -
9 discard - sink null
11 systat - users #Active Users
13 daytime -
17 qotd - quote #Quote of the Day
18 msp - Message Send Protocol
19 chargen - ttytst source #Character Generator
20 ftp-data - File Transfer [Default Data]
21 ftp - File Transfer [Control]
22 ssh - Secure Shell Login
23 telnet -
24 - any private mail system
25 smtp - mail #Simple Mail Transfer
27 nsw-fe - NSW User System FE
29 msg-icp - MSG ICP
31 msg-auth - MSG Authentication
33 dsp - Display Support Protocol
35 - any private printer server
37 time - timserver
Load Set
Save set
Select All
Ok
Port number
Port description
Add Port
Delete Port


InterNetView - [Scan Window]
File
Map
SNMP
Window
Help
Pinging 192.168.200.1
ICMP Received.
Pinging 192.168.200.2
ICMP Received.
Scanning: 192.168.200.2
Connection established! Port135
Connection established! Port139
OK

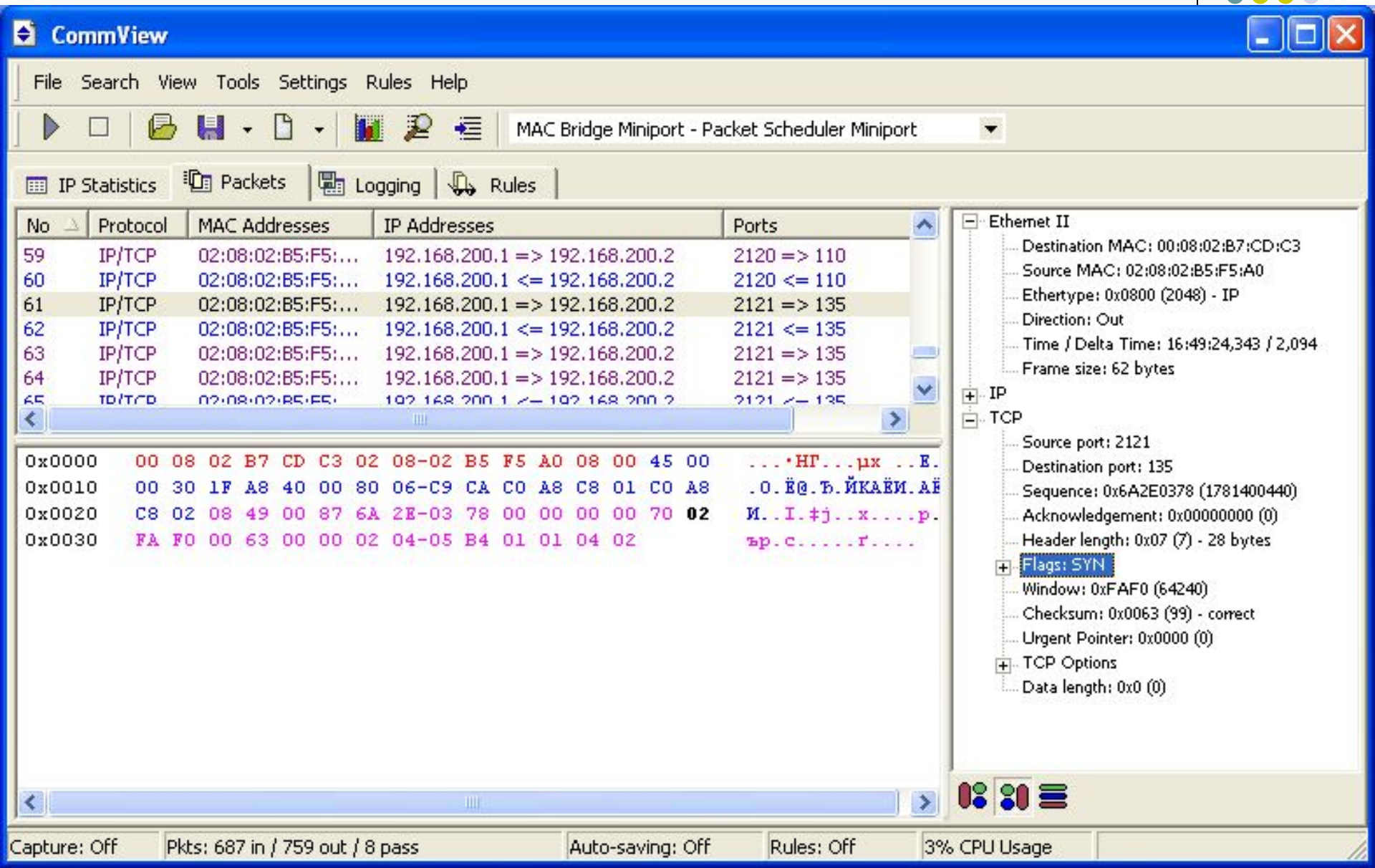
Connect()-сканирование, порт 21



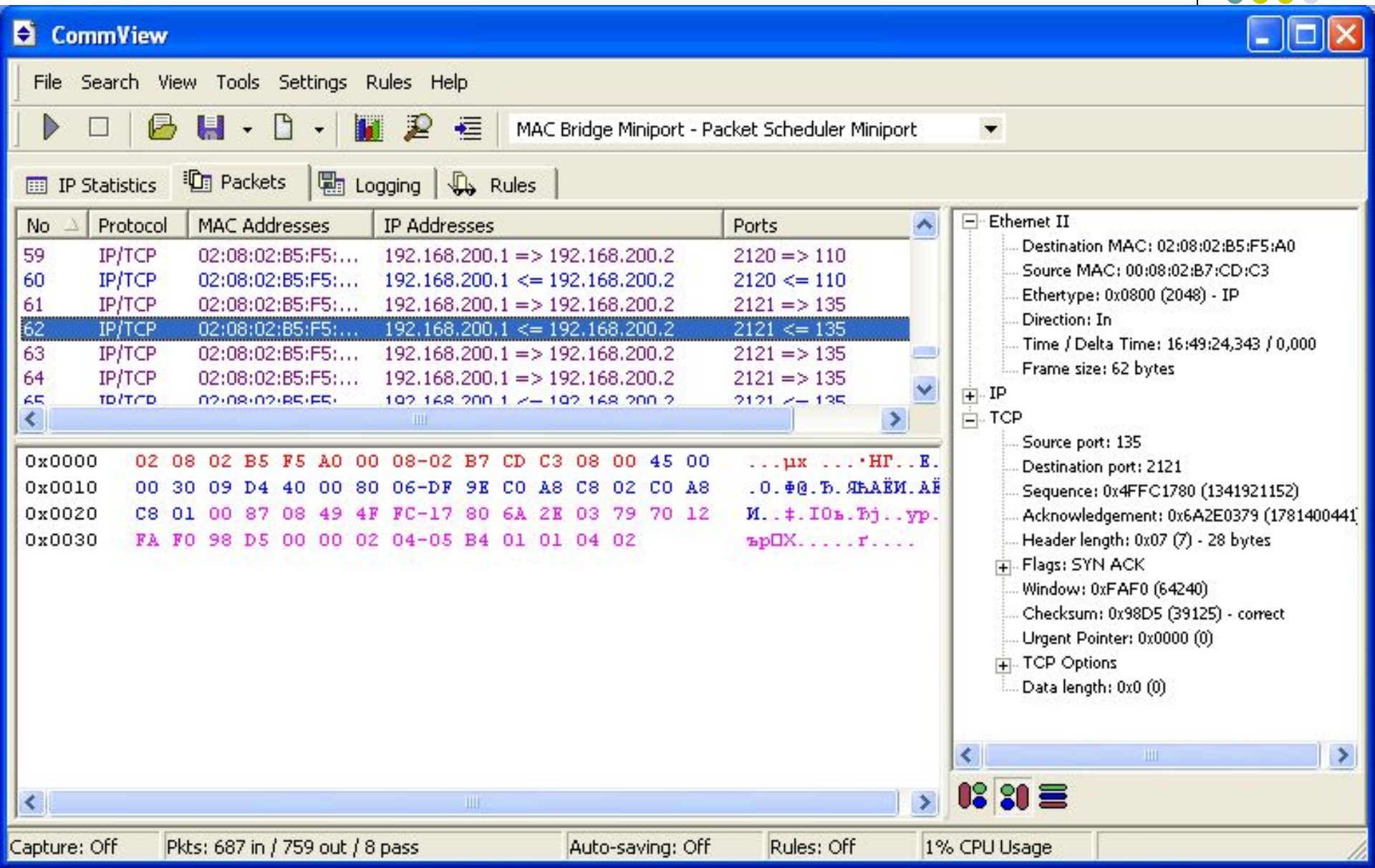
Ответ - «закрытый порт»



Connect()-сканирование, порт 135

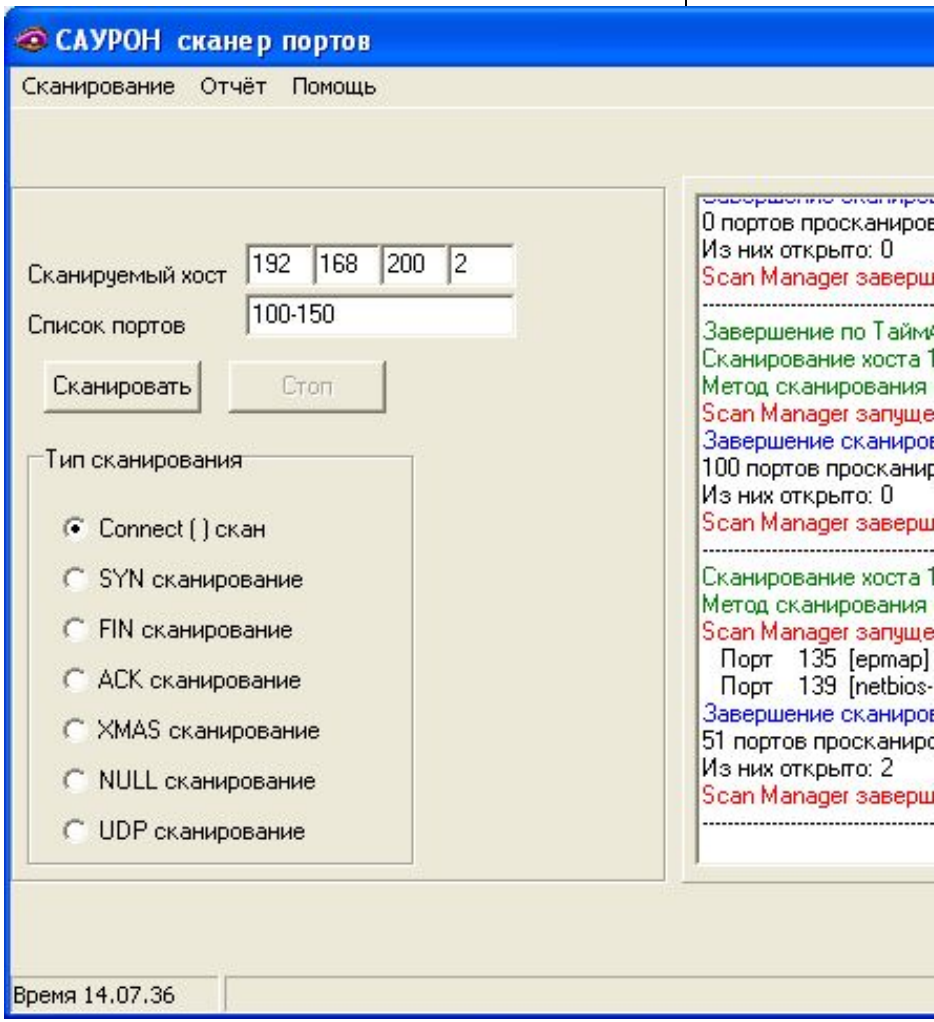


Ответ - «открытый порт»

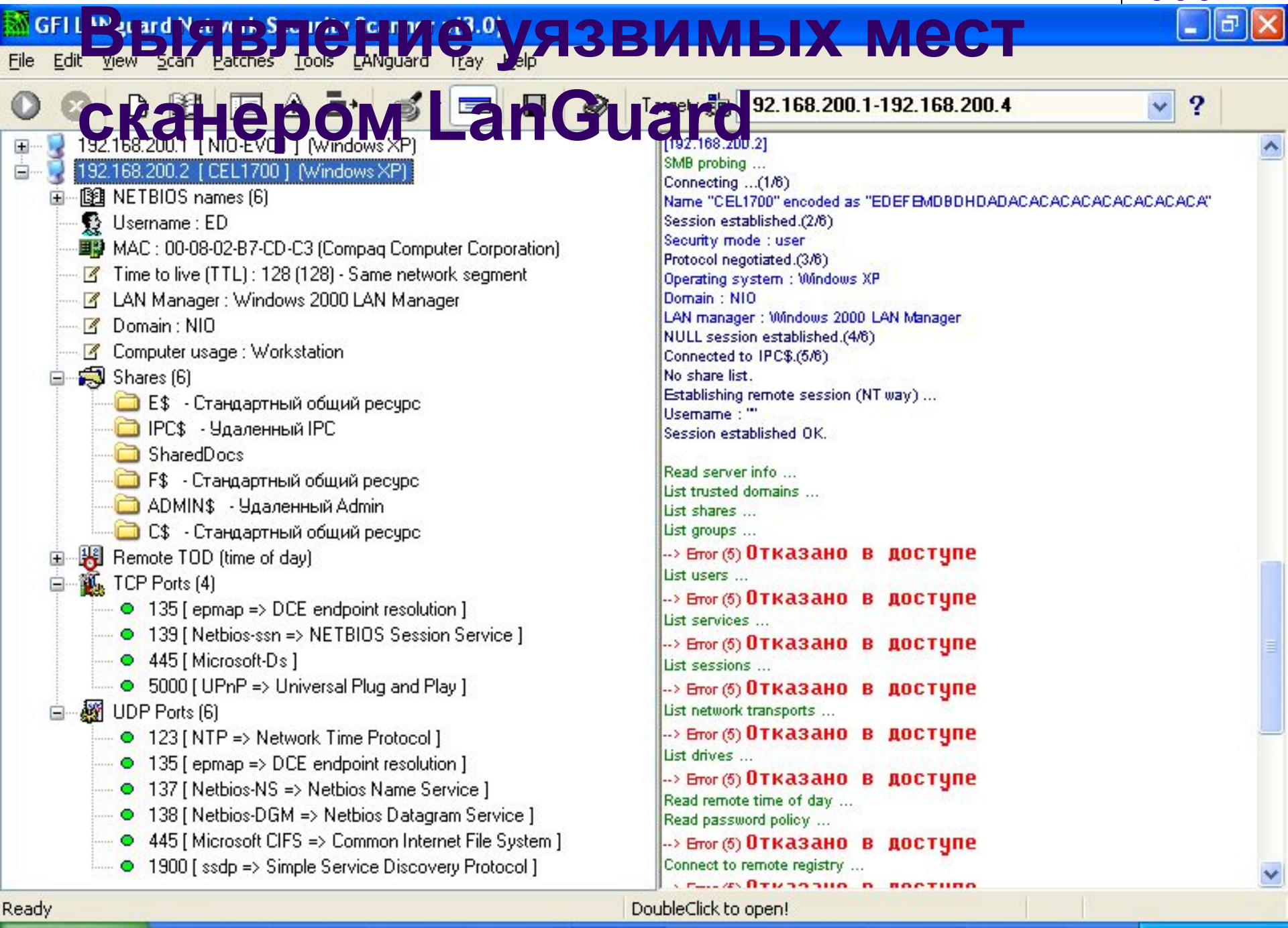


Иные способы сканирования

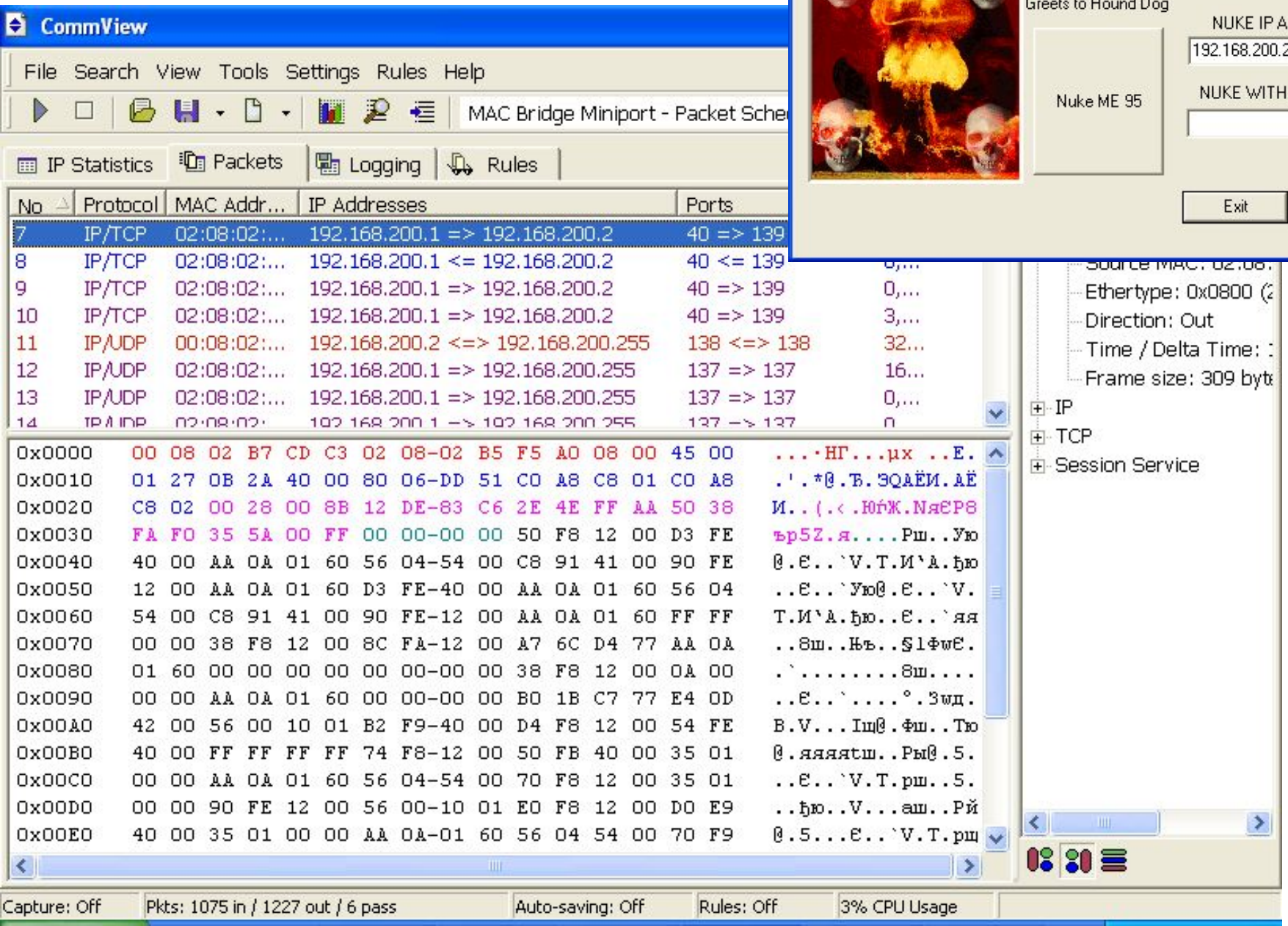
- SYN-сканирование,
- FIN-сканирование,
- ACK-сканирование,
- XMAS-сканирование,
- NULL-сканирование,
- UDP-сканирование



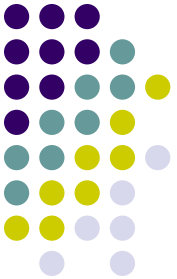
Выявление уязвимых мест сканером LanGuard



Реализации атак



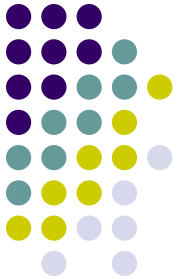
Реализации атак



- Анонимное подключение в ОС Windows

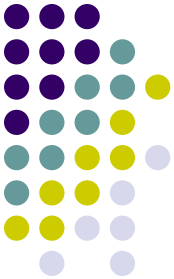
net use *.*.*.*\IPC$ "" /user:""

Общие принципы защиты



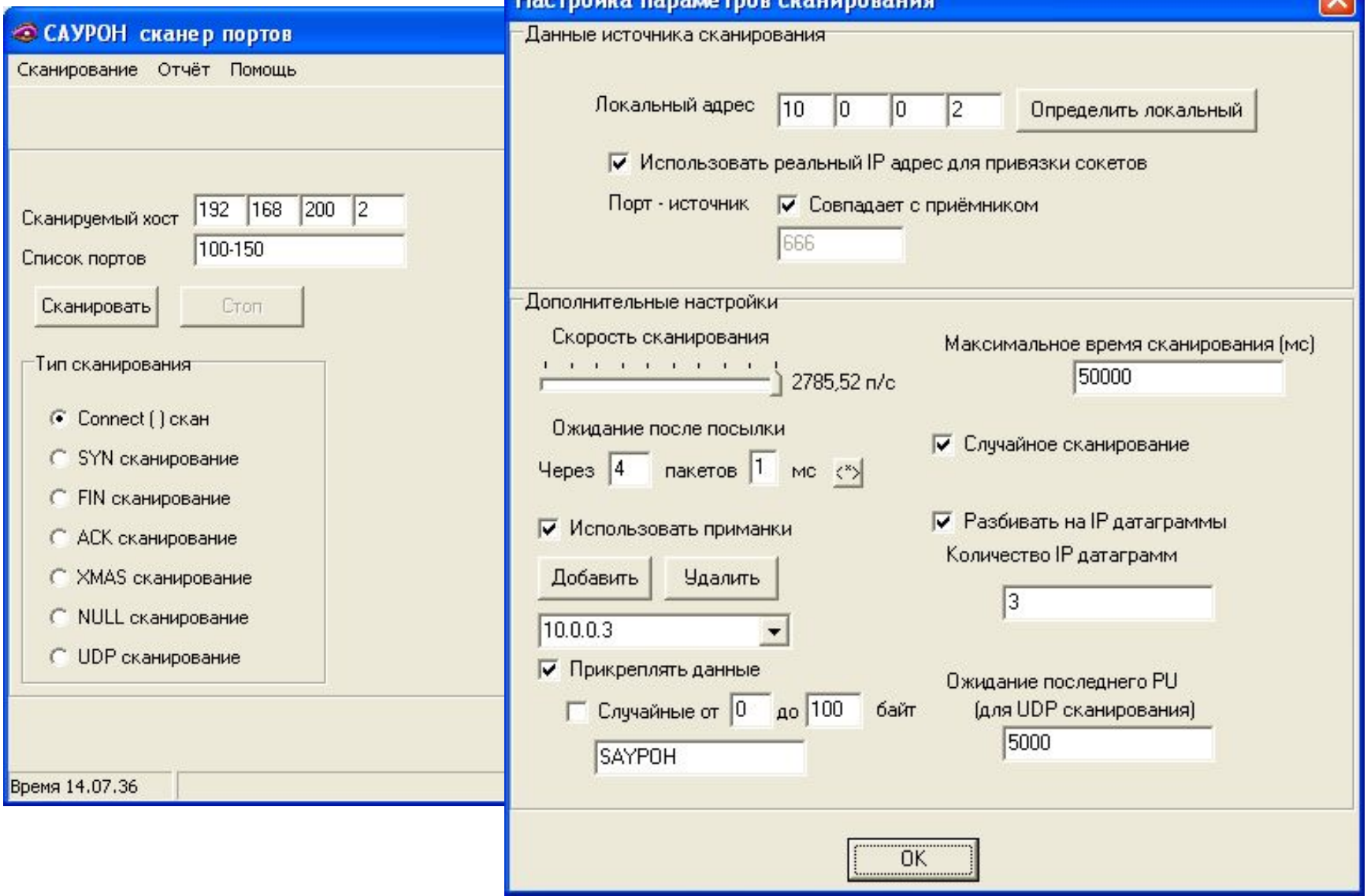
- Обнаружение и запрет:
  - входящих ICMP-запросов
  - исходящих ICMP-ответов
  - установки TCP-соединений извне
  - опасных TCP- и UDP-портов

Усложненные атаки



- последовательность опроса узлов
- 07:11:38.123565 200.0.0.200 > 200.0.0.**34**: icmp: echo request
  07:11:51.456342 200.0.0.200 > 200.0.0.**47**: icmp: echo request
  07:11:04.678432 200.0.0.200 > 200.0.0.**3**: icmp: echo request
  07:12:18.985667 200.0.0.200 > 200.0.0.**12**: icmp: echo request
  07:12:31.024657 200.0.0.200 > 200.0.0.**11**: icmp: echo request
  07:12:44.044567 200.0.0.200 > 200.0.0.**9**: icmp: echo request
  07:12:57.071234 200.0.0.200 > 200.0.0.**104**: icmp: echo request
  ....
- увеличение интервала времени
- 12:01:38.234455 200.0.0.200 > 200.0.0.**67**: icmp: echo request
  12:03:51.543524 200.0.0.200 > 200.0.0.**87**: icmp: echo request
  12:05:04.655342 200.0.0.200 > 200.0.0.**134**: icmp: echo request
  12:07:18.573256 200.0.0.200 > 200.0.0.**23**: icmp: echo request
  12:09:31.676899 200.0.0.200 > 200.0.0.**11**: icmp: echo request
  12:11:44.896754 200.0.0.200 > 200.0.0.**104**: icmp: echo request
  12:13:57.075356 200.0.0.200 > 200.0.0.**2**: icmp: echo request

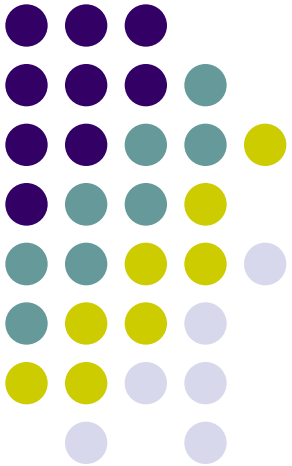
Усложненные атаки



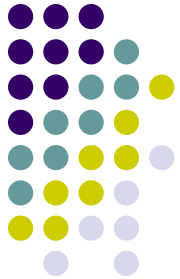
Обнаружение атак

Системы обнаружения атак, СОА

(intrusion detection systems, IDS)



Система обнаружения атак



- программный или программно-аппаратный комплекс, предназначенный для выявления и, по возможности, предупреждения, действий, угрожающих безопасности информационной системы
- СОА, СОКА, СОПКА
- Система обнаружения вторжений
- IDS, NIDS

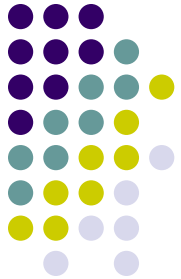
Классификация СОА

- по методу обнаружения:
  - системы сигнатурного анализа
  - системы обнаружения аномалий;
- по способу обработки данных:
  - системы реального времени
  - системы отложенной обработки;
- по типу анализируемых данных:
  - узловые (host-based)
  - сетевые (network-based);
- по конфигурации:
  - компактные
  - распределенные системы

COA Snort

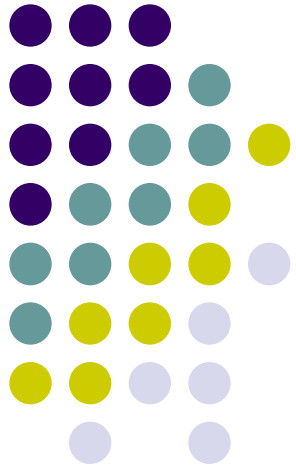
- по методу обнаружения:
  - система сигнатурного анализа
- по способу обработки данных:
  - система реального времени
- по типу анализируемых данных:
  - сетевая (network-based);
- по конфигурации:
  - компактная

COA Snort

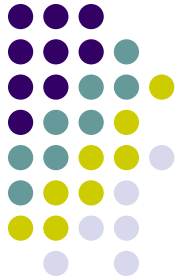


- Сигнатуры атак описываются при помощи правил (rules)
- Набор правил требует обновления
- Доступно зарегистрированным пользователям

С ИСПОЛЬЗОВАНИЕМ МЕЖСЕТЕВЫХ ЭКРАНОВ

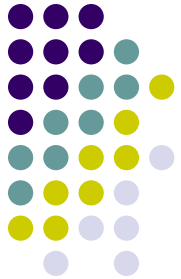


Стандартные требования



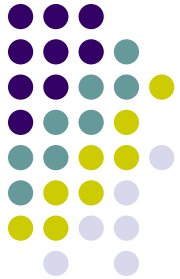
- К Web-серверам организации должен быть разрешен доступ из Интернет
- В организацию должна приходить почта
- Из внутренней сети должен быть разрешен доступ к внешним Web- и FTP-серверам
- Необходимо разрешить отправлять исходящую почту

Стандартная задача



- Между Интернетом и внутренней сетью не должно быть прямого трафика

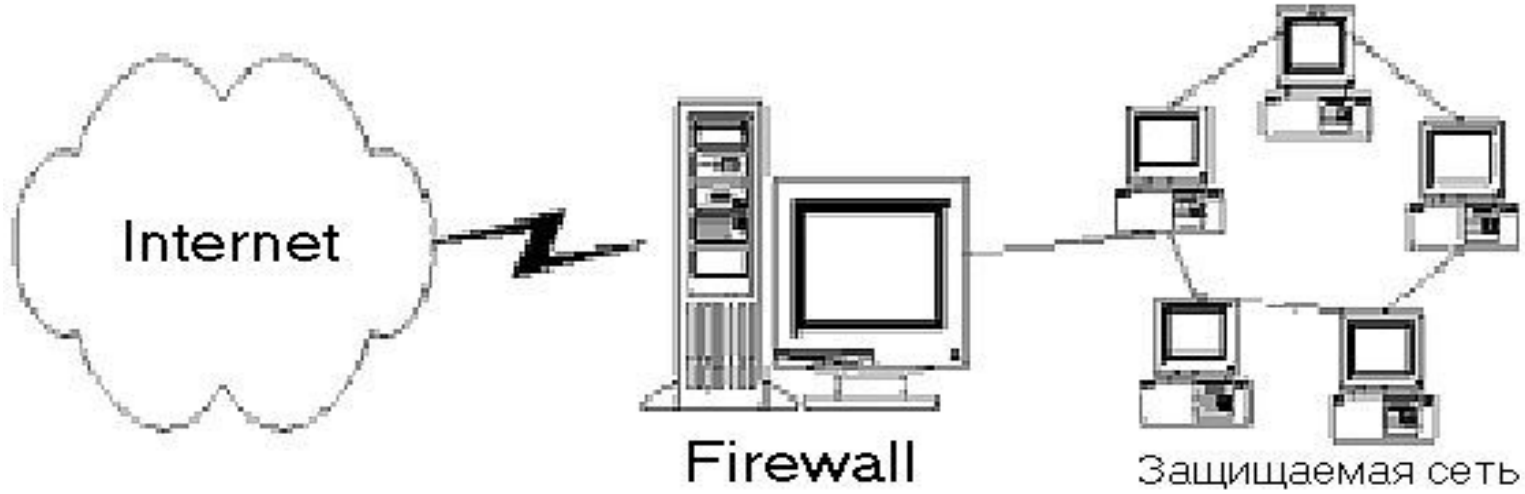
Межсетевой экран (МЭ)



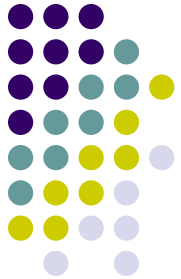
- Система межсетевой защиты, позволяющая разделить общую сеть на две части и более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую
- Firewall, брандмауэр

Межсетевой экран (МЭ)

- Локальное или функционально-распределенное аппаратно-программное (программное) средство, реализующее контроль за информацией, поступающей в АС и/или выходящей из АС

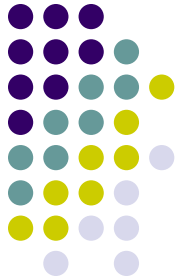


Политика сетевой безопасности



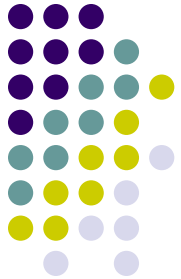
- Политика доступа к сетевым ресурсам
- Политика реализации МЭ

Политика сетевой безопасности



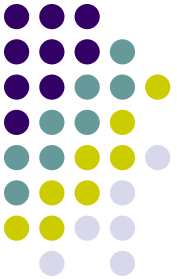
- Политика доступа к сетевым ресурсам
  - запретить доступ из Интернет во внутреннюю сеть, но разрешить доступ из внутренней сети в Интернет
  - разрешить ограниченный доступ во внутреннюю сеть из Интернет

Политика сетевой безопасности



- Политика реализации МЭ
  - запрещать все, что не разрешено
  - разрешать все, что не запрещено

Основные компоненты МЭ



- Фильтрующие маршрутизаторы
- Шлюзы сетевого уровня
- Шлюзы прикладного уровня

Фильтрующий маршрутизатор

- Фильтрация входящих и исходящих пакетов на основе информации, содержащейся в TCP- и IP- заголовках пакетов

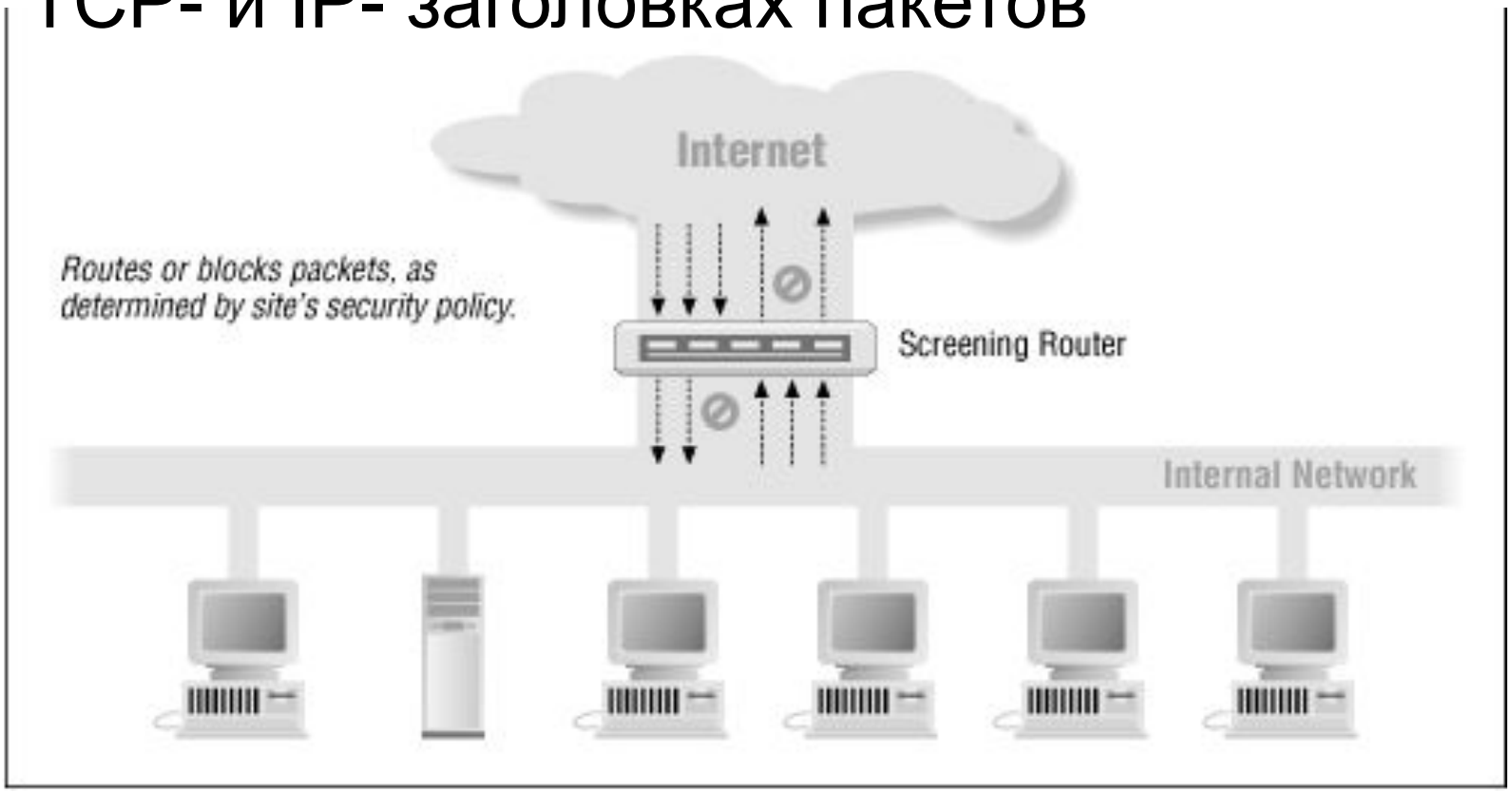


Схема инкапсуляции данных в стеке протоколов TCP/IP

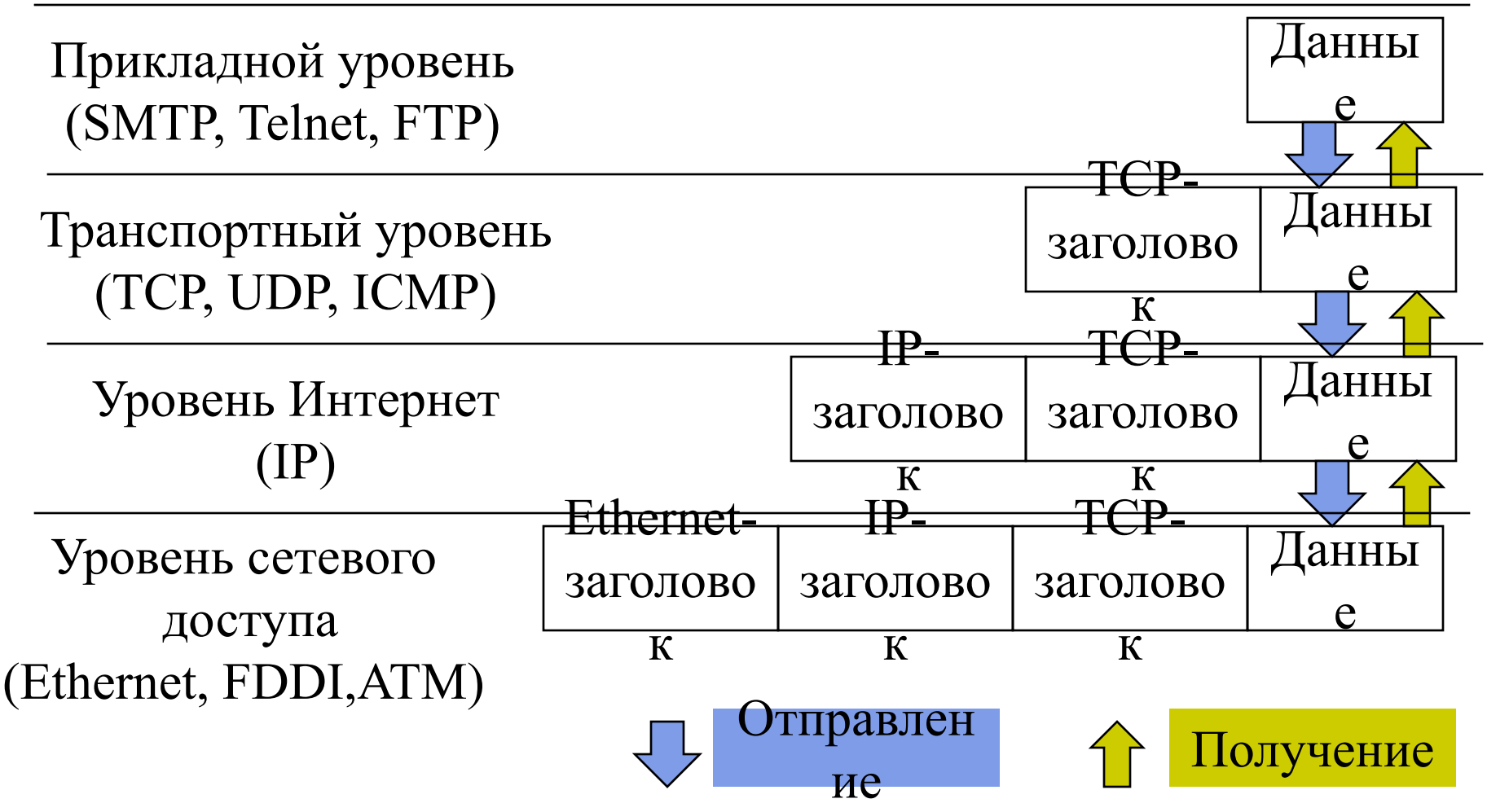
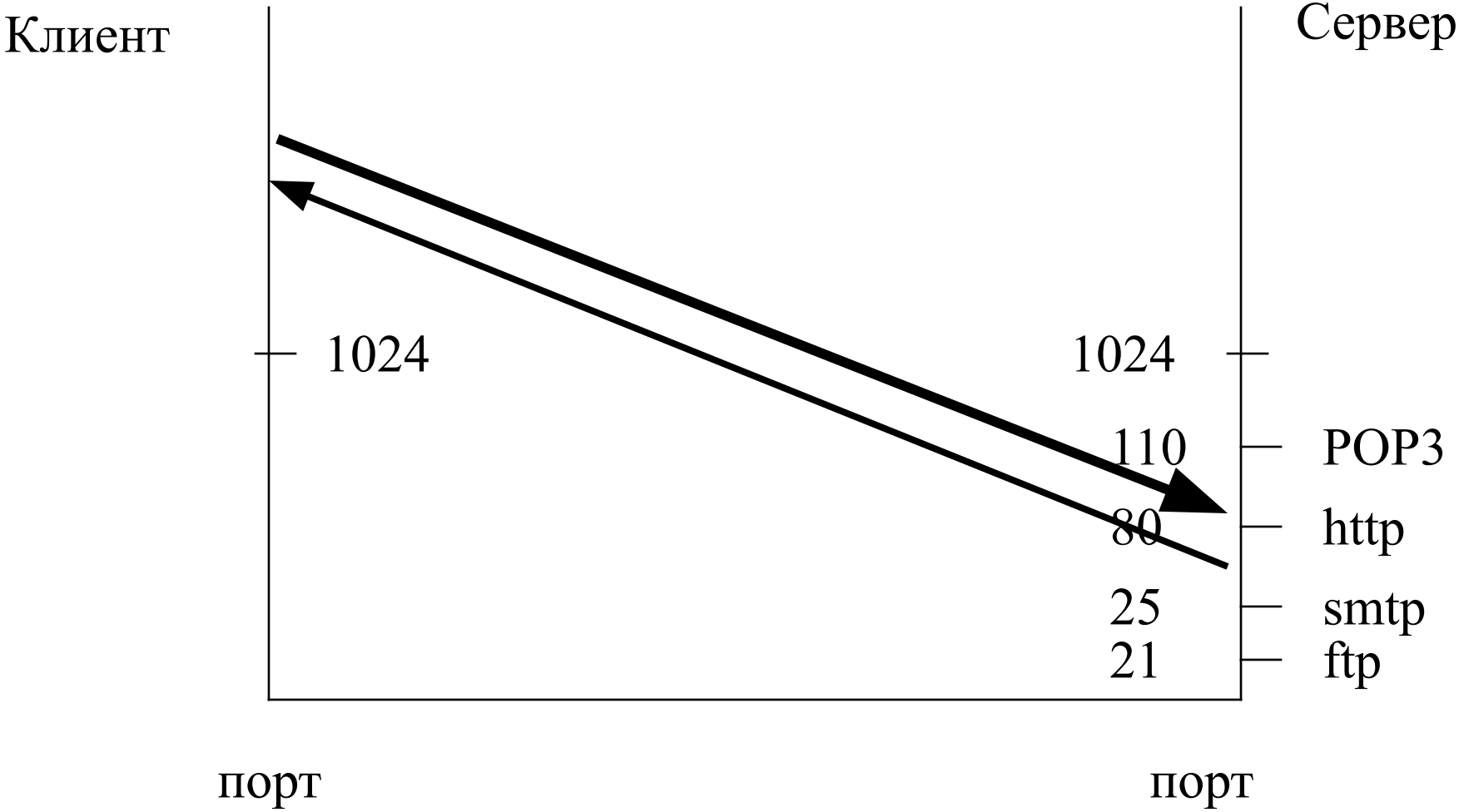
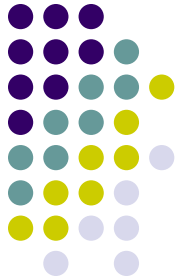


Схема информационного обмена

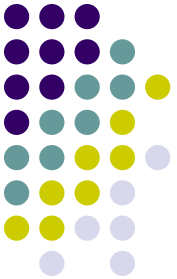


Критерии фильтрации пакетов



- IP-адрес отправителя
- IP-адрес получателя
- тип протокола (TCP, UDP, ICMP)
- порт отправителя (TCP, UDP)
- порт получателя (TCP, UDP)
- тип сообщения (ICMP)

Задача 1



- Обеспечить обмен электронной почтой между внутренним и внешним SMTP серверами
- протоколTCP, порт:25

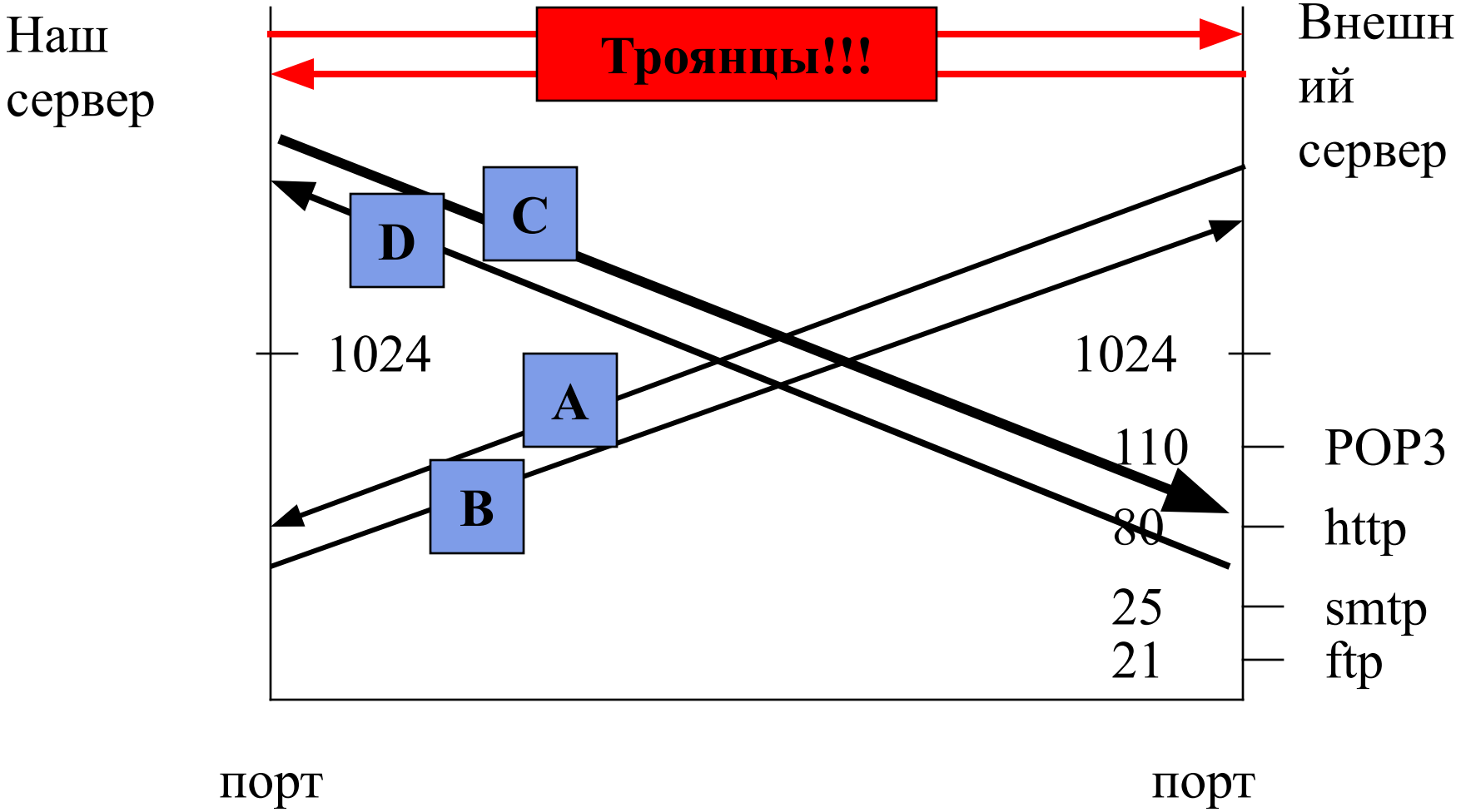
Правила A, B - чтобы на наш сервер приходили письма

Правила C, D - чтобы наш сервер мог отправлять письма

Правило E - запрещает иные пакеты

Правило	Направление	Тип	Источник	Получатель	Порт получателя	Действие
A	вход	TCP	внешн	внутр	25	разреш.
B	выход	TCP	внутр	внешний	>=1024	разреш.
C	выход	TCP	внутр	внешний	25	разреш.
D	вход	TCP	внешн	внутр	>=1024	разреш.
E	любое	любой	любой	любой	любой	отказ

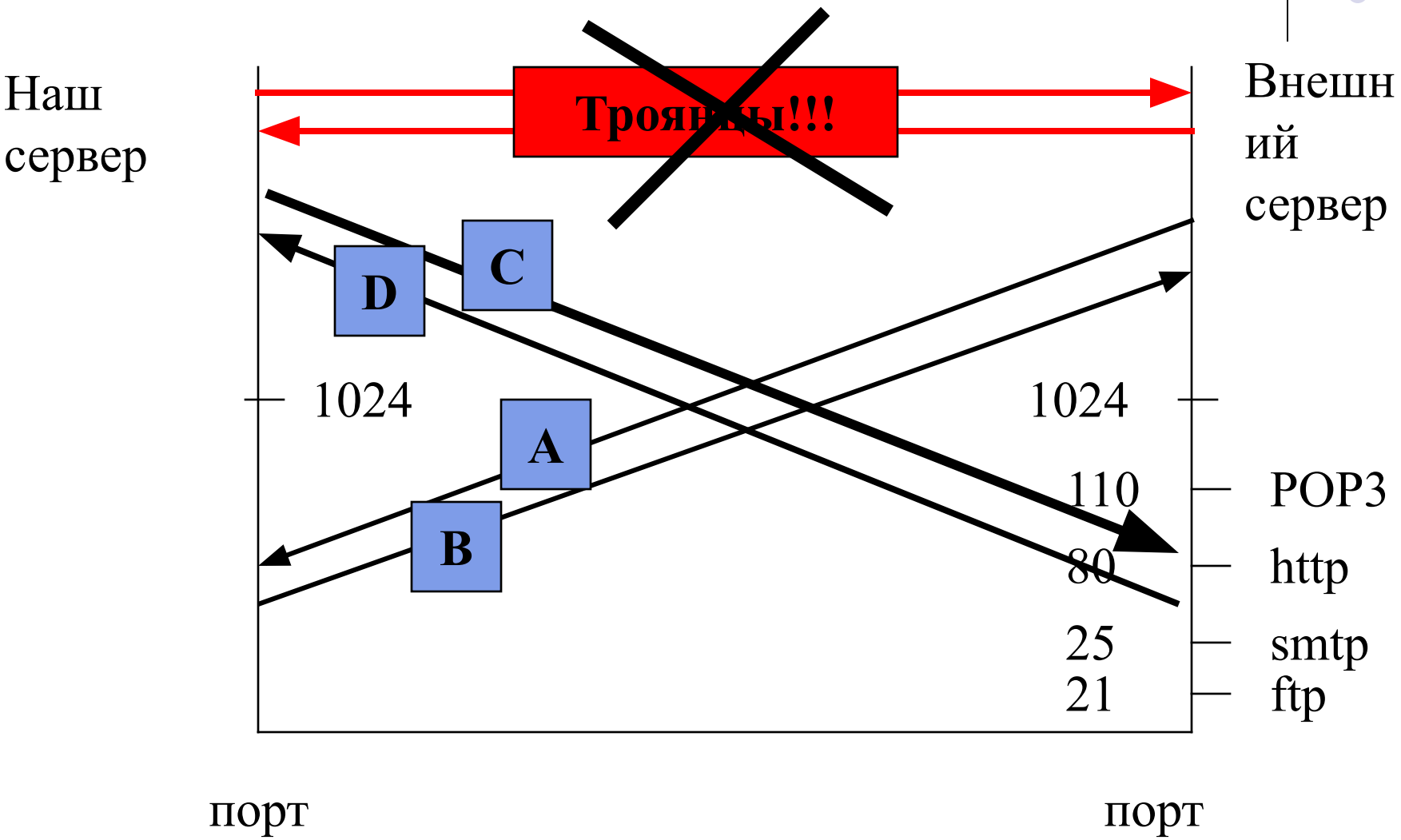
Правила A,B,C,D,E



Улучшенные правила

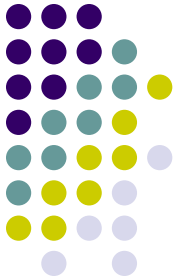
Правило	Направление	Тип	Источник	Порт источника	Получатель	Порт получателя	Действие
A	вход	TCP	внешн	>=1024	внутр	25	разреш.
B	выход	TCP	внутр	25	внешний	>=1024	разреш.
C	выход	TCP	внутр	>=1024	внешний	25	разреш.
D	вход	TCP	внешн	25	внутр	>=1024	разреш.
E	любое	любой	любой	любой	любой	любой	отказ

Улучшенные правила A,B,C,D,E

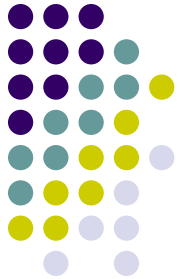


Задача 2

- Защищаемая организация имеет сеть 123.45.0.0/16
- Запретить из Интернет доступ в сеть 123.45.0.0/16
- Но разрешить доступ в подсеть 123.45.6.0/24 данной сети из сети 135.79.0.0/16
- При этом специально запретить в защищаемую сеть доступ из подсети 135.79.6.0/24, за исключением доступа к подсети 123.45.6.0/24

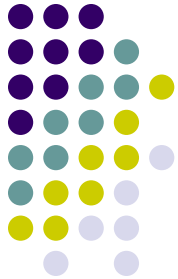


Пояснение - маска подсети



- Адрес в сети:
  - 123.45.6.0
  - 01111011.00101101.00000110.00000000
  - 255.255.255.255
  - 11111111.11111111.11111111.11111111
  - /16
  - 255.255.0.0
  - /24
  - 255.255.255.0

Правила фильтрации пакетов, поступающих извне



Правило	Адрес источника	Адрес назначения	Действие
A	135.79.0.0/16	123.45.6.0/24	разрешение
B	135.79.6.0/24	123.45.0.0/16	отказ
C	0.0.0.0/0	0.0.0.0/0	отказ

Примеры пакетов

Пакет	Адрес источника	Адрес назначения	Требуемое действие	Действие ABC	Действие BAC
1	135.79.6.1	123.45.1.1	отказ	Отказ (B)	Отказ (B)
2	135.79.6.1	123.45.6.1	разрешение	разр.(A)	Отказ (B)
3	135.79.1.1	123.45.6.1	разрешение	разр.(A)	разр.(A)
4	135.79.1.1	123.45.1.1	отказ	Отказ (C)	Отказ (C)

Пример при удалении правила B

Пакет	Адрес источника	Адрес назначения	Требуемое действие	Действие АС
1	135.79.6.1	123.45.1.1	отказ	Отказ (С)
2	135.79.6.1	123.45.6.1	разрешение	Разрешение (А)
3	135.79.1.1	123.45.6.1	разрешение	Разрешение (А)
4	135.79.1.1	123.45.1.1	отказ	Отказ (С)

Задача 3

- Защищаемая организация имеет сеть 123.4.0.0/16
- Входящие соединения TELNET разрешаются только с хостом 123.4.5.6
- Входящие соединения SMTP разрешаются только с хостами 123.4.5.7 и 123.4.5.8
- Входящий обмен по NNTP разрешается только от сервера новостей 129.6.48.254 и только с хостом 123.4.5.9
- Входящий протокол NTP (сетевого времени) - разрешается для всех

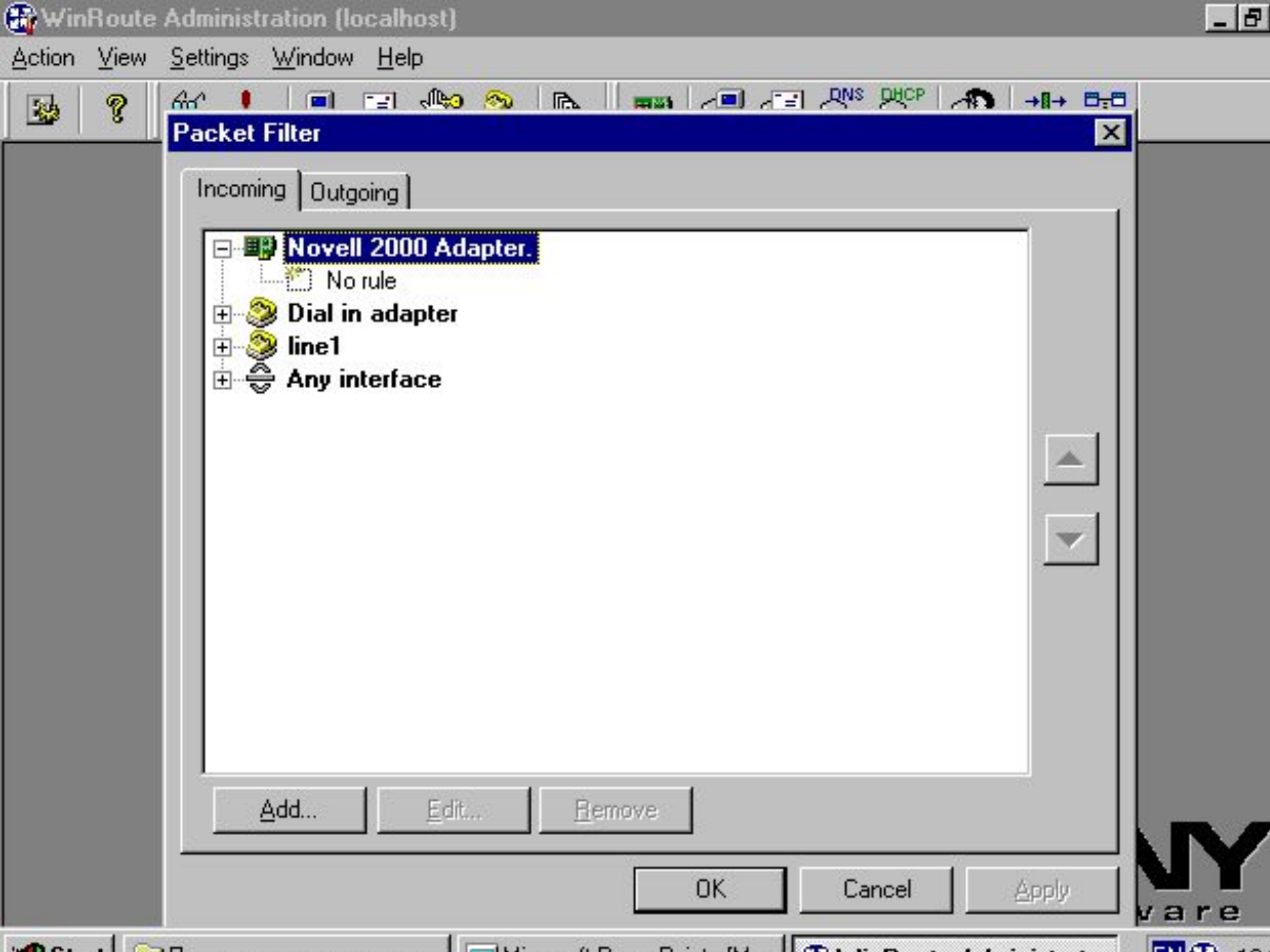
Правила фильтрации

Правило	Направление	Тип	Адрес источника	Порт источника	Адрес получателя	Порт получателя	Действие
A	вход	TCP	любой	>=1024	123.4.5.6	23	разреш.
B	вход	TCP	любой	>=1024	123.4.5.7	25	разреш.
C	вход	TCP	любой	>=1024	123.4.5.8	25	разреш.
D	вход	TCP	129.6.48.254	>=1024	123.4.5.9	119	разреш.
E	вход	UDP	любой	>=1024	123.4.0.0/16	123	разреш.
F	вход	любой	любой	любой	любой	любой	отказ

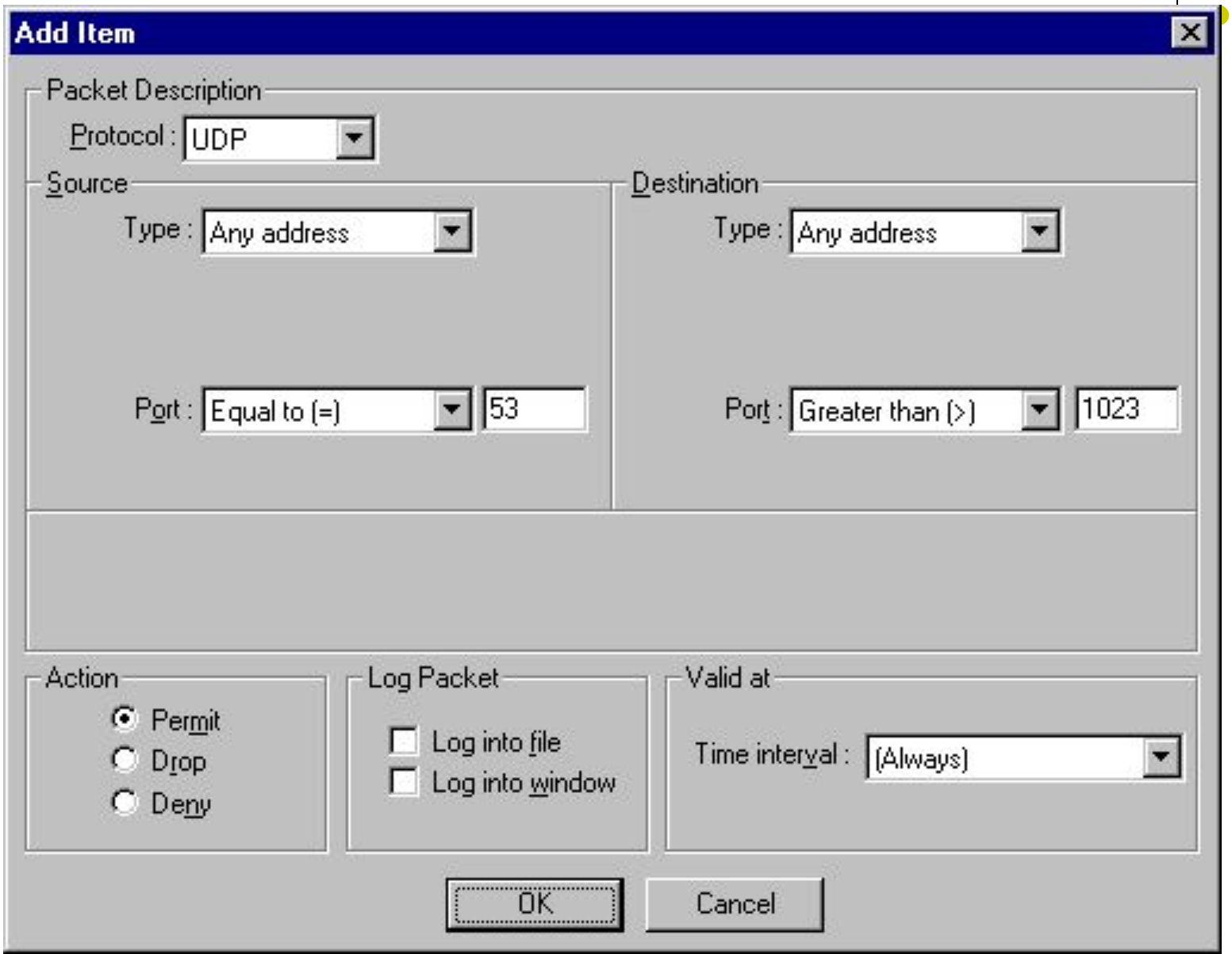
Установка TCP соединения (3-way handshake)

Пример настройки правил фильтрации входящих пакетов

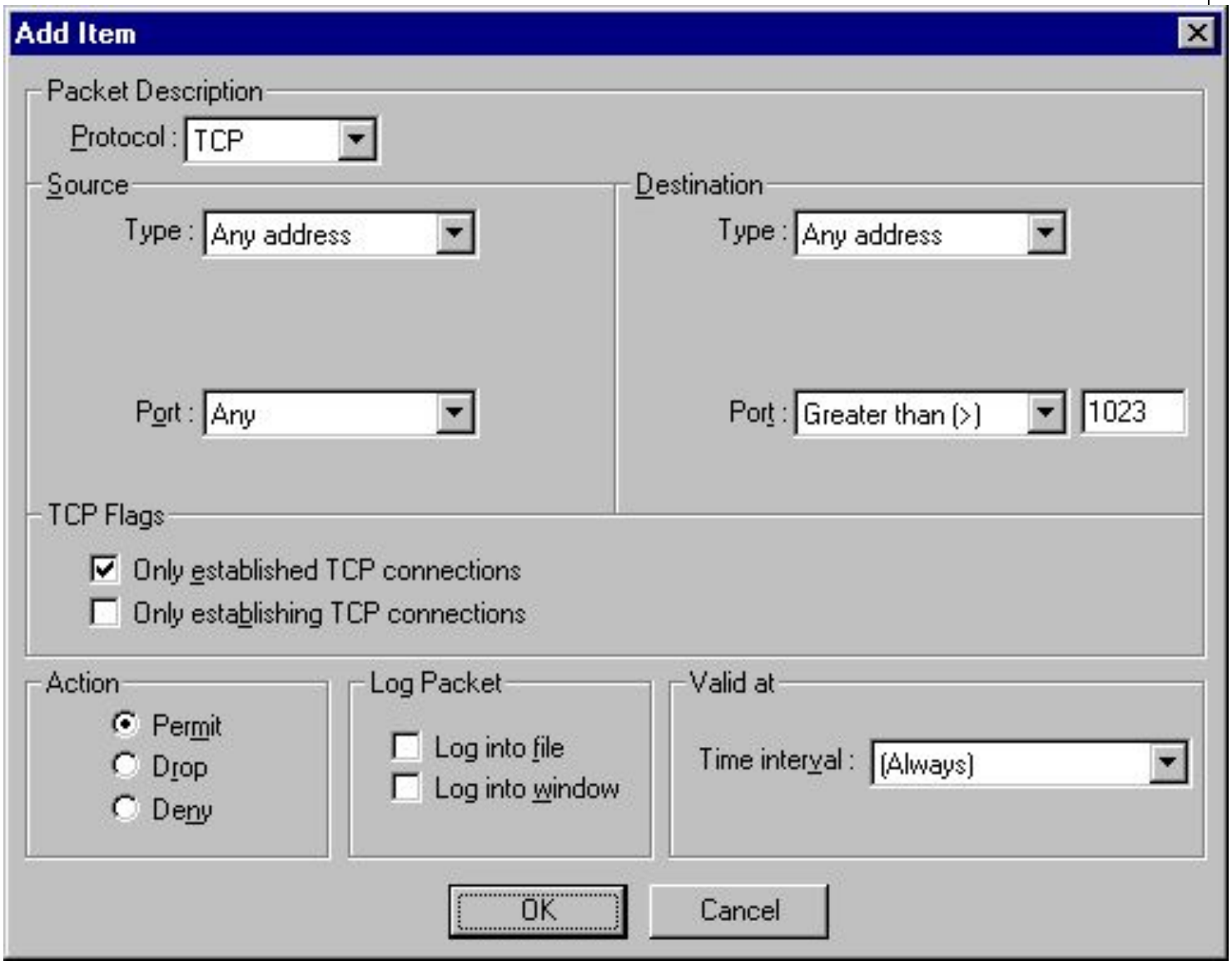
Протокол	Отправитель	Адресат	Типы ICMP	Действие	Запись	Описание
UDP	Любой адрес, порт = 53	Любой адрес, порт > 1023		Разрешить		Разрешение определять DNS внешними средствами
TCP	Любой адрес, любые порты	Любой адрес, порт > 1023		Разрешить только установленные TCP соединения		Разрешение на возврат всего TCP-трафика, инициированного локальным узлом
ICMP	Любой адрес	Любой адрес	Эхо-ответ	Разрешить		Разрешение на эхо-тестирование внешних узлов с запретом на эхо-тестирование Ваших узлов
IP	Любой адрес	Любой адрес		Игнорировать	В окне	Правило подстраховки, блокирующее весь трафик, не отвечающий условиям установленных выше правил.


WinRoute Administration (localhost)
Action View Settings Window Help
DNS DHCP
Packet Filter
Incoming Outgoing
Novell 2000 Adapter.
No rule
Dial in adapter
line1
Any interface
Add... Edit... Remove
OK Cancel Apply

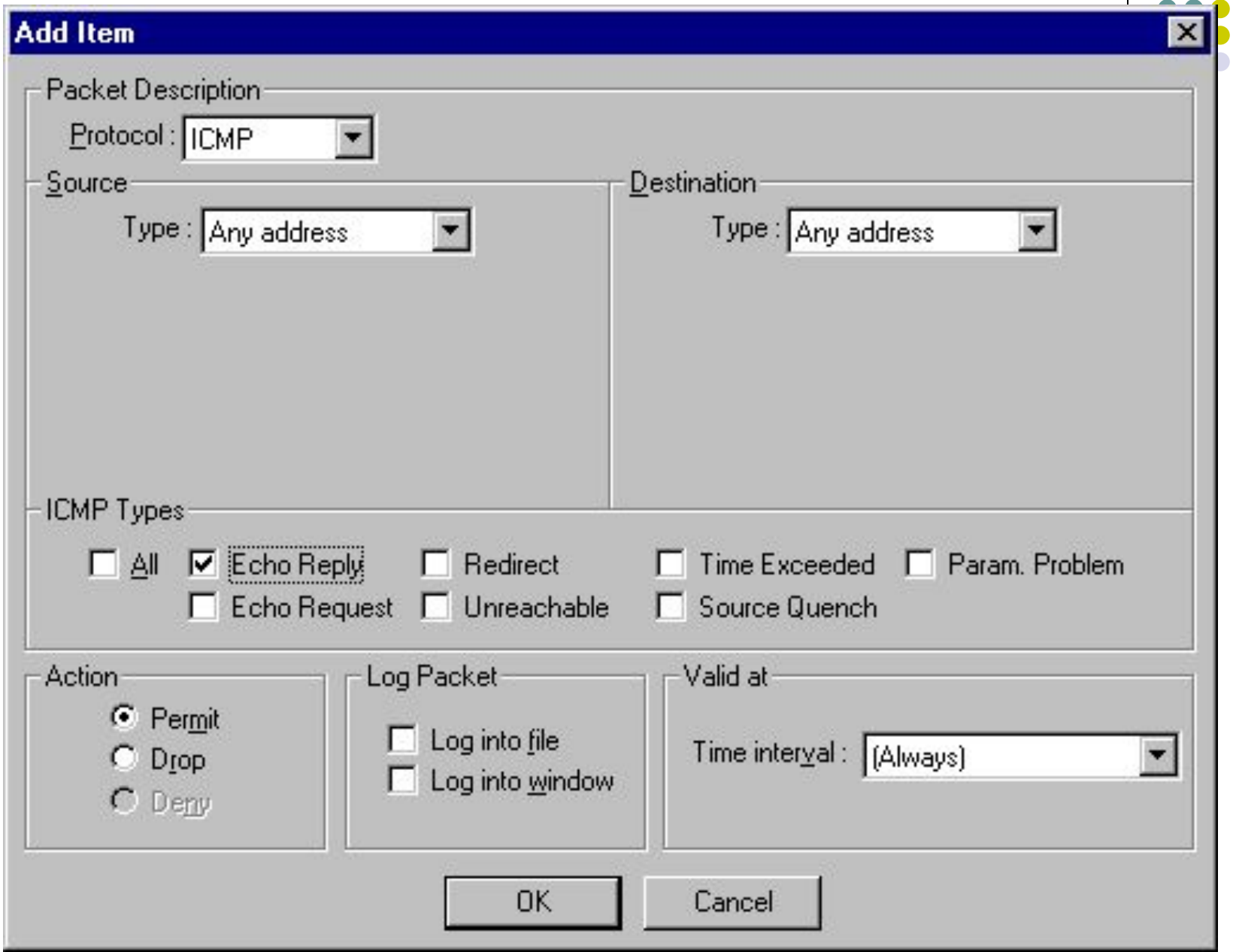
Протокол	Отправитель	Адресат	Типы ICMP	Действие	Запись
UDP	Любой адрес, порт = 53	Любой адрес, порт > 1023		Разрешить	



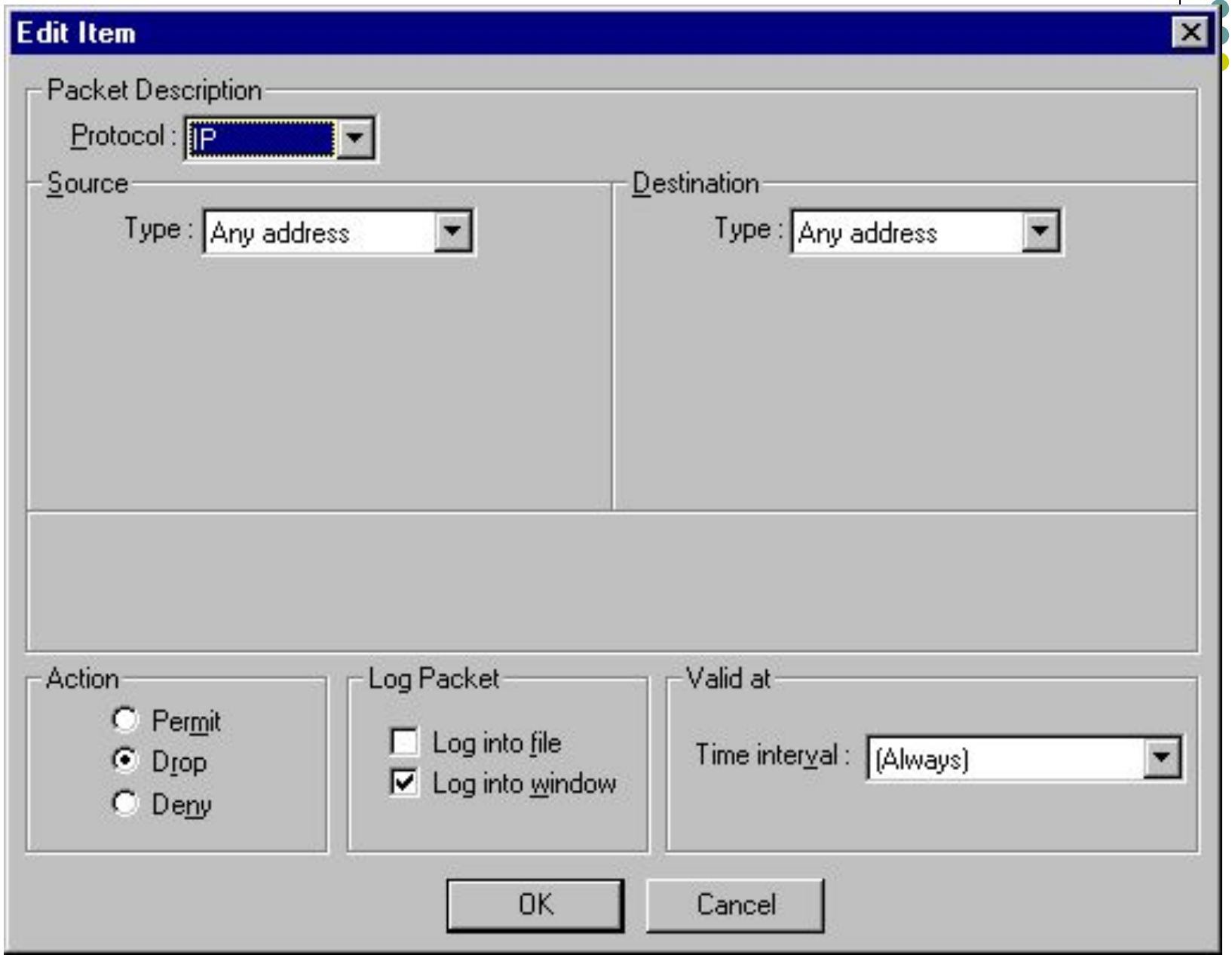
Протокол	Отправитель	Адресат	Действие	Запись
TCP	Любой адрес, любые порты	Любой адрес, порт > 1023	Разрешить только установленные TCP соединения	

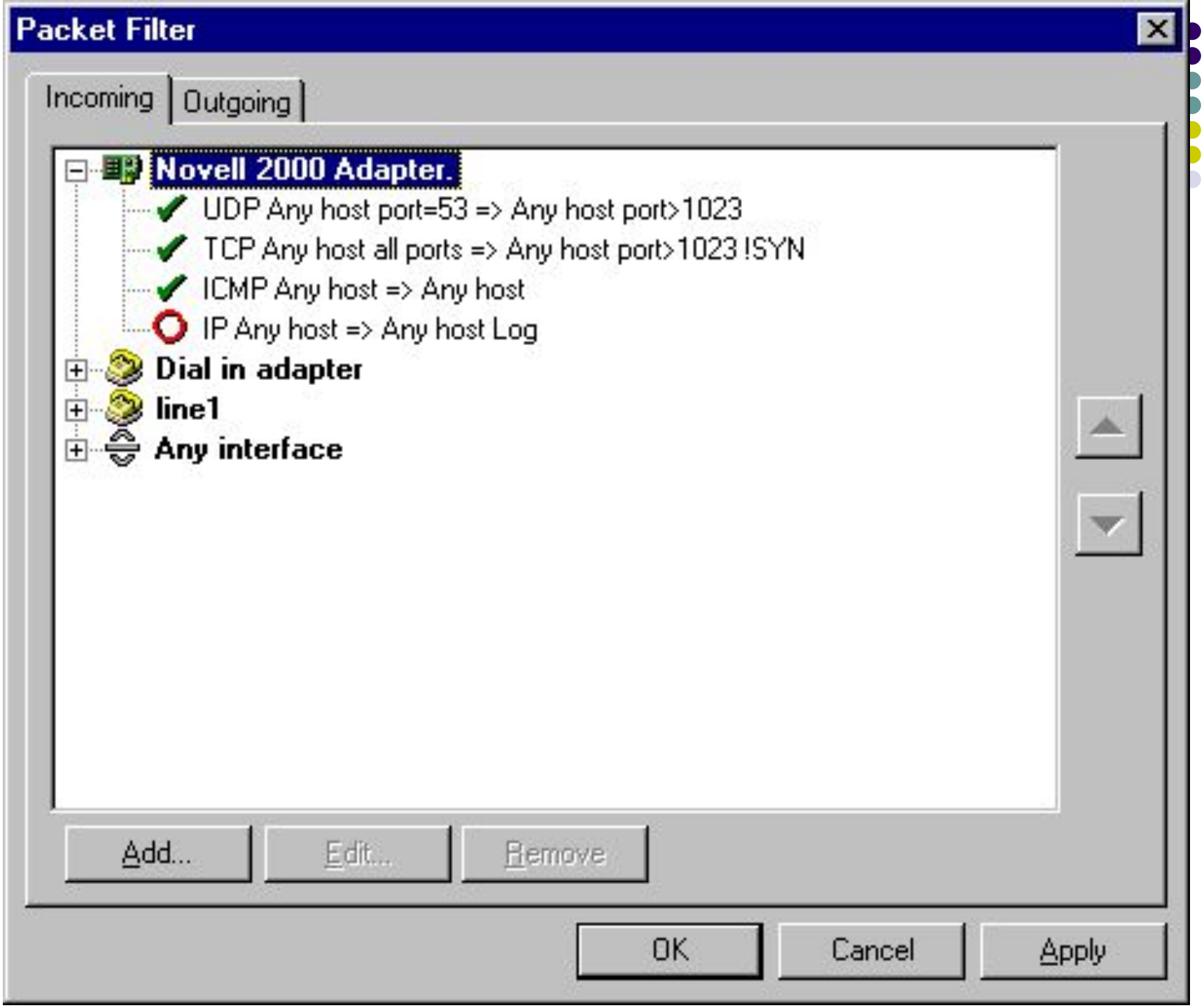


Протокол	Отправитель	Адресат	Типы ICMP	Действие	Запись
ICMP	Любой адрес	Любой адрес	Эхо-ответ	Разрешить	



Протокол	Отправитель	Адресат	Типы ICMP	Действие	Запись
IP	Любой адрес	Любой адрес		Игнорировать	В окне




Packet Filter
Incoming
Outgoing
Novell 2000 Adapter.
UDP Any host port=53 => Any host port>1023
TCP Any host all ports => Any host port>1023 !SYN
ICMP Any host => Any host
IP Any host => Any host Log
Dial in adapter
line1
Any interface
Add...
Edit...
Remove
OK
Cancel
Apply

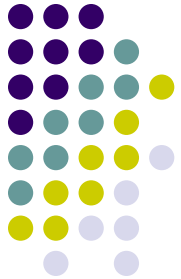
Пример настройки правил фильтрации исходящих пакетов

Протокол	Отправитель	Адресат	Типы ICMP	Действие	Запись	Описание
UDP	Любой адрес, порт > 1023	Любой адрес, порт = 53		Разрешить		Разрешение определять DNS внешними средствами
TCP	Любой адрес, порт > 1023	Любой адрес, любые порты		Разрешить только установку TCP соединения		Разрешение инициализацию TCP-трафика
ICMP	Любой адрес	Любой адрес	Эхо-запрос	Разрешить		Разрешение на эхо-тестирование внешних узлов с запретом на эхо-тестирование Ваших узлов
IP	Любой адрес	Любой адрес		Игнорировать	В окне	Правило подстраховки, блокирующее весь трафик, не отвечающий условиям установленных выше правил.

Фильтрующие маршрутизаторы

- невысокая стоимость
- гибкость в определении правил фильтрации
- небольшая задержка при прохождении пакетов
- внутренняя сеть видна (маршрутизируется)
- правила фильтрации трудны в описании и требуют хороших знаний технологии TCP и UDP
- невозможность полного тестирования правил фильтрации, нет защиты от непротестированных атак
- при выключении МЭ все компьютеры становятся незащищенными либо недоступными
- возможна подмена IP-адреса атакующего
- отсутствует аутентификация на пользовательском уровне

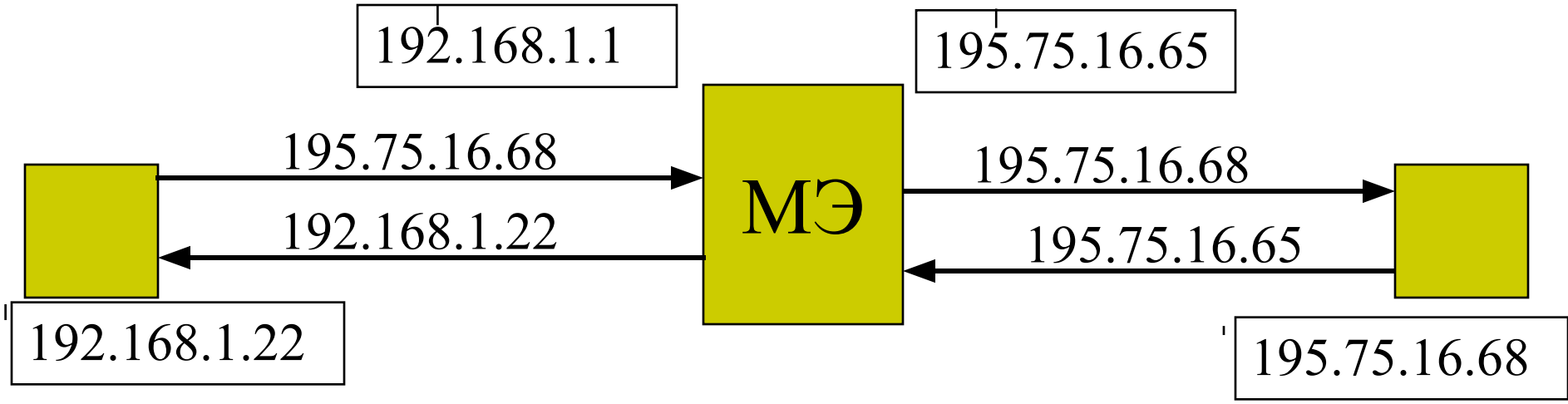
Дополнительные возможности фильтрующих маршрутизаторов



- NAT - для подключения локальной сети с частными адресами к Интернет при использовании одного IP-адреса
- Port Mapping - возможность переадресации сетевых служб на внутренние адреса несмотря на использование NAT

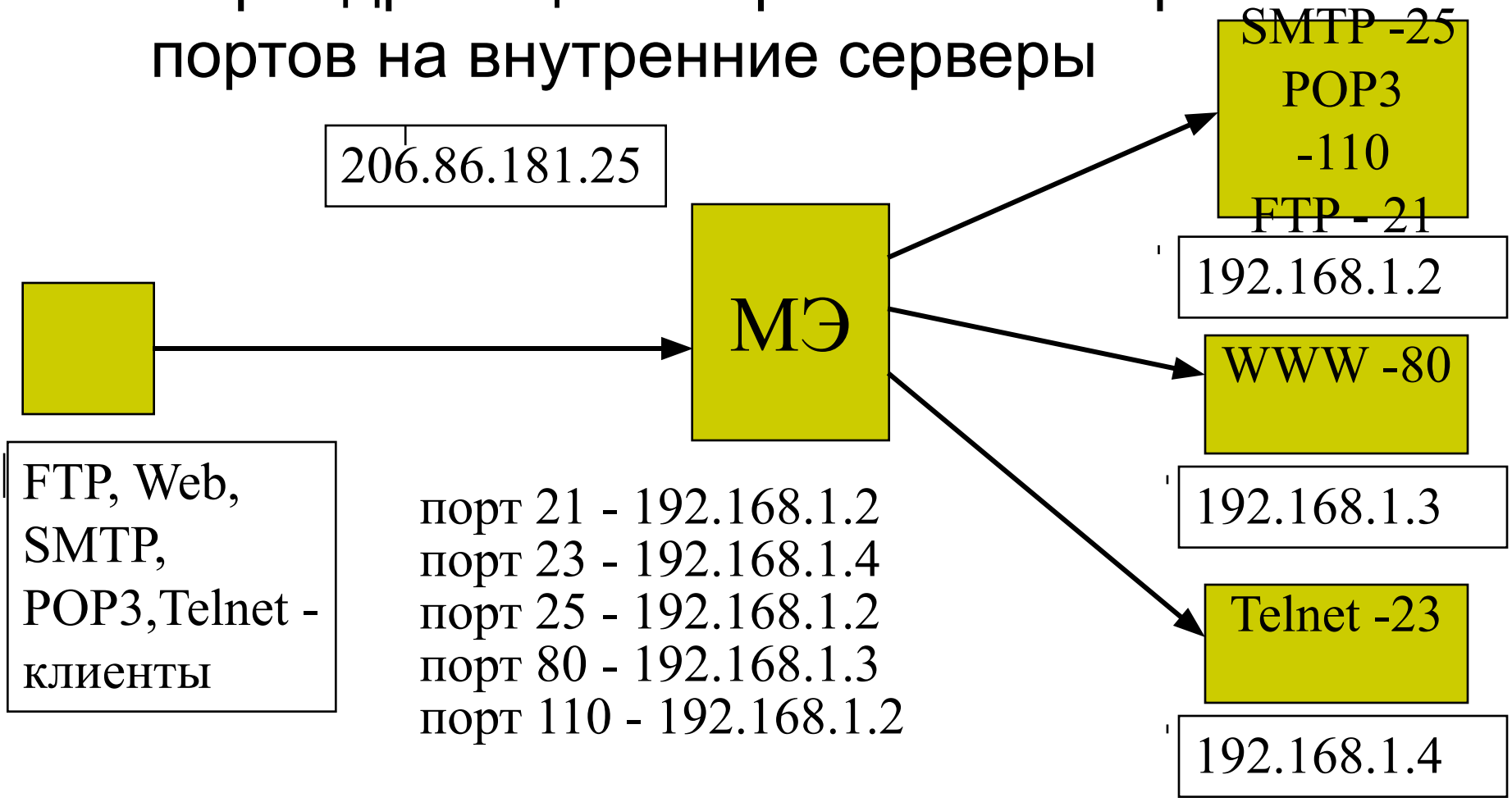
NAT

- замена IP-адресов внутренней сети на адрес внешнего интерфейса

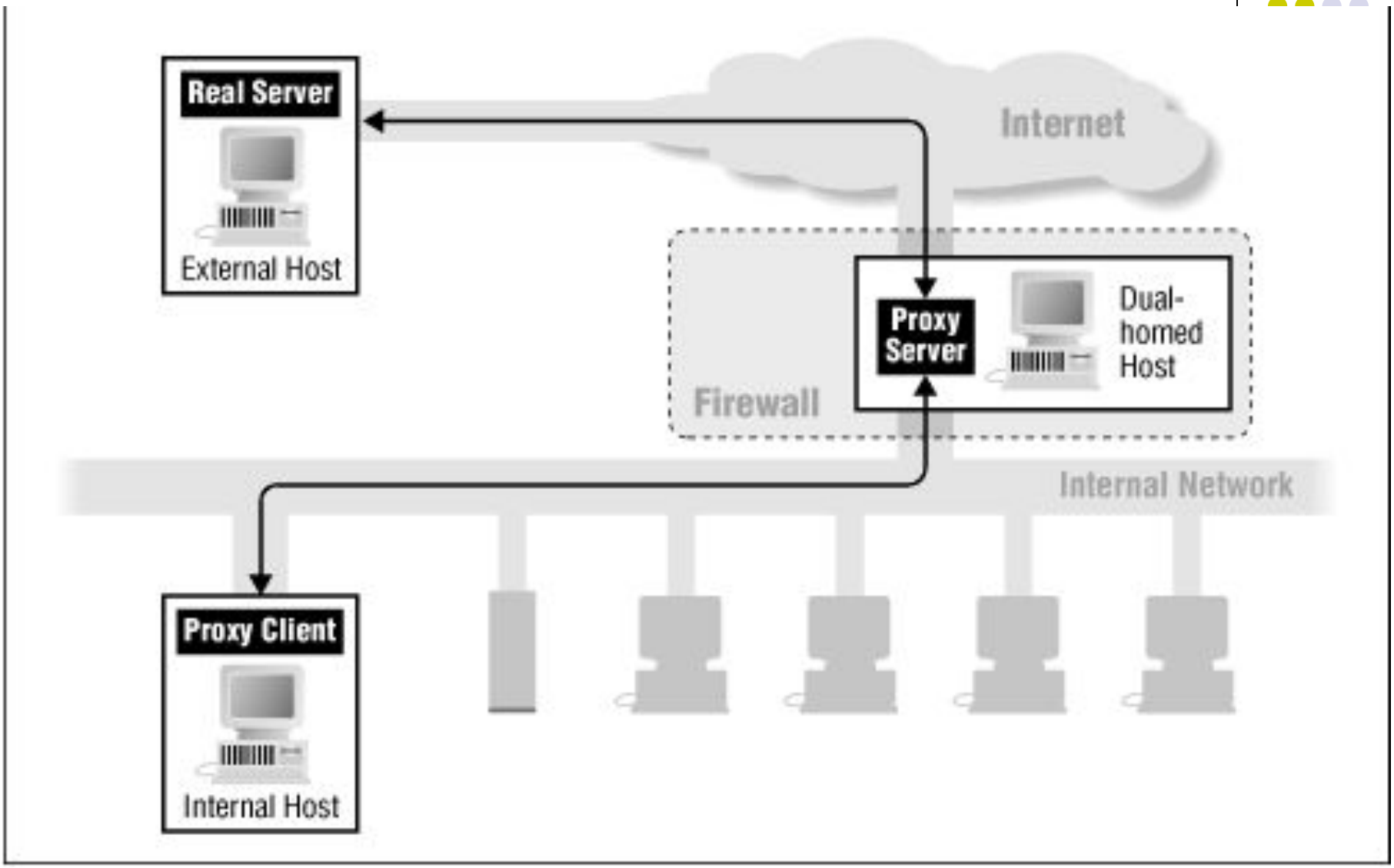


Port Mapping

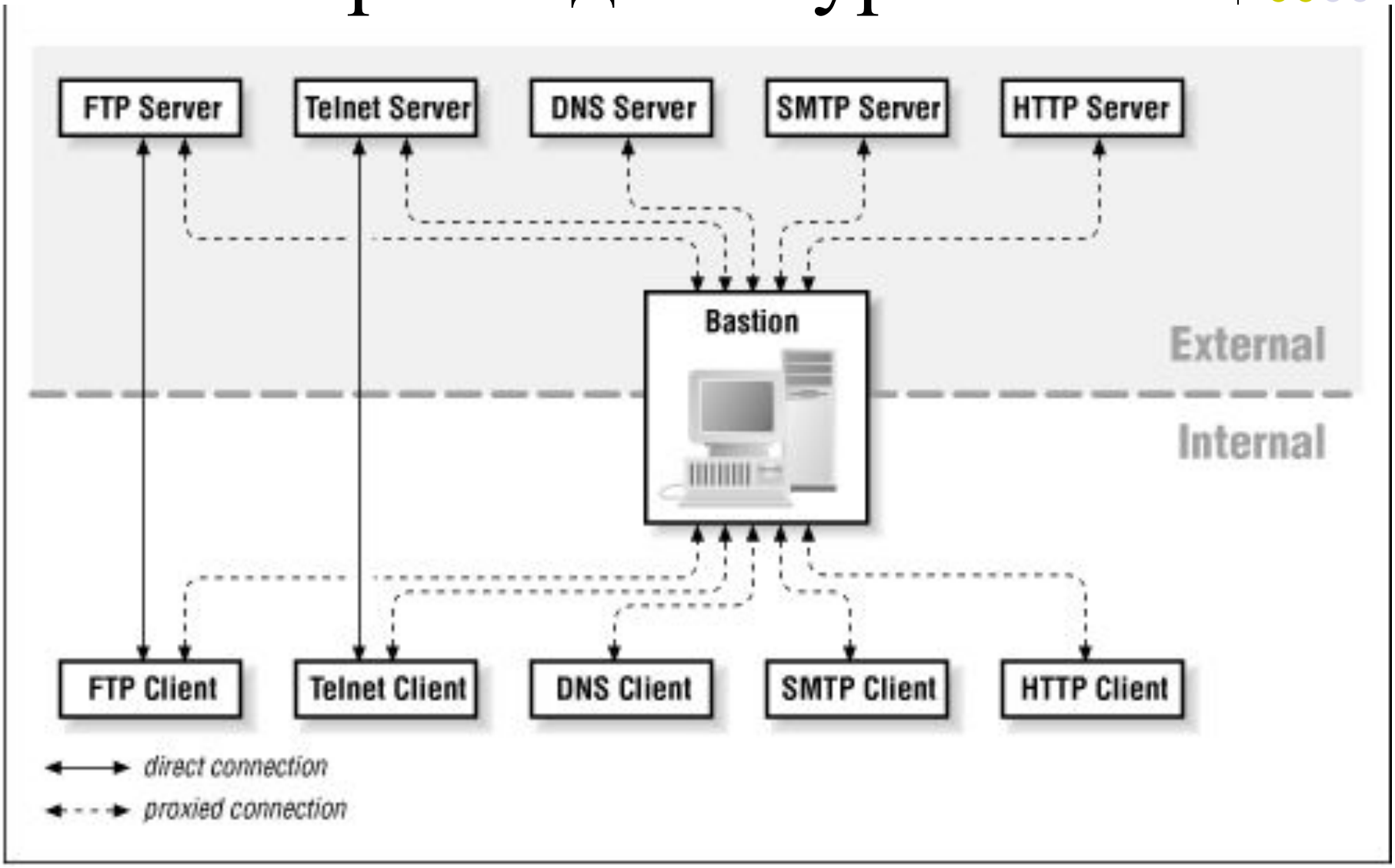
- Переадресация запросов некоторых портов на внутренние серверы



Шлюз прикладного уровня



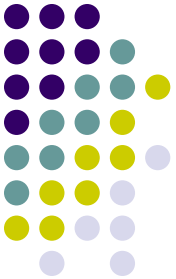
Реализация шлюза прикладного уровня



Укрепленный компьютер

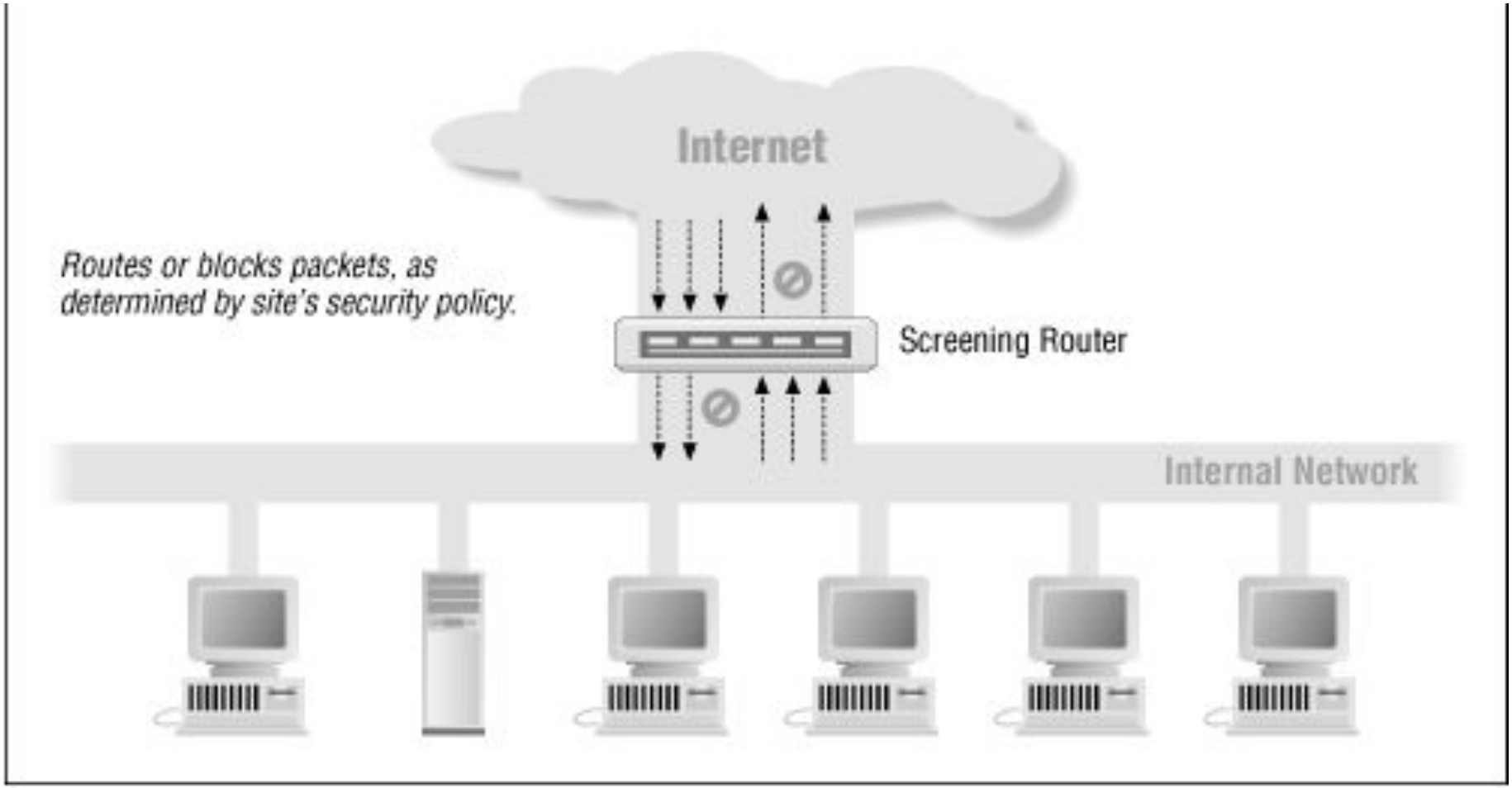
- установка защищенной версии ОС
- удаление ненужных сетевых служб
- удаление ненужных приложений
- защита ресурсов и контроль доступа
- настройка регистрации и аудита

Основные схемы сетевой защиты на базе МЭ

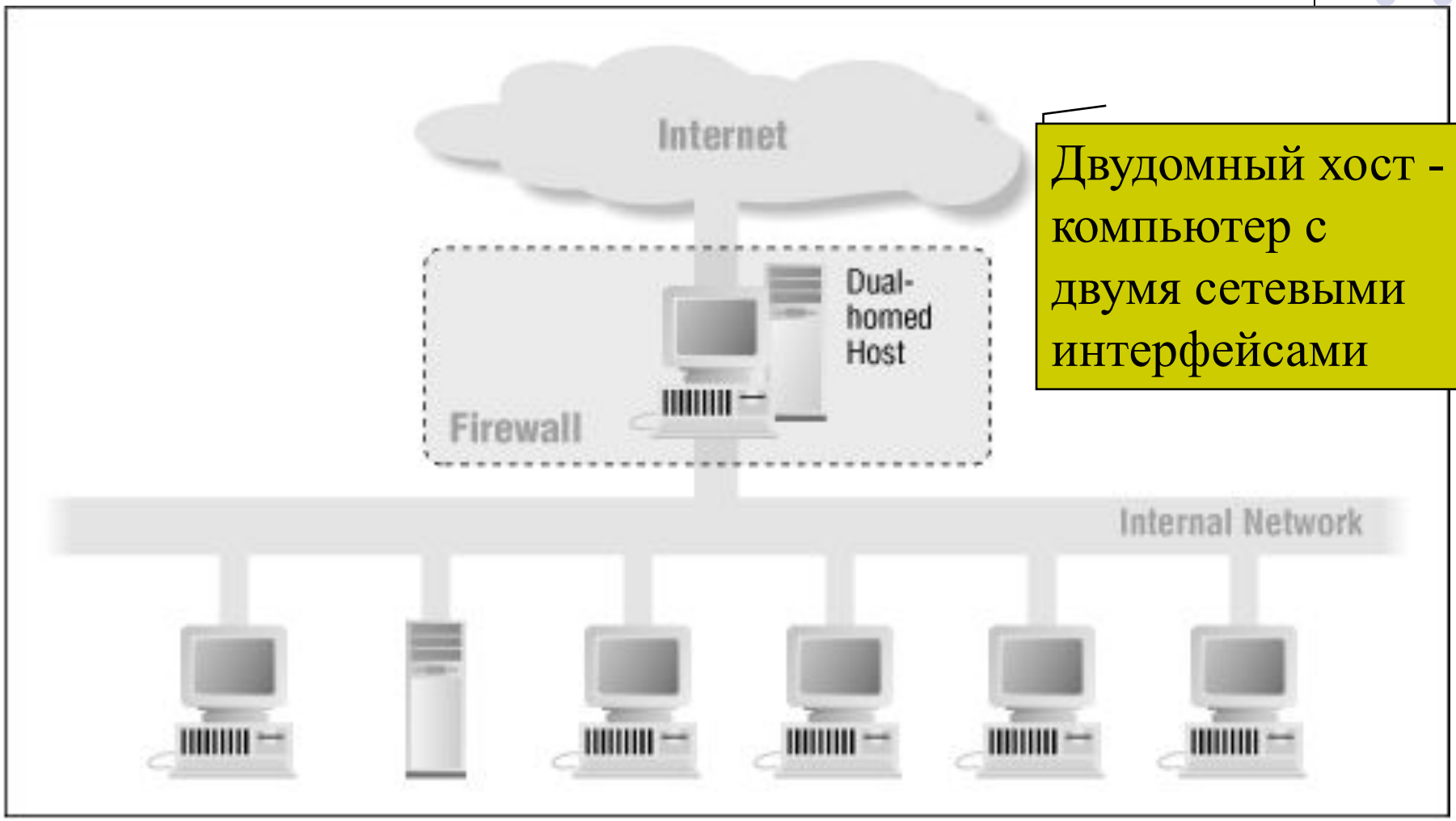


- МЭ - фильтрующий маршрутизатор
- МЭ на основе двупортового шлюза
- МЭ на основе экранированного шлюза
- МЭ - экранированная подсеть

МЭ -фильтрующий маршрутизатор

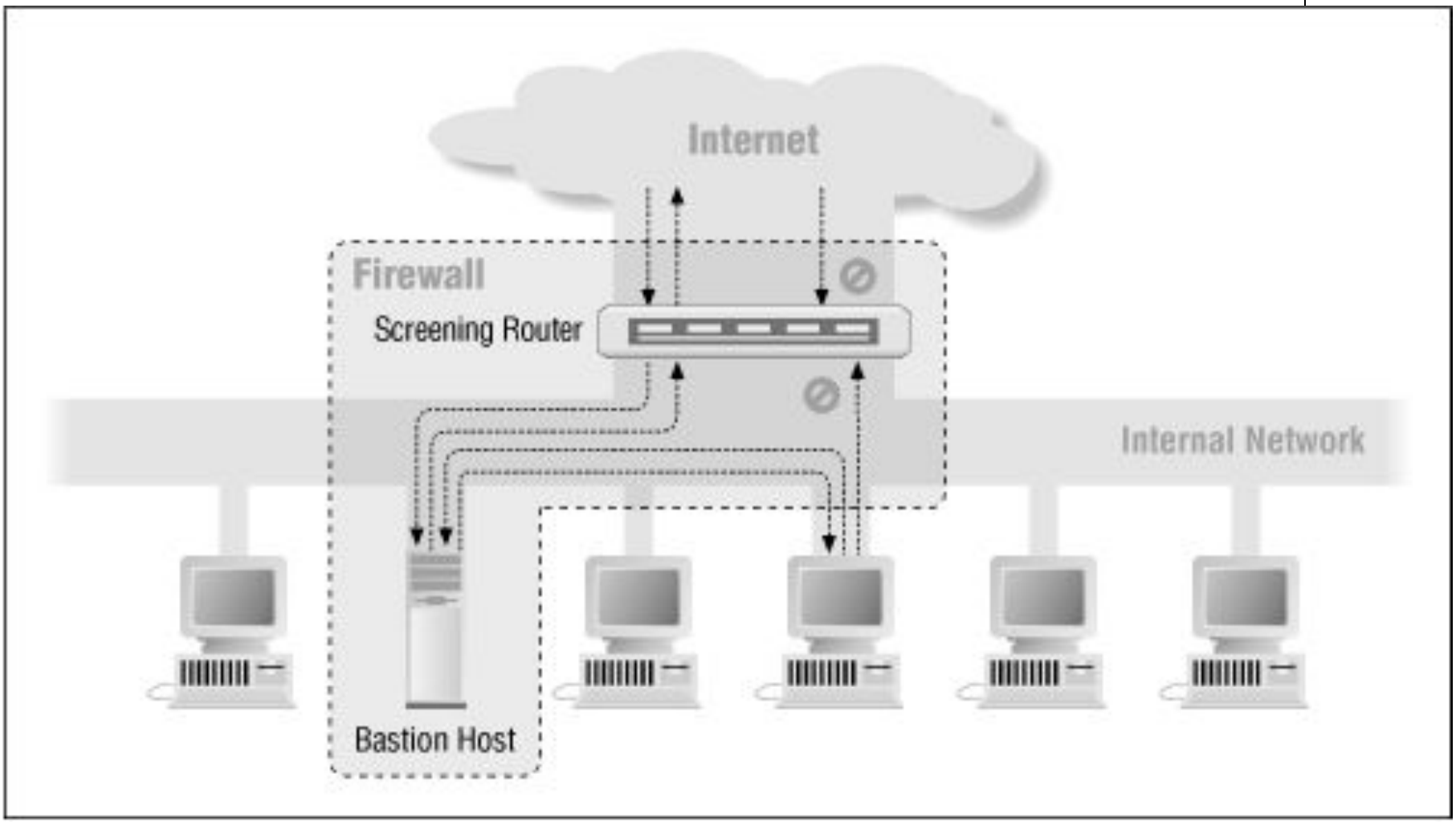


Двупортовый шлюз

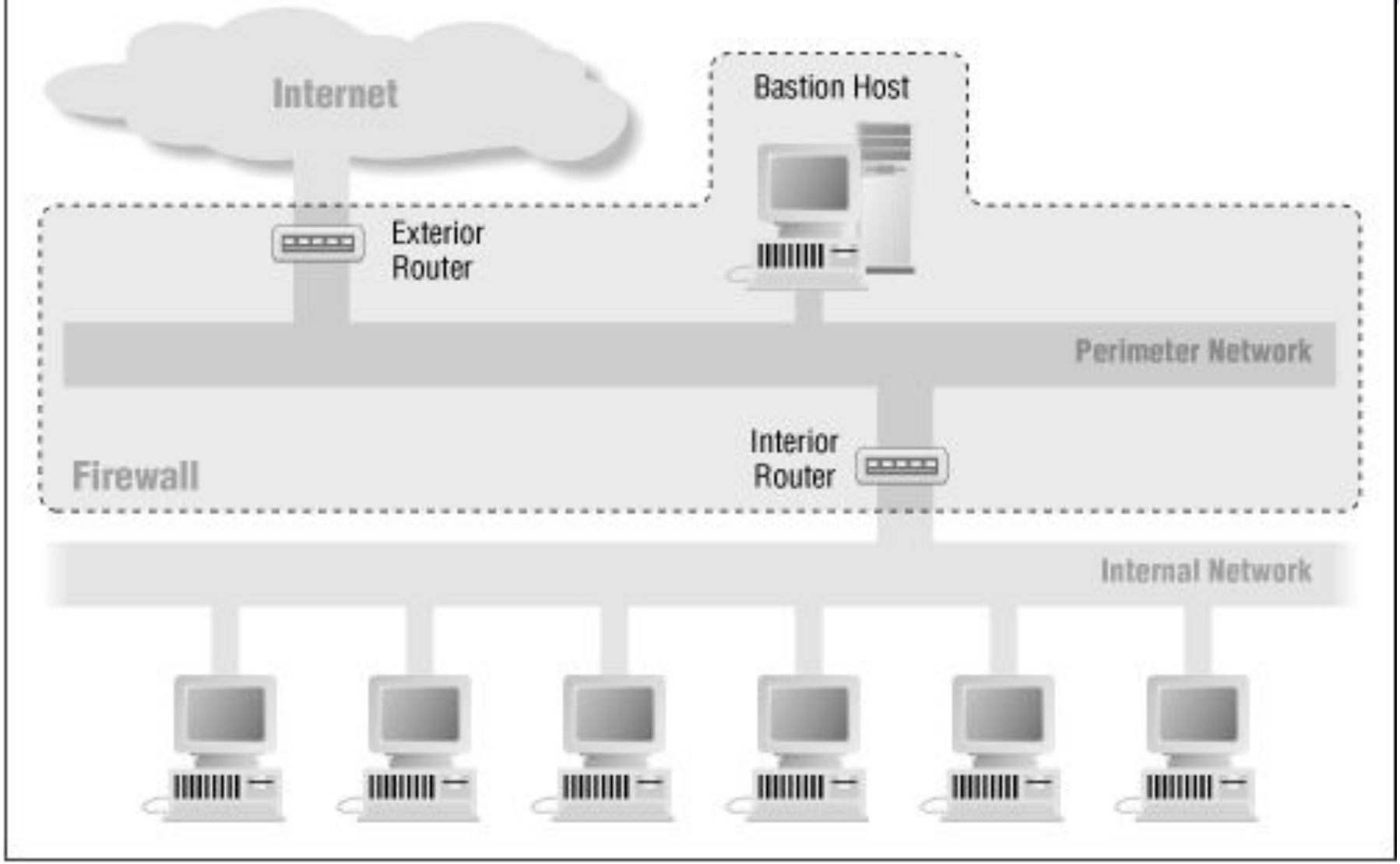


Двудомный хост - компьютер с двумя сетевыми интерфейсами

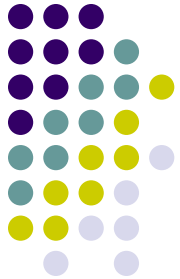
Экранированный шлюз



Экранированная подсеть



Политика сетевой безопасности



- Доступ из Интернет в корпоративную сеть:
- во внутреннюю приватную сеть доступ извне запрещен
- к МЭ извне доступ запрещен
- В ДМЗ доступ разрешен ТОЛЬКО к следующим портам на объектах (в остальных случаях доступ запрещен):
  - Web-сервер.
    - анонимный доступ всем разрешен только к 80 порту.
    - разрешен авторизованный FTP-доступ на 21 порт и 20 порт (возможно с предварительной идентификацией / аутентификацией на МЭ) администратору Web-сервера только из сегмента административного управления (с приватного IP-адреса администратора).
    - из приватной сети, только из сегмента административного управления (с IP-адреса администратора) возможен удаленный терминальный доступ по протоколу rsh на Web-сервер
  - Mail-сервер (SMTP и POP3)
    - разрешен доступ только из приватной корпоративной сети к сервису POP3 - 110 порт
    - разрешен доступ к SMTP сервису - 25 порт только из приватной сети
- Доступ из корпоративной сети в Интернет разрешен без ограничений

Виртуальные частные сети

Virtual Private Network (VPN) – это технология, объединяющая доверенные сети, узлы и пользователей через открытые сети, к которым нет доверия

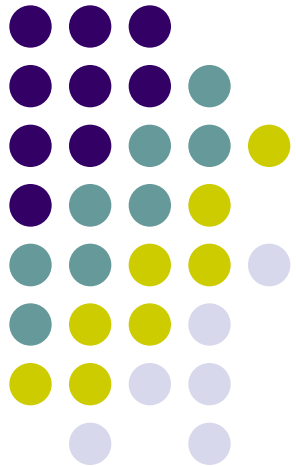
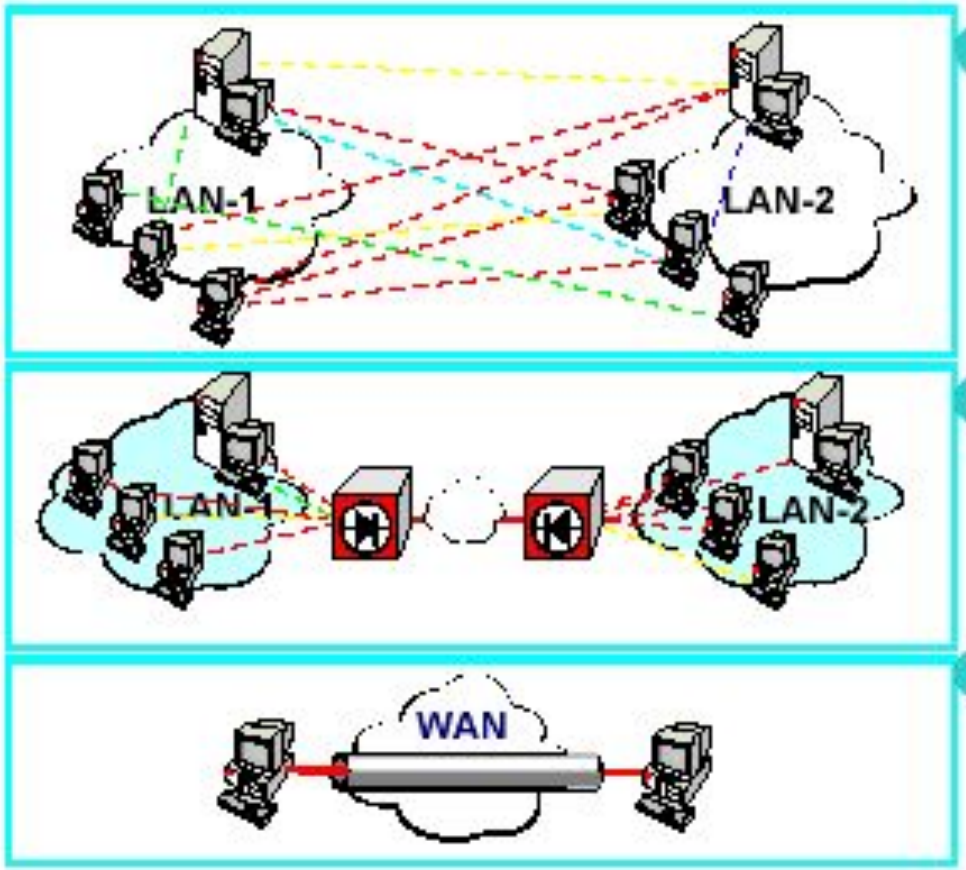
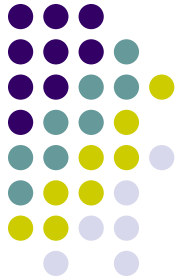


Схема VPN



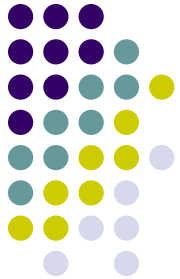
1. реально установленные соединения
2. организация защиты
3. ситуация для внешнего наблюдателя

Задачи, решаемые VPN



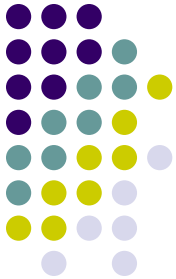
- Защита (конфиденциальность, целостность, подлинность) передаваемой по сетям информации
- Защита внутренних сегментов сети от НСД извне
- Идентификация и аутентификация пользователей

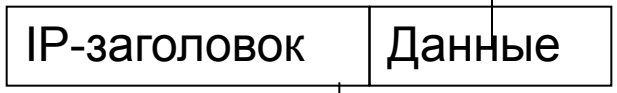
Требования к VPN



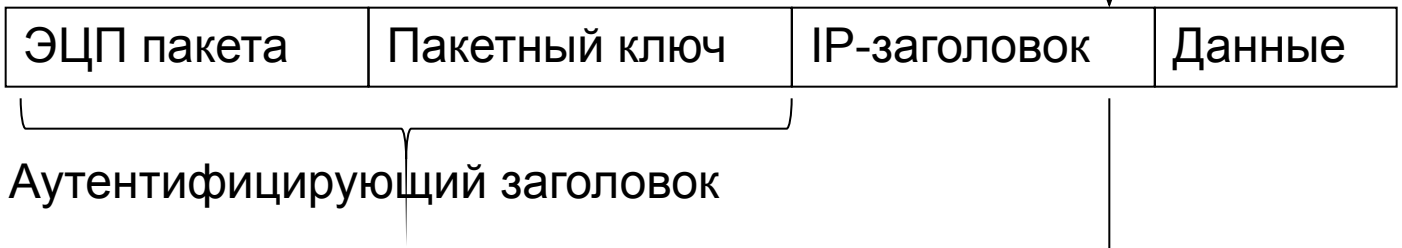
- Масштабируемость
- Интегрируемость
- Легальность используемых алгоритмов
- Пропускная способность сети
- Стойкость криптоалгоритмов
- Унифицируемость
- Общая совокупная стоимость

Туннелирование в VPN



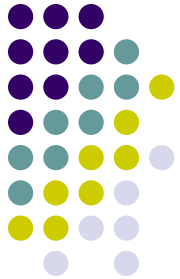


Шифруются на пакетном ключе и подписываются ЭЦП



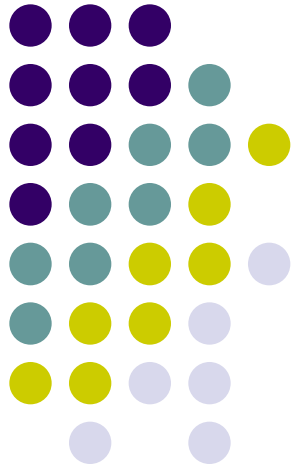
Пакетный ключ шифруется на ключе связи, формируется новый IP-пакет (IP-адреса устройств защиты)

Уровни защищенных каналов

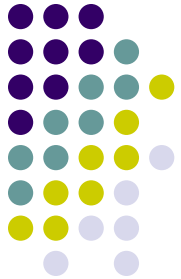


Прикладной	S/MIME /PGP /SHTTP
Транспортный (TCP/UDP)	SSL /TLS / SOCKS
Сетевой (IP)	IPSec / SKIP
Канальный	PPTP / L2F /L2TP

Защита данных на канальном уровне



Защита данных на канальном уровне



- Прозрачность для приложений и служб прикладного уровня
- Независимость от транспортного и сетевого уровня (IP, IPX, NetBEUI)
- Протоколы
  - PPTP (Point-to-Point Tunneling Protocol)-MS
  - L2F (Layer-2 Forwarding) – Cisco Systems
  - L2TP (Layer-2 Tunneling Protocol) – объединенный

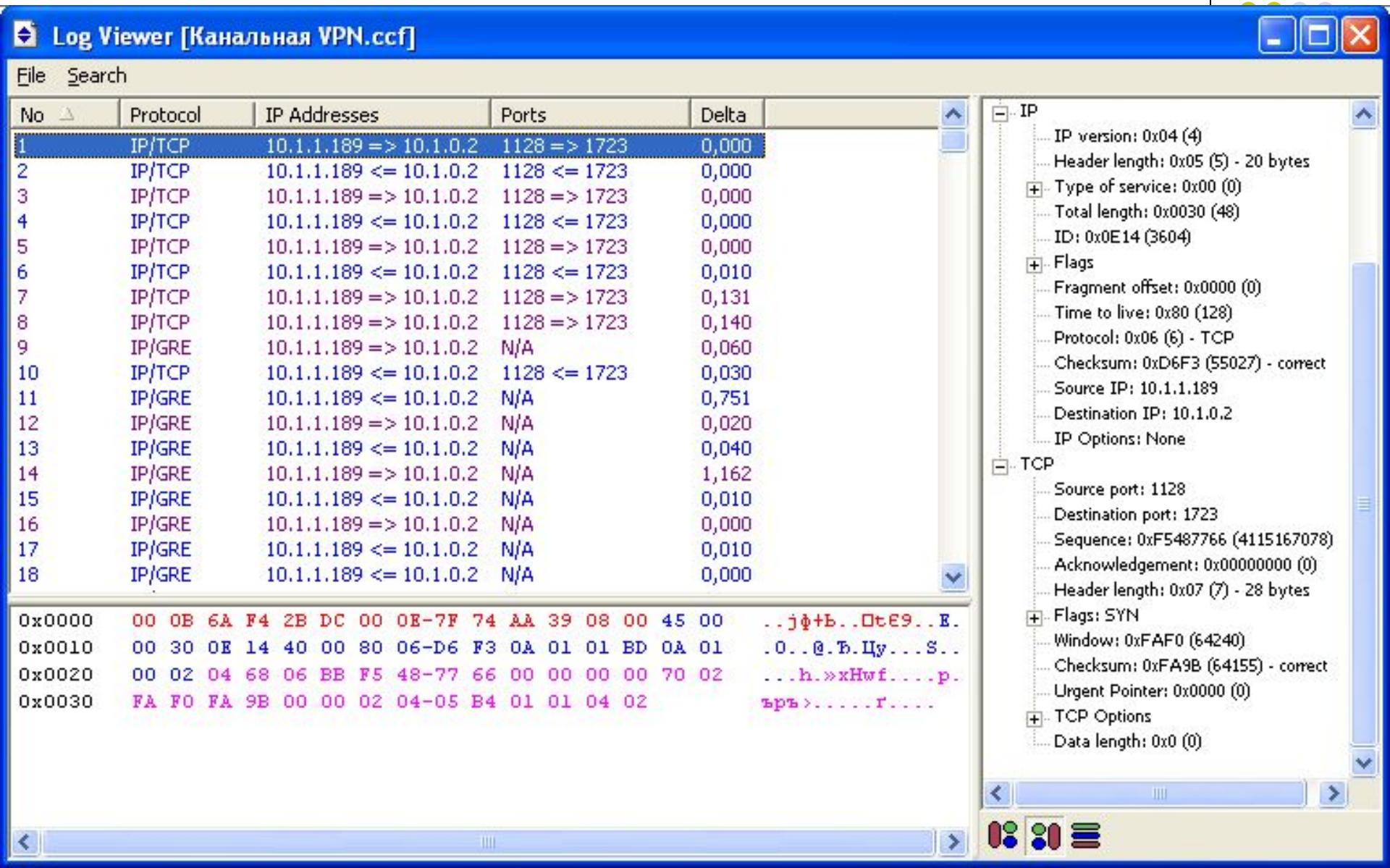
PPTP

- Сначала производится инкапсуляция данных с помощью протокола PPP, затем протокол PPTP выполняет шифрование данных и собственную инкапсуляцию

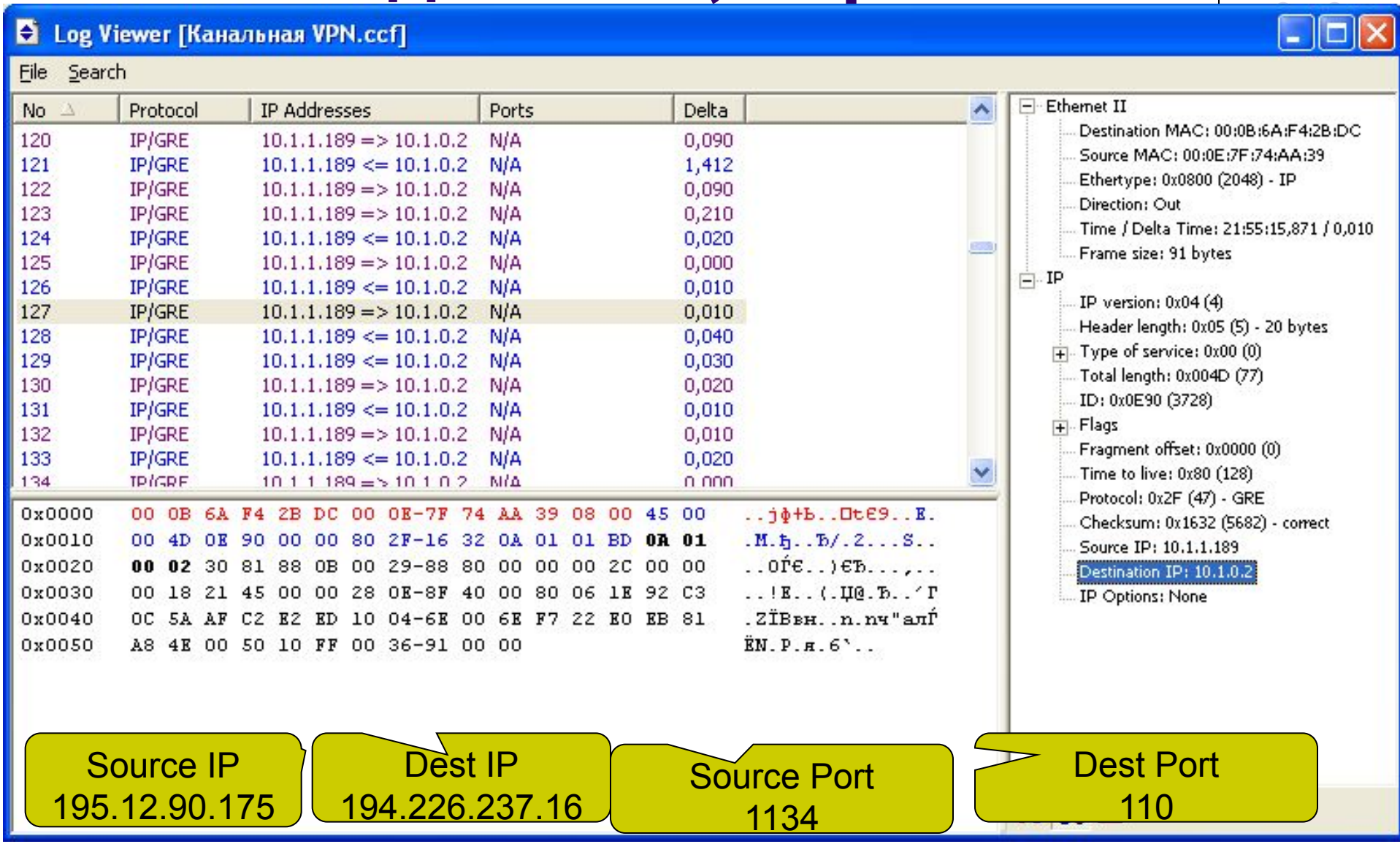
P

IP заголовок	GRE заголовок	PPP заголовок	**IP заголовок**	TCP, UDP	Данные

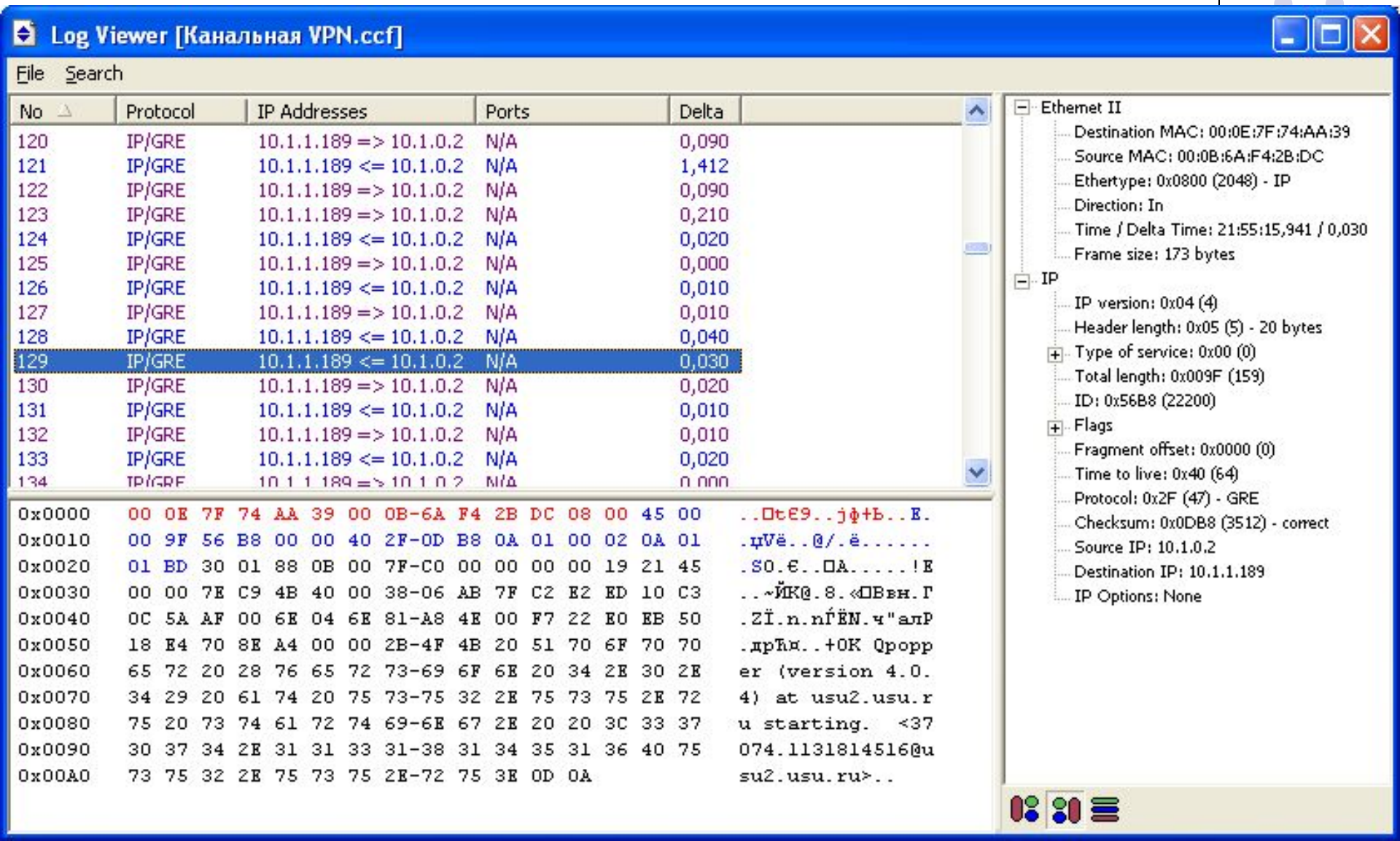
Установка соединения

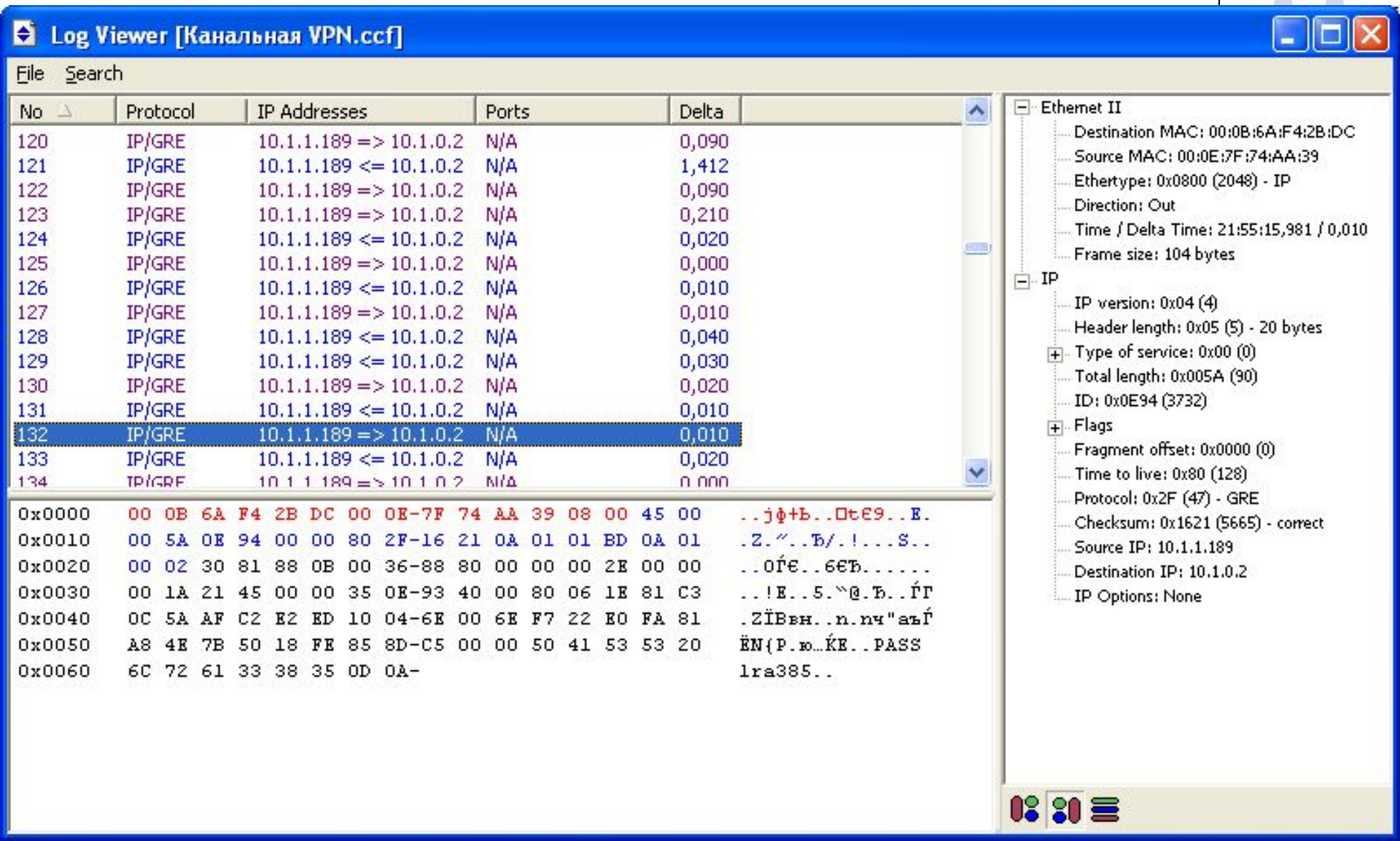


TCP-соединение, порт 110

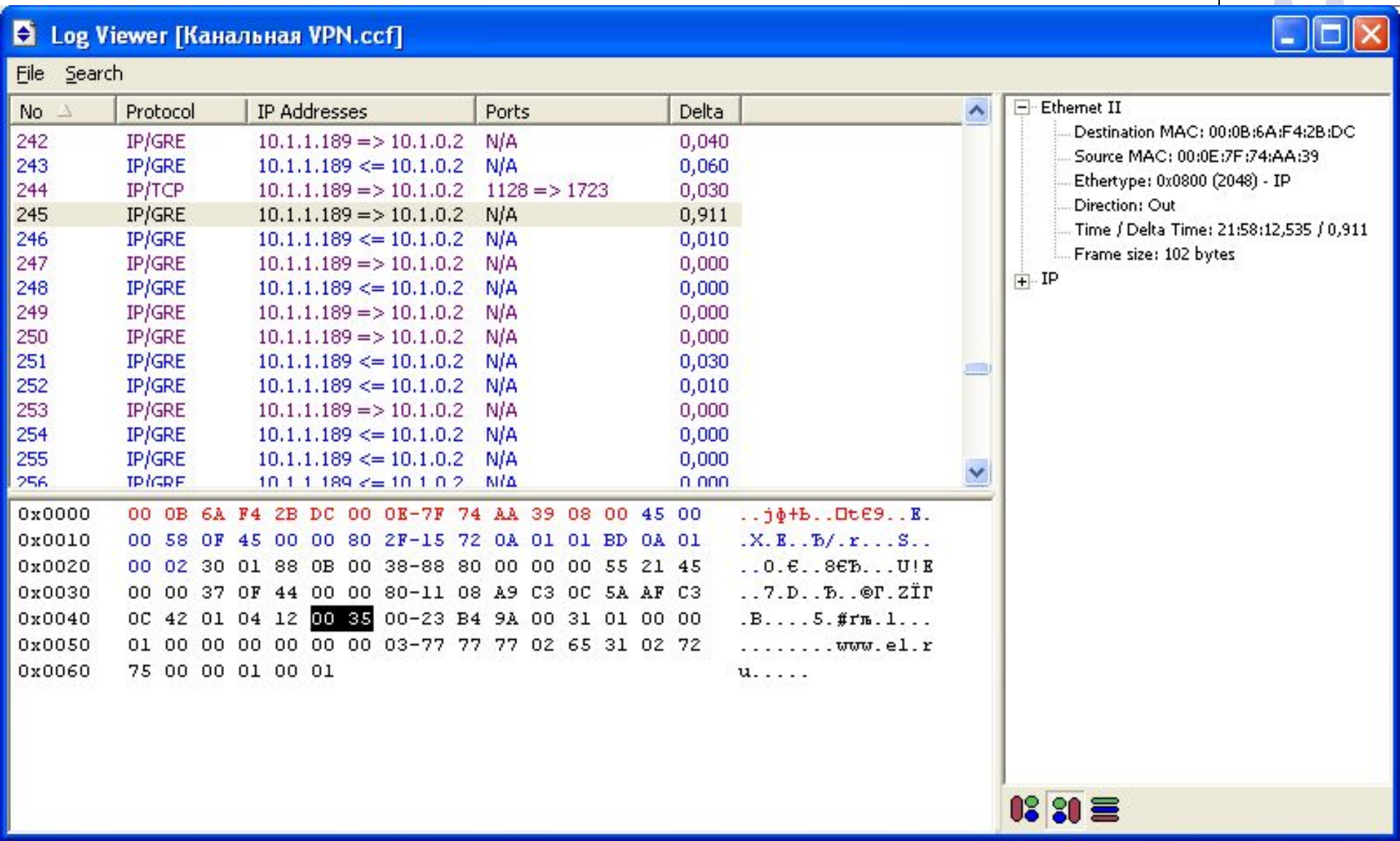


Протокол POP3

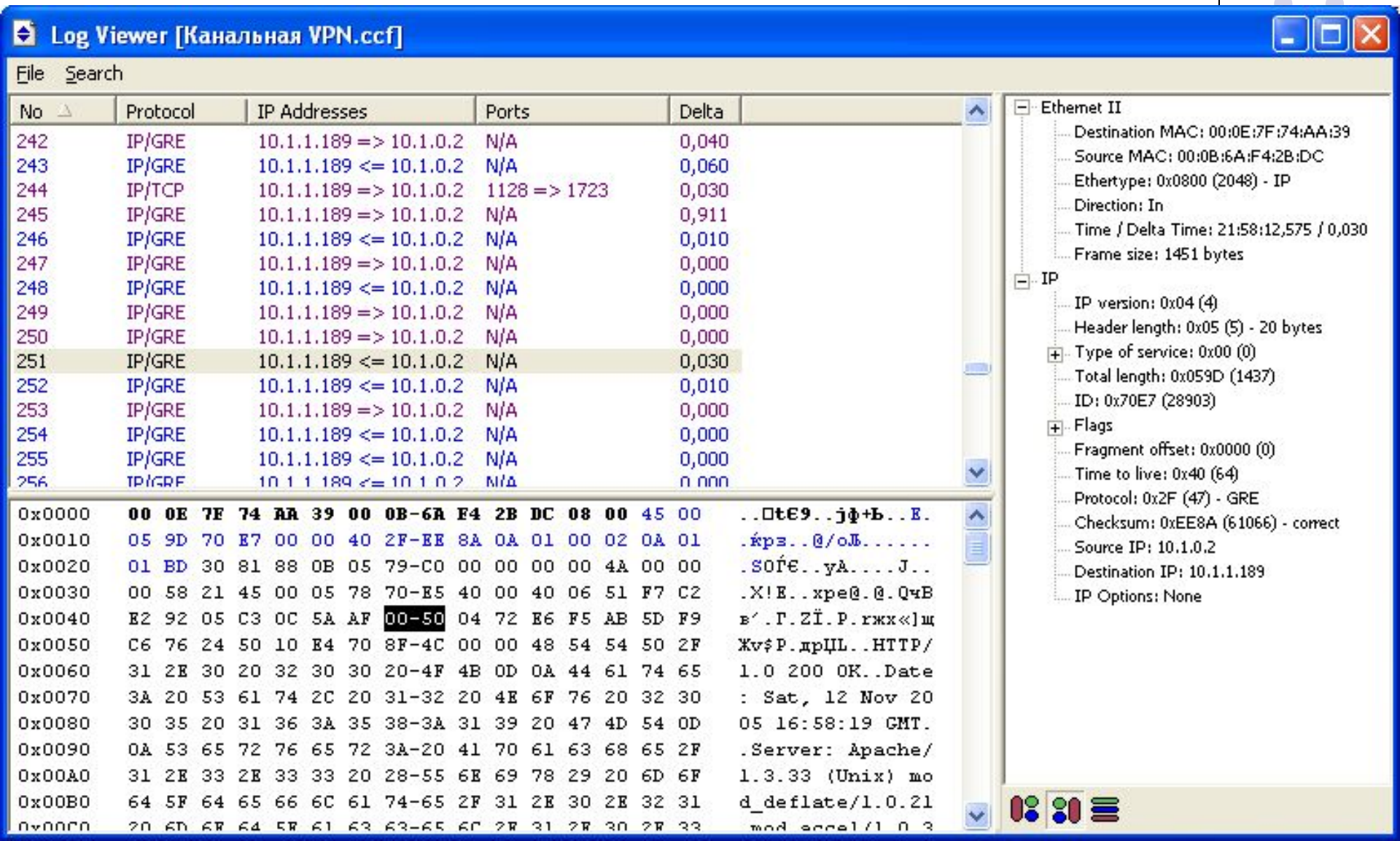



Log Viewer [Канальная VPN.ccf]
File Search
No Protocol IP Addresses Ports Delta
120 IP/GRE 10.1.1.189 => 10.1.0.2 N/A 0,090
121 IP/GRE 10.1.1.189 <= 10.1.0.2 N/A 1,412
122 IP/GRE 10.1.1.189 => 10.1.0.2 N/A 0,090
123 IP/GRE 10.1.1.189 => 10.1.0.2 N/A 0,210
124 IP/GRE 10.1.1.189 <= 10.1.0.2 N/A 0,020
125 IP/GRE 10.1.1.189 => 10.1.0.2 N/A 0,000
126 IP/GRE 10.1.1.189 <= 10.1.0.2 N/A 0,010
127 IP/GRE 10.1.1.189 => 10.1.0.2 N/A 0,010
128 IP/GRE 10.1.1.189 <= 10.1.0.2 N/A 0,040
129 IP/GRE 10.1.1.189 <= 10.1.0.2 N/A 0,030
130 IP/GRE 10.1.1.189 => 10.1.0.2 N/A 0,020
131 IP/GRE 10.1.1.189 <= 10.1.0.2 N/A 0,010
132 IP/GRE 10.1.1.189 => 10.1.0.2 N/A 0,010
133 IP/GRE 10.1.1.189 <= 10.1.0.2 N/A 0,020
0x0000 00 0B 6A F4 2B DC 00 0E-7F 74 AA 39 08 00 45 00
0x0010 00 5A 0E 94 00 00 80 2F-16 21 0A 01 01 BD 0A 01
0x0020 00 02 30 81 88 0B 00 36-88 80 00 00 00 2E 00 00
0x0030 00 1A 21 45 00 00 35 0E-93 40 00 80 06 1E 81 C3
0x0040 0C 5A AF C2 E2 ED 10 04-6E 00 6E F7 22 E0 FA 81
0x0050 A8 4E 7B 50 18 FE 85 8D-C5 00 00 50 41 53 53 20
0x0060 6C 72 61 33 38 35 0D 0A-
Ethernet II
Destination MAC: 00:0B:6A:F4:2B:DC
Source MAC: 00:0E:7F:74:AA:39
Ethertype: 0x0800 (2048) - IP
Direction: Out
Time / Delta Time: 21:55:15,981 / 0,010
Frame size: 104 bytes
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Total length: 0x005A (90)
ID: 0x0E94 (3732)
Flags
Fragment offset: 0x0000 (0)
Time to live: 0x80 (128)
Protocol: 0x2F (47) - GRE
Checksum: 0x1621 (5665) - correct
Source IP: 10.1.1.189
Destination IP: 10.1.0.2
IP Options: None

DNS-запрос, порт 53

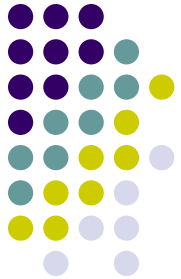


HTTP-ответ, порт 80



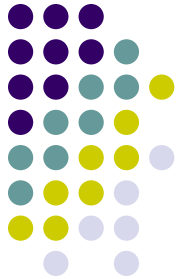
Отсутствие шифрования данных

Аутентификация пользователей PPTP



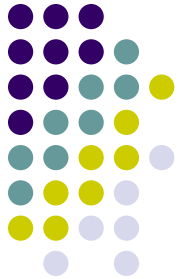
- Extensible Authentication Protocol (EAP),
- Microsoft Challenge Handshake Authentication Protocol (MSCHAP) версии 1 и 2,
- Challenge Handshake Authentication Protocol (CHAP),
- Shiva Password Authentication Protocol (SPAP)
- Password Authentication Protocol (PAP)
- Наилучший - MSCHAP версии 2 - взаимная аутентификация клиента и сервера

Варианты аутентификации Microsoft PPTP



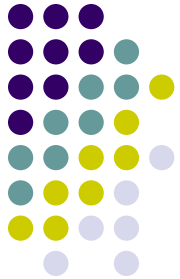
- Текстовый пароль: Клиент передает серверу пароль в открытом виде
- Хэшированный пароль: Клиент передает серверу хэш пароля
- Вызов/Отклик: Аутентификация сервера и клиента с использованием протокола MS-CHAP (вызов/отклик)

Аутентификация MSCHAP



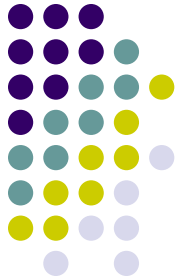
- Клиент запрашивает вызов сетевого имени.
- Сервер возвращает восьмибитовый случайный вызов.
- Клиент вычисляет хэш-функцию Lan Manager, добавляет пять нулей для создания 21-байтовой строки и делит строку на три семибайтовых ключа. Каждый ключ используется для шифрации вызова, что приводит к появлению 24-разрядного шифрованного значения. Оно возвращается серверу как отклик. Клиент выполняет то же самое с хэш-функцией Windows NT.
- Сервер ищет значение хэш-функции в своей базе данных, шифрует запрос с помощью хэш-функции и сравнивает его с полученными шифрованными значениями. Если они совпадают, аутентификация заканчивается.

Шифрование в PPTP



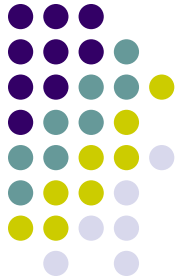
- Версия шифрования DES компании RSA Data Security, получившей название "шифрование двухточечной связи Microsoft" (Microsoft Point-to-Point Encryption - MPPE).
- Существование секретного ключа, известного обоим участникам соединения
- Используется поточный шифр RC4 с 40- либо 128-разрядным ключом

Формирование ключа RC4



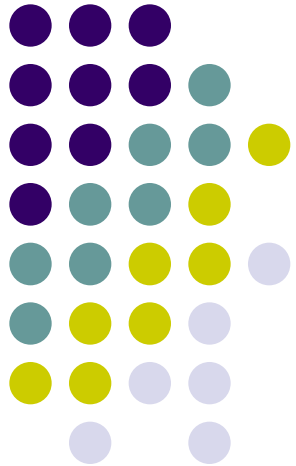
- 40-битовый
  - Генерация определяющего 64-битового ключа из хэш-функции Lan Manager пароля пользователя (известного пользователю и серверу) с помощью SHA.
  - Установка старших 24 бит ключа в значение 0xD1269E
- 128-битовый
  - Объединение хэша Windows NT и 64-битового случайного значения, выданного сервером при работе по протоколу MS-CHAP. Данное число посылается клиенту по протоколу обмена, потому оно известно и клиенту, и серверу.
  - Генерация определяющего 128-битового ключа из результатов предыдущего этапа с помощью SHA.

Уровни защищенных каналов

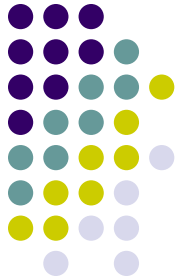


Прикладной	S/MIME /PGP /SHTTP
Транспортный (TCP/UDP)	SSL /TLS / SOCKS
Сетевой (IP)	IPSec / SKIP
Канальный	PPTP / L2F /L2TP

Защита на сетевом уровне

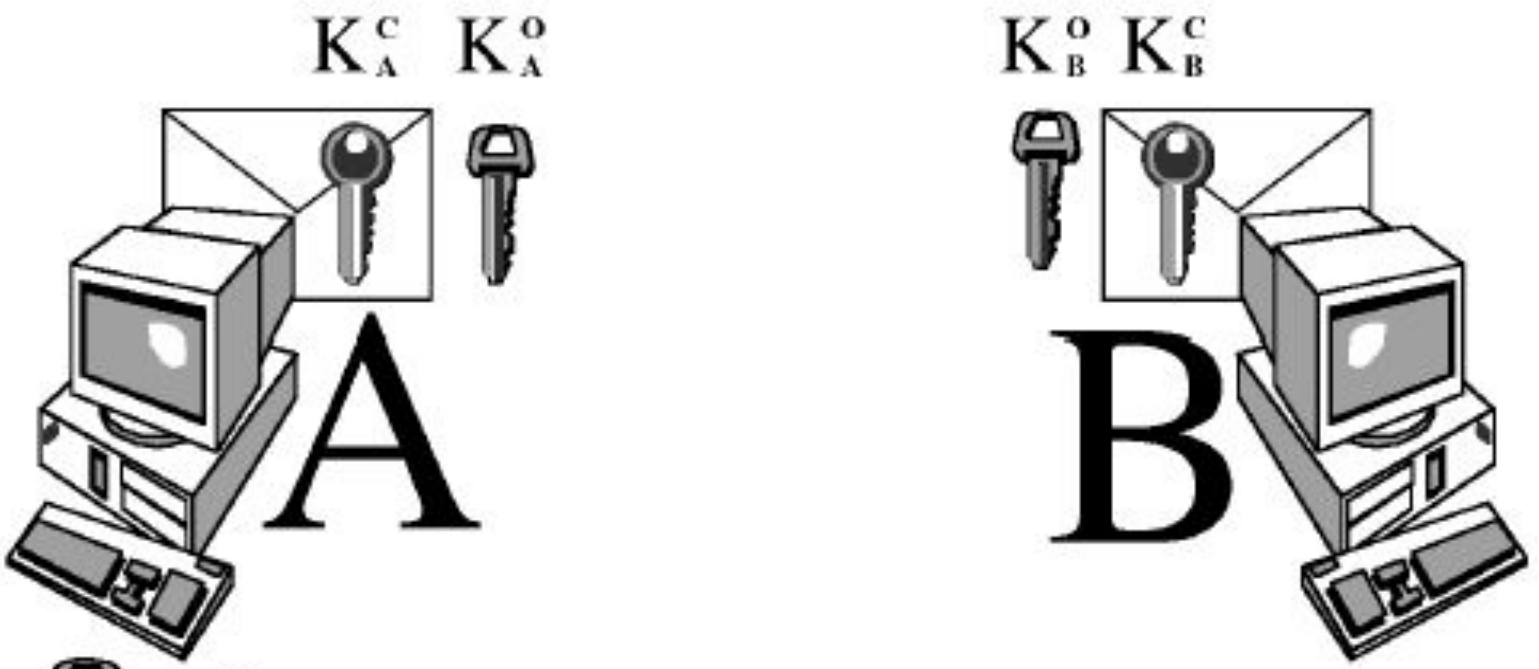


Защита на сетевом уровне



- Протокол SKIP (Simple Key management for Internet Protocol – простое управление ключами для IP-протокола)
- Разработчик – Sun Microsystems, 1994
- Аппаратная независимость
- Прозрачность для приложений
- Независимость от системы шифрования

Система открытых ключей Диффи-Хеллмана



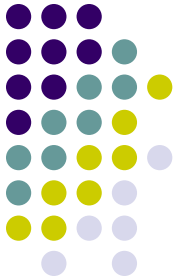
K_i^O

Открытые ключи генерируются, сертифицируются (снабжаются цифровой подписью доверительной стороны) и свободно распространяются центром распределения ключей

K_i^C

Секретный ключ известен только владельцу, что обеспечивает конфиденциальность информации

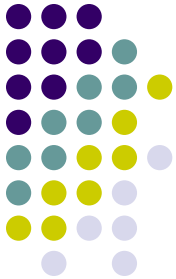
Система открытых ключей Диффи-Хеллмана



- Каждый пользователь системы защиты информации имеет *секретный ключ* **Кс**, известный только ему, и *открытый ключ* **Ко**.
- Открытый ключ **Ко** вычисляется из секретного ключа следующим образом:

- $\mathbf{Ko = g^{Kc} \bmod n,}$
- где **g** и **n** - некоторые заранее выбранные достаточно длинные простые целые числа.

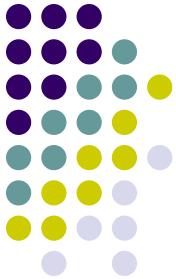
Протокол SKIP



- Узел **I**, адресующий свой трафик к узлу **J**, на основе логики открытых ключей вычисляет разделяемый секрет $\mathbf{K_{ij}}$.
- $\mathbf{K_{ij} = (K_{oj})^{Kci} \bmod n = (g^{Kcj})^{Kci} \bmod n = g^{Kci*Kcj} \bmod n}$
- Ключ $\mathbf{K_{ij}}$ является *долговременным разделяемым секретом* для любой пары абонентов **I** и **J** и не может быть вычислен третьей стороной.
- Отправитель и получатель пакета могут вычислить разделяемый секрет на основании собственного секретного ключа и открытого ключа партнера:
- $\mathbf{K_{ij} = (K_{oj})^{Kci} \bmod n = (K_{oi})^{Kcj} \bmod n = K_{ji}}$

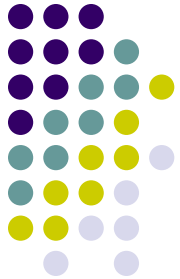
Схема создания SKIP пакета

Преимущества



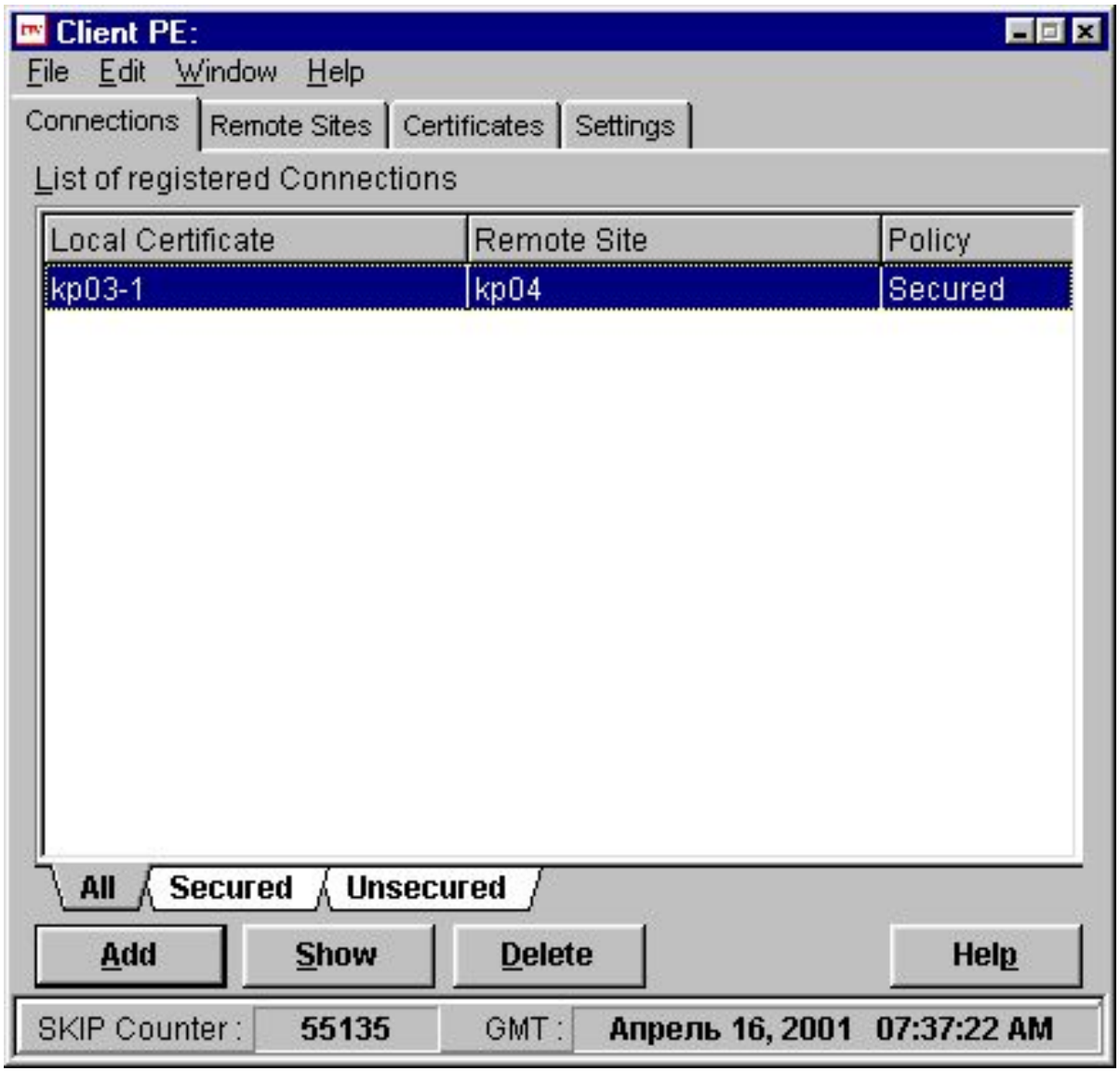
- дополнительная защита разделяемого секрета, так как он используется для шифрования малой части трафика и не даёт вероятному противнику материал для статистического криптоанализа в виде большого количества информации, зашифрованного им;
- в случае компрометации пакетного ключа ущерб составит лишь небольшая группа пакетов, зашифрованных им.

Дополнительные меры защиты разделяемого секрета

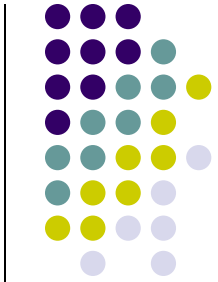


- Включение параметра (n), используемого для вычисления ключа $\mathbf{K_{ijn}}$
- Для получения $\mathbf{K_p}$ применяется результат хэш-функции (MD5) из $\mathbf{K_{ij}}$ и n.
- n – время в часах, отсчитанное от 00 час 00 мин 01.01.95
- Если n различается более чем на 1 час, то пакет отбрасывается

SKIP counter



Конфиденциальность и аутентификация

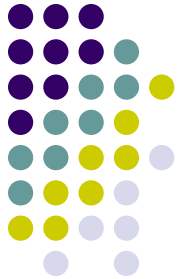


IP	SKIP	AH	ESP	Inner protocol

IP - заголовок протокола IP
SKIP - заголовок протокола SKIP
AH - аутентификационный заголовок
ESP - заголовок, включающий данные об инкапсулированном протоколе
Inner protocol - пакет инкапсулируемого протокола.

- Если применяется режим только аутентификации или только шифрования, заголовки AH и ESP, могут изыматься из пакета.

Проблемы организации



- способа хранения секретных ключей **Kc** и кэширования разделяемых секретов **Kij**
- способа генерации и хранения (в течение относительно короткого времени жизни) пакетных ключей **Kp**
- сертификации открытых ключей.

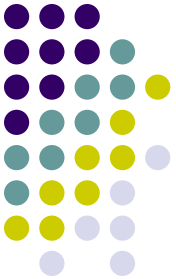
Атака man-in-the-middle

- Атакующая сторона находится внутри сети, где обмениваются информацией пользователи **i** и **j.**
- Цель атаки - предложить от своего имени пользователю **i** "поддельный" открытый ключ **Koj**, а пользователю **j** -соответственно, ключ **Koi**.
- После этого третья сторона может принимать весь шифрованный трафик от одного абонента, расшифровывать, читать, шифровать под другим ключом и передавать другому.

Зашита от атаки

- Распределением открытых ключей должна заниматься заслуживающая доверия сторона и ключи должны сертифицироваться (сопровождаться электронной подписью этой доверительной стороны).
- ***Нотариус*** (Certificate Authority – ***CA***) подписывает не только открытый ключ, но и целый ряд фактической информации, а также информацию о дате выдаче и дате окончания действия его подписи.
- Центр Сертификации (ЦС)
- Получившийся документ (файл) называется сертификатом открытого ключа

Сертификат

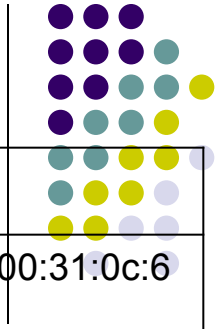


- Цифровой документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Он содержит определенную, цифровым образом подписанную информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название доверенного центра и т.д.
- Наиболее распространен формат сертификата, установленный Международным Телекоммуникационным Союзом (ITU Rec. X.509)

X.509

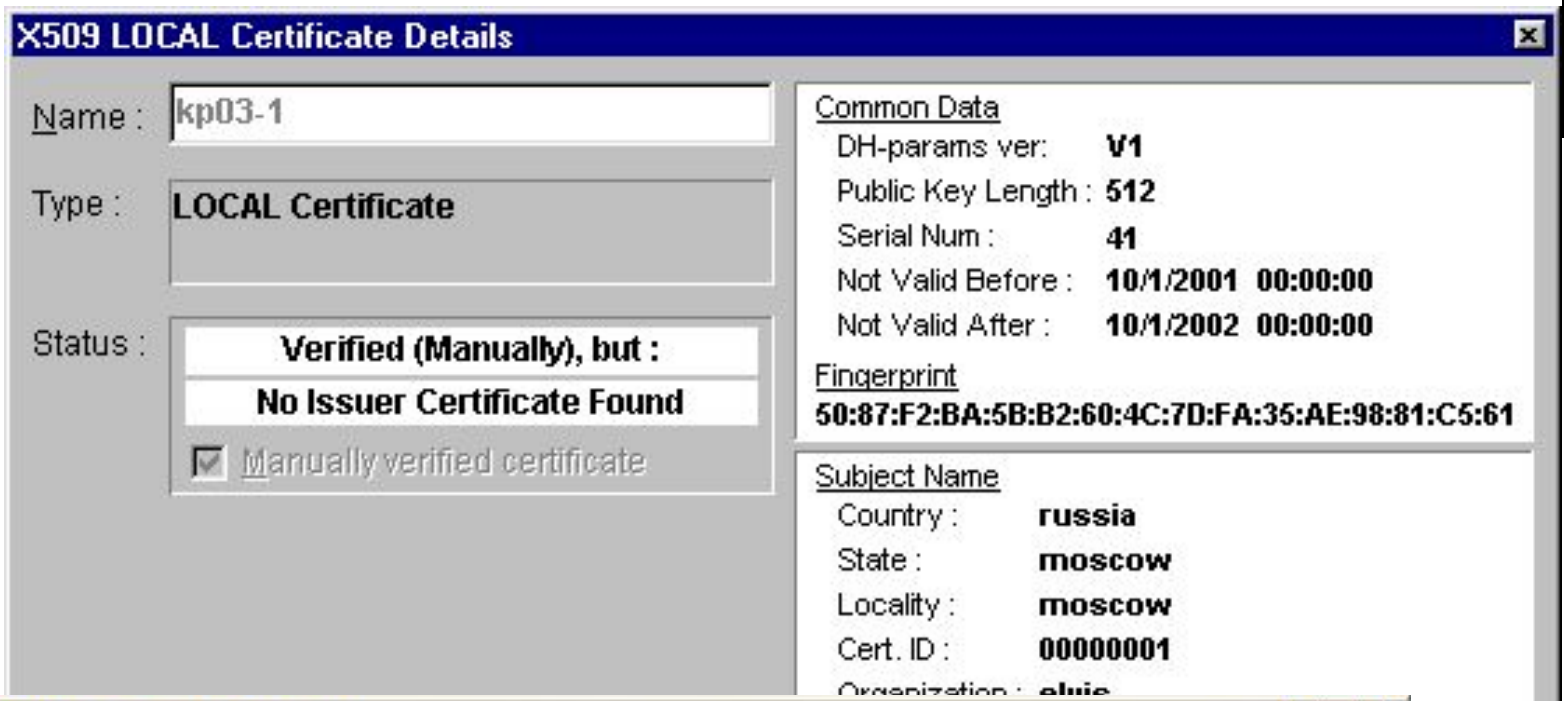
- Стандарт X.509 ITU-T - определение формата электронного сертификата и списков отозванных сертификатов (COC)
  - имя Издателя сертификата;
  - имя Владельца сертификата;
  - открытый ключ Издателя;
  - срок действия открытого (секретного) ключа Издателя и Владельца;
  - дополнения, используемые при верификации цепочек (basicConstraints, nameConstraints);
  - COC для каждого Издателя (даже если он не содержит отзываемых сертификатов).

Электронный сертификат X.509

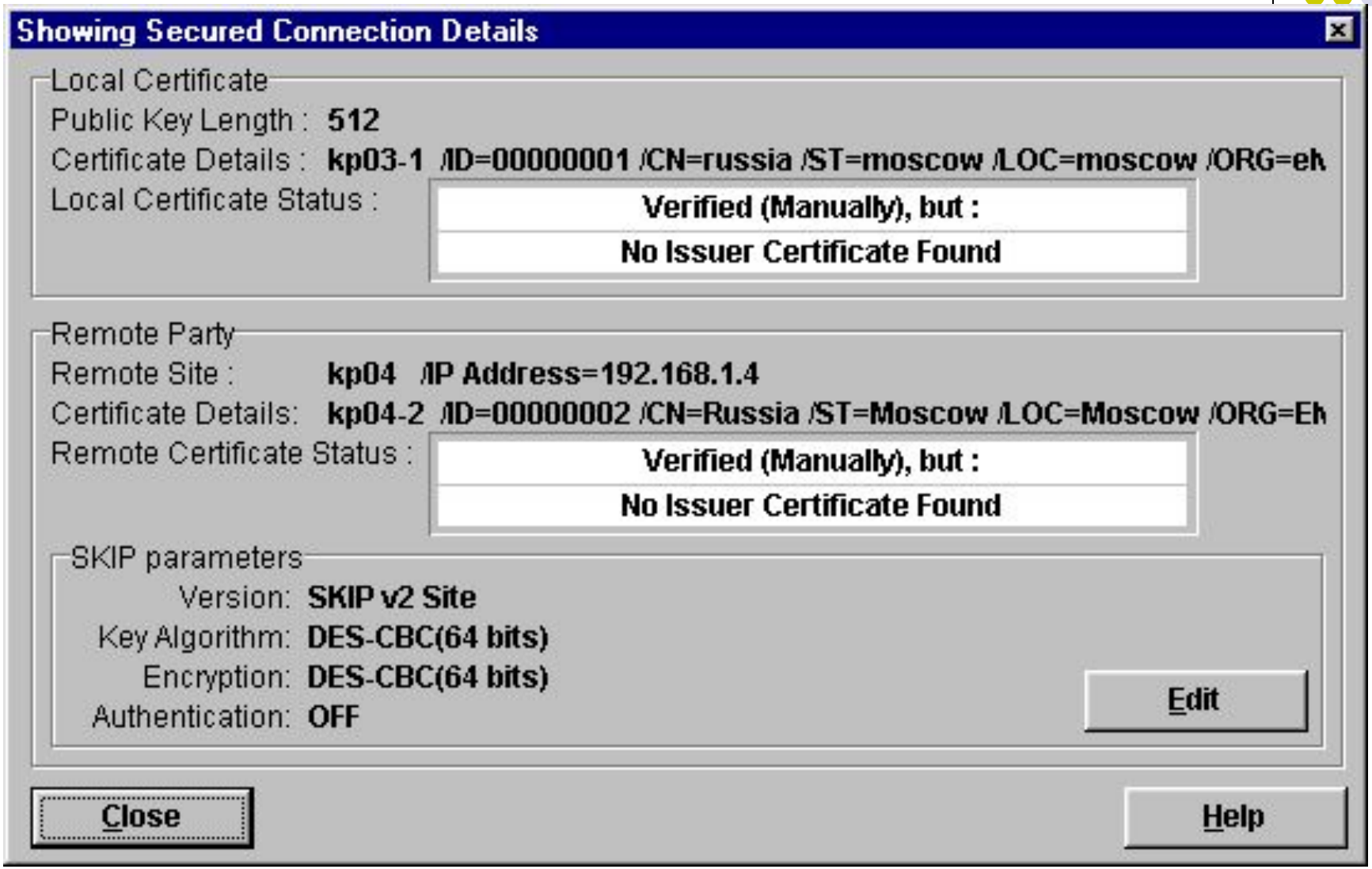


Version	Версия сертификата	1, 2, 3
Certificate Serial Number	Серийный номер сертификата	40:00:00:00:00:00:00:ab:38:1e:8b:e9:00:31:0c:60
Signature Algorithm Identifier	Идентификатор алгоритма ЭЦП	ГОСТ Р 34.10-94
Issuer X.500 Name	Имя Издателя сертификата	C=RU, ST=Moscow,O=PKI, CN=Certification Authority
Validity Period	Срок действия сертификата	Действителен с : Ноя 2 06:59:00 1999 GMT Действителен по : Ноя 6 06:59:00 2004 GMT
Subject X.500 Name	Имя Владельца сертификата	C=RU, ST=Moscow, O=PKI, CN=Sidorov
Subject Public Key Info	Открытый ключ Владельца	тип ключа: Открытый ключ ГОСТ длина ключа: 1024 значение: AF:ED:80:43.....
Issuer Unique ID version 2	Уникальный идентификатор Издателя	
Subject Unique ID version 2	Уникальный идентификатор Владельца	
CA Signature ЭЦП Центра Сертификации		

X.509


X509 LOCAL Certificate Details
Name :
kp03-1
Type :
LOCAL Certificate
Status :
Verified (Manually), but :
No Issuer Certificate Found
Manually verified certificate
Common Data
DH-params ver: V1
Public Key Length : 512
Serial Num : 41
Not Valid Before : 10/1/2001 00:00:00
Not Valid After : 10/1/2002 00:00:00
Fingerprint
50:87:F2:BA:5B:B2:60:4C:7D:FA:35:AE:98:81:C5:61
Subject Name
Country : russia
State : moscow
Locality : moscow
Cert. ID : 00000001
Выбрать view 1.dsa - Far
E:\...tes\Certificates-31_12_01\1\1.dsa DOS 581 Col 0 100%

X.509


Showing Secured Connection Details
Local Certificate
Public Key Length : 512
Certificate Details : kp03-1 /ID=00000001 /CN=russia /ST=moscow /LOC=moscow /ORG=eh
Local Certificate Status :
Verified (Manually), but :
No Issuer Certificate Found
Remote Party
Remote Site : kp04 /IP Address=192.168.1.4
Certificate Details: kp04-2 /ID=00000002 /CN=Russia /ST=Moscow /LOC=Moscow /ORG=Eh
Remote Certificate Status :
Verified (Manually), but :
No Issuer Certificate Found
SKIP parameters
Version: SKIP v2 Site
Key Algorithm: DES-CBC(64 bits)
Encryption: DES-CBC(64 bits)
Authentication: OFF
Edit
Close
Help

Персональная карточка

Защищенная Станция 1

Номер действующего ключа подписи: 1

Дата и время формирования: 16:31 31-03-2000

Дата окончания срока действия подписи: 15:31 05-03-2005

Сигнатура открытого ключа подписи

C0 D6 6F 9B FD 1C 59 96 73 0A C0 7F 9C 29 40 8D 2A 5E 61 B0 EB 3F 5F AF F0 7A 05 D7 FB 0E 14 01 3D
76 4F 76 2F 66 DD A8 1D 08 30 BD 9E F7 54 3B 72 77 EB 47 50 03 2A BE 72 4D 83 F9 9E 05 AF 9C

Дата сертификации подписи: 16:31 31-03-2000

Сертификат подписал: 10E10034

Срок действия подписи, подписавшего сертификат: 12 месяцев

Сигнатура открытого ключа подписи, подписавшего сертификат

B3 94 F0 2A 6A 48 31 9D 77 77 FD 42 93 B2 15 1C C7 2E 45 6D A0 E5 55 A8 A5 78 88 C9 0F 61 55 49 69
9C 6A 6E 56 95 73 21 3F 9A 5A C1 36 0A C9 5F E6 49 66 DC 3D C7 AC 2C C7 B3 37 16 BD A2 24 32

Сигнатура подписи сертификата

8B B2 B2 09 B6 65 E6 F7 66 2E CB 16 20 D1 78 F5 66 00 6E DA 61 A3 37 B0 33 6D 36 2B 62 F5 32 11 97
F1 A7 11 31 86 83 BC 8E FC 72 76 6A 32 D0 86 96 EA 47 01 0C A9 7C 97 8F FF 70 DE 38 73 9E 6A

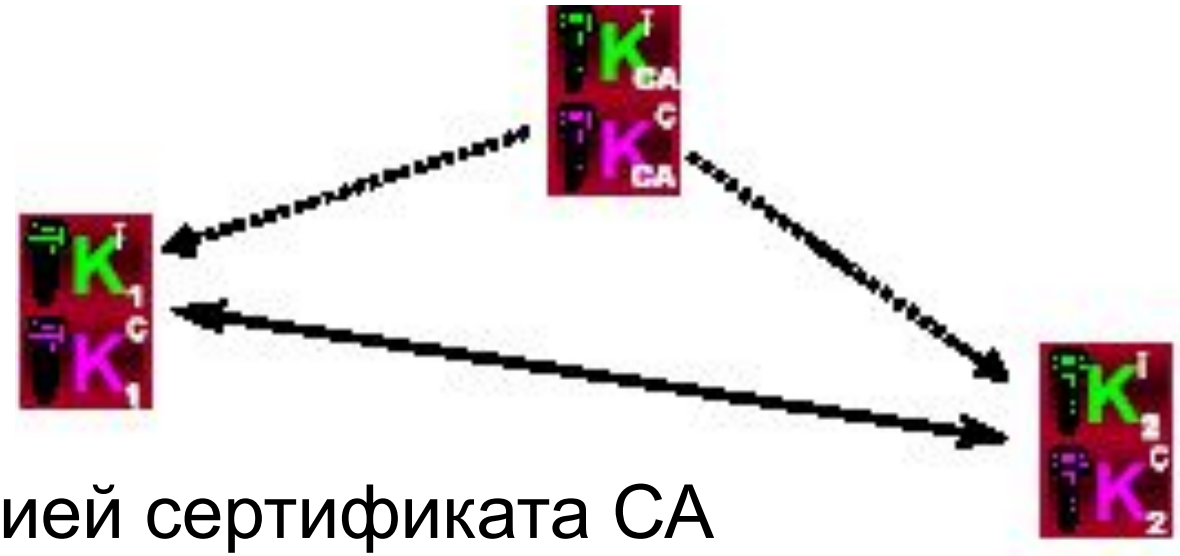
12:08 16-04-2004 Результат проверки сертификата: Сертификат действителен

Принять | Напечатать | Сохранить

PKI (public key infrastructure)
Инфраструктура Открытых Ключей (ИОК)

- PKI – инфраструктура управления открытыми ключами, состоит из сети нотариусов

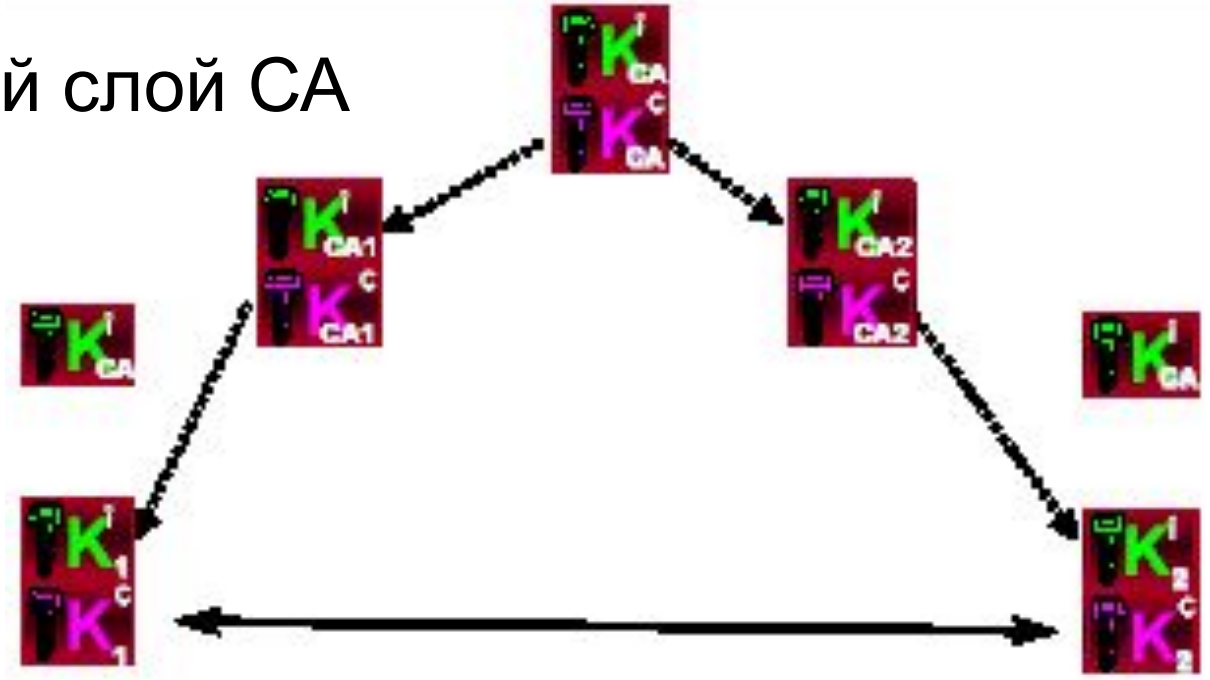
Участники взаимодействия должны:



- Располагать неподдельной копией сертификата CA
- Автоматически проверять любой сертификат партнера, используя открытый сертификат CA

Двухслойная иерархия CA

Иерархический слой CA

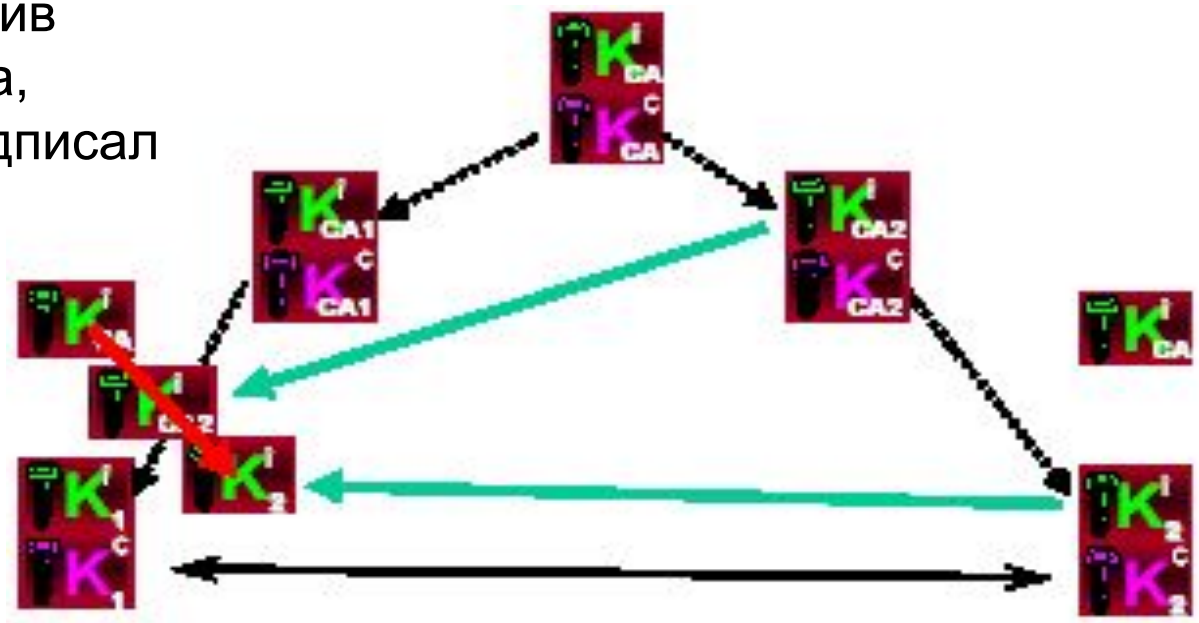


- подписывают свои сертификаты у центрального CA
- подписывают сертификаты рядовых пользователей своими закрытыми ключами точно так же, как это делал центральный CA

Проверка сертификата удаленного абонента

Пользователь, получив сертификат партнера, выясняет, что его подписал незнакомый ему CA

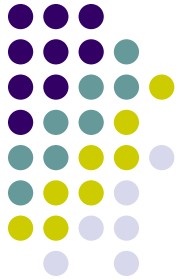
Он просит партнера предоставить ему сертификат этого CA



Получив сертификат CA, он проверяет его сертификатом центрального CA

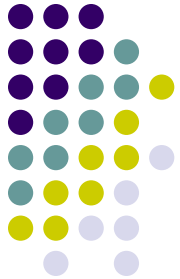
В случае успешной проверки он начинает доверять этому CA и проверяет с помощью его сертификата сертификат удаленного пользователя

Защита от внешних и внутренних атак



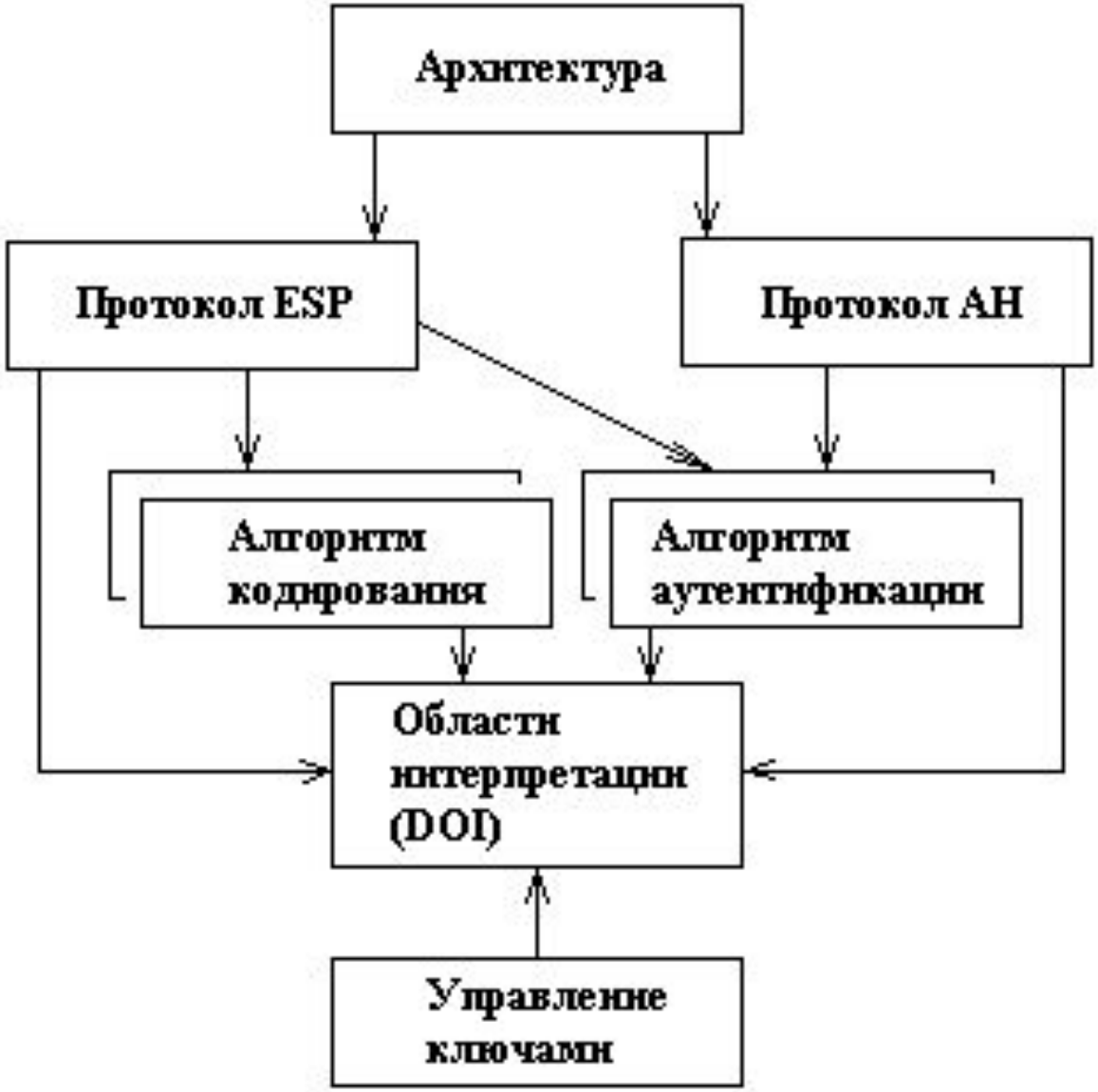
- не могут обнаружить вирусы и атаки типа "отказ в обслуживании"
- не могут фильтровать данные по различным признакам
- защита лишь части трафика, например, направленного в удаленный филиал. Остальной трафик (например, к публичным Web-серверам) проходит через VPN-устройство без обработки
- нет защиты от действий пользователей, имеющих санкционированный доступ в корпоративную сеть

Защита на сетевом уровне

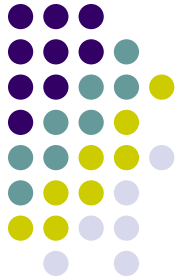


- Протокол IPSec
- Аутентификация (протокол IKE - Internet Key Exchange)
- Защита целостности (Заголовок аутентификации AH - Authentication Header)
- Шифрование (ESP - Encapsulating Security Payload)

Архитектура IPSec

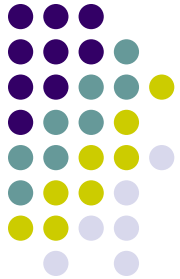


Аутентифицирующий заголовок (AH)



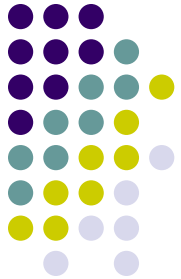
- Защита от атак, связанных с несанкционированным изменением содержимого пакета
- Специальное применение алгоритма MD5:
  - в процессе формирования AH последовательно вычисляется хэш-функция от объединения самого пакета и некоторого предварительно согласованного ключа
  - затем от объединения полученного результата и преобразованного ключа.

Заголовок ESP



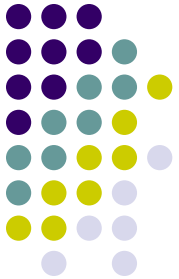
- Обеспечение конфиденциальности данных
- Формат ESP может претерпевать значительные изменения в зависимости от используемых криптографических алгоритмов
- Любой симметричный алгоритм шифрования

IKE

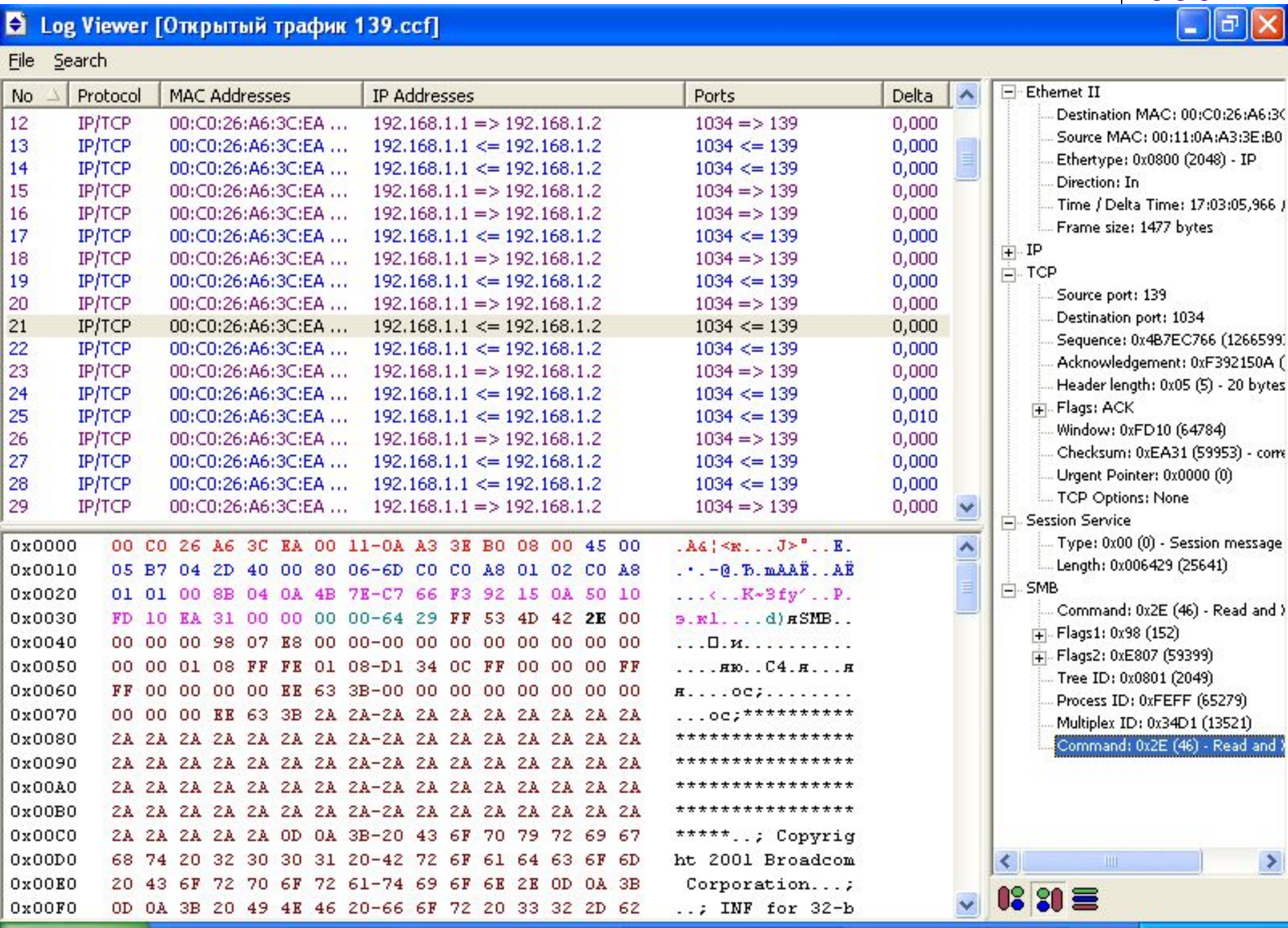


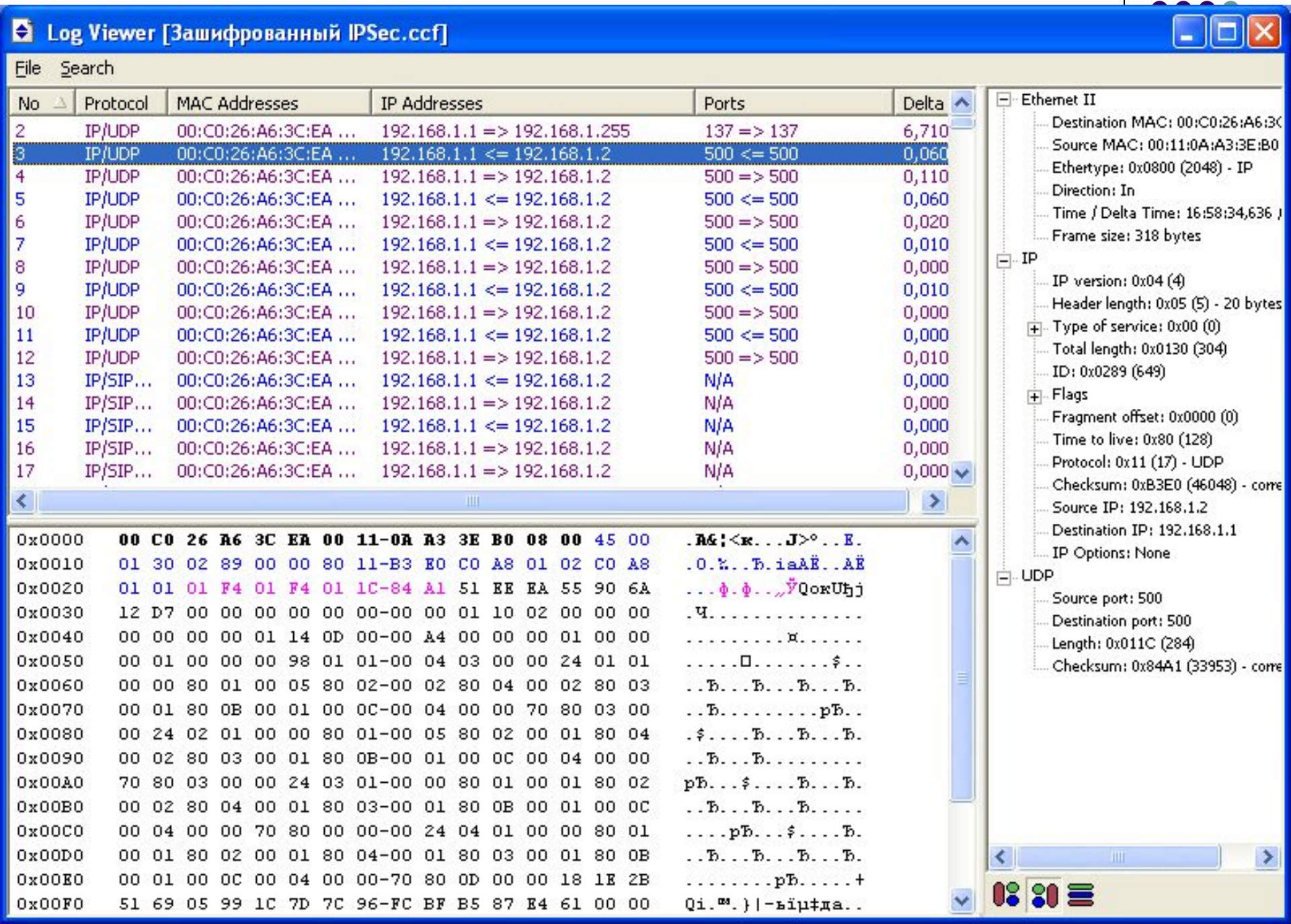
- IKE – протокол обмена ключами
- Первоначальный этап установки соединения
- Способ инициализации защищенного канала
- Процедуры обмена секретными ключами
- Методы шифрования

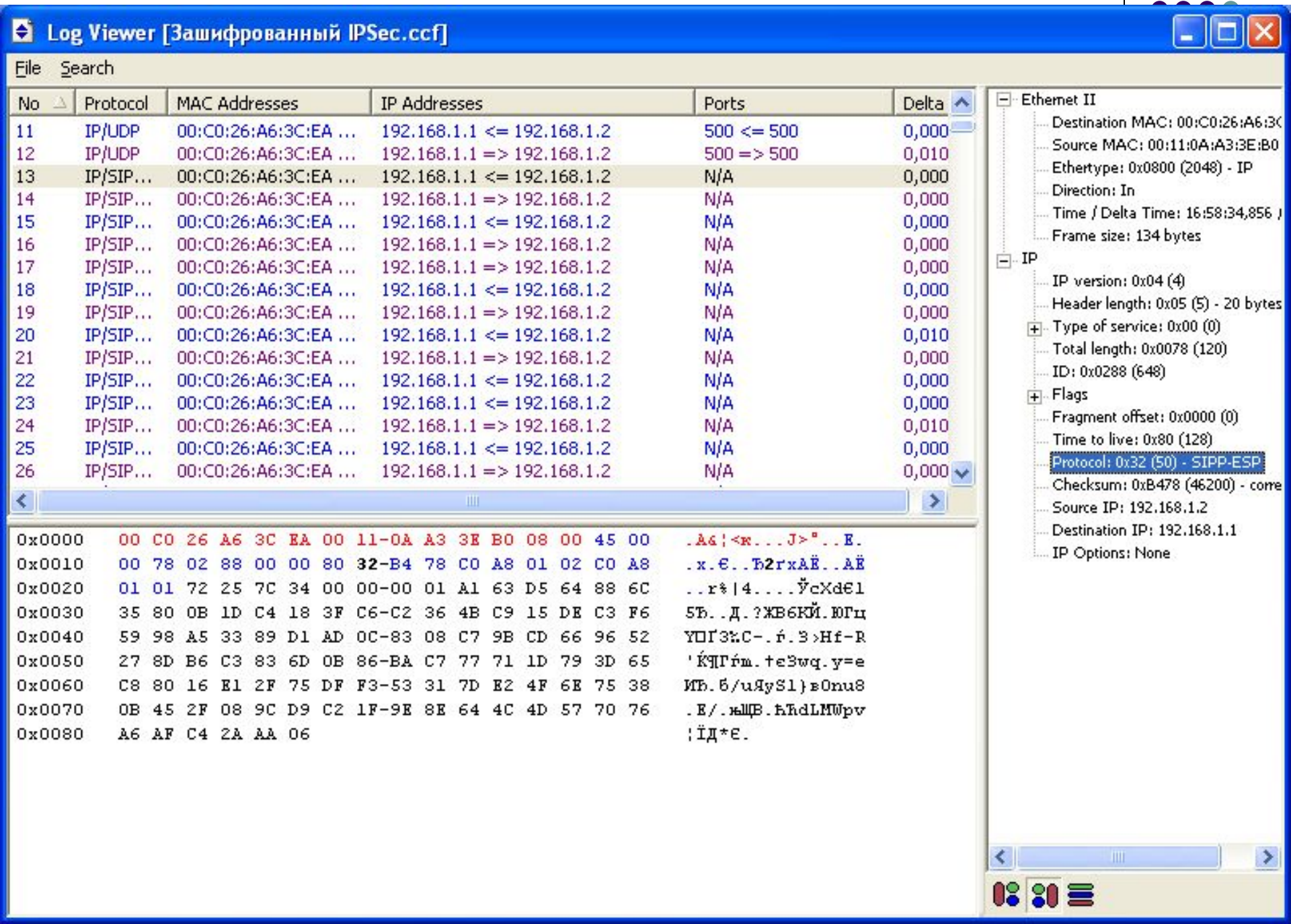
Способы аутентификации IKE



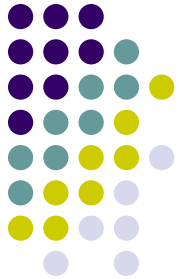
- «Запрос-ответ» с использованием хэш-функции с общим секретным ключом
- Сертификаты открытых ключей
- Керберос


Log Viewer [Открытый трафик 139.ccf]
File
Search
No
Protocol
MAC Addresses
IP Addresses
Ports
Delta
12 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 1034 => 139 0,000
13 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 1034 <= 139 0,000
14 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 1034 <= 139 0,000
15 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 1034 => 139 0,000
16 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 1034 => 139 0,000
17 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 1034 <= 139 0,000
18 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 1034 => 139 0,000
19 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 1034 <= 139 0,000
20 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 1034 => 139 0,000
21 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 1034 <= 139 0,000
22 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 1034 <= 139 0,000
23 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 1034 => 139 0,000
24 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 1034 <= 139 0,000
25 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 1034 <= 139 0,010
26 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 1034 => 139 0,000
27 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 1034 <= 139 0,000
28 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 1034 <= 139 0,000
29 IP/TCP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 1034 => 139 0,000
0x0000 00 C0 26 A6 3C EA 00 11-0A A3 3E B0 08 00 45 00 .A&¦<к...J>°..E.
0x0010 05 B7 04 2D 40 00 80 06-6D C0 C0 A8 01 02 C0 A8 .·.-@.Ъ.mAAË..AË
0x0020 01 01 00 8B 04 0A 4B 7E-C7 66 F3 92 15 0A 50 10 ...‹..K~Зfу'..P.
0x0030 FD 10 EA 31 00 00 00 00-64 29 FF 53 4D 42 2E 00 э.кl....d)яSMB..
0x0040 00 00 00 98 07 E8 00 00-00 00 00 00 00 00 00 00 ...□.и..........
0x0050 00 00 01 08 FF FE 01 08-D1 34 0C FF 00 00 00 FF ....яю..С4.я...я
0x0060 FF 00 00 00 00 EE 63 3B-00 00 00 00 00 00 00 00 я....oc;........
0x0070 00 00 00 EE 63 3B 2A 2A-2A 2A 2A 2A 2A 2A 2A 2A ...oc;**********
0x0080 2A 2A 2A 2A 2A 2A 2A 2A-2A 2A 2A 2A 2A 2A 2A 2A **********
0x0090 2A 2A 2A 2A 2A 2A 2A 2A-2A 2A 2A 2A 2A 2A 2A 2A **********
0x00A0 2A 2A 2A 2A 2A 2A 2A 2A-2A 2A 2A 2A 2A 2A 2A 2A **********
0x00B0 2A 2A 2A 2A 2A 2A 2A 2A-2A 2A 2A 2A 2A 2A 2A 2A **********
0x00C0 2A 2A 2A 2A 2A 0D 0A 3B-20 43 6F 70 79 72 69 67 *****..; Copyrig
0x00D0 68 74 20 32 30 30 31 20-42 72 6F 61 64 63 6F 6D ht 2001 Broadcom
0x00E0 20 43 6F 72 70 6F 72 61-74 69 6F 6E 2E 0D 0A 3B Corporation...;
0x00F0 0D 0A 3B 20 49 4E 46 20-66 6F 72 20 33 32 2D 62 ..; INF for 32-b
Ethernet II
Destination MAC: 00:C0:26:A6:3C
Source MAC: 00:11:0A:A3:3E:B0
Ethertype: 0x0800 (2048) - IP
Direction: In
Time / Delta Time: 17:03:05,966
Frame size: 1477 bytes
IP
TCP
Source port: 139
Destination port: 1034
Sequence: 0x4B7EC766 (1266599
Acknowledgement: 0xF392150A (
Header length: 0x05 (5) - 20 bytes
Flags: ACK
Window: 0xFD10 (64784)
Checksum: 0xEA31 (59953) - corr
Urgent Pointer: 0x0000 (0)
TCP Options: None
Session Service
Type: 0x00 (0) - Session message
Length: 0x006429 (25641)
SMB
Command: 0x2E (46) - Read and
Flags1: 0x98 (152)
Flags2: 0xE807 (59399)
Tree ID: 0x0801 (2049)
Process ID: 0xFEFF (65279)
Multiplex ID: 0x34D1 (13521)
Command: 0x2E (46) - Read and


Log Viewer [Зашифрованный IPSec.ccf]
File
Search
No
Protocol
MAC Addresses
IP Addresses
Ports
Delta
2 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.255 137 => 137 6,710
3 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 500 <= 500 0,060
4 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 500 => 500 0,110
5 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 500 <= 500 0,060
6 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 500 => 500 0,020
7 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 500 <= 500 0,010
8 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 500 => 500 0,000
9 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 500 <= 500 0,010
10 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 500 => 500 0,000
11 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 500 <= 500 0,000
12 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 500 => 500 0,010
13 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 N/A 0,000
14 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 N/A 0,000
15 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 N/A 0,000
16 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 N/A 0,000
17 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 N/A 0,000
0x0000 00 C0 26 A6 3C EA 00 11-0A A3 3E B0 08 00 45 00 .A&;<к...J>°..E.
0x0010 01 30 02 89 00 00 80 11-B3 E0 C0 A8 01 02 C0 A8 .0.‰..Ъ.iaAЁ..AЁ
0x0020 01 01 01 F4 01 F4 01 1C-84 A1 51 EE EA 55 90 6A ...ф.ф..„ўQокUђj
0x0030 12 D7 00 00 00 00 00 00-00 00 01 10 02 00 00 00 .Ч.............
0x0040 00 00 00 00 01 14 0D 00-00 A4 00 00 00 01 00 00 ....¤......
0x0050 00 01 00 00 00 98 01 01-00 04 03 00 00 24 01 01 .....□.......$..
0x0060 00 00 80 01 00 05 80 02-00 02 80 04 00 02 80 03 ..Ъ...Ъ...Ъ...Ъ.
0x0070 00 01 80 0B 00 01 00 0C-00 04 00 00 70 80 03 00 ..Ъ.........pЪ..
0x0080 00 24 02 01 00 00 80 01-00 05 80 02 00 01 80 04 .$....Ъ...Ъ...Ъ.
0x0090 00 02 80 03 00 01 80 0B-00 01 00 0C 00 04 00 00 ..Ъ...Ъ.........
0x00A0 70 80 03 00 00 24 03 01-00 00 80 01 00 01 80 02 pЪ...$....Ъ...Ъ.
0x00B0 00 02 80 04 00 01 80 03-00 01 80 0B 00 01 00 0C ..Ъ...Ъ...Ъ.....
0x00C0 00 04 00 00 70 80 00 00-00 24 04 01 00 00 80 01 ....pЪ...$....Ъ.
0x00D0 00 01 80 02 00 01 80 04-00 01 80 03 00 01 80 0B ..Ъ...Ъ...Ъ...Ъ.
0x00E0 00 01 00 0C 00 04 00 00-70 80 0D 00 00 18 1E 2B ....pЪ.....+
0x00F0 51 69 05 99 1C 7D 7C 96-FC BF B5 87 E4 61 00 00 Qi.™.}|-ьїµ‡дa..
Ethernet II
Destination MAC: 00:C0:26:A6:3C
Source MAC: 00:11:0A:A3:3E:B0
Ethertype: 0x0800 (2048) - IP
Direction: In
Time / Delta Time: 16:58:34,636 /
Frame size: 318 bytes
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Total length: 0x0130 (304)
ID: 0x0289 (649)
Flags
Fragment offset: 0x0000 (0)
Time to live: 0x80 (128)
Protocol: 0x11 (17) - UDP
Checksum: 0xB3E0 (46048) - corre
Source IP: 192.168.1.2
Destination IP: 192.168.1.1
IP Options: None
UDP
Source port: 500
Destination port: 500
Length: 0x011C (284)
Checksum: 0x84A1 (33953) - corre


Log Viewer [Зашифрованный IPSec.ccf]
File
Search
No
Protocol
MAC Addresses
IP Addresses
Ports
Delta
11 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 500 <= 500 0,000
12 IP/UDP 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 500 => 500 0,010
13 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 N/A 0,000
14 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 N/A 0,000
15 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 N/A 0,000
16 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 N/A 0,000
17 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 N/A 0,000
18 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 N/A 0,000
19 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 N/A 0,000
20 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 N/A 0,010
21 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 N/A 0,000
22 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 N/A 0,000
23 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 N/A 0,000
24 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 N/A 0,010
25 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.2 N/A 0,000
26 IP/SIP... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.2 N/A 0,000
0x0000 00 C0 26 A6 3C EA 00 11-0A A3 3E B0 08 00 45 00 .A&¦<к...J>°..E.
0x0010 00 78 02 88 00 00 80 32-B4 78 C0 A8 01 02 C0 A8 .x.Є..Ђ2ґxAЁ..AЁ
0x0020 01 01 72 25 7C 34 00 00-00 01 A1 63 D5 64 88 6C ..r%|4....ЎcXdЄl
0x0030 35 80 0B 1D C4 18 3F C6-C2 36 4B C9 15 DE C3 F6 5Ђ..Д.?ЖВ6КЙ.ЮГц
0x0040 59 98 A5 33 89 D1 AD 0C-83 08 C7 9B CD 66 96 52 YШГ3%С-.ѓ.З›Hf-R
0x0050 27 8D B6 C3 83 6D 0B 86-BA C7 77 71 1D 79 3D 65 'Ќ¶Гѓm.†єЗwq.y=e
0x0060 C8 80 16 E1 2F 75 DF F3-53 31 7D E2 4F 6E 75 38 ИЂ.б/uЯуS1}вOnu8
0x0070 0B 45 2F 08 9C D9 C2 1F-9E 8E 64 4C 4D 57 70 76 .E/.ьЩВ.ћЋdLMWpv
0x0080 A6 AF C4 2A AA 06 ¦ЇД*Є.
Ethernet II
Destination MAC: 00:C0:26:A6:3C
Source MAC: 00:11:0A:A3:3E:B0
Ethertype: 0x0800 (2048) - IP
Direction: In
Time / Delta Time: 16:58:34,856 /
Frame size: 134 bytes
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Total length: 0x0078 (120)
ID: 0x0288 (648)
Flags
Fragment offset: 0x0000 (0)
Time to live: 0x80 (128)
Protocol: 0x32 (50) - SIPP-ESP
Checksum: 0xB478 (46200) - corre
Source IP: 192.168.1.2
Destination IP: 192.168.1.1
IP Options: None

Производительность

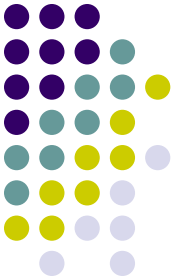


- Задержки при установлении защищенного соединения
  - Смена ключа – редкое дело
- Задержки связанные с шифрованием
  - Время зашифрования существенно меньше времени отправки пакетов
- Задержки, связанные с добавлением нового заголовка
  - Добавляется до 60% трафика

Производительность

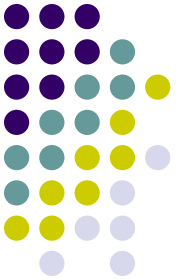
Алгоритм (разработчик)	DES	ГОСТ (Анкад)	ВЕСТА (ЛАН Крипто)
Скорость обработки полезного трафика, Мбит/сек			
Pentium -133	6	5	10
Pentium II/300	8	6	13
SPARC Ultra 1	8	3	19
SPARC Ultra 450	38	17	61
Увеличение длины IP пакета, байт	62	86	86

Варианты решений



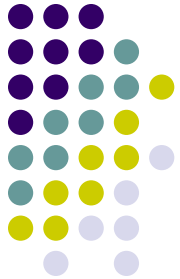
- VPN на базе сетевых операционных систем (ОС);
- VPN на базе маршрутизаторов;
- VPN на базе межсетевых экранов (МЭ);
- VPN на базе специализированного программного обеспечения

VPN на базе сетевых ОС



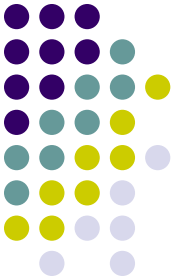
- Штатные средства ОС Windows NT/2000/XP (протоколы PPTP и IPSec)
- Недостаток - ошибки и слабые места существующих версий ОС

VPN на базе маршрутизаторов



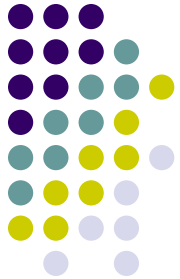
- Маршрутизаторы Cisco Systems
- Совокупность виртуальных защищенных туннелей типа “точка-точка” от одного мартшутизатора к другому
- Алгоритм DES
- Требует значительных вычислительных ресурсов на мартшутизаторе

VPN на базе МЭ



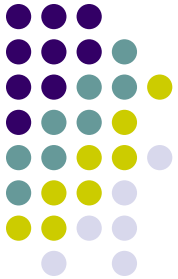
- Программные продукты компании CheckPoint Software Technologies – CheckPoint Firewall-1 /VPN-1
  - протокол IPSec, алгоритмы DES, CAST, IDEA, FWZ
- ФПСУ-IP компании “Амикон”,
- DataGuard компании “Сигнал-Ком”,
- комплекс МЭ ЗАСТАВА с модулем построения VPN
  - SKIP

VPN на базе МЭ



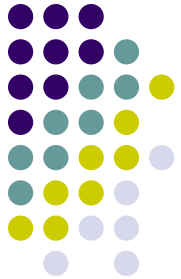
- Объединение функций МЭ и VPN шлюза в одной точке под контролем единой системы управления и аудита
- Недостаток - высокая стоимость в пересчете на одно рабочее место корпоративной сети и достаточно высокие требования к производительности МЭ

VPN на базе СПО



- криптографический комплекс "Шифратор IP-пакетов" (ШИП) производства МО ПНИЭИ
  - отдельное программно-аппаратное устройство (криптошлюз), которое осуществляет шифрование всего исходящего из локальной сети трафика на базе реализации протокола SKIP

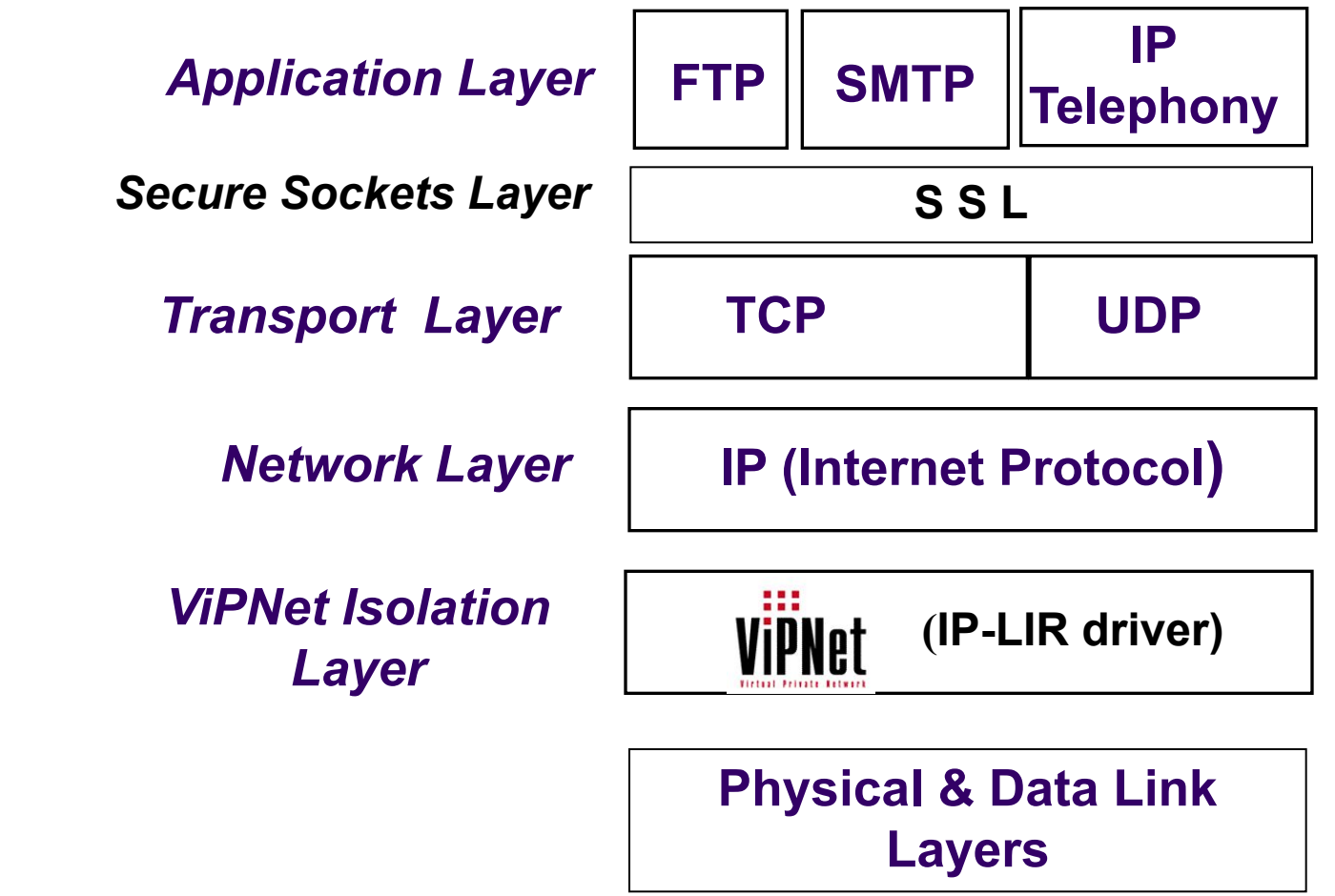
VPN на базе СПО



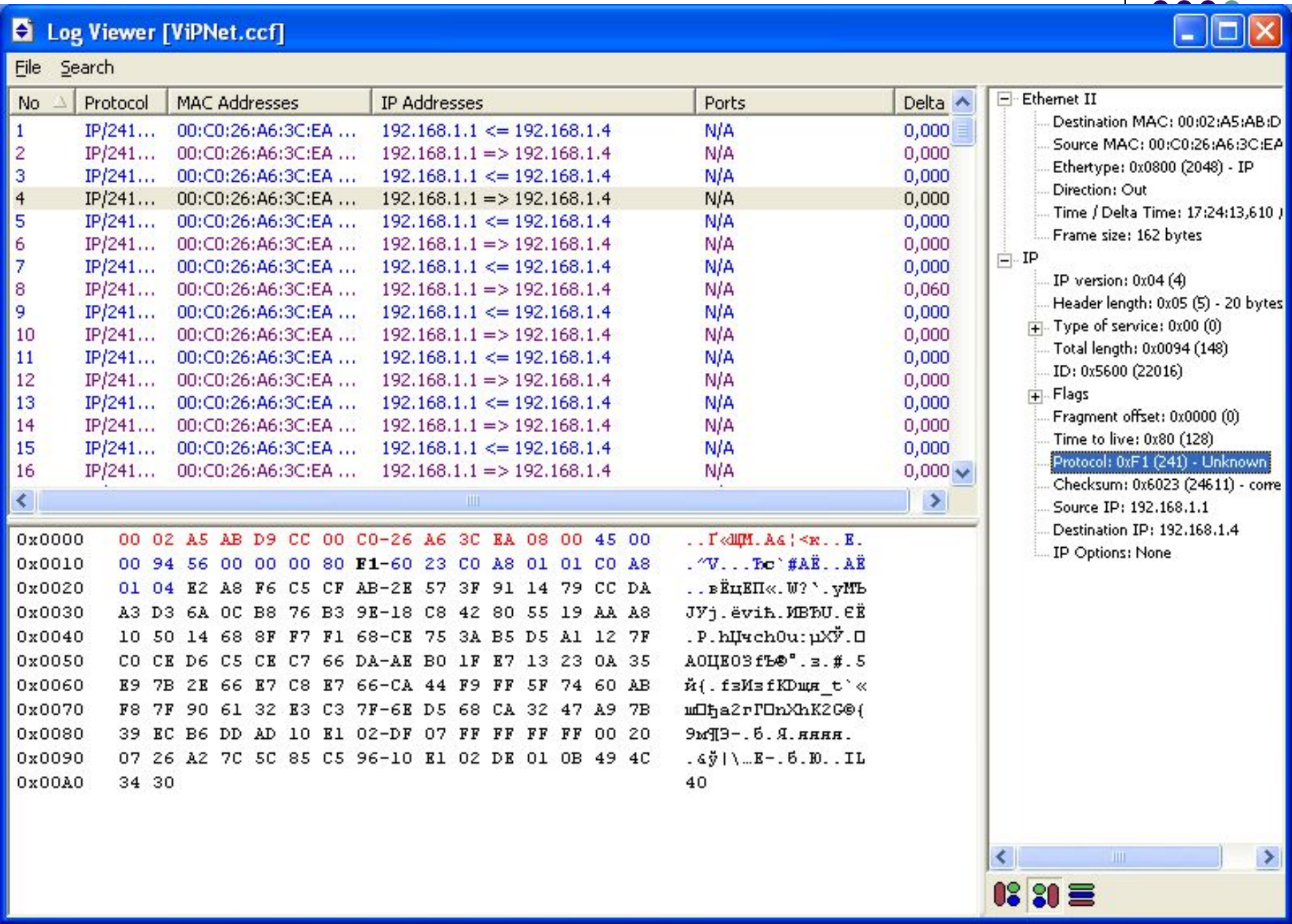
- Линейка программных продуктов "Застава" версии 2.5
  - протокол SKIP1
  - отсутствие встроенных криптоалгоритмов

VPN на базе СПО

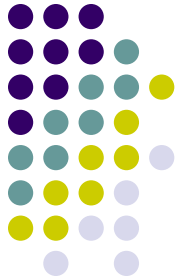
- Программный комплекс ViPNet компании «Инфотекс»



Драйвер IP-LIR программного комплекса ViPNet резидентно размещается между уровнем IP и физическим сетевым уровнем, что обеспечивает максимум защиты сетевых ресурсов и передаваемой информации, а также активное сопротивление попыткам разрушить жизнедеятельность сети.

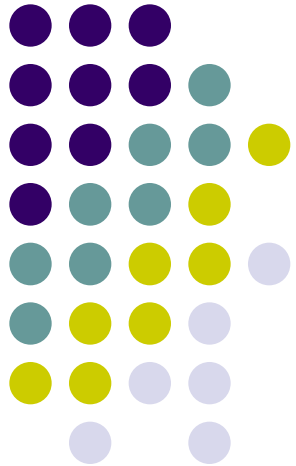

Log Viewer [ViPNet.ccf]
File
Search
No
Protocol
MAC Addresses
IP Addresses
Ports
Delta
1 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.4 N/A 0,000
2 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.4 N/A 0,000
3 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.4 N/A 0,000
4 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.4 N/A 0,000
5 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.4 N/A 0,000
6 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.4 N/A 0,000
7 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.4 N/A 0,000
8 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.4 N/A 0,060
9 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.4 N/A 0,000
10 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.4 N/A 0,000
11 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.4 N/A 0,000
12 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.4 N/A 0,000
13 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.4 N/A 0,000
14 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.4 N/A 0,000
15 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 <= 192.168.1.4 N/A 0,000
16 IP/241... 00:C0:26:A6:3C:EA ... 192.168.1.1 => 192.168.1.4 N/A 0,000
0x0000 00 02 A5 AB D9 CC 00 C0-26 A6 3C EA 08 00 45 00 ..Г«ЩМ.А¦<к..E.
0x0010 00 94 56 00 00 00 80 F1-60 23 C0 A8 01 01 C0 A8 .“V...Ъс`#АЁ..АЁ
0x0020 01 04 E2 A8 F6 C5 CF AB-2E 57 3F 91 14 79 CC DA ..вЁцЕП«.W?`.yМЪ
0x0030 A3 D3 6A 0C B8 76 B3 9E-18 C8 42 80 55 19 AA A8 JУj.ёvіћ.ИВЂU.ЄЁ
0x0040 10 50 14 68 8F F7 F1 68-CE 75 3A B5 D5 A1 12 7F .P.hЏчchОu:µХЎ.□
0x0050 C0 CE D6 C5 CE C7 66 DA-AE B0 1F E7 13 23 0A 35 АОЦЕОЗfЪ®°.з.#.5
0x0060 E9 7B 2E 66 E7 C8 E7 66-CA 44 F9 FF 5F 74 60 AB й{.fзИзfКDщя_t`«
0x0070 F8 7F 90 61 32 E3 C3 7F-6E D5 68 CA 32 47 A9 7B шЉђа2гГ□nХhК2G©{
0x0080 39 EC B6 DD AD 10 E1 02-DF 07 FF FF FF FF 00 20 9мЉЭ-.б.Я.яяяя.
0x0090 07 26 A2 7C 5C 85 C5 96-10 E1 02 DE 01 0B 49 4C .&ў|\…Е-.б.Ю..IL
0x00A0 34 30 40
Ethernet II
Destination MAC: 00:02:A5:AB:D
Source MAC: 00:C0:26:A6:3C:EA
Ethertype: 0x0800 (2048) - IP
Direction: Out
Time / Delta Time: 17:24:13,610 /
Frame size: 162 bytes
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Total length: 0x0094 (148)
ID: 0x5600 (22016)
Flags
Fragment offset: 0x0000 (0)
Time to live: 0x80 (128)
Protocol: 0xF1 (241) - Unknown
Checksum: 0x6023 (24611) - corre
Source IP: 192.168.1.1
Destination IP: 192.168.1.4
IP Options: None

Уровни защищенных каналов

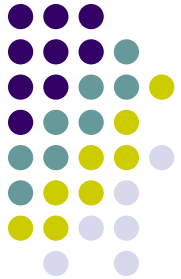


Прикладной	S/MIME /PGP /SHTTP
Транспортный (TCP/UDP)	SSL /TLS / SOCKS
Сетевой (IP)	IPSec / SKIP
Канальный	PPTP / L2F /L2TP

Защита на транспортном уровне



Защита на транспортном уровне



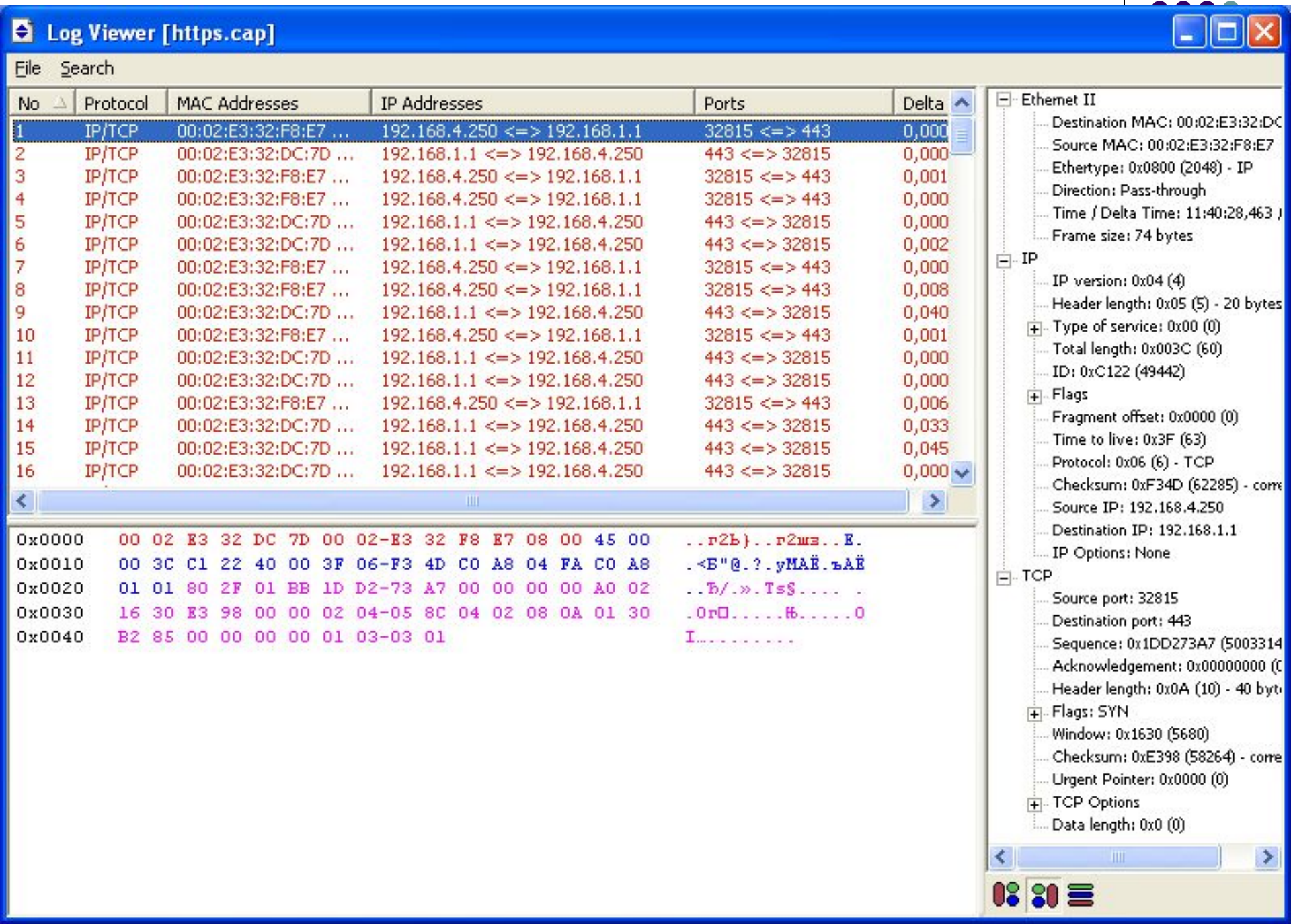
- Протокол SSL (Secure Socket Layer)
  - Netscape Communications, версия 3.0
- Протокол TLS (Transport Layer Secur)
  - 1999г., версия 1.0
- Независимость от прикладного уровня, чаще всего для HTTP (режим HTTPS)

Протокол SSL

- Аутентификация сервера (клиента редко)
  - Путем обмена цифровыми сертификатами при установлении сессии
- Шифрование данных
  - Симметричный сеансовый ключ
  - Обмен симметричными сеансовыми ключами при установлении соединения
  - Сеансовые ключи шифруются при передаче с помощью открытых ключей
- Целостность данных
  - К сообщению добавляется хеш-код

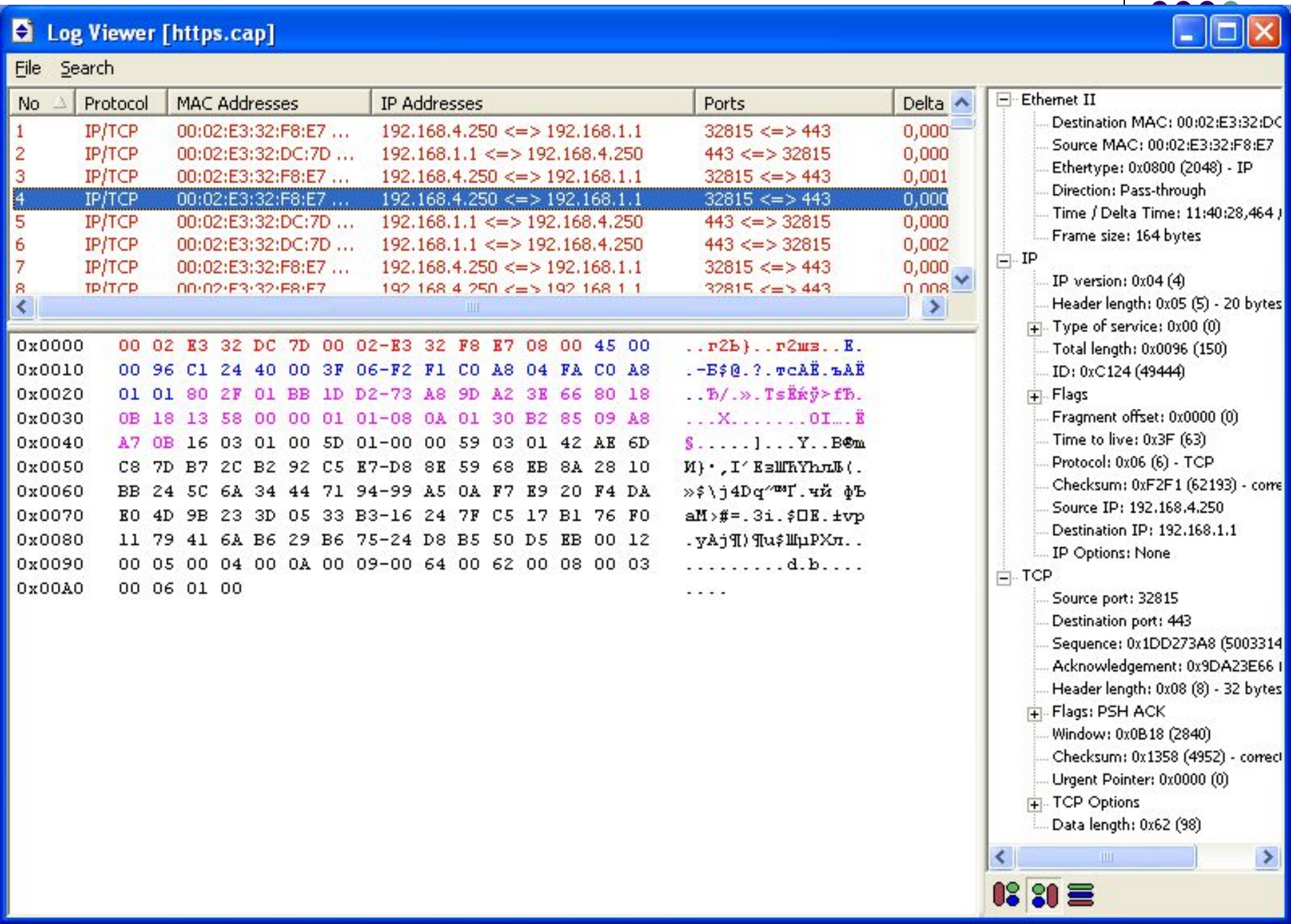
Этапы установки SSL-соединения

- Установка стандартного TCP-соединения, порт 443


Log Viewer [https.cap]
File
Search
No
Protocol
MAC Addresses
IP Addresses
Ports
Delta
1 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,000
2 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
3 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,001
4 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,000
5 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
6 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,002
7 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,000
8 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,008
9 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,040
10 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,001
11 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
12 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
13 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,006
14 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,033
15 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,045
16 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
0x0000 00 02 E3 32 DC 7D 00 02-E3 32 F8 E7 08 00 45 00
0x0010 00 3C C1 22 40 00 3F 06-F3 4D C0 A8 04 FA C0 A8
0x0020 01 01 80 2F 01 BB 1D D2-73 A7 00 00 00 00 A0 02
0x0030 16 30 E3 98 00 00 02 04-05 8C 04 02 08 0A 01 30
0x0040 B2 85 00 00 00 00 01 03-03 01
Ethernet II
Destination MAC: 00:02:E3:32:DC
Source MAC: 00:02:E3:32:F8:E7
Ethertype: 0x0800 (2048) - IP
Direction: Pass-through
Time / Delta Time: 11:40:28,463 /
Frame size: 74 bytes
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Total length: 0x003C (60)
ID: 0xC122 (49442)
Flags
Fragment offset: 0x0000 (0)
Time to live: 0x3F (63)
Protocol: 0x06 (6) - TCP
Checksum: 0xF34D (62285) - corr
Source IP: 192.168.4.250
Destination IP: 192.168.1.1
IP Options: None
TCP
Source port: 32815
Destination port: 443
Sequence: 0x1DD273A7 (5003314
Acknowledgement: 0x00000000 (
Header length: 0x0A (10) - 40 byt
Flags: SYN
Window: 0x1630 (5680)
Checksum: 0xE398 (58264) - corr
Urgent Pointer: 0x0000 (0)
TCP Options
Data length: 0x0 (0)

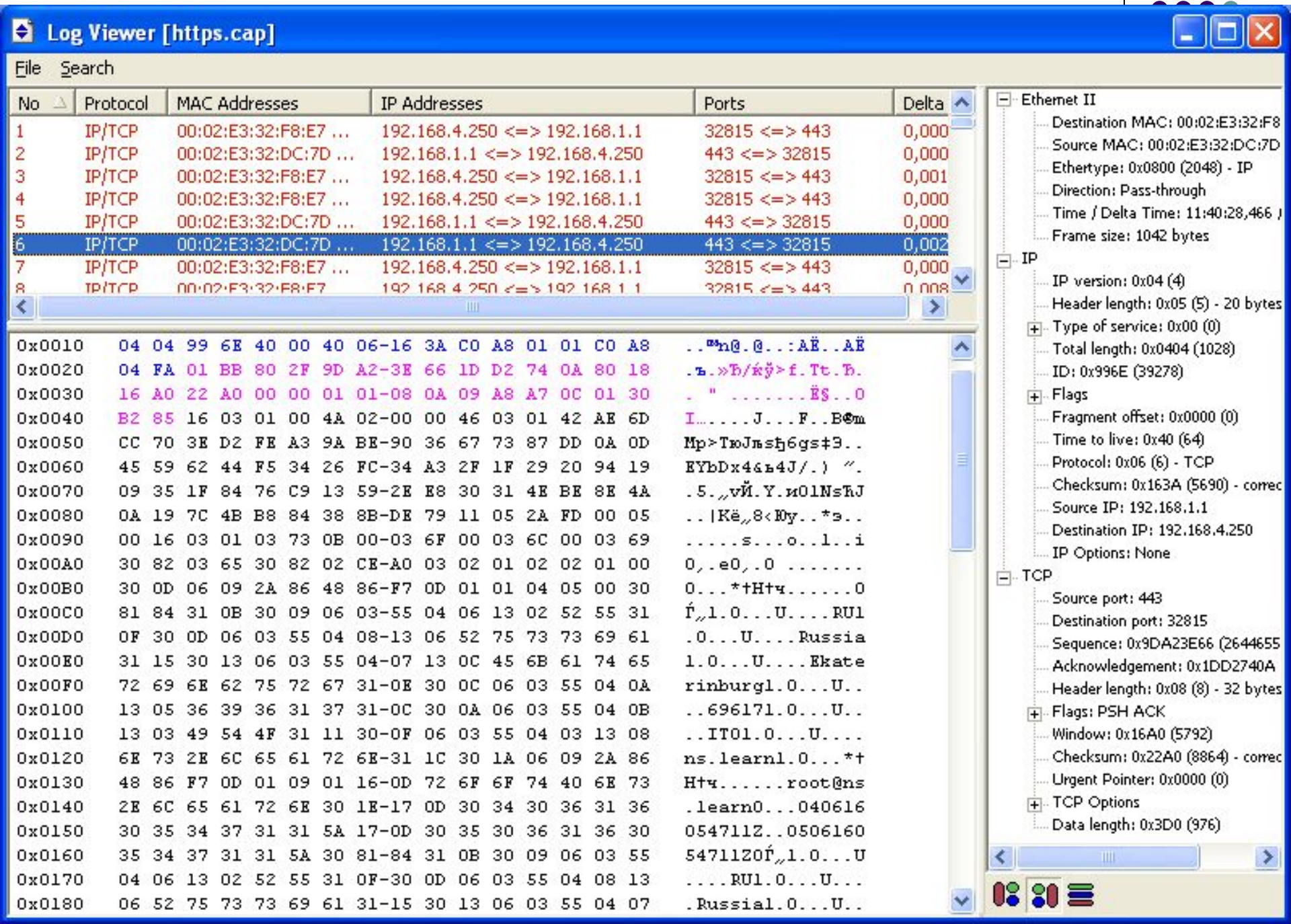
Этапы установки SSL-соединения

- Установка стандартного TCP-соединения, порт 443
- Сообщение Client-Hello
  - Версия SSL
  - Challenge_Data – случайная последовательность


Log Viewer [https.cap]
File
Search
No
Protocol
MAC Addresses
IP Addresses
Ports
Delta
1 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,000
2 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
3 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,001
4 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,000
5 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
6 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,002
7 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,000
0x0000 00 02 E3 32 DC 7D 00 02-E3 32 F8 E7 08 00 45 00
0x0010 00 96 C1 24 40 00 3F 06-F2 F1 C0 A8 04 FA C0 A8
0x0020 01 01 80 2F 01 BB 1D D2-73 A8 9D A2 3E 66 80 18
0x0030 0B 18 13 58 00 00 01 01-08 0A 01 30 B2 85 09 A8
0x0040 A7 0B 16 03 01 00 5D 01-00 00 59 03 01 42 AE 6D
0x0050 C8 7D B7 2C B2 92 C5 E7-D8 8E 59 68 EB 8A 28 10
0x0060 BB 24 5C 6A 34 44 71 94-99 A5 0A F7 E9 20 F4 DA
0x0070 E0 4D 9B 23 3D 05 33 B3-16 24 7F C5 17 B1 76 F0
0x0080 11 79 41 6A B6 29 B6 75-24 D8 B5 50 D5 EB 00 12
0x0090 00 05 00 04 00 0A 00 09-00 64 00 62 00 08 00 03
0x00A0 00 06 01 00
Ethernet II
Destination MAC: 00:02:E3:32:DC
Source MAC: 00:02:E3:32:F8:E7
Ethertype: 0x0800 (2048) - IP
Direction: Pass-through
Time / Delta Time: 11:40:28,464
Frame size: 164 bytes
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Total length: 0x0096 (150)
ID: 0xC124 (49444)
Flags
Fragment offset: 0x0000 (0)
Time to live: 0x3F (63)
Protocol: 0x06 (6) - TCP
Checksum: 0xF2F1 (62193) - corre
Source IP: 192.168.4.250
Destination IP: 192.168.1.1
IP Options: None
TCP
Source port: 32815
Destination port: 443
Sequence: 0x1DD273A8 (5003314
Acknowledgement: 0x9DA23E66
Header length: 0x08 (8) - 32 bytes
Flags: PSH ACK
Window: 0x0B18 (2840)
Checksum: 0x1358 (4952) - correct
Urgent Pointer: 0x0000 (0)
TCP Options
Data length: 0x62 (98)

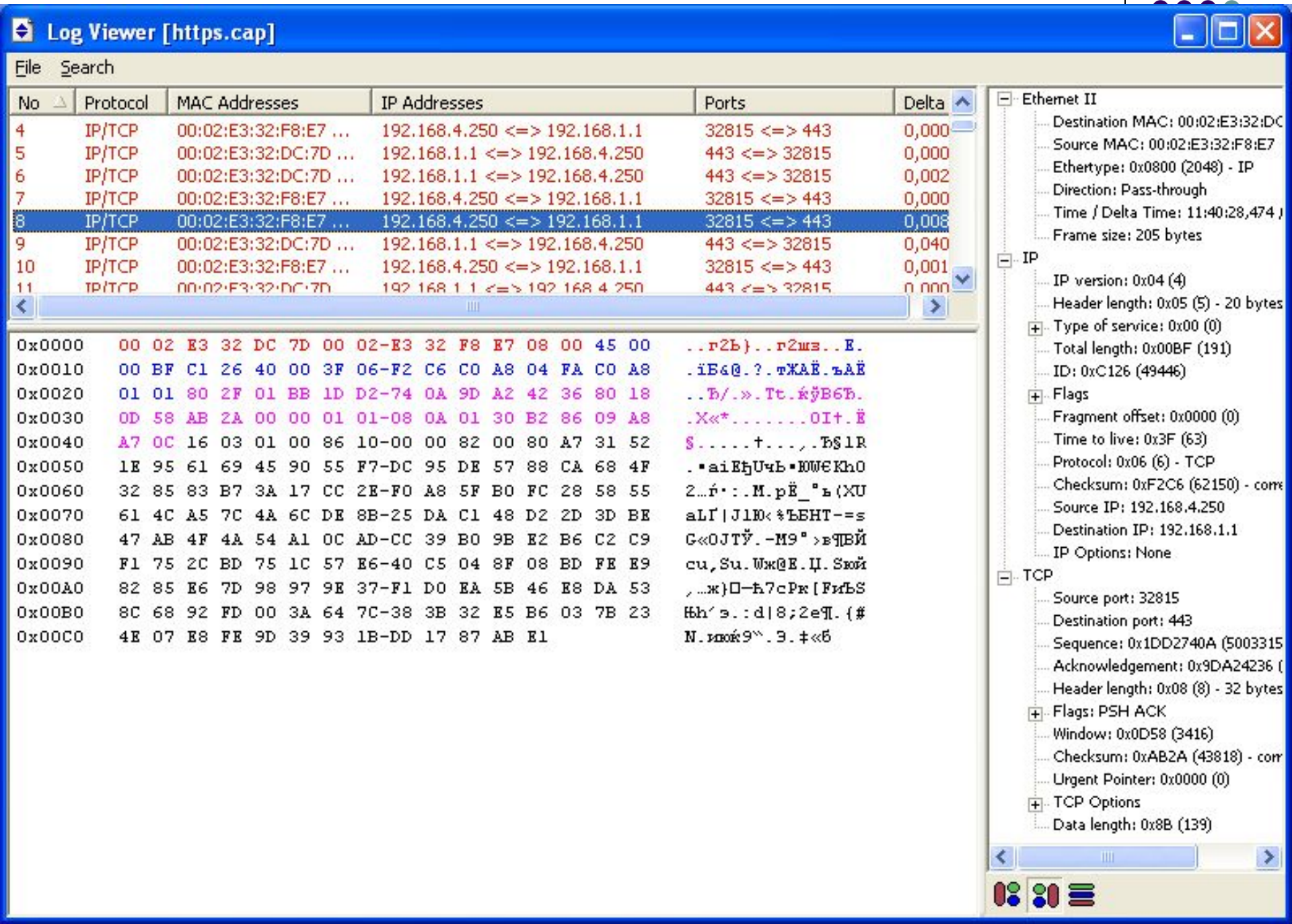
Этапы установки SSL-соединения

- Установка стандартного TCP-соединения, порт 443
- Сообщение Client-Hello
- Сообщение Server-Hello
  - Версия SSL
  - Идентификатор соединения Connection_id
  - Список базовых шифров (протоколов)
  - Сертификат сервера (подписанный открытый ключ)


Log Viewer [https.cap]
File
Search
No
Protocol
MAC Addresses
IP Addresses
Ports
Delta
1 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,000
2 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
3 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,001
4 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,000
5 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
6 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,002
7 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,000
0x0010 04 04 99 6E 40 00 40 06-16 3A C0 A8 01 01 C0 A8
0x0020 04 FA 01 BB 80 2F 9D A2-3E 66 1D D2 74 0A 80 18
0x0030 16 A0 22 A0 00 00 01 01-08 0A 09 A8 A7 0C 01 30
0x0040 B2 85 16 03 01 00 4A 02-00 00 46 03 01 42 AE 6D
0x0050 CC 70 3E D2 FE A3 9A BE-90 36 67 73 87 DD 0A 0D
0x0060 45 59 62 44 F5 34 26 FC-34 A3 2F 1F 29 20 94 19
0x0070 09 35 1F 84 76 C9 13 59-2E E8 30 31 4E BE 8E 4A
0x0080 0A 19 7C 4B B8 84 38 8B-DE 79 11 05 2A FD 00 05
0x0090 00 16 03 01 03 73 0B 00-03 6F 00 03 6C 00 03 69
0x00A0 30 82 03 65 30 82 02 CE-A0 03 02 01 02 02 01 00
0x00B0 30 0D 06 09 2A 86 48 86-F7 0D 01 01 04 05 00 30
0x00C0 81 84 31 0B 30 09 06 03-55 04 06 13 02 52 55 31
0x00D0 0F 30 0D 06 03 55 04 08-13 06 52 75 73 73 69 61
0x00E0 31 15 30 13 06 03 55 04-07 13 0C 45 6B 61 74 65
0x00F0 72 69 6E 62 75 72 67 31-0E 30 0C 06 03 55 04 0A
0x0100 13 05 36 39 36 31 37 31-0C 30 0A 06 03 55 04 0B
0x0110 13 03 49 54 4F 31 11 30-0F 06 03 55 04 03 13 08
0x0120 6E 73 2E 6C 65 61 72 6E-31 1C 30 1A 06 09 2A 86
0x0130 48 86 F7 0D 01 09 01 16-0D 72 6F 6F 74 40 6E 73
0x0140 2E 6C 65 61 72 6E 30 1E-17 0D 30 34 30 36 31 36
0x0150 30 35 34 37 31 31 5A 17-0D 30 35 30 36 31 36 30
0x0160 35 34 37 31 31 5A 30 81-84 31 0B 30 09 06 03 55
0x0170 04 06 13 02 52 55 31 0F-30 0D 06 03 55 04 08 13
0x0180 06 52 75 73 73 69 61 31-15 30 13 06 03 55 04 07
Ethernet II
Destination MAC: 00:02:E3:32:F8
Source MAC: 00:02:E3:32:DC:7D
Ethertype: 0x0800 (2048) - IP
Direction: Pass-through
Time / Delta Time: 11:40:28,466 /
Frame size: 1042 bytes
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Total length: 0x0404 (1028)
ID: 0x996E (39278)
Flags
Fragment offset: 0x0000 (0)
Time to live: 0x40 (64)
Protocol: 0x06 (6) - TCP
Checksum: 0x163A (5690) - correc
Source IP: 192.168.1.1
Destination IP: 192.168.4.250
IP Options: None
TCP
Source port: 443
Destination port: 32815
Sequence: 0x9DA23E66 (2644655
Acknowledgement: 0x1DD2740A
Header length: 0x08 (8) - 32 bytes
Flags: PSH ACK
Window: 0x16A0 (5792)
Checksum: 0x22A0 (8864) - correc
Urgent Pointer: 0x0000 (0)
TCP Options
Data length: 0x3D0 (976)

Этапы установки SSL-соединения

- Установка стандартного TCP-соединения, порт 443
- Сообщение Client-Hello
- Сообщение Server-Hello
- Сообщение Client_Master_Key
  - Передача симметричного ключа, зашифрованного открытым ключом сервера
  - Только сервер может расшифровать симметричный ключ


Log Viewer [https.cap]
File
Search
No
Protocol
MAC Addresses
IP Addresses
Ports
Delta
4 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,000
5 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
6 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,002
7 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,000
8 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,008
9 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,040
10 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,001
0x0000 00 02 E3 32 DC 7D 00 02-E3 32 F8 E7 08 00 45 00
0x0010 00 BF C1 26 40 00 3F 06-F2 C6 C0 A8 04 FA C0 A8
0x0020 01 01 80 2F 01 BB 1D D2-74 0A 9D A2 42 36 80 18
0x0030 0D 58 AB 2A 00 00 01 01-08 0A 01 30 B2 86 09 A8
0x0040 A7 0C 16 03 01 00 86 10-00 00 82 00 80 A7 31 52
0x0050 1E 95 61 69 45 90 55 F7-DC 95 DE 57 88 CA 68 4F
0x0060 32 85 83 B7 3A 17 CC 2E-F0 A8 5F B0 FC 28 58 55
0x0070 61 4C A5 7C 4A 6C DE 8B-25 DA C1 48 D2 2D 3D BE
0x0080 47 AB 4F 4A 54 A1 0C AD-CC 39 B0 9B E2 B6 C2 C9
0x0090 F1 75 2C BD 75 1C 57 E6-40 C5 04 8F 08 BD FE E9
0x00A0 82 85 E6 7D 98 97 9E 37-F1 D0 EA 5B 46 E8 DA 53
0x00B0 8C 68 92 FD 00 3A 64 7C-38 3B 32 E5 B6 03 7B 23
0x00C0 4E 07 E8 FE 9D 39 93 1B-DD 17 87 AB E1
Ethernet II
Destination MAC: 00:02:E3:32:DC
Source MAC: 00:02:E3:32:F8:E7
Ethertype: 0x0800 (2048) - IP
Direction: Pass-through
Time / Delta Time: 11:40:28,474 /
Frame size: 205 bytes
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Total length: 0x00BF (191)
ID: 0xC126 (49446)
Flags
Fragment offset: 0x0000 (0)
Time to live: 0x3F (63)
Protocol: 0x06 (6) - TCP
Checksum: 0xF2C6 (62150) - corr
Source IP: 192.168.4.250
Destination IP: 192.168.1.1
IP Options: None
TCP
Source port: 32815
Destination port: 443
Sequence: 0x1DD2740A (5003315
Acknowledgement: 0x9DA24236 (
Header length: 0x08 (8) - 32 bytes
Flags: PSH ACK
Window: 0x0D58 (3416)
Checksum: 0xAB2A (43818) - corr
Urgent Pointer: 0x0000 (0)
TCP Options
Data length: 0x8B (139)

Этапы установки SSL-соединения

- Установка стандартного TCP-соединения, порт 443
- Сообщение Client-Hello
- Сообщение Server-Hello
- Сообщение Client_Master_Key
- Сообщение Server-Verify
  - Challenge_Data, зашифрованная симметричным ключом

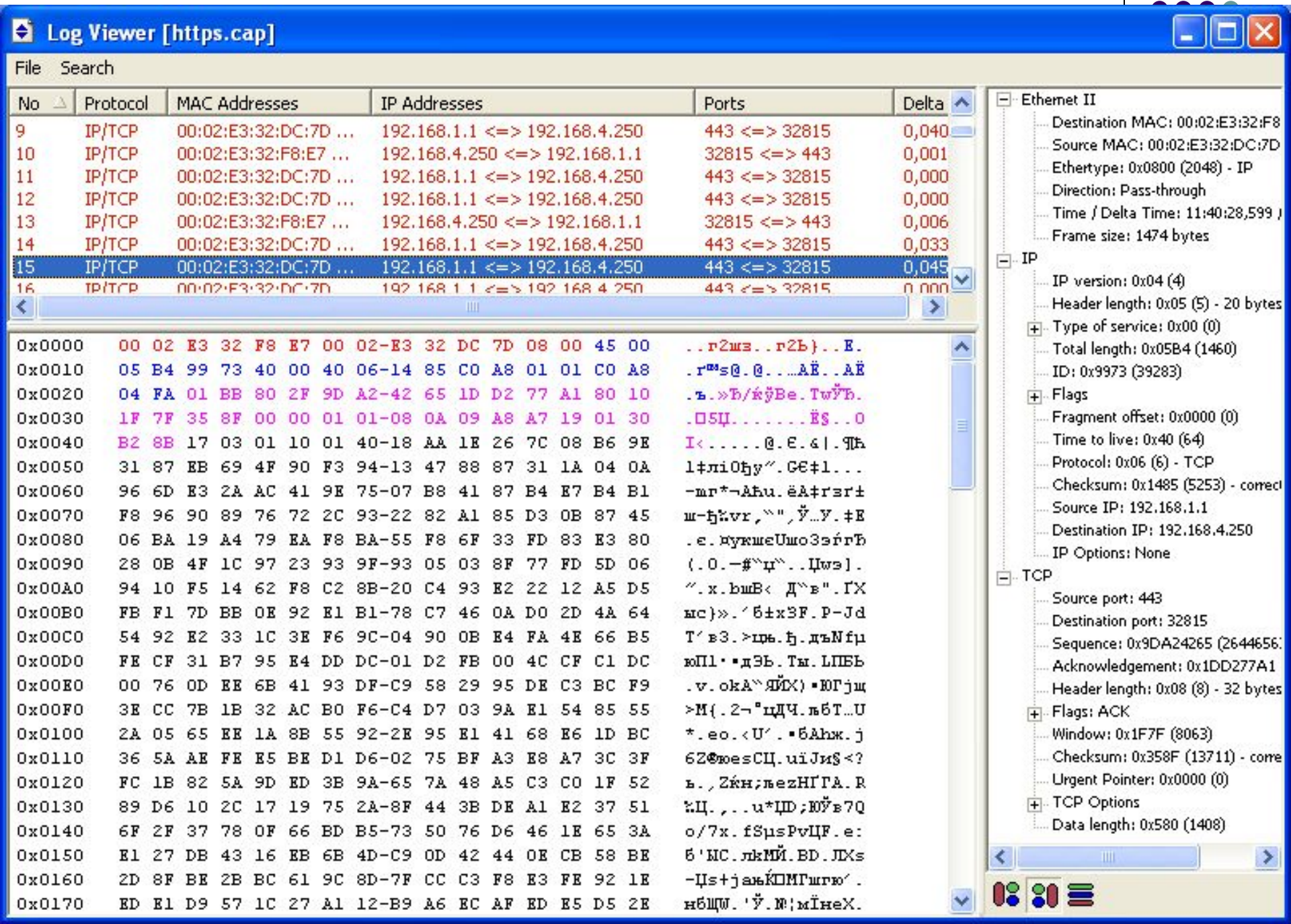
Этапы установки SSL-соединения

- Установка стандартного TCP-соединения, порт 443
- Сообщение Client-Hello
- Сообщение Server-Hello
- Сообщение Client_Master_Key
- Сообщение Server-Verify
- Сообщение Client-Finished
  - Идентификатор соединения Connection_id, зашифрованный клиентом

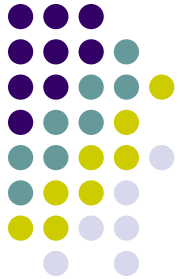
Этапы установки SSL-соединения

- Установка стандартного TCP-соединения, порт 443
- Сообщение Client-Hello
- Сообщение Server-Hello
- Сообщение Client_Master_Key
- Сообщение Server-Verify
- Сообщение Client-Finished

- Соединение установлено, сервер проверен

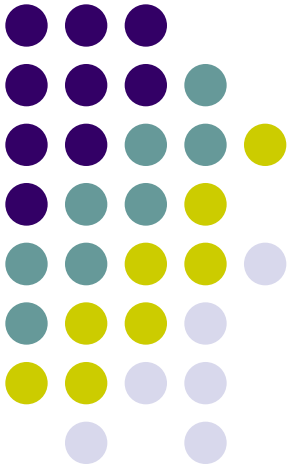

Log Viewer [https.cap]
File
Search
No
Protocol
MAC Addresses
IP Addresses
Ports
Delta
9 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,040
10 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,001
11 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
12 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,000
13 IP/TCP 00:02:E3:32:F8:E7 ... 192.168.4.250 <=> 192.168.1.1 32815 <=> 443 0,006
14 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,033
15 IP/TCP 00:02:E3:32:DC:7D ... 192.168.1.1 <=> 192.168.4.250 443 <=> 32815 0,045
0x0000 00 02 E3 32 F8 E7 00 02-E3 32 DC 7D 08 00 45 00
0x0010 05 B4 99 73 40 00 40 06-14 85 C0 A8 01 01 C0 A8
0x0020 04 FA 01 BB 80 2F 9D A2-42 65 1D D2 77 A1 80 10
0x0030 1F 7F 35 8F 00 00 01 01-08 0A 09 A8 A7 19 01 30
0x0040 B2 8B 17 03 01 10 01 40-18 AA 1E 26 7C 08 B6 9E
0x0050 31 87 EB 69 4F 90 F3 94-13 47 88 87 31 1A 04 0A
0x0060 96 6D E3 2A AC 41 9E 75-07 B8 41 87 B4 E7 B4 B1
0x0070 F8 96 90 89 76 72 2C 93-22 82 A1 85 D3 0B 87 45
0x0080 06 BA 19 A4 79 EA F8 BA-55 F8 6F 33 FD 83 E3 80
0x0090 28 0B 4F 1C 97 23 93 9F-93 05 03 8F 77 FD 5D 06
0x00A0 94 10 F5 14 62 F8 C2 8B-20 C4 93 E2 22 12 A5 D5
0x00B0 FB F1 7D BB 0E 92 E1 B1-78 C7 46 0A D0 2D 4A 64
0x00C0 54 92 E2 33 1C 3E F6 9C-04 90 0B E4 FA 4E 66 B5
0x00D0 FE CF 31 B7 95 E4 DD DC-01 D2 FB 00 4C CF C1 DC
0x00E0 00 76 0D EE 6B 41 93 DF-C9 58 29 95 DE C3 BC F9
0x00F0 3E CC 7B 1B 32 AC B0 F6-C4 D7 03 9A E1 54 85 55
0x0100 2A 05 65 EE 1A 8B 55 92-2E 95 E1 41 68 E6 1D BC
0x0110 36 5A AE FE E5 BE D1 D6-02 75 BF A3 E8 A7 3C 3F
0x0120 FC 1B 82 5A 9D ED 3B 9A-65 7A 48 A5 C3 C0 1F 52
0x0130 89 D6 10 2C 17 19 75 2A-8F 44 3B DE A1 E2 37 51
0x0140 6F 2F 37 78 0F 66 BD B5-73 50 76 D6 46 1E 65 3A
0x0150 E1 27 DB 43 16 EB 6B 4D-C9 0D 42 44 0E CB 58 BE
0x0160 2D 8F BE 2B BC 61 9C 8D-7F CC C3 F8 E3 FE 92 1E
0x0170 ED E1 D9 57 1C 27 A1 12-B9 A6 EC AF ED E5 D5 2E
Ethernet II
Destination MAC: 00:02:E3:32:F8
Source MAC: 00:02:E3:32:DC:7D
Ethertype: 0x0800 (2048) - IP
Direction: Pass-through
Time / Delta Time: 11:40:28,599 /
Frame size: 1474 bytes
IP
IP version: 0x04 (4)
Header length: 0x05 (5) - 20 bytes
Type of service: 0x00 (0)
Total length: 0x05B4 (1460)
ID: 0x9973 (39283)
Flags
Fragment offset: 0x0000 (0)
Time to live: 0x40 (64)
Protocol: 0x06 (6) - TCP
Checksum: 0x1485 (5253) - correct
Source IP: 192.168.1.1
Destination IP: 192.168.4.250
IP Options: None
TCP
Source port: 443
Destination port: 32815
Sequence: 0x9DA24265 (2644656
Acknowledgement: 0x1DD277A1
Header length: 0x08 (8) - 32 bytes
Flags: ACK
Window: 0x1F7F (8063)
Checksum: 0x358F (13711) - corre
Urgent Pointer: 0x0000 (0)
TCP Options
Data length: 0x580 (1408)

Уровни защищенных каналов

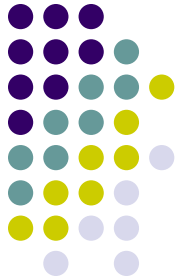


Прикладной	S/MIME /PGP /SHTTP
Транспортный (TCP/UDP)	SSL /TLS / SOCKS
Сетевой (IP)	IPSec / SKIP
Канальный	PPTP / L2F /L2TP

Защита на прикладном уровне

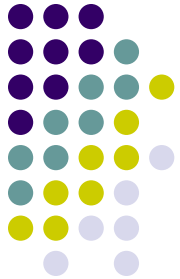


Защита на прикладном уровне



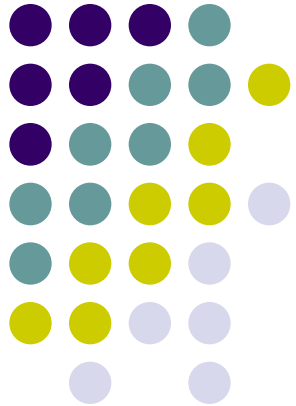
- S-HTTP – Secure HTTP
- Не требует сертификата открытого ключа
- Режим операции – шифрование или подписывание
- Криптографические алгоритмы
- Сертификаты
- Аутентификация

Инкапсуляция HTTP

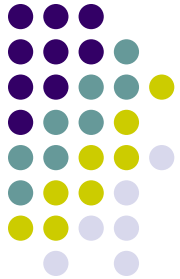


- Сообщение S-HTTP состоит из:
  - Строки запроса (с указанием версии протокола)
    - Запрос: Secure * Secure-HTTP/1.1
    - Ответ: Secure-HTTP/1.1 200 OK
  - Заголовки RFC-822
  - Инкапсулированное содержание

ЗАЩИТА СЕТЕВОГО ТРАФИКА С ИСПОЛЬЗОВАНИЕМ ПРОТОКОЛА IPSec В WINDOWS 2000.XP

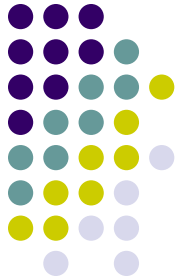


Возможности IPSec



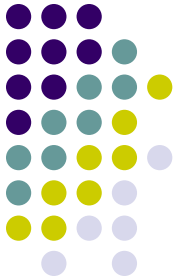
- Аутентификация (протокол IKE - Internet Key Exchange)
- Защита целостности (Заголовок аутентификации AH - Authentication Header)
- Шифрование (ESP - Encapsulating Security Payload)

Режимы действия IPSec



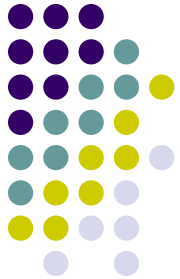
- Транспортный режим
- Туннельный режим

Режимы действия IPSec



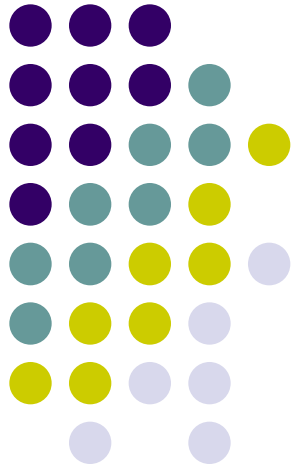
- Транспортный режим
  - Защита соединения между клиентом и сервером
- Туннельный режим

Режимы действия IPSec

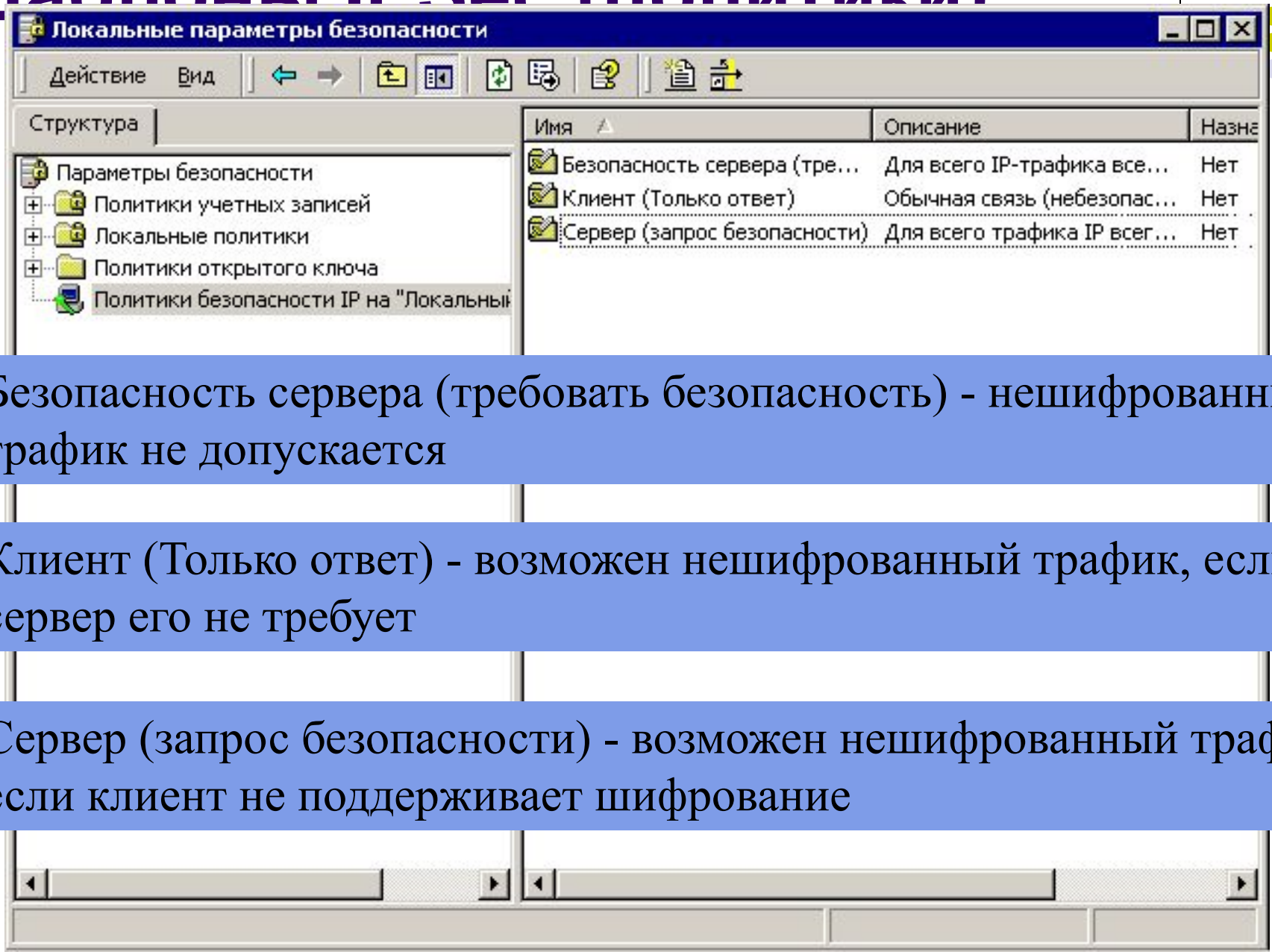


- Транспортный режим
- Туннельный режим
  - Защищенное соединение между двумя защищенными шлюзами (МЭ). Пропускается IP-трафик в «IP- туннеле». Сами клиент и сервер могут не использовать IPSec
  - Создание VPN - Виртуальной частной сети

Настройка IPSec



Шаблоны IPSec (политики)

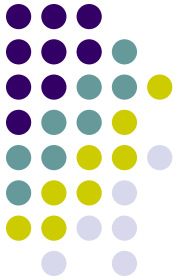


Безопасность сервера (требовать безопасность) - нешифрованный трафик не допускается

Клиент (Только ответ) - возможен нешифрованный трафик, если сервер его не требует

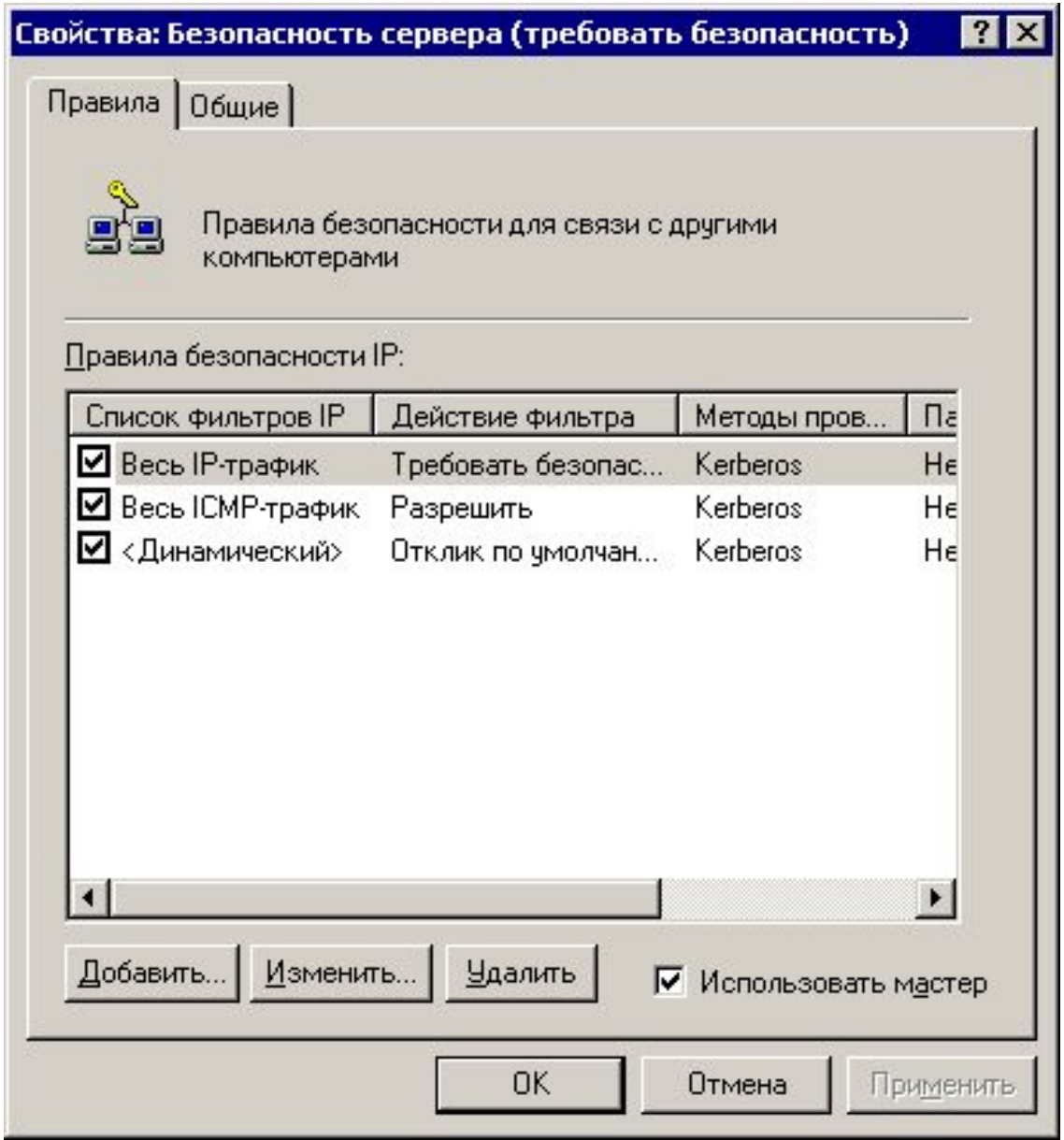
Сервер (запрос безопасности) - возможен нешифрованный трафик, если клиент не поддерживает шифрование

Политики и правила

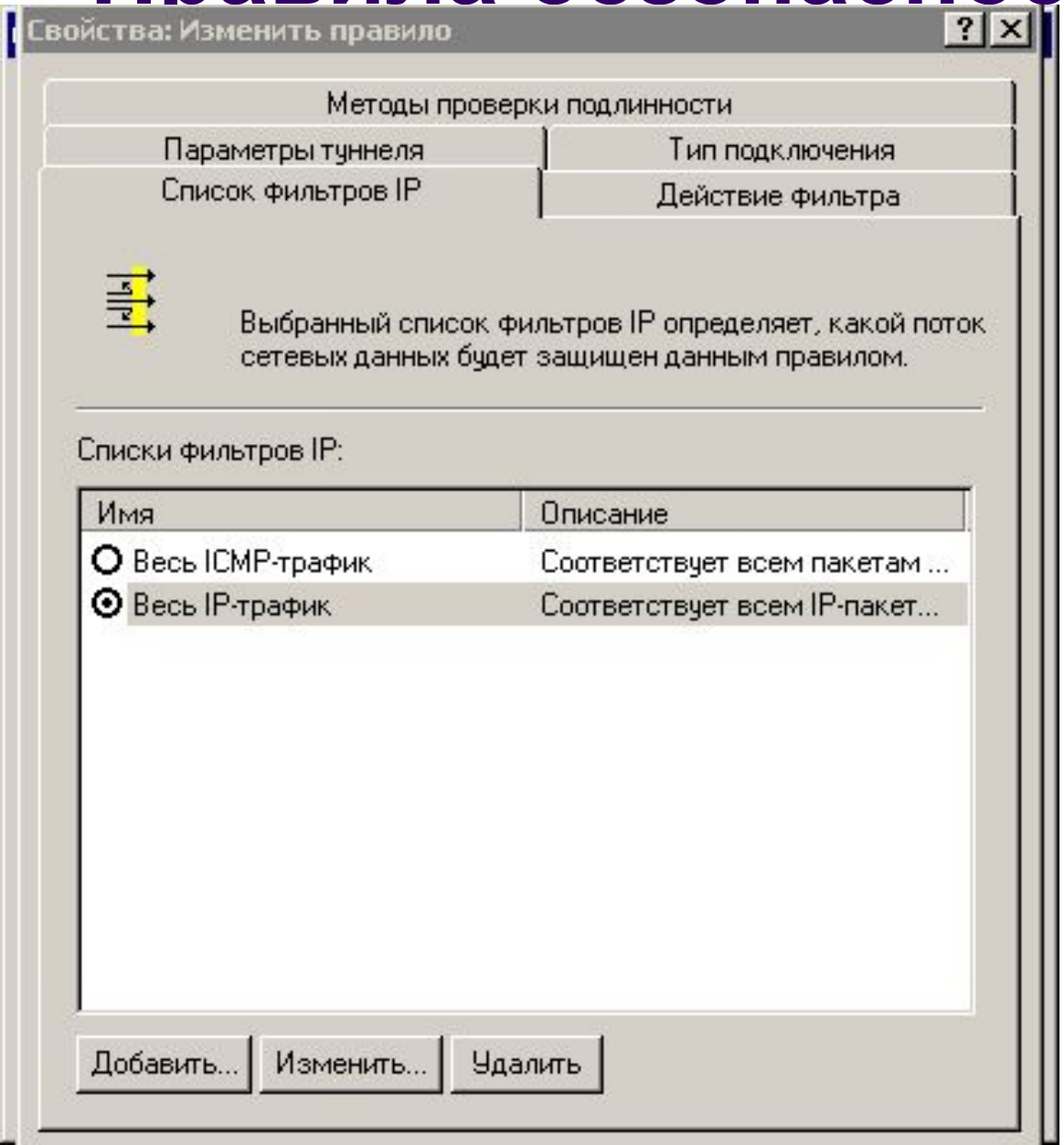


- Только одна политика может быть назначена
- Политика состоит из нескольких правил
- Правило определяет, какое действие предпринять, если будет найдено соответствие списку фильтров

Правила безопасности

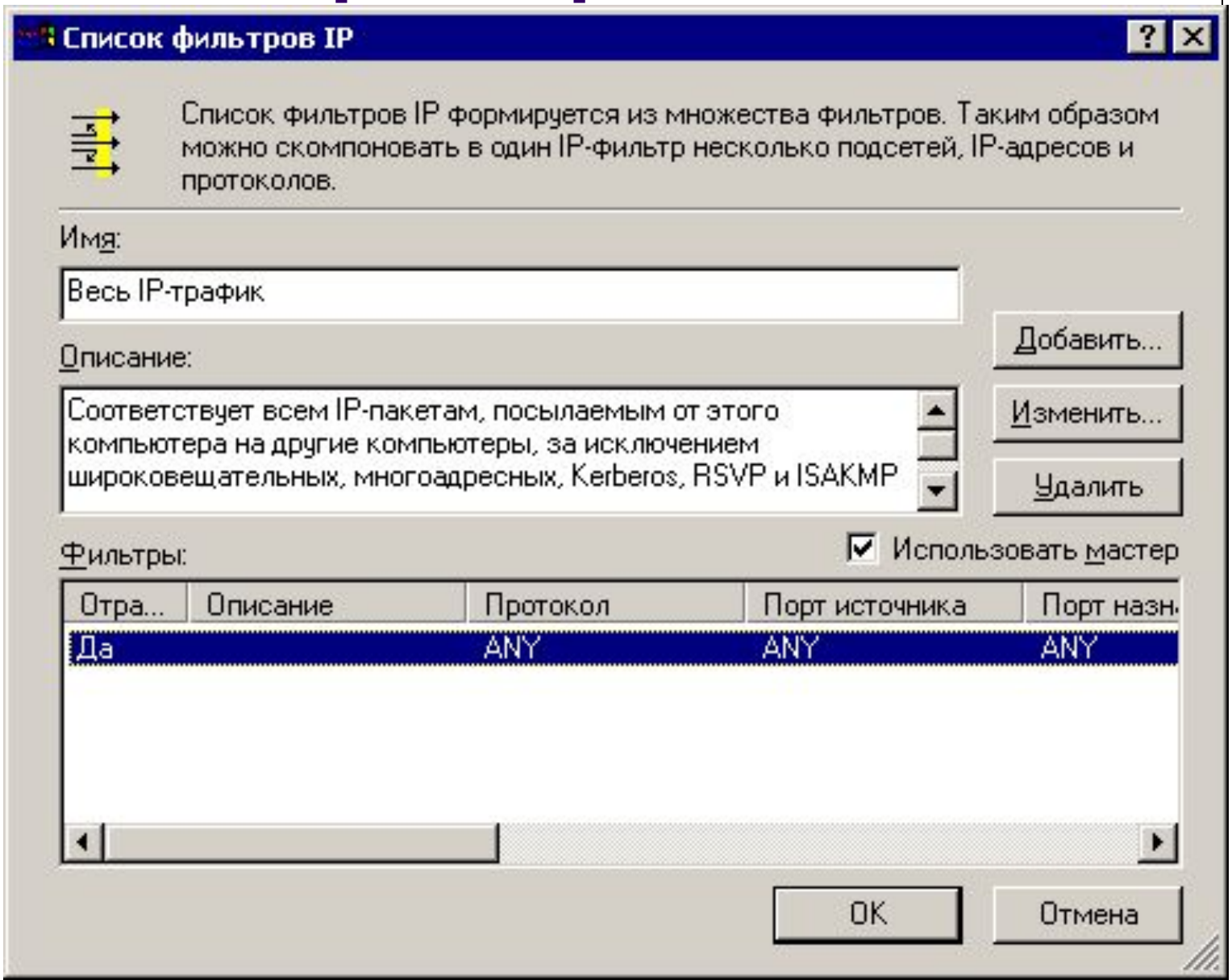


Правила безопасности

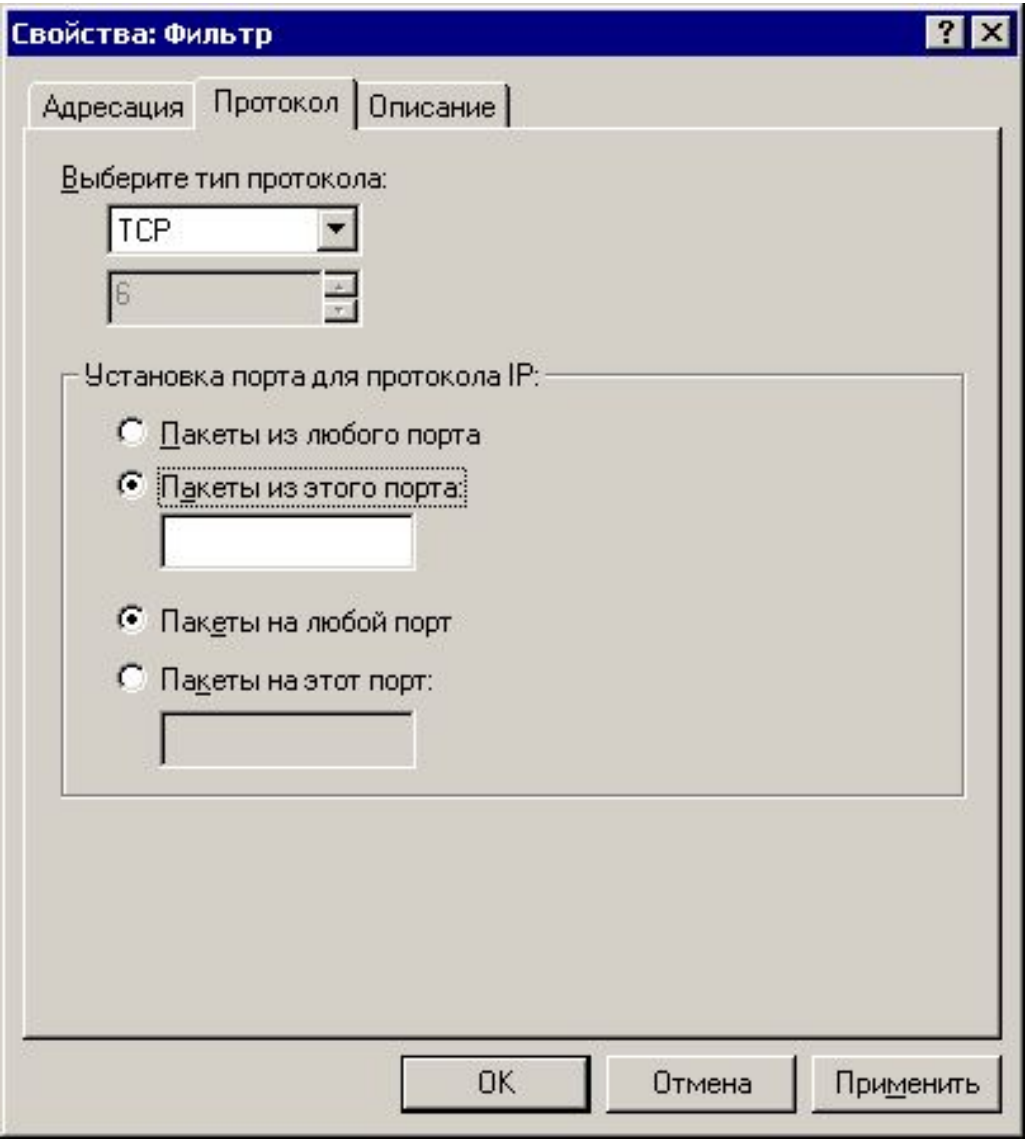


- Список фильтров
- Действие
- Тип подключения
- Параметры туннеля
- Метод проверки подлинности

Список фильтров

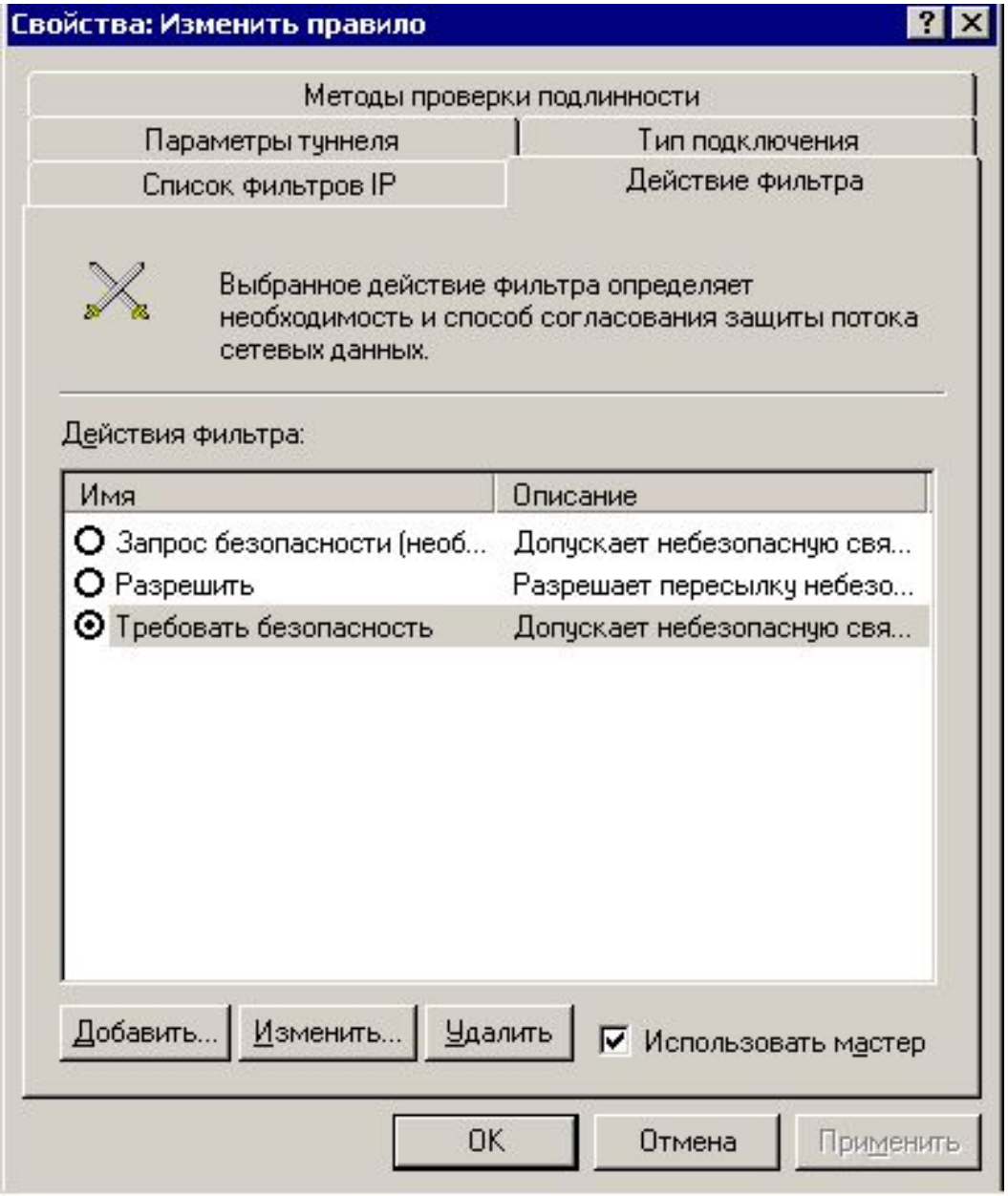


Список фильтров



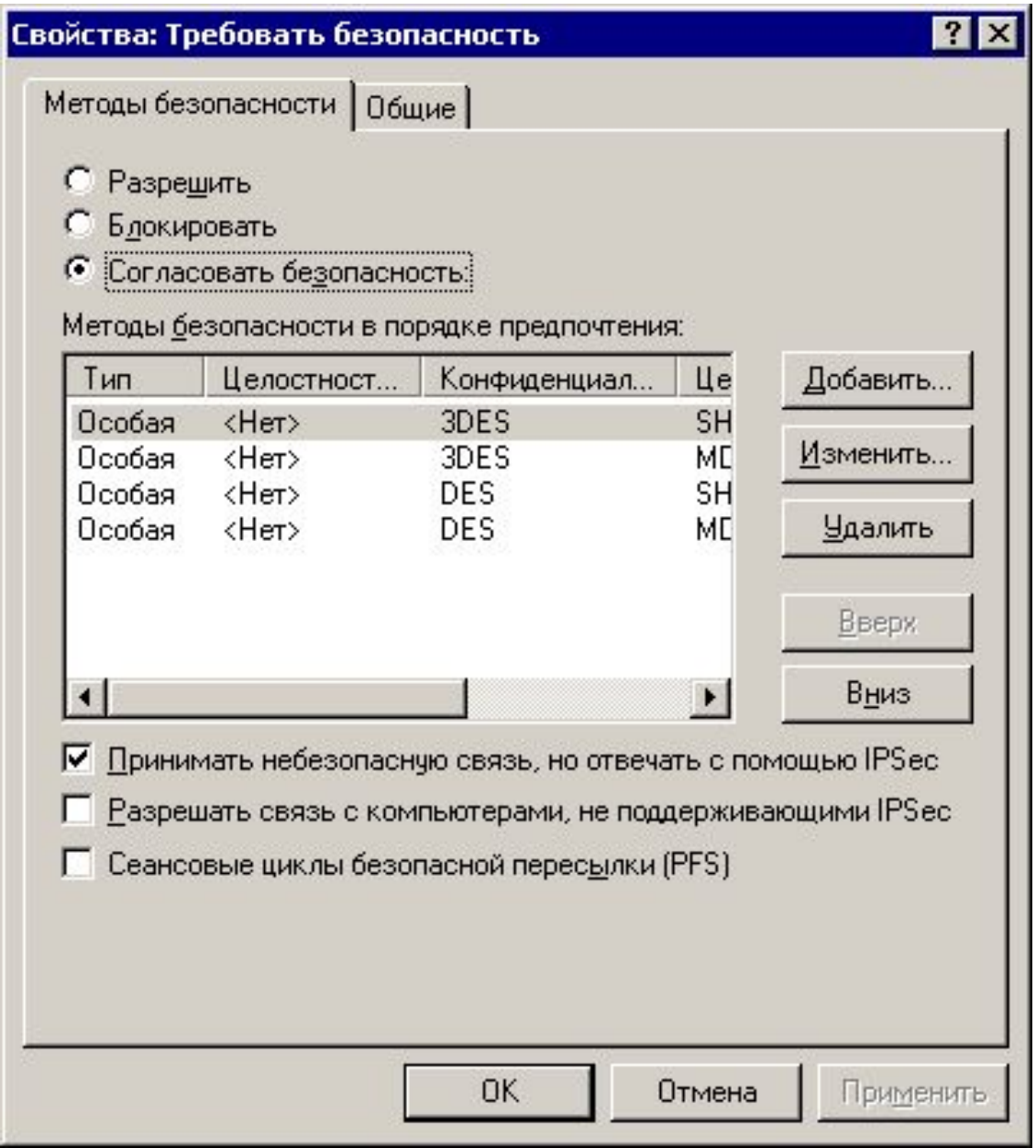
- Адрес источника
- Адрес назначения
  - Тип протокола
  - Порт источника
  - Порт приемника

Действие



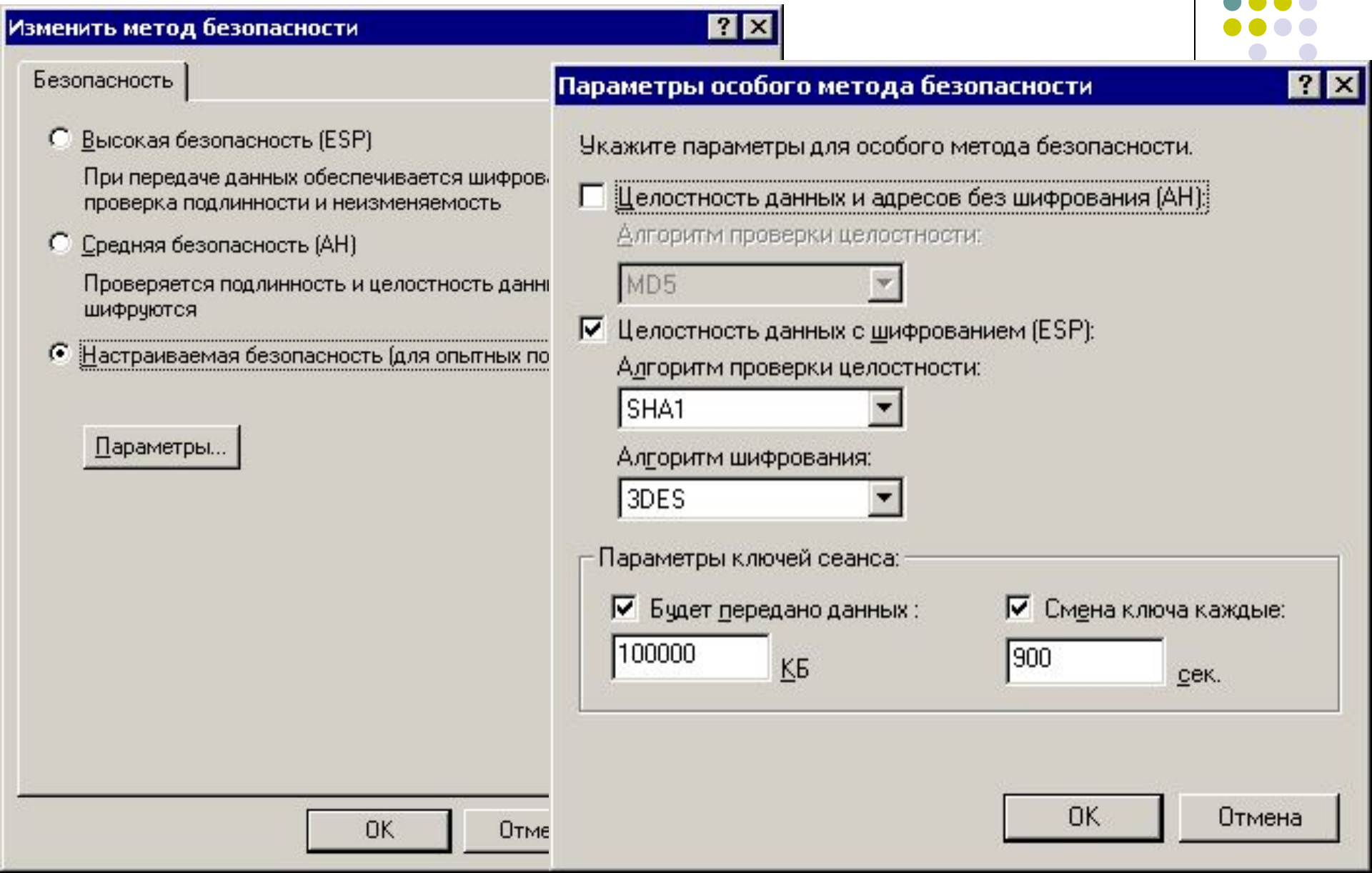
- Если найдено соответствие какому-либо фильтру из списка, принимается действие

Действие

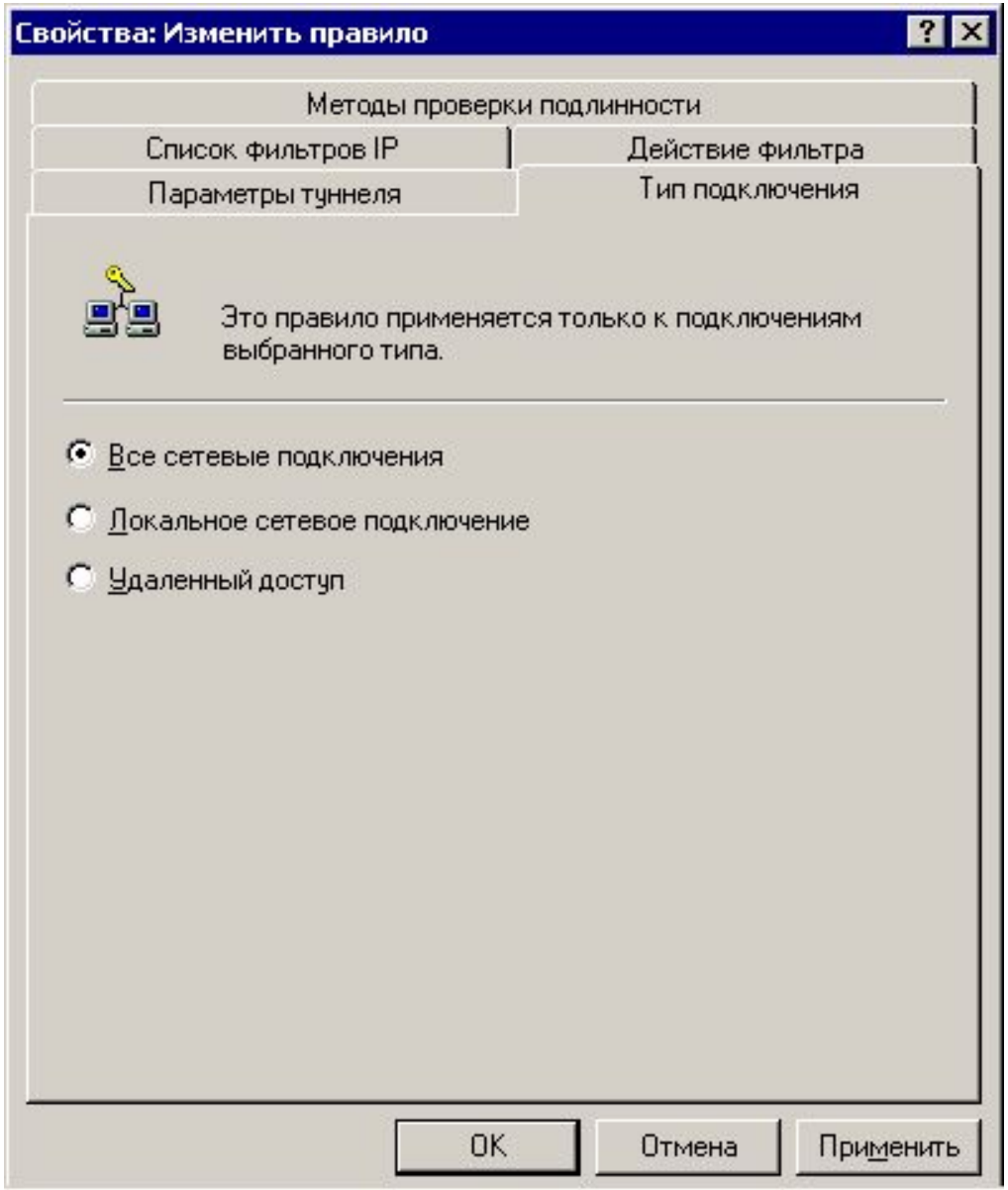


- Разрешить
- Блокировать
- Выбрать метод безопасности

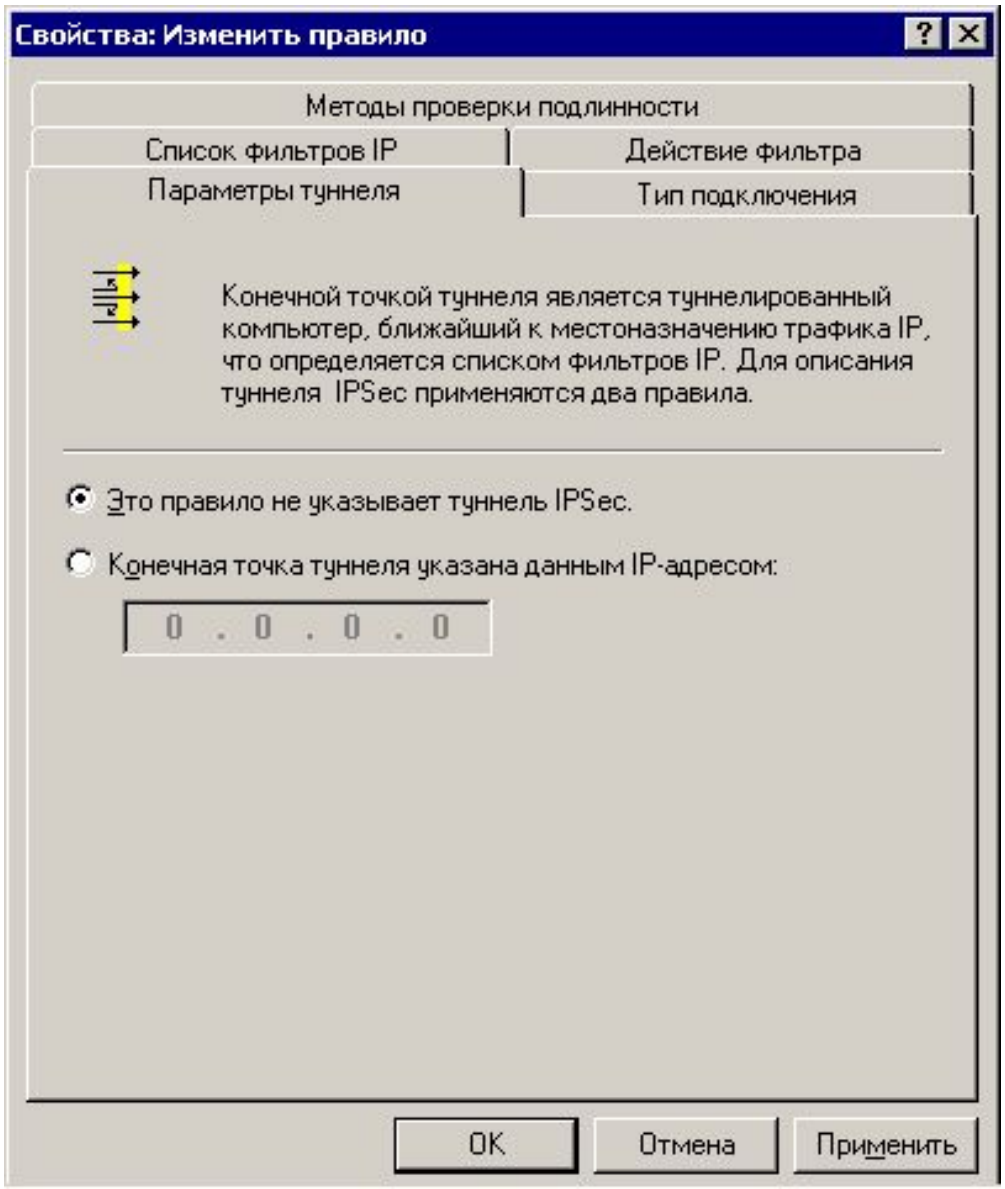
Метод безопасности



Тип подключения

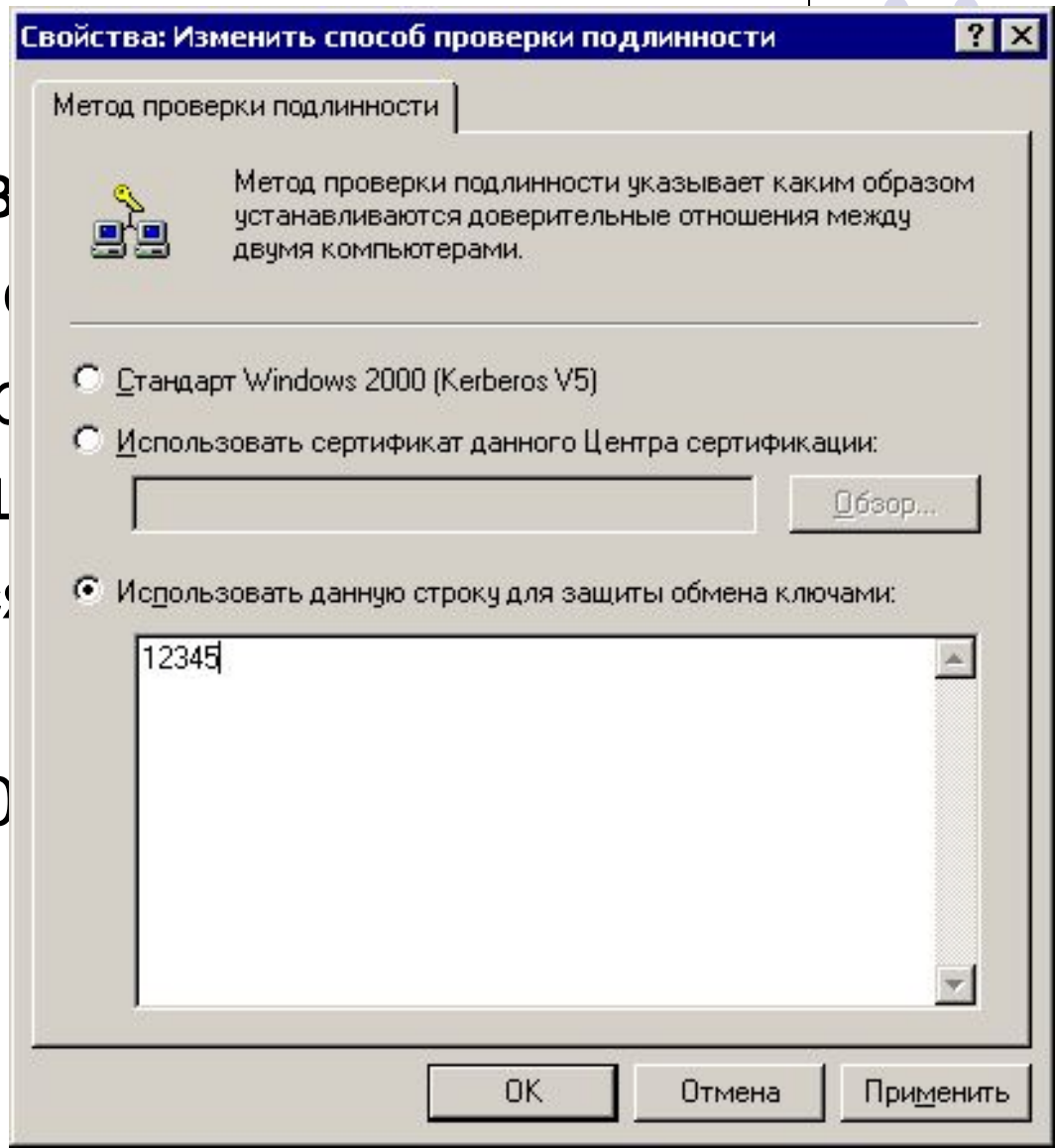


Параметры туннеля

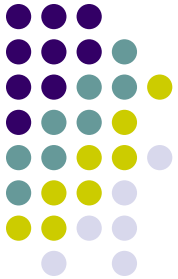


Методы проверки подлинности

- Использование раз
  - Ограниченное числ
- Подписывание откр
ключами при помо
  - Ключи генерируютс
- Протокол Kerberos
  - Домен Windows 200

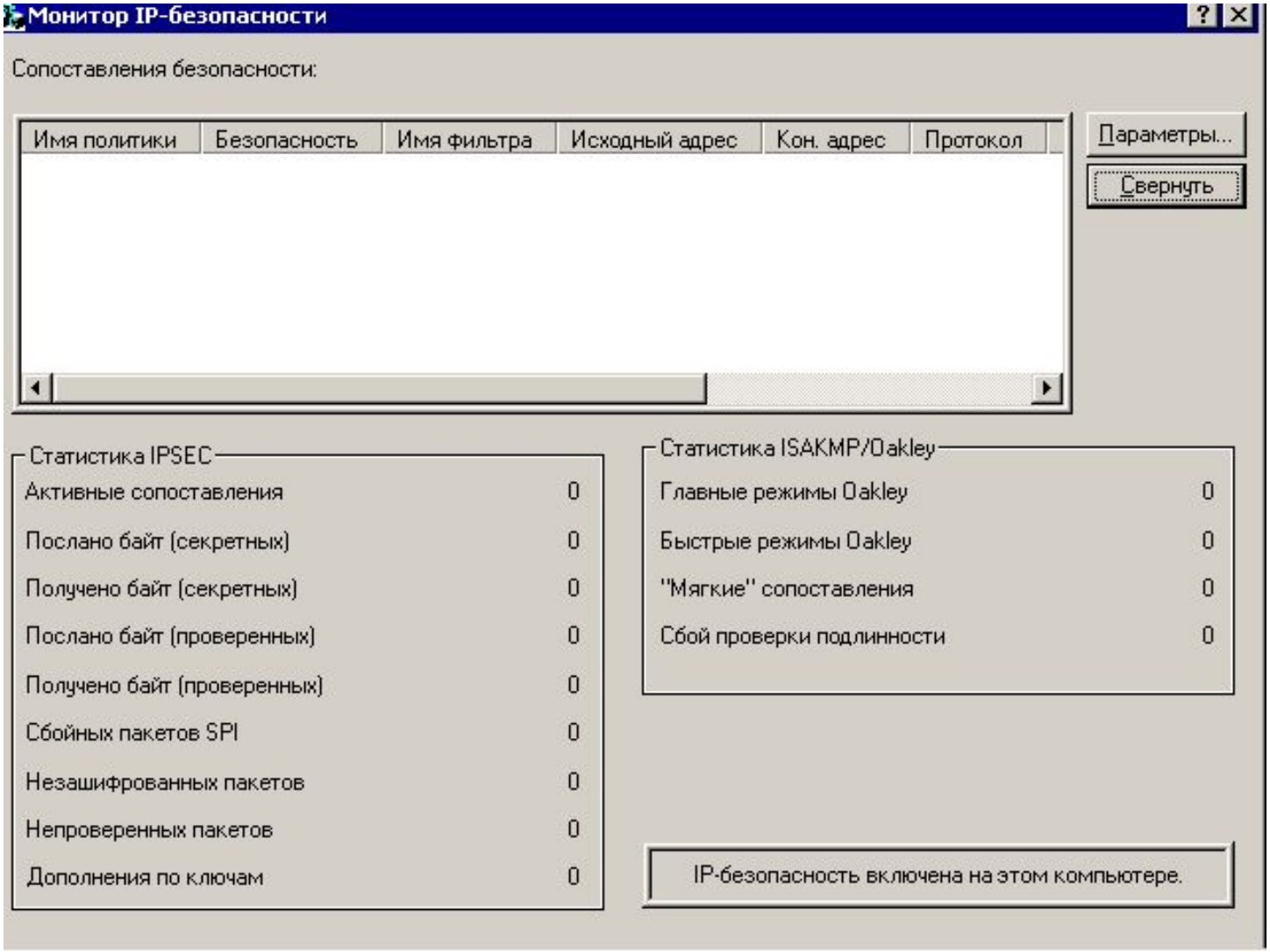


Политика IPSec

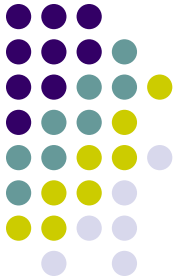


- Разрешенные типы сетевого взаимодействия
- Требуется ли IPSec для соединения
  - тип аутентификации для установки сессии
  - тип шифрования и/или целостности данных
- Пример:
  - соединение с SQL-сервером должно аутентифицироваться при помощи сертификатов X.509 и должно быть зашифровано с помощью 3-DES

Проверка соединения IPSec - IP Security Monitor (ipsecmon.exe)

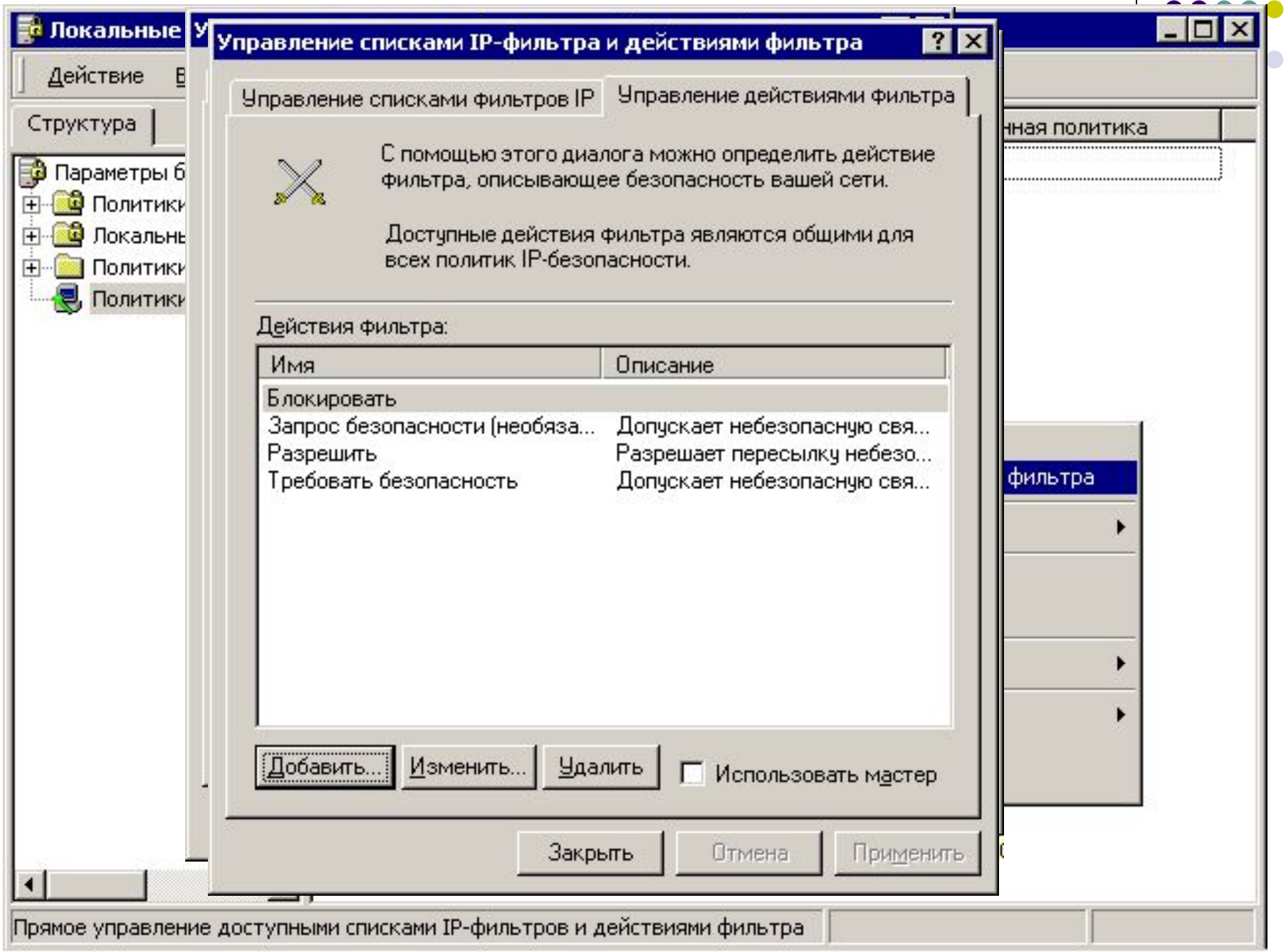


Пример

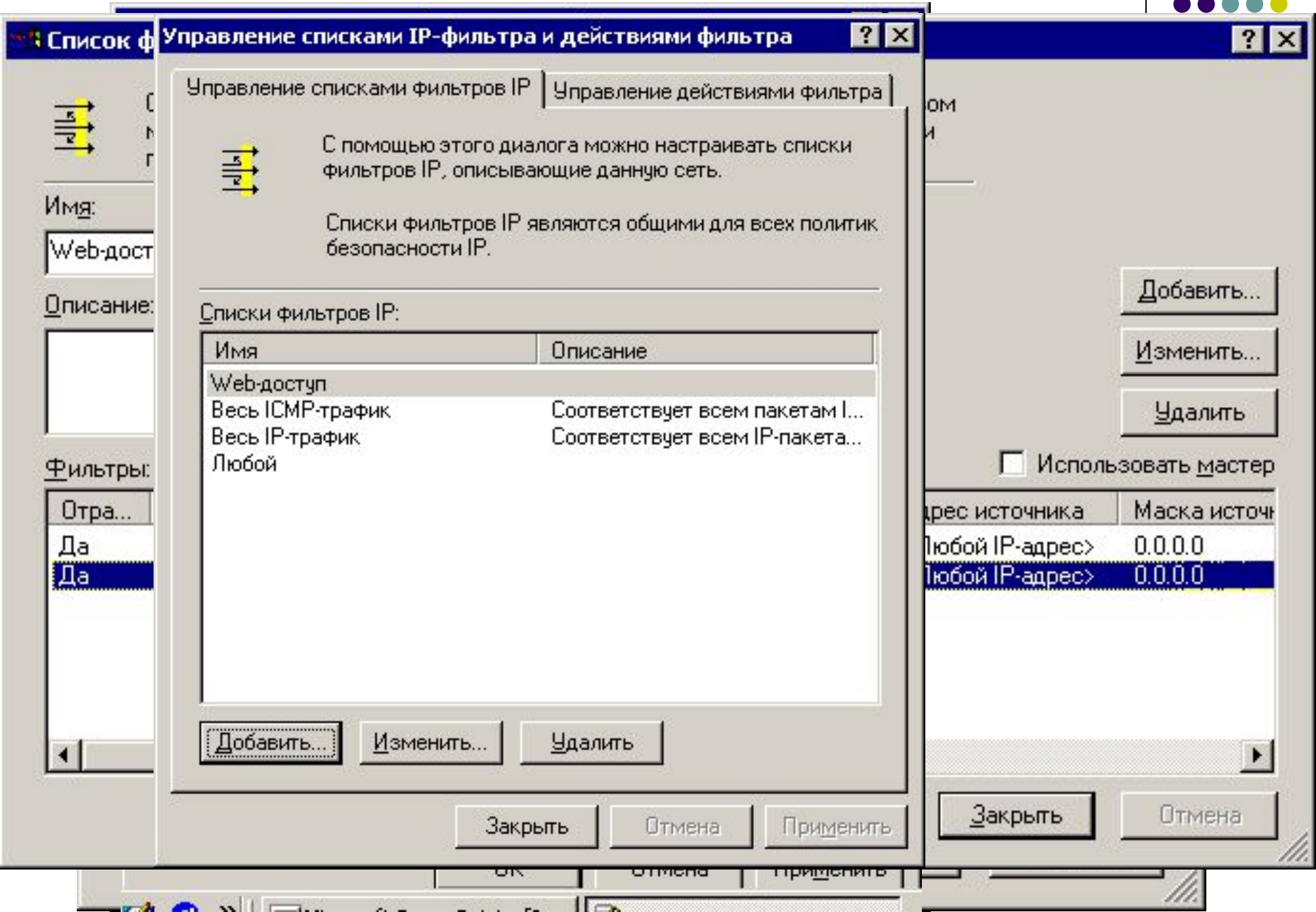


- Разработать политику для Web-сервера, на котором разрешен трафик на портах TCP/80 и TCP/443 из любой точки

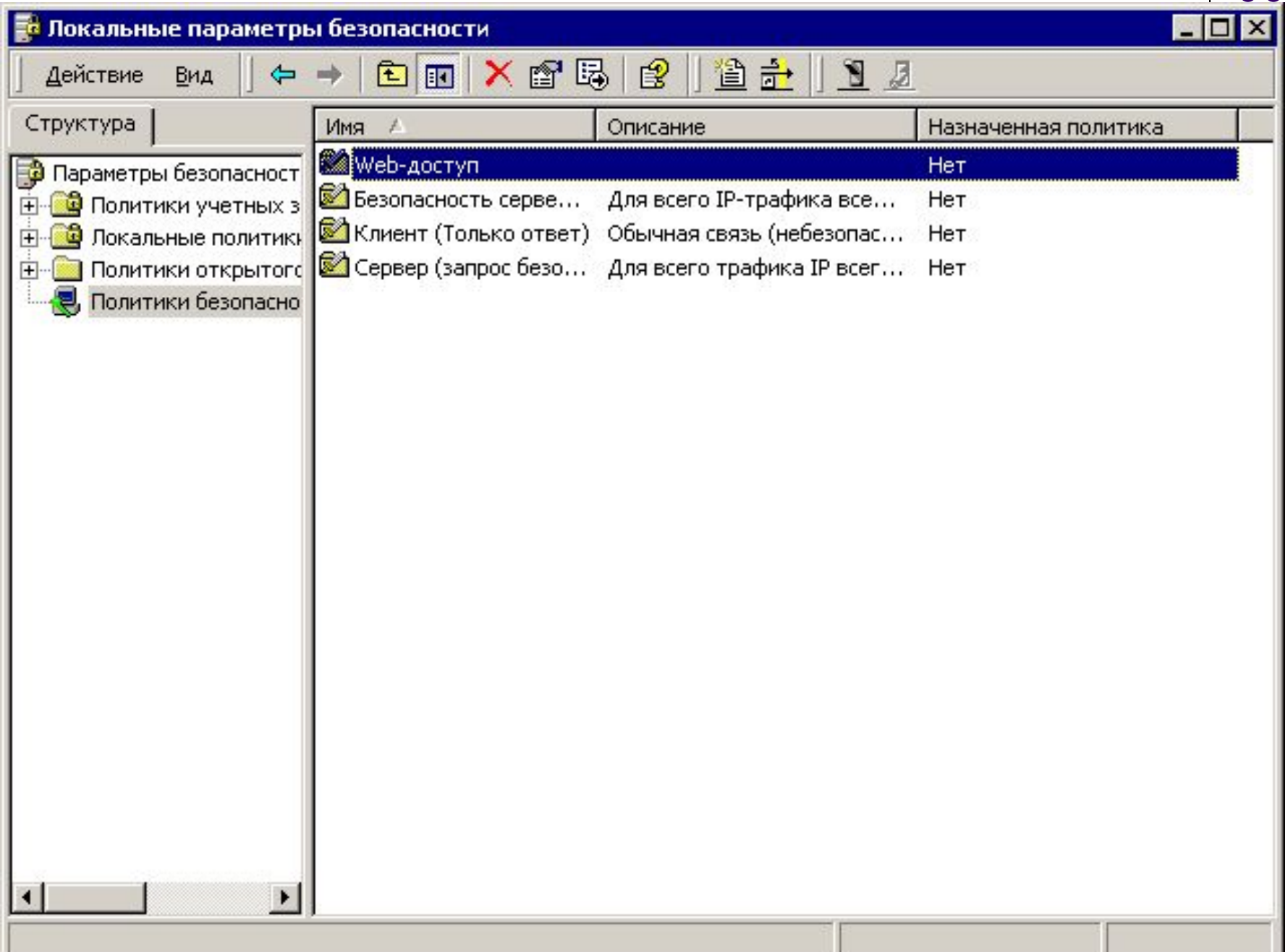
1. Создать действия



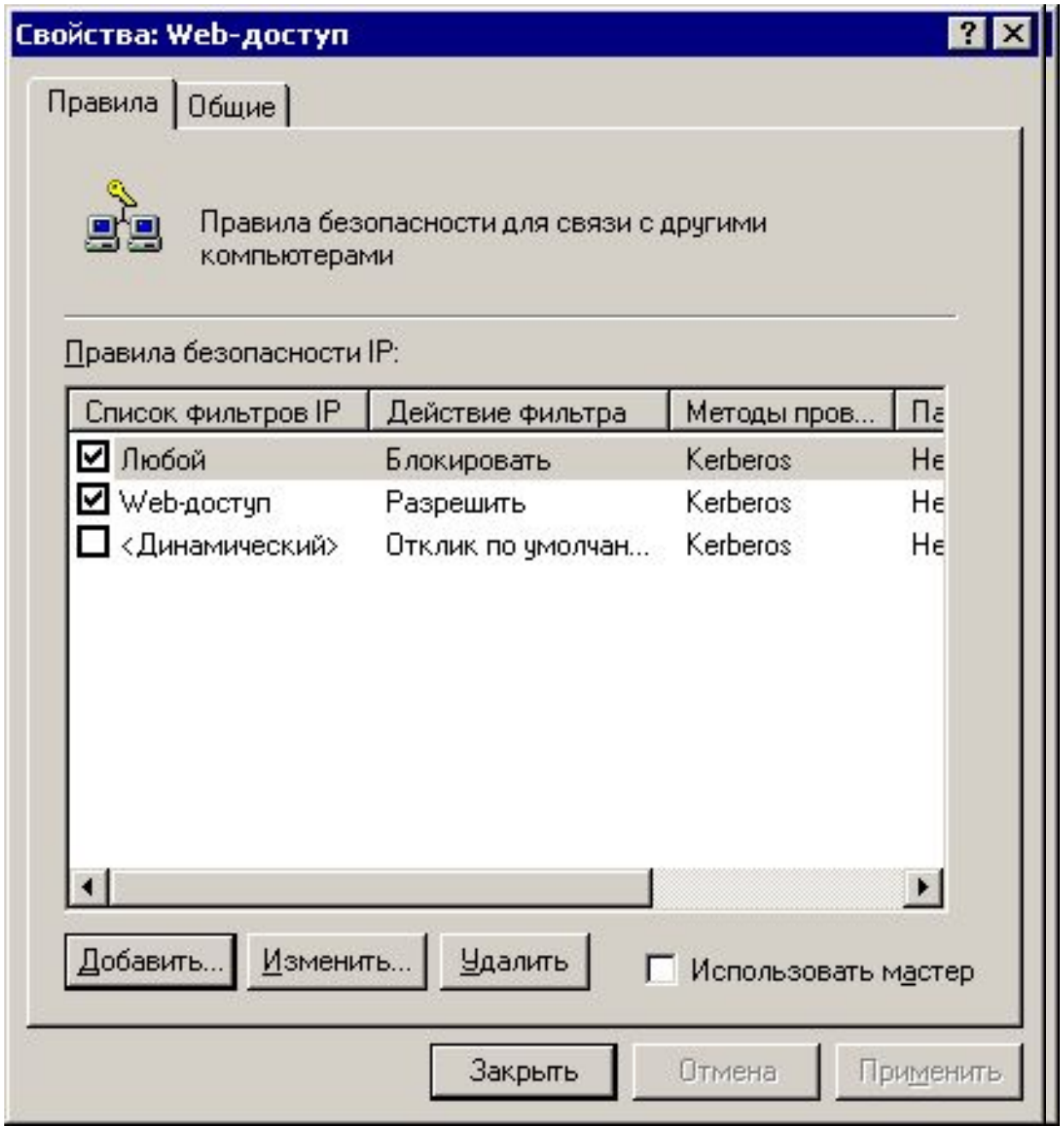
2. Создать списки фильтров



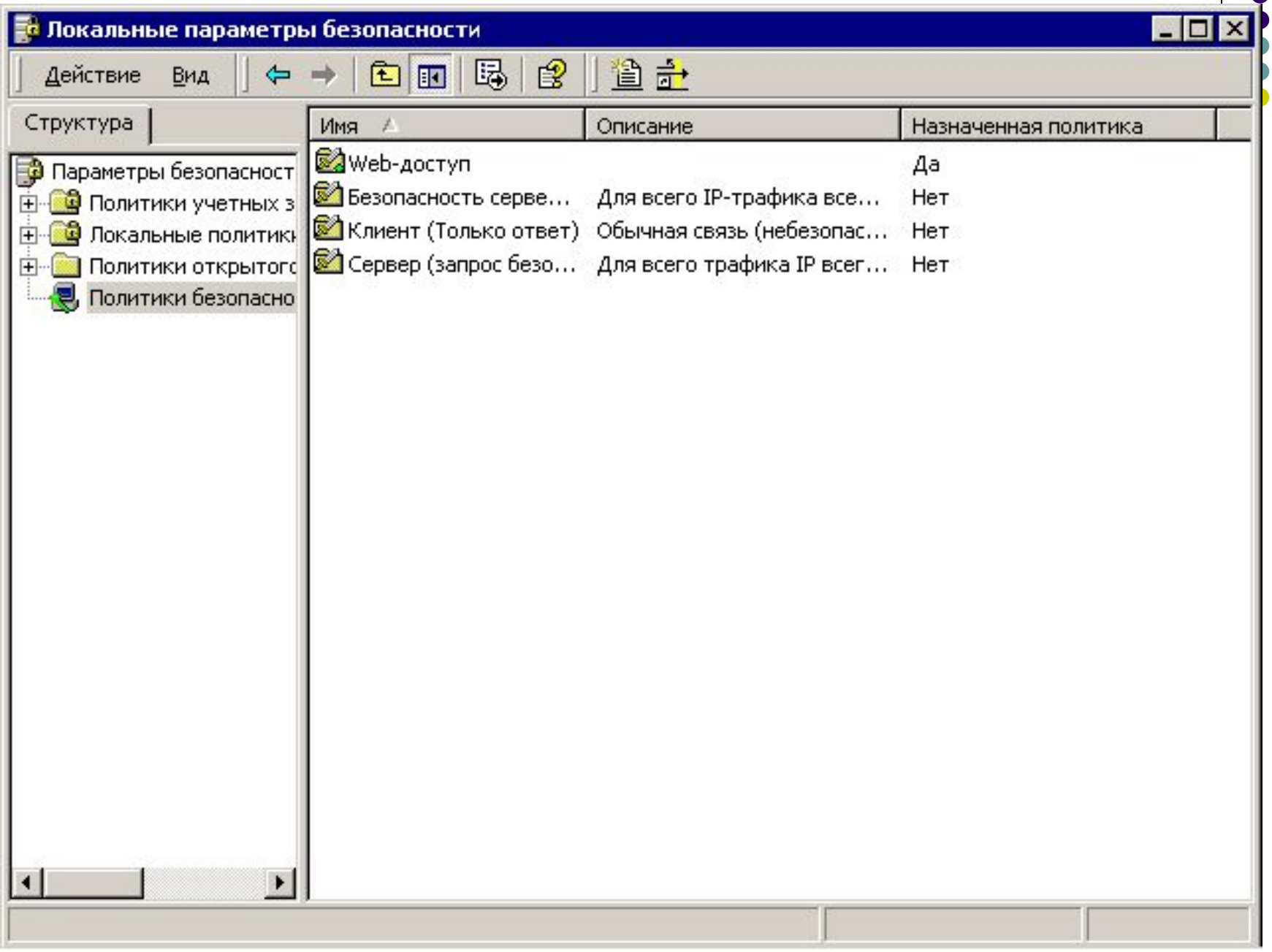
3. Создать новую политику



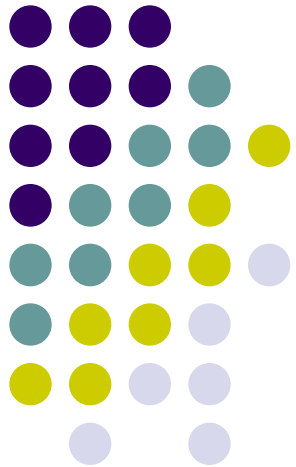
4. Добавить правила и действия



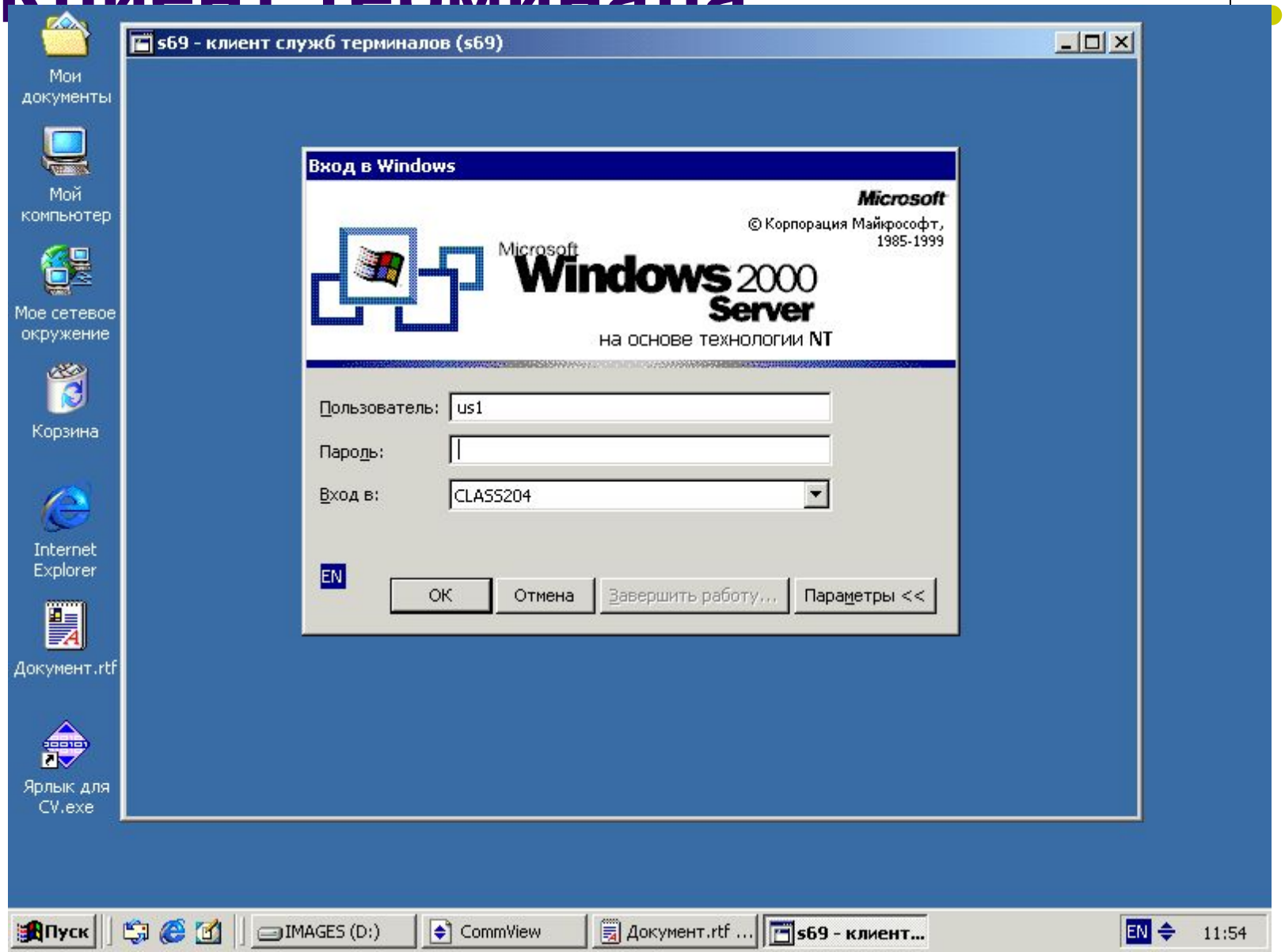
5. Назначить политику



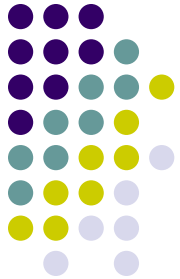
Применение технологии терминального доступа для организации защищенной компьютерной системы



Клиент терминала



Преимущества

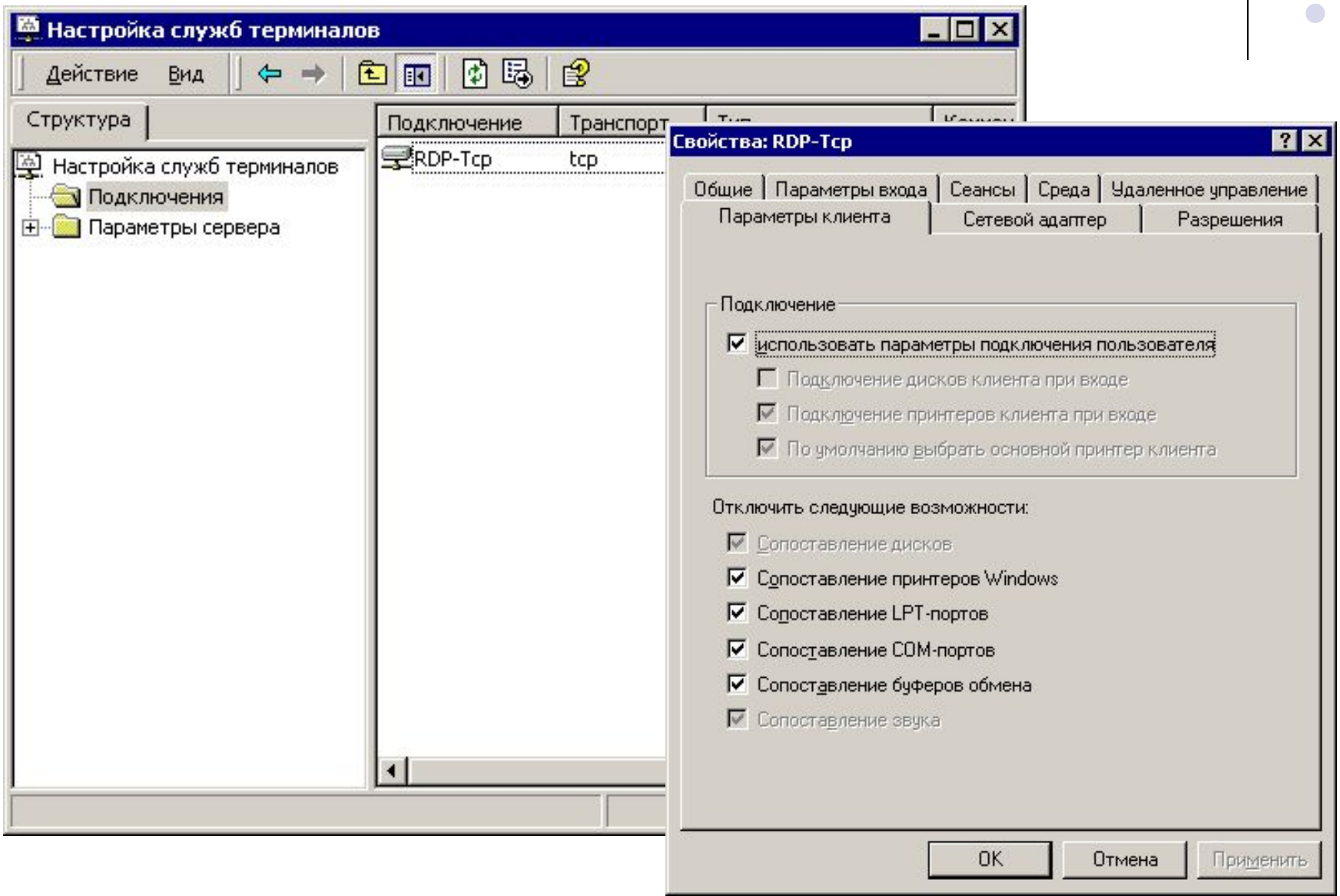


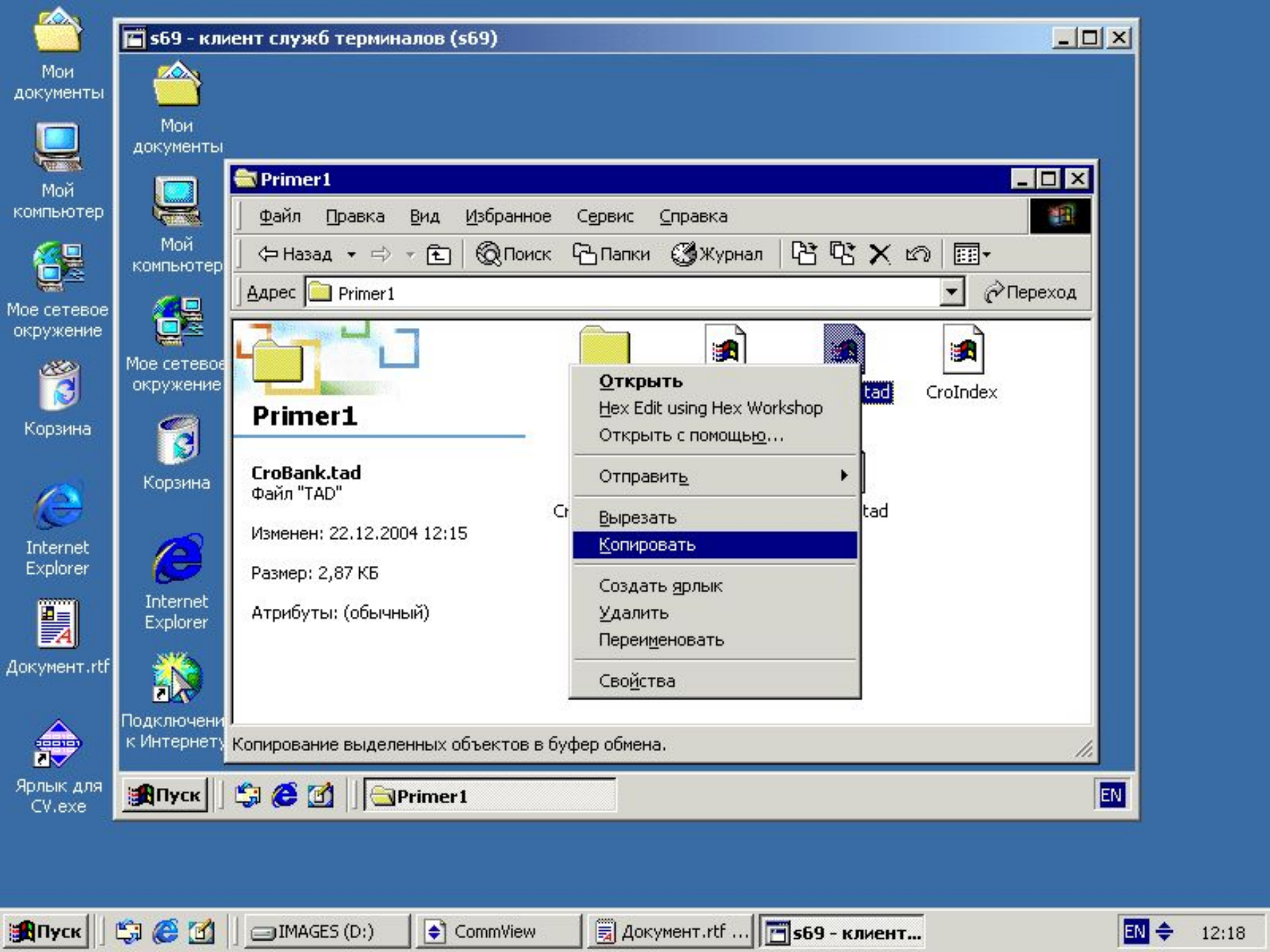
- Вычислительная нагрузка переносится на сервер
- Рабочие станции – любые ПК, с любой версией Windows
- Уменьшение нагрузки на сеть
- Повышенная безопасность
- Упрощение администрирования

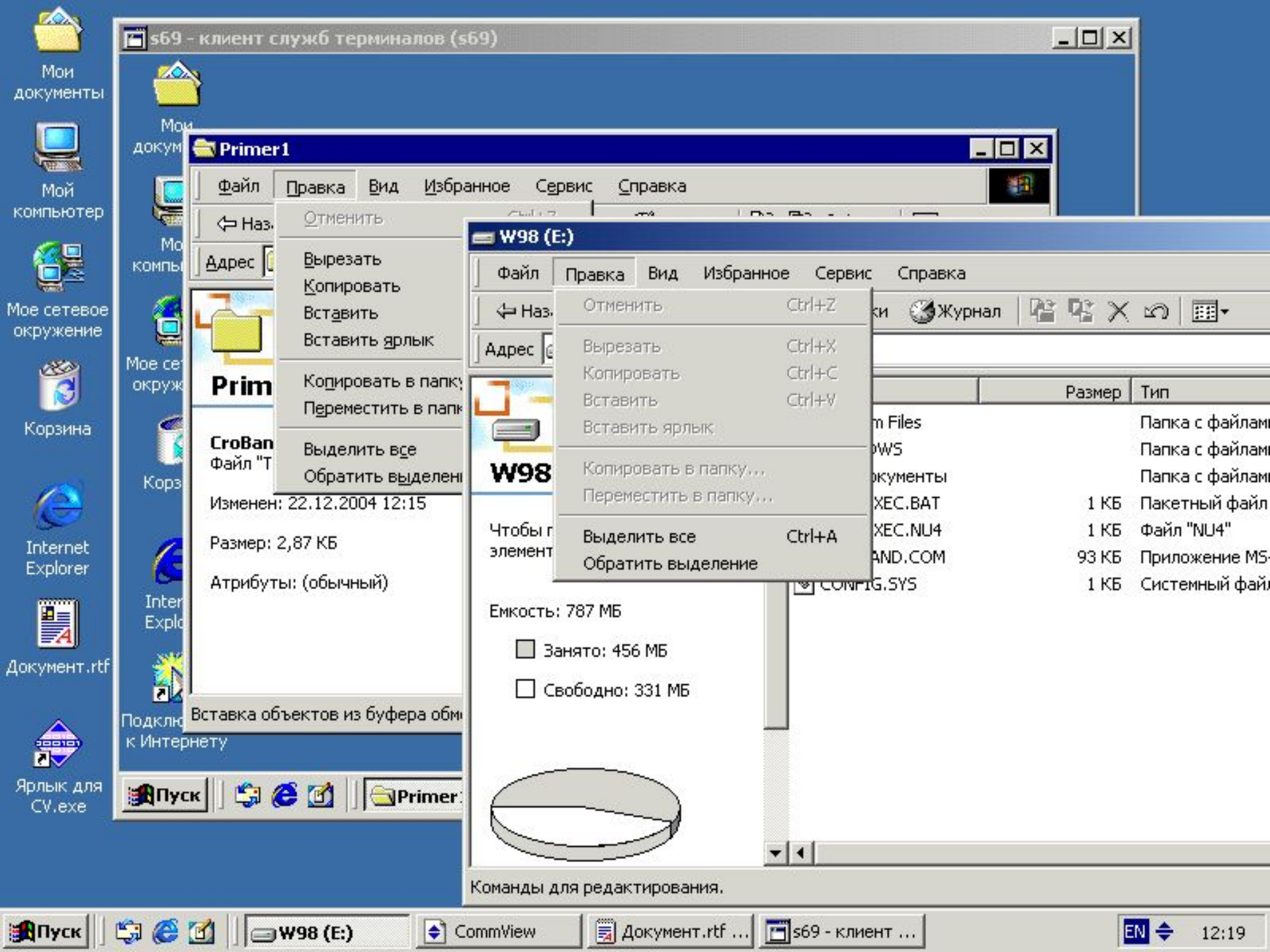
Повышенная безопасность

- Отсутствие возможности частичного или полного копирования информации на рабочие станции
- Нет необходимости защищать рабочие станции
- Отсутствует на сервере служба NetBIOS
- Единственный дисковод – на сервере
- Единственный принтер – на сервере
- Отсутствие вредоносных программ
- Встроенные средства шифрования трафика

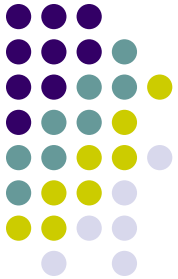
Настройки, запрещающие копирование




Мои документы
Мой компьютер
Мое сетевое окружение
Корзина
Internet Explorer
Документ.rtf
Ярлык для CV.exe
s69 - клиент служб терминалов (s69)
Мои документы
Мой компьютер
Мое сетевое окружение
Корзина
Internet Explorer
Подключени к Интернету
Primer1
Файл Правка Вид Избранное Сервис Справка
Назад Поиск Папки Журнал
Адрес Primer1
Переход
Primer1
CroBank.tad
Файл "TAD"
Изменен: 22.12.2004 12:15
Размер: 2,87 КБ
Атрибуты: (обычный)
Открыть
Hex Edit using Hex Workshop
Открыть с помощью...
Отправить
Вырезать
Копировать
Создать ярлык
Удалить
Переименовать
Свойства
tad
CroIndex
Копирование выделенных объектов в буфер обмена.
Пуск
Primer1
EN
Пуск
IMAGES (D:)
CommView
Документ.rtf ...
s69 - клиент...
EN
12:18

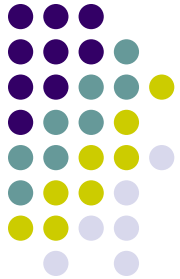

s69 - клиент служб терминалов (s69)
Primer1
Файл Правка Вид Избранное Сервис Справка
Отменить
Вырезать
Копировать
Вставить
Вставить ярлык
Копировать в папку
Переместить в папк
Выделить все
Обратить выделени
Адрес
Изменен: 22.12.2004 12:15
Размер: 2,87 КБ
Атрибуты: (обычный)
Вставка объектов из буфера обм
W98 (E:)
Файл Правка Вид Избранное Сервис Справка
Отменить Ctrl+Z
Вырезать Ctrl+X
Копировать Ctrl+C
Вставить Ctrl+V
Вставить ярлык
Копировать в папку...
Переместить в папку...
Выделить все Ctrl+A
Обратить выделение
Журнал
Размер
Тип
Емкость: 787 МБ
Занято: 456 МБ
Свободно: 331 МБ
Команды для редактирования.
Мои документы
Мой компьютер
Мое сетевое окружение
Корзина
Internet Explorer
Документ.rtf
Ярлык для CV.exe
Подключ к Интернету
Пуск
Primer1
W98 (E:)
CommView
Документ.rtf ...
s69 - клиент ...
EN
12:19

Безопасность MSTS



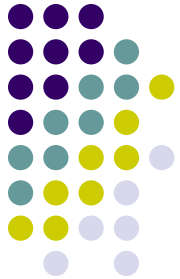
- Безопасность ОС Windows Server 2003;
- Безопасность серверной части MSTS;
- Безопасность протокола терминального доступа — RDP;
- Безопасность клиента терминального доступа.

ОС Windows Server 2003

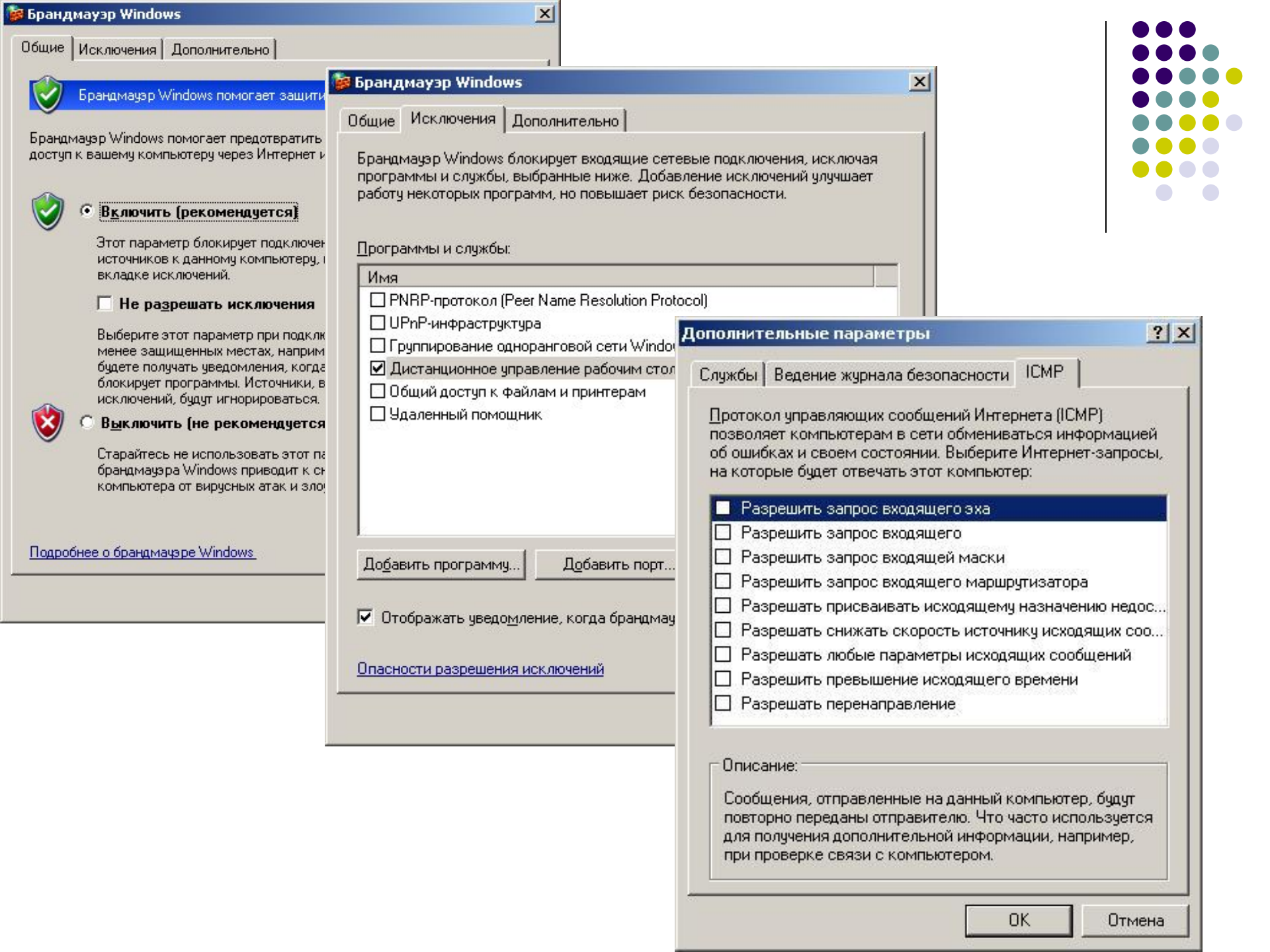


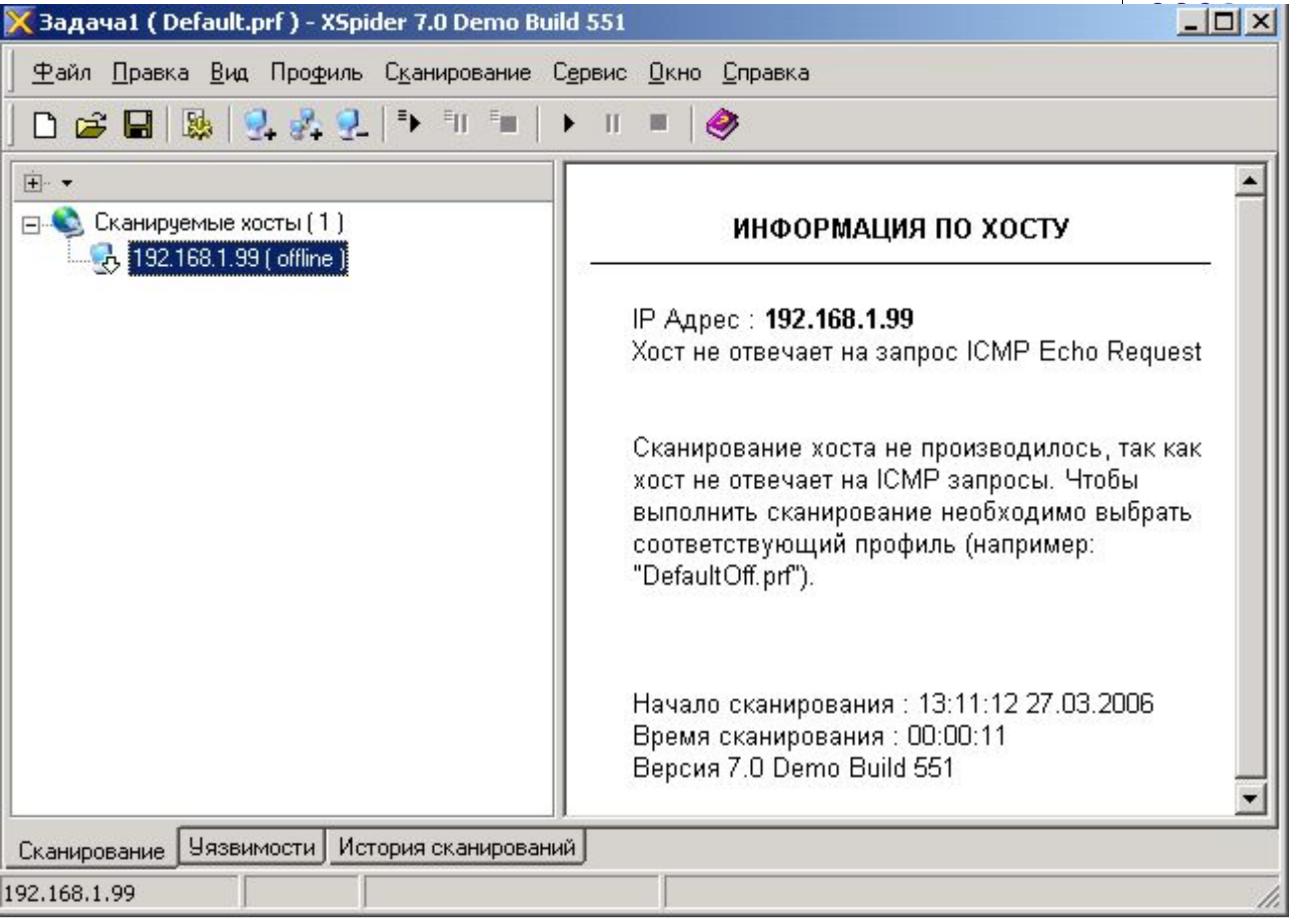
- Возможность сетевого доступа к информации, обрабатываемой на сервере
- Возможность расширения полномочий при осуществлении локального доступа

ОС Windows Server 2003

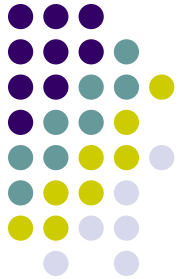


- Запрет возможности сетевого доступа к информации, обрабатываемой на сервере
  - Запрет сетевых служб, применение МЭ
  - Только TCP 3389
  - Запрет ICMP
- «Брандмауэр Windows»


Брандмауэр Windows
Общие
Исключения
Дополнительно
Брандмауэр Windows помогает защити
Брандмауэр Windows помогает предотвратить доступ к вашему компьютеру через Интернет и
Включить (рекомендуется)
Этот параметр блокирует подключен источников к данному компьютеру, вкладке исключений.
Не разрешать исключения
Выберите этот параметр при подклк менее защищенных местах, наприм будете получать уведомления, когда блокирует программы. Источники, в исключений, будут игнорироваться.
Выключить (не рекомендуется
Старайтесь не использовать этот па брандмауэра Windows приводит к сн компьютера от вирусных атак и зло
Подробнее о брандмауэре Windows
Брандмауэр Windows
Общие
Исключения
Дополнительно
Брандмауэр Windows блокирует входящие сетевые подключения, исключая программы и службы, выбранные ниже. Добавление исключений улучшает работу некоторых программ, но повышает риск безопасности.
Программы и службы:
Имя
PNRP-протокол (Peer Name Resolution Protocol)
UPnP-инфраструктура
Группирование одноранговой сети Windo
Дистанционное управление рабочим стол
Общий доступ к файлам и принтерам
Удаленный помощник
Добавить программу...
Добавить порт...
Отображать уведомление, когда брандмау
Опасности разрешения исключений
Дополнительные параметры
Службы
Ведение журнала безопасности
ICMP
Протокол управляющих сообщений Интернета (ICMP) позволяет компьютерам в сети обмениваться информацией об ошибках и своем состоянии. Выберите Интернет-запросы, на которые будет отвечать этот компьютер:
Разрешить запрос входящего эха
Разрешить запрос входящего
Разрешить запрос входящей маски
Разрешить запрос входящего маршрутизатора
Разрешать присваивать исходящему назначению недос...
Разрешать снижать скорость источнику исходящих соо...
Разрешать любые параметры исходящих сообщений
Разрешить превышение исходящего времени
Разрешать перенаправление
Описание:
Сообщения, отправленные на данный компьютер, будут повторно переданы отправителю. Что часто используется для получения дополнительной информации, например, при проверке связи с компьютером.
OK
Отмена

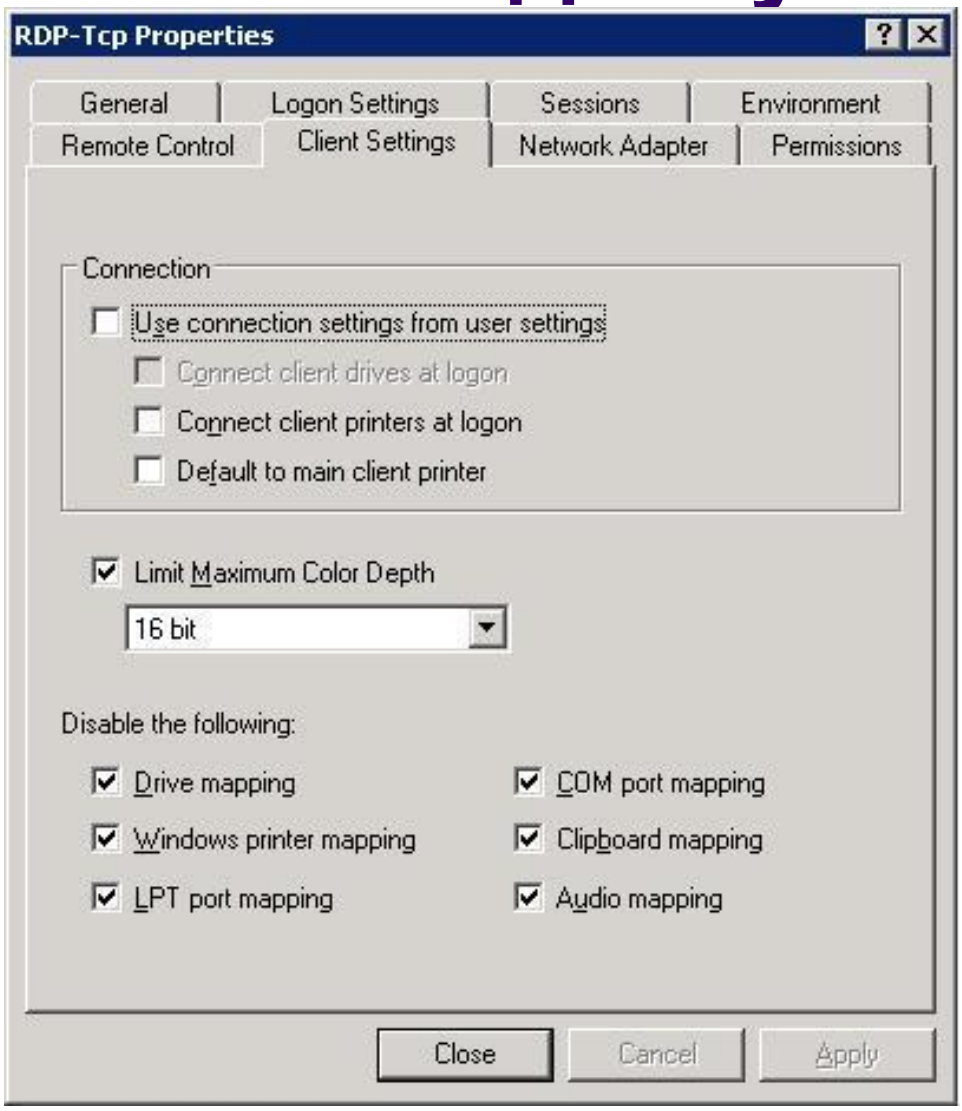

Задача1 (Default.prf) - XSpider 7.0 Demo Build 551
Файл Правка Вид Профиль Сканирование Сервис Окно Справка
Сканируемые хосты (1)
192.168.1.99 (offline)
ИНФОРМАЦИЯ ПО ХОСТУ
IP Адрес : 192.168.1.99
Хост не отвечает на запрос ICMP Echo Request
Сканирование хоста не производилось, так как хост не отвечает на ICMP запросы. Чтобы выполнить сканирование необходимо выбрать соответствующий профиль (например: "DefaultOff.prf").
Начало сканирования : 13:11:12 27.03.2006
Время сканирования : 00:00:11
Версия 7.0 Demo Build 551
Сканирование
Уязвимости
История сканирований
192.168.1.99

ОС Windows Server 2003

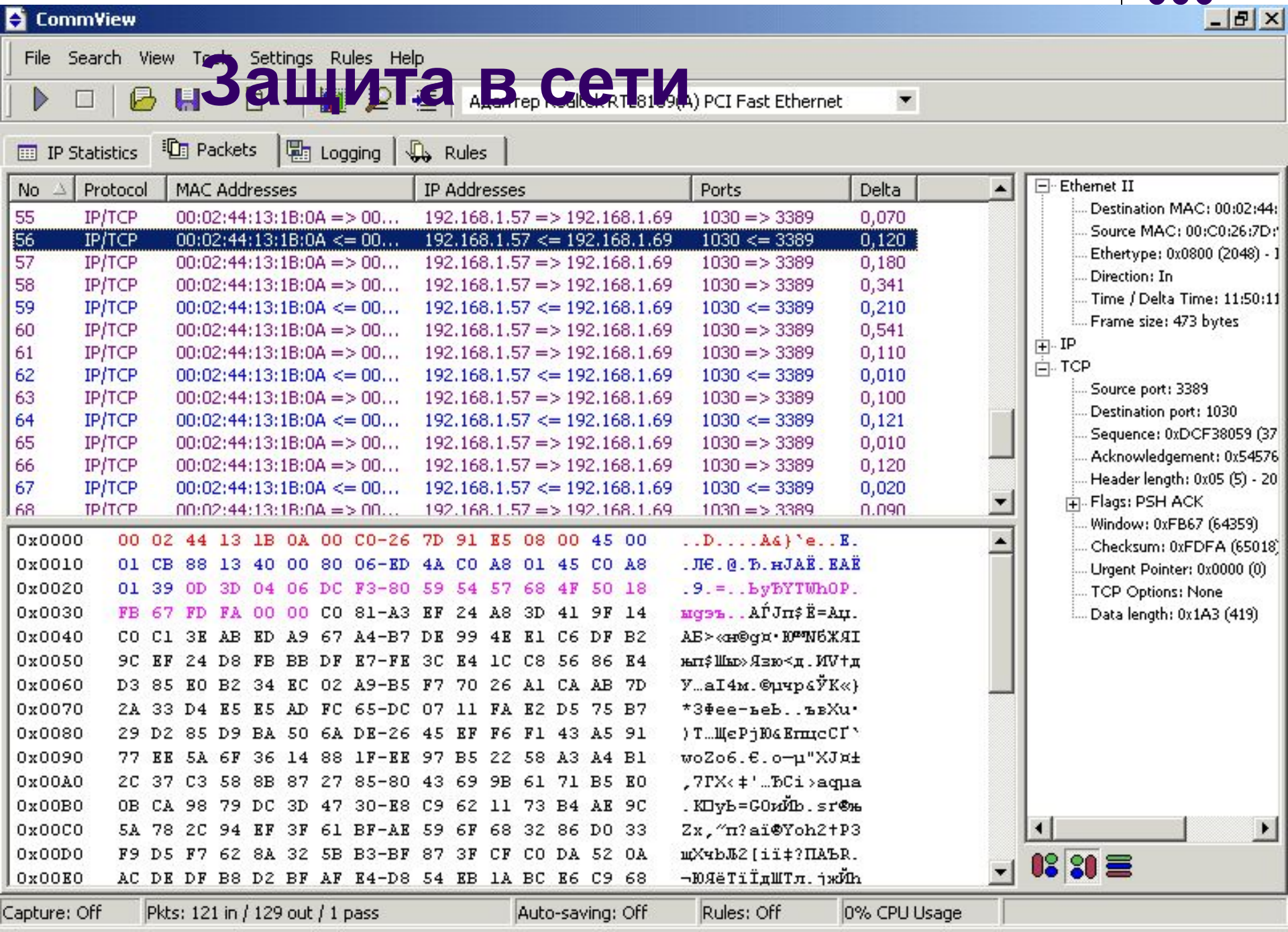


- Запрет возможности расширения полномочий при осуществлении локального доступа
  - Включение пользователей в группу «Remote Desktop Users»
  - Запрет доступа для Administrators

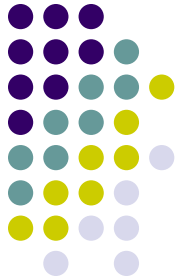
Безопасность протокола терминального доступа RDP



Защита в сети

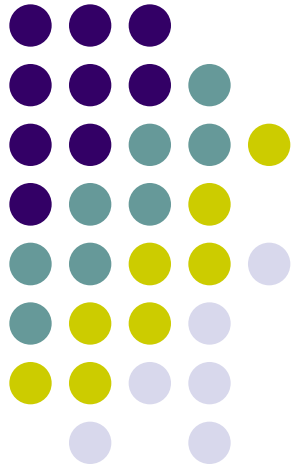


Безопасность клиента терминального доступа



- Загрузка клиента MSTS из ОС рабочей станции с HDD
- Загрузка клиента MSTS с бездисковых станций

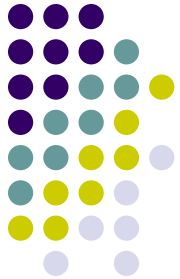
Аудит безопасности компьютерных систем



Литература

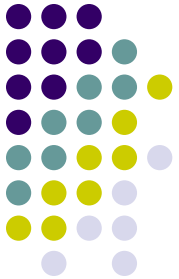
- Петренко С.А., Петренко А.А. Аудит безопасности Intranet. - М.: ДМК Пресс, 2002. - 416 с.
- ГОСТ Р ИСО/МЭК 15408-1-2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий
- ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью

Аудит безопасности



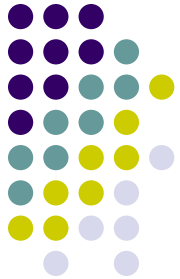
- Системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности (ИБ) организации в соответствии с определенными критериями и показателями безопасности на всех основных уровнях обеспечения безопасности

Основные уровни обеспечения безопасности



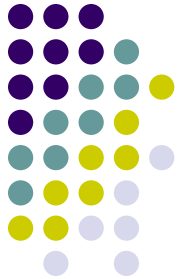
- нормативно-методологический
- организационно-управленческий
- технологический
- технический

Цель аудита безопасности



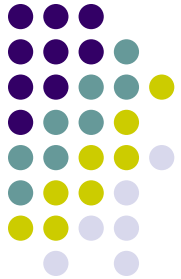
- Объективная оценка уровня защищенности объекта
- Выработка практических рекомендаций по управлению и обеспечению информационной безопасности организации, адекватных поставленным целям и задачам развития бизнеса

Стандарты оценки и управления ИБ



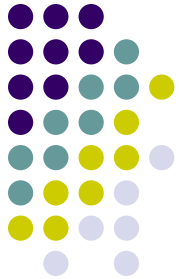
- международные стандарты
  - ISO 15408-99, ISO 17799-2000
- национальные стандарты
  - BS 7799, BSI
- иные стандарты
  - COBIT, SAC, COSO и др.
- Государственный стандарт РФ
  - ГОСТ Р ИСО/МЭК 15408-1-2002
  - ГОСТ Р ИСО/МЭК 17799-2005

Практические подходы к аудиту ИБ

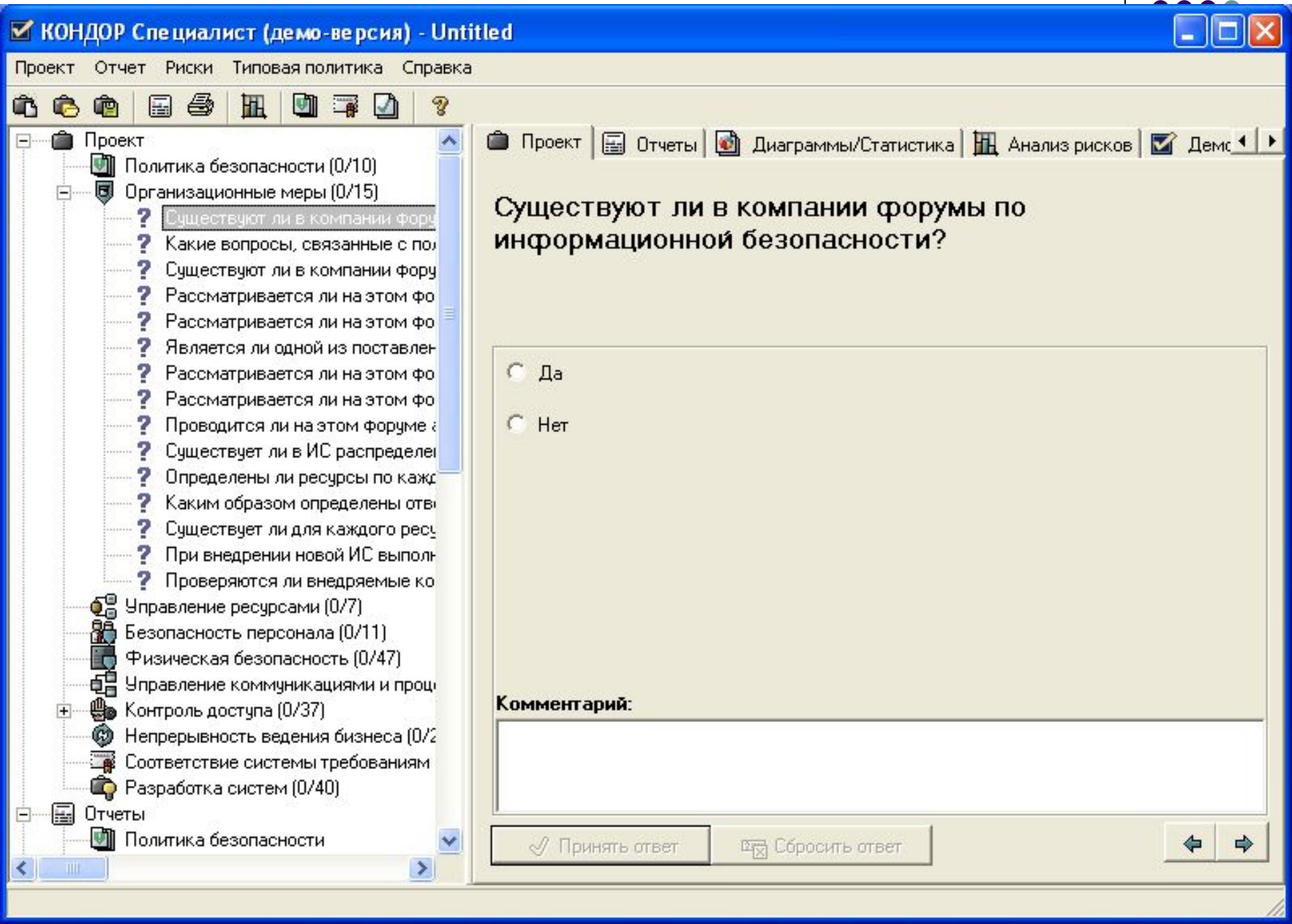


- анализ требований к системе ИБ: проверка соблюдения на практике некоторых общих требований обеспечения ИБ
- инструментальные проверки состояния ИБ организации
- анализ информационных рисков организации

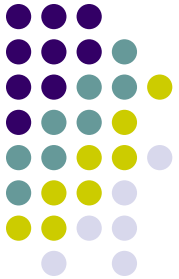
Выбор показателей эффективности системы ИБ



- Два способа:
  - определение минимального набора необходимых для защиты информации функций, соответствующих конкретному классу защищенности (РД ГТК РФ)
  - определение профиля защиты, учитывающего особенности решения задач защиты информации на предприятии (ISO 15408, ISO 17799)

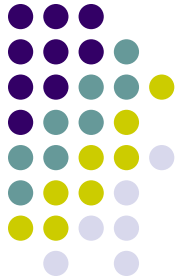

КОНДОР Специалист (демо-версия) - Untitled
Проект Отчет Риски Типовая политика Справка
Проект
Политика безопасности (0/10)
Организационные меры (0/15)
Существуют ли в компании фору
Какие вопросы, связанные с пол
Существуют ли в компании фору
Рассматривается ли на этом фо
Рассматривается ли на этом фо
Является ли одной из поставлен
Рассматривается ли на этом фо
Рассматривается ли на этом фо
Проводится ли на этом форуме а
Существует ли в ИС распределе
Определены ли ресурсы по кажд
Каким образом определены отв
Существует ли для каждого рес
При внедрении новой ИС выполн
Проверяются ли внедряемые ко
Управление ресурсами (0/7)
Безопасность персонала (0/11)
Физическая безопасность (0/47)
Управление коммуникациями и проц
Контроль доступа (0/37)
Непрерывность ведения бизнеса (0/2
Соответствие системы требованиям
Разработка систем (0/40)
Отчеты
Политика безопасности
Проект
Отчеты
Диаграммы/Статистика
Анализ рисков
Демо
Существуют ли в компании форумы по информационной безопасности?
Да
Нет
Комментарий:
Принять ответ
Сбросить ответ

Интегрированный подход



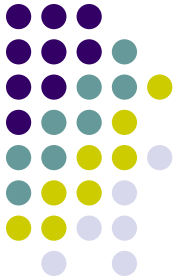
- организационно-правовой аспект,
- учет технических каналов утечки,
- анализ систем управления доступом пользователей к СВТ,
- программно-аппаратная составляющая
- и т.д.

Инструментальные проверки (ИП)



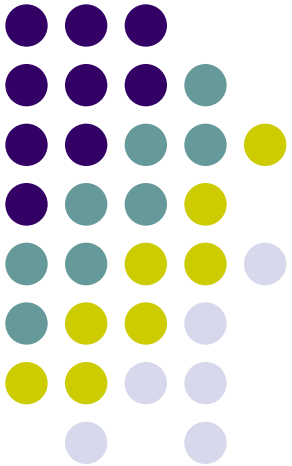
- Проверка на соответствие заявленным целям и задачам политики безопасности нижнего технического уровня обеспечения ИБ

Три этапа проведения ИП:

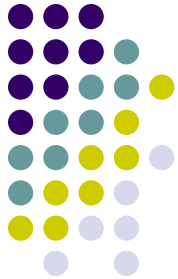


- Анализ структуры АИС
- Внутренний аудит
- Внешний аудит

Этап 1. Анализ структуры АИС

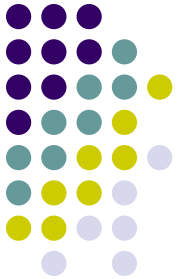


Анализ структуры АИС



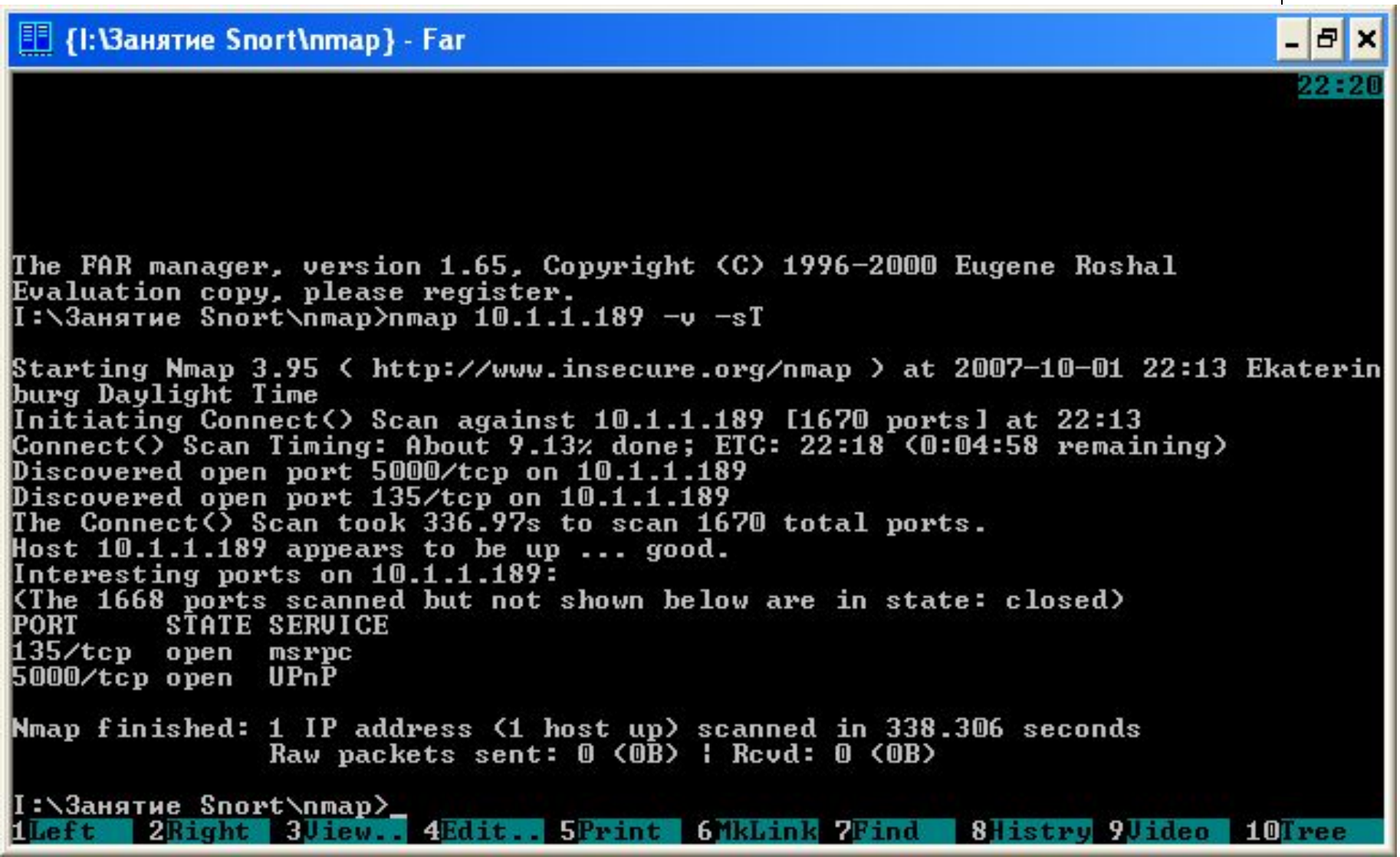
- Анализ и инвентаризация информационных ресурсов:
  - перечень сведений, составляющих коммерческую или служебную тайну;
  - информационные потоки, структура и состав АИС;
  - категорирование ресурсов, подлежащих защите

Инвентаризация сетевых ресурсов



- IP-адреса сетевых узлов и подсетей;
- открытые TCP- и UDP-порты на обнаруженных узлах;
- версии ОС и сетевых сервисов, работающих на обнаруженных сетевых узлах

Сканер nmap


{I:\Занятие Snort\nmap} - Far
22:20
The FAR manager, version 1.65, Copyright (C) 1996-2000 Eugene Roshal
Evaluation copy, please register.
I:\Занятие Snort\nmap>nmap 10.1.1.189 -v -sT
Starting Nmap 3.95 (http://www.insecure.org/nmap) at 2007-10-01 22:13 Ekaterin
burg Daylight Time
Initiating Connect() Scan against 10.1.1.189 [1670 ports] at 22:13
Connect() Scan Timing: About 9.13% done; ETC: 22:18 (0:04:58 remaining)
Discovered open port 5000/tcp on 10.1.1.189
Discovered open port 135/tcp on 10.1.1.189
The Connect() Scan took 336.97s to scan 1670 total ports.
Host 10.1.1.189 appears to be up ... good.
Interesting ports on 10.1.1.189:
(The 1668 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
135/tcp open msrpc
5000/tcp open UPnP
Nmap finished: 1 IP address (1 host up) scanned in 338.306 seconds
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)
I:\Занятие Snort\nmap>
1Left 2Right 3View.. 4Edit.. 5Print 6MkLink 7Find 8Histry 9Video 10Tree

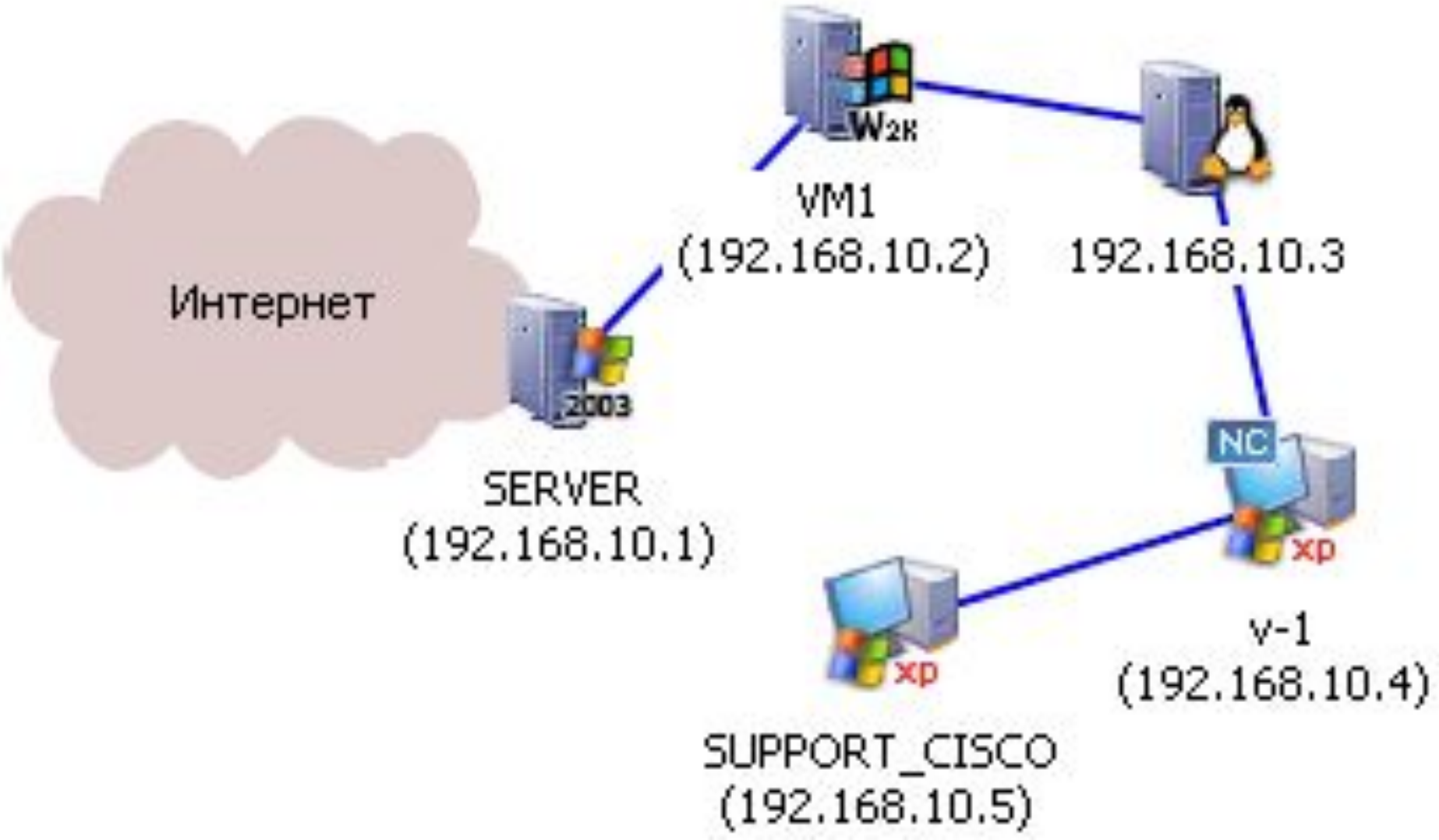
Утилита netstat -aon

C:\WINDOWS\System32\cmd.exe

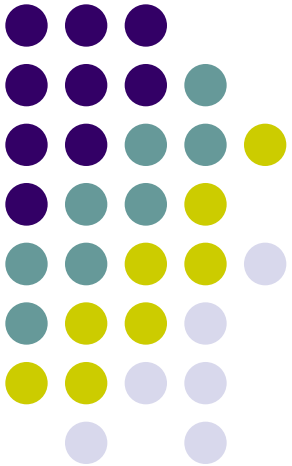
```
C:\Documents and Settings\user>netstat -aon

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       852
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING       1120
  UDP    0.0.0.0:445            *:*                                    4
  UDP    0.0.0.0:500            *:*                                    684
  UDP    0.0.0.0:1040           *:*                                    916
  UDP    0.0.0.0:1043           *:*                                    1096
  UDP    0.0.0.0:1087           *:*                                    1096
  UDP    10.1.1.189:123         *:*                                    916
  UDP    10.1.1.189:1900        *:*                                    1120
  UDP    127.0.0.1:123          *:*                                    916
  UDP    127.0.0.1:1531         *:*                                    916
  UDP    127.0.0.1:1900         *:*                                    1120
```

<table>
<tr><td>№</td><td>Наименование</td><td colspan="4">Выводимые результаты</td></tr>
<tr><td></td><td>Обследуемый сегмент сети</td><td colspan="4">Сканируемый диапазон IP-адресов</td></tr>
<tr><td></td><td>Характер обнаруженных узлов в сегменте</td><td colspan="4">Рабочие станции, Web-серверы, контроллеры домена и т.п.</td></tr>
<tr><td></td><td>Возможность идентификации сетевых узлов</td><td colspan="4">Результаты использования Ping – разведки
Результаты, полученные с использованием других ICMP сообщений
Результаты, полученные при использовании переноса зоны DNS</td></tr>
<tr><td rowspan="4"></td><td rowspan="4">Выявленные узлы</td><td>IP</td><td>Назначение узла</td><td>Тип и версия ОС</td><td>Представленные сетевые сервисы и их версии, открытые порты</td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td>Карта сетевого сегмента и его подключения к другим сетям</td><td colspan="4">Карта сети в графическом или табличном варианте</td></tr>
</table>

Карта сети (программа NetCrunch)



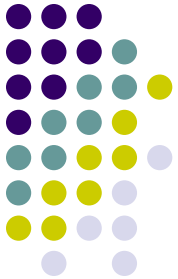
Этап 2. Внутренний аудит



Внутренний аудит АИС

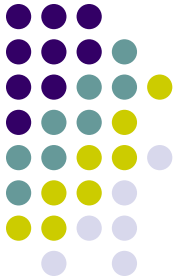
- Средства защиты ПК
  - **возможность отключения программно-аппаратных систем защиты при физическом доступе к выключенным станциям;**
  - **использование и надежность встроенных средств парольной защиты BIOS**
- Состояние антивирусной защиты
  - **наличие в АИС вредоносных программ,**
  - **возможность их внедрения через машинные носители, сеть Интернет**

Внутренний аудит АИС



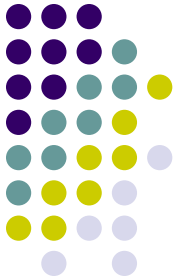
- Настройки операционных систем
  - **наличие требуемых настроек безопасности, специфичных для различных ОС**
- Парольная защита в ОС
  - **получение файлов с зашифрованными паролями и их последующего дешифрования;**
  - **подключение с пустыми паролями,**
  - **подбор паролей, в том числе, по сети**

Внутренний аудит АИС



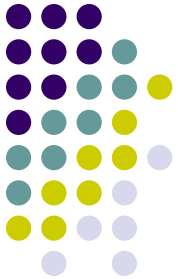
- Система разграничения доступа пользователей АИС к её ресурсам
  - **формирование матрицы доступа;**
  - **анализ дублирования и избыточности в предоставлении прав доступа;**
  - **определение наиболее осведомленных пользователей и уровней защищенности конкретных ресурсов;**
  - **оптимальность формирования рабочих групп**

Внутренний аудит АИС



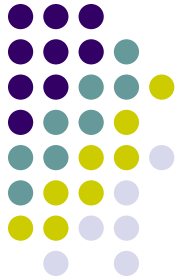
- Сетевая инфраструктура
  - **возможность подключения к сетевому оборудованию для получения конфиденциальной информации путем перехвата и анализа сетевого трафика;**
  - **настройки сетевых протоколов и служб**
- Аудит событий безопасности
  - **настройка и реализация политики аудита**

Внутренний аудит АИС



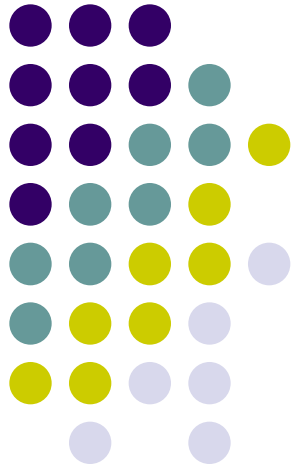
- Прикладное программное обеспечение
  - **надежность элементов защиты используемых АРМ;**
  - **возможные каналы утечки информации;**
  - **анализ версий используемого программного обеспечения на наличие уязвимых мест**

Внутренний аудит АИС



- Системы защиты информации
  - **надежность и функциональность используемых СЗИ;**
  - **наличие уязвимых мест в защите;**
  - **настройка СЗИ**

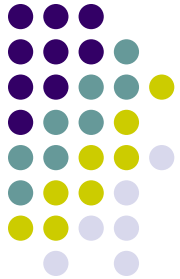
Этап 3. Внешний аудит



Средства активного аудита

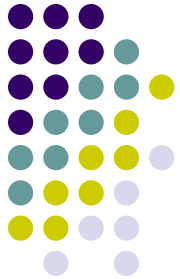
- Выявление уязвимостей в ПО сетевых узлов с применением сканеров безопасности
  - Internet Scanner, System Security Scanner компания Internet Security Systems
  - NetRecon компании Symantec
  - Enterprise Security Manager компании Symantec
  - Cisco Secrure Scanner (NetSonar)
  - **Nessus**
  - **LanGuard Security Scanner**
  - **XSpider**

Средства активного аудита



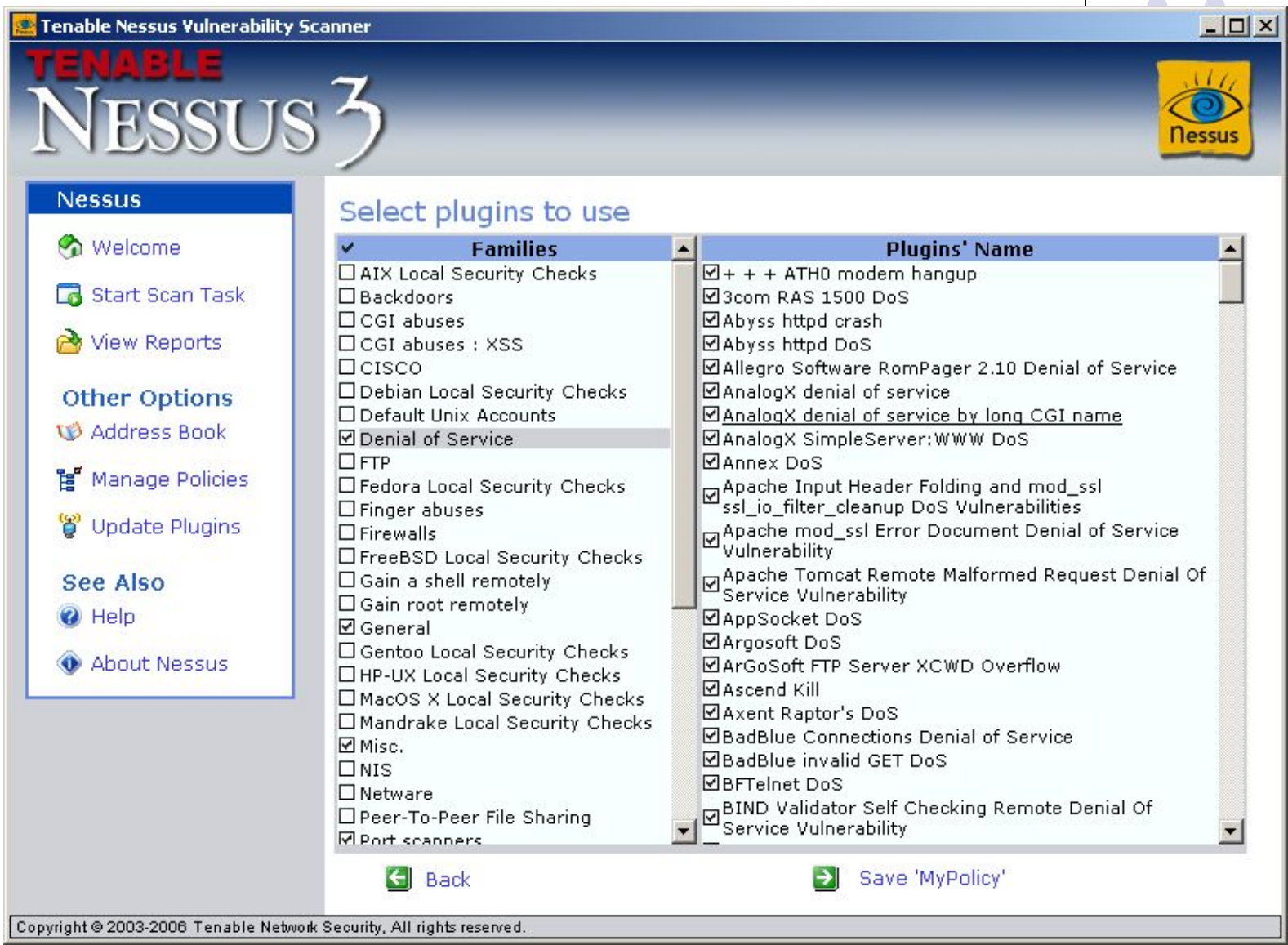
- определение уязвимых мест в средствах защиты
- моделирование известных методов, используемых для несанкционированного проникновения в КС
- база данных, информация о вариантах взлома сети
- результат - отчет о найденных уязвимостях и перечень мер защиты

Средства активного аудита

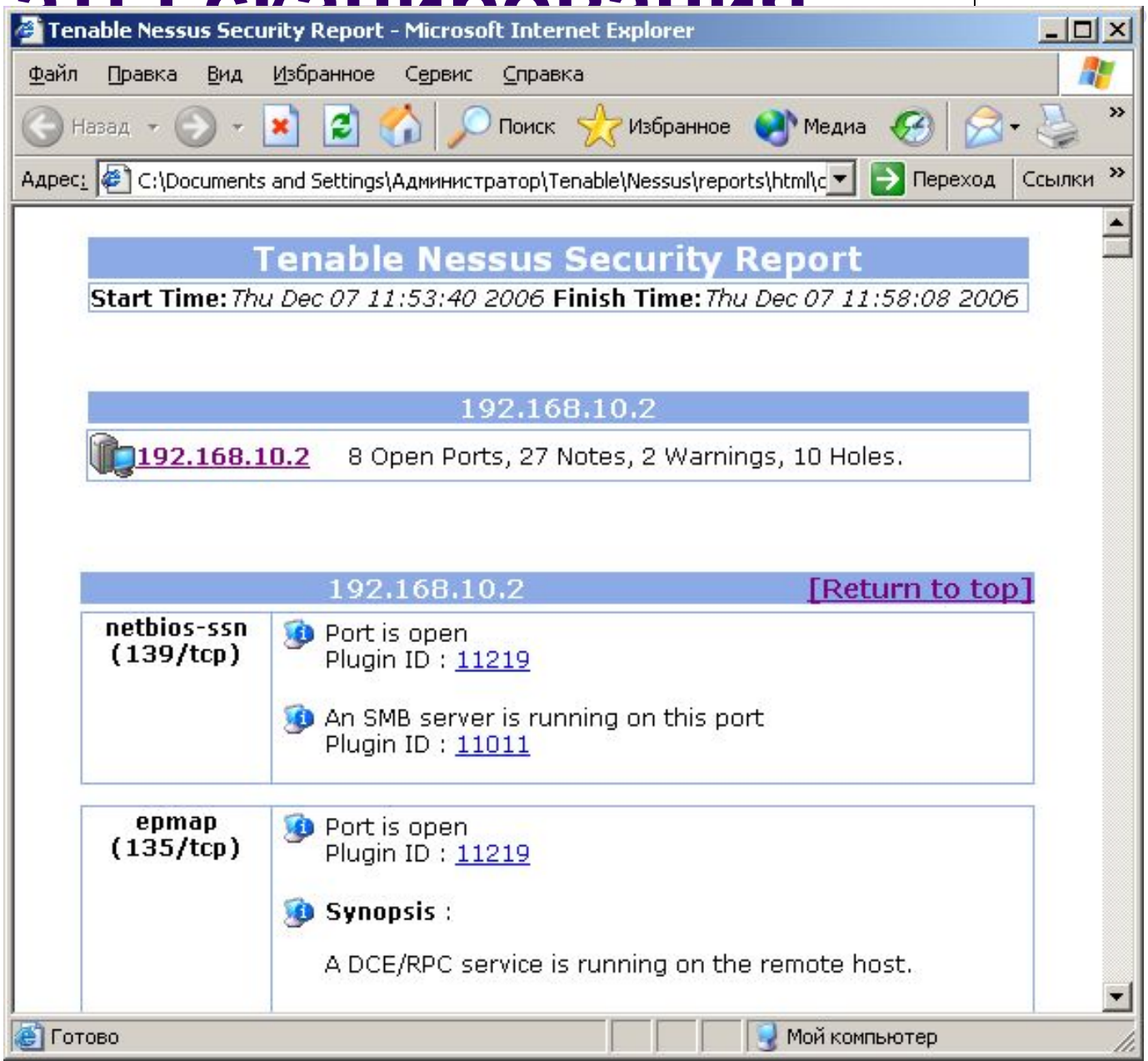


- Недостатки:
  - необходимы, но недостаточны для качественного исследования состояния ИБ
  - только технический уровень, нет оценки общего уровня ИБ.

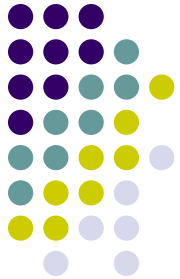
Использование сканера безопасности Nessus



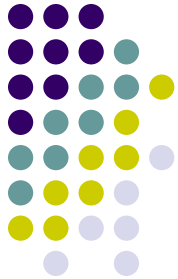
Результаты сканирования



IP-адрес: 192.168.10.1	
Степень опасности: критическая	
Идентификация уязвимости: CVE: CVE-2003-0715, CVE-2003-0528, CVE-2003-0605 BID: 8458, 8460 IAVA: 2003-A-0012	
Краткий обзор: Существует возможность удаленного выполнения произвольного программного кода на данном сетевом узле	
Описание: На узле установлена операционная система Windows, имеющая уязвимость в реализации одного из программных модулей. При наличии доступа злоумышленника к данному узлу по сети существует возможность запуска на нем произвольного программного кода с максимальными полномочиями (полный контроль над узлом).	
Меры по устранению: Требуется перенастройка операционной системы и/или установка обновлений безопасности. Подробная информация может быть получена с официального Web-сайта Microsoft: http://www.microsoft.com/technet/security/bulletin/MS03-039.msps.	

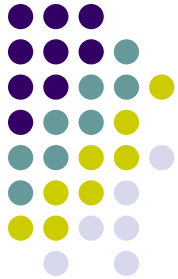


Внешний аудит АИС



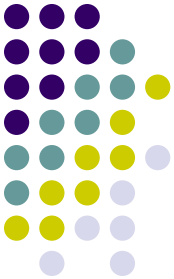
- Получение данных о внутренней структуре АИС
  - **наличие на Web-узлах информации конфиденциального характера;**
  - **выявление настроек DNS-сервера и почтового сервера, позволяющих получить информацию о внутренней структуре АИС**

Внешний аудит АИС



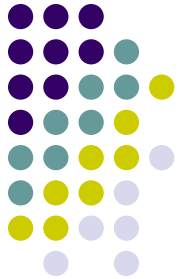
- Выявление компьютеров, подключенных к сети и достижимых из Интернет
  - **сканирование портов по протоколам ICMP, TCP, UDP;**
  - **определение доступности информации об используемом в АИС программном обеспечении и его версиях;**
  - **выявление активных сетевых служб;**
  - **определение типа и версии ОС, сетевых приложений и служб**

Внешний аудит АИС



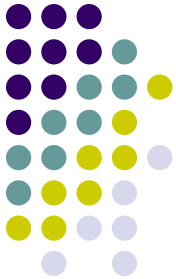
- Получение информации об учетных записях, зарегистрированных в АИС
  - **применение утилит, специфичных для конкретной ОС**
- Подключение к доступным сетевым ресурсам
  - **определение наличия доступных сетевых ресурсов и возможности подключения к ним**

Внешний аудит АИС



- Атаки на межсетевые экраны
  - **определение типа МЭ и ОС путем сканирования портов;**
  - **использование известных уязвимостей в программном обеспечении МЭ;**
  - **выявление неверной конфигурации МЭ**

Внешний аудит АИС

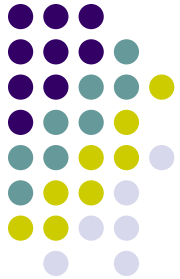


- Атаки на сетевые приложения
  - **анализ защищенности Web-серверов,**
  - **тестирование стойкости систем удаленного управления,**
  - **анализ возможности проникновения через имеющиеся модемные соединения**
- Атаки типа «Отказ в обслуживании»
  - **выявление версий ОС и сетевых приложений, подверженных таким атакам**

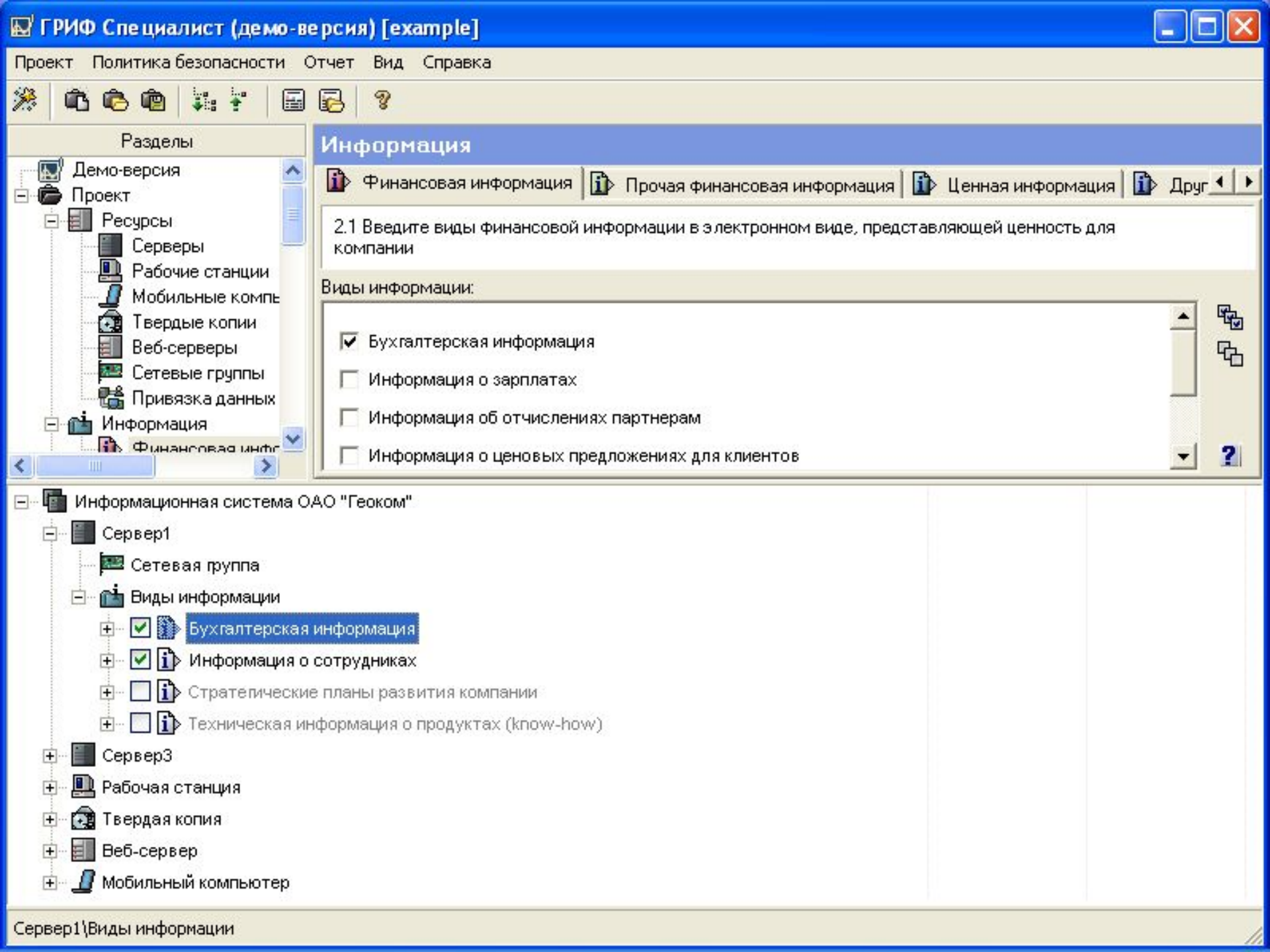
Результат тестирования - экспертное заключение (Акт проверки защищенности АИС от НСД)

- **реальное состояние защищенности АИС от внутренних и внешних угроз,**
- **перечень найденных изъянов в настройках систем безопасности**
- **рекомендации по повышению степени защищенности АИС**

Анализ информационных рисков организации



- определение, что именно подлежит защите
- построение перечня угроз
- анализ способов защиты
- определение вероятности угроз
- оценка ущерба в случае реализации атак


ГРИФ Специалист (демо-версия) [example]
Проект
Политика безопасности
Отчет
Вид
Справка
Разделы
Демо-версия
Проект
Ресурсы
Серверы
Рабочие станции
Мобильные компь
Твердые копии
Веб-серверы
Сетевые группы
Привязка данных
Информация
Информация
Финансовая информация
Прочая финансовая информация
Ценная информация
Друг
2.1 Введите виды финансовой информации в электронном виде, представляющей ценность для компании
Виды информации:
Бухгалтерская информация
Информация о зарплатах
Информация об отчислениях партнерам
Информация о ценовых предложениях для клиентов
Информационная система ОАО "Геоком"
Сервер1
Сетевая группа
Виды информации
Бухгалтерская информация
Информация о сотрудниках
Стратегические планы развития компании
Техническая информация о продуктах (know-how)
Сервер3
Рабочая станция
Твердая копия
Веб-сервер
Мобильный компьютер
Сервер1\Виды информации