Устранение неполадок средств безопасности маршрутизаторов Cisco ISR G2

© 2010 Cisco Systems, Inc. All rights reserved.

План презентации

- Обзор маршрутизаторов ISR G2
- Устранение неполадок межсетевого экрана Cisco IOS
- Устранение неполадок системы предотвращения вторжений Cisco IOS

© 2010 Cisco Systems, Inc. All rights reserved.

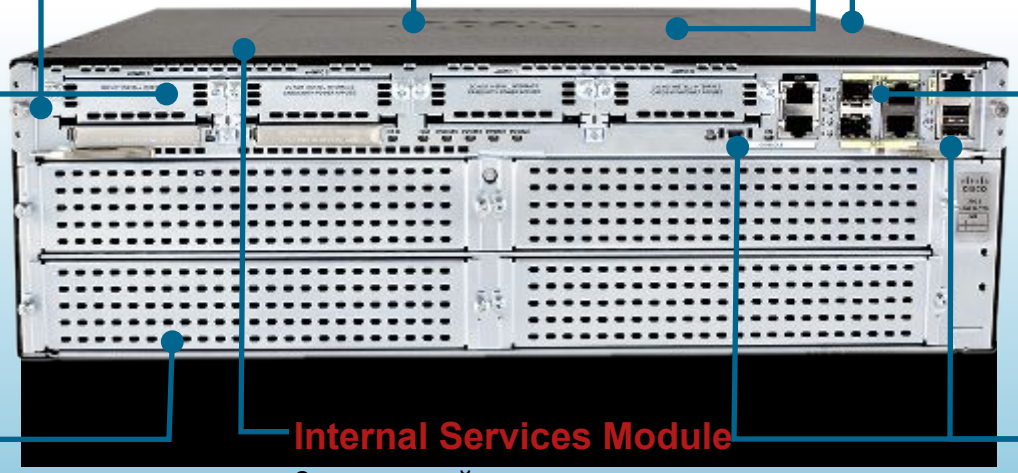
Маршрутизатор следующего поколения

Services Performance Engine (3900)
- Повышение производительности устройства

Многоядерный процессор
- 4x-кратный прирост производительности

Multi Gigabit Fabric
- Связь модулей
- Приоритезация и шейпинг пакетов

DSP-модули следующего поколения
- Поддержка видео
- 4x-кратное увеличение сессий аудиоконференций и транскодинга
- Режим экономии электропитания



EHWIC
- 2x-кратный прирост производительности
- Непосредственная поддержка HWIC/WIC/VWIC/VIC
- Проддержка EPoE

Порты GE
- Дополнительный порт GE (3 на 2911 и выше)
- SFP на 2921 и выше

Service Modules
- 3x-7x-кратный прирост производительности сервисного модуля
- Адаптер для установки текущих NM
- Поддержка EPoE

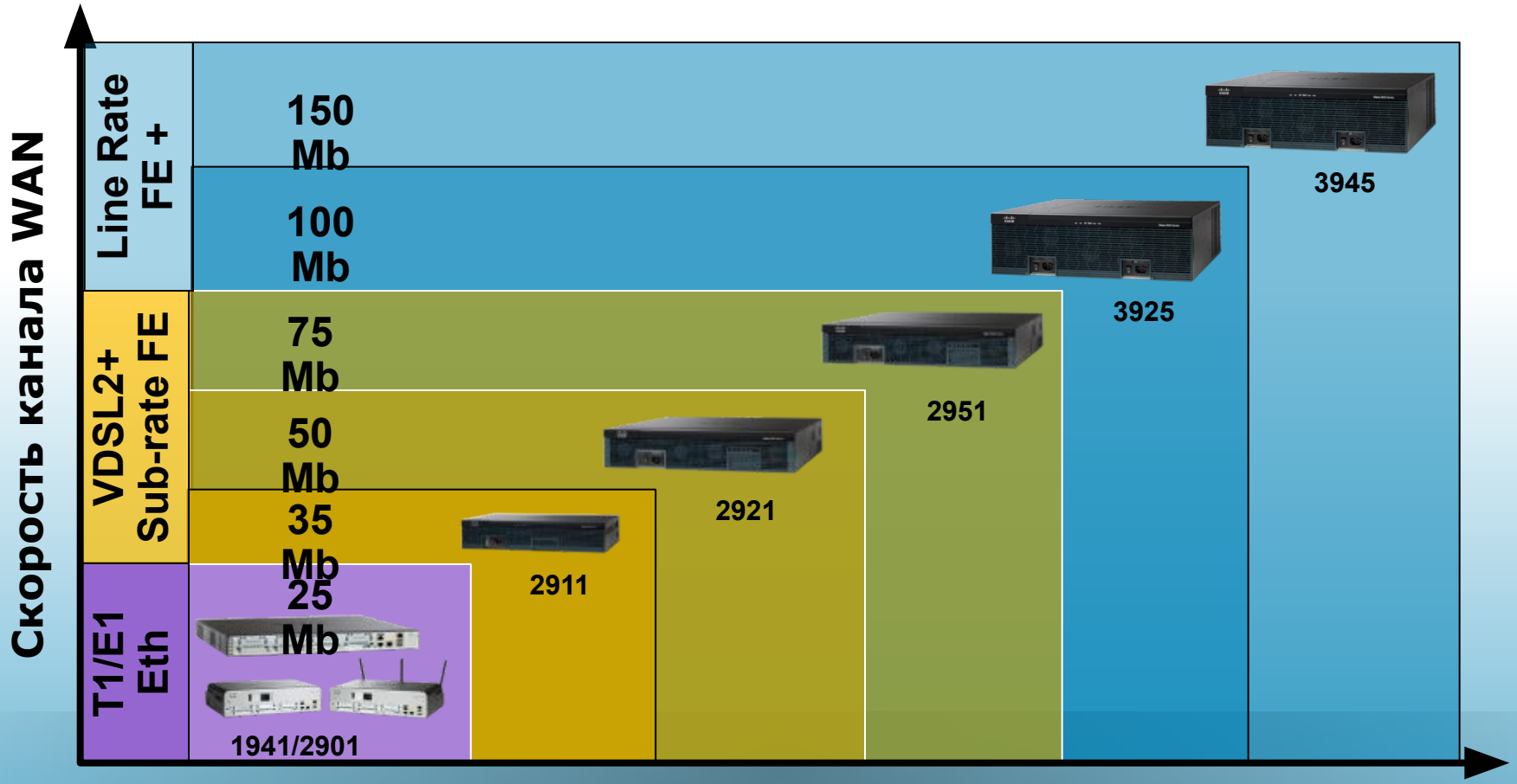
Internal Services Module
- 3x-кратный прирост производительности сервисного модуля
- Режим экономии электропитания
- Опция для 802.11n на 1941W

USB
- Консоль через USB
- Хранение файлов

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Позиционирование ISR G2 по производительности

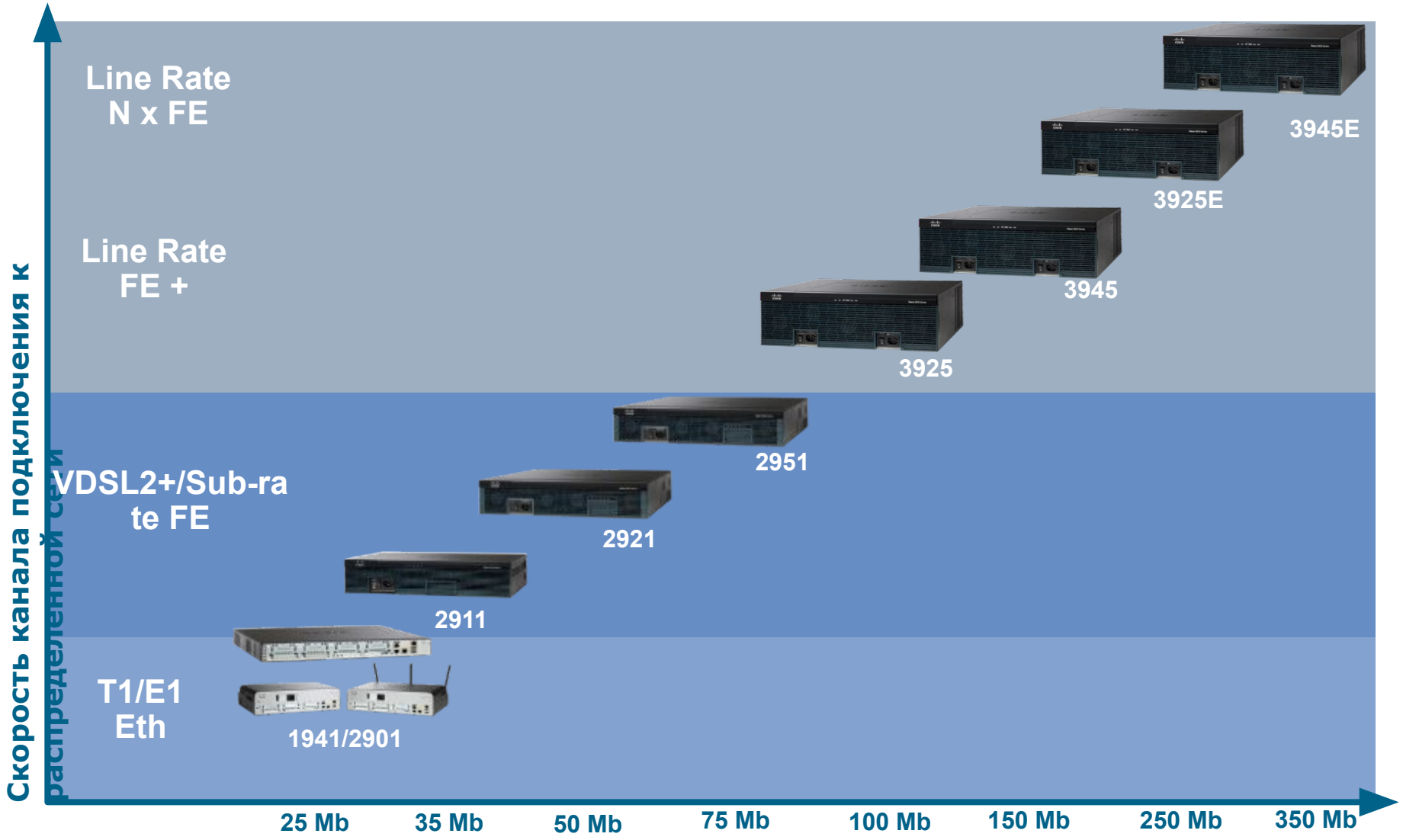
Производительность с сервисами при 75% загрузке процессора



© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Позиционирование ISR G2 по производительности

Производительность с сервисами при 75% загрузке процессора



© 2010 Cisco Systems, Inc. All rights reserved.

Функции безопасности ISR G2

- Трансляция сетевых адресов (NAT)
- Списки доступа (ACL)
- Межсетевой экран на основе политик зон (ZBFW)
- Система предотвращения вторжений (IPS)
- Фильтрация контента (Content Filtering)
- Поддержка модуля NME-RVPN

© 2010 Cisco Systems, Inc. All rights reserved.

Рост производительности функций безопасности ISR G2 по сравнению с ISR*

Платформа	Пропускная способность NAT+ACL	Пропускная способность FW	Пропускная способность FW+NAT	Пропускная способность IPS
3945 и 3845	2,7	1,9	1,9	1,5
3925 и 3825	3,4	2,4	2,0	1,8
2951 и 2851	3,4	2,0	1,5	1,2
2921 и 2821	2,1	2,1	1,6	1,5
2911 и 2811	5,1	4,1	5,5	2,7
2901 и 2801	4,5	3,2	4,5	3,2
1941 и 1841	3,9	2,7	3,7	2,3

* Размер объекта HTTP 64KB, IMIX 409B (загрузка ЦПУ - 75%)

© 2010 Cisco Systems, Inc. All rights reserved.

План презентации

- Обзор маршрутизаторов ISR G2
- Устранение неполадок межсетевого экрана Cisco IOS
  - Обзор межсетевого экрана Cisco IOS
  - Обработка пакетов межсетевым экраном Cisco IOS
  - Устранение неполадок межсетевого экрана Cisco IOS
  - Типовые неполадки и способы их устранения
  - Резюме
- Устранение неполадок системы предотвращения вторжений Cisco IOS

© 2010 Cisco Systems, Inc. All rights reserved.

Модели настройки МСЭ Cisco IOS

Две модели настройки

Классический МСЭ IOS	МСЭ на основе политик зон
▪ Анализ трафика с учетом состояния сеансов **на базе интерфейсов** ▪ Политика МСЭ = политика анализа в сочетании с политикой ACL ▪ Корреляция политик затруднена ▪ Трудно использовать группы объектов (команды object-group)	▪ Анализ трафика с учетом состояния сеансов **на базе зон** ▪ Политики МСЭ основаны на передаче трафика *между зонами* ▪ Корреляция политик проста, просто устранять неполадки ▪ Некоторые функции схожи с группами объектов ASA/PIX ▪ Более тонкая настройка политики анализа

Концептуальные различия классического МСЭ Cisco IOS и МСЭ на основе политик зон: http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5710/ps1018/prod_white_paper0900aecd806f31f9.html

* МСЭ на базе политик зон поддерживается с версии IOS 12.4(6)T

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

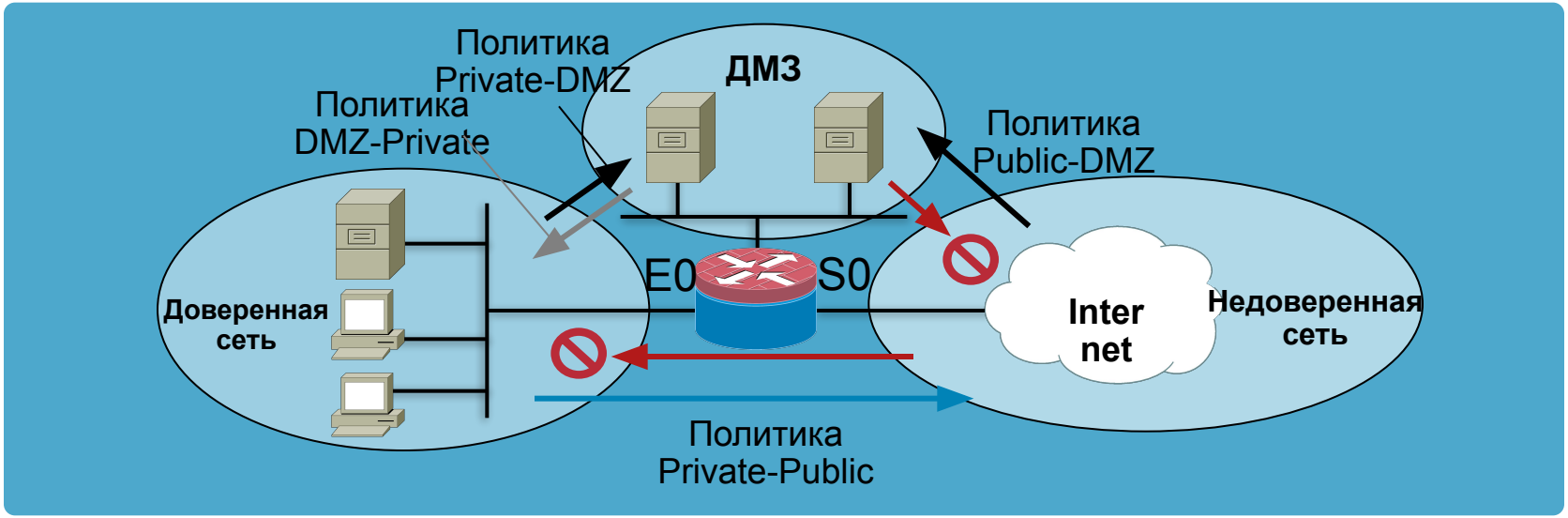
Обзор МСЭ на основе политик зон

12.4(6)T

- Поддержка группирования физических и виртуальных интерфейсов по зонам
- Политики МСЭ применяются к трафику, передающемуся между зонами
- Простота добавления и удаления интерфейсов, а также их интеграции в политику МСЭ

Поддерживаемые функции

- Учет состояния сеансов
- Анализ трафика уровня приложений: IM, POP, IMAP, SMTP/ESMTP, HTTP
- Фильтрация по URL
- Настройка параметров в соответствии с политикой
- Прозрачный МСЭ
- МСЭ с учетом VRF



© 2010 Cisco Systems, Inc. All rights reserved.

План презентации

- Обзор маршрутизаторов ISR G2
- Устранение неполадок межсетевого экрана Cisco IOS
  - Обзор межсетевого экрана Cisco IOS
  - Обработка пакетов межсетевым экраном Cisco IOS
  - Устранение неполадок межсетевого экрана Cisco IOS
  - Типовые неполадки и способы их устранения
  - Резюме
- Устранение неполадок системы предотвращения вторжений Cisco IOS

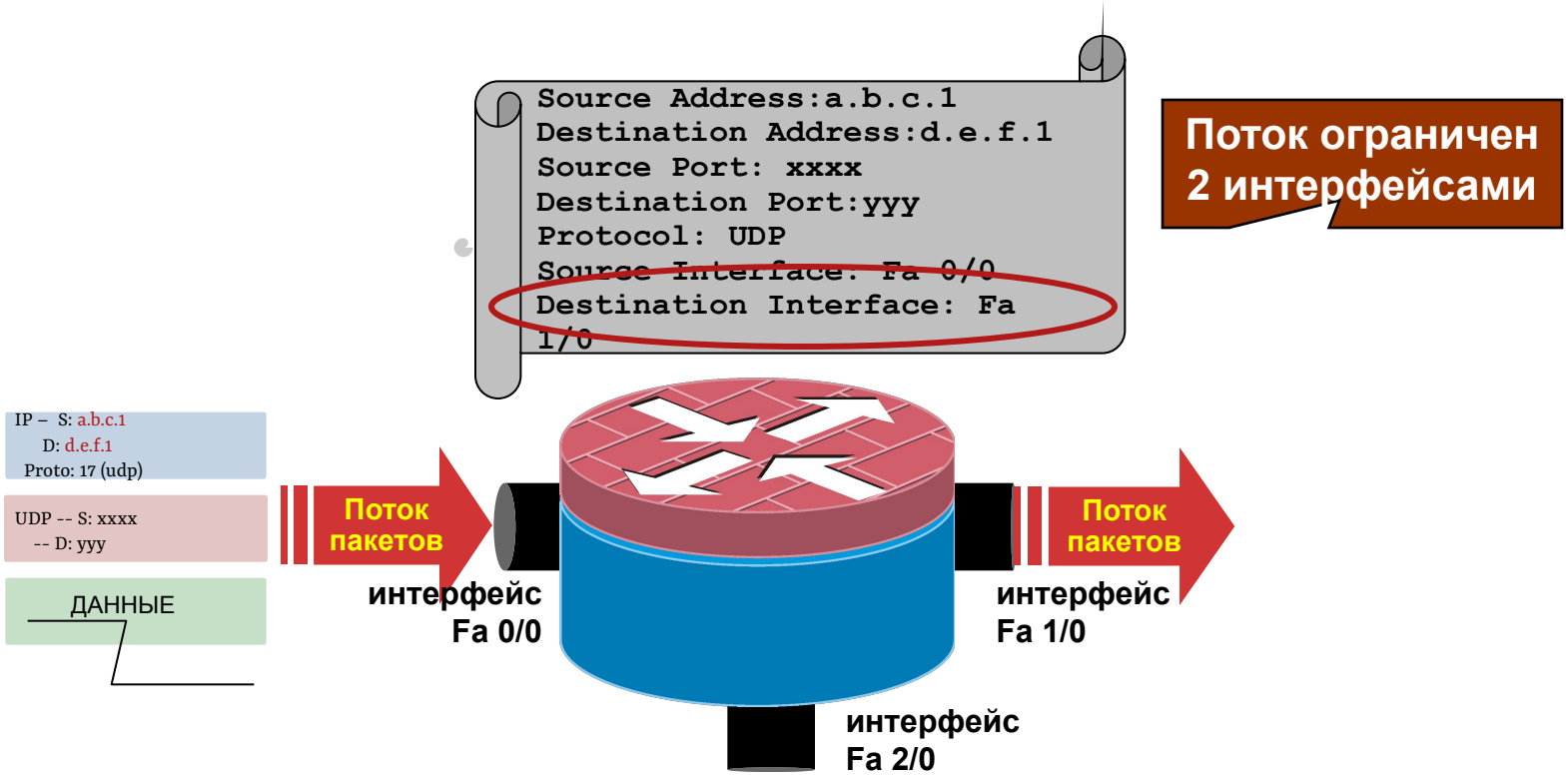
© 2010 Cisco Systems, Inc. All rights reserved.

Понимание схемы обработки пакетов

- Необходимо определить полный путь передачи пакета
- Локализовать неполадку до уровня отдельного устройства
- Определить правила обработки на основании IP-адреса отправителя, IP-адреса получателя, порта отправителя, порта получателя и протокола
- Определить интерфейсы/зоны между которыми передается пакет
- Выполнить систематическую отладку обработки пакета устройством в соответствии с настроенными функциями

© 2010 Cisco Systems, Inc. All rights reserved.

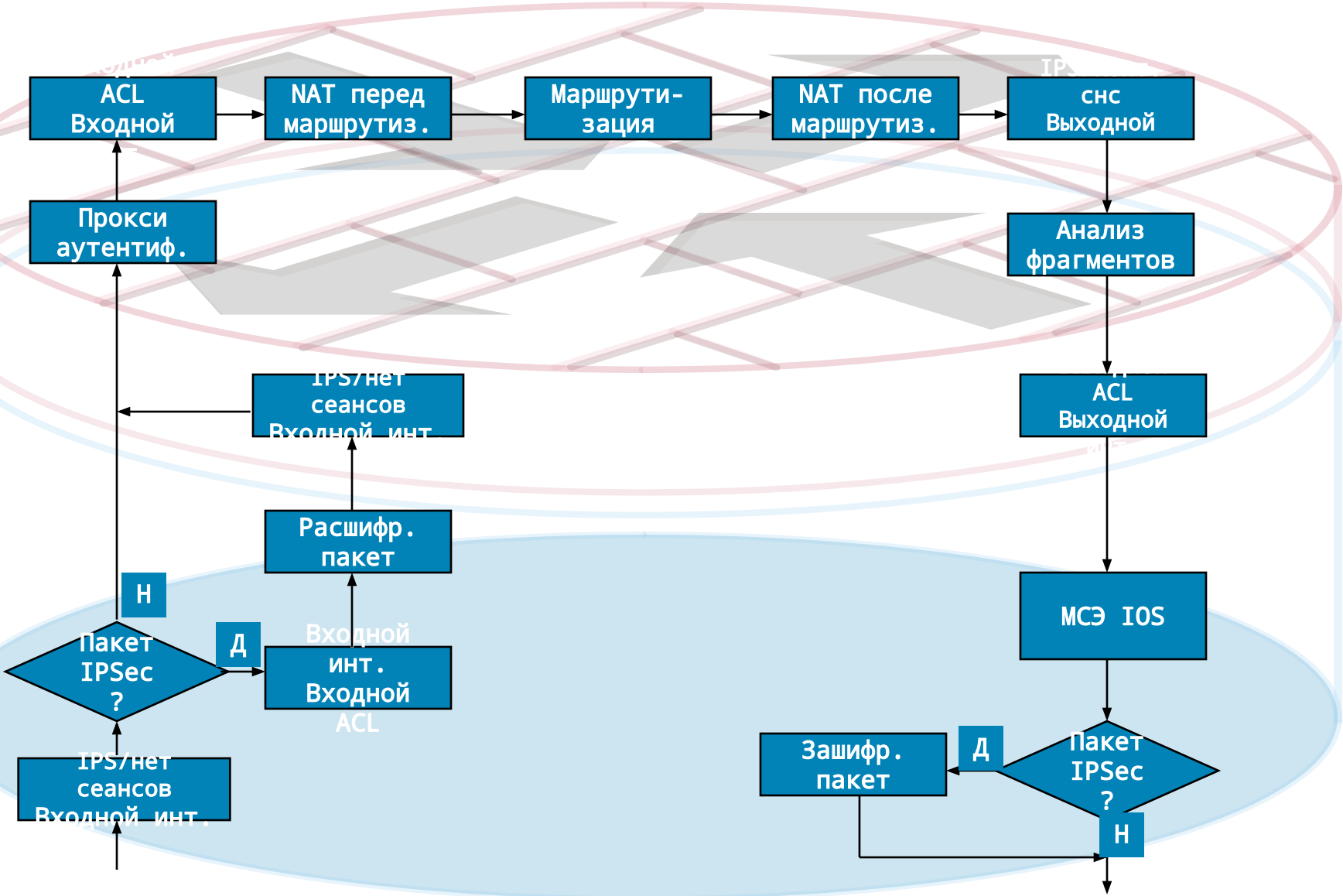
Обработка на устройстве



- Определение схемы обработки на устройстве позволяет сузить процесс устранения неполадки (проверки конфигурации и трассировки пакетов) до двух интерфейсов

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Общая схема обработки пакетов



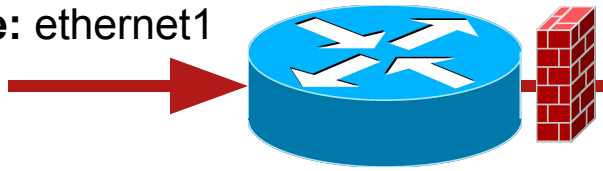
© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Поток пакетов: Private -> Public

Политика МСЭ применяется на интерфейсе Public

```
interface ethernet1
 ip access-group 101 in
 ip nat inside
```

```
interface ethernet0
 ip access-group 100 out
 ip nat outside
 ip inspect fw-policy out
 crypto map ipsec-policy
```



Интерфейс Private

Вход пакета → **Входной ACL** → **NAT** → **Маршру-тизация**

Интерфейс Public

NAT → **Выходной ACL** → **Выход МСЭ IOS** → **Шифро-вание IPSec**

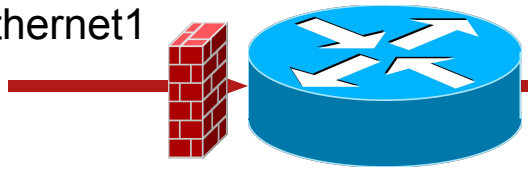
© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Поток пакетов: Private -> Public

Политика МСЭ применяется на интерфейсе Private

```
interface ethernet1
 ip access-group 101 in
 ip nat inside
 ip inspect fw-policy
in
```

```
interface ethernet0
 ip access-group 100 out
 ip nat outside
 crypto map ipsec-policy
```



Private: ethernet1

Public : ethernet0

Интерфейс Private

Вход пакета → **Входной ACL** → **NAT и маршру-тизация** → **Вход МСЭ IOS**

Интерфейс Public

NAT → **Выходной ACL** → **Маршру-тизация** → **Шифро-вание IPSec**

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Agenda

- Обзор маршрутизаторов ISR G2
- Устранение неполадок межсетевого экрана Cisco IOS
  - Обзор межсетевого экрана Cisco IOS
  - Обработка пакетов межсетевым экраном Cisco IOS
  - Устранение неполадок межсетевого экрана Cisco IOS
  - Типовые неполадки и способы их устранения
  - Резюме
- Устранение неполадок системы предотвращения вторжений Cisco IOS

© 2010 Cisco Systems, Inc. All rights reserved.

Конфигурация МСЭ на основе политик зон

```
class-map type inspect match-any myprotocol
 match protocol smtp
 match protocol ftp
 match protocol http

class-map type inspect match-all myclass
 match access-group 102
 match class-map myprotocol

policy-map type inspect mypolicy
 class type inspect myclass
  inspect

zone security private
zone security public

zone-pair security priv-pub source private destination public
 service-policy type inspect mypolicy

interface Ethernet0
 zone-member security private

interface Serial0
 zone-member security public

access-list 102 permit ip 192.168.0.0 0.0.255.255 any
```

Определение сервисов, анализируемых политикой

Сервисы с ACL для определения разрешенных/ заблокированных хостов (необязательно)

Определение действия МСЭ для трафика

Настройка зон

Формирование пары зон и применение политики

Назначение интерфейсов зонам

ACL 101 на исходящем интерфейсе больше не нужен для блокировки трафика.

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Средства устранения неполадок

- Syslog
- Команды *show*
- Анализ трассировки пакетов
- Команды *debug*

© 2010 Cisco Systems, Inc. All rights reserved.

Syslog

- Наиболее эффективное средство устранения неполадок межсетевого экрана на основе политик для зон
- Средство для формирования уведомления и формирования журналов аудита
- Средство для обнаружения удаления пакетов МСЭ
- Средство для сбора выходных данных команды *debug*

© 2010 Cisco Systems, Inc. All rights reserved.

Syslog — структура сообщения Syslog

Симптом: пользователь не может пользоваться web-сервером с IP-адресом 172.16.1.100

```
EC-SUN[100]# grep "172.16.1.100"
```

```
Jul 26 13:58:16 200.1.1.1 2166: Jul 26 18:0
%FW-6-SESS_AUDIT_TRAIL_START: (target:class
publicPrivateOut:myClassMap):Start http session: initiator
(10.1.1.100:3372) -- responder (172.16.1.100:80)
Jul 26 13:58:16 200.1.1.1 2167: Jul 26 18:02:34.907 UTC:
%APPFW-4-HTTP_JAVA_APPLET: HTTP Java Applet detected -
resetting session 172.16.1.100:80 10.1.1.100:3372 on
zone-pair publicPrivateOut class myClassMap appl-class
HttpAic
Jul 26 13:58:16 200.1.1.1 2168: Jul 26 18:02:34.919 UTC:
%FW-6-SESS_AUDIT_TRAIL:
(target:class)-(publicPrivateOut:myClassMap):Stop http
session: initiator
(10.1.1.100:3372) sent 297 bytes -- responder
:80) sent 0 bytes
```

Причина закрытия соединения

Имя пары зон

Имя карты классов

Имя политики AIC

© 2010 Cisco Systems, Inc. All rights reserved.

Syslog — анализ удаленных пакетов

- Введите команду "ip inspect log drop-pkt" для журналирования пакетов, удаленных МСЭ, с указанием причины удаления
- Функция добавлена в IOS версии 12.3(8)T
- Результаты выдаются 1 раз в 30 секунд

```
Router(config)#ip inspect log drop-pkt

Router#
...
*Mar 25 19:21:27.811: %FW-6-DROP_PKT: Dropping tcp session
   1.1.1.20:0 2.1.1.2:0  due to Invalid Header length with
   ip ident 7205
...
*Mar 25 19:30:23.131: %FW-6-DROP_PKT: Dropping tcp session
   1.1.1.20:59807 2.1.1.2:23  due to RST inside current
   window with ip ident 14992 tcpflags 0x5004 seq.no 7916131
   ack 1538156964
```


© 2010 Cisco Systems, Inc. All rights reserved.

Syslog — типовые причины удаления пакетов

Invalid Header length	Поле данных IP-пакета настолько мало, что в нем не может содержаться заголовок TCP, UDP или ICMP.
Segment matching no TCP connection	Получен не первый TCP-сегмент, для которого в таблице соединений нет соответствующего соединения.
Invalid Seq#	В сегменте содержится недопустимый порядковый номер данных TCP.
Invalid Ack (или no Ack)	В сегменте содержится недопустимый номер подтверждения данных TCP.
SYN inside current window	Сегмент с флагом SYN передается в рамках уже установленного TCP-соединения.
Out-Of-Order Segment	Обнаружен TCP-сегмент, который не соответствует установленному окну.
Stray Segment	Обнаружен TCP-сегмент, который не должен быть получен в данном состоянии конечного автомата TCP, например, сегмент "TCP SYN" в состоянии "listen".
Invalid Window scale option	Процесс-приемник TCP предлагает недопустимый вариант размера окна, а процесс-источник не предлагает установить размер окна.
RST inside current window	Сегмент с флагом RST передается в рамках уже установленного TCP-соединения.
SYN with data или with PSH/URG flags	В сегменте TCP SYN содержатся данные.

© 2010 Cisco Systems, Inc. All rights reserved.

Команды *show*

- Используются для отображения конфигурации и статистической информации о сетевых соединениях.
- БОЛЬШИНСТВО неполадок можно обнаружить с помощью команд *syslog* и *show.*
- Команды *show* для классического МСЭ Cisco IOS и МСЭ на основе политик зон различаются.

© 2010 Cisco Systems, Inc. All rights reserved.

Команды *show* — МСЭ на основе политик зон

- Отображение зоны и входящих в нее интерфейсов

```
show zone security [zone-name]
```

- Отображение сведений о паре зон

```
Router#show zone-pair security source private destination public
Zone-pair name priv-pub
    source-Zone private  Destination-Zone public
    service-policy priv-pub-pol
```

- Отображение статистики политики и сеансов

```
show policy-map type inspect { <policy name> [class <class name>]
  | zone-pair [<zone-pair name>] [sessions | urlfilter cache] }
```


© 2010 Cisco Systems, Inc. All rights reserved.

Команды *show* — МСЭ на основе политик зон

- Отображение статистики МСЭ

```
Router#show policy-map type inspect zone-pair

policy exists on zp priv-pub
 Zone-pair: priv-pub

  Service-policy inspect : firewall-pmap

    Class-map: L4-inspect-class (match-any)
      Match: protocol tcp
        1 packets, 24 bytes
        30 second rate 0 bps

   Inspect
        Packet inspection statistics [process switch:fast switch]
        tcp packets: [44:0]

        Session creations since subsystem startup or last reset 1
        Current session counts (estab/half-open/terminating) [1:0:0]
        Maxever session counts (estab/half-open/terminating) [1:1:0]
        Last session created 00:00:40
        Last statistic reset never
        Last session creation rate 1
        Maxever session creation rate 1
        Last half-open session total 0

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```


© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Команды *show* — МСЭ на основе политик зон

- Отображение сеансов МСЭ

```
Router#show policy-map type inspect zone-pair sessions

policy exists on zp priv-pub
 Zone-pair: priv-pub

  Service-policy inspect : firewall-pmap

    Class-map: L4-inspect-class (match-any)
      Match: protocol tcp
        1 packets, 24 bytes
        30 second rate 0 bps

   Inspect

      Number of Established Sessions = 1
      Established Sessions
        Session 5346C90 (1.1.1.20:44181)=>(2.1.1.2:23) tcp SIS_OPEN
          Created 00:09:22, Last heard 00:09:17
          Bytes sent (initiator:responder) [46:119]

    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```


© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

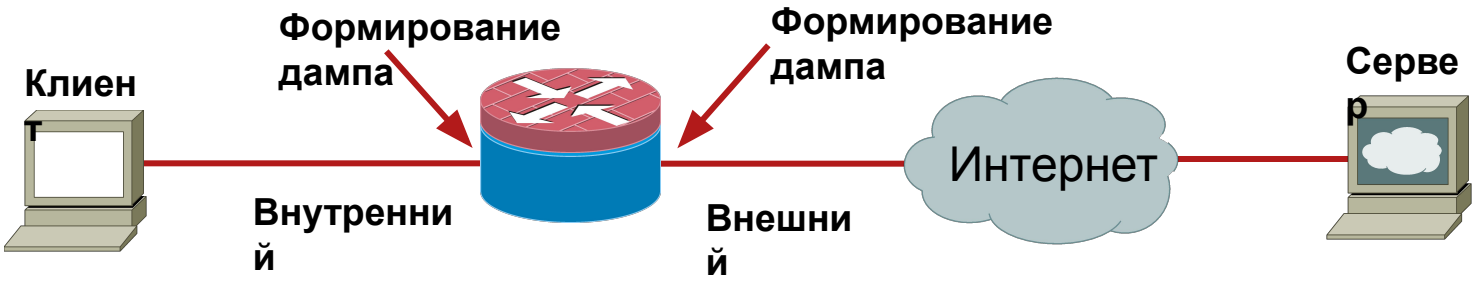
Использование дампов трафика

- В дампах трафика может содержаться подробная информация, недоступная с помощью команд *show* или сообщений *syslog*
- Формирование дампов выполняется вне МСЭ
- Мощное средство устранения неполадок L4 и L7
- Новая инфраструктура формирования дампов трафика, введенная в версии 12.4(20)T, упрощает сбор данных
  - Возможность формирования дампов трафика IPv4 и IPv6 в пути CEF
  - Настраиваемый буфер и параметры точки формирования дампа
  - Расширяемые возможности фильтрации и экспорта данных
  - Поддержка различных типов инкапсуляции в каналах WAN

© 2010 Cisco Systems, Inc. All rights reserved.

Использование дампов пакетов для устранения неполадок МСЭ

- Типовой сценарий: сбой приложения x при попытке работы через МСЭ



  - Настройка фильтра для формирования дампа нужного потока
  - Запуск формирования дампов на входе и выходе МСЭ
  - Запуск приложения
  - Сравнение дампов для обнаружения удаленных пакетов и сопоставления с журналами МСЭ

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Использование встроенных средств формирования дампа IOS

- Основные этапы настройки
  - Создание буфера и точки формирования дампа
  - Связывание точки формирования с буфером
  - Запуск/остановка формирования дампа

```
Router#monitor capture buffer  test-buffer
Router#monitor capture buffer test-buffer filter  access-list 120
Filter Association succeeded
Router#
Router#monitor capture point ip cef test-capture serial 2/0 both
*Mar 26 20:33:10.896: %BUFCAP-6-CREATE: Capture Point test-capture
created.
Router#monitor capture point  associate test-capture test-buffer
Router#monitor capture point  start test-capture
*Mar 26 20:34:03.108: %BUFCAP-6-ENABLE: Capture Point test-capture
enabled.
Router#
Router#monitor capture point  stop test-capture
*Mar 26 20:34:21.636: %BUFCAP-6-DISABLE: Capture Point test-capture
disabled.
```


© 2010 Cisco Systems, Inc. All rights reserved.

Использование встроенных средств формирования дампа IOS

Дамп готов, что дальше?

- Просмотр пакетов на маршрутизаторе

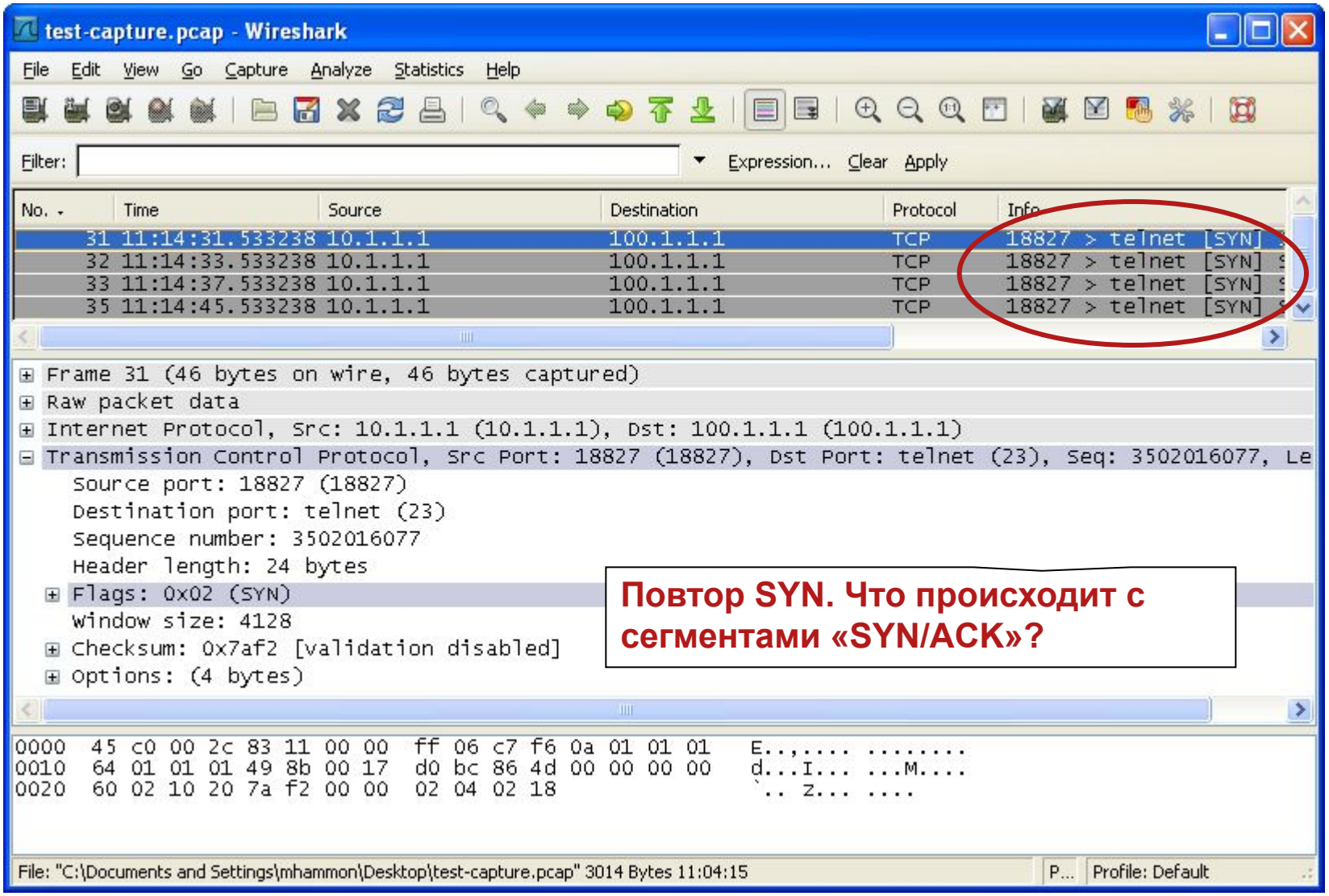
```
Router#show monitor capture buffer test-buffer dump
15:34:07.228 EST Mar 26 2010 : IPv4 LES CEF    : Se2/0 None

05CECE30:                   0F000800 45C0002C          ....E@.,
05CECE40: 6D170000 FE0649DD 02010102 01010114  m...~.I].........
05CECE50: 0017A353 0FB6B952 3EF1499C 60121020  ..#S.69R>qI.`..
05CECE60: 917A0000 02040218 00                 .z.......
.
.
```

- Или экспорт и анализ в Ethereal/Wireshark

```
Router# monitor capture buffer test-buffer export ?
  ftp:    Location to dump buffer
  http:   Location to dump buffer
  https:  Location to dump buffer
  rcp:    Location to dump buffer
  scp:    Location to dump buffer
  tftp:   Location to dump buffer
```


© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Использование Wireshark для анализа дампа



Повтор SYN. Что происходит с сегментами «SYN/ACK»?

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Команды *debug*

- Команды *debug* — **последнее** средство устранения неполадки.
- Использование команд *debug* может создать существенную нагрузку на ЦП устройства.
- Команды *debug* для МСЭ Cisco IOS не поддерживают задание условий
- Перед запуском команды *debug* необходимо оценить загруженность маршрутизатора
- При запуске команд *debug* необходимо следовать оптимальным методикам
- Нередко команды *debug* используют для обнаружения ошибок в МСЭ Cisco IOS, а не для устранения неполадок

© 2010 Cisco Systems, Inc. All rights reserved.

Команда отладки МСЭ Cisco IOS

Отладка TCP-соединения через МСЭ

```
Router#debug policy-firewall protocol tcp
Policy-Firewall TCP debugging is on
Router#debug policy-firewall detail
Policy-Firewall detailed debugging is on

FIREWALL: NEW PAK 4DC7548 (0:1.1.1.20:12573) (0:2.1.1.2:23) tcp

FIREWALL sis 5347070: pak 4DC7548 --> SIS_OPENING/SYNSENT processed
    seg iisn 4010527639 i_rcvnxt 0 i_sndnxt 4010527640 i_rcvwnd 4128
    i_rcvlmt 0 r_rcvlmt 0 risn 0 r_rcvnxt 0 r_sndnxt 0 r_rcvwnd 0

FIREWALL sis 5347070: pak 4A53B18 --> SIS_OPENING/SYNRCVD processed
    seg ...

FIREWALL sis 5347070: pak 4DC7F58 --> SIS_OPEN/ESTAB processed seg ...

FIREWALL sis 5347070: L4 result: PASS packet 0x04DC7F58
    (1.1.1.20:12573) (2.1.1.2:23) bytes 32
```


© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Полезные команды *debug*

- Для прозрачного МСЭ (команды *show* напоминают команды для МСЭ L3)

```
ISR-1841#debug ip inspect l2-transparent ?
  dhcp-passthrough  DHCP passthrough
  packets           L2 Inspection packets
```

- Другие команды *debug*

  debug policy-firewall obj-creation

  debug policy-firewall obj-deletion

  debug policy-firewall events

  debug policy-firewall protocol <протокол>

© 2010 Cisco Systems, Inc. All rights reserved.

План презентации

- Обзор маршрутизаторов ISR G2
- Устранение неполадок межсетевого экрана Cisco IOS
  - Обзор межсетевого экрана Cisco IOS
  - Обработка пакетов межсетевым экраном Cisco IOS
  - Устранение неполадок межсетевого экрана Cisco IOS
  - Типовые неполадки и способы их устранения
  - Резюме
- Устранение неполадок системы предотвращения вторжений Cisco IOS

© 2010 Cisco Systems, Inc. All rights reserved.

Типовые неполадки и способы их устранения

- Снижение производительности «при включении МСЭ IOS»
- МСЭ Cisco IOS удаляет легитимные пакеты
- Анализ выполняется при передаче трафика не в том направлении
- Фрагментация и МСЭ Cisco IOS
- IPSec и неполадки МСЭ Cisco IOS
- Закрытие HTTP-соединений
- Не работает приложение, использующее многоканальный протокол (FTP, VoIP)

© 2010 Cisco Systems, Inc. All rights reserved.

Снижение производительности

Симптом:

- После включения МСЭ IOS скорость передачи резко падает
- Легитимные пакеты начинают удаляться через некоторое время после включения МСЭ

Этапы устранения неполадки:

Шаг 1. Определение процесса, создающего наибольшую нагрузку на ЦП

```
Router# show processes cpu | exclude 0.00
CPU utilization for five seconds: 70%/39%; one minute: 52%; five minutes: 43%
 PID Runtime(ms)   Invoked      uSecs   5Sec   1Min   5Min TTY Process
  74        1388     31823         43  0.08%  0.04%  0.04%   0 EAPFramework
  84      983836    305327       3222 38.18% 37.74% 37.02%   0 IP Input
 120       24468      3070       7970  1.22%  1.27%  1.26%   0 Inspect process
```

Решение:

- Процесс IP Input должен характеризоваться наибольшими показателями
- Если показатели любого процесса > показателей процесса IP Input, следует проанализировать этот процесс (возможно, МСЭ IOS ни при чем)
- Если показатели процесса IP Input ВЕЛИКИ, неполадка может быть связана с работой МСЭ IOS

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Снижение производительности (продолжение)

Этапы устранения неполадки:

Шаг 2a. Просмотр статистики МСЭ

```
Router# show ip inspect statistics
< Removed >
Session creations since subsystem startup or last reset 2
Current session counts (estab/half-open/terminating) [421416853:566]
Maxever session counts (estab/half-open/terminating) [421416853:566]
```

Шаг 2b. Проверка параметров защиты от атак типа «отказ в обслуживании»

```
ip inspect max-incomplete high value (default 500)
ip inspect max-incomplete low value (default 400)
ip inspect one-minute high value (default 500)
ip inspect one-minute low value (default 400)
ip inspect tcp max-incomplete host value (default 50) [block-time
    minutes
```


© 2010 Cisco Systems, Inc. All rights reserved.

Снижение производительности (продолжение)

Решение:

Настройка параметров защиты от атак типа «отказ в обслуживании»

Шаг 1. Убедитесь, что на хостах сети нет вирусов или червей, которые могут создавать множество соединений.

Шаг 2. Установите очень большие значения для параметров группы max-incomplete. Если производительность возрастет, откорректируйте их значения в соответствии с трафиком в сети.

```
ip inspect max-incomplete high 20000000
ip inspect one-minute high 100000000
ip inspect tcp max-incomplete host 100000 block-time 0
```

До версии 12.4(11)T значения параметров защиты от атак типа «отказ в обслуживании» по умолчанию были небольшими
http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_white_paper0900aec
С версии 12.4(11)T по умолчанию установлены большие значения

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Снижение производительности (продолжение)

Этапы устранения неполадки:

Шаг 3. Проанализируйте политику МСЭ IOS и убедитесь, что выполняется анализ HTTP-трафика

```
ip inspect name IOSFirewall http
ip inspect name IOSFirewall https
ip inspect name IOSFirewall pop3
ip inspect name IOSFirewall smtp
ip inspect name IOSFirewall dns
```

Команда "Inspect http" добавляет возможность анализировать возвращаемое содержимое для Java-апплетов, т. е. сказывается на производительности

Решение:

Если фильтрация Java-апплетов НЕ требуется, отключите анализ http-трафика. В противном случае создайте список (Java-list), чтобы отключить анализ контента с доверенных сайтов.

```
ip inspect name IOSFirewall http  java-list 20
ip inspect name IOSFirewall smtp
ip inspect name IOSFirewall dns

access-list 20 permit 10.1.1.0 0.0.0.255
```


© 2010 Cisco Systems, Inc. All rights reserved.

Снижение производительности (продолжение)

Этапы устранения неполадки:

Шаг 4. Проверьте, не были ли изменены значения тайм-аута для UDP и DNS, принятые по умолчанию

- Если для тайм-аута DNS или UDP было установлено слишком ВЫСОКОЕ значение, маршрутизатор окажется перегружен в результате слишком большого числа активных, но неиспользуемых UDP- или DNS-сеансов.
- Если для тайм-аута UDP или DNS было установлено слишком НИЗКОЕ значение, сеанс может закрываться преждевременно, что в итоге приведет к созданию намного большего числа сеансов, чем необходимо

Решение:

- Установите для **тайм-аута UDP значение 30 секунд (по умолчанию**, а для **тайм-аута DNS — 5 секунд (по умолчанию)**, если нет четких причин для изменения этих значений.

```
Router(config)#ip inspect dns-timeout 5
```

- Настройка DNS в политике МСЭ приводила к снижению производительности (bug ID: CSCse35588). **Ошибка устранена в версии IOS 12.4(11)T.**

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Анализ выполняется при передаче трафика не в том направлении

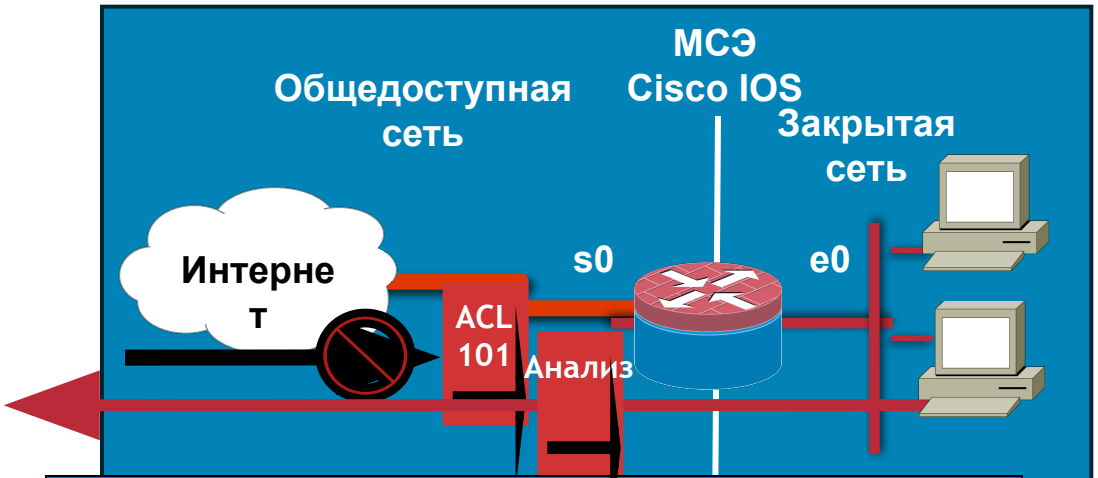
Симптом:

Через маршрутизатор не передается трафик в обратном направлении, возможно, он удаляется ACL

```
access-list 101 deny ip any any
interface Serial0
  description outside
  ip access-group 101 in
```

```
ip inspect name IOSFW tcp
ip inspect name IOSFW udp
```

```
interface Serial0
  description outside
  ip inspect IOSFW in
```



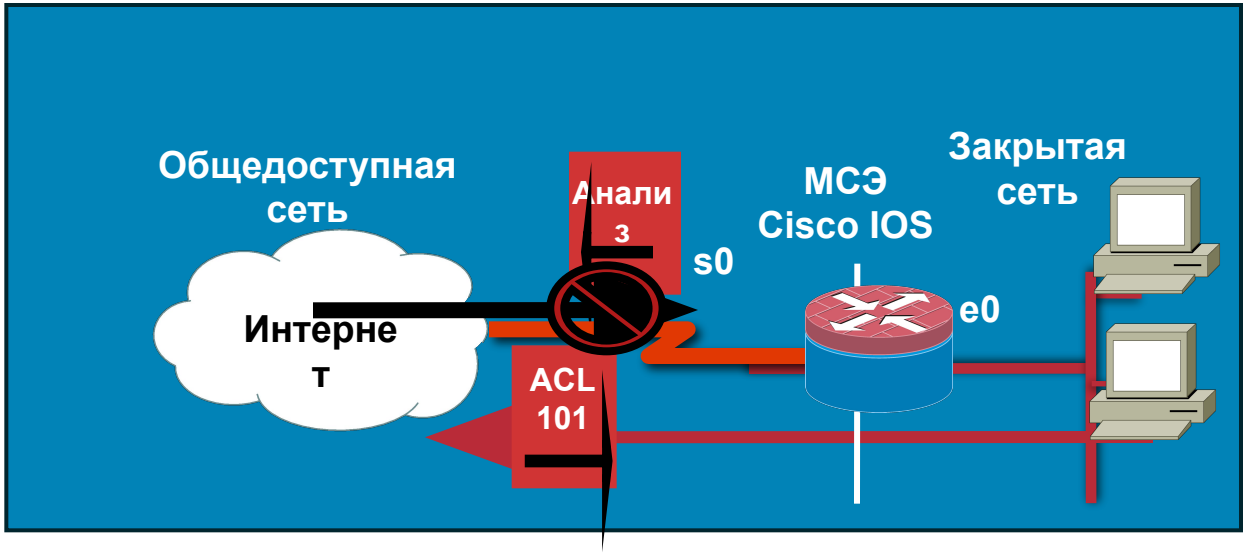
Политика анализа входящего трафика и ACL применяются на выходном интерфейсе, трафик из Интернета удаляется ACL 101

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Анализ выполняется при передаче трафика не в том направлении

Этапы устранения неполадки:

- Выполните команду show ip inspect sessions на маршрутизаторе, чтобы просмотреть таблицу сеансов (она будет пуста)
- Проверьте направление трафика, обрабатываемого на интерфейсе ACL и средствами анализа; анализ и ACL распространяются на входящий трафик



© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Фрагментация и МСЭ Cisco IOS

- До IOS версии 12.3(8)T

  Использование анализа фрагментированных пакетов в ситуациях, когда легитимные фрагменты могли поступать с нарушением порядка следования, могли привести к снижению производительности (фрагменты удалялись).

  ```
  Router(config)# ip inspect name inspection-name fragment
  ```

- С версии 12.3(8)T

  Теперь МСЭ IOS использует "механизм виртуальной сборки фрагментированных пакетов" (VFR). IOS поддерживает буфер для переупорядочивания и виртуальной сборки фрашментированных IP-датаграмм, соответственно, МСЭ IOS может управлять сеансами, в которых передаются фрагментированные пакеты. Этот режим необходимо включить как на внешнем, так и на внутреннем интерфейсах.

  ```
  Router(config-if)# ip virtual-reassembly
  ```


© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

IPSec и МСЭ Cisco IOS

Описание проблемы:

Как выполняется обработка IPSec-трафика на МСЭ Cisco IOS

Решения:

МСЭ IOS обрабатывает трафик IPSec в одном из двух режимов:

- МСЭ IOS и ядро IPSec функционируют на одном маршрутизаторе
  - МСЭ IOS не анализирует расшифрованные входящие пакеты
  - МСЭ IOS анализирует исходящие пакеты перед шифрованием для передачи на внешний интерфейс
  - Для работы IPSec на интерфейсе необходимо разрешить трафик UDP/500 (ISKMP), UDP/4500 (NAT-T), IP 50 (ESP)/ IP 51 (AH)
- Транзитный трафик IPSec через МСЭ IOS
  - МСЭ IOS не будет анализировать зашифрованные IPSec-пакеты, поскольку значение поля "протокол" в IP-заголовке отличается от TCP/UDP
  - Будет анализироваться трафик ISKMP (UDP/500)
  - Для передачи IPSec-трафика маршрутизатор должен допускать передачу UDP/500 (ISKMP) UDP/4500 (NAT-T), IP 50 (ESP)/ IP 51 (AH)

© 2010 Cisco Systems, Inc. All rights reserved.

IPSec и межсетевой экран на основе политик зон

- Два типа IPSec-конфигурации
- Классическая конфигурация (к интерфейсу применяется криптосхема, нет ассоциации интерфейса VPN с зоной)
- Конфигурация IPSec на интерфейсе
  - GRE over IPSec
  - DMVPN
  - Статический VTI (интерфейс виртуального туннеля)
  - EzVPN с использованием динамического VTI
- VPN-интерфейс должен принадлежать к зоне безопасности

© 2010 Cisco Systems, Inc. All rights reserved.

Классическая конфигурация IPSec на МСЭ на основе политик зон

- Определение политик безопасности зон

Исходная зона \ Целевая зона	Private	Public
Private	N/A	Разрешить весь исходящий TCP/UDP/ICMP-трафик
Public	Разрешить TCP/UDP/ICMP-трафик из туннеля и web-трафик на сервер 192.168.1.10	N/A

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Классическая конфигурация IPSec с МСЭ на основе политик зон - конфигурация

```
class-map type inspect match-any
all-traffic
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-all
pub-pri-cmap
 match class-map all-traffic
 match access-group name
tunnel-traffic
class-map type inspect match-all
inbound-web
 match protocol http
 match access-group name web-server
!
policy-map type inspect pri-pub-pmap
 class type inspect all-traffic
  inspect
policy-map type inspect pub-pri-pmap
 class type inspect pub-pri-cmap
 inspect
 class type inspect inbound-web
  inspect
```

```
zone security public
 description Internet facing zone
zone security private
 description Secure private zone
zone-pair security pub-pri source public
destination private
 service-policy type inspect pub-pri-pmap
zone-pair security pri-pub source private
destination public
 service-policy type inspect pri-pub-pmap
!
interface FastEthernet0/0
zone-member security public
 crypto map test
!
interface FastEthernet1/0
 zone-member security private
!
ip access-list extended tunnel-traffic
 permit ip 192.168.2.0 0.0.0.255
192.168.1.0 0.0.0.255
ip access-list extended web-server
 permit ip any host 192.168.1.10
```


© 2010 Cisco Systems, Inc. All rights reserved.

Настройка IPSec на интерфейсах для МСЭ на основе политик зон

- Определение политик безопасности зон

Исходная зона \ Целевая зона	Private	Public	VPN
Private	N/A	Разрешить весь TCP/UDP/ICMP-трафик	Разрешить весь TCP/UDP/ICMP-трафик
Public	Разрешить web-трафик на адрес 192.168.1.10	N/A	Запретить
VPN	Разрешить весь TCP-трафик	Запретить	N/A

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Настройка IPSec на интерфейсах для МСЭ на основе политик зон — конфигурация

```
class-map type inspect match-any
tcp-traffic
 match protocol tcp
!
policy-map type inspect pri-pub-pmap
 class type inspect all-traffic
  inspect
policy-map type inspect pub-pri-pmap
 class type inspect inbound-web
  inspect
policy-map type inspect pri-vpn-pmap
 class type inspect all-traffic
  inspect
policy-map type inspect vpn-pri-pmap
 class type inspect tcp-traffic
  inspect
!
zone security public
 description Internet facing zone
zone security private
 description Secure private zone
zone security vpn
 description This is the VPN zone
```

```
zone-pair security pub-pri source public
destination private
 service-policy type inspect pub-pri-pmap
zone-pair security pri-pub source private
destination public
 service-policy type inspect pri-pub-pmap
zone-pair security vpn-pri source vpn
destination private
 service-policy type inspect vpn-pri-pmap
zone-pair security pri-vpn source private
destination vpn
 service-policy type inspect pri-vpn-pmap
!
interface Tunnel0
 zone-member security vpn
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile test
!
interface FastEthernet0/0
 zone-member security public
!
interface FastEthernet1/0
 zone-member security private
```


© 2010 Cisco Systems, Inc. All rights reserved.

Принудительное закрытие HTTP-соединения

Симптом:

Неожиданное принудительное закрытие соединения при пользовании web-сайтом.

Этапы устранения неполадки:

Шаг 1a. Анализ сообщений *syslog* от маршрутизатора

```
Jul 26 13:58:16 200.1.1.1 2167: Jul 26 18:02:34.907 UTC: %APPFW-4-
    HTTP_JAVA_APPLET: HTTP Java Applet detected - resetting session
    172.16.1.100:80 10.1.1.100:3372 on zone-pair publicPrivateOut
    class myClassMap appl-class HttpAic
```

Шаг 1b. Анализ конфигурации с помощью команды *show*.

```
class-map type inspect http match-any HttpAic
match response body java-applet
exit
policy-map type inspect http HttpAicPolicy
class type inspect http HttpAic
reset
log
Exit
```

Решение:

Удалить кома

Причина закрытия соединения

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Принудительное закрытие HTTP-соединения (продолжение)

Этапы устранения неполадки:

Шаг 2a. Анализ сообщений *syslog* от маршрутизатора –

```
Jul 26 15:03:51 200.1.1.1 2768: Jul 26 19:08:08.751 UTC:
  %APPFW-4-HTTP_CONTENT_LENGTH: Content length (82271) out
  of range - resetting session 208.254.0.103:80
  10.1.1.100:3491 on zone-pair publicPrivateOut class
  myClassMap appl-class HttpAic
```

Шаг 2b. Использование команды *show* показывает, что для параметра "Body Length" web-трафика установлено слишком НИЗКОЕ значение.

Решение:

Увеличить допустимую запроса/ответа –

```
class-map type inspect http match-any  HttpAic
match req-resp body length  gt 1000000
exit
```


© 2010 Cisco Systems, Inc. All rights reserved.

Принудительное закрытие HTTP-соединения (продолжение)

Этапы устранения неполадки:

Шаг 3a. В ходе анализа сообщений *syslog* обнаружено следующее –

```
Jul 27 13:12:39 200.1.1.1 5448:
Sig:12 HTTP URI length exceeded. Received
10.1.1.100:1451 to 216.73.86.52:
```

Шаг 3b. При анализе конфигурации с помощью команды *show* может выясниться, что для параметра "Request URI Length" установлено слишком НИЗКОЕ значение.

Решение:

Задание длины URI, равной 256 байт –

```
class-map type inspect http match-any HttpAic
match request uri length gt 256
exit
```


© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Нарушение работы многоканальных протоколов

Симптомы:

- Пример 1. FTP-соединение с сервером устанавливается, просмотр каталогов (ls) невозможен.
- Пример 2. Вызовы принимаются и отправляются, но ничего не слышно.

Этапы устранения неполадки:

Проверка состояния соединения для передачи данных с помощью команды **"show ip inspect session"**.

Анализ сообщений *syslog*.

Решение:

Необходимо проанализировать работу каждого многоканального протокола в отдельности.

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

План презентации

- Обзор маршрутизаторов ISR G2
- Устранение неполадок межсетевого экрана Cisco IOS
  - Обзор межсетевого экрана Cisco IOS
  - Обработка пакетов межсетевым экраном Cisco IOS
  - Устранение неполадок межсетевого экрана Cisco IOS
  - Типовые неполадки и способы их устранения
  - Резюме
- Устранение неполадок системы предотвращения вторжений Cisco IOS

© 2010 Cisco Systems, Inc. All rights reserved.

Резюме

- ВСЕГДА СЛЕДУЙТЕ системному подходу при устранении неполадок МСЭ IOS
- НЕ ИЗМЕНЯЙТЕ установленные по умолчанию значения тайм-аутов для сеансов UDP и DNS
- Определите профиль трафика в своей сети, проходящего через МСЭ IOS, и настройте параметры защиты от DoS-атак соотвествующим образом
- ВСЕГДА применяйте анализ трафик в направлении исходного потока трафика
- Для многоканальных протоколов ВСЕГДА анализируйте работу протокола уровня приложений

© 2010 Cisco Systems, Inc. All rights reserved.

Резюме

- Руководство по проектированию и применению МСЭ Cisco IOS на основе политик зон

  http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml

- Страница, посвященная средствам безопасности маршрутизаторов

  http://www.cisco.com/en/US/products/sw/secursw/ps1018/index.html

© 2010 Cisco Systems, Inc. All rights reserved.

План презентации

- Обзор маршрутизаторов ISR G2
- Устранение неполадок межсетевого экрана Cisco IOS
- Устранение неполадок системы предотвращения вторжений Cisco IOS
  - Обзор IPS Cisco IOS
  - Обработка пакетов
  - Устранение неполадок
  - Типовые неполадки и способы их устранения
  - Резюме

© 2010 Cisco Systems, Inc. All rights reserved.

Система предотвращения вторжений Cisco IOS — обзор

- До версии 12.3(8)T называлась IDS, использовалась команда "ip audit"
- С версии 12.3(8)T называется "IPS Cisco IOS"
- Программный сенсор системы предотвращения вторжений при транзитной передаче трафика
- Поддерживает формат сигнатур Cisco IPS версии 5.x с версии 12.4(11)T*
- Анализ пакетов на основе сигнатур, набор сигнатур соответствует платформе сенсоров IPS 4200
- Динамическое обновление сигнатур, не требующее обновления образа IOS
- Возможность настройки различных событий для сигнатуры и категории
- Простота управления — CCP, CSM**

* Формат сигнатур версии 5.x не совместим с форматом сигнатур версии 4.x

** CCP = Cisco Configuration Professional; CSM = Cisco Security Manager

© 2010 Cisco Systems, Inc. All rights reserved.

Система предотвращения вторжений Cisco IOS — системные компоненты

- Микроядра сигнатур (SME)

  SME определяет параметры сигнатур в категории для определенного протокола, например HTTP

- Файлы сигнатур

  Содержат ядро сигнатур, сведения о параметрах (например, имя сигнатуры, ИД сигнатуры, действия при срабатывании сигнатуры) и т. п.

- Категории сигнатур*

  В категории сигнатур содержатся заранее сформированные наборы сигнатур для определенной уязвимости

- SEAP (Signature Event Action Processor, процессор действий для сигнатур)

  SEAP обеспечивает возможность расширенной фильтрации действий и позволяет переопределять основные параметры механизма ERR (Event Risk Rating)

- Мониторинг событий

  Сообщения *syslog* и/или уведомления SDEE** для событий, сформированных IPS IOS

* Только для формата сигнатур версии 5.x (IOS 12.4(11)T или более поздней версии)

** SDEE = Security Device Event Exchange

© 2010 Cisco Systems, Inc. All rights reserved.

Категории сигнатур

- В IPS IOS с сигнатурами в формате Cisco IPS 5.x/6.x используются категории сигнатур
- Категория сигнатур представляет собой группу соответствующих сигнатур, объединенных под информативным именем
- Все сигнатуры разделены на категории
- Отдельная сигнатура может принадлежать к нескольким категориям

```
Router#sh ip ips category ?

  adware/spyware          Adware/Spyware (more sub-categories)
  attack                  Attack (more sub-categories)
  ddos                    DDoS (more sub-categories)
  dos                     DoS (more sub-categories)
  email                   Email (more sub-categories)
  instant_messaging       Instant Messaging (more sub-categories)
  ios_ips                 IOS IPS (more sub-categories)
  l2/l3/l4_protocol       L2/L3/L4 Protocol (more sub-categories)
  network_services        Network Services (more sub-categories)
  os                      OS (more sub-categories)
  other_services          Other Services (more sub-categories)
  p2p                     P2P (more sub-categories)
  reconnaissance          Reconnaissance (more sub-categories)
  releases                Releases (more sub-categories)
  viruses/worms/trojans   Viruses/Worms/Trojans (more sub-categories)
  web_server              Web Server (more sub-categories)
```

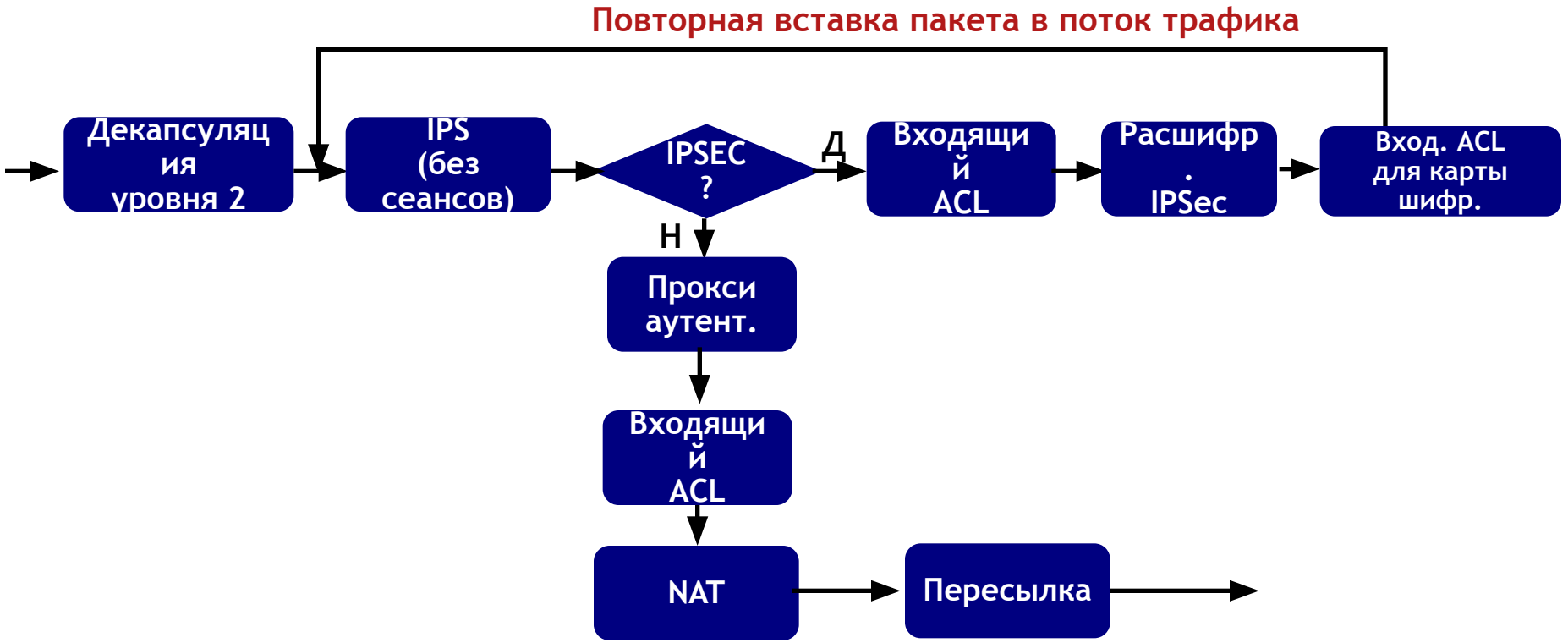

© 2010 Cisco Systems, Inc. All rights reserved.

План презентации

- Обзор маршрутизаторов ISR G2
- Устранение неполадок межсетевого экрана Cisco IOS
- Устранение неполадок системы предотвращения вторжений Cisco IOS
  - Обзор IPS Cisco IOS
  - Обработка пакетов
  - Устранение неполадок
  - Типовые неполадки и способы их устранения
  - Резюме

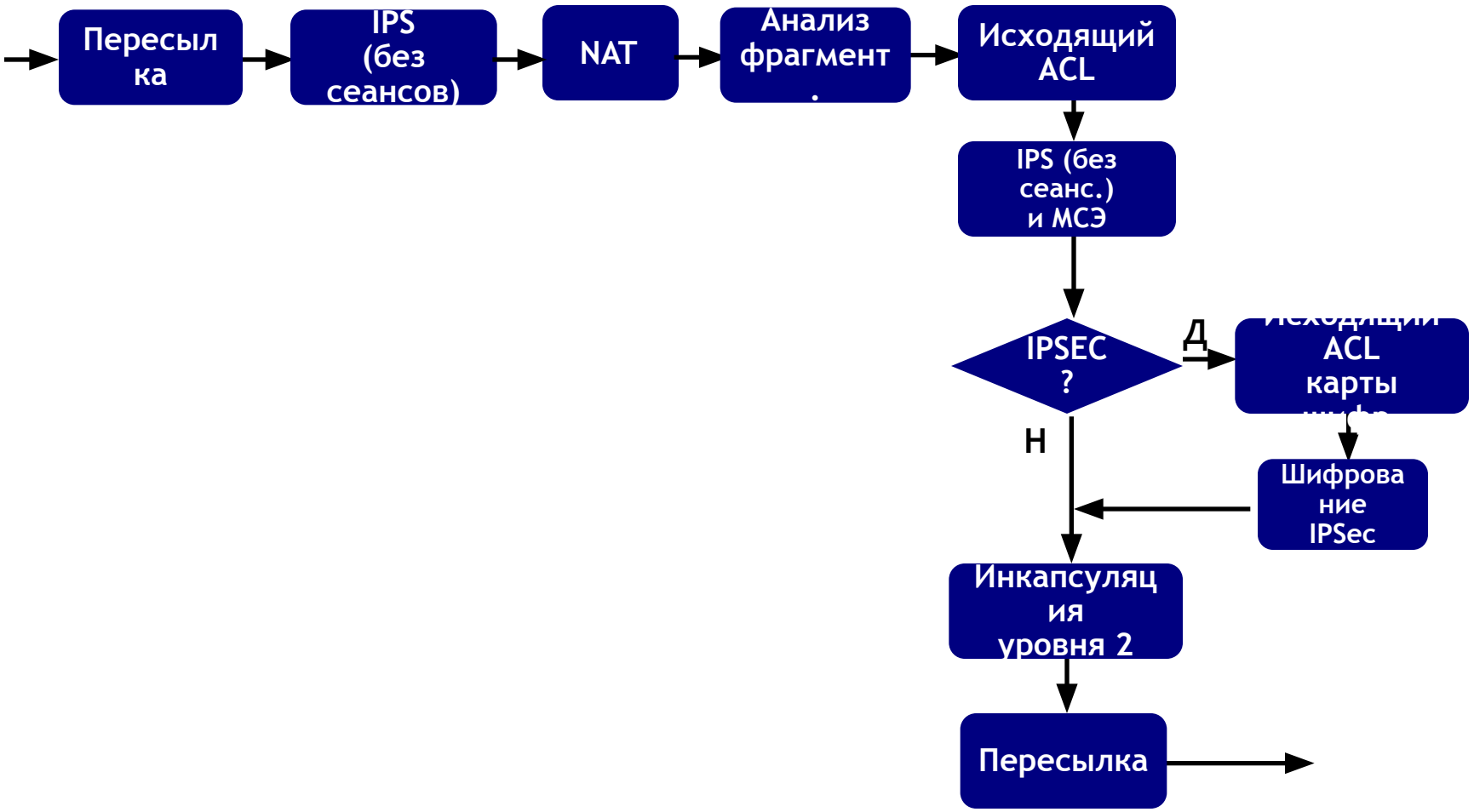
© 2010 Cisco Systems, Inc. All rights reserved.

Обработка пакетов в IPS Cisco IOS — входящий трафик



© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Обработка пакетов IPSec/IPS — исходящий трафик



© 2010 Cisco Systems, Inc. All rights reserved.

План презентации

- Обзор маршрутизаторов ISR G2
- Устранение неполадок межсетевого экрана Cisco IOS
- Устранение неполадок системы предотвращения вторжений Cisco IOS
  - Обзор IPS Cisco IOS
  - Обработка пакетов
  - Устранение неполадок
  - Типовые неполадки и способы их устранения
  - Резюме

© 2010 Cisco Systems, Inc. All rights reserved.

Пример базовой конфигурации

```
ip ips config location flash:ips/ retries 1
ip ips notify SDEE
ip ips name iosips
```

```
ip ips signature-category
  category all
   retired true
  category ios_ips advanced
   retired false
```

В начале ВСЕГДА выбирается категория “all” И блокируются все сигнатуры

```
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
   |
   snip
   |
   F3020301 0001
  quit
```

Ключ IPS IOS

```
interface GigabitEthernet0/1
 ip address 10.1.1.6 255.255.255.0
 ip ips iosips in
 ip virtual-reassembly
 duplex auto
 speed auto
```

Включение политики IPS IOS на интерфейсе

© 2010 Cisco Systems, Inc. All rights reserved.

Настройка уведомлений о событиях с использованием SDEE

- Сообщения SDEE передаются по HTTP/HTTPS
- Для использования SDEE необходимо включить HTTP/HTTPS
- При использовании IME рекомендуется установить количество одновременных подписок, равное 3

```
Router(config)#ip sdee subscriptions ?
      <1-3>  Number of concurrent SDEE subscriptions
```

- Формат сообщения в журнале IPS IOS:

```
*Mar 22 03:53:13.827: %IPS-4-SIGNATURE: Sig:5114 Subsig:1 Sev:75 WWW IIS
  Unicode Attack [10.1.1.252:4150 -> 192.168.1.249:80] RiskRating:75

*Mar 22 03:53:13.827: %IPS-4-SIGNATURE: Sig:5081 Subsig:0 Sev:100
 WWW WinNT cmd.exe Access [10.1.1.252:4150 -> 192.168.1.249:80]
  RiskRating:100
```


© 2010 Cisco Systems, Inc. All rights reserved.

Типовые этапы устранения неполадок

1. Проверьте конфигурацию IPS IOS, чтобы убедиться, что политика применена к нужному интерфейсу в нужном направлении

```
show run
```

2. Проверьте состояние сигнатур, чтобы убедиться, что они скомпилированы

```
show ip ips config
show ip ips signatures count
```

3. Проверьте потоки трафика, анализируемые IPS IOS, чтобы убедиться, что IPS IOS анализирует трафик

```
show ip ips sessions detail
```

4. Проверяйте уведомления SDEE / сообщения *syslog*, чтобы убедиться, что атаки обнаруживаются

```
show ip sdee alerts
show logging
```

5. Используйте соответствующие команды *debug*

© 2010 Cisco Systems, Inc. All rights reserved.

Команды для устранения неполадок IPS IOS

Шаг 1. Проверка конфигурации IPS IOS

```
Router#sh run
Building configuration...

-- output skipped --
!
ip ips config location flash:ips/ retries 1
ip ips notify SDEE
ip ips name iosips
!
ip ips signature-category
  category all
   retired true
  category ios_ips advanced
   retired false
!
crypto key pubkey-chain rsa
 named-key realm-cisco.pub signature
  key-string
   30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101

  -- output skipped --

   F3020301 0001
  quit
!
interface GigabitEthernet0/1
 ip address 10.1.1.6 255.255.255.0
 ip ips iosips in
 ip virtual-reassembly
```


© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Команды для устранения неполадок IPS IOS

Шаг 2. Проверка конфигурации IPS IOS и состояния сигнатур

```
Router#sh ip ips all

IPS Signature File Configuration Status
    Configured Config Locations: flash:ips/
    Last signature default load time: 16:42:08 PST Mar 1 2008
    Last signature delta load time: 22:59:57 PST Mar 3 2008
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 581
    Total Inactive Signatures: 1623

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name iosips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface GigabitEthernet0/1
        Inbound IPS rule is iosips
        Outgoing IPS rule is not set

IPS Category CLI Configuration:
    Category all:
        Retire: True
    Category ios_ips advanced:
        Retire: False
```

Определение кол-ва активных сигнатур

Проверка, что политика IPS IOS применена к нужному интерфейсу в нужном направлении

Проверка использования категории сигнатур

© 2010 Cisco Systems, Inc. All rights reserved.

Команды для устранения неполадок IPS IOS

Шаг 2. Проверка состояния сигнатур

```
Router#show ip ips signatures count

Cisco SDF release version S318.0
Trend SDF release version V0.0

Signature Micro-Engine: multi-string: Total Signatures 8
      multi-string enabled signatures: 8
      multi-string retired signatures: 8

- output omitted -

Signature Micro-Engine: service-msrpc: Total Signatures 27
      service-msrpc enabled signatures: 27
      service-msrpc retired signatures: 19
      service-msrpc compiled signatures: 1
      service-msrpc inactive signatures - invalid params: 7

Total Signatures: 2204
   Total Enabled Signatures: 873
   Total Retired Signatures: 1617
   Total Compiled Signatures: 580
   Total Signatures with invalid parameters: 7
   Total Obsoleted Signatures: 11
```

Проверка версии выпуска сигнатур

Проверка, что сигнатуры скомпилированы

© 2010 Cisco Systems, Inc. All rights reserved.

Команды для устранения неполадок IPS IOS

Шаг 3. Проверка потоков, анализируемых IPS IOS

```
Router#show ip ips sessions detail
Established Sessions

 Session 47506A34 (10.1.1.252:3959)=>(192.168.1.249:21) tcp SIS_OPEN
  Created 00:02:49, Last heard 00:02:44
  Bytes sent (initiator:responder) [25:95]
  sig cand list ID 14272
  sig cand list ID 14273
```


© 2010 Cisco Systems, Inc. All rights reserved.

Команды для устранения неполадок IPS IOS

Шаг 4. Проверка уведомлений

```
Router#sh logging
   Syslog logging: enabled (12 messages dropped, 7 messages rate-limited,
                   0 flushes, 0 overruns, xml disabled, filtering disabled)

   -- output skipped --

   Log Buffer (4096 bytes):

   *Mar 22 03:53:13.827: %IPS-4-SIGNATURE: Sig:5114 Subsig:1 Sev:75 WWW IIS Unicode
   Attack [10.1.1.252:4150 -> 192.168.1.249:80] RiskRating:75
   *Mar 22 03:53:13.827: %IPS-4-SIGNATURE: Sig:5081 Subsig:0 Sev:100 WWW WinNT cmd.exe
   Access [10.1.1.252:4150 -> 192.168.1.249:80] RiskRating:100
```

```
Router#sh ip sdee alerts
   Alert storage: 200 alerts using 75200 bytes of memory
                                  SDEE Alerts
         SigID    Sig Name                      SrcIP:SrcPort          DstIP:DstPort
                                                  or Summary Info
      1:  5114:1  WWW IIS Unicode Attack         10.1.1.252:4150      192.168.1.249:80
      2:  5081:0  WWW WinNT cmd.exe Access       10.1.1.252:4150      192.168.1.249:80
```

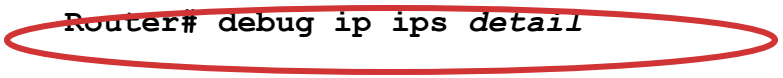

© 2010 Cisco Systems, Inc. All rights reserved.

Команды отладки IPS Cisco IOS

Шаг 5. Использование команд *debug*

- Включение отладки определенных ядер IPS IOS

```
Router# debug ip ips timers
Router# debug ip ips [object-creation | object-deletion]
Router# debug ip ips function trace
Router# debug ip ips detail
```



Не рекомендуется в производственной сети

- Команды *debug* L3/L4:

```
Router# debug ip ips [ip | icmp | tcp | udp]
```

- Команды *debug* уровня приложений:

```
Router# debug ip ips [tftp | smtp | ftp-cmd | ftp-token]
```

- Включение отладки по определенным атрибутам SDEE

```
Router# debug ip sdee [alerts | details | messages | requests | subscriptions ]
```


© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

План презентации

- Обзор маршрутизаторов ISR G2
- Устранение неполадок межсетевого экрана Cisco IOS
- Устранение неполадок системы предотвращения вторжений Cisco IOS
  - Обзор IPS Cisco IOS
  - Обработка пакетов
  - Устранение неполадок
  - Типовые неполадки и способы их устранения
  - Резюме

© 2010 Cisco Systems, Inc. All rights reserved.

Типовые неполадки

- Неверное толкование терминов, используемых для описания состояния сигнатур
- Ошибки выделения памяти при компиляции сигнатур
- Общее число сигнатур, которое можно успешно скомпилировать
- Сбой при компиляции сигнатуры
- Этапы настройки
- Применение политики IPS Cisco IOS в неверном направлении/к неверному интерфейсу
- Несрабатывание сигнатуры при соответствующем ей трафике
- Трафик, соответствующий сигнатуре, обнаруживается, но не удаляется по умолчанию
- Удаление пакетов в связи с рассинхронизацией соединения

© 2010 Cisco Systems, Inc. All rights reserved.

Неверное толкование терминов, используемых для описания состояния сигнатур

- *Retire* и *unretire* (блокировка и разблокировка)
- *Enable* и *disable* (включение и отключение)
- *Compiled* и *loaded* (скомпилировано и загружено)
- В IPS Cisco IOS эти термины унаследованы от аппаратной IPS серии 4200
- С учетом ограничений по объему памяти большая часть сигнатур на маршрутизаторе заблокированы по умолчанию
- Пользователям IPS IOS необходимо контролировать как состояние «enable/disable», так и состояние «retire/unretire»

© 2010 Cisco Systems, Inc. All rights reserved.

Неверное толкование терминов, используемых для описания состояния сигнатур (продолж.)

Retire и **Unretire** (блокировка и разблокирование)

- Команды позволяют выбирать сигнатуры, которые используются IPS IOS для анализа трафика
- **Блокировка** сигнатуры означает, что IPS IOS НЕ будет компилировать эту сигнатуру в памяти для анализа трафика
- **Разблокирование** сигнатуры означает, что IPS IOS скомпилирует сигнатуру в памяти и будет использовать эту сигнатуру для анализа трафика
- Для блокировки и разблокирования отдельных сигнатур и целых категорий сигнатур может использоваться как интерфейс командной строки (*CLI*), так и *SDM/CCP*

© 2010 Cisco Systems, Inc. All rights reserved.

Неверное толкование терминов, используемых для описания состояния сигнатур (продолж.)

Enable и **Disable** (включение и выключение)

- Включение/выключение не означает включение/исключение сигнатур из набора, используемого IPS IOS
- **Включение** сигнатуры означает, что при срабатывании сигнатуры по пакету или сочетанию факторов будет выполнено связанное с сигнатурой действие

  Необходимо помнить, что действующими являются только *включенные* И *успешно скомпилированные* И *разблокированные* сигнатуры. Иными словами, если сигнатура заблокирована, то даже при ее включении она не будет скомпилирована (поскольку она заблокирована), и связанное с сигнатурой действие не будет выполнено
- **Выключение** сигнатуры означает, что при срабатывании сигнатуры по пакету или сочетанию факторов НЕ БУДЕТ выполняться связанное с сигнатурой действие

  Иными словами, если сигнатура выключена, то даже если она разблокирована и успешно скомпилирована, связанное с сигнатурой действие не будет выполнено
- Для включения и выключения отдельных сигнатур и целых категорий сигнатур может использоваться как интерфейс командной строки (*CLI*), так и *SDM/CCP*

© 2010 Cisco Systems, Inc. All rights reserved.

Неверное толкование терминов, используемых для описания состояния сигнатур (продолж.)

Compiled и **Loaded** (скомпилировано и загружено)

- **Загрузка** означает процесс анализа IPS IOS файлов сигнатур (файлов XML в расположении *config*) и заполнения БД сигнатур

  Это происходит при загрузке сигнатур с помощью команды "*copy <файл сиген.> idconf*" или при перезагрузке маршрутизатора с настроенной IPS IOS

- **Компиляция** означает процесс компиляции значений параметров разблокированных сигнатур в таблицу регулярных выражений

  Это происходит при разблокировании сигнатур или при изменении других параметров сигнатур, используемых в регулярных выражениях

  После компиляции сигнатур анализ трафика выполняется путем сопоставления пакетов со скомпилированными сигнатурами

© 2010 Cisco Systems, Inc. All rights reserved.

Ошибки выделения памяти при компиляции сигнатур

- Число сигнатур, которое можно скомпилировать, определяется объемом свободной памяти маршрутизатора.
- Если объем свободной памяти маршрутизатора недостаточно велик, сообщения о сбое при выделении памяти будут занесены в журнал.
- Для анализа трафика используются скомпилированные сигнатуры. После сбоя при выделении памяти компиляция сигнатур для текущего ядра будет прервана. IPS IOS перейдет к компиляции сигнатур для следующего ядра.

```
*Mar 18 07:09:36.887: %SYS-2-MALLOCFAIL: Memory allocation of 65536 bytes failed from 0x400C1024, alignment 0
Pool: Processor  Free: 673268  Cause: Memory fragmentation
Alternate Pool: None  Free: 0  Cause: No Alternate pool
 -Process= "Exec", ipl= 0, pid= 3,  -Traceback= 0x4164F41C 0x400AEF1C 0x400B4D58 0x400B52C4 0x400C102C
0x400C0820 0x400C23EC 0x400C0484 0x424C1DEC 0x424C2A4C 0x424C2FF0 0x424C31A0 0x430D6ECC 0x430D7864 0x430F0210
0x430FA0E8
*Mar 18 07:09:36.911: %SYS-2-CHUNKEXPANDFAIL: Could not expand chunk pool for regex. No memory available
-Process= "Chunk Manager", ipl= 3, pid= 1,  -Traceback= 0x4164F41C 0x400C06FC
*Mar 18 07:09:37.115: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 12024:0 - compilation of regular
expression failed
*Mar 18 07:09:41.535: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5280:0 - compilation of regular
expression failed
*Mar 18 07:09:44.955: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5284:0 - compilation of regular
expression failed
*Mar 18 07:09:44.979: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 12023:0 - compiles discontinued for this
engine
```


© 2010 Cisco Systems, Inc. All rights reserved.

Ошибки выделения памяти при компиляции сигнатур — решение

- Заранее определенные категории сигнатур IPS IOS *Basic* и *Advanced* содержат оптимальный набор сигнатур для всех конфигураций со стандартным объемом памяти
- Не следует разблокировать категорию *all*
- Для маршрутизаторов с объемом памяти 128 Мбайт рекомендуется использовать категорию IPS IOS *Basic*
- Для маршрутизаторов с объемом памяти 256 Мбайт рекомендуется использовать категорию IPS IOS *Advanced*
- Затем можно настроить набор сигнатур путем блокировки/разблокирования нескольких сигнатур в нужное время
- Объем свободной памяти необходимо контролировать после выполнения каждой операции, связанной с блокировкой/разблокированием сигнатур

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Общее число сигнатур, которое можно успешно скомпилировать

- Универсальной формулы не существует!
- Это число зависит от многих факторов:

  Объем свободной памяти маршрутизатора

  Типы разблокируемых сигнатур, например сигнатуры сложного ядра STRING.TCP
- Разблокирование сигнатур следует немедленно прекращать, как только объем свободной памяти маршрутизатора станет составлять менее 10% от общего объема памяти маршрутизатора

© 2010 Cisco Systems, Inc. All rights reserved.

Сбой при компиляции сигнатуры

- Существуют три основные причины сбоев при компиляции сигнатур
  - Ограничения по объему памяти
  - Отсутствие поддержки сигнатур в IPS IOS: сигнатуры META
  - Слишком большой объем таблицы регулярных выражений (таблица для конкретного ядра не должна превышать 32 Мбайт)
- Список сигнатур, поддерживаемых IPS IOS:

  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd8062ac75.html
- Для экономии памяти следует блокировать сигнатуры, которые не поддерживаются IPS IOS или не применимы к вашей сети

© 2010 Cisco Systems, Inc. All rights reserved.

Этапы настройки

- Выполняйте начальную настройку IPS Cisco IOS в следующем порядке:

  Шаг 1. Загрузите пакет сигнатур IPS IOS на ПК

  Шаг 2. Создайте конфигурационный каталог IPS IOS

  Шаг 3. Настройте криптографический ключ IPS IOS

  Шаг 4. Создайте политику IPS IOS и примените ее к интерфейсам

  Не забудьте СРАЗУ заблокировать категорию *all*

  Шаг 5. Загрузите пакет сигнатур IPS IOS на маршрутизаторе

- Затем проверьте конфигурацию и количество скомпилированных сигнатур:

  show ip ips configuration

  show ip ips signatures count

© 2010 Cisco Systems, Inc. All rights reserved.

Этапы настройки (продолжение)

- Теперь можно выполнить тонкую настройку набора сигнатур, используя следующие варианты:

  Блокировка/разблокирование сигнатур (добавление/удаление сигнатур из списка скомпилированных)

  Включение/выключение сигнатур (разрешение/запрет действий)

  Изменение действий, связанных с сигнатурами

- Краткое руководство по началу работы:

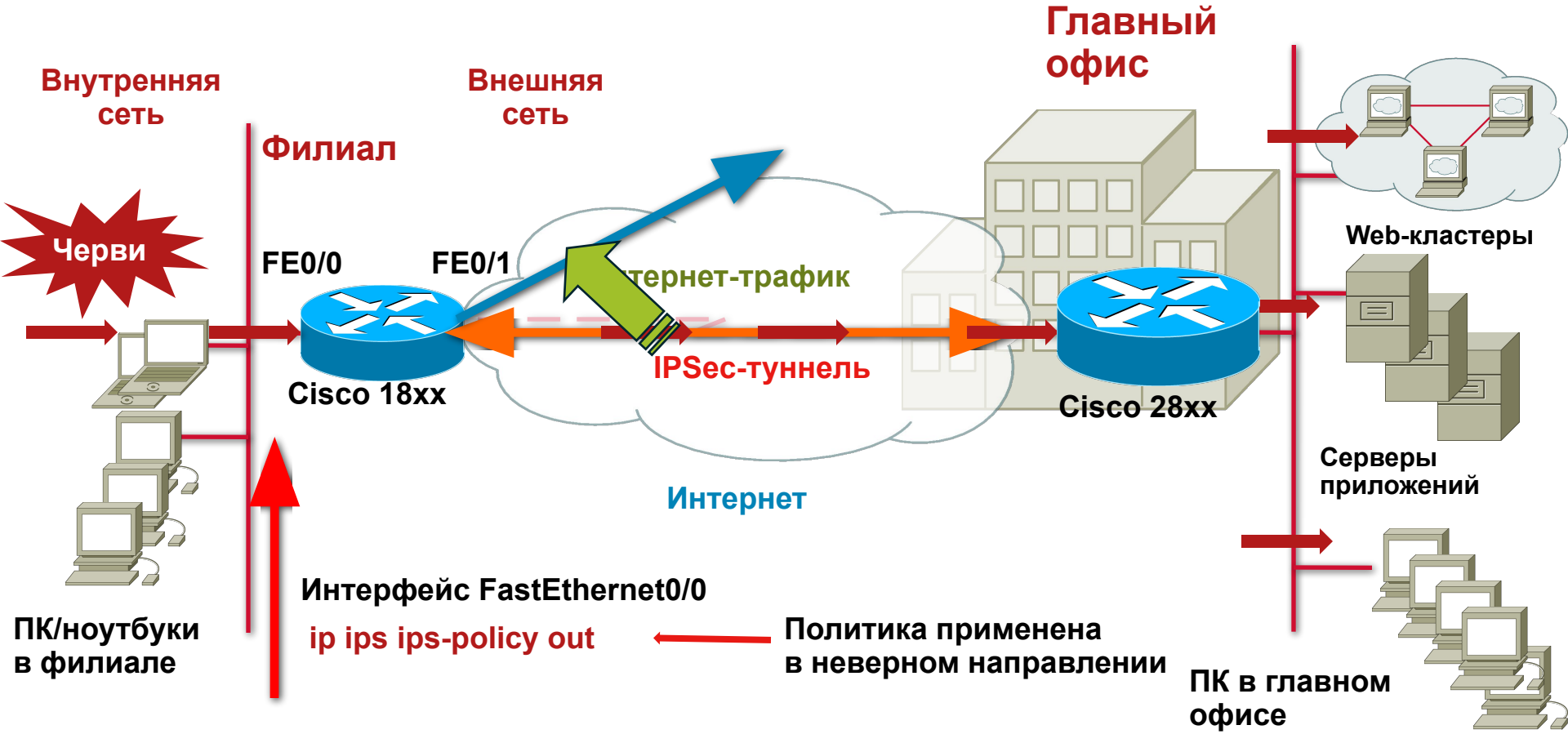
  http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

© 2010 Cisco Systems, Inc. All rights reserved.

Политика IPS IOS применяется к неверному направлению/интерфейсу — неверная конфигурация

Пример A: проблема

Защита от атак из внутренней сети

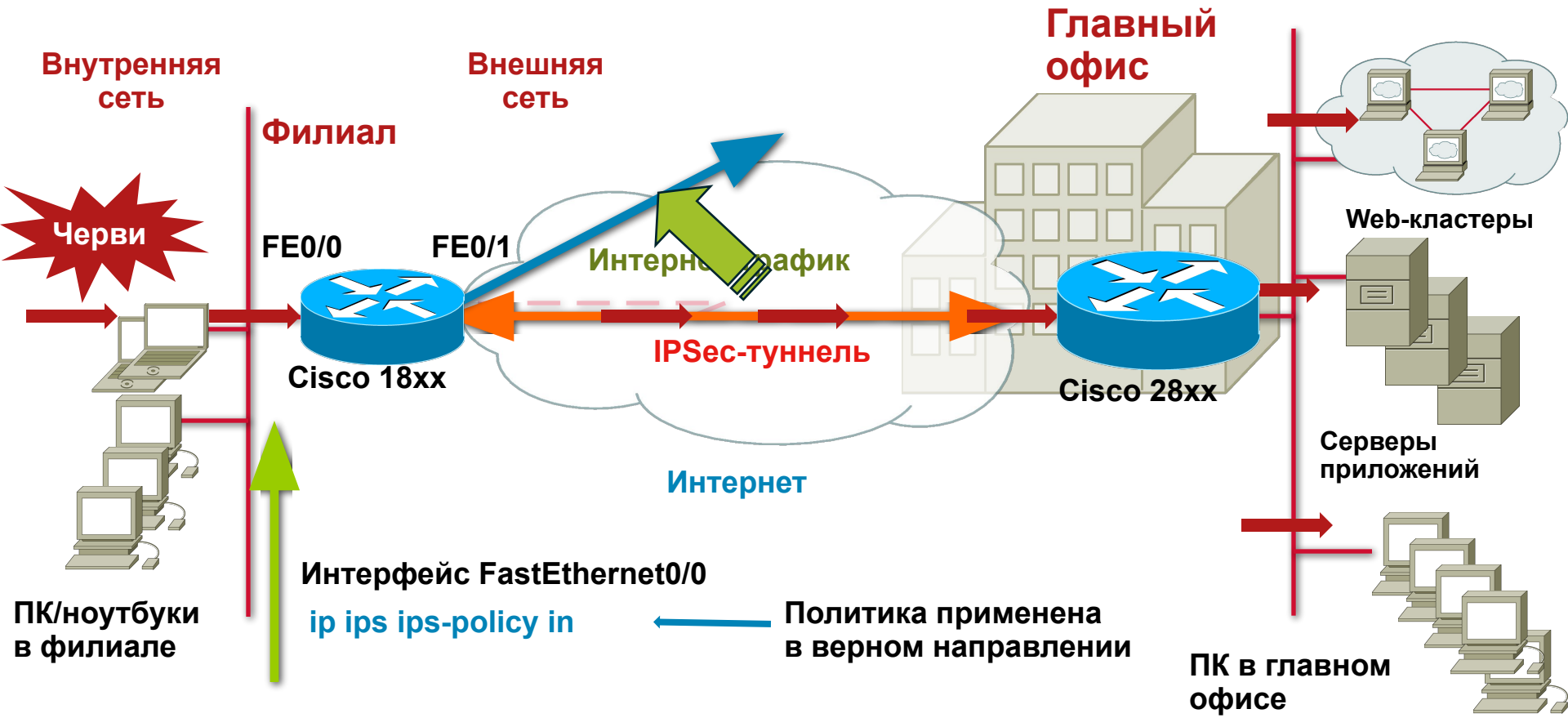


© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Политика IPS IOS применяется к неверному направлению/интерфейсу — решение

Пример A: решение

Защита от атак из внутренней сети



© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Политика IPS IOS применяется к неверному направлению/интерфейсу — неверная конфигурация

Пример B: проблема

Защита от атак из внешней сети

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Политика IPS IOS применяется к неверному направлению/интерфейсу — решение

Пример B: решение

Защита от атак из внешней сети

© 2010 Cisco Systems, Inc. All rights reserved. Cisco Partner

Несрабатывание сигнатуры при соответствующем ей трафике

- Убедитесь, что средства анализа IPS IOS используются в нужном направлении (входящий/исходящий) на нужном интерфейсе
- Включены ли уведомления о событиях IPS IOS (*syslog/SDEE*)?
- Есть ли сигналы/уведомления, подтверждающие соответствие сигнатуре?
- Необходимо убедиться, что трафик вызывает срабатывание сигнатуры
- Для контроля количества срабатываний сигнатуры используйте команду *show ip ips signatures statistics | i <Ид сиг. >*
- Выполните команду *debug*:

  debug ip ips <*имя ядра*>

  debug ip ips detailed

  debug ip ips function-trace (если две предыдущих команды не позволили получить нужную информацию)

© 2010 Cisco Systems, Inc. All rights reserved.

Трафик, соответствующий сигнатуре, обнаруживается, но не удаляется по умолчанию

- В выпусках пакетов сигнатур в формате версии 4.x (т. е., до версии IOS 12.4(11)T) в прекомпилированных файлах сигнатур (128/256MB.sdf) версии 5 и более ранних версий для сигнатур с рейтингом риска (RR) не меньше 95 по умолчанию задано удаление пакетов
- Эта настройка действия по умолчанию вызвала нарекания со стороны ряда активных пользователей
- Для обеспечения согласованности с работой автономного устройства Cisco IPS с версии 6 прекомпилированных файлов пакетов сигнатур (128/256MB.sdf) для таких сигнатур установлено действие по молчанию *produce-alert*
- В выпуске IOS 12.4(11)T и более поздних выпусках (формат сигнатур версии 5.x) для сигнатур IPS IOS установлено действие по умолчанию *produce-alert*

© 2010 Cisco Systems, Inc. All rights reserved.

Удаление пакетов на МСЭ в связи с рассинхронизацией соединения

Удаление пакетов на МСЭ в связи с рассинхронизацией TCP-соединения может замедлить сетевой трафик

После включения IPS время отклика систем, использующих web-трафик, может увеличиться. Проверьте, не поступают ли от маршрутизатора *syslog*-сообщения об удалении пакетов

```
*Jan  6 19:08:45.507: %FW-6-DROP_PKT: Dropping tcp pkt10.10.10.2:1090 => 199.200.9.1:443
*Jan  6 19:09:47.303: %FW-6-DROP_PKT: Dropping tcp pkt10.10.10.2:1091 => 199.200.9.1:443
*Jan  6 19:13:38.223: %FW-6-DROP_PKT: Dropping tcp pkt66.102.7.99:80 =>
192.168.18.21:1100
```

Команда *debug ip inspect detail* позволяет получить информацию о рассинхронизации

```
*Jan  6 19:15:28.931: CBAC* sis 84062FEC L4 inspectresult: SKIP packet 83A6F83C (199.200.9.1:443)
(192.168.18.21:1118) bytes 174 ErrStr = Out-Of-OrderSegment tcp
*Jan  6 19:15:28.931: CBAC* sis 84062FEC pak 83A6FF64SIS_OPEN/ESTAB TCP ACK 842755785 SEQ
2748926608 LEN 0 (10.10.10.2:1118) => (199.200.9.1:443)
*Jan  6 19:15:28.931: CBAC* sis 84062FEC pak 83A6F83CSIS_OPEN/ESTAB TCP ACK 2748926608 SEQ
842755785 LEN 1317 (199.200.9.1:443) <= (192.168.18.21:1118)
*Jan  6 19:15:28.931: CBAC* sis 84062FEC L4 inspectresult: SKIP packet 83A6F83C (199.200.9.1:443)
(192.168.18.21:1118) bytes 1317 ErrStr = RetransmittedSegment tcp
*Jan  6 19:15:28.935: CBAC* sis 84062FEC pak 83A6F83CSIS_OPEN/ESTAB TCP PSH ACK 2748926608
SEQ 842758636 LEN 137 (199.200.9.1:443) <=(192.168.18.21:1118)
*Jan  6 19:15:28.935: CBAC* sis 84062FEC L4 inspectresult: SKIP packet 83A6F83C (199.200.9.1:443)
(192.168.18.21:1118) bytes 137 ErrStr = Out-Of-OrderSegment tcp
```


© 2010 Cisco Systems, Inc. All rights reserved.

Удаление пакетов на МСЭ в связи с рассинхронизацией соединения — решение

Удаление пакетов на МСЭ в связи с рассинхронизацией TCP-соединения может замедлить сетевой трафик

- Для анализа трафика с использованием сигнатур IPS необходимо своевременное получение пакетов в нужном порядке, поэтому пакеты, поступающие с нарушением порядка следования удаляются; это одна из причин увеличения времени отклика
- IPS IOS поддерживает обработку пакетов, прибывших с нарушением порядка следования, начиная с выпуска 12.4(9)T2
- Эта ошибка не исправлена в выпусках 12.4, принадлежащих к основной линии
- Исправление *Out-of-Order* также распространяется на МСЭ уровня приложений
- Исправление *Out-of-order* НЕ распространяется на случай, когда интерфейс IPS IOS включен в зону МСЭ на основе политик зон
- Исправление *Out-of-order* работает при использовании IPS IOS и классического МСЭ IOS (ip inspect)
- При использовании выпуска, в котором отсутствует данное исправление, для устранения неполадки можно использовать ACL для направления потока трафика в обход IPS IOS

```
router(config)#access-list 120 deny ip any host 199.200.9.1
router(config)#access-list 120 deny ip host 199.200.9.1 any
router(config)#access-list 120 permit ip any any
router(config)#ip ips name myips list 120
```

- В этом примере ACL 120 запрещает весь трафик и предотвращает анализ трафика с использованием IPS; в этом случае не будут возникать задержки при передаче трафика

© 2010 Cisco Systems, Inc. All rights reserved.

План презентации

- Обзор маршрутизаторов ISR G2
- Устранение неполадок межсетевого экрана Cisco IOS
- Устранение неполадок системы предотвращения вторжений Cisco IOS
  - Обзор IPS Cisco IOS
  - Обработка пакетов
  - Устранение неполадок
  - Типовые неполадки и способы их устранения
  - Резюме

© 2010 Cisco Systems, Inc. All rights reserved.

Резюме

- Используйте "Краткое руководство по началу работы" в качестве справочника для проверки правильности конфигурации IPS IOS.
- Не забывайте в начале ЗАБЛОКИРОВАТЬ ВСЕ сигнатуры.

```
ip ips signature-category
  category all
    retired true
```

- Следуйте рекомендациям по использованию предопределенной категории IPS IOS *Basic* или *Advanced* и последующей настройке этой категории
- Команды IPS Cisco IOS *show* являются эффективным средством устранения неполадок
- Ссылка на документацию по IPS Cisco IOS: http://www.cisco.com/go/iosips

© 2010 Cisco Systems, Inc. All rights reserved.

Дополнительная информация

© 2010 Cisco Systems, Inc. All rights reserved.

Документация по средствам безопасности Cisco IOS

- Средства безопасности маршрутизаторов

  www.cisco.com/go/routersecurity

- Справочник по командам Cisco IOS, связанным с обеспечением безопасности

  http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a7f84.html#wp1187286

- Межсетевой экран Cisco IOS

  www.cisco.com/go/iosfw

- IPS Cisco IOS

  http://www.cisco.com/go/iosips

- Cisco Configuration Professional (CCP)

  http://www.cisco.com/go/ccp

© 2010 Cisco Systems, Inc. All rights reserved.

Ваши вопросы?

Security-request@cisco.com

© 2010 Cisco Systems, Inc. All rights reserved.

© 2010 Cisco Systems, Inc. All rights reserved.