CISCO EXPO 2004

Защита корпоративных сетей

Михаил Кадер
Инженер-консультант
mkader@cisco.com

Содержание

Cisco.com

- **Введение**
- **Инфраструктура**
- **Услуги и технологии**
- **Мониторинг**

Цели обсуждения

Cisco.com

- Определение основных настроек защиты
- Изучение современных методов защиты
- Обзор различных технологий аутентификации
- Изучение возможностей защиты в технологиях установления соединений и коммутации
- Обзор различных методов и технологий контроля доступа к сети
- Обзор современных средств и технологий мониторинга

Инфраструктура

Содержание

Cisco.com

- Введение
- Инфраструктура
  - Настройка устройств
  - Администрирование доступа пользователей к устройствам
  - Защита протоколов маршрутизации
  - Уровень 2 / Коммутаторы
- Услуги и технологии
- Мониторинг

Защита сети

Cisco.com

- Общее заблуждение:

**Сеть будет в безопасности,
если я установлю межсетевой экран**

- Правильный подход:
  - Каждое устройство в сети должно быть защищено
    - НЕ ИСКЛЮЧАЯ МАРШРУТИЗАТОРЫ И КОММУТАТОРЫ!
- Совокупность сетевых устройств представляет собой сетевую инфраструктуру
  - Зачем рисковать безопасностью целой сети, экономя на защите сетевых устройств?

Настройки устройств CISCO IOS, CATALYST OS, PIX OS

Предупреждения

- Обычно настройки для Cisco IOS®, Catalyst® OS, и PIX® OS одинаковы
- Существенные различия в настройках подробно освещаются в предлагаемых примерах

Заводские установки

Cisco.com

- **Установите имя хоста**

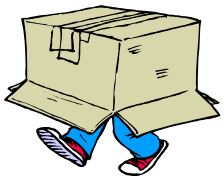
```
hostname something-unique
```

- **Установите время**

```
clock timezone GMT-08
no clock summertime
      or
clock set hh:mm:ss month day year
```

- **Создайте внутренний логический интерфейс**

```
interface Loopback0
   ip address X.X.X.X Y.Y.Y.Y
   no shut
```



Сообщение при загрузке

Cisco.com

- **При загрузке должно выводиться ясное сообщение:**


```
banner motd #
C i s c o  S y s t e m s
       ||        ||
       ||        ||            Cisco Systems, Inc.
      ||||      ||||           Enterprise Network Services
  ..:||||||:..:||||||:..

US, Asia & Americas support:    + 1 222 555 1234
EMEA support:                   +21 010 555 1234

UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
All attempts to access this system and/or its resources are recorded.
Unauthorized attempts may subject you to a fine and/or imprisonment in
accordance with Title 18, USC, Section 1030.]
```

- **Для использования с PIX:**

```
auth-prompt If You Are Not Authorized…
```

Сообщение после авторизации

Cisco.com

- **Авторизовавшимся пользователям бывает полезно напомнить о местных реалиях:**

```
banner exec ^
IT administered router.
Mail "net-americas" with any proposed configuration
changes, or call the Technical Resource Center at x5-
5555.
^
```


Пароли

Cisco.com

- **Установите защищенный паролем доступ к командам управления:**
  - Старое шифрование пароля 7 (код Виженера)

```
router(config)# enable password <some password>
router(config)# service password-encryption
```

  - Новое шифрование пароля 5 (хеширование MD5)

```
router(config)# enable secret <some password>
router(config)# no enable password
```

- **Введите пароли**
  - Служит для резервной аутентификации
  - Используется шифрование пароля 7

```
router(config)# line vty 0 4
router(config-line)# password <some other password>
```

- **Замечание: во всех устройствах для защиты паролем должен использоваться режим ‘enable secret’**

Дополнительные функции

Cisco.com

- Отключите эти функции! (отключены по умолчанию в 12.x)
- Дополнительные функции UDP и TCP могут быть использованы для атак DoS
  - echo, discard, systat, daytime

```
router(config)# no service udp-small-servers
router(config)# no service tcp-small-servers
```

- Finger—текущие имена пользователей

```
router(config)# no service finger
```

- Bootp—bootp сервер

```
router(config)# no service finger
```


Дополнительные функции

Cisco.com

- Отключите эти функции! (отключены по умолчанию в 12.x)
- IDENT—удаленные функции IDENT

```
router(config)# no ip identd
```

- X.25 PAD—обмен информацией о каналах X.25

```
router(config)# no service pad
```

- MOP—выключение протокола управления DEC

```
router(config-if)# no service-mop
```

- DHCP—выключение DHCPd

```
pix(config)# no dhcpd enable
```

Дополнительные функции интерфейсов

Cisco.com

- **IP redirects—маршрутизатор отсылает сообщение о перенаправлении в случае отправки пакета через интерфейс получения**

```
router(config-int)# no ip redirects
```

- **Direct-broadcast—если пакет предназначен для широковещательного адреса в сети, маршрутизатор начнет вещание на физическом уровне в прилегающей сети (механизм всех атак SMURF в интернет)**

```
router(config-int)# no ip direct-broadcast
```

- **Proxy-arp**

```
router(config-int)# no ip proxy-arp
pix(config)# sysopt noproxyarp
```

- **Source routing—в протоколе IP содержится разрешение хост-станции источника определять маршрут по интернету**

```
router(config-int)# no ip source-route
```


Дополнительные сервисные функции

Cisco.com

- **CDP**
- **HTTP Server**
- **NTP**

Cisco Discovery Protocol (CDP): что это?

Cisco.com

- CDP - это фирменный протокол Cisco

  Протокол уровня L2, информирующий устройство о наличии в сети других устройств; CDP работает в различных средах; дает информацию о IP адресе, физическом порте, версии SW, платформе HW

- Позволяет администраторам сети обнаружить работающее в ближайшем окружении оборудование Cisco, дает информацию о номерах моделей и версиях ПО
- Будьте осторожны: существует ПО, заполняющее пакеты обновления CDP бесполезной или фальсифицированной информацией

Cisco Discovery Protocol

Cisco.com

```
switch#show cdp neighbors detail
-------------------------
Device ID: Excalabur
Entry address(es):
  IP address: 4.1.2.1
Platform: cisco RSP2,  Capabilities: Router
Interface: FastEthernet1/1,  Port ID (outgoing port):
   FastEthernet4/1/0
Holdtime : 154 sec

Version :
Cisco Internetwork Operating System Software
IOS (tm) RSP Software (RSP-K3PV-M), Version 12.0(9.5)S, EARLY
   DEPLOYMENT MAINTENANCE INTERIM SOFTWARE
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Fri 03-Mar-00 19:28 by htseng
```

Нужно ли Вам использовать CDP?

Cisco.com

- Нужно найти компромисс между простотой устранения неполадок и накоплением избыточной информации
- Протокол необходим для использования некоторых функций
  - Управление сетью
  - Автоответчик экстренных служб Cisco (911)
  - Aux VLANs (используется в IP-телефонии)
  - Сканирование неавторизованных точек доступа (Rogue Access Point) (с помощью APtools)

Cisco Discovery Protocol

Cisco.com

- Если у Вас нет причин для использования CDP, полностью отключите его поддержку
  - Полное отключение

```
router(config)# no cdp run
```

- Как минимум, протокол должен быть отключен на всех интерфейсах, выходящих во внешние сети (операторские и т.д.)
  - Отключение на интерфейсе

```
router(config-int)# no cdp enable
```

IP HTTP Сервер

Cisco.com

- Без использования на сервере HTTP secure-http либо встроенной аутентификации с ACL, сервер не защищен и может быть атакован
- Где может понадобиться сервер HTTP:
  - Управление правилами QoS
  - Управление защитой устройств
  - Управление защитой устройств PIX

IP HTTP Сервер

Cisco.com

- Если вам необходимо использовать сервер HTTP, защитите его с помощью HTTPS и воспользуйтесь локальными паролями username/password, TACACS+ или RADIUS

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
crypto key generate rsa usage 1024
ip http secure-server
ip http authentication aaa
```

- Отключение

```
no ip http server
```

NTP: Протокол сетевого времени

Cisco.com

- NTP является открытым стандартом, описан в RFC 1305
- NTP синхронизирует часы в сетевых устройствах / системном оборудовании
- NTP необходим для:
  - Точного протоколирования
  - Подтверждения подлинности сертификатов
  - Kerberos tickets
- NTP поддерживается во всем оборудовании Cisco, а также многими (если не всеми) операционными системами

Аутентификация NTP

Cisco.com

- Аутентификация источника времени чрезвычайно важна для того, чтобы быть уверенным, что атака извне не повлияла на часы станций
- Прекращает неавторизованные попытки обновлениях данных синхронизации от неизвестных источников
- В результате протоколирования можно определить адреса, пытающиеся изменить системное время

Аутентификация NTP: Cisco IOS

Cisco.com

- **Установите синхронизацию времени в значения X.X.X.X и Y.Y.Y.Y при помощи NTP (версия 3); обратите внимание, что ключ аутентификации NTP 10 является условием обмена**

```
access-list 13 permit X.X.X.X
access-list 13 permit Y.Y.Y.Y
ntp server X.X.X.X version 3 key 10
ntp server Y.Y.Y.Y version 3 key 10
ntp access-group peer 13
```

- **Определите интерфейс источника**

```
ntp source LoopBack0
```

- **Установите аутентификацию для NTP, установите пароль и задайте рабочие ключи**

```
ntp authenticate
ntp authentication-key 10 md5 <password>
ntp trusted-key 10
```


Аутентификация NTP: Catalyst OS

Cisco.com

- **Задайте сервер NTP и ключ**

```
switch> set ntp server X.X.X.X key 10
NTP server 10.0.1.1 with key 10 added.
```

- **Задайте режим (клиентский)**

```
switch> set ntp client enable
NTP Client Mode enabled.
```

- **Настройте аутентификацию, пароль и рабочие ключи**

```
switch> set ntp authentication enable
NTP Authentication feature enabled
switch> set ntp key 10 trusted md5 <some password>
```

Необходимые функции: временные метки

Cisco.com

- **Для обеспечения достоверности записи информации**

```
router(config)# service timestamps debug datetime
msec localtime show-timezone
router(config)# service timestamps log datetime msec
localtime show-timezone
router(config)# clock timezone <timezone standard
time> <offset>
router(config)# clock summer-time <timezone summer>
recurring
```

Необходимые функции: протоколирование

Cisco.com

- **Многие функции могут быть запротоколированы**
- **Получатели журнально информации:**
  - **Консоли**
  - **Сервер UNIX syslog (по умолчанию, это local7.debug)**
  - **Сессии удаленных пользователей VTY**
  - **Локальный буфер протокола (в RAM маршрутизатора)**
- **Протоколирование обеспечивает фиксацию активности**
- **Протоколируемые события делятся по уровням (обычный—приоритетный)**

Необходимые функции: протоколирование

Cisco.com

- **Протоколирование информации на сервер протоколирования (syslog)**

```
router(config)# logging 192.0.2.2
```

- **Воспользуйтесь возможностью полной детализации протоколирования для детального контроля активности**

```
router(config)# logging buffered 16384
router(config)# logging trap informational
router(config)# logging facility local7
router(config)# logging source-interface ethernet 0
router(config)# no logging console
```


Системное протоколирование: PIX

Cisco.com

- **Воспользуйтесь возможностью полной детализации протоколирования для детального контроля активности**

```
logging buffered 16384
logging console critical
logging trap informational
logging facility 23
```

- **Укажите сервер Syslog**

```
logging 10.0.0.252
```

Администрирование доступа пользователей к устройствам

Основные положения администрирования доступа пользователей к устройствам

Cisco.com

- SNMP
- Установки VTY
- Настройки SSH
- Локальные учетные записи
- TACACS+
- RADIUS
- Kerberos
- Уровни привилегий
- Доступ CLI на основе ролей
- Управление настройками и протоколирование
- Автозащита

SNMP

Cisco.com

- **Версия 1—все еще широко поддерживается**
  - **В качестве модели аутентификации используются обычные текстовые ключи групп**
- **Версия 2—применяется в настоящее время**
  - **Все еще использует обычные текстовые ключи групп**
- **Версия 3—стандарт IETF с дополнительной защитой**
  - **Аутентификация: username + password**
  - **Защита личных данных: DES**
  - **Контроль доступа: модель досупа к данным на основе групп**

Настройка SNMPv2

Cisco.com

Пример настройки:

```
snmp-server trap-source Loopback0
! NMS server in the US
snmp-server host 10.0.0.251
snmp-server host 192.168.0.252 envmon bgp snmp
snmp-server location Somewhere, Some State
snmp-server contact Example.com NOC, 555-1212
snmp-server community <some password> RO 1
snmp-server community <some other password> RW 2
! NMS server in the US
access-list 1 permit 10.0.0.251
access-list 2 permit 192.168.0.252
```

Настройка SNMPv3

Cisco.com

- **Поддерживается начиная с 12.0.3(T) на определенных платформах**
- **Обратите внимание, получатель должен понимать SNMPv3**

```
snmp-server trap-source Loopback0
! NMS server in the US
snmp-server group remotegroup v3 noauth
snmp-server user remoteuser remotegroup remote
10.0.0.251 v3
snmp-server host 10.0.0.251 informs version 3
  noauth remoteuser config
! NMS server in the US
access-list 1 permit 10.0.0.251
```


Настройка SNMP для PIX

Cisco.com

Пример настройки:

```
snmp-server location Somewhere, Some State
snmp-server contact Example.com NOC, 555-1212

snmp-server host 10.0.0.251
snmp-server host 192.168.0.252
snmp-server community <some password>
snmp-server enable traps
```

Возможности защиты SNMP

Cisco.com

Версия	Уровень	Аутентификация	Шифрование	Описание
V1	NoAuth NoPriv	Community String	Нет	Для аутентификации используется ключ группы
V2c	NoAuth NoPriv	Community String	Нет	Для аутентификации используется ключ группы
V3	NoAuth NoPriv	Username	Нет	Для аутентификации используется Username
V3	Auth NoPriv	MD5 либо SHA	Нет	Аутентификация на основе HMAC
V3	Auth Priv	MD5 либо SHA	DES	Аутентификация на основе HMAC 56-bit DES шифрование

Безопасность VTY

Cisco.com

Доступ к VTY должен контролироваться и авторизовываться

- Контроль ведется с помощью списков доступа
- Аутентификация: пароль на локальной станции, TACACS+, RADIUS, Kerberos
- Механизмом передачи должен быть только SSH

Настройка портов VTY

Cisco.com

- Время бездействия на асинхронных портах по умолчанию 10 minutes 0 seconds

```
exec-timeout 10 0
```

- Значение времени бездействия 0 означает постоянное соединение
- Активируйте контроль соединения TCP на входящих сессиях

```
service tcp-keepalives-in
```

- Активируйте контроль соединения TCP на исходящих сессиях

```
service tcp-keepalives-out
```


Консольные сервера

Cisco.com

- Что вы думаете о консолях?

  Консоль защищена системным паролем, верно?
  Вам действительно нужен еще один пароль доступа?

- Прерванные сессии могут оставлять на системных консолях сессию доступа (доступ к маршрутизатору!)

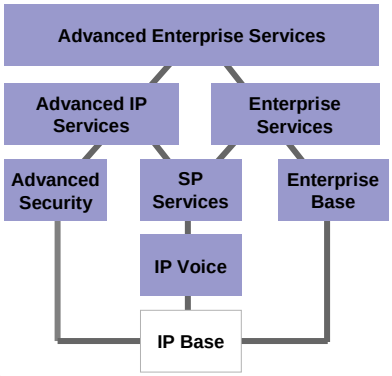
```
$
$ telnet server-con
Trying 192.0.2.101...
Connected to server-con (192.0.2.101)
server #
```

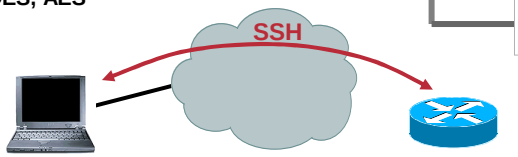
- Необходимо всегда контролировать доступ к консольным устройствам

SSH: Cisco IOS

Cisco.com

- Предоставляет управляемую, зашифрованную сессию работы с маршрутизатором
- SSH версия 1 поддерживается в:
  - Начиная с 12.1(1)T—только сервер
  - Начиная с 12.1(3)T—сервер и клиент
- SSH версия 2 поддерживается в :
  - Начиная с 12.1(19)E/12.2(22)S—только сервер
  - Начиная с 12.3(4)T—сервер и клиент
- Поддержка типов шифрования:
  - V1—DES, 3DES
  - V2—3DES, AES





Настройка SSH: Cisco IOS

Cisco.com

- Настройте имя домена
  `IP domain-name something.com`
- Создайте и проверьте ключ RSA
  `crypto key generate rsa`
- Ограничьте доступ хост-станций / подсетей к маршрутизатору SSH
  `access-list 11 permit X.X.X.X Y.Y.Y.Y`
  `access-list 11 permit Y.Y.Y.Y Y.Y.Y.Y`
- Задайте время бездействия и количество попыток ввода пароля
  `ip ssh time-out 60`
  `ip ssh authentication-retries 2`
- Задайте SSH на линиях VTY маршрутизатора
  `line vty 0 4`
  `transport input ssh`
- По желанию, можно разрешить использовать только одну версию SSH
  `ip ssh version 2`

Настройка SSH: Catalyst OS

Cisco.com

- Создайте и проверьте ключ RSA

```
vega> (enable) set crypto key rsa 1024
Generating RSA keys.. [OK]
```

- Ограничьте доступ хост-станций / подсетей к коммутатору SSH

```
vega> (enable) set ip permit 144.254.3.0 255.255.255.128
```

- Активируйте SSH на коммутаторе

```
vega> (enable) set ip permit enable ssh
  SSH permit list enabled.
```

- По желанию, можно разрешить использовать только одну версию SSH (с версии 8.3)

```
set ssh mode v2
```

- Если вы забудете задать хост-станцию / подсеть, коммутатор выдаст предупреждение: WARNING!! IP permit list has no entries

Настройка SSH: PIX

Cisco.com

- Создайте и проверьте ключ RSA

```
ca gen rsa key 1024
```

- Ограничьте доступ хост-станций / подсетей к SSH для PIX в сети

```
ssh X.X.X.X Y.Y.Y.Y inside
```

- Задайте время бездействия и количество попыток ввода пароля

```
ssh timeout 60
```

- Отключите telnet

```
no telnet 0.0.0.0 255.255.255.255
```

Установление соединения с устройством Cisco с помощью SSH

Cisco.com

- **Поддерживаемые приложения: Execution shell, remote command execution и Secure Copy Protocol (SCP)**
- **Не поддерживаются X11, TCP и agent forwarding**
- **С командной строки**

```
ssh –c 3des routername
```

- **Примеры SSH со стороны клиента:**

  В этом примере пользователь joeuser должен ввести свой пароль; в случае ввода правильного пароля команда вернет значение “show ip route”

```
ssh -l joeuser inet-rtr-us-1 ‘show ip route’
```

  В этом примере пользовательr jimuser устанавливает 3DES соединение с маршрутизатором inet-rtr-ua-1 и имеет до 4 попыток ввода пароля

```
ssh -l jimuser -c des3 -o numberofpasswdprompts 4
       inet-rtr-us-1
```


SCP: копирование в целях безопасности

Cisco.com

- **SCP поддерживается в:**

  12.1.(1)T—сервер

  12.1.(3)T—клиент

- **После настройки SSH активируйте SCP**

```
ip scp server enable
```

- **Примеры SCP со стороны клиента :**

  В этом примере действующей конфигурацией копируется с маршрутизатора на хост назначения с помощью scp

```
rtr-us-1# copy running-confg scp://tiger@10.1.1.2/
Address or name of remote host [10.1.1.2]? <ret> Destination username
  [tiger]? <ret>
  Destination filename [rtr-us-1-confg]? <ret>
  Writing rtr-us-1-confg
  Password: f00bar
rtr-us-1# exit
```

Аутентификация доступа у устройству

Cisco.com

- Локальные пароли (username, password)
- Kerberos
- TACACS+
- RADIUS
- Уровни привилегий
- Просмотры CLI на основе ролей

Объезд: пароли

Cisco.com

- Не используйте легко подбираемые или очевидные пароли
- Изменяйте пароли «по умолчанию»
- Сделайте управление паролями централизованным
  - RADIUS, TACACS+
- Не используйте одинаковые пароли в системах различных типов

Относительная эффективность паролей

Cisco.com

Пароли Windows NT/2000

Cisco.com

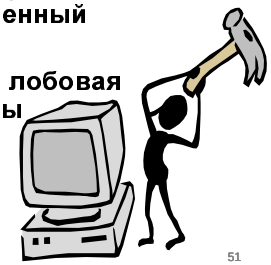
- Пары паролей хранятся в Security Account Manager (SAM)
  - LAN Manager (слабый) использует DES 56
  - NT hash (сильнее) использует шифрование MD4
- Пароли LAN Manager нечувствительны к регистру
  - Перед созданием последовательности LAN Manager пароль конвертируется в верхний регистр
  - 14-знаковый пароль разбивается на два отдельных выражения
  - Каждое 7-знаковое выражение шифруется по DES; 8-знаковые зашифрованные выражения суммируются для создания 16-знаковой последовательности
- pwdump3 (http://www.polivec.com/pwdump3.html) извлекает хеши паролей из реестра Windows удаленно

Методология взлома паролей

Cisco.com

Средства взлома используют различные методологии, среди них:

- Подбор по словарю взламывает самые слабые пароли (самый быстрый метод)
- Гибридный подход добавления нескольких символов к словарю / списку слов (более медленный, чем метод словаря / списка слов)
- Лобовая атака подбором комбинаций символов, включая и специальные символы (самый медленный метод)
- При эвристическом сканировании применяется лобовая атака вместе со статистической оценкой частоты символов, встречающихся в паролях



Локальная аутентификация

Cisco.com

- Используется локальная база данных username/password
- Можно установить “local” в качестве предпочтительного метода или резервного метода
- Можно установить тип шифрования пароля (тип 7 или тип 5) либо не использовать пароль (тип “0”)
- Можно использовать список доступа для контроля доступа по IP адресам
- При большом количестве используемых маршрутизаторов возникают трудности в управлении

Локальная аутентификация

Cisco.com

- **Настройка локальной аутентификации**

```
aaa authentication login default local enable
```

- **Объявление пар username/password (тип 7)**

```
username jsmith password mypassword
```

- **Используйте ‘username secret’ для однонаправленного алгоритма шифрования (тип 5)**

```
router(config)#username jsmith secret mypassword
```


TACACS+

Cisco.com

- **Для обмена информацией между клиентом и сервером используется TCP**
- **Поддержка нескольких дублируемых серверов TACACS**
- **Возможность использования функций AAA (authentication, authorization, accounting)**
- **База данных хранится в хешируемой таблице**
- **Существует опция шифрования информации с помощью MD5 перед передачей по сети**

Настройка аутентификации TACACS+: Cisco IOS

Cisco.com

- **Активизируйте TACACS**

```
aaa new-model
aaa authentication login default tacacs+ enable
```

Обязательная настройка для шифрования пакетов

- **Задайте ключ сервера**

```
tacacs-server key Bre3kD0wn
```

- **Задайте сервер TACACS и резервный сервер**

```
tacacs-server host 10.0.0.253
tacacs-server host 10.0.0.254
tacacs-server timeout 15
```


Настройка аутентификации TACACS+: PIX

Cisco.com

- **Настройте TACACS**

```
aaa-server Outgoing protocol tacacs+
```

- **Определите сервер(а) TACACS и задайте пароль**

```
aaa-server Outgoing (inside) host 10.0.0.253
<password> timeout 5
aaa-server Outgoing (inside) host 10.0.0.254
<password> timeout 5
```

Настройка аутентификации TACACS+: CatOS

Cisco.com

```
Turn on TACACS
TACACS server
Do this in this order, otherwise if you get
disconnected, it will still be asking for TACACS.
!Step 1
set authentication login local enable
! Step 2
set authentication login tacacs enable
set tacacs server 10.0.0.253
set tacacs server 10.0.0.254
set tacacs key BreAk1td0wn
```

Обязательная настройка для шифрования пакетов

Учетная система TACACS+

Cisco.com

- Ведет учет используемых услуг
- Ведет учет потребления сетевых ресурсов
- Учет может производиться на уровнях сети, соединения либо EXEC
- Типы записей учета: начало события, окончание события
- Каждая запись содержит 6 основных полей данных: временные отметки, имя устройства, имя пользователя, порт, адрес, тип записи
- Запись осуществляется в форме пар “атрибут-значение”

Настройка учетной системы TACACS+

Cisco.com

```
! Turn on tacacs+
aaa new-model
aaa authentication login default tacacs+ enable
tacacs-server key <some password>
tacacs-server host 10.0.0.253
tacacs-server host 10.0.0.254
tacacs-server timeout 15
! set up TACACS accounting
aaa accounting exec start-stop tacacs+
aaa accounting connection start-stop tacacs+
aaa accounting network start-stop tacacs+
aaa accounting system start-stop tacacs
```


Система отчетов TACACS+

Cisco.com

TACACS+ предоставляет детальные отчеты по событиям на сетевых устройствах

User-Name	Group-Name	cmd	priv-lvl	service	NAS-Portname	task_id	NAS-IP-	reason
kuiperl	NOC	enable <cr>	0	shell	tty0	4	210.210.51.224	
kuiperl	NOC	exit <cr>	0	shell	tty0	5	210.210.51.224	
kuiperl	NOC	no aaa accounting exec Worksho	0	shell	tty0	6	210.210.51.224	
kuiperl	NOC	exit <cr>	0	shell	tty0	8	210.210.51.224	
pfs	NOC	enable <cr>	0	shell	tty0	11	210.210.51.224	
pfs	NOC	exit <cr>	0	shell	tty0	12	210.210.51.224	
kuiperl	NOC	enable <cr>	0	shell	tty0	14	210.210.51.224	
kuiperl	NOC	show accounting <cr>	15	shell	tty0	16	210.210.51.224	
kuiperl	NOC	write terminal <cr>	15	shell	tty0	17	210.210.51.224	
kuiperl	NOC	configure <cr>	15	shell	tty0	18	210.210.51.224	
kuiperl	NOC	exit <cr>	0	shell	tty0	20	210.210.51.224	
kuiperl	NOC	write terminal <cr>	15	shell	tty0	21	210.210.51.224	
kuiperl	NOC	configure <cr>	15	shell	tty0	22	210.210.51.224	
kuiperl	NOC	aaa new-model <cr>	15	shell	tty0	23	210.210.51.224	
kuiperl	NOC	aaa authorization commands 0 de	15	shell	tty0	24	210.210.51.224	
kuiperl	NOC	exit <cr>	0	shell	tty0	25	210.210.51.224	
kuiperl	NOC	ping <cr>	15	shell	tty0	32	210.210.51.224	
kuiperl	NOC	show running-config <cr>	15	shell	tty66	35	210.210.51.224	
kuiperl	NOC	router ospf 210 <cr>	15	shell	tty66	45	210.210.51.224	
kuiperl	NOC	debug ip ospf events <cr>	15	shell	tty66	46	210.210.51.224	

RADIUS

Cisco.com

- Похож на TACACS+, является стандартом
- Так же предоставляет возможность использования функций AAA
- Для связи с сервером используется UDP (порт 1645/1812) и работы системы учета (порт 1646/1813)
- Имеет функцию временного ограничения для паролей для; аутентификацию как и TACACS+
- Пароли можно шифровать с помощью DES

Настройка аутентификации RADIUS: Cisco IOS

Cisco.com

```
! Turn on RADIUS
aaa new-model
aaa authentication login default radius local
aaa authentication ppp dialin radius local
! Specify radius server and backup servers
radius-server key Bu1ldUp
radius-server host 192.168.0.253
radius-server host 192.168.0.254
radius-server timeout 15
```

Настройка аутентификации RADIUS: PIX

Cisco.com

```
! Turn on Radius
aaa-server RADIUS protocol radius
aaa-server AuthInbound (inside) host 192.168.0.253 <some
  password> timeout 20
aaa-server AuthInbound (inside) host 192.168.0.254 <some
  password> timeout 20
! Shared password
radius-server key <some password>
! Specifies RADIUS server auth port
sysopt radius auth-port 1645
! Specifies RADIUS server accounting port
sysopt radius acct-port 1646
```


Настройка аутентификации RADIUS: CatOS

Cisco.com

```
! Turn on Radius server
! Do this in this order, otherwise if you get
! disconnected, it will still be asking for Radius
! Step 1
set authentication login local enable
! Step 2
set authentication login radius enable
set radius server 192.168.0.253 auth-port 1645 acct-port 1646
  primary
set radius server 192.168.0.254 auth-port 1645 acct-port 1646
set radius key <password>
```

Система учета RADIUS

Cisco.com

- Уникальные идентификаторы учетных записей облегчают учет ресурсов
- Общее время фиксируется в записи окончания события
- Записи заносятся в буфер до подтверждения их получения
- Записям учета присваиваются флаги “начало” или “конец” записи
- Атрибуты учета определены в файле `/etc/raddb/dictionary`

Настройка системы учета RADIUS: Cisco IOS

Cisco.com

```
! Turn on RADIUS
aaa new-model
aaa authentication login default radius enable
radius-server key Bu1ldUp
radius-server host 192.168.0.253
radius-server host 192.168.0.254
radius-server timeout 15
! set up RADIUS accounting
aaa accounting exec start-stop radius
aaa accounting connection start-stop radius
aaa accounting network start-stop radius
aaa accounting system start-stop radius
```

Kerberos

Cisco.com

- Система аутентификации запросов от ресурсов сети
- Для работы необходим сервер Kerberos
- Поддерживаемые системы команд:
  - telnet, rlogin, rsh и rcp
- Основные процессы:
  - Пользователь аутентифицируется на маршрутизаторе
  - Получает разрешительную запись (TGT)
  - Пользователь аутентифицирован для использования услуг сети

Настройка Kerberos

Cisco.com

```
service password-encryption
hostname router1
!Set default user authentication to be Kerberos 5
aaa new-model
aaa authentication login default krb5 enable
kerberos local-realm example.com
kerberos srvtab entry host/router1.example.com@EXAMPLE.com
   /etc/krb5.keytab
kerberos server example.com 10.0.0.252
kerberos credentials forward
!
line vty 0 4
   access-class 11 in
   transport preferred telnet
   login authentication default
```

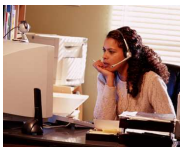
Сравнение RADIUS, TACACS+, Kerberos

Cisco.com

	RADIUS	TACACS+	KERBEROS
Использование UDP	X		
Использование TCP		X	X
Шифрование	Только пароль	Все кроме заголовка	Все кроме заголовка
Поддержка нескольких протоколов		X	
Контроль учета использования маршрутизатора		X	X
Контроль процесса аутентификации на маршрутизаторе		X	X
Поддержка LEAP	X		
Поддержка XAUTH	X	X	X

Детальная авторизация

Cisco.com


Оператор


Сетевые операции


DBMS/ инженер приложений


Операции защиты


Планирование емкости
- Отображение
- И т.д..


Сетевой инженер
- Настройка
- Отображение
- И т.д.

Дифференцированный подход для обеспечения обслуживания

Уровни привилегий

Cisco.com

- Уровни могут присваиваться каким-либо командам
- Это обеспечивает больше возможностей для детальной авторизации
- По умолчанию на маршрутизаторе установлено три уровня привилегий:
  - Уровень привилегий 1 = без привилегий (команда router>), уровень по умолчанию для авторизации
  - Уровень привилегий 15 = привилегированный (команда router#), уровень после входа в режим enable
  - Уровень привилегий 0 = редко используемый, включает 5 команд: disable, enable, exit, help и logout

Пример: уровни привилегий

Cisco.com

```
username jsmith privilege 9 password secret TiaP4tCy
username joeuser privilege 6 password secret NagP@tTn
username poweruser privilege 15 password secret S3pn2spu
username inout password inout
username inout privilege 15 autocommand show running
privilege configure level 8 snmp-server community
privilege exec level 6 show running
privilege exec level 8 configure terminal
```

Пример: уровни привилегий

Cisco.com

```
Router#show priv
Current privilege level is 9
Router#configure terminal
Router(config)#?
Configure commands:
  exit         Exit from configure mode
  help         Description of the interactive help system
  no           Negate a command or set its defaults
  snmp-server  Modify SNMP engine parameters
Router(config)#exit
Router#show run
Building configuration...

Current configuration : 157 bytes
!
!
snmp-server community 5Nm@Str1n6 RO
snmp-server enable traps tty
snmp-server host 192.168.0.3 traps
!
end

Router#
```


Доступ к интерфейсу командной строки (CLI) на основе ролей

Cisco.com

- Новая функция: CLI на основе ролей или наборы команд CLI
- Функция доступа к CLI на основе административных ролей
- Безопасность

  Увеличивает защищенность устройств, задавая набор команд CLI , доступных конкретному пользователю
- Эксплуатационные характеристики

  Позволяет избежать случайного исполнения команд CLI неавторизованным персоналом
- Эксплуатационная эффективность

  Не позволяет пользователям видеть недоступные им команды CLI, что увеличивает эксплуатационную пригодность

Как это работает

Cisco.com

- Администратор должен задать набор команд, используя базовый набор “root”
  - Нет наборов по умолчанию
  - Для доступа к набору root необходимо иметь уровень привилегий 15
  - Необходимо создать набор и задать команды для него
- Пользователь имеет доступ к набору
  - Имя набора и пароль вводятся вручную
  - Набор присваивается автоматически при вводе имени пользователя
  - Пользователи, находящиеся в рамках определенного, могут использовать только команды его команды
  - Пользователи могут переходить между наборами, вводя имена и пароли

Как наборы команд CLI работает с другими настройками

Cisco.com

- Аутентификация, Авторизация и Учет (AAA)
  - Сначала с помощью команды `aaa new-model` необходимо включить AAA
  - С пользователем в локальной базе данных или на внешнем сервере AAA ассоциирован один набор
  - При подключении после обычной процедуры аутентификации пользователь получает доступ к соответсвующим командам определенного набора
- Уровень привилегий
  - Набор имеет преимущество использования перед уровнем привилегий
  - Пользователь помещается в уровень привилегий, если набор не существует
- Имя набора
  - Для пользователя может настраиваться только одно имя набора
  - Если имя набора не установлено, пользователю присваивается уровень привилегий
  - Имя набора и пароль чувствительны к регистру

Настройка

Cisco.com

- **Создайте набор**

  `parser view outsource-1`

- **Установите для него пароль**

  `Router(config-view)# password 5 V14o5g1`

- **Добавьте команды**

  `commands <parser mode> {include | include-exclusive} [all] command`

  `commands exec include show version`

- **Вход в набор**

  `enable view outsource-1`

Возможности наборов

Cisco.com

Operator

```
Router#enable view operator
Password: Oper@torPswd
*…view 'operator'
Router# ?
Exec commands:
 exit
 ping
 show
Router#show ?
 hardware
 interfaces
 version
```

NetOps

```
Router#enable view NetOps
Password: NetOps@Pswd
*…view 'NetOps'
Router# ?
Exec commands:
 clear
 configure
 copy
 enable
 exit
 ping
 show
Router#show ?
 controllers
 hardware
 interfaces
 version
Router#configure terminal
Router(config)#?
 access-list
 clock
 hostname
 interface
 ip
 line
```

SecOps

```
Router#enable view SecOps
Password: SecOps@Pswd
*…view 'SecOps'
Router# ?
Exec commands:
 configure
 copy
 enable
 exit
 login
 ping
 show
Router#show ?
 controllers
 crypto
 hardware
 interfaces
 key
 version
Router#configure terminal
Router(config)#?
 access-list
 crypto
 key
 li-view
```

Уведомление о смене настроек и протоколирование

Cisco.com

- Позволяет отслеживать изменения настроек, осуществленные в сессиях пользователями путем ведения протокола настроек
- Ведется запись каждой команды настройки, автора команды, возвратный код обработчика этой команды и время ввода команды
- Добавлен механизм уведомления, высылающий асинхронные уведомления зарегистрированным приложениям при изменении протокола настроек

Протоколирование изменений настроек

Cisco.com

- В протокол вносится следующая информация
  - Выполненная команда
  - Режим настройки, в котором выполнялась команда
  - Имя пользователя, давшего команду
  - Время подачи команды
  - Номер последовательности смены настройки
- Не протоколируются следующие типы команд
  - Команды – части файла настройки, применяющегося при исполнении команд копирования
  - Команды, вызвавшие синтаксическую ошибку
  - Неполные команды, вызывающие включение системы справки маршрутизатора

Уведомление о смене настроек и протоколирование

Cisco.com

- Активируйте режим архивирования для протоколирования изменения

```
Router(config)# archive
Router(config-archive)# log config
```

- Активируйте протоеолирование

```
Router(config-archive-log-cfg)#logging enable
```

- Определите максимальное число записей в протоколе

```
Router(config-archive-log-cfg)# logging size 200
```

- Запретите запись паролей в протоколе

```
Router(config-archive-log-cfg)# hidekeys
```

Не настроено по умолчанию

- Настройте передачу изменения на внешний сервер syslog

```
Router(config-archive-log-cfg)# notify syslog
```


Пример уведомления о смене настроек

Cisco.com

```
%SYS-5-CONFIG_I: Configured from console by kuiperl
%PARSER-5-CFGLOG_LOGGEDCMD: User:kuiperl  logged command:notify syslog
%PARSER-5-CFGLOG_LOGGEDCMD: User:kuiperl  logged command:privilege configure level 7 snmp-server host
%PARSER-5-CFGLOG_LOGGEDCMD: User:kuiperl  logged command:privilege configure level 7 snmp-server enable
%PARSER-5-CFGLOG_LOGGEDCMD: User:kuiperl  logged command:privilege configure level 7 snmp-server
%PARSER-5-CFGLOG_LOGGEDCMD: User:kuiperl  logged command:privilege exec level 7 ping
%PARSER-5-CFGLOG_LOGGEDCMD: User:kuiperl  logged command:privilege exec level 7 configure terminal
%PARSER-5-CFGLOG_LOGGEDCMD: User:kuiperl  logged command:privilege exec level 7 configure
%PARSER-5-CFGLOG_LOGGEDCMD: User:kuiperl  logged command:privilege exec level 6 show
%PARSER-5-CFGLOG_LOGGEDCMD: User:kuiperl  logged command:username joeuser privilege 6 password 0 xxxx
%SYS-5-CONFIG_I: Configured from console by kuiperl
%SYS-5-CONFIG_I: Configured from console by jsmith on vty0 (192.168.0.3)
%PARSER-5-CFGLOG_LOGGEDCMD: User:jsmith  logged command:snmp-server host 192.168.0.3 traps
%PARSER-5-CFGLOG_LOGGEDCMD: User:jsmith  logged command:snmp-server community xxxx
%SYS-5-CONFIG_I: Configured from console by jsmith on vty0 (192.168.0.3)
```

Пароли не записаны

Обзор автозащиты Cisco (AutoSecure)

Cisco.com

- Активация защиты устройства путем нажатия одной клавиши; быстро и без труда нейтрализуются потенциальные угрозы защите системы
- Изменение защитных состояний маршрутизаторов Cisco
  - Защищает уровень управления
  - Защищает уровень пересылки пакетов
- Стандартная функция Cisco IOS, начиная с версий 12.3 и 12.3T
- Поддерживаемые платформы:
- маршрутизаторы Cisco серий 800, 1700, 2600, 3600, 3700 и 7200

Автозащита Cisco

Cisco.com

- Отключает стандартные функции IP, которые можно использовать для атаки
- Включает функции IP, которые могут помочь при защите сети
- Добавлено новое свойство усиления: установка минимальной длины пароля
- Автозащита может быть установлена в двух основных режимах работы:
  - Интерактивный режим—предлагает пользователю выбрать включение / выключение функций и других процессов, относящихся к безопасности (работающих по умолчанию); обеспечивает гибкие возможности контроля
  - Не интерактивный режим—автоматически выполняет команду AutoSecure, используя рекомендованные по умолчанию установки; обеспечивает быстрое развертывание защиты маршрутизатора без участия человека

Ограничения автозащиты

Cisco.com

- **Версии ранее 12.3(8)T**
  - **Нет возврата к предшествующей вводу команды AutoSecure конфигурации**
  - **Необходимо сохранить текущую конфигурацию перед выполнением AutoSecure**
- **Версии старше 12.3(8)T**
  - **Сохраняет слепок текущей конфигурации при выполнении AutoSecure**
  - **Автоматический возврат в предыдущую конфигурацию при неудачном выполнении AutoSecure**

Автозащита отключает

Cisco.com

Основные

- **Finger**
- **Pad**
- **Small servers**
- **bootp**
- **http server**
- **cdp**
- **Identification service**
- **NTP**
- **Source routing**

Интерфейсные

- **icmp redirects**
- **icmp unreachables**
- **icmp mask reply messages**
- **proxy-arp**
- **Направленное вещание**
- **mop**

Автозащита активирует

Cisco.com

- Service-password encryption
- Service tcp-keepalives-in
- Service tcp-keepalives-out
- Системные сообщения
- Transport input/output
- Transport is only telnet and SSH
- Exec timeout 10
- Криптографические настройки ssh и scp с минимальным временем ожидания
- Отключает SNMP со свойствами “public”/“private”
- Logging console critical
- Logging buffered
- Logging trap debugging
- Запрос профиля настроек AAA
- CBAC

Если ПО поддерживает CBAC он будет настроен

Уровень пересылки пакетов: автозащита

Cisco.com

- **Включение CEF**
- **Включение uRPF**
- **Настройка следующих поименованых списков ACL:**
  - **autosec_iana_reserved_block**
  - **autosec_private_block**
  - **autosec_complete_block**

```
Configuring the named acls for Ingress filtering
autosec_iana_reserved_block: This block may subject to change by iana and for updated
list visit www.iana.org/assignments/ipv4-address-space.
1/8, 2/8, 5/8, 7/8, 23/8, 27/8, 31/8, 36/8, 37/8, 39/8,…
autosec_private_block:
10/8, 172.16/12, 192.168/16
autosec_complete_block: This is union of above two and the addresses of source multicast,
class E addresses and addresses that are prohibited for use as source.
source multicast (224/4), class E(240/4), 0/8, 169.254/16, 192.0.2/24, 127/8.
```

Средство проверки маршрутизатора Router Audit Tool

Cisco.com

Загружает настройки проверяемых устройств (по выбору), а затем сверяет их с заданными в эталонах настройками; для каждой проверяемой настройки составляется отчет со следующими данными:

- **Список всех проверенных правил с отметками о выполнении / невыполнении**
- **Средний процент соответствий**
- **Усредненный параметр соответствий (1–10)**
- **Список команд Cisco IOS которые помогут устранить имеющиеся проблемы**
- **Дополнительно, составит сводный отчет со списком всех правил (настроек) со всех устройств, а также усредненный параметр соответствия**

http://www.cisecurity.com/

Пример: средство проверки маршрутизатора

Cisco.com

Router Audit Tool report for
Router.example.com
Audit Date: Tue May 18 11:08:49 2004 GMT

Importance	Pass/Fail	Rule Name	Device	Line Number
10	Pass	no username Cisco	Router.example.com	
10	Pass	No ip pim accept-rp auto-rp	Router.example.com	
10	Fail	No ip http server	Router.example.com	
9	Pass	access-list 95 deny any	Router.example.com	
9	Pass	aaa new-model	Router.example.com	
9	Pass	aaa authentication login admin group tacacs+ enable	Router.example.com	
9	Fail	service password-encryption	Router.example.com	
8	Pass	no ip source route	Router.example.com	
7	Pass	no service udp-small-servers	Router.example.com	
7	Pass	no service tcp-small-servers	Router.example.com	
6	Pass	ip classless	Router.example.com	
6	Pass	ip domain-name example.com	Router.example.com	
5	Pass	snmp-server community trapcomm RO 95	Router.example.com	
4	Pass	logging x.x.x.x	Router.example.com	
4	Pass	logging buffered 16384 debugging	Router.example.com	

Защита протоколов маршрутизации

Удостоверение подлинности маршрута

Cisco.com

- Удостоверение подлинности пакетов обновлений маршрутов
- В обновления маршрутизации включается общий ключ
  - Обычный текст—защищает только от случайных ошибок
  - Message Digest 5 (MD5)—защищает и от случайных, и от умышленных ошибок
- Механизм часто не внедряется
  - “Даже не слышал ни о каких атаках”
  - “Коллеги этим не пользуются”

Удостоверение подлинности протокола маршрутизации

Cisco.com

- Не позволяет обновлять маршруты неустановленным источникам
- Обеспечивает управление контролем изменений в сети
- Отслеживает моменты, начиная с которых удаленная сеть более не может отсылать информацию (следит за состоянием поля истечения жизни информации для соединений с партнерами, операторами связи, либо локальной сетью), т.к. эта информация не может считаться достоверной
- Становится частью политики парольной защиты, которая может требовать периодической смены паролей

Удостоверение подлинности протокола маршрутизации

Cisco.com

- Внутренние протоколы маршрутизации
  - Удостоверение подлинности маршрута RIP v2
  - Удостоверение подлинности маршрута EIGRP
  - Удостоверение подлинности маршрута OSPF
- Внешние протоколы маршрутизации
  - Удостоверение подлинности маршрута BGP

Удостоверение подлинности маршрута RIP v2: Cisco IOS

Cisco.com

```
int Serial AA/BB
  ip rip authentication mode md5
  ip rip authentication key-chain rip-keys
key chain rip-keys
   key 1
   key-string <some password>
   send-lifetime infinite
   accept-lifetime 00:00:01 Jan 1 2002
        23:59:59 Dec 31 2002
router rip
  version 2
  passive interface default
  no passive Serial AA/BB
  redistribute static
  network X.X.X.X
  no default-information out
  no auto-summary
```


Удостоверение подлинности маршрута RIPv2: PIXOS

Cisco.com

Пример настроек:

```
rip outside passive version 2 authentication md5 <some
  password> 2

rip outside default version 2 authentication md5 <some
  password> 2
```

Удостоверение подлинности маршрута EIGRP

Cisco.com

```
int Serial AA/BB
  ip authentication mode eigrp 16799 md5
  ip authentication key-chain eigrp 16799 eigrp-keys
key chain eigrp-keys
   key 16799
   key-string <some password>
   send-lifetime infinite
   accept-lifetime 00:00:01 Jan 1 2002
        23:59:59 Dec 31 2002
router eigrp 6799
  eigrp log-neighbor-changes
  eigrp log-neighbor-warnings 60
  passive interface default
  no passive Serial AA/BB
  redistribute connected
  redistribute static
  network X.X.X.X
  no auto-summary
```


Удостоверение подлинности маршрута OSPF

Cisco.com

```
! OSPF Route Authentication to our Europe ISP

int Serial AA/BB
  ip ospf network non-broadcast
  ip ospf message-digest-key 1 md5 <password>
router ospf 1
  log-adjacency-changes
  passive-interface default
  no passive interface SerialAA/BB
  neighbor X.X.X.X
  network X.X.X.X Y.Y.Y.Y area 0
  area 0 authentication message-digest
```

Удостоверение подлинности маршрута BGP

Cisco.com

- Работает с соседним маршрутизатором либо всей группой маршрутизаторов
- Два маршрутизатора с несоответствующими паролями:

  %TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:179
- Один маршрутизатор с паролем, второй без:

  %TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's IP address]:179

Удостоверение подлинности маршрута BGP

Cisco.com

```
router bgp 200
 no synchronization
 neighbor 4.1.2.1 remote-as 300
 neighbor 4.1.2.1 description Link to Excalabur
 neighbor 4.1.2.1 send-community
 neighbor 4.1.2.1 version 4
 neighbor 4.1.2.1 soft-reconfiguration inbound
 neighbor 4.1.2.1 route-map Community1 out
 neighbor 4.1.2.1 password C2Ebgp
```

Уровень 2 / коммутаторы

Уровень 2 / коммутатор: основные вопросы

Cisco.com

- Контроль штормов
- Защита портов
- Инспектирование ARP
- Отслеживание DHCP
- Объединение
- PVLAN
- VACL
- Остовное дерево (Spanning Tree Protocol)

Контроль штормов (Storm control)

Cisco.com

Останавливает затопление широковещательными пакетоами на входных интерфейсах:

```
interface e0
 port storm-control threshold rising 120000 100000
 port storm-control filter
 port storm-control trap
 show port storm-control e0
```


Проблема: переполнение таблицы CAM!

Cisco.com

- Dsniff (macof) может генерировать на коммутаторе до 155,000 записей MAC в минуту
- Предполагая, что функция хэширования не дает ошибок, таблица CAM будет полностью заполнена после 131,052 (около 16,000 x 8) записи
  - Так как хэширование все же дает ошибки, на самом деле для переполнения таблицы CAM достаточно 70 секунд

```
CAT6506 (enable) sho cam count dynamic
Total Matching CAM Entries = 131052
```

- Как только таблица заполнится, трафик без записи в CAM распространяется во всей виртуальной локальную сети. Трафик, для которго уже были записи в CAM пересылается правильно.
- Эта атака также переполнит таблицы CAM ближайших коммутаторов

На выходе не-SPAN порта 10.1.1.50

```
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.1, 10.1.1.1 ?
10.1.1.22 -> (broadcast)  ARP C Who is 10.1.1.19, 10.1.1.19 ?
10.1.1.26 -> 10.1.1.25    ICMP Echo request (ID: 256 Sequence number: 7424) ← OOPS
10.1.1.25 -> 10.1.1.26    ICMP Echo reply (ID: 256 Sequence number: 7424) ← OOPS
```

Решение: Защита порта

Cisco.com

- Позволяет Вам назначать адреса MAC для каждого порта, либо обучаться коммутатору определенному количеству адресов MAC на порт
- Минимум один адрес
  - Возможности зависят от платформы
- Если кто-либо уберет машину и добавит новую, коммутатор не сможет переслать трафик

Защита порта

Cisco.com

- Защита порта
  - Настройте защиту порта или диапазона портов

```
CatOS> (enable) set port security mod/port... [enable | disable] [mac_addr]
[age {age_time}] [maximum {num_ of_mac}] [shutdown {shutdown_time}]
[violation {shutdown | restrict}]
IOS(config-if)# port security [action {shutdown | trap} | max-mac-count
addresses
```

  - Позволяет Вам назначать адреса MAC для каждого порта, либо возможность обучению определенному количеству адресов MAC на порт
  - При определении неверного MAC, коммутатор можно настроить для блокирования MAC либо блокирования всего порта
- Записи защиты портов (статические записи CAM) не удаляются

Примеры защиты портов

Cisco.com

```
CatOS> (enable) set port security 3/21 enable age 10 maximum 5 violation
shutdown
```

- Опция блокирования будет включена при атаке dsniff и порт будет закрыт

```
2004 Jul 03 15:40:32 %SECURITY-1-PORTSHUTDOWN:Port 3/21 shutdown
  due to no space
```

- Используйте команду *show port security* для отображения настройки защиты порта

Установки по умолчанию: Catalyst OS

Cisco.com

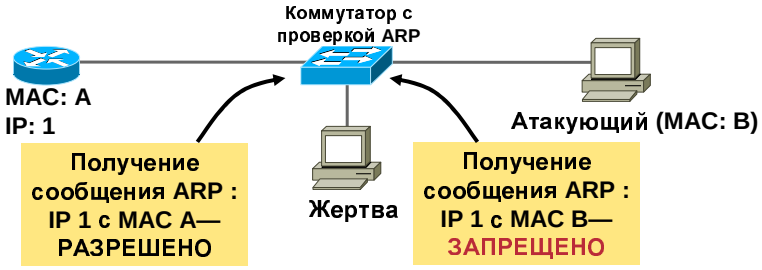
Установки защиты порта по умолчанию:

- Количество адресов на порт - один
- Действие при атаке – блокирование порта
- Время - постоянное (адреса не устаревают)
- Время блокирования - бесконечность

Защита от подмены ARP: проверка ARP

Cisco.com

- Впервые представлена недавно, в версии Catalyst OS (7.5) на 6K
- Использует VACL для ограничения пакетов ARP на конкретные IP адреса и конкретные адреса MAC
- Чрезмерное средство для всех систем, но применимое для шлюзов по умолчанию и других ключевых устройств



Пример проверки ARP

Cisco.com

```
CatOS> (enable) set security acl ip ACL-95 permit arp-inspection host 10.0.2.1 00-d0-b7-11-13-14
CatOS> (enable) set security acl ip ACL-95 deny arp-inspection host 10.0.2.1 any log
CatOS> (enable) set security acl ip ACL-95 permit arp-inspection host 10.0.2.2 00-d0-00-ea-43-fc
CatOS> (enable) set security acl ip ACL-95 deny arp-inspection host 10.0.2.2 any log
CatOS> (enable) set security acl ip ACL-95 permit arp-inspection any any
CatOS> (enable) set security acl ip ACL-95 permit ip any any
CatOS> (enable) commit security acl ACL-95
```

Смягчение последствий атаки злоумышленника с использованием DHCP

Cisco.com

Отслеживание DHCP

- Впервые появилось в 12.1(12c) на Catalyst 4000 Cisco IOS
- Определяет порты, которые могут отсылать ответы DHCP
- Может также ограничивать сообщения DHCP по скорости (используется для защиты коммутатора—порты закрываются, если скорость превышает предел)

```
! Enable DHCP Snooping
Switch(config)# ip dhcp snooping
! Enable DHCP on specific VLANs
Switch(config)# ip dhcp snooping vlan number [number]
! Set port with DHCP server as trusted
Switch(config-if)# ip dhcp snooping trust
! Rate-limit untrusted ports
Switch(config-if)# ip dhcp snooping limit rate rate
```


Динамический протокол магистрали (DTP) Административные состояния

Cisco.com

- Автоматизирует настройку магистрали ISL/802.1Q
- Состояния магистрали, настраиваемые администратором

ON	Я хочу быть магистралью и мне все равно, что вы там думаете! (используется, если на удаленном конце нет поддержки DTP)
OFF	Я не хочу быть магистралью и мне все равно, что вы там думаете! (используется когда на удаленном конце не выполняется ISL или .1Q)
Desirable	Мне хотелось бы стать магистралью VLAN; вы не против? (используется когда вы заинтересованы в том, чтобы быть магистралью)
Auto	Готов работать с чем вашей душе угодно! (По умолчанию на многих коммутаторах!)
Non-negotiate	Хочу быть магистралью и буду магистралью вот такого вида! (используется если необходима конкретная магистраль ISL или .1Q)

Отключение автоматических функций магистрали

Cisco.com

- Изменение установок по умолчанию в зависимости от коммутатора; всегда проверяйте:
  - Из документации Cisco: “Режим по умолчанию зависит от платформы…”
  - Для проверки из CLI:

```
CatOS> (enable) show trunk [mod|mod/port]
IOS(config-if)#show interface type number switchport
```

- Отключите автоматические функции магистрали на всех станционных портах:

```
CatOS> (enable) set trunk <mod/port> off
IOS(config-if)#switchport mode access
```


Проверенные методы защиты VLAN и магистрали

Cisco.com

- **Всегда** используйте особый VLAN ID для всех магистральных портов
- Отключайте неиспользуемые порты и помещайте их в неиспользуемые VLAN
- Соблюдайте сверх-осторожность: не пользуйтесь VLAN 1 ни для чего (если возможно)
- Установите все порты пользователей в режим «не-магистрали» (DTP off)

Коммутаторы LAN: PVLAN

Cisco.com

- Впервые представленные в серии коммутаторов 6500, частные VLAN (PVLAN) дают возможность изоляции Уровня 2 между портами в сети частной VLAN; это, так сказать, «VLAN внутри VLAN»

Частные VLAN

Cisco.com

- Для получения максимального эффекта при создании подсетей IP необходимо иметь крупные VLAN (особенно при использовании существующих IP адресов)
- С точки зрения безопасности наилучшим вариантом является выделение каждого пользователя в самостоятельную подсеть

Частные VLAN, 6500 и 4000

Cisco.com

На платформах 6500 и 4000 существует возможность изоляции портов одной и той же VLAN

- Это позволяет создать “виртуальную VLAN” внутри VLAN
- Эта возможность может распространяться на несколько устройств
- Совместима с защитой портов

Частные VLAN состоят из трех типов

Cisco.com

- Общие—с возможностью взаимодействия со всеми другими портами VLAN; обычно используются на портах, подключенных к маршрутизатору
- Изолированные—с полной изоляцией Уровня 2 от других портов коммутатора, за исключением общих портов
- Групповые—изоляция уровня 2 от портов, не являющихся частью группы, за исключением общих портов

Частные VLAN, ограничения

Cisco.com

- По соображениям безопасности, записи ARP на интерфейсах частных VLAN не устаревают
- Это создает проблемы при использовании DHCP

  Если пользователь отключает свой PC, нет возможности присвоить освободившийся IP адрес другому пользователю

  Однако, существует возможность отключения с 12.1.11E

```
MSFC:
Switch1(config)# int vlan 310
Switch1(config-if)# Description public part of pvlan
Switch1(config-if)# no ip pvlan-sticky-arp
```


Коммутаторы LAN: PVLAN

Cisco.com

```
set vlan 1 pvlan-type primary
set vlan 601 pvlan-type isolated
set vlan 602 pvlan-type community
! bind vlan 601 to vlan 1, and
! assign port 4/3 as vlan 601s isolated port
set pvlan 1 601 4/3
! bind vlan 602 to vlan 1, and
! assign ports 4/4-6 as community ports
set pvlan 1 602 4/4-6
! Set up the promiscuous ports
set pvlan mapping 1 601 3/1
set pvlan mapping 1 602 3/1
```

Граничные частные VLAN (Защищенные порты)

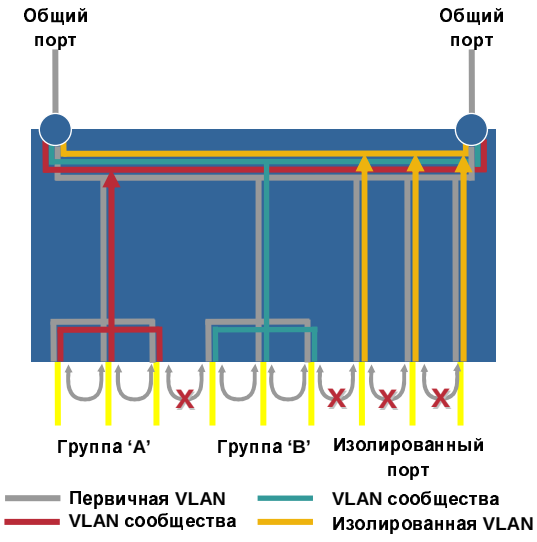
Cisco.com

- Функция версии PVLAN в 2950/3550
- Защищенный порт не пересылает трафик (рассылки в одном, нескольких, всех направлениях) на любой порт, также являющийся защищенным
- Пересылка от защищенного порта к незащищенному порту происходит по обычной схеме
- Работает только «внутри» одного коммутатора
- Не совместимо с защитой портов

Частные VLAN

Cisco.com

- Хост на изолированной VLAN может взаимодействовать только со шлюзом «по умолчанию»—но НЕ с другими хостами сети
- Взломанный веб-сервер не сможет атаковать другие PVLAN
- Изолируйте трафик в выделенных группах для создания определенных «сетей» внутри обычных VLAN
- Примечание: Обычно взаимодействие между хостами не происходит при включении PVLAN



VLAN ACL (VACL)

Cisco.com

- Итак, если мы можем использовать маршрутизатор для передачи трафика между частными сетями VLAN, как еще можно защитить хосты?
- В 6500 имеется возможность фильтрации на уровне L3 даже внутри одной и той же VLAN, VACL [список доступа VLAN], а также на уровнях настроек PVLAN
- Дает возможность контроля доступа для всех пакетов, перенаправляемых внутри VLAN либо имеющих точку назначения внутри или вне VLAN
- Применяется ко всему трафику VLAN—фильтрация по IP, IPX, либо смешанная (основанная на EtherType и адресе MAC)
- Безусловное “deny any any”
- На уровне контроля требуется PFC
- Обработка на уровне аппаратного обеспечения
- VACL ACE устанавливаются на TCAM
- Будьте осторожны: протоколирование VACL может повлиять на CPU; активизируйте функцию протоколирования с большой осторожностью

Настройка VACL

Cisco.com

- **Объявите VACL ACE**

```
Cat6k> (enable) set security acl ip TestACL deny tcp host 10.1.1.1 any eq telnet
Cat6k> (enable) set security acl ip TestACL deny icmp any host 10.1.1.254
Cat6k> (enable) set security acl ip TestACL permit any any
```

- **Передайте VACL**

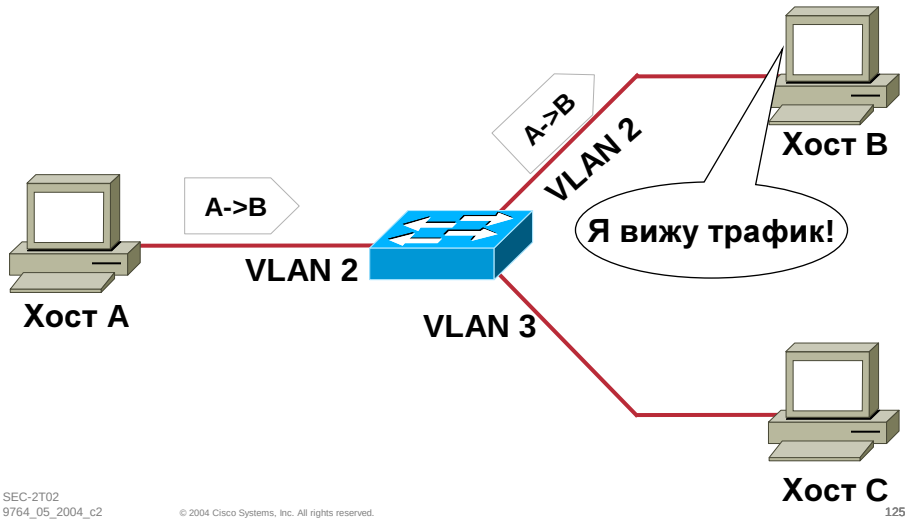
```
Cat6k> (enable) commit security acl TestACL
```

- **Отобразите на VLAN**

```
Cat6k> (enable) set security acl map TestACL 100
```

Обычная VLAN

Cisco.com

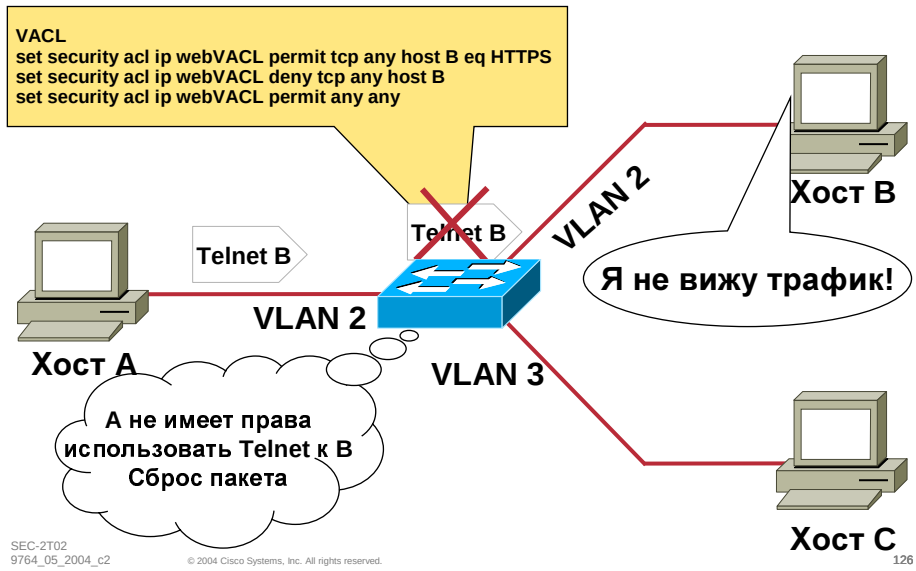


SEC-2T02
9764_05_2004_c2

125

Поведение VACL интра-VLAN (1/2)

Cisco.com

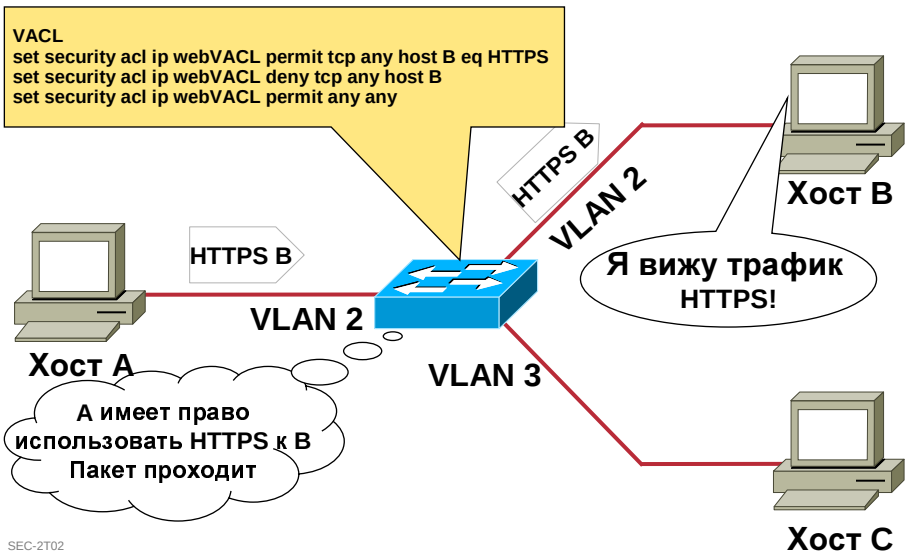


SEC-2T02
9764_05_2004_c2

126

Поведение VACL интра-VLAN(2/2)

Cisco.com

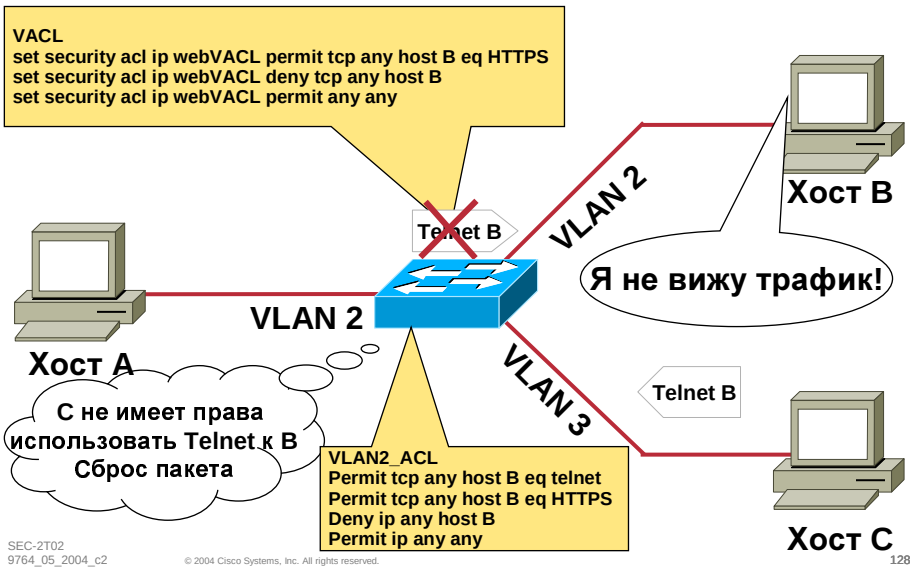


SEC-2T02
9764_05_2004_c2

127

Поведение VACL интер-VLAN (1/2)

Cisco.com

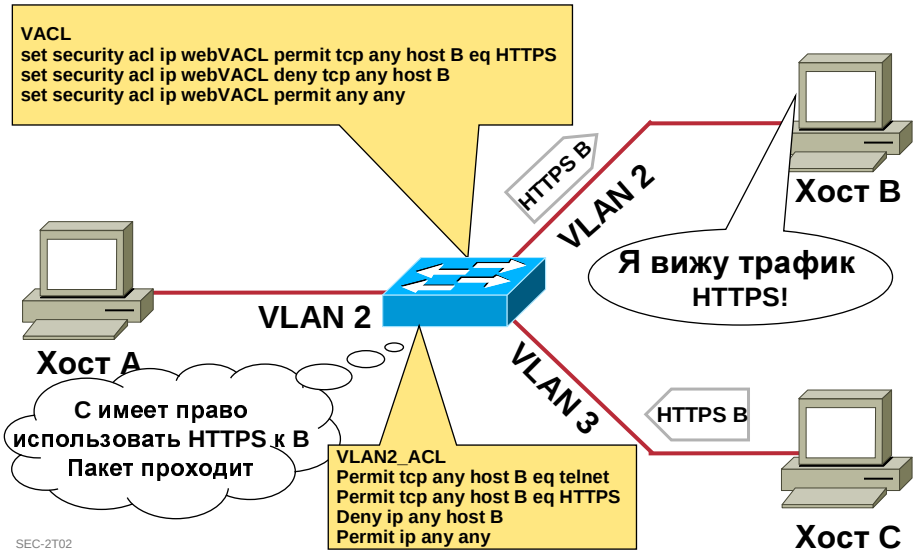


SEC-2T02
9764_05_2004_c2

128

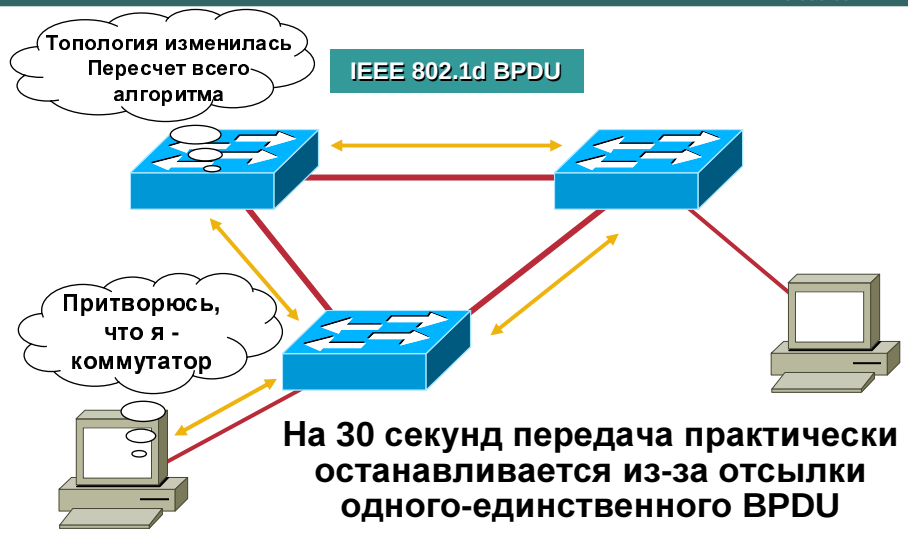
Поведение VACL интер-VLAN (2/2)

Cisco.com



Атака DoS с псевдо-коммутатора

Cisco.com



На 30 секунд передача практически останавливается из-за отсылки одного-единственного BPDU

Протокол Spanning Tree: BPDU Guard

Cisco.com

- Требуется настройка port fast
- Применяется на портах хостов
- Отключает порт при получении BPDU
- Переключение вручную либо через время, задаваемое командой set errordisable-timeout
- Порт не участвует в STP
- Настройка для каждого порта:

```
spanning-tree portfast
spanning-tree bpduguard enable
```


Защита от петель - Loop Guard

Cisco.com

- Не зависит от BPDU guard
- Применяется на портах хостов и портах к магистральным устройствам
- Не может применяться вместе с Root Guard (либо то, либо другое)
- Предотвращает заблокированному порту в избыточной топологии переход в состояние передачи при отсутствии отклика получения BPDU соседнего коммутатора
- Порт участвует в STP
- Осуществляет те же функции, что и UDLD

Root Guard

Cisco.com

- Не зависит от BPDU Guard
- Применяется на портах хостов
- Не может применяться вместе с Loop Guard (либо то, либо другое для порта)
- Блокирует соединение порт с устройством, пытающимся стать Root и высылающим BPDU приоритетного уровня
- Порт участвует в STP, за исключением случаев попыток получить уровень Root

УСЛУГИ И ТЕХНОЛОГИИ

Содержание

Cisco.com

- Введение
- Инфраструктура
- **Услуги и технологии**
- Мониторинг

КОНТРОЛЬ ДОСТУПА (ACL И МЕЖСЕТЕВЫЕ ЭКРАНЫ)

Списки контроля доступа (ACL)

Cisco.com

- ACL служат в качестве механизма первичного фильтра трафика на маршрутизаторах и коммутаторах:
  - Возможность контроля входящего/исходящего трафика
  - Возможность запрета обновлений маршрутов
- ACL применяются на уровне каждого интерфейса
- Существует несколько типов:
  - Стандартный, числовой диапазон 1–99, 1300–1999
  - Расширенный, числовой диапазон 100–199, 2000–2699
  - Именнованные, с именами, не номерами
  - Динамические ACL
  - Возвратные
  - На временной основе

Списки контроля доступа

Cisco.com

- ACL вводятся на уровне каждого протокола
- Соответствия ищутся сверху вниз, после нахождения первого соответствия обработка заканчивается
- Существует безоговорочное «deny any», но в основном добавляют эту строку для целей протоколирования
- При нахождении соответствия «deny», отсылается сообщение “host unreachable”
- ACL должны размещаться как можно ближе к фильтруемому источнику

Несколько важных предупреждений

Cisco.com

- Вы не можете удалить одно из объявлений в ACL, можно удалить лишь список целиком
  - Существует очень короткий промежуток времени, когда устройство уязвимо при отсутствии списков доступа
- Если существует запись, разрешающая весь трафик, то другие записи после неё не будут проверяться
- Общая маска Cisco IOS имеет противоположное маске подсети значение
  - Для 0.0.0.0 маской является 255.255.255.255
- ЗАМЕЧАНИЕ: генерируемые маршрутизатором пакеты (т.е. NTP или обновления маршрутов) могут проверяться только списками доступа на входе в устройство

Нумерация последовательности ACL

Cisco.com

- Каждое новая запись помещается в конец списка
- С версии 12.3(2)T вы можете пользоваться вставлением записей контроля доступа (ACE)
  - Не используется для динамических, возвратных либо Cisco IOS-FW ACL
  - Может использоваться с именованными или нумерованными ACL
- Номер последовательности по умолчанию 10

Нумерация последовательности ACL

Cisco.com

```
Router# show access-list special
Extended IP access list special
    10 permit ip host 10.3.3.3 host 172.16.5.34
    20 permit icmp any any
    30 permit tcp any host 10.3.3.3
    40 permit ip host 10.4.4.4 any
    50 Dynamic test permit ip any any
    60 permit ip host 172.16.2.2 host 10.3.3.12
    70 permit ip host 10.3.3.3 any log
    80 permit tcp host 10.3.3.3 host 10.1.2.2
    90 permit ip host 10.3.3.3 any
    100 permit ip any any
Router(config)# ip access-list extended special
Router(config-std-nacl)# 15 deny ip host 10.3.3.3 host 172.16.10.5
```


Когда и где применять ACL?

Cisco.com

Для большинства сетей требуется фильтрация и входящего и исходящего трафика

- **Входящий/ исходящий на межсетевых экранах**
- **Входящий/ исходящий на шлюзах операторов связи**
- **Входящий от лабораторной сети к корпоративной сети**
- **Входящий/ исходящий от сетей третьих лиц**
- **Входящий на линии VTY маршрутизатора**

Стандартные ACL

Cisco.com

- Обеспечивают фильтрацию только по адресам источников
- Количество списков должно быть между 1 и 99, 1300–1999
- Пример:

```
access-list 24 remark allow traffic in from this net
access-list 24 permit 10.0.1.0 0.0.0.255
access-list 24 remark deny all other traffic and log
access-list 24 deny any log
```

- ЗАМЕЧАНИЕ: стандартные ACL обеспечивают ограниченные возможности фильтрации, не соответствующие сегодняшней сложности сетей

Расширенные ACL - extended

Cisco.com

- Предоставляют широкий диапазон атрибутов фильтрации:
  - Адреса SRC (источника) и DST (назначения)
  - Протокол (TCP, IP, ICMP, UDP)
  - По маске
  - По биту Established
- Количество списков должно быть между 100–199, 2000–2699
- Два типа комментариев
  - “!” в текстовом файле не используется на маршрутизаторе
  - “Remark” часть ACL, но является комментарием
- Пример:

```
access-list 101 REMARK Allow SMTP access
access-list 101 permit tcp any host X.X.X.X eq smtp
! Deny everything else and log it
access-list 101 deny ip any any log
```

Именованные ACL - named

Cisco.com

- Именованные ACL предоставляют альтернативный путь обращения к стандартным и расширенным ACL
- Именованные ACL могут использоваться, когда исчерпаны возможности существующих нумерованных списков
- Список с именем более интуитивен чем список с номером
- Пример:

```
Extended IP access list protect_me
    permit ip host 10.3.3.3 host 172.16.5.34
    ! Allow icmp to any one
   permit icmp any any
    REMARK allow HTTPS Traffic to web server
    permit tcp any host 10.4.4.4 eq https
```


Возвратные ACL - reflexive

Cisco.com

- Равнозначны использованию ключевого слова “established” в списке доступа
- При запросе на соединение изнутри сети, возвратный список доступа создаст временный список для разрешения всего возвратного трафика для этого соединения
- Необходимо использовать расширенные именные списки доступа
- Временный список удаляется по окончании соединения

Списки доступа

Cisco.com

- **Пример (возвратные ACL):**

```
interface Serial1
  description Access to the Internet via this interface
  ip access-group inboundfilters in
  ip access-group outboundfilters out
!
ip reflexive-list timeout 120
!
ip access-list extended outboundfilters
  permit tcp any any reflect tcptraffic
!
ip access-list extended inboundfilters
  permit bgp any any
  permit eigrp any any
  deny icmp any any
  evaluate tcptraffic
```


ACL по времени – time based

Cisco.com

- **Позволяют ACL базироваться на временном диапазоне (день недели, текущее время)**
- **Позволяют пользователям разрешать/запрещать трафик основываясь на текущем времени**
- **Предоставляет дополнительный контроль потока трафика:**
  - **Более определенные правила безопасности в нерабочее время**
  - **Возможность открытия систем для поставщика в определенное время**
- **Может использоваться с именованными и нумерованными списками доступа**
- **Требует установки точного времени на маршрутизаторе**
- **Возможные использования:**
  - **Запрет доступа в Интернет в нерабочее время**
  - **Обеспечение периодического доступа производителя к некоторым портам источника/назначения**

Пример ACL по времени

Cisco.com

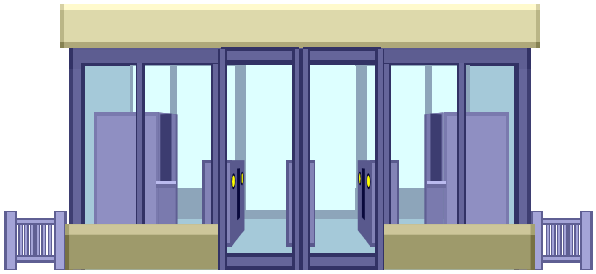
- Запрет FTP трафика с понедельника по пятницу в диапазоне 8:00 – 18:00 разрешение всего остального трафика без временных ограничений

```
!
time-range FTP-NO-WKDAYS
  periodic weekdays 8:00 to 18:00
!
access-list 109 deny tcp any any eq ftp time-range
FTP-NO-WKDAYS
access-list 109 permit ip  any any
```


ACL на основе аутентификации

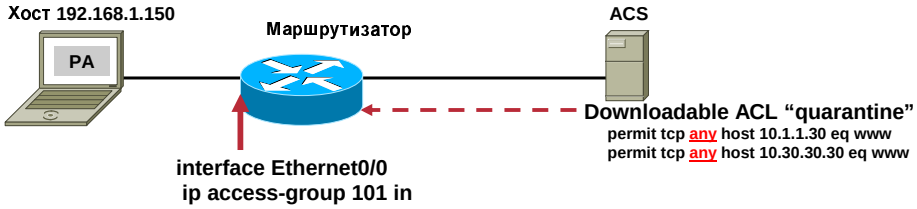
Cisco.com

- Динамические ACL
- «Замок и ключ» - lock&key
- Proxy Authentication (IOS FW)
- Cut-thru (PIX Firewall)



Как используются загружаемые ACL

Cisco.com



Динамический ACL →

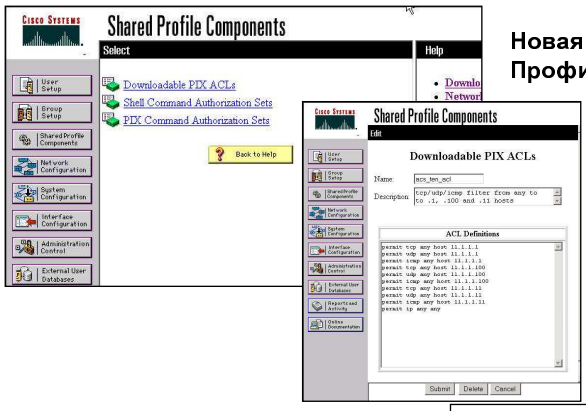
Extended IP access list 101
permit tcp host 192.168.1.150 host 10.1.1.30 eq www
permit tcp host 192.168.1.150 host 10.30.30.30 eq www
10 permit udp any host 10.20.20.20 eq domain
20 deny ip any 10.0.0.0 0.255.255.255

Загружаемый ACL →

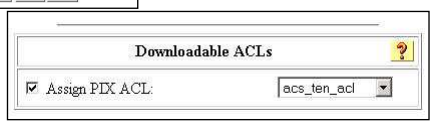
Extended IP access list xACSACLx-IP-quarantine-409036df
10 permit tcp any host 10.1.1.30 eq www
20 permit tcp any host 10.30.30.30 eq www

Загружаемые ACL при использовании ACS 3.0

Cisco.com



Новая кнопка Установка Общего Профиля для установки ACL

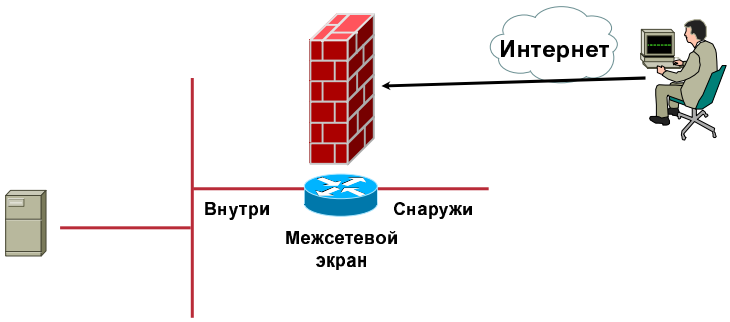


Ассоциируйте имя созданного ACL с пользователем

Пример доступа пользователя с аутентификацией (1/3)

Cisco.com

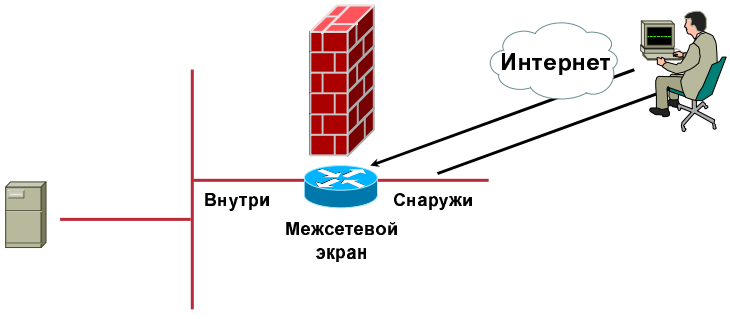
Пользователь хочет получить доступ на веб-сервер



Пример доступа пользователя с аутентификацией (2/3)

Cisco.com

Пользователь проходит процедуру аутентификации на межсетевом экране



Пример доступа пользователя с аутентификацией (3/3)

Cisco.com

Пользователю дан доступ

Доступ пользователя с аутентификацией через межсетевой экран

Cisco.com

	Lock&Key	Auth-proxy	Cut-thru proxy
Методы доступа	Telnet	FTP, Telnet, HTTP, HTTPS	FTP, Telnet, HTTP, HTTPS
Платформа	Cisco IOS	Cisco IOS FW	PIX
Методы аутентификации	Local/RADIUS/ TACACS+	RADIUS/ TACACS+	RADIUS/ TACACS+

«Замок и ключ»

Cisco.com

- Временные списки доступа, создающиеся определенными событиями, например, при аутентификации пользователя
- Синтаксически очень похоже на расширенные списки доступа
- Для использования технологии «замок и ключ» необходимо разрешить входящие сессии telnet к маршрутизатору
- Трафик фильтруется динамическими списками доступа
- Пользователь должен сначала открыть сессию telnet маршрутизатор и пройти процедуру аутентификации (с помощью TACACS+, RADIUS, token)

Настройка «замка и ключа»

Cisco.com

```
aaa authentication login lockkey tacacs+ enable
access-list 101 temp remoteSSH timeout
    15 permit ip any any eq 22
access-list 101 permit tcp any host 16.0.0.1
   eq telnet
!
interface Serial0
    ip address 16.0.0.1 255.255.255.252
    ip access-group 101 in
!
radius-server host 192.168.0.253
radius-server host 192.168.0.254
radius-server key <some password>
line vty 0 4
    password 7 090B69005A220C1103
    login authentication lockkey
    autocommand access-enable timeout 5
```

Недостатки «Замка и ключа»

Cisco.com

Недостатки

- Доступ базируется на IP адресе
  - Оператор может быть заменить IP адрес пользователя
  - Может быть транслированным сетевым адресом (NAT)
- Однократный пароль – не единственный метод аутентификации
  - Может быть telnet username/password (в открытом виде)
- Управление списком доступа – сложное дело
  - На уровне пользователя? Вряд ли; вероятнее, на уровне групп пользователей

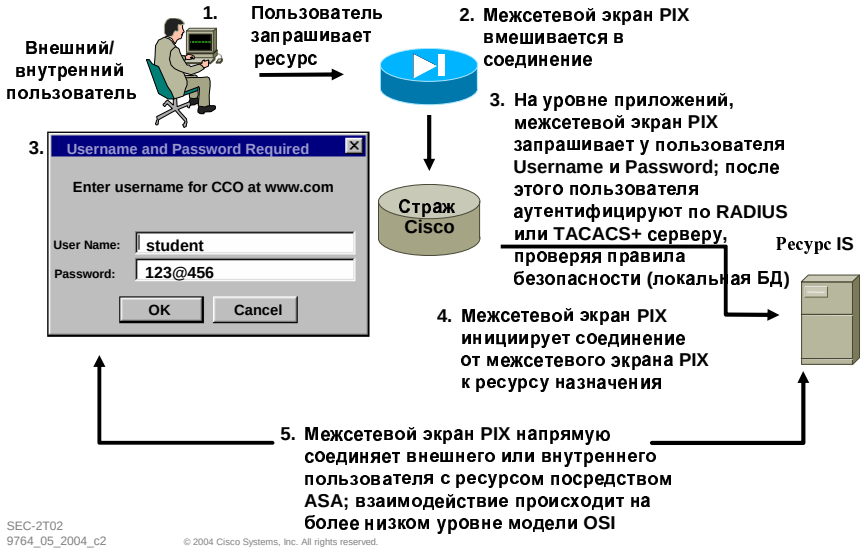
Cut-thru proxy на межсетевом экране PIX

Cisco.com

- Аутентификация с использованием FTP, Telnet, HTTP либо HTTPS соединений через PIX посредством TACACS+/RADIUS
- Использование HTTPS позволяет cut-thru proxy передавать в зашифрованном виде username и password между броузером пользователя и PIX

Cut-thru proxy (HTTPS)

Cisco.com



Пример настройки с сервером AAA (аутентификации, авторизации и учета

Cisco.com

```
access-list 101 permit tcp any any eq telnet
access-list 101 permit tcp any any eq ftp
access-list 101 permit tcp any any eq www
access-list 101 permit tcp any any eq https

aaa-server AuthInbound protocol tacacs+
aaa-server AuthOutbound (inside) host 171.69.89.135
cisco timeout 5
aaa authentication match 101 outside AuthInbound
aaa authorization match 101 outside AuthInbound
aaa authentication secure-http-client
```

01

Прокси с аутентификацией HTTPS: предупреждения

Cisco.com

- PIX имеет ограничение: одновременно возможно только 16 уникальных запросов аутентификации HTTPS
- Продолжительность запроса определяется с момента включения соединения по HTTPS (посылка username и password); запрос оканчивается в момент отправки страницы ‘успешно’ или ‘отклонено’

  ЗАМЕЧАНИЕ: время нахождения пользователя на странице аутентификации (набор username/password) не засчитывается; запрос начинается с момента нажатия кнопки OK

Загружаемые для каждого пользователя списки ACL

Cisco.com

- Работает только с RADIUS
- Существующие расширения:
  - Не нужно настраивать ACL в PIX
  - Шаблон группы для применения на нескольких пользователях
  - Проверка версии на соответствие в загруженных списках доступа
  - Не вводится никаких новых команд

Slide 163

D1 Deleted a slide immediately following because it was an exact duplicate of this one.
Dell, 5/27/2004

Загружаемые для каждого пользователя ACL: предупреждения

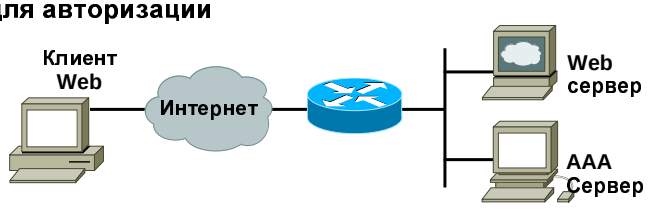
Cisco.com

- Аутентификация пользователя не переносится на резервный PIX
- При переключении на резервный PIX сессия сохраняется; при новом соединении требуется новая аутентификация, ACL будет загружаться заново

Auth-proxy: Cisco IOS FW

Cisco.com

- Позволяет администратору сети применять особые правила безопасности по отношению к каждому пользователю
- Пользователи аутентифицируются и авторизуются в соответствии с их профилями на серверах TACACS+ либо RADIUS
- Используется для аутентификации и авторизации
- Запись для пользователя; аутентификация осуществляется по username/password, имени хоста и т.д.; сервер AAA затем может передавать ACL маршрутизатору для авторизации



Пример auth-proxy

Cisco.com

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+

! Configure AAA for the authentication proxy
aaa authorization auth-proxy default group tacacs+

! Create the authentication proxy rule PXY
ip auth-proxy name pxy http

! Turn on display of the router name in the authentication proxy
! login page
ip auth-proxy auth-proxy-banner
interface Serial0/0
 ip address 10.0.0.2 255.0.0.0
 ip access-group 105 in
 ip auth-proxy pxy

! Create ACL 105 to block all traffic inbound on interface
  Serial0/0.
! Permit only IP protocol traffic.*/
access-list 105 deny   tcp any any
access-list 105 deny   udp any any
access-list 105 permit ip any any
```

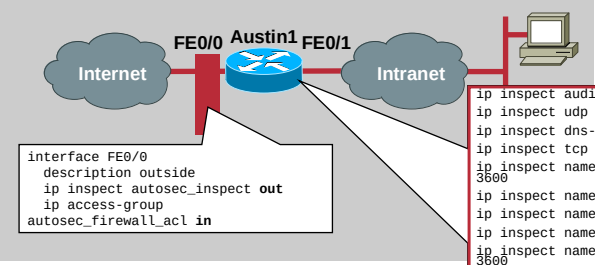

CBAC: контекстно-ориентированный контроль доступа

Cisco.com

- Метод фильтрации TCP/UDP основанный на информации сессии уровня приложения
- Дает возможность предоставления доступа для протоколов, открывающих несколько каналов (т.е., FTP и SQLnet)
  - Для протоколов UDP, сессии являются условными
- “Временные” списки доступа создаются для трафика, исходящего из сети
  - Идет контроль состояния соединения
- CBAC может быть применен только для расширенных списков ACL

Настройка CBAC

Cisco.com

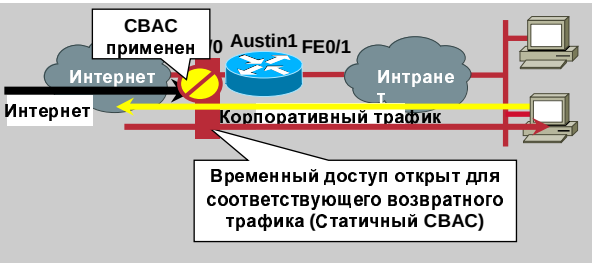



```
ip inspect audit-trail
ip inspect udp idle-time 1800
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect name autosec_inspect cuseeme timeout
3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout
3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
ip audit notify log
ip audit po max-events 100
!
ip access-list extended autosec_firewall_acl
  permit udp any any eq bootpc
  deny  ip any any
```

- CBAC предоставляет дополнительное межсетевое экранирование и функции фильтрации трафика
- Протоколирование CBAC предоставляет записи доступа к сети через межсетевой экран Cisco IOS, включая попытки несанкционированного доступа, а также входящие и исходящие услуги

Основы CBAC…

Cisco.com



- ACL на внешнем интерфейсе останавливает все
- CBAC добавляет динамические, временные записи ACL для определения соответствия проверяемого возвратного трафика

Note: This CBAC configuration includes default settings for TCP Intercept features, including:

ip inspect one-minute high	(default 500 half-opens)
ip inspect one-minute low	(default 400 half-opens)
ip inspect max-incomplete high	(default 500 half-opens)
ip inspect max-incomplete low	(default 400 half-opens)
ip inspect tcp max-incomplete host	(default 50 half-opens, same dest)
ip inspect tcp finwait-time	(default 5 seconds)
ip inspect tcp synwait-time	(default 30 seconds)
ip inspect tcp idle-time	(default 3600 seconds)
ip inspect udp idle-time	(default 30 seconds)

Еще о CBAC

Cisco.com

- CBAC может противостоять некоторым видам атак типа «Отказ обслуживания» (DoS):
  - Затопление SYN
  - Подделка последовательности TCP
  - Атаки фрагментирования IP
- CBAC можно настроить для предприятия следующих действий:
  - Протоколирование предупреждающих сообщений
  - Установка значений времени действия и порога
  - Сброс или блокировка пакетов

Предупреждения и проверки CBAC

Cisco.com

- Генерирует в режиме реального времени предупреждения и проверки на уровне протокола каждого приложения
- Сообщения протоколируются в системный журнал (syslog):
  - Предоставляет возможность записи строго заданных уровней
  - Возможность добавления к сообщению информации о дате/времени
- Пример сообщения проверки:

```
%FW-6-SESS_AUDIT_TRAIL: tcp session initiator (192.168.1.13:33192) sent
  22 bytes -- responder (192.168.129.11:25) sent 208 bytes
```

Межсетевой экран PIX

Cisco.com

Предоставляет следующие возможности:

- **Фильтрация пакетов**
- **Группировка объектов**
- **Аутентификации и авторизации**
- **Анализ приложений**
- **Фильтрация URL**
- **Наблюдение за состоянием (посредством адаптивного алгоритма безопасности)**

Настройка межсетевого экрана PIX

Cisco.com

```
pixfw#fixup protocol ?
      fixup protocol ftp 21
      fixup protocol h323 h225 1720
      fixup protocol h323 ras 1718-1719
      fixup protocol http 80
      fixup protocol ils 389
      fixup protocol rsh 514
      fixup protocol rtsp 554
      fixup protocol sip 5060
      fixup protocol sip udp 5060
      fixup protocol skinny 2000
      fixup protocol smtp 25
      fixup protocol sqlnet 1521
```

Функция MailGuard (обработчик почты)

Cisco.com

- Позволяет одному из внутренних хостов действовать в качестве почтового сервера для предотвращения перегрузки почтовыми сообщениями
- Принудительно вводит безопасный набор команд SMTP: `HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT.`
- Протоколирует все соединения SMTP в журнал хоста
- Пример настройки:

```
static (inside, outside) 10.1.1.1 161.44.1.2 netmask
255.255.255.0
access-list inside_access permit tcp any host
202.32.207.201 eq smtp
fixup protocol smtp 25
```


Фильтрация FTP и URL

Cisco.com

- Обе функции включены по умолчанию
- Для проверки, воспользуйтесь:

```
fixup protocol http 80
  !note security risk in some FTP versions.
fixup protocol ftp 21
```

- Сообщения протоколируются на уровне 7
- Примеры протоколируемых сообщений:

```
10.0.2.1 accessed URL 10.0.0.1/secrets.gif
10.0.2.1 Retrieved 10.0.0.42:feathers.tar
10.0.2.1 Stored 10.0.42.69:privacy.zip
```

Группировка объектов

Cisco.com

- **ACL традиционно выглядели вот так:**

```
access-list inside_access_out deny ip any host 130.127.31.127
access-list inside_access_out deny ip any host 211.181.197.222
access-list inside_access_out deny ip any host 202.32.207.201
access-list inside_access_out deny ip any host 131.128.32.83
```

- **Теперь существует возможность записи ACL на PIX вот таким образом:**

```
access-list inside_access_out deny ip any object-group KickGroup
```


Определение объектов сети

Cisco.com

```
name 212.251.68.0 Kick1
name 61.42.65.0 Kick2
name 206.107.23.0 Kick3
name 219.176.146.0 Kick4
object-group network KickGroup
description ISC Cited Restriction List
network-object Kick1 255.255.255.0
network-object Kick2 255.255.255.0
network-object Kick3 255.255.255.0
network-object Kick4 255.255.255.0
access-list inside_access_in deny ip any object-group
KickGroup
```

Объекты сети и диапазоны портов

Cisco.com

```
object-group service MS-sql-m tcp-udp port-object range 1433 1434
object-group service Kuang-virus tcp port-object range 17300
17300
object-group service AnalogX tcp port-object range 6588 6588
…
access-list inside_access_in deny tcp any any object-group ms-
sql-m
access-list inside_access_in deny tcp any any object-group Kuang-
virus
access-list inside_access_in deny tcp any any object-group
AnalogX
```


Возможности: Cisco IOS FW

Cisco.com

- Auth-proxy—на каждую сеть, на каждого пользователя существуют настройки правил аутентификации / авторизации
- Динамическое назначение портов—позволяет поддерживаемым CBAC приложениям работать на нестандартных портах (т.е. www по порту 8080)
- 101 запись определения вторжения
  - Для средних и крупных маршрутизаторов
- Предупреждения и проверки CBAC на уровне каждого приложения
- Сегодня применимо на любых платформах, вплоть до 7200
- Начиная с версии 12.3(11)T – IOS Prevention System – расширяемый список сигнатур для оределения вторжений

Защита от подмены адресов (АНТИ-СПУФИНГ)

Основные вопросы анти-спуфинга

Cisco.com

- ACL
- uRPF
- Перехват TCP
- CAR/Политика трафика/NBAR

Фильтрация входящих и исходящих маршрутов

Cisco.com

- **Маршруты, которые НЕ должны использоваться в Интернете**
  - **RFC 1918 и сети “Martian”**
  - **127.0.0.0/8 и широковещательные блоки**
  - **Смотрите ресурс Cymru Bogon:**
    - **http://www.cymru.com/Bogons/index.html**

- **Эти маршруты должны быть отфильтрованы и на входе, и на выходе**

Фильтрация входящих пакетов

Cisco.com

Вы не должны посылать никаких IP пакетов в Интернет с адресами источников, не соответствующими вам присвоенным!

RFC 2827 (BCP 38)

Фильтрация RFC 2827 (BCP 38)

Cisco.com

```
interface Serial n
  ip access-group 101 in
!
access-list 101 permit 142.142.0.0  0.0.255.255 any
access-list 101 deny ip any any
```

- Выходящие пакеты должны исходить с адресов пользователей

- Пакеты на входе не должны быть от пользователя

```
interface Serial n
  ip access-group 120 in
  ip access-group 130 out
!
access-list 120 deny ip 142.142.0.0  0.0.255.255 any
access-list 120 permit ip any any
!
access-list 130 permit 142.142.0.0  0.0.255.255 any
access-list 130 deny ip any any
```


Советы

Cisco.com

- **Входящие**
  - разрешите icmp
  - Разрешите установленные соединения TCP (т.е. блокируйте TCP-SYN)
  - Разрешите трафик к концентратору VPN
  - Разрешите WWW к webserver
  - Разрешите SMTP к mailserver
  - Разрешите DNS к nameserver
  - Разрешите NTP для синхронизации
  - Блокируйте NFS
  - Разрешите только непривилегированные порты UDP
  - Блокируйте все остальное и ведите журнал
- **Исходящие**
  - Разрешите пакеты только из моего адресного пространства
  - Блокируйте все остальное и ведите журнал

Одноадресная проверка передачи по обратному пути

Cisco.com

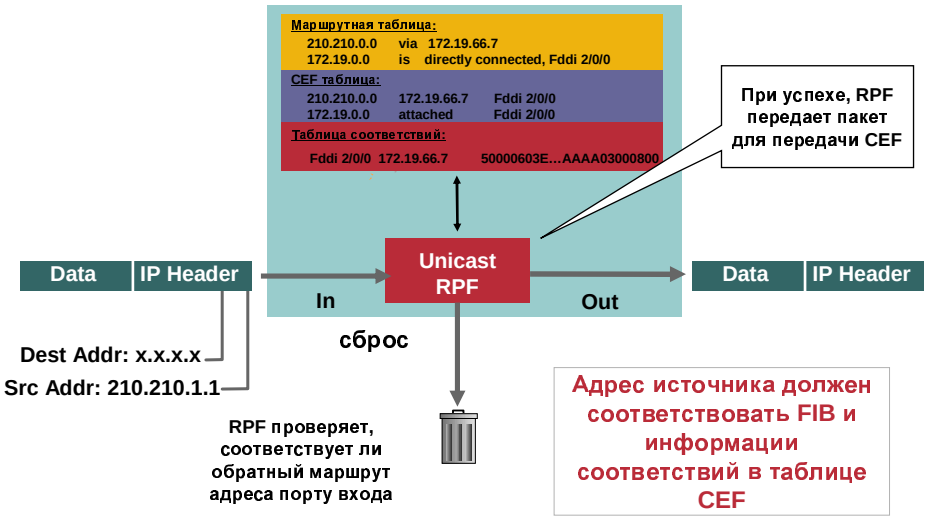
- Поддержка начиная с 11.1(17)CC
- CEF коммутация должна быть разрешена
- Источники IP пакетов проверяются для удостоверения в том, что обратный маршрут к источнику использует тот же интерфейс
- Осторожность нужна в ситуациях наличия нескольких каналов
- Два вида uRPF:

  Строгая для BCP 38/RFC 2827 фильтров на входе

  Нестрогая для взаимодействия операторов и для удаленно включаемой фильтрации в “черную дыру”

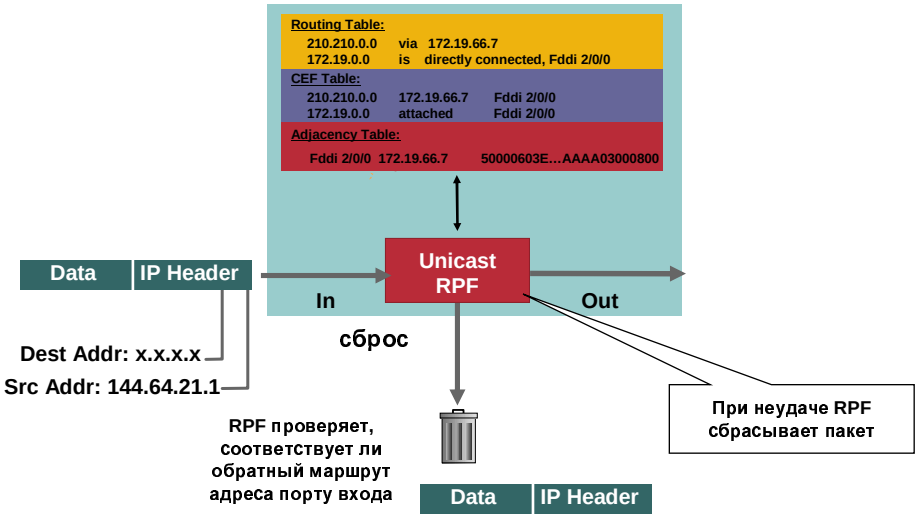
Проверка uRPF (строгая)

Cisco.com



Проверка uRPF (строгая)

Cisco.com



Где вы используете защиту соединений TCP?

Cisco.com

- На маршрутизаторах, защищающих доступные из других сетей сервера, т.е. web сервер, FTP сервер, e-mail сервер
- На маршрутизаторах, защищающих корпоративную сеть в случае атаки на внутренние ресурсы

Какую защиту предлагает метод TCP Intercept?

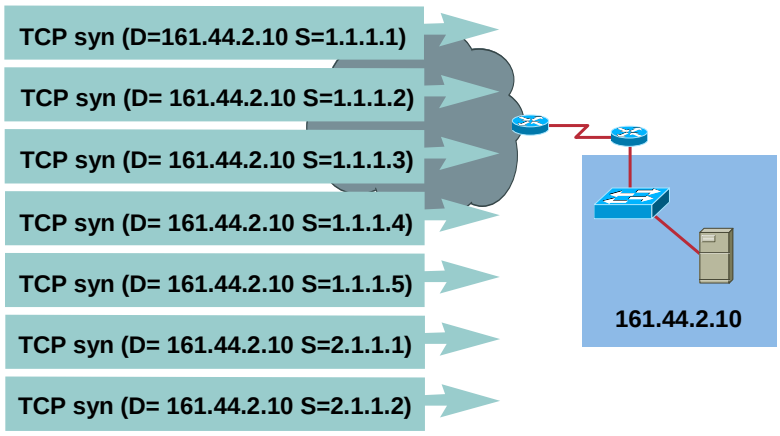
Cisco.com

- Атакуемый сервер не будет вынужден работать со всей нагрузкой, что позволит ему выдержать даже интенсивную атаку
- Позволяет маршрутизатору взять на себя руководство при атаке на уровне сети, что является более эффективным нежели отражение атаки с помощью сервера
- Добавление протоколируемых событий, что позволяет определить атаку DoS

Итак: что представляет из себя атака TCP SYN?

Cisco.com

Примечание: все адреса источников (S) различны



Настройка защиты перехвата TCP: Cisco IOS

Cisco.com

```
version 11.3
hostname inet-rtr-us-1
interface Ethernet 1
 ip address 161.44.2.1 255.255.255.0
!
access-list 101 permit any 161.44.2.0 255.255.255.0
!! Set the policy; protect machines in ACL 102,
! Intercept, and if you exceed max connections
! during an attack, get aggressive and
! drop the oldest ones
ip tcp intercept list 101
ip tcp intercept intercept
ip tcp intercept drop-mode oldest
```


Настройка защиты перехвата TCP : PIX

Cisco.com

```
static (dmz2,dmz1) 161.44.2.0 netmask 255.255.255.0 em_limit
1000
conduit permit tcp any eq www 161.44.2.0 255.255.255.0
```

Ограничение скорости как средство защиты

Cisco.com

- Зачем кому-либо посылать трафик ICMP со скоростью более 45 Мб/с?
  - Если это произошло, как это можно прекратить?
  - Ответ—ограничьте скорость шумового трафика
- При использовании правил ограничения потока данных (CAR – committed access rate), определенные виды трафика не повлияют на производительность вашей сети

Использование CAR

Cisco.com

- Ограничьте весь эхо- и ответный трафик ICMP получаемый с периферии значением 256 Кб/с с небольшим значением возможного превышения:

```
! traffic we want to limit
access-list 102 permit icmp any any echo
access-list 102 permit icmp any any echo-reply
! interface configurations for borders
interface Serial3/0/0
 rate-limit input access-group 102 256000 8000 8000 conform-
  action transmit exceed-action drop
```

- К интерфейсам для контроля других видов трафика также можно добавить и другие команды “rate-limit”

Определение приложения на основе сети (NBAR)

Cisco.com

- Возможность классификации приложений, имеющих:
  - Статически присвоенные номера портов TCP и UDP
  - Не-TCP и не-UDP IP протоколы
  - Присваиваемые динамически во время установления соединения номера портов TCP и UDP
  - Классификация базируется на глубоком анализе пакетов: NBAR имеет возможность более детального анализа пакетов для определения приложений
  - HTTP трафик по URL, имени хоста или типа MIME при использовании регулярных выражений (*, ?, [ ]), трафик Citrix ICA, классификация по типам полезной нагрузки RTP
- В настоящее время поддерживается 88 протоколов/ приложений

Правила для трафика

Cisco.com

- Используйте NBAR для классификации трафика:

```
class-map match-any p2p
  match protocol fasttrack
  match protocol gnutella
  match protocol napster
  match protocol http url \.hash=*
  match protocol http url /.hash=*
  match protocol kazaa2
```

- Используйте правила для трафика с целью ограничения трафика:

```
policy-map p2p
  class p2p
    police cir 8000 bc 1500 be 1500 conform-action drop exceed-action
drop
Interface fastethernet 0/0
  ip nbar protocol-discovery
  service-policy input p2p
```

PIX

Cisco.com

- **FloodGuard**

  Свойство PIX позволяющее PIX защитить другие системные ресурсы при атаке на систему аутентификации пользователя (AAA), PIX ответит на ввод имени пользователя:

  ```
  ! PIX command
  floodguard enable | disable
  ```

- **DNS защита**

  Если несколько DNS серверов запрошены по адресам, через PIX пройдет только один ответ

Мониторинг

Содержание

Cisco.com

- Введение
- Инфраструктура
- Услуги и технологии
- **Мониторинг**
  - **Протоколирование**
  - **IDS**
  - **NetFlow**
  - **Riverhead**

Важность протоколирования

Cisco.com

“Меня изумляют пользователи, высоко оценивающие развитие IDS и совершенно пренебрегающие протоколированием.”

Инженер-консультант по безопасности Cisco

Важность протоколирования

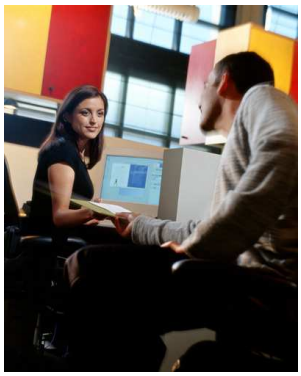
Cisco.com

- Просмотр событий
- Устранение неисправностей
- Протоколирование команд
- Поиск инцидентов
- Анализ тенденций и основных направлений

Архитектура протоколирования

Cisco.com

- Приоритет устройств
- Где вести журнал (несколько серверов? Один для истории, второй как временный? Ярусный метод?)
- Что записывать (уровни записей)
- Некоторые серверы и протоколы имеют особенности
- Соображения масштабирумости (для сервера, для сетевого устройства, фильтрация записей на основе приоритета событий)



Системные журналы: вещь обоюдоострая

Cisco.com

- Недостаточно информации – и весь объем теряет ценность
- Переизбыток также сведет все ваши усилия на нет

Получение полного журнала

Cisco.com

- UNIX системы обычно ведут системный журнал (syslog) по умолчанию
- Оборудование Cisco поддерживает syslog
- Системы с Windows используют собственный формат записи событий
  - Обычные средства позволяют запись исключительно в формате ASCII
  - Существуют средства для ведения журнала событий на шлюзах

Запись событий Windows и syslog

Cisco.com

- NTSyslog
  - Открытый источник: http://ntsyslog.sourceforge.net/
- EventReporter
  - Коммерческий продукт: http://www.eventreporter.com/
- Perl's Win32::EventLog и Net::Syslog
  - Программное обеспечение: http://www.cpan.org/

```
Jun 18 21:37:34 test1.demo.cisco.com security[success]
Successful Logon:  User Name:Administrator  Domain:TEST1
Workstation Name:TEST1
```


Анализ журнала

Cisco.com

- Существует несколько хороших продуктов и сервисов для корреляции событий журналов и уведомления о важных событиях
- Если вы хотите делать все ' по-своему'
  - Языки perl и python прекрасно подходят для анализа/сравнения журналов
  - Вводите категории событий по меньшей мере 3 уровней:
    - События срабатывания защиты
    - Обычные системные события
    - Все остальное
  - Минимизируйте категорию 'все остальное' применением масок для остальных категорий

Проблемы объема

Cisco.com

- С увеличением объема журнала, единственный сервер протоколирования должен стать распределенной системой
  - Требования к дисковому пространству
  - Потребление сетевых ресурсов трафика
  - Время обработки записей
  - Задержки между временем наступления события и уведомлением
- Даже если журнал ведется одной станцией, необходимо планировать инфраструктуру протоколирования

Пример: Событие в сети становится событием безопасности

Cisco.com

Пользователь обнаружил в журнале:

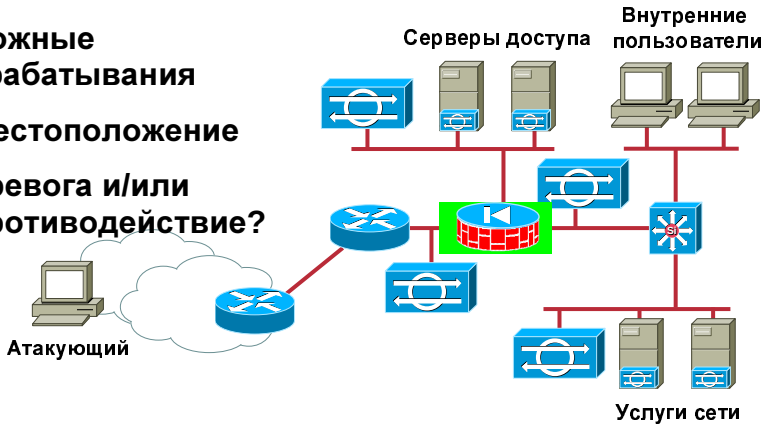
```
%OSPF-5-ADJCHG: Process 100, Nbr 192.168.100.1 on Serial0/0/0.1
from LOADING to FULL, Loading Done
%OSPF-5-ADJCHG: Process 100, Nbr 192.168.100.1 on Serial0/0/0.1
from FULL to DOWN, Neighbor Down: Dead timer expired
%OSPF-5-ADJCHG: Process 100, Nbr 192.168.100.1 on Serial0/0/0.1
from INIT to DOWN, Neighbor Down: Interface down or detached
```

- Новое устройство становится маршрутизирующим OSPF
- Обыкновенное событие, если не учитывать, что устройство неизвестное
  - Затрагивает доступ в сеть
  - Влияет на трафик

Системы обнаружения вторжения

Cisco.com

- Станция и сеть
  - Всему свое место
- Ложные срабатывания
- Местоположение
- Тревога и/или противодействие?



Структурирование и реализация сигнатур

Cisco.com

- Реализация сигнатур
  - Контекстно-зависимые данные содержатся в заголовке пакета
  - Контекстно-зависимые данные содержатся в содержимом пакета
- Структурирование подписей
  - Атомарные данные в единственном пакете
  - Части данных содержатся в нескольких пакетах

Классы сигнатур

Cisco.com

- **Зондирование**
  - Включается при активности, заведомо или потенциально ведущей к несанкционированному открытию систем, сервисов или систем защиты
- **Доступ**
  - Включается при активности, заведомо или потенциально ведущей к несанкционированному запросу данных, доступу в систему, присвоению привилегий
- **Отказ обслуживания**
  - Включается при активности, заведомо или потенциально ведущей к выводу из строя сети, системы или сервиса
- **Информационный**
  - Включается при нормальной сетевой активности, которая сама по себе не может рассматриваться как аварийная но может быть использована для определения успеха атаки либо разведки

Ответные действия IDS

Cisco.com

- **Запись IP сессии**
  - Полезно для анализа событий
  - Обычно записывается только пакет инициатор и следующие за ним
- **Разрыв соединения TCP**
  - Запросы на разрыв, посланные с интерфейса мониторинга
  - Пакет инициатор проходит
  - Требуется угадать правильный номер последовательности TCP
- **Блокировка**
  - Используйте осторожно и только в отдельные моменты времени для минимизации возможности блокировки полезного трафика
  - По возможности используйте “Никогда не блокируемые адреса”

Сбор информации о пользователях

Cisco.com

Основные пользователи?
Как долго в сети?

Какие интернет сайты используют?
Что делают в сети?

Процент используемого трафика?
Используемые приложения?
Схемы пользования?

Происхождение NetFlow

Cisco.com

Изначально разрабатывался как путь коммутации
Ценная информация в “cache” была побочным эффектом

- NetFlow сейчас является главной сетевой технологией учета
- Дает администраторам сетей информацию о “потоке пакетов”
- Позволяет:
  - Анализ потоков трафика
  - Мониторинг безопасности
  - Определение аномалий
- Позволяет обрабатывать IP трафик, отвечая на вопросы: кто,что, где, когда, и как

Принципы NetFlow

Cisco.com

- Только входящий трафик
- Однонаправленный поток
- Учитывает и транзитный трафик и трафик к маршрутизатору
- Работает с Cisco Express Forwarding (CEF) или быстрой коммутацией (fast switching)
  - Не способ коммутации
- Поддерживается всеми интерфейсами и Cisco IOS платформой ПО
- Возвращает информацию о логических интерфейсах в записях о потоках

NetFlow для защиты

Cisco.com

- Идентификация атаки
  - Подсчет потоков
  - Неактивные потоки – сигнал атаки «червя»
- Классификация атаки
  - Потоки малого размера на то же направление
  - Кого и кто атакует

Формат NetFlow

Cisco.com

- Чаще всего используется v5 с матрицей автономных систем
- Есть отличия в формате записи в каждой версии
- Версия 9 - основа для стандарта IETF IPFIX (Internet Protocol Flow information eXport)

  www.ietf.org/internet-drafts/draft-bclaise-netflow-9-00.txt

Версия 5: Формат экспорта потока

Cisco.com

Версия 5 используется очень широко

Настройка NetFlow

Cisco.com

- **Пример настройки:**

```
interface serial 5/0
 ip route-cache flow
```

- **Если CEF не настроена, NetFlow улучшает существующий путь коммутации (optimum switching)**
- **Если CEF настроена, NetFlow становится сборщиком информации о потоке**

NetFlow: определение и отражение атак

Cisco.com

- **Команда “sh ip cache flow” для обнаружения больших потоков**
- **Идентификация источника атаки**
- **Запись списка запрета доступа**
- **Мониторинг посредством записей “show ip cache flow” и “Null” в поле DestIf для отображения блокируемого**
- **Настройка агрегации по портам при использовании “sh ip cache flow aggregation prefix-port”**

Преимущества NetFlow

Cisco.com

- **Основные преимущества NetFlow:**
  - **Отсутствие изменений на маршрутизаторе атакуемой сети; пассивный мониторинг**
  - **Можно использовать скрипты для сравнения по сети**
  - **MIB для доступа SNMP внедрено начиная с 12.3(7)T**
    - **администрирование NetFlow**
    - **Порты протоколов Top N, флаги TCP, пакеты, байты, автономные системы, отправители и получатели**
    - **Пакеты Top N Flows основаны на значениях кэша (т.е. Адресов назначения)**

Настройка NetFlow

Cisco.com

- **Экспорт информации:**
  - **Маршрутизатор**
  - `ip flow-export version 5 [origin-as|peer-as]`
  - `ip flow-export destination x.x.x.x <udp-port>`
- **Агрегация потоков (новинка в 12.0S):**
  - **Маршрутизатор высылает агрегированные записи**
  - `ip flow-aggregation cache as|prefix|dest|source|proto`
    - `enabled`
    - `export destination x.x.x.x <udp-port>`

Пример: NetFlow маршрутизатор (1)

Cisco.com

Пример выходных данных с маршрутизатора:

```
sjc-k-isp-gw1#show ip cache flow
IP packet size distribution (289573M total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .003 .335 .077 .118 .026 .013 .014 .009 .009 .004 .005 .005 .007 .004 .003

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .003 .004 .025 .044 .281 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 6553988 bytes
  3212 active, 62324 inactive, 3509220366 added
  1045966333 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet    28518777      6.6         6   117     43.0       5.0      19.1
TCP-FTP       79378311     18.4         4    75     82.9       3.7      17.5
TCP-FTPD       6865946      1.5       130   620    209.2       6.0      18.2
TCP-WWW     6329485720   1473.7        17   592  25662.6       3.7      10.6
TCP-SMTP     283417501     65.9        20   592   1331.3       7.1      11.7
Et1/1          144.254.153.50  Local         144.254.153.51  06 701D 0017    63
```


Пример: NetFlow маршрутизатор(2)

Cisco.com

Hex

SrcIf	SrcIPaddress	DstIf	DstIPaddress	Pr	SrcP	DstP	Pkts
Gi9/0/0	128.107.241.183	PO2/0/0	200.33.148.193	11	0035	0035	1
Gi1/0/0	128.107.108.134	PO2/0/0	66.121.15.146	32	AED3	362F	37
Gi1/0/0	171.69.60.172	PO2/0/0	212.195.195.27	06	0A02	1236	1
PO2/0/0	198.10.10.190	Null	224.2.133.133	11	0401	2692	6
PO2/0/0	198.10.10.190	Null	224.2.133.134	11	0402	2694	2
Gi9/0/0	171.70.192.87	PO2/0/0	24.141.141.120	11	2710	0417	1
Gi9/0/0	64.101.141.82	PO2/0/0	194.73.82.242	11	0035	0035	1
Gi1/0/0	64.104.109.53	PO2/0/0	64.108.41.150	06	05B7	008B	6
Gi9/0/0	198.133.219.25	PO2/0/0	200.66.243.43	06	0050	0579	46
Gi1/0/0	64.104.109.53	PO2/0/0	64.108.41.157	06	05D3	008B	15

Пример: NetFlow 6500

Cisco.com

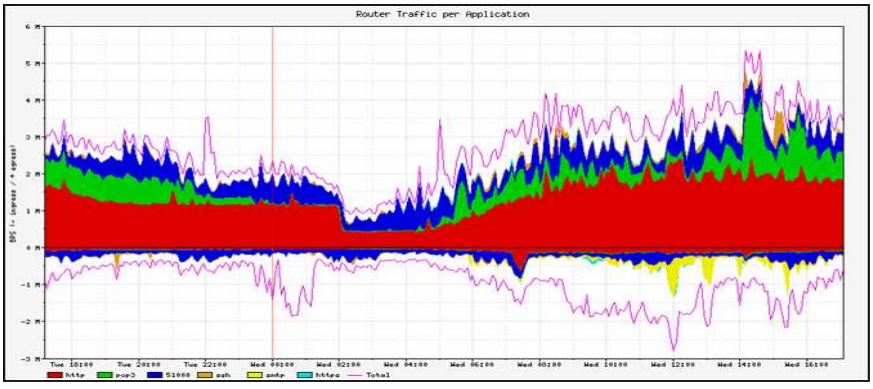
```
sjce-dirty-gw1#show mls ip det
Displaying NetFlow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------

    QoS     Police Count Threshold    Leak      Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+----------+----+-------+-------+----------+
64.104.76.230   24.221.161.5    udp :32772  :dns      1017: 0
2            162         68    18:54:08   L3 - Dynamic
  0x0          0              0        0       NO   81        NO       NO
143.127.4.15    171.70.81.27    udp :10000  :10000    1024: 0
68           2079        673   18:54:42   L3 - Dynamic
  0x0          0              0        0       NO   29        NO       NO
202.56.200.22   198.133.219.25  icmp:0      :0        1028: 0
41           3198        612   18:54:33   L3 - Dynamic
  0x0          0              0        0       NO   78        NO       NO
128.107.241.185 209.240.213.120 udp :dns    :dns      400 : 0
0            0           15    18:54:30   L3 - Dynamic
  0x0          0              0        0       NO   67        NO       NO
```

No Hex

NetFlow: поток приложения

Cisco.com

Используйте Arbor Networks Peakflow для выяснения работающих в сети приложеинй

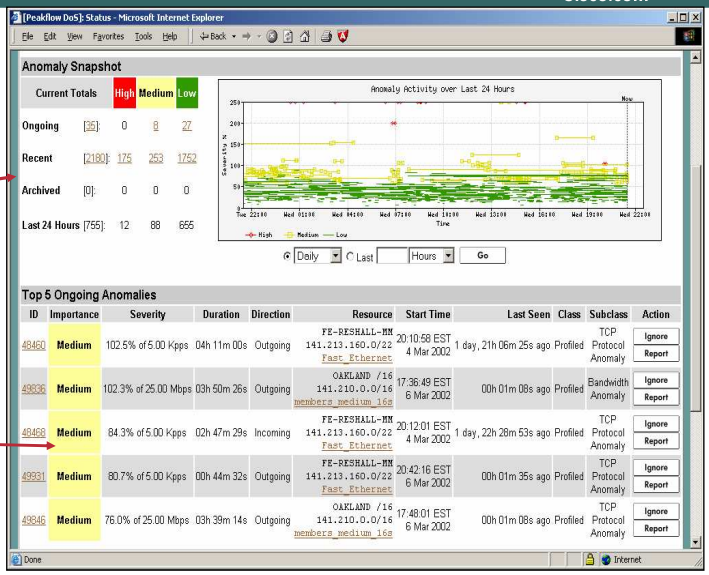


Определение аномалий NetFlow

Cisco.com

Фиксация аномального трафика в сети

Аномалии классифицируются как низкие, средние, крупные; крупные вызывают тревогу (E-mail, SNMP, и т.д.)

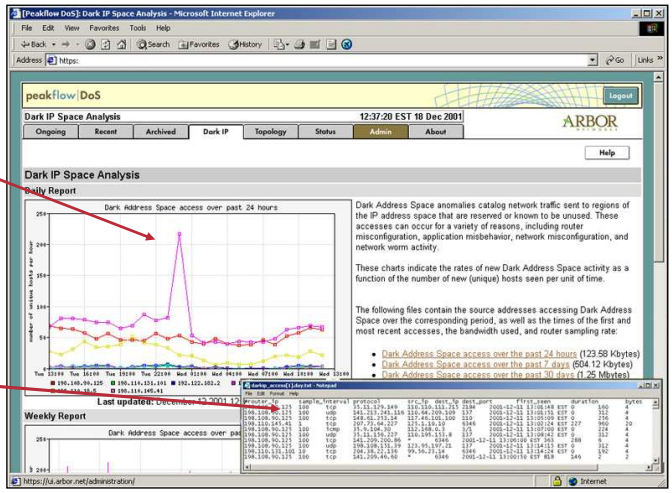


Обнаружение «червя» NetFlow

Cisco.com

Оператор уведомляется о «черве»

Система автоматически составляет список инфицированных серверов для отправки в карантин и лечения



Cisco Guard

Cisco.com

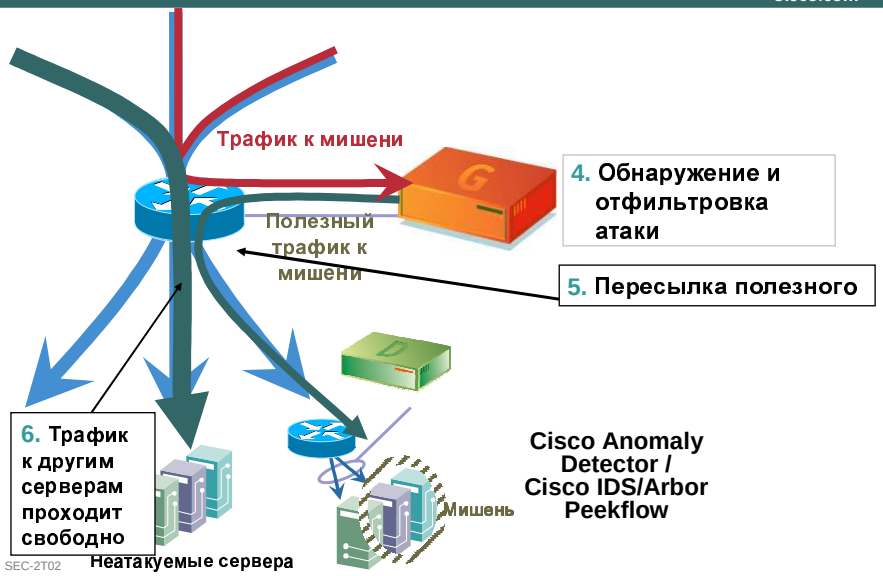
- Ранее назывался Riverhead Guard
- Не просто обнаружение аномалий
  - Предпринимает действия при обнаружении
- Внешнее устройство
  - Выход из строя Cisco guard не скажется на сети
- Начальный этап (режим обучения)
- Фильтрует плохой трафик и пропускает полезный
- Фильтрация на основе профилей

Обзор

Cisco.com

Обзор

Cisco.com



Дополнительные URL

Cisco.com

- **Справочники настроек безопасности:**
  - http://www.cisecurity.com
  - http://www.nsa.gov/snac/cisco/guides/cis-1.pdf
  - http://www.cymru.com/Documents/
  - http://www.cymru.com/Bogons/index.html
- **Поиск уязвимых мест**
  - http://packetstormsecurity.org
  - http://isc.sans.org/
  - http://www.cert.org
  - http://www.whitehats.com/
  - http://www.cisco.com/go/psirt
  - http://microsoft.com/technet/security/

Ресурсы

Cisco.com

- SANS
  http://www.sans.org
- CAIDA статья “Inferring Internet Denial-of-Service Activity”
  www.caida.org/outreach/papers/2001/BackScatter/usenixsecurity01.pdf
- Paper from S. Fluhrer (Cisco Systems), I. Mantin and A. Shamir (Weizmann Institute)
  www.crypto.com/papers/others/rc4_ksaproc.ps
- Другие средства защиты
  www.insecure.org/tools.html
- Информационная страница об отказе обслуживания
  http://www.denialinfo.com/
- RFC 2827 “Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing”
  ftp://ftp.isi.edu/in-notes/rfc2827.txt
- Distributed Systems Intruder Tools workshop report
  http://www.cert.org/reports/dsit_workshop.pdf
- RFC2196 (Site Security Handbook)
- FIRST
  http://www.first.org/

Дополнительная информация Cisco

Cisco.com

- Cisco основы безопасности
  http://www.cisco.com/go/safe
- Cisco IOS о шифровании паролей
  www.cisco.com/warp/public/701/64.html
- Cisco IOS основы—для всех ISP
  http://www.cisco.com/public/cons/isp/documents/IOSEssentialsPDF.zip
- Характеристики и отслеживание затопления пакетами с использованием маршрутизаторов Cisco
  http://www.cisco.com/warp/public/707/22.html
- Стратегии защиты от распределенных DoS атак
  http://www.cisco.com/warp/public/707/newsflash.html
- Улучшение защиты на маршрутизаторах Cisco
  http://www.cisco.com/warp/public/707/21.html
- Защита беспроводных LAN
  www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm

ПРИЛОЖЕНИЕ

Уровни системных журналов (строгие)

Cisco.com

Уровень	Описание
0	Неотложная необходимость
1	тревога
2	критический
3	ошибки (по умолчанию)
4	предупреждение
5	уведомление
6	Для информации
7	Легкие ошибки

Уровни системных журналов: PIX

Cisco.com

приоритет (PIX)	Syslog “свойство”
16	Local0
17	Local1
18	Local2
19	Local3
20	Local4
21	Local5
22	Local6
23	Local7

AutoSecure: Cisco IOS оборудование

Cisco.com

AutoSecure доступна…

выпуск	платформа
12.3(6)	1700,2600,3660,3700
12.3(5b)	1700,2600,3660,3700
12.3(4)XD	2600,3660,3700
12.3(4)T3	827,1700,2600,3660,3700,7300,7600-MWAM,CAT6000-MWAM
12.3(2)XF	1700
12.3(2)XE	83x,1700
12.3(2)XC1	83x
12.3(2)XA1	1700
12.3(2)T4	827,1700,2600,3660,3700,7300
12.3(1a)BW	7600-MWAM,CAT6000-MWAM
12.3(1)BW	7300

Сбор данных с доменов NetFlow

Cisco.com

- **Открытый источник: RRDTool, Flow-Tools, FlowScan, and CUFlow**

  http://www.linuxgeek.org/netflow-howto.php