Новое поколение сетевых устройств со встроенной безопасностью

Михаил Кадер

mkader@cisco.com

Security-request@cisco.com

План презентации

- Маршрутизаторы с интеграцией сервисов ISR G2
- Стимулы развития интегрированных средств безопасности
- Интегрированные средства управления угрозами
- Управление и мониторинг
- Соображения по проектированию
- Модели развертывания
- Резюме

Маршрутизаторы с интегрированными сервисами второго поколения

Успех предыдущего поколения

- Более 100 сетевых интерфейсов и модулей
- Самая широкая поддержка сервисов в индустрии
- До 70% снижения операционных затрат

Лидер с 2005

#1

Access Routing

Source: Dell 'Oro

Маршрутизатор следующего поколения

Services Performance Engine (3900)

Повышение производительности устройства

Многоядерный процессор

4x-кратный прирост производительности

Multi Gigabit Fabric

Связь модулей

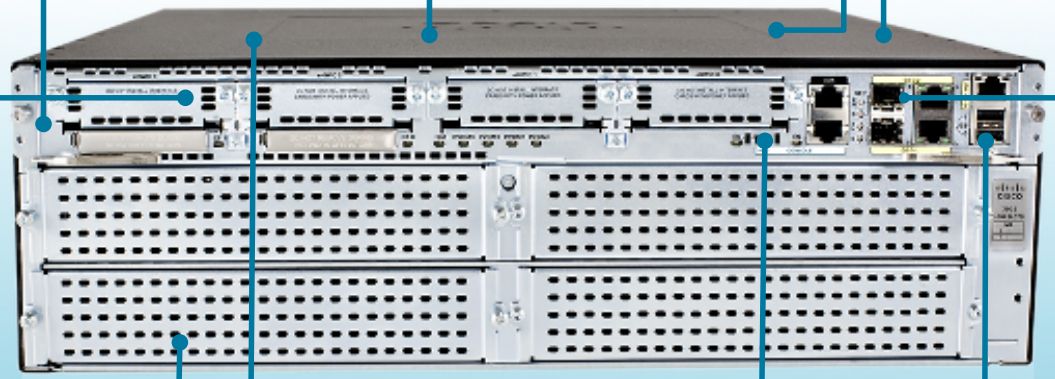
Приоретизация и шейпинг пакетов

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

Сервисные модули

3x-7x-кратный прирост производительности сервисного модуля

Адаптер для установки текущих NM

Поддержка EPoE

Встроенные модули

3x-кратный прирост производительности сервисного модуля

Режим экономии электропитания

Опция для 802.11n на 1941W

USB

Консоль через USB

Хранение файлов

Позиционирование ISR G2 по производительности

Производительность с сервисами при 75% загрузке процессора

Разнообразие сервисных модулей

Сеть и безопасность

Сетевые сервисы

Выжми из сети больше

- Wireless LAN Controller (WLC)
- Infoblox core network services (AXP)
- Cisco Network Analysis (NAM)
- Cisco Wide Area Application Services (WAAS)

Информационная и физическая безопасность

Защита и соответствие регуляторам

- Video Surveillance
- Intrusion Prevention

Совместная работа

Унифицированные коммуникации

Новые возможности

- Cisco Unity® Express module (voicemail, IVR)
- NICE Voice Recording (AXP)
- Sagem Interstar Fax over IP (AXP)
- SingleWire Informacast (AXP)

Обработка данных и приложения

Инфраструктурные приложения

Консолидация

- Cisco Application Extension Platform (AXP)
- Integrated Storage System
- Industry leading virtualization
- Windows Server

Промышленные приложения

Разработка приложений

- ICW Healthcare Connector on AXP
- Tiani Medical Data Exchange on AXP
- Global Protocols Skipware (AXP)

- В планах
- Доступны

Эволюция функциональных наборов IOS

1990-ые

IOS

Десятки образов, сложно поддерживать

2004+

IOS Reformation

Появились с ISR

Уменьшение сложности/ количества образов (8)

Лицензирование некоторых элементов

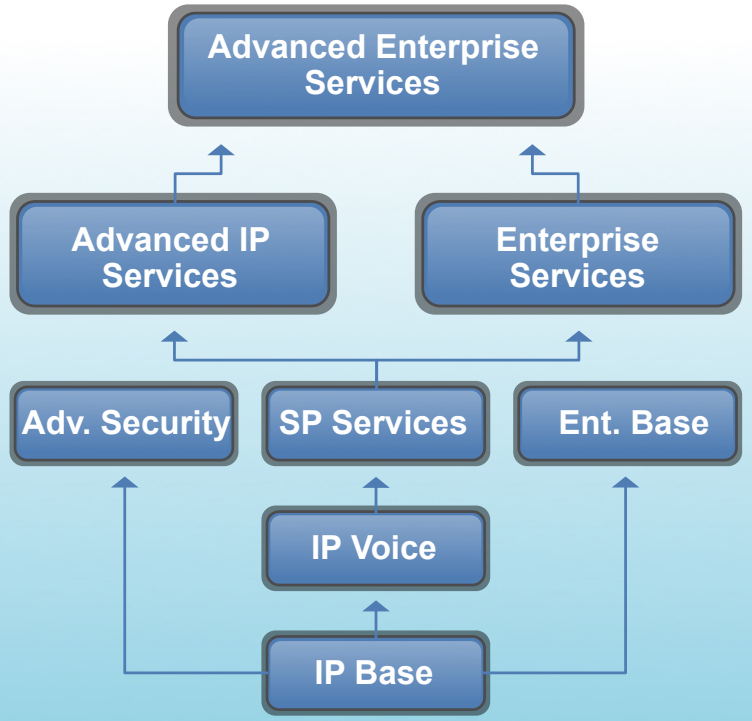
2010+

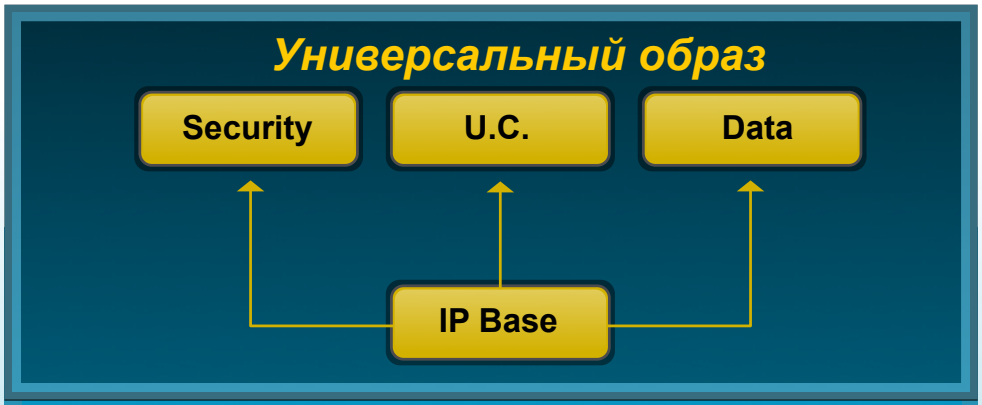
Software Activation

Простота приобретения и сопровождения

Включение сервисов по требованию

Новые технологические функциональные наборы





- **Упрощение управления ПО**
  - Единый универсальный образ Cisco IOS для всех платформ
  - Четыре лицензии на IOS обеспечивают полный набор функций, которые ранее предлагались в восьми вариантах образа IOS
- **Облегченный процесс апгрейда**
  - Апгрейд функциональности IOS происходит включением новой лицензии, не требуя копирования нового образа IOS в филиалы
- **Новая бизнес-модель ПО**
  - Сервисы по требованию—приобретение апгрейдов по мере необходимости

ISR G2: когда лучшее – … друг хорошему

Готовность к видео

Виртуализация сервисов

Превосходная эксплуатация

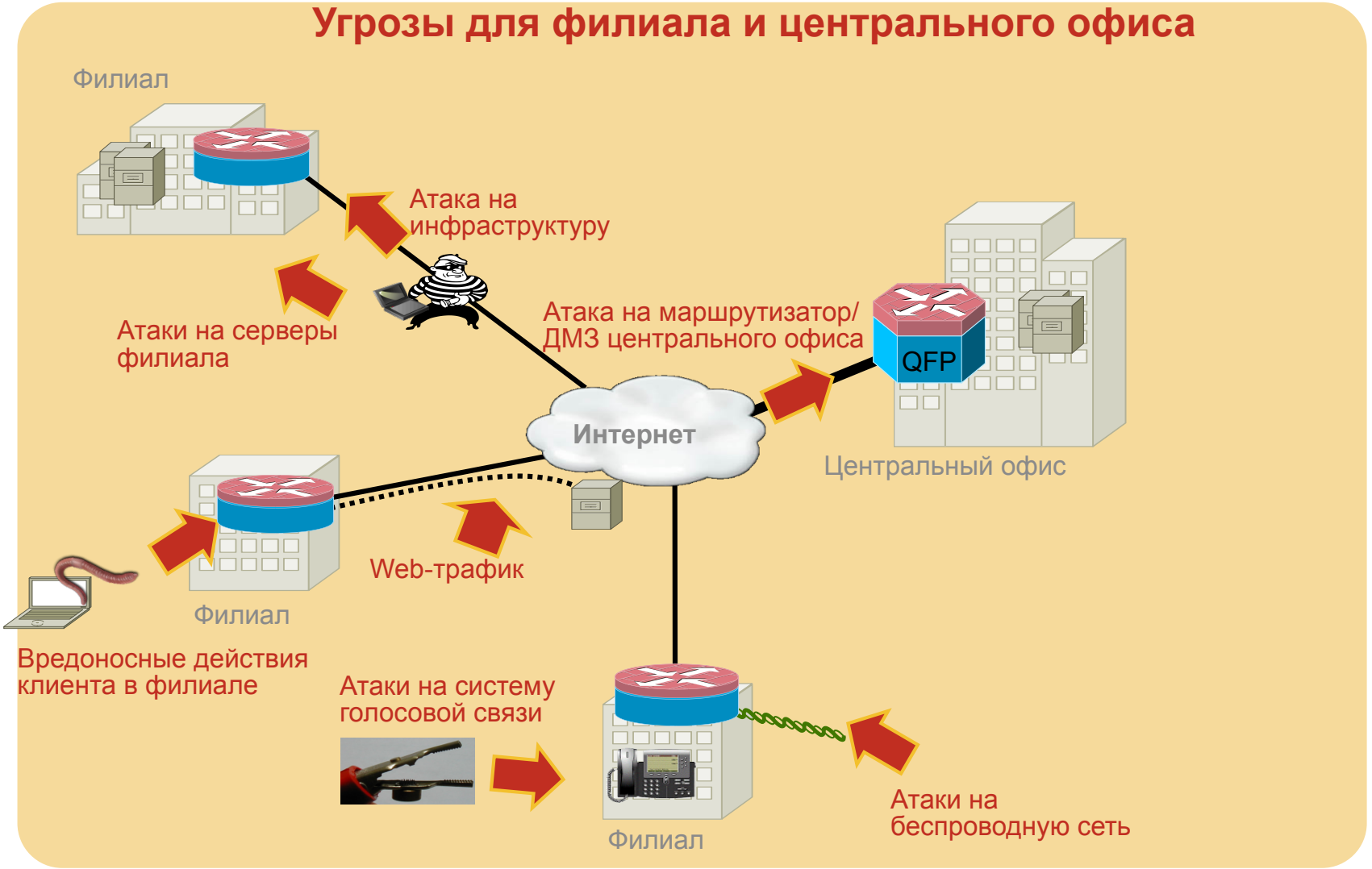
	Cisco ISR	Cisco ISR G2
Производительность	До 45 Mbps с сервисами	До 150 Mbps с сервисами
Процессор	Одноядерный	Многоядерный
DSP	Только голос	Голос + видео
Модули коммутаторов	FE+ PoE (Catalyst 3560/3750)	FE/Gig E + PoE+ (Catalyst 3560–E/2960)
Сервисные модули	1X с 160GB HDD	7x с 1TB HDD, двухядерный, RAID 0/1
Образ IOS	Множество	Единый универсальный
Приложения	Привязаны к оборудованию	Виртуальные сервисы по требованию
Отказоустойчивость	Отказоустойчивость по электроснабжению на 38xx Единая системная плата	Отказоустойчивость по электроснабжению Сменяемая системная плата
Управление энергопотреблением	EnergyWise на модулях коммутаторов	Cisco EnergyWise + контроль подачи питания на разъем/ отсек

Производительность в 5 раз выше. Цена та же

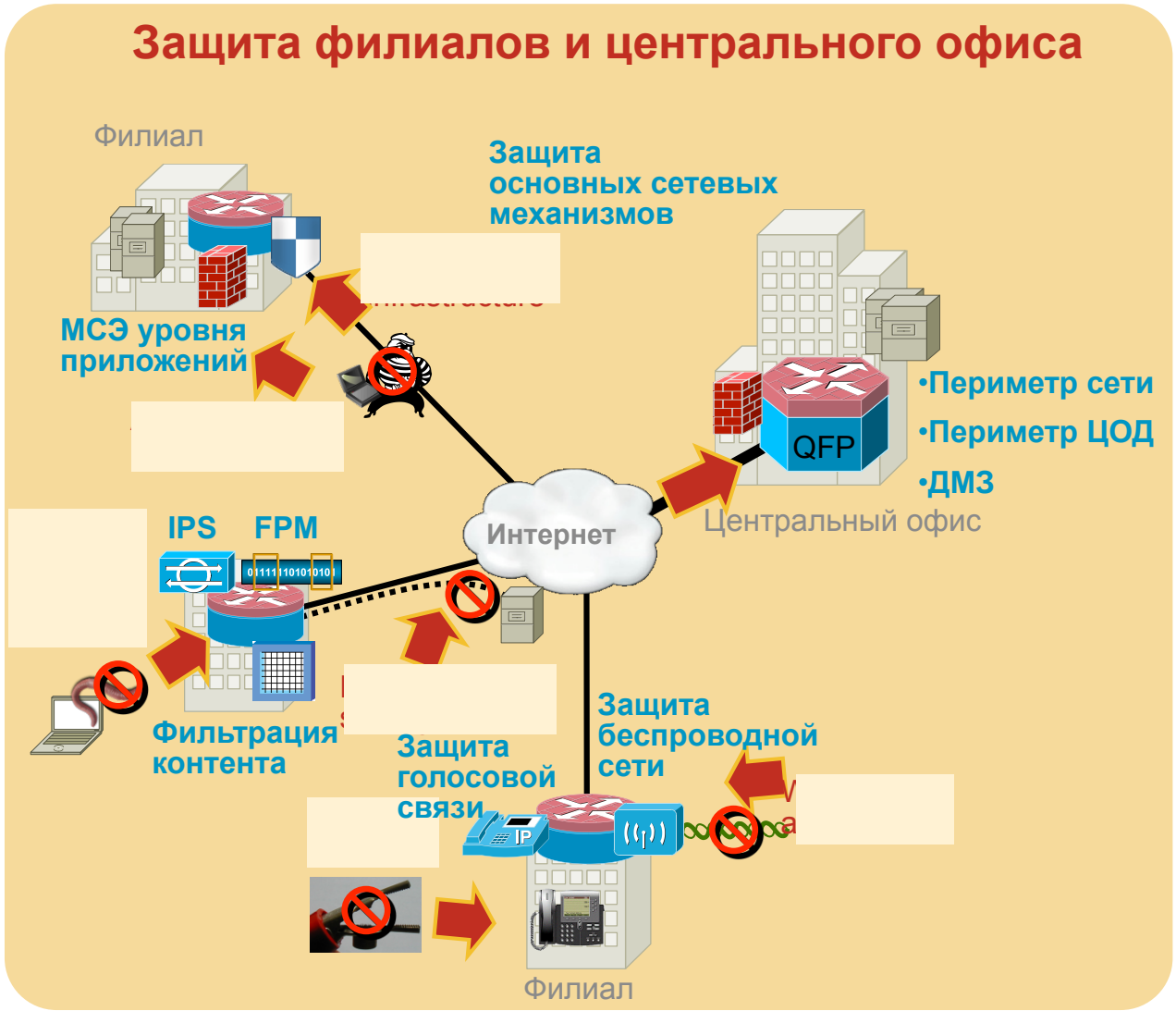
План презентации

- Маршрутизаторы с интеграцией сервисов ISR G2
- Стимулы развития интегрированных средств безопасности
- Интегрированные средства управления угрозами
- Управление и мониторинг
- Соображения по проектированию
- Модели развертывания
- Резюме

Угрозы и технические проблемы



Потребность в интегрированных средствах безопасности Средства безопасности IOS

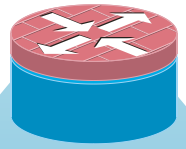


- Защищенный доступ к Интернету в филиале без установки дополнительных устройств
- Борьба с интернет-червями и вирусами прямо в сети филиала, снижение нагрузки на канал подключения к глобальной сети
- Защита маршрутизатора от взлома и атак типа "отказ в обслуживании"

План презентации

- Маршрутизаторы с интеграцией сервисов ISR G2
- Стимулы развития интегрированных средств безопасности
- Интегрированные средства управления угрозами
- Управление и мониторинг
- Соображения по проектированию
- Модели развертывания
- Резюме

Сквозное решение для защиты глобальной сети



Только маршрутизаторы Cisco® предоставляют все эти функции

Защищенные сетевые решения

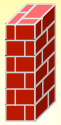

Непрерывность бизнеса

Защита голосовой связи


Защищенная мобильность


Соответствие нормативным требованиям

Интегрированные средства управления угрозами


Расширенный МСЭ


Фильтрация контента


Предотвра-щение вторжений

Средства FPM


Средства NAC


802.1x


Защита основных сетевых механизмов

Защищенные подключения


GET VPN

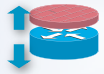

DMVPN


Easy VPN


SSL VPN

Управление и мониторинг


CCP


Ролевой доступ


NetFlow


IP SLA

Интегрированные средства управления угрозами

- МСЭ на основе политик зон Cisco IOS
- Управление логикой работы приложений Cisco IOS
- Система предотвращения вторжений Cisco IOS
- Решение для фильтрации контента Cisco IOS
- Средства гибкого анализа пакетов (FPM) Cisco IOS
- Средства защиты основных сетевых механизмов (NFP) Cisco IOS

Межсетевой экран Cisco IOS
Обзор

МСЭ с учетом состояния сеансов. Полная поддержка гибкого анализа пакетов на уровнях с 3 по 7

Гибкий встроенный шлюз уровня приложений (ALG). Модули динамического анализа протоколов и трафика приложений для реализации тонкого контроля доступа.

Средства контроля и управления работой приложений (AIC). Возможность мониторинга каналов управления и каналов передачи данных для контроля соблюдения политик безопасности приложениями.

Виртуальный МСЭ. Разделение виртуальных контекстов с возможностью использования перекрывающихся пространств IP-адресов.

Прозрачный МСЭ (уровень 2). Может развертываться в существующей сети без изменения существующей статической схемы IP-адресации.

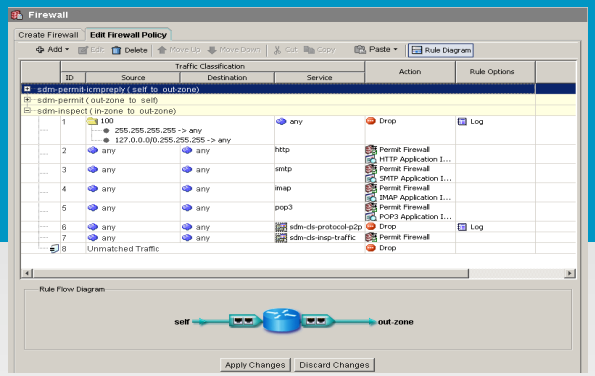
Интуитивно понятный GUI для управления. Простая настройка политик и тонкая настройка с помощью CCP и CSM.

Отказоустойчивость. Обеспечение высокой доступности для пользователей и приложений за счет поддержки аварийного переключения межсетевого экрана с сохранением состояния сеансов.

Интерфейсы. Большинство интерфейсов глобальных и локальных сетей.

Выдержка из списка поддерживаемых протоколов

- HTTP, HTTPS и JAVA
- E-mail: POP, SMTP, ESMTP, IMAP
- P2P и IM (AIM, MSN и Yahoo!)
- FTP, TFTP и Telnet
- Голос: H.323, SIP и SCCP
- СУБД: Oracle, SQL и MYSQL
- Citrix: ICA и CitrixImaClient
- Мультимедиа: Apple и RealAudio



Common Criteria

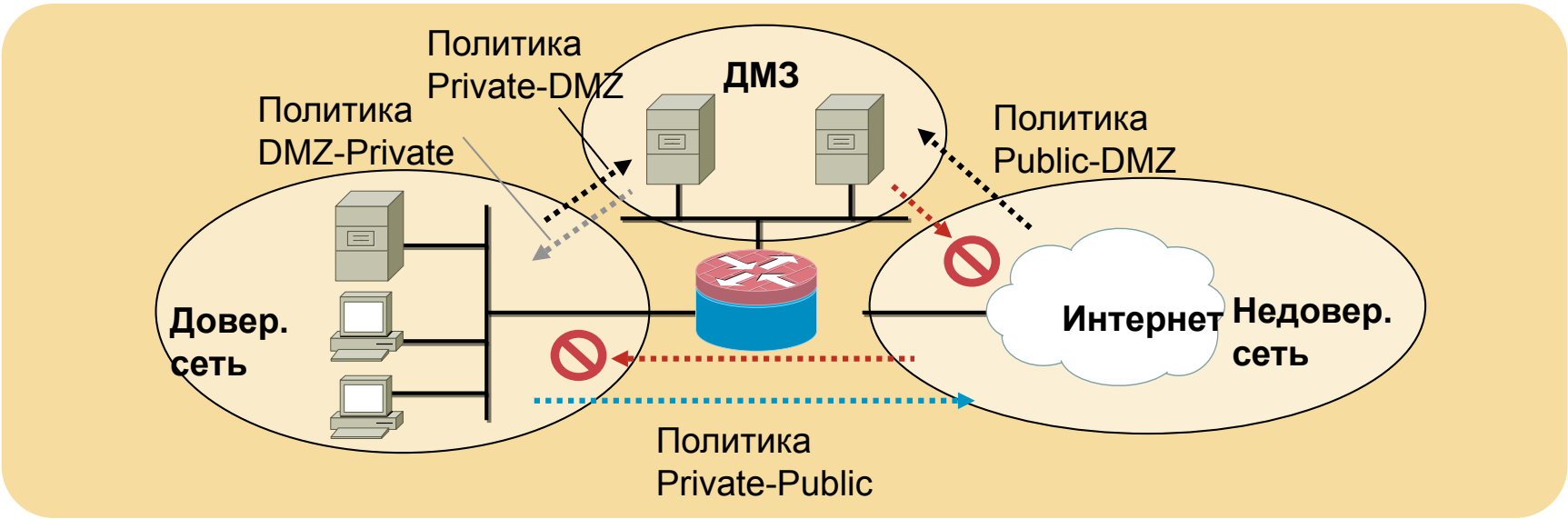
PCI Security Standards Council

МСЭ на основе политик зон Cisco IOS

- Возможность группировки физических и логических интерфейсов в зоны
- Политики МСЭ применяются к трафику, передаваемому между зонами
- Простота добавления и удаления интерфейсов, а также интеграции в политику МСЭ

Поддерживаемые функции

- Анализ с учетом состояния сеанса
- Анализ работы приложений: IM, POP, IMAP, SMTP/ESMTP, HTTP
- Фильтрация контента
- Настройка параметров политик
- Прозрачный МСЭ
- МСЭ с поддержкой VRF (виртуальный МСЭ)



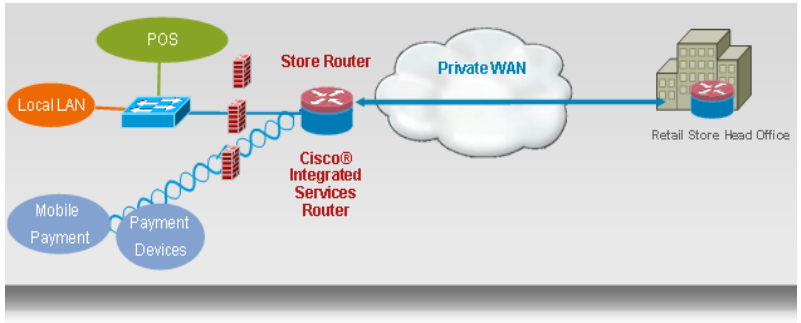
МСЭ на основе политик зон Cisco IOS Примеры использования

МСЭ филиала:

- Технология Split Tunnel — филиал/ удаленный офис/магазин
- Виртуальный МСЭ — виртуальные контексты (VRF) в рамках филиала
- Прямое подключение к Интернету – малый офис, управляемые услуги
- Внутренний МСЭ — удаленные или недоверенные объекты или сегменты, нередко для выполнения требований PCI
  - Прозрачные или маршрутизируемые среды
  - Беспроводные и проводные сегменты
  - Защита основных ресурсов (например, серверов)
  - Филиалы финансовых организаций

МСЭ центрального офиса:

•Интернет-периметр сети
•Интернет-периметр ЦОД
•ДМЗ



- PCI compliance requires retail stores to firewall wired and wireless segments

Конфигурация МСЭ на основе политик зон Cisco IOS (интерфейс командной строки)

```
class-map type inspect match-any services
 match protocol tcp
!
policy-map type inspect firewall-policy
 class type inspect services
  inspect
!
zone security private
zone security public
!
zone-pair security private-public source private destination public
 service-policy type inspect firewall-policy
!
interface fastethernet 0/0
 zone-member security private
!
interface fastethernet 0/1
 zone-member security public
```

Определение сервисов, анализируемых политикой

Настройка действия МСЭ для трафика

Определение зон

Описание пар зон, применение политики

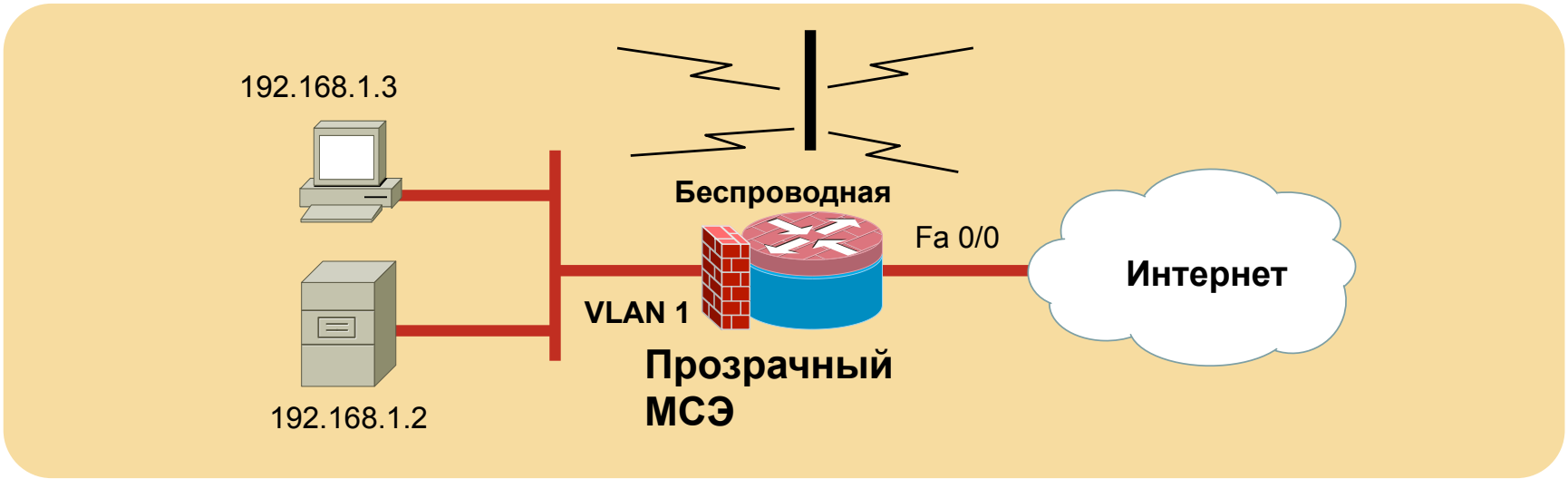
Назначение интерфейсов зонам

Прозрачный МСЭ Cisco IOS

- Возможность создания "невидимого межсетевого экрана"
  - С МСЭ не связан IP-адрес (нечего атаковать)
  - Не требуется выполнять перенумерацию или разделение IP-подсетей
  - Маршрутизатор под управлением IOS выполняет функции моста между двумя "половинами" сети

Пример использования: МСЭ между проводной и беспроводной сетями

- Проводной и беспроводной сегменты принадлежат к одной подсети 192.168.1.0/24
- VLAN 1 — защищенная "закрытая" сеть.
- Пользователям беспроводной сети не разрешается обращаться к ресурсам проводной



Конфигурация прозрачного МСЭ Cisco IOS (интерфейс командной строки)

Классификация:

```
class-map type inspect match-any protocols
        match protocol dns
        match protocol https
        match protocol icmp
        match protocol imap
        match protocol pop3
        match protocol tcp
        match protocol udp
```

Политика безопасности:

```
policy-map type inspect firewall-policy
class type inspect protocols
Inspect
```

Зоны безопасности:

```
zone security wired
zone security wireless
```

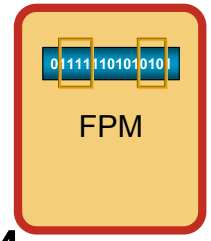
Политика зон безопасности:

```
zone-pair security zone-policy source wired
    destination wireless
service-policy type inspect firewall-policy
!
interface VLAN 1
description private interface
bridge-group 1
zone-member security wired
!
interface VLAN2
description public interface
bridge-group 1
zone-member security wireless
```

Конфигурация уровня 2:

```
bridge configuration
bridge irb
bridge 1 protocol ieee
bridge 1 route ip
```

Средства гибкого анализа пакетов (FPM) Cisco IOS



Оперативная реакция на новые и популярные атаки

- Сетевым администраторам требуются средства отражения совершенно новых атак, например, до выпуска сигнатур IPS
- Традиционные списки ACL могут оказаться слишком грубым решением, поскольку могут привести к блокированию легитимного трафика

  Пример: для борьбы с червем Slammer с помощью списков ACL необходимо заблокировать порт 1434 — что приведет к блокированию транзаций Microsoft SQL
- FPM обеспечивает гибкие средства тонкого анализа пакетов на уровнях 2–7

  Пример: порт1434 + длина пакета 404 байта + определенный шаблон данных → Slammer

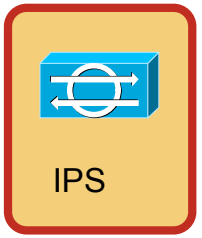
Cisco.com/go/fpm

Конфигурация FPM Cisco IOS
Фильтр для борьбы с червем Slammer

```
Class-map stack ip-udp
        Match field ip protocol eq 17 next udp

Class-map access-control slammer
        Match field udp dport eq 1434
        Match start ip version offset 224 size 4 eq 0x04011010
        Match start network-start offset 224 size 4 eq 0x04011010


Policy-map access-control udp-policy
        Class slammer
                Drop

Poliyc-map access-control fpm-policy
        Class ip-udp
        service-policy udp-policy
```

Класс access-control определяет шаблон трафика: udp-порт получателя, по смещению 224 байта от начала IP-заголовка должно находиться 4-байтовое значение 0x04041010

Система предотвращения вторжений Cisco IOS (IPS)



Распределенная система защиты от червей и вирусов

- IPS Cisco IOS блокирует атаки в самом начале их пути распространения, позволяет защитить пропускную способность каналов подключения к WAN и защищает маршрутизатор и удаленную сеть от атак типа "отказ в обслуживании"
- Интегрированное решение упрощает развертывание IPS на малых и средних предприятиях, в домашних офисах и в удаленных филиалах
- Более 2000 сигнатур, база данных совпадает с БД сигнатур сенсоров Cisco IPS
- Возможность создания пользовательских наборов сигнатур и действий для оперативной реакции на новые угрозы

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

Примеры использования IPS Cisco IOS

1 Защита ПК филиала от интернет-червей

IPS и МСЭ на маршрутизаторе Cisco позволяют защититься от интернет-червей

2 Защита от червей на периметре сети

Анализ трафика, направленного из филила в центральный офис, с помощью IPS для предотвращения распространения червей и проведения атак с зараженных ПК филиала

3 Защита серверов филиала

IPS и МСЭ на маршрутизаторе филиала позволяют защитить локальные серверы филиала от атак

Для защиты серверов не требуется отдельное устройство

4 Выполнение нормативных требований PCI

5 Прозрачная IPS (уровень 2)

Конфигурация IPS Cisco IOS (с помощью интерфейса командной строки)

Загрузите файлы IPS Cisco IOS на свой ПК

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

IOS-Sxxx-CLI.pkg

realm-cisco.pub.key.txt

Настройте ключ шифрования IPS Cisco IOS

mkdir **ipstore** (создание каталога на flash-карте)

Вставьте ключ шифрования из файла

realm-cisco.pub.key.txt

Конфигурация IPS Cisco IOS

```
ip ips config location flash:ipstore retries 1
ip ips notify SDEE
ip ips name ips-policy
ip ips signature-category
category all
retired true
category ios_ips basic
```

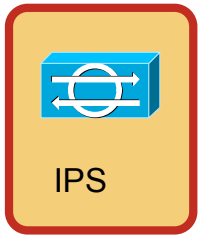
Конфигурация IPS Cisco IOS (продолжение)

```
retired false

interface fast Ethernet 0
ip ips ips-policy in
```

Загрузите сигнатуры с TFTP-сервера

```
copy tftp://192.168.10.4/IOS-S289-CLI.pkg idconf
Loading IOS-S259-CLI.pkg from 192.168.10.4 :!!!

show ip ips signature count
Total Compiled Signatures:
 338 -Total active compiled signatures
```

Удобные и масштабируемые средства управления IPS



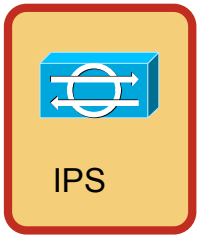
Интегрированное решение для защиты филиала

- Полный спектр вариантов управления:
  - Cisco CCP † обеспечивает полное управление и мониторинг IPS на одном маршрутизаторе
  - Cisco Security Manager 3.1† / CS-MARS для управления IPS в масштабах организации
  - Настройка с помощью интерфейсной командной строки позволяет автоматически выделять ресурсы и обновлять сигнатуры†
  - Cisco Configuration Engine для MSSP — масштабирование до тысяч устройств‡
- Согласованность процедур эксплуатации всего набора решений Cisco IPS
- Рейтинг риска и процессор действий по событию (SEAP) позволяет снизить число ложных срабатываний ‡
- Расширенная поддержка сигнатур для ОС Microsoft (MSRPC и SMB)†

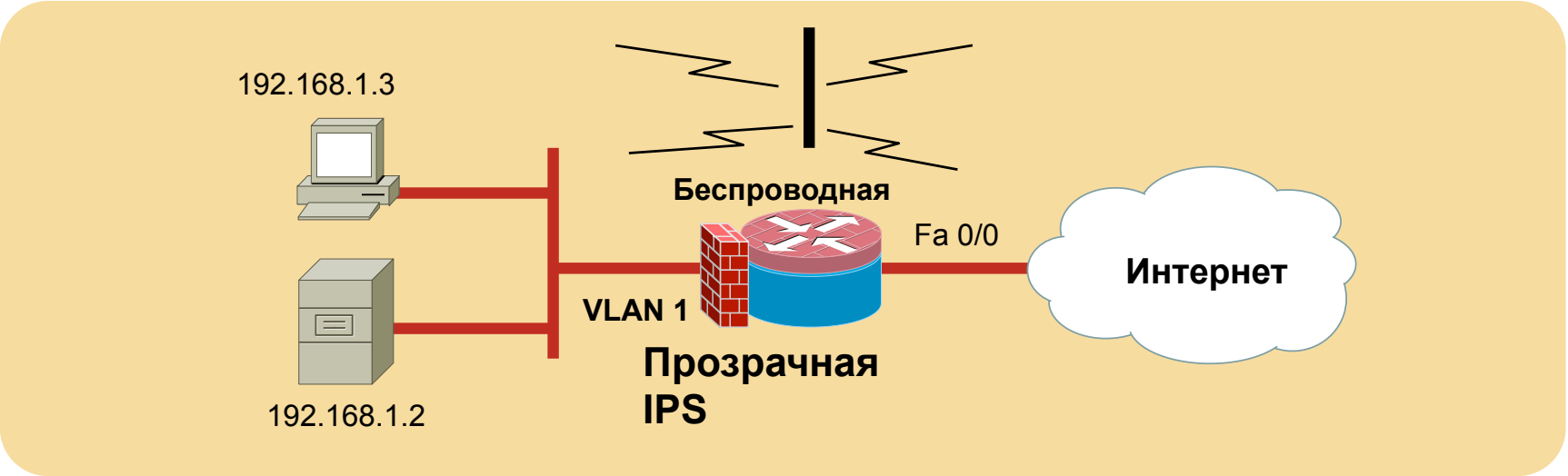
† Новая функция в Cisco IOS 12.4(15)T2
‡ Уникальное для отрасли решение

Прозрачная IPS Cisco IOS

Пример использования: IPS между беспроводным и проводным сегментом



- Возможность развертывания "невидимой IPS"
  - С IPS не связан IP-адрес (нечего атаковать)
  - Маршрутизатор под управлением IOS выполняет функции моста между двумя "половинами" сети
- Проводной и беспроводной сегменты находятся в одной подсети 192.168.1.0/24
- VLAN 1 — защищенная "частная" сеть.



Конфигурация IPS Cisco IOS (с помощью интерфейса командной строки)

Загрузите файлы IPS Cisco IOS на свой ПК

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

IOS-Sxxx-CLI.pkg

realm-cisco.pub.key.txt

Настройте ключ шифрования IPS Cisco IOS

mkdir **ips5** (создание каталога на flash-карте)

Вставьте ключ шифрования из файла

realm-cisco.pub.key.txt

Конфигурация IPS Cisco IOS

```
ip ips config location flash:ips5 retries 1
ip ips notify SDEE
ip ips name ips-policy
ip ips signature-category
category all
retired true
category ios_ips basic
retired false
```

Конфигурация IPS Cisco IOS (продолжение)

```
interface VLAN 1
description private interface
bridge-group 1
ip ips ips-policy out

interface VLAN 2
description private interface
bridge-group 1
ip ips ips-policy in
```

Загрузите сигнатуры с TFTP-сервера

```
copy tftp://192.168.10.4/IOS-S289-CLI.pkg
    idconf
Loading IOS-S259-CLI.pkg from 192.168.10.4 :!!!

show ip ips signature count
Total Compiled Signatures:
 338 -Total active compiled signatures
```

Средства Cisco IOS® для фильтрации контента

Решение для защиты web-трафика, позволяющее обеспечить защиту от известных и новых угроз при одновременном повышении эффективности работы сотрудников

- Оптимальное решение для филиала или офиса малого/среднего предприятия
- Блокировка вредоносных сайтов, обеспечение выполнения корпоративных политик
- Реализация рейтингов производительности и безопасности на основе категорий
- Нормативные требования, такие как HIPAA, FISMA, CIPA (Children's Internet Protection Act), включают развертывания надежной системы фильтрации контента
- Политика реализуется и поддерживается на маршрутизаторе локально

Архитектура сервиса фильтрации контента Cisco IOS (подписка)

Подробное описание функциональных возможностей

- **Гибкость конфигурации**

  Кэширование информации о категории URL-адреса (производительность/безопасность)

  Объем кэша по умолчанию: 300 кбайт -> ~100 URL-адресов

  После перезагрузки кэш очищается

  Время хранения информации в кэше по умолчанию – 24 часа

- **Обеспечение высокой доступности**

  Информация с сервера Trend Micro поступает на маршрутизатор с использованием DNS, что обеспечивает простоту переключения между серверами Trend Micro при выходе одного из них из строя

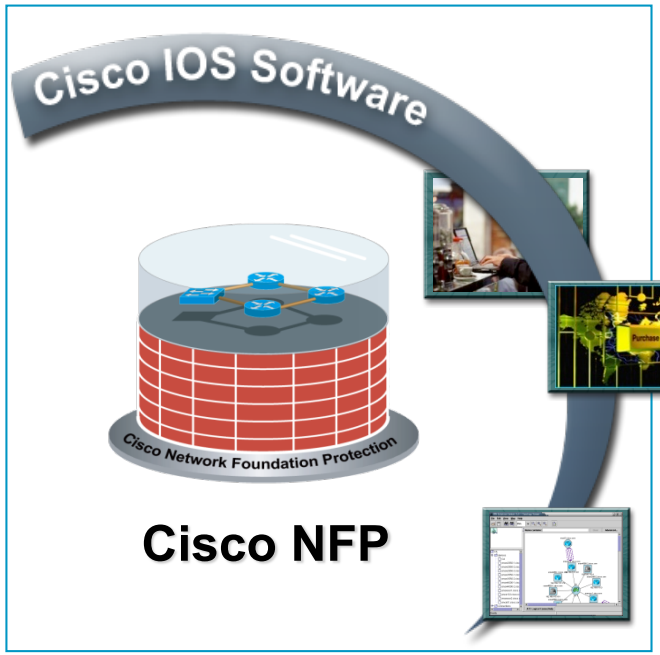
- **Простота использования**

  Trend Micro поддерживает и обновляет базы данных о безопасности и производительности, поэтому не требуется хранить на маршрутизаторе локальную базу данных

- Регистрация и настройка маршрутизатора выполняются с помощью Cisco Configuration Professional®
- Локальная фильтрация в IOS с использованием черного и белого списков
- Поддержка частичных доменных имен
- Образ IOS 12.4(15)XZ для фиксированных платформ, 12.4(20)T для модульных платформ

Повышение уровня защищенности маршрутизатора

Network Foundation Protection



Уровень данных

Возможность пересылки данных

Уровень управления маршрутизацией

Возможность маршрутизации

Уровень управления

Возможность управления

Маршрутизатор можно логически разделить на три функциональных уровня:

1. **Уровень данных.** Большинство пакетов, обрабатываемых маршрутизатором, передаются через его уровень данных.
2. **Уровень управления.** Трафик протоколов управления и других протоколов интерактивного доступа, таких как Telnet, SSH и SNMP, передается через уровень управления.
3. **Уровень управления маршрутизацией.** Протоколы управления маршрутизацией, сообщения об активности, сообщения ICMP и пакеты, которые передаются на локальный IP-адрес маршрутизатора, передаются через тот уровень.

Применяйте методологию «Разделяй и властвуй" для защиты трех уровнй

Cisco IOS AutoSecure

Network Foundation Protection

Автоматическое включение защиты

Отключение ненужных сервисов

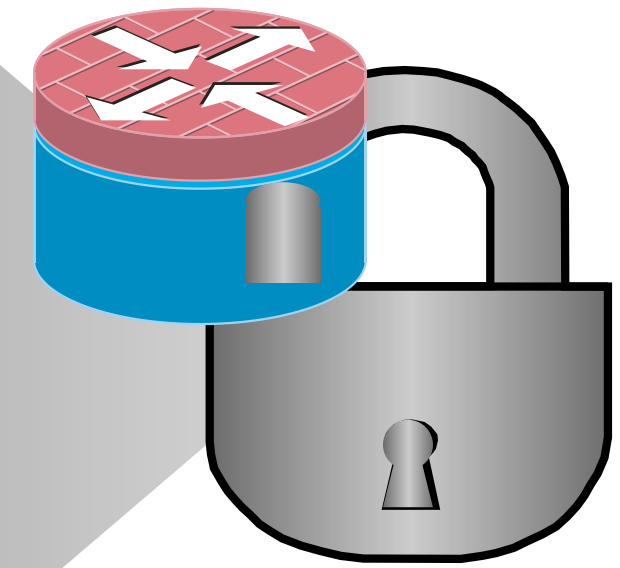
- Предотвращение DoS-атак с использованием поддельных запросов
- Отключение механизмов, которые могут содержать уязвимости

Обеспечение защищенного доступа

- Повышение уровня защиты методов доступа к устройству
- Расширенные журналы безопасности
- Не позволяет атакующему получать сведения об удаляемых пакетах

Защита уровня пересылки

- Защита от шторма SYN-запросов
- Защита от подделки адреса отправителя
- Включение МСЭ с контролем состояния сеансов на внешних интерфейсах, на которых это возможно



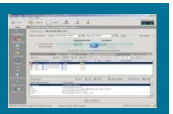
http://www.cisco.com/go/autosecure

План презентации

- Маршрутизаторы с интеграцией сервисов ISR G2
- Стимулы развития интегрированных средств безопасности
- Интегрированные средства управления угрозами
- Управление и мониторинг
- Соображения по проектированию
- Модели развертывания
- Резюме

Набор решений Cisco для управления информационной безопасностью

Cisco® Configuration Professional



Самый быстрый способ настройки

Мастера настройки МСЭ, IPS, VPN, QoS и WiFi

Поставляется с устройством

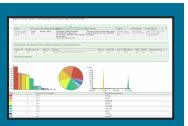
Cisco Security Manager

Новое решение для настройки маршрутизаторов, устройств, коммутаторов

Новый удобный интерфейс

Новые уровни масштабируемости

Cisco Security MARS



Решение для мониторинга и отражения атак

Для отражения атак используются средства, заложенные в ИТ-инфраструктуру

Визуализация пути атаки

МСЭ Cisco IOS на основе политик зон Таблица правил (CCP)

Firewall

Create Firewall | Edit Firewall Policy

Add | Edit | Delete | Move Up | Move Down | Cut | Copy | Paste | Rule Diagram

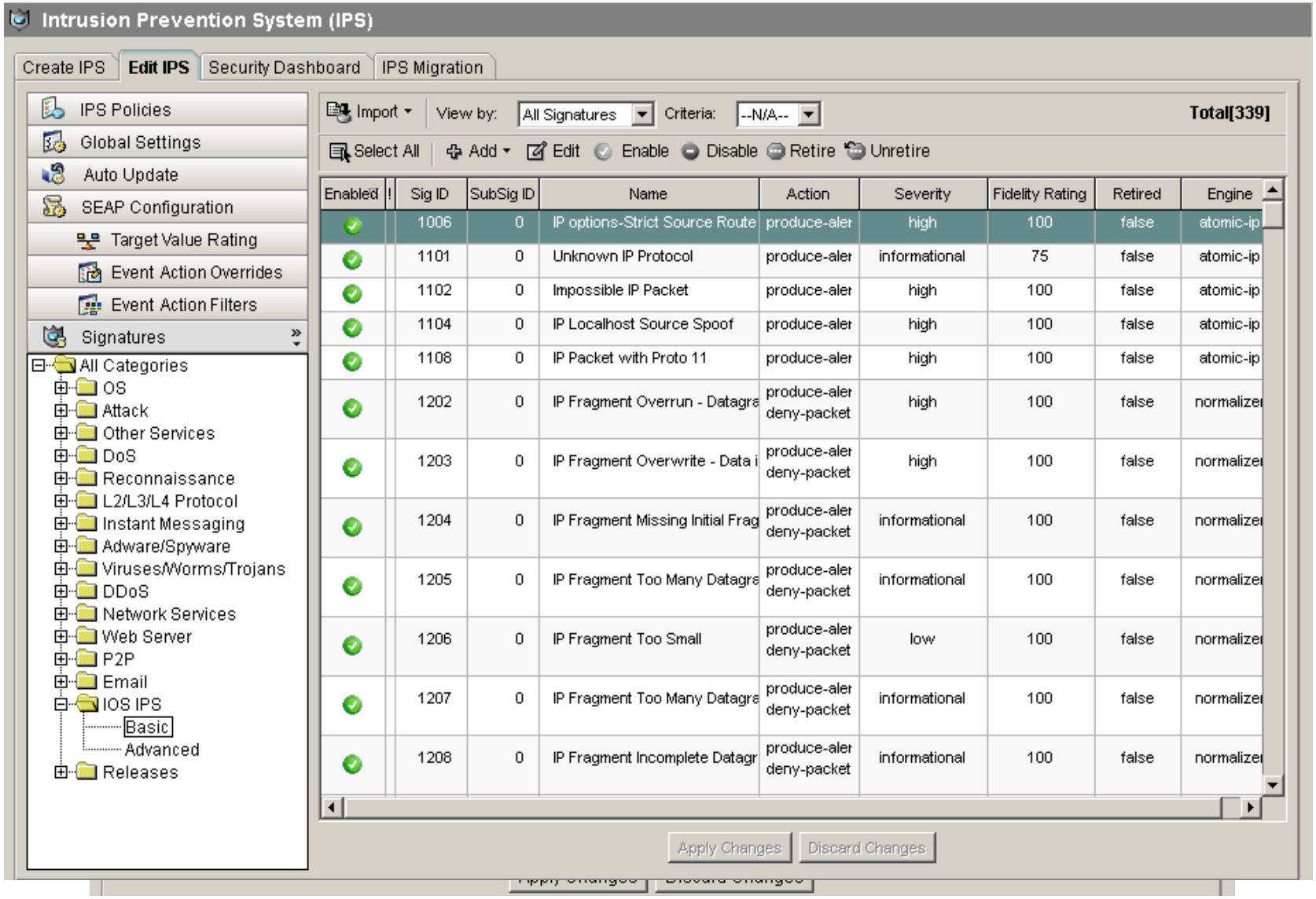
	ID	Traffic Classification: Source	Destination	Service	Action	Rule Options
sdm-permit-icmpreply (self to out-zone)						
sdm-permit (out-zone to self)						
sdm-inspect (in-zone to out-zone)						
	1	100 255.255.255.255 -> any 127.0.0.0/0.255.255.255 -> any		any	Drop	Log
	2	any	any	http	Permit Firewall HTTP Application I...	
	3	any	any	smtp	Permit Firewall SMTP Application I...	
	4	any	any	imap	Permit Firewall IMAP Application I...	
	5	any	any	pop3	Permit Firewall POP3 Application I...	
	6	any	any	sdm-cls-protocol-p2p	Drop	Log
	7	any	any	sdm-cls-insp-traffic	Permit Firewall	
	8	Unmatched Traffic			Drop	

Rule Flow Diagram

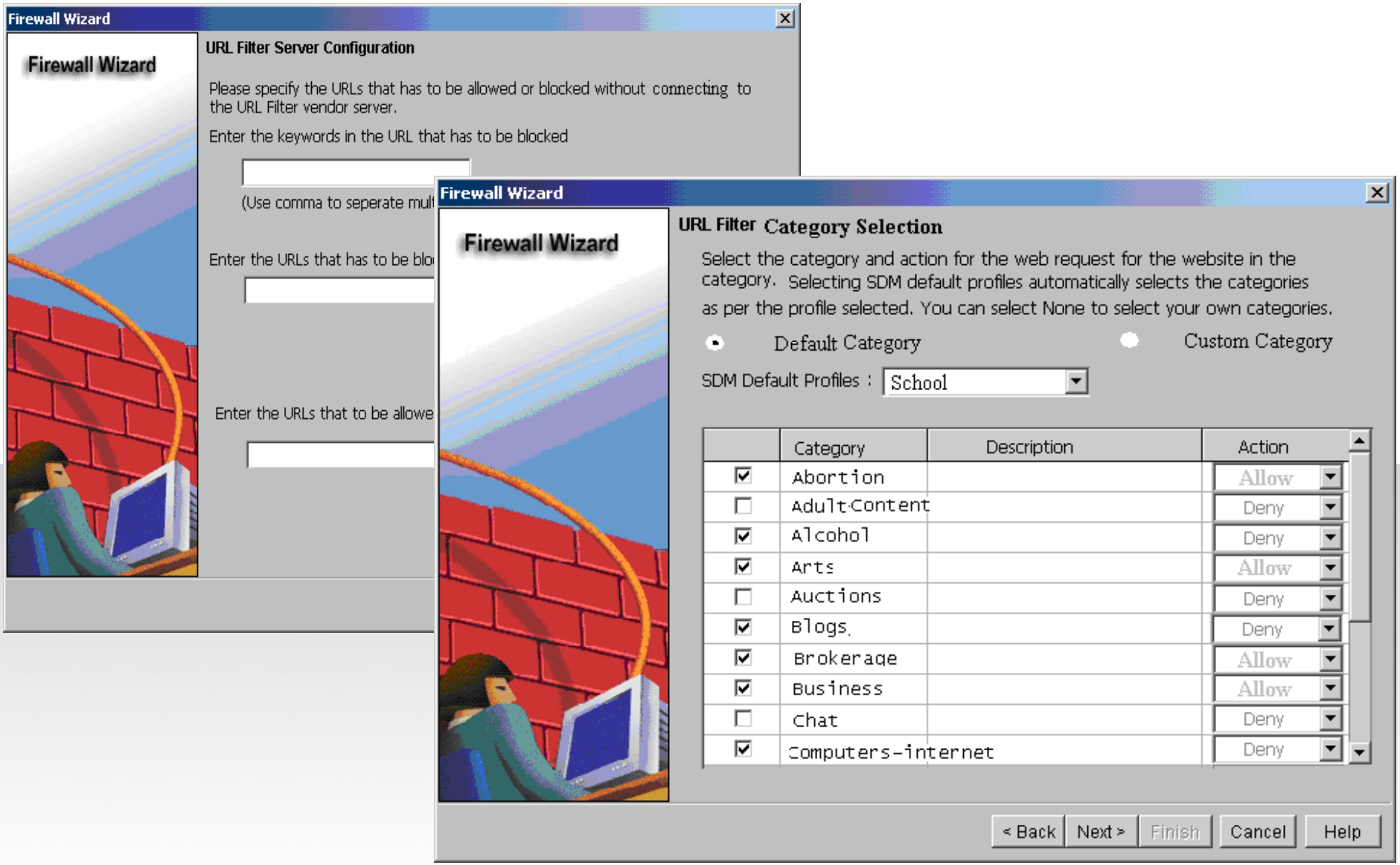
Apply Changes | Discard Changes

Конфигурация IPS Cisco IOS (CCP)

IPS

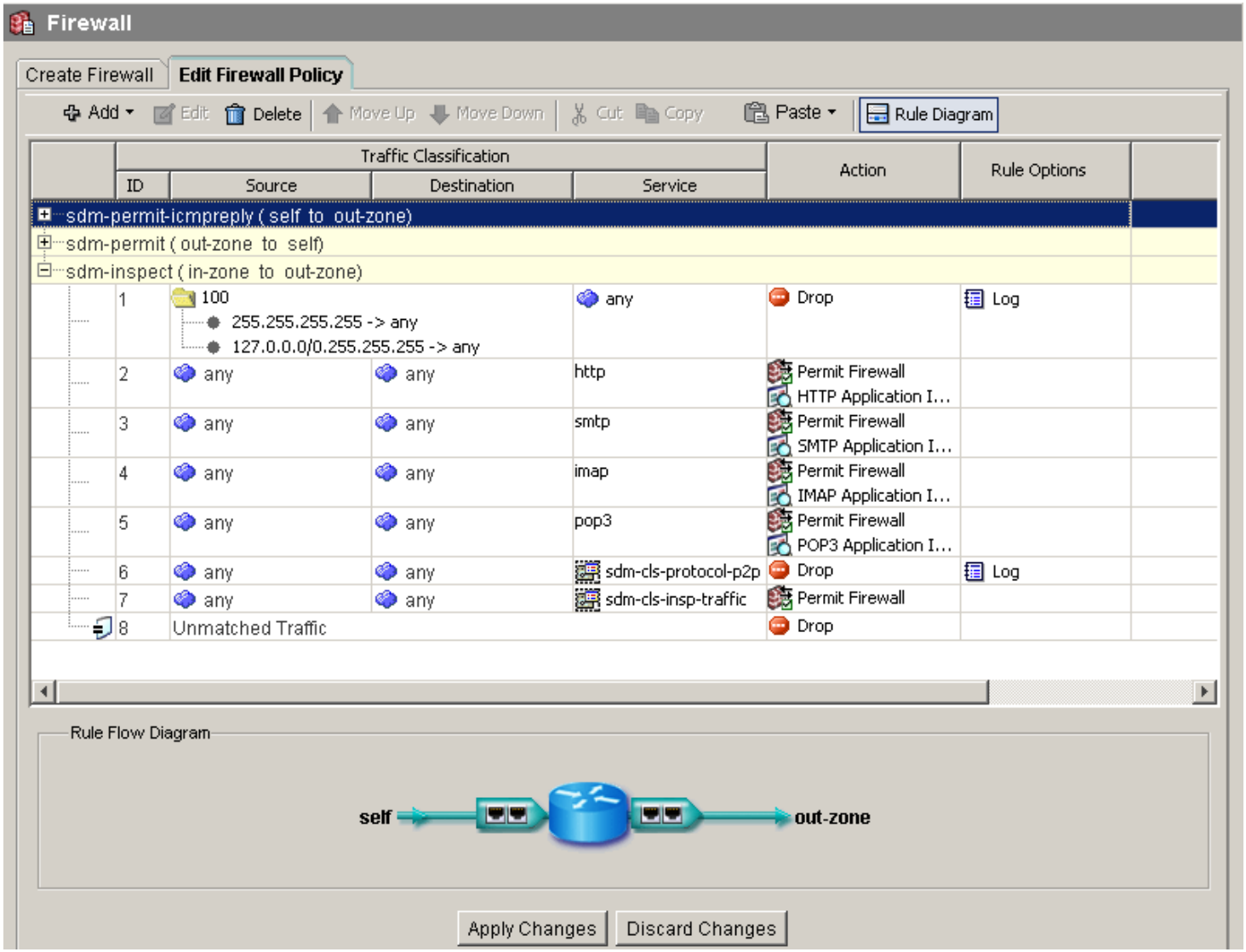


Управление средствами фильтрации контента Cisco IOS®: Cisco® Configuration Professional



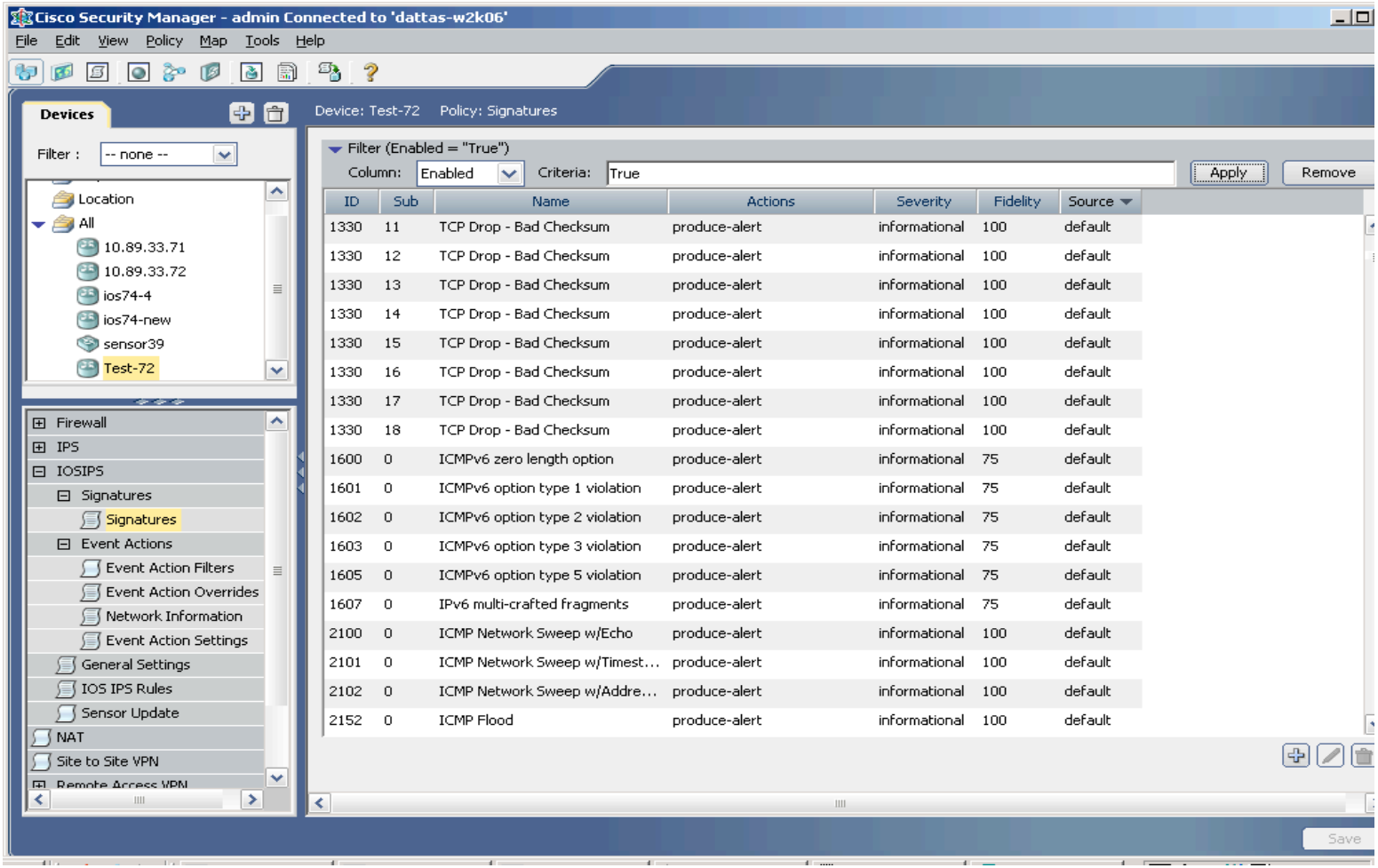
Cisco Security Manager 3.3

МСЭ Cisco IOS на основе политик зон



Cisco Security Manager 3.3

Представление списка сигнатур IPS Cisco IOS



Мониторинг

Качество системы сетевого управления не превышает качество информации, получаемой от устройств

IP Service Level Agent (IP SLA)	**Информация о производительности сети (задержка и ее колебания)**
NetFlow и NBAR	**Подробная статистика обо всех потоках данных в сети**
SNMP V3 и поддержка SNMP inform	**Надежная доставка сообщений SNMP Trap с помощью запросов SNMP inform**
Syslog Manager и syslog с поддержкой XML	**Гибкость разбора и управления сообщениями *syslog* на маршрутизаторе**
Сценарии Tcl и задания Kron (Cron)	**Гибкие средства программного управления работой маршрутизатора**
Ролевая модель доступа к CLI	**Удобные средства разграничения прав доступа (например, "сеть" и "безопасность")**
EEM	**Решение задач в сфере ИБ с помощью Embedded Event Manager**

План презентации

- Маршрутизаторы с интеграцией сервисов ISR G2
- Стимулы развития интегрированных средств безопасности
- Интегрированные средства управления угрозами
- Управление и мониторинг
- Соображения по проектированию
- Модели развертывания
- Резюме

Соображения по проектированию
МСЭ Cisco IOS

- Классический МСЭ или МСЭ на основе политик зон
  - МСЭ на основе политик зон 12.4(4)T или классический МСЭ
  - Все новые функции будут реализовываться в модели МСЭ на основе политик зон;
  - ISR G2 поддерживает только МСЭ IOS на основе политик зон с журналированием событий сетевой безопасности
- Управляемость
  - Создание политик МСЭ: Cisco Security Manager, Cisco Configuration Professional, Config Engine и CLI
  - Мониторинг работы межсетевого экрана:
    Syslog, snmp, выходные данные команды "show"
  - Изменение политик безопасности
    CCP поддерживает МСЭ на основе политик зон
- Совместимость
  - МСЭ Cisco IOS может совместно использоваться с другими средствами: NAT, VPN, IPS, WCCP/WAAS, прокси-сервер, средства фильтрации по URL и средства обеспечения QoS
- Использование памяти
  - Для обработки одного TCP- или UDP-сеанса (уровень 3/4) используется 600 байт памяти
  - Для обработки сеанса многоканального протокола используется более 600 байт памяти

Соображения по проектированию

МСЭ Cisco IOS на основе зон политик

Произошла смена парадигмы МСЭ Cisco IOS

В версии 12.4(4)T и более поздних версиях реализован МСЭ на основе политик зон

До версии 12.4(4)T и 12.4 (основная)	Версия 12.4(4)T и более поздние версии
Политики на основе интерфейсов	Политики на основе зон
Нет тонкой настройки	Очень гибкие политики МСЭ
Поддержка классического МСЭ IOS	Поддержка классического МСЭ IOS. Для классического МСЭ IOS не разрабатываются новые функции.
Нет расширенной поддержки AIC	Расширенная поддержка анализа протоколов (P2P, IM, VoIP, ...)
Классический МСЭ IOS	**Cisco IOS и IOS XE**
Поддержка в CSM и CCP	
Поддержка MIB	MIB — в планах
Поддержка IPv6	IPv6 — в планах
Поддержка аварийного переключения в режиме "активный/пассивный"	Аварийное переключение в режиме "активный/пассивный" — в планах

Соображения по проектированию

МСЭ Cisco IOS

Параметры защиты от DoS-атак	Значение по умолч.
Max-incomplete high	Неогранич.
Max-incomplete low	Неогранич.
On-minute high	Неогранич.
One-minute low	Неогранич.
Tcp max-incomplete host	Неогранич.

- Настройки защиты от атак типа "отказ в обслуживании"

  В версиях до 12.4(11)T для параметров защиты от DoS-атак по умолчанию были установлены низкие значения

  http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_white_paper0900aecd804e5098.shtml

  В версиях 12.4(11)T и IOS XE для них установлены максимальные значения

- Адресация

  Эффективность политик МСЭ существенно повышается за счет использования продуманной схемы IP-адресации

- Производительность

  Рекомендации по обеспечению производительности МСЭ Cisco IOS для маршрутизаторов Cisco ISR (800-3800)
  http://www.cisco.com/en/US/partner/products/ps5855/products_white_paper0900aecd8061536b.shtml

  Производительность анализа TCP/ICMP/UDP ASR1000 – до 20 Гбит/с при выборе наиболее популярных протоколов (SIP UDP, FTP (акт.), TFTP, DNS, H.323v2, SCCP, RTSP)

Соображения по проектированию

Функции МСЭ Cisco IOS по защите голосовой связи

Протокол	ISR	Комментарии
H.323 V1 и V2	Да	Протестировано с использованием CME 4.0
H.323 V3 и V4	Да	
H.323 RAS	Да	
H.323 T.38 Fax	Нет	
SIP UDP	Да	Поддержка CCM 4.2 RFC 2543, RFC 3261 не поддерживаются
SIP TCP	Да	
SCCP	Да	Протестировано с CCM 4.2/CME 4.0
Анализ локального SIP/SCCP-трафика	Да	

Соображения по проектированию

IPS Cisco IOS версий 4.x и 5.x

Произошла смена парадигмы IPS Cisco IOS

В версии 12.4(11)T2 и более поздних версиях поддерживается IPS 5.x

	До версии 12.4(11)T2 и 12.4 (основная)	Версия 12.4(11)T2 и более поздняя
Внутренняя версия IPS IOS (show subsys name ips)	2.xxx.xxx	3.000.000
Формат сигнатур	4.x	5.x
URL для загрузки сигнатур	http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup	http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup
Распространение сигнатур	Комплекты сигнатур Basic/ Advanced (файл SDF)	Файл сигнатур IOS-Sxxx-CLI.pkg
Загрузка сигнатур	Из одного файла SDF	Из набора конфигурационных файлов
Конфигурация сигнатур	Подход на основе одного файла SDF	Иерархический подход (несколько уровней и файлов)

Обновление сигнатур Cisco IOS IPS 4.X (12.4(9)T или более ранняя версия)

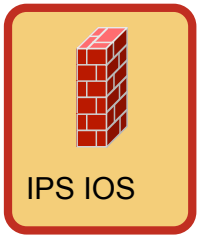
Соображения по проектированию

Миграция на IPS Cisco IOS 5.x (12.4(11)T2)

- Вариант 1. Существующий заказчик, использующий стандартные файлы сигнатур (SDF)
  - Миграция сигнатур не требуется
  - Сигнатуры, описанные в файле 128MB.sdf, — категория IOS-Basic
  - Сигнатуры, описанные в файле 256MB.sdf, — категория IOS-Advanced
- Вариант 2. Существующий заказчик, использующий доработанные файлы сигнатур (SDF)
  - На сайте Cisco.com доступен TCL-скрипт для миграции доработанных файлов SDF в формат 5.x
  - Этот скрипт не обеспечивает миграцию пользовательских сигнатур
- Руководство по миграции:
  - http://www.cisco.com/en/US/products/ps6634/products_white_paper0900aecd8057558a.shtml

Соображения по проектированию

IPS Cisco IOS — версия 12.4(11)T2 и более поздние



Управляемость

- Формирование политик IPS:

  CLI, Cisco Security Manager, CCP и Config Engine

- Настройка и обновление сигнатур:

  Категория "basic" содержит рекомендуемый Cisco набор сигнатур для маршрутизаторов со 128 Мбайт ОЗУ, категория "advanced" — для маршрутизаторов с 256 Мбайт ОЗУ

  С версии 12.4(11)T настройка сигнатур может выполняться с помощью интерфейса командной строки

  Процедура обновления соответствует процедуре обновления сигнатур для сенсоров Cisco 42xx (автообновление с помощью CSM).

- Мониторинг работы IPS:

  Формирование отчетов с помощью CS-MARS (поддержка SDEE и syslog), выходные данные команд "show"

- Изменение политик безопасности:

  CCP и CSM поддерживают IPS

Соображения по проектированию

Система предотвращения вторжений Cisco IOS

- Производительность

  Добавление сигнатур не влияет на производительность маршрутизатора.

- Использование памяти

  Процесс компиляции сигнатур создает значительную нагрузку на процессор. Число сигнатур, которое можно загрузить на маршрутизаторе, определяется объемом памяти.

- Фрагментация

  Для обнаружения атак, основанных на фрагментации, в IPS Cisco IOS используется механизм VFR (Virtual Fragmentation Reassembly).

Соображения по проектированию

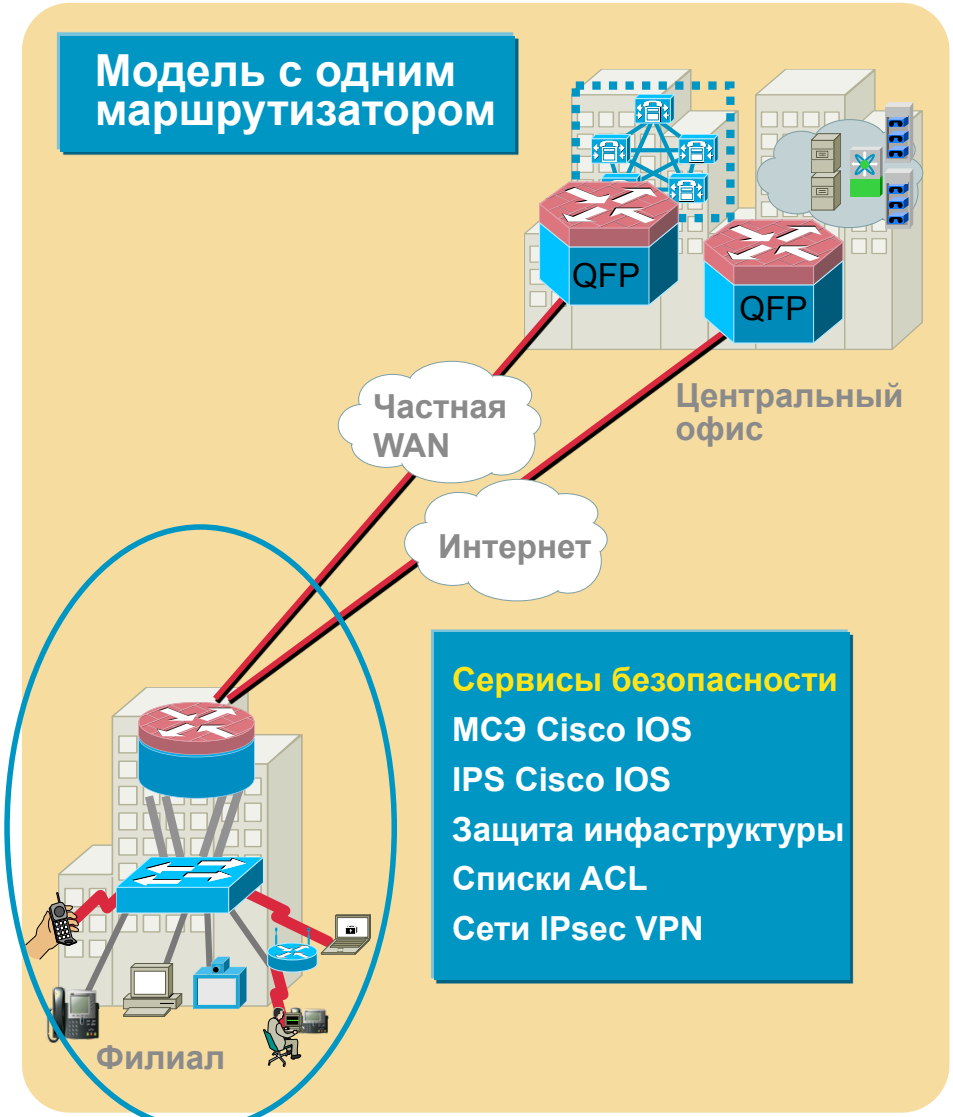
IPS IOS и устройства/модули IPS

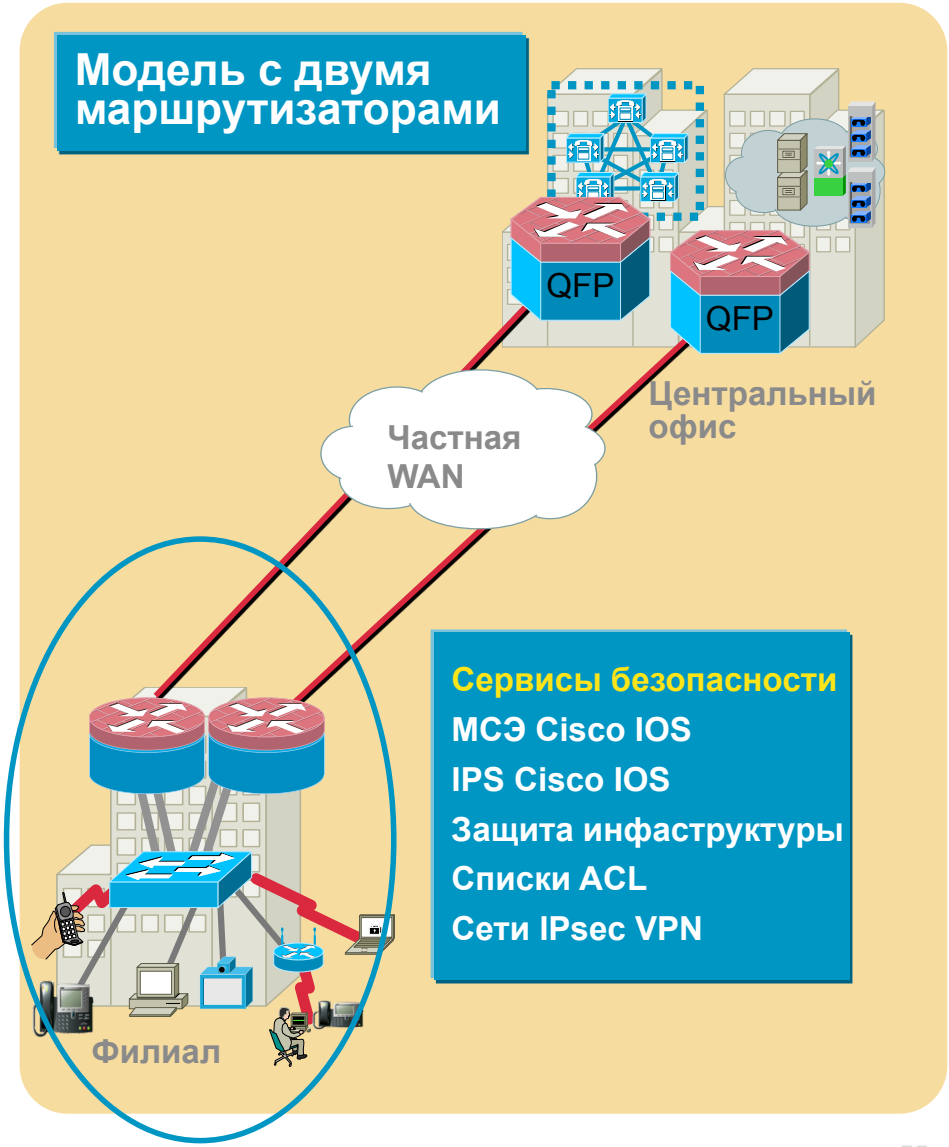
	Cisco IOS IPS Release 12.4(9)T	Cisco IOS IPS Release 12.4(11)T	Сенсоры Cisco IPS 42xx, модули IDSM2, SSM-AIP, NM-CIDS
Формат сигнатур	4.x	5.x/6.0	5.x/6.0
Обновление и настройка сигнатур	SDF	IDCONF	IDCONF
Поддерживаемые сигнатуры	*Подмножество* более чем 1700 сигнатур (зависит от модели/объема ОЗУ)		По умолчанию выбрано более 1900 сигнатур
Рекомендованные наборы сигнатур	Basic или Advanced SDF	Категория IOS-Basic или IOS-Advanced	Все сигнатуры в режиме alarm-only
Обнаружение аномалий	Нет		В версии 6.0
Прозрачная IPS (L2)	Да		Да
Ограничение скорости передачи	Нет		Да
Обнаружение в IPv6	Нет		Да
Настройка действий по событию сигнатуры	Нет	Да	Да
Мета-сигнатуры	Нет		Да
Ядра анализа голосового трафика, сканирования и шторма запросов	Нет		Да (H.225 для голоса)
Уведомления о событиях	Syslog и SDEE		SDEE

План презентации

- Маршрутизаторы с интеграцией сервисов ISR G2
- Стимулы развития интегрированных средств безопасности
- Интегрированные средства управления угрозами
- Управление и мониторинг
- Соображения по проектированию
- Модели развертывания
- Резюме

Профили филиала и центрального офиса





План презентации

- Маршрутизаторы с интеграцией сервисов ISR G2
- Стимулы развития интегрированных средств безопасности
- Интегрированные средства управления угрозами
- Управление и мониторинг
- Соображения по проектированию
- Модели развертывания
- Резюме

Резюме

- ЗАЩИЩАЙТЕ МАРШРУТИЗАТОР – вашу первую линию обороны
- ОДНО НАРУШЕНИЕ БЕЗОПАСНОСТИ может серьезно повредить бизнесу
- СОБЛЮДАЙТЕ нормативные требования по защите данных и сети
- Обеспечьте БЕЗОПАСНУЮ консолидацию голоса/видео/данных и проводной/беспроводной сетей
- Единое решение (маршрутизатор/VPN/МСЭ/IPS/ фильтрация контента) ЛЕГКО в управлении
- СОКРАТИТЕ ЗАТРАТЫ на поддержку и обслуживание: единый контракт
- Полный набор средств безопасности для подключения к WAN

Такие средства обеспечения безопасности реализованы только на маршрутизаторах Cisco®

Ваши вопросы?

Security-request@cisco.com