Системы управления сетевыми политиками безопасности

Владимир Илибман

Технический консультант

 © 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

О чем будем говорить

- Задачи управления и мониторинга ИБ в сети
- Обзор решений для управления политиками сетевой безопасностью
  - Управление отдельными устройствами
  - Cisco Security Manager
  - Cisco Network Compliance Manager
- Практические сценарии совместного использования систем управления сетевым департаментом и службой ИБ

 © 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Задачи управления и мониторинга ИБ в сети

© 2010 Cisco Systems, Inc. All rights reserved.

Информационная безопасность как процесс

Сетевая политика безопасности – набор правил или параметров, которые определяют различные аспекты конфигурации безопасности сетевых устройств

2) Защита ресурсов
МСЭ, шифрование, аутентификация, аудит

5) Управление и улучшение
Разбор полетов, анализ инцидентов, модификация планов/процедур

3) Мониторинг и реагирование
Обнаружение атак, работа с инцидентами

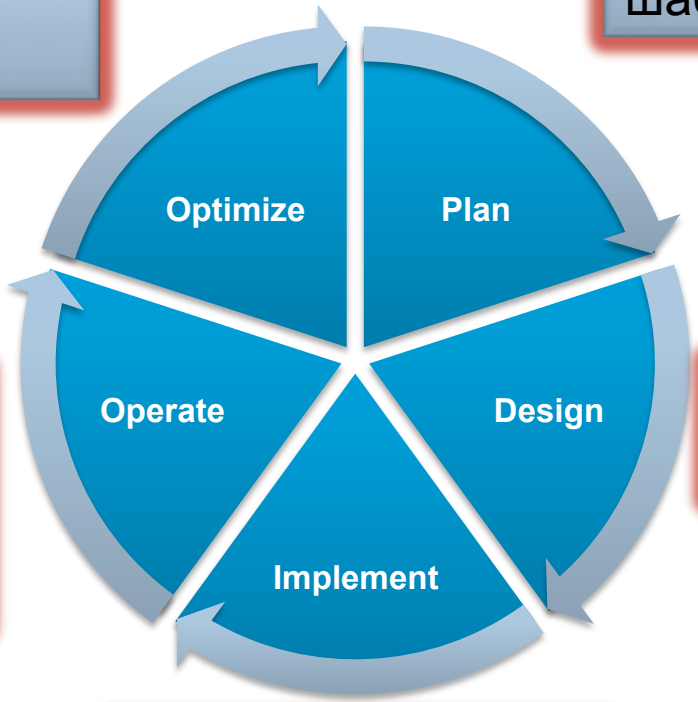
4) Тестирование, практика, обучение
Сканирование уязвимостей

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

Жизненный цикл политики сетевой безопасности

Оптимизация, “стратегические” правки

Планирование задач, принципов, процедур, шаблонов



Сбор событий и инцидентов, “тактические” правки

Разработка политик

Внедрение на сетевых устройствах

© 2010 Cisco Systems, Inc. All rights reserved.

Сложность управления политиками

Управление
Как быстро внедрять новые политики, стандарты конф.

Совместимость
Как управлять много-вендорными сетями

Центры обработки данных

Надомные работники

Разделение полномочий
Как подружить Security & Network team

Интеграция
Как совместно использовать разные механизмы управления

Мобильные пользователи

Удаленные офисы

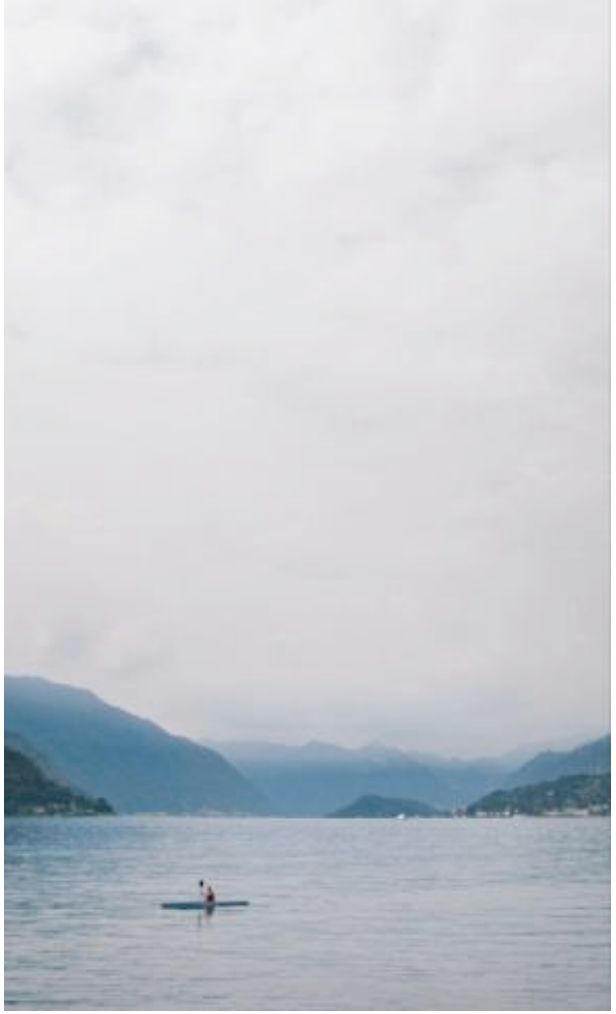
Управление ПО и конфигурациями
Образы, инвентаризация, патчи…

“Груз прошлого”
Исторически сложившиеся конфигурации

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

Когда внедрение систем управления становится актуальным?

1. Увеличение размеров сети
   - Унификация используемых решений
2. Повышение уровня информационной безопасности
   - Контроль действий администраторов ИБ и сетевых администраторов
   - Своевременное информирование о проблемах с ПО и конфигурацией
3. Нормативные документы
   - Контроль выполнения требований



Результаты аудита сетей:

- 47% изменений не учтены
- 60% простоев связаны с человеческими ошибками

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

Управление отдельными элементами сети
Element Management

© 2010 Cisco Systems, Inc. All rights reserved.

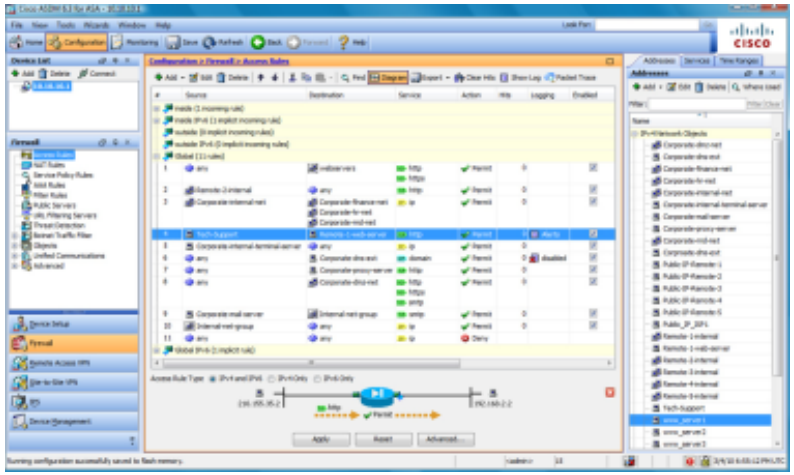
Управление индивиуальными устройствами

- CLI (Console, SSH, Telnet, Embedded Event Management)
- XML-интерфейс - Web Services Management Agent (WSMA)
- CCP – Cisco Configuration Professional
  http://www.cisco.com/en/US/products/ps9422/index.html
- ASDM – Adaptive Security Device Manager
  http://www.cisco.com/en/US/products/ps6121/index.html
- IDM – IPS Device Manager Express
  http://www.cisco.com/en/US/products/ps9610/index.html

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

Device Managers

- Преимущество
  - GUI утилиты
  - Используются для element management и мониторинга
  - Бесплатны!
- Недостатки
  - Сколько устройств, столько раз и настраивать
  - Настроил в одном месте, забыл в другом
  - В каждом случае настраивать с разными параметрами
  - Контроль действий администратора



© 2010 Cisco Systems, Inc. All rights reserved.

Управление сетью и безопасностью
Network & Security Management System

© 2010 Cisco Systems, Inc. All rights reserved.

Cisco Security Manager (CSM)

Основные возможности

- Управление политиками безопасности
- Поддержка PIX/ASA, FWSM, VPNSM, VPN SPA, IDSM, IPS
- Настройка параметров интерфейсов, туннелей, QoS, VPN
- Отображение карты сети
- Контроль производительности
- Мастеры настроек
- Транзакции

Когда нужно

Необходимость управления сетью через графический интерфейс

Настройка VPN, отображение сети

Управление политиками безопасности на оборудовании

Преимущества

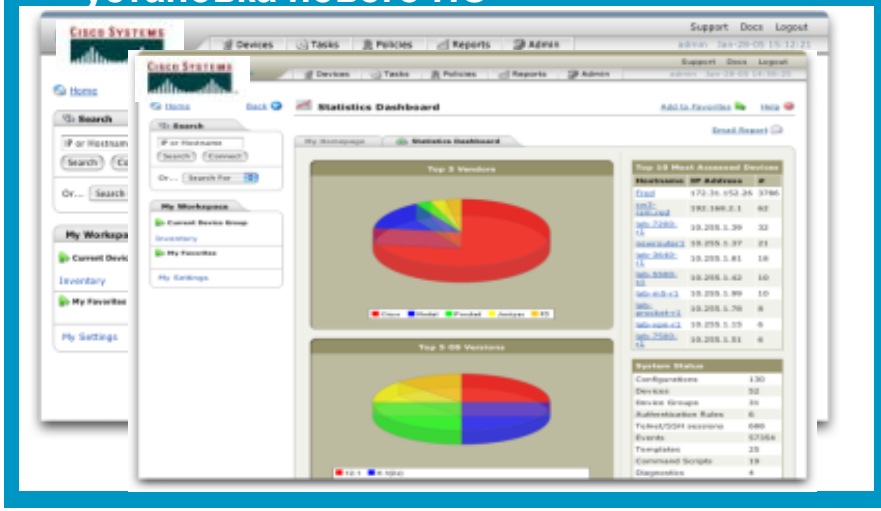
- Управление на основе стандартов
- Уменьшение количества ошибок
- Управление всеми политиками безопасности из одной системы с контролем доступа

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

CiscoWorks Network Compliance Manager (NCM)

Основные возможности

- Работает с оборудованием около 30 производителей
- Аудит корректности настроек сетевого оборудования, аудит ошибок ПО
- Отчетность по соответствию конфигурации оборудования рекомендациям и стандартам (SOX, VISA CISP, ITIL, CobiT, COSO, и др.)
- Резервное копирование и восстановление конфигураций, установка нового ПО



Когда нужно

Необходимость выполнения различных регуляторных требований (SOX, ITIL, …)

Контроль администраторов оборудования на предмет некорректных действий

Нехватка знаний/ресурсов для аудита сети и контроля изменений

Преимущества

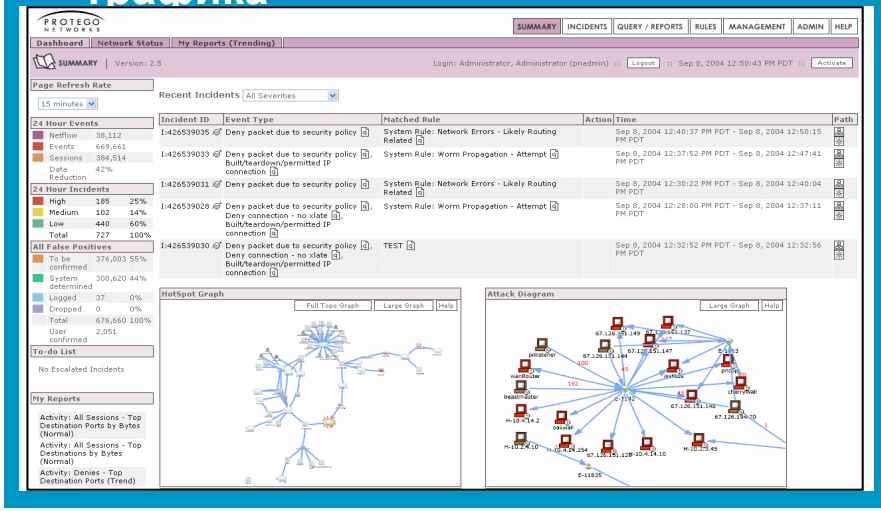
- Внедрение процесса управления изменениями– полный контроль работ на сетевом оборудовании
- Повышение безопасности сети
- Предотвращение возможных отказов оборудования – лучше, чем решение проблемы.
- Выполнение требований SOX, ITIL …
- Готовность к внешним аудитам

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

Monitoring, Analysis and Response System (MARS)

Основные возможности

- Сбор событий и их хранение
- Корреляционный анализ данных
- Быстрое обнаружение инцидентов , их изоляция и противодействие
- Привязка к топологии
- Визуализация инцидента
- Анализ профилей сетевого трафика



Когда нужно

Большое кол-во событий

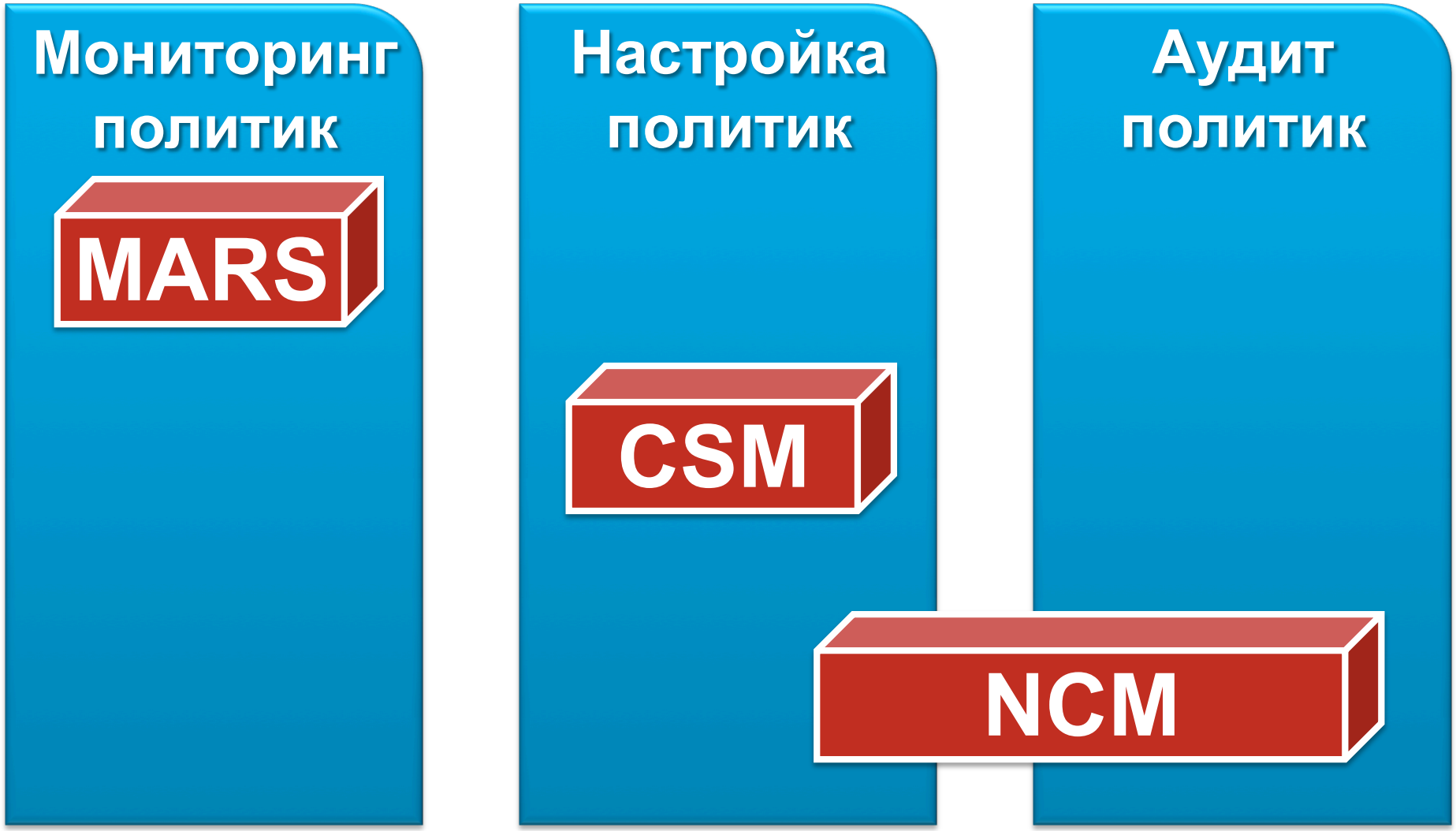
Инциденты и расследования

Преимущества

- Снижение нагрузки на администраторов
- Уменьшение времени реакции
- Единая консоль для устройств Cisco

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

Позиционирование CSM, NCM, MARS



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

Cisco Security Manager 4.0

- Время выхода: Q2 CY2010
- Новая функциональность: прием событий от ASA и IPS, поиск, фильтрация, сопоставление с правилами политики
- Подробности

  http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/data_sheet_c78-584863.html

  http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5739/ps6498/product_bulletin_c25-586395.html

© 2010 Cisco Systems, Inc. All rights reserved.

Позиционирование CSM, NCM, MARS

© 2010 Cisco Systems, Inc. All rights reserved.

Cisco Security Manager

CSM

© 2010 Cisco Systems, Inc. All rights reserved.

Что умеет делать CSM ?

- Масштабируемость от десятков до тысяч устройств
- Единая политика на всех устройствах
- Ролевой доступ
- Рабочий процесс (workflow)
- Контролирование, кто, и что можно делать на устройствах
- Абстрагировать политики от способов реализации правил на различных платформах

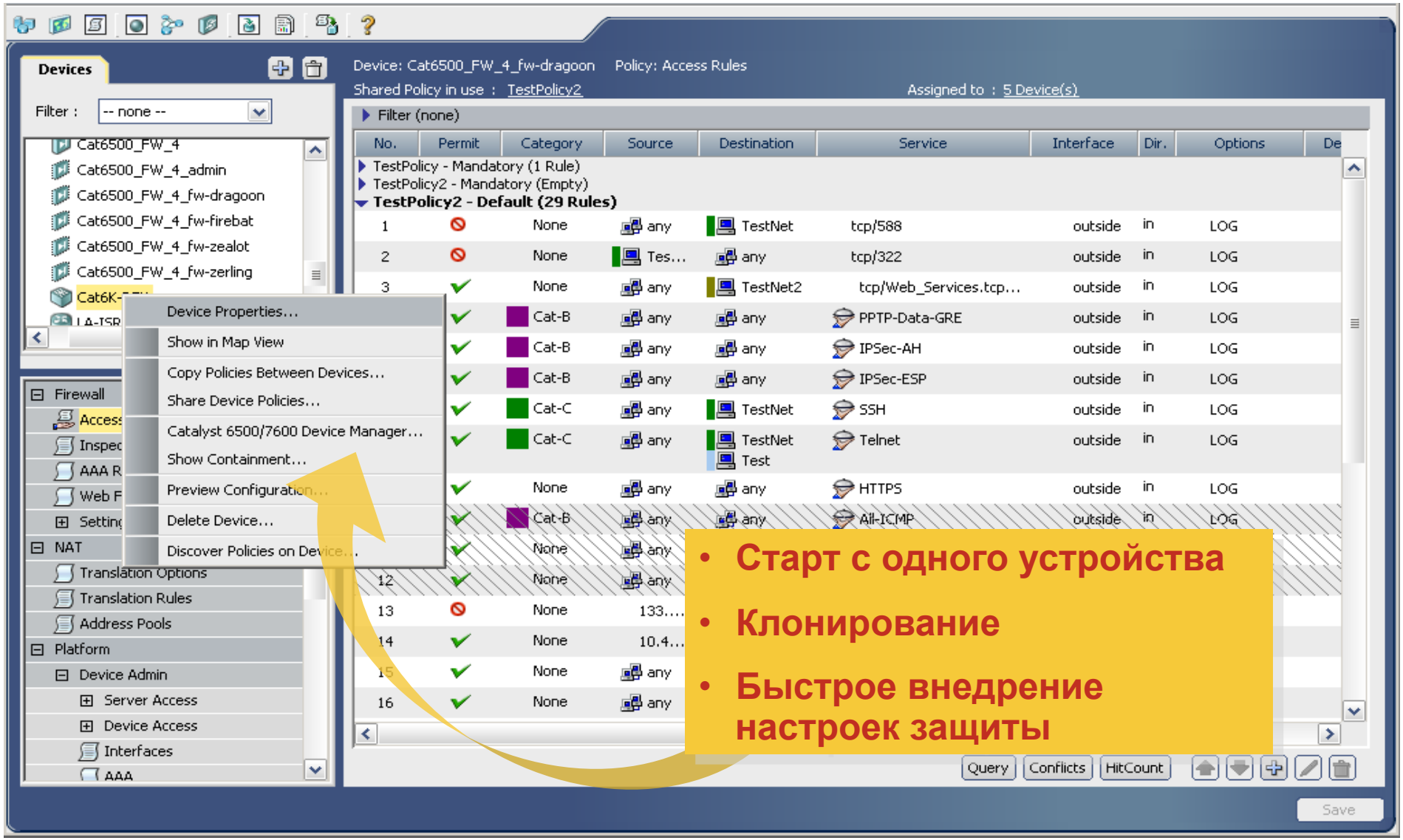
© 2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Управление сетью

- Удобный и гибкий в настройке интерфейс управления
- Различные отображения для решения различных целей
  - Device View
  - Topology View
  - Policy View
- Унифицированное управление всеми средствами защиты , как абстрактным устройством
  - Firewall, VPN, IPS…
- Поддержка ASA, PIX, IPS Sensors, ISR, C6k и Catalyst Service modules

© 2010 Cisco Systems, Inc. All rights reserved.

Просмотр с точки зрения устройства



- Старт с одного устройства
- Клонирование
- Быстрое внедрение настроек защиты

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

Просмотр с точки зрения политики

Policy Types
Firewall
Access Rules
Inspection Rules
AAA Rules
Web Filter Rules (PIX/FWSM
Web Filter Rules (IOS)
Transparent Rules
Settings
NAT (PIX)

Filter : -- none --

TestPolicy
TestPolicy2
East-Region
West-Region
CorporatePolicy
EngineeringPolicy
Manufactu
DataCent

Save Policy As...
Rename Policy...
Edit Policy Inheritance...
New Access Rules Policy...
Delete Policy...

Policy Type: Access Rules Policy: EngineeringPolicy

Details Assignments

Filter (none)

No.	Permit	Category	Source	Destination	Service	Interface	Dir.	Options	Description
CorporatePolicy - Mandatory (2 Rules)									
1	⊘	Cat-E	any	any	Telnet	All-Int...	in	LOG	
2	✓	Cat-E	any	any	HTTP HTTPS ICMP-Echo ...	All-Int...	in	LOG	
EngineeringPolicy - Mandatory (2 Rules)									
1	⊘	Cat-B	any	Engine...	FTP	All-Int...	in	LOG	
2	✓	Cat-B	any	any	NetMeeting	All-Int...	in	LOG	
EngineeringPolicy - Default (1 Rule)									
1	✓	Cat-C	any						
CorporatePolicy - Default (Empty)									

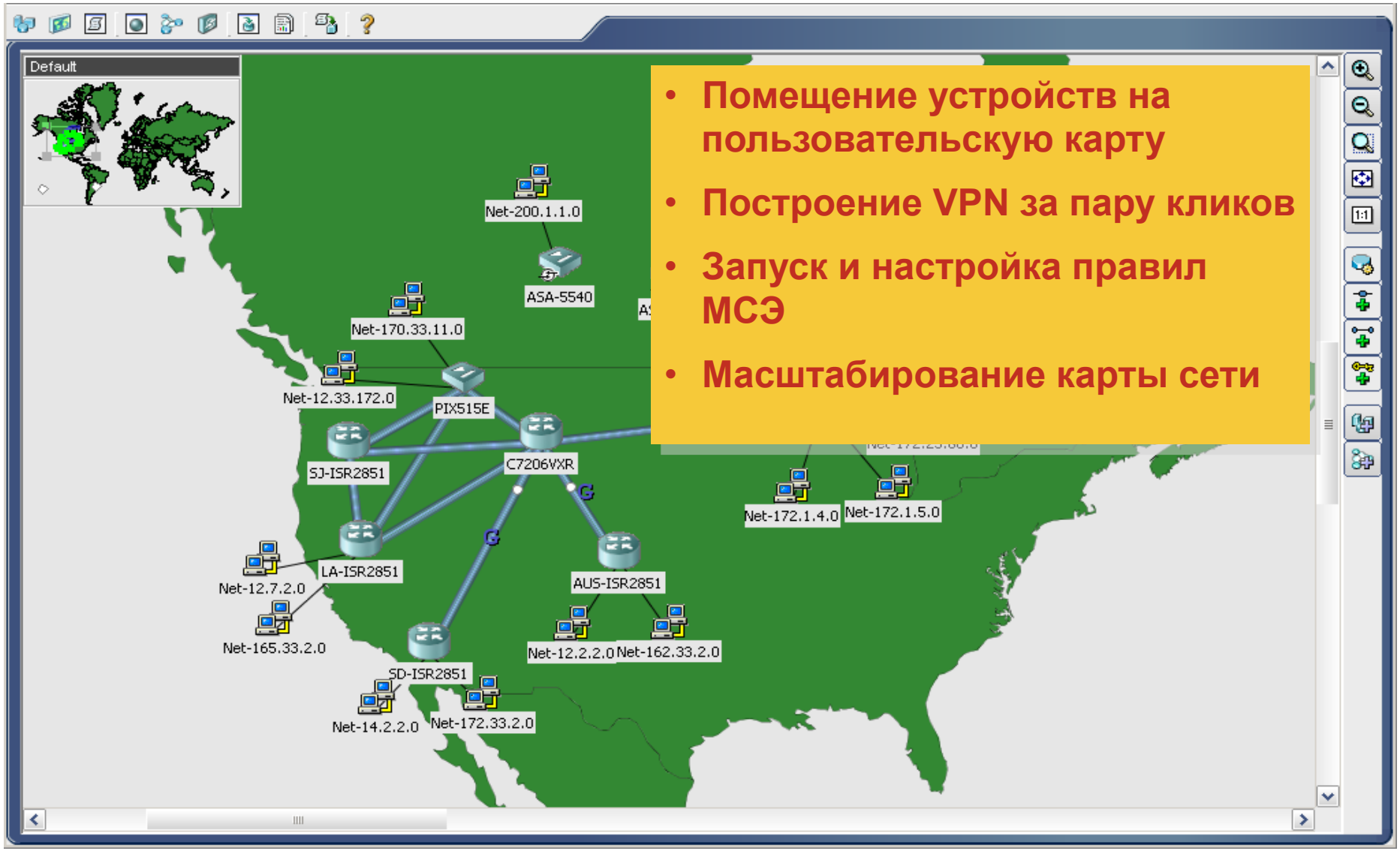
Query Conflicts HitCount

Save

- **Централизованное управление политикой**
- **Наследование, распределение, контроль непротиворечивости**

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

Просмотр с точки зрения топологии



- Помещение устройств на пользовательскую карту
- Построение VPN за пару кликов
- Запуск и настройка правил МСЭ
- Масштабирование карты сети

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

Лучшие методики

Совместное использование общих политик

Требования

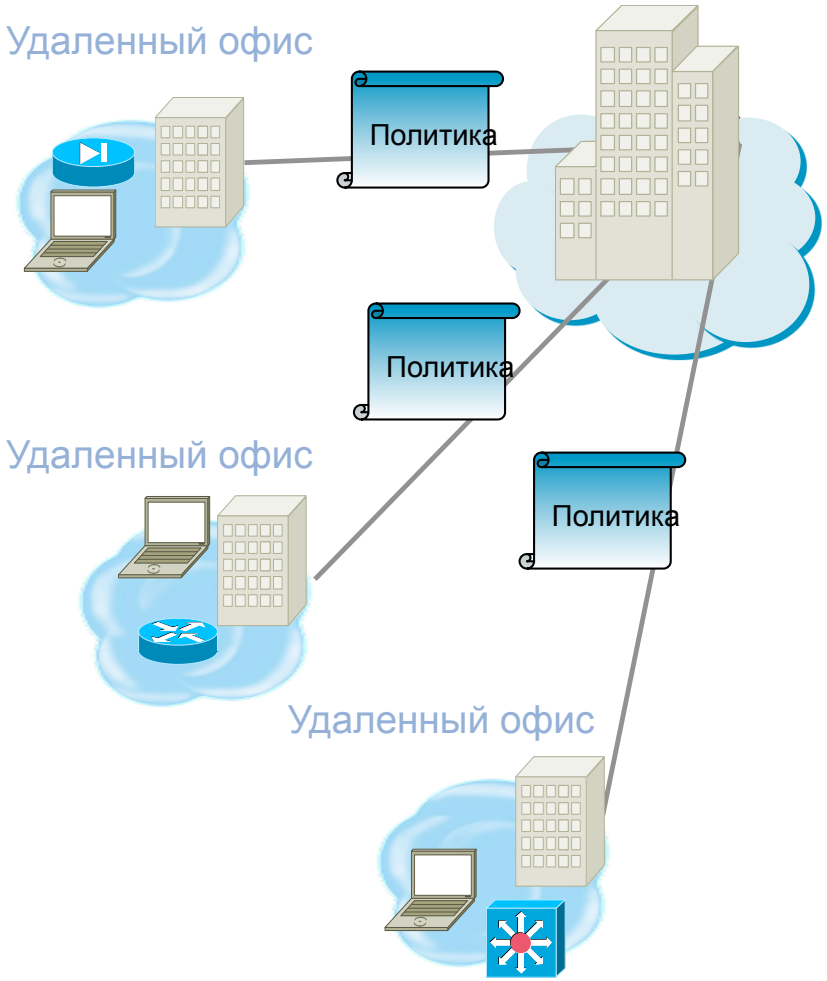
- Совместное использование политик на разных платформах
- Уточнение на уровне удаленных офисов

Примеры

- Для удаленных офисов 90% правил идентичны
- Различия минимальны
- Унификация правил
- Возможность переопределить правила на уровне удаленного офиса

Преимущества

- Поддержка одной последовательной политики приводит к упрощению
- Упрощение и ускорение внесений изменений



© 2010 Cisco Systems, Inc. All rights reserved.

Лучшие методики

Иерархичные политики и наследование

Требования

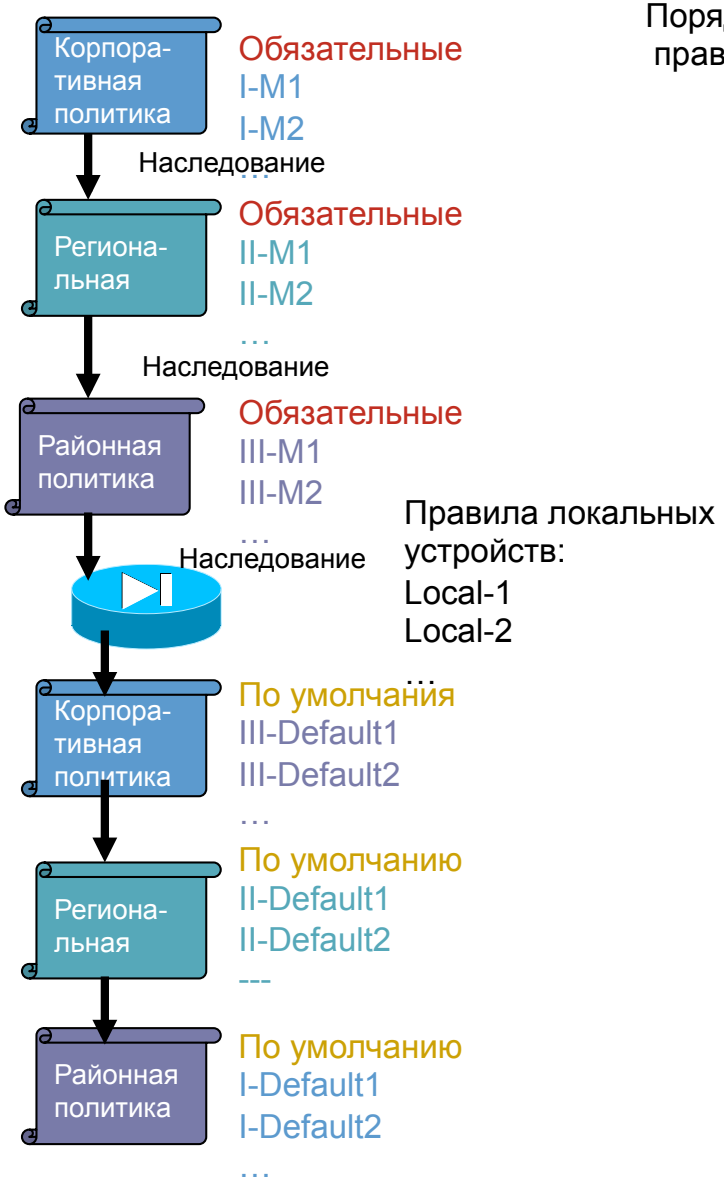
- Возможность создание обязательных и наследуемых политик
- Возможность по внесению исключений

Примеры

- Запретить IM file transfer
- Разрешить SSH, SSL

Преимущества

- Контроль организационного уровня
- Интеграция разрозненных политик
- Уменьшения вероятности ошибок



Порядок применяемых правил на устройстве:

I-Manditory1
I-Manditory2
…

II-Manditory1
II-Manditory2
…

III-Manditory1
III-Manditory2
…

Local-1
Local-2
…

III-Default1
III-Default2
…

II-Default1
II-Default2
…

I-Default1
I-Default2
…

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

Определение ролей интерфейсов

Что это такое?

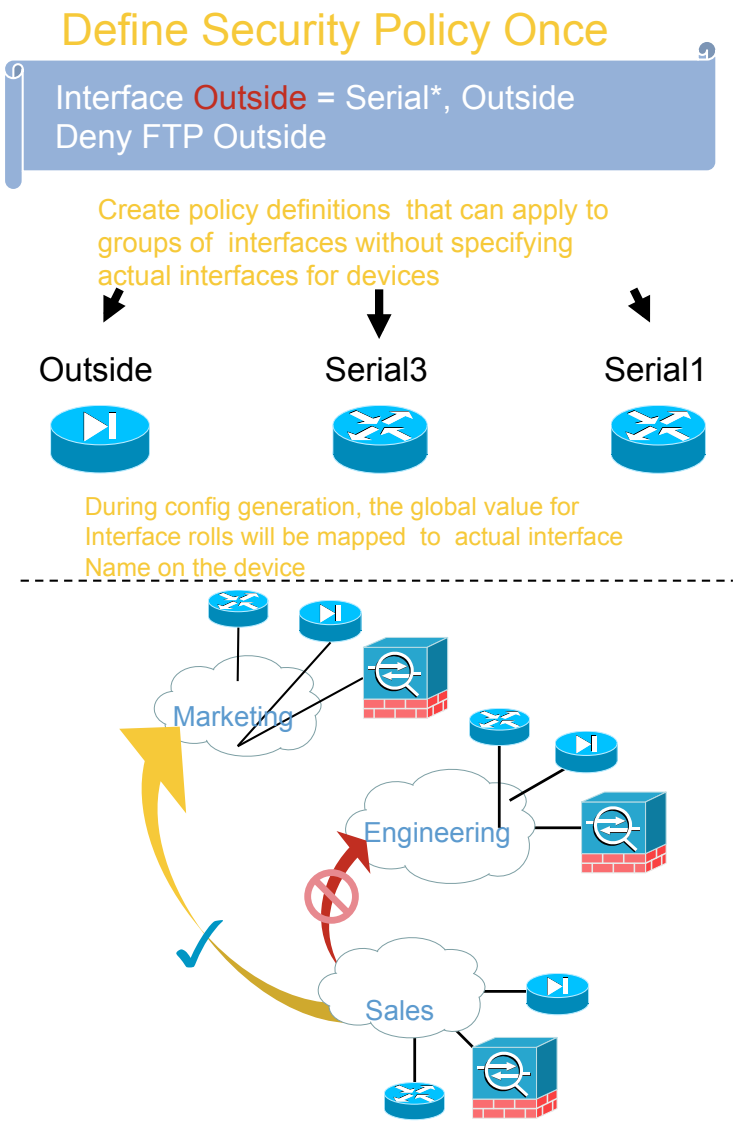
- Масштабируемый метод определения политик безопасности без знания актуальных значений интерфейсов устройства

Пример

- Администратор хочет блокировать FTP на всех внешних последовательных интерфейсах
- Он определяет глобальную переменную для всех последовательных интерфейсов
- При размещении политики глобальная переменная сама транслируется в специфичное значение интерфейса

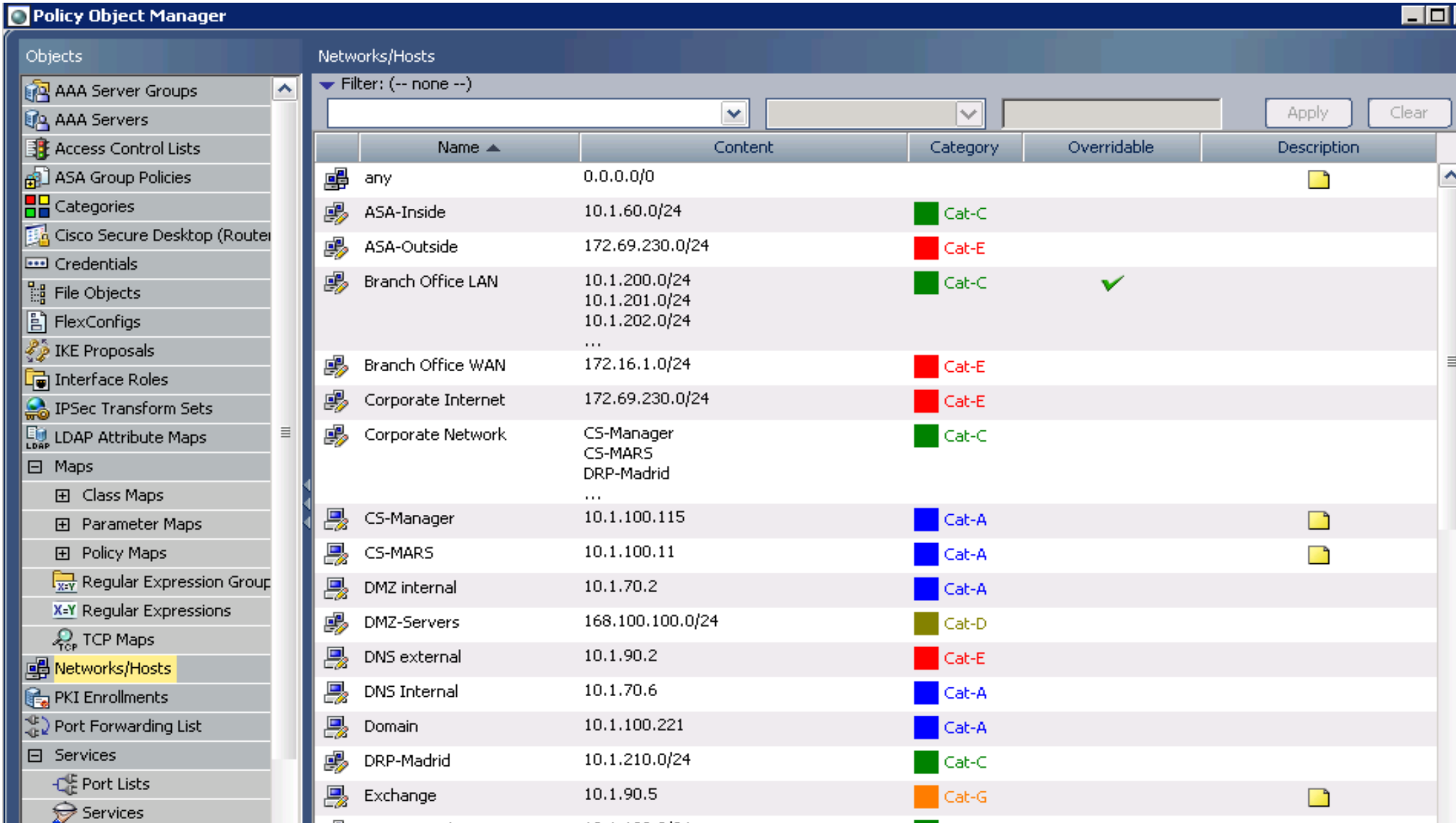
Преимущества

- Рост масштабируемости и гибкости
- Одна политика для множества устройств
- Снижение времени на создание политик

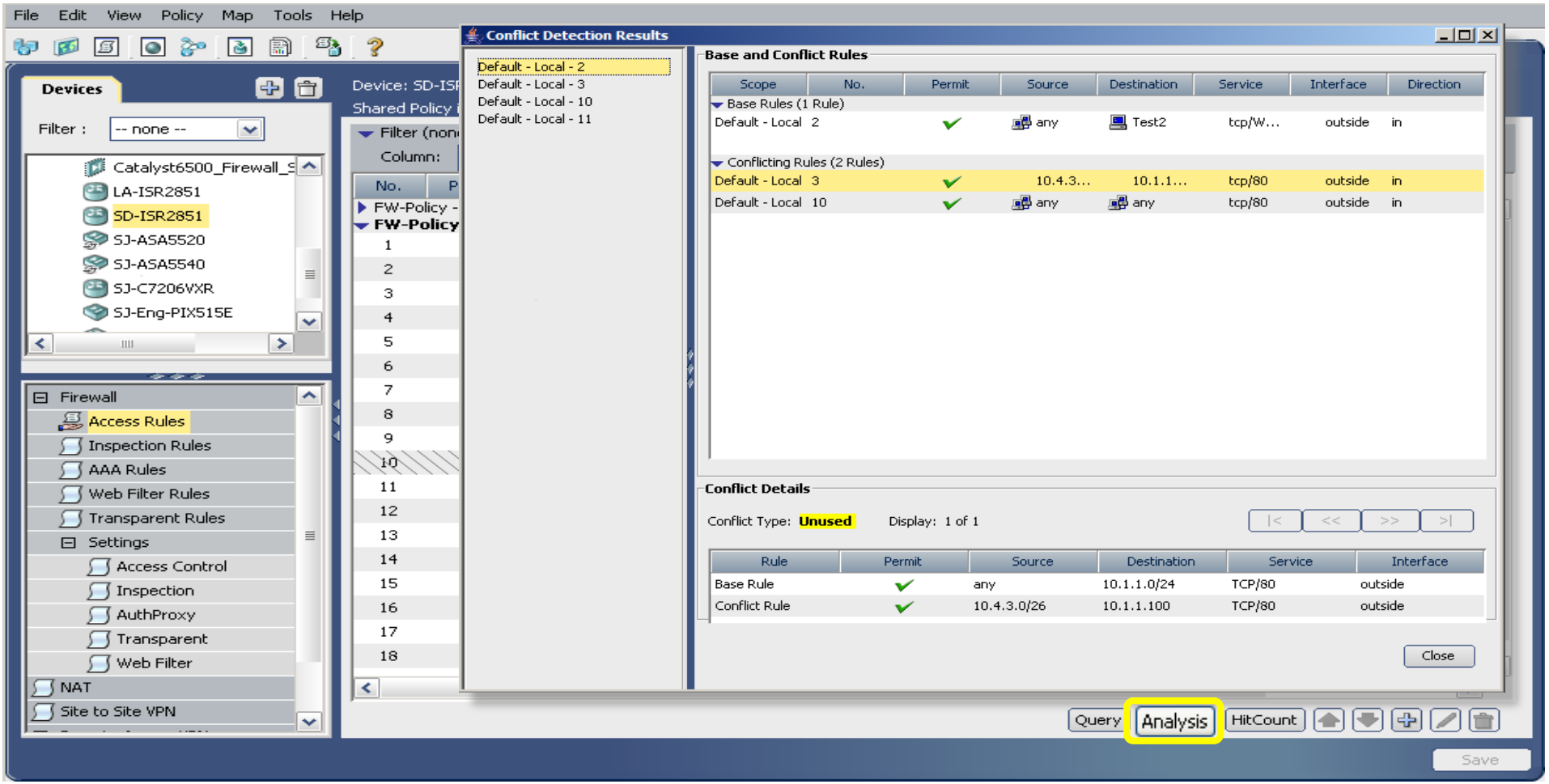


© 2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Использование объектов для сетей, хостов и сервисов



Анализ правил фильтрации



- Поиск дублирующих, перекрывающих или противоречивых правил в таблице

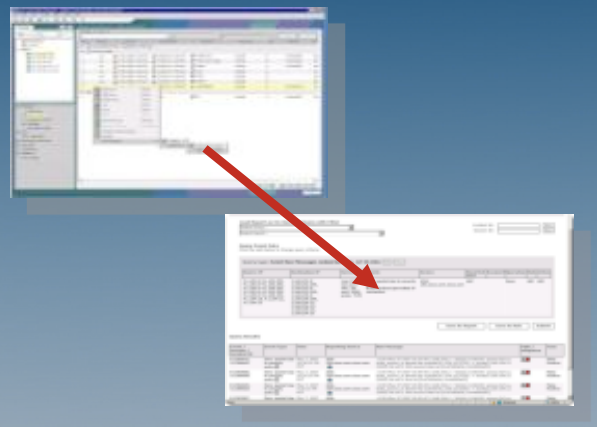
© 2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Интеграция CS-M и MARS

Упрощение управления за счет совместной работы

Связи событий МСЭ: «правила-события» и «события-правила»

Связи событий IPS: «сигнатура-события» и «события-сигнатура»

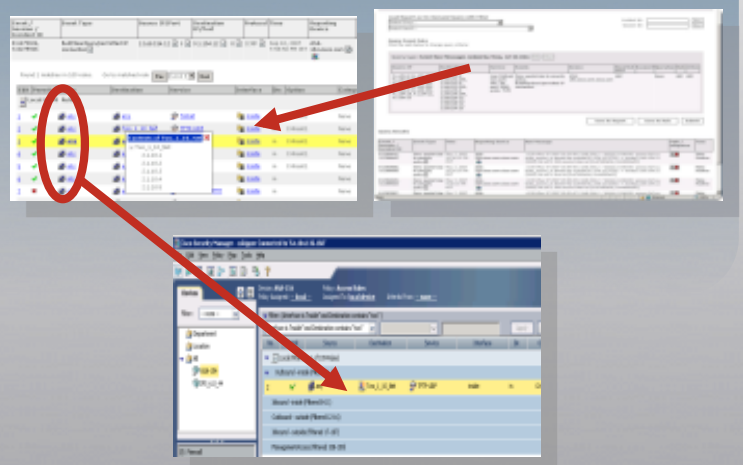


«События-правила»

- Отслеживание событий до уровня правил создания, возможность внесения изменений
- Лучшее понимание исходных данных журнала

«Правила-события»

- Уменьшение времени поиска неполадок соединения
- Моментальная проверка новых развернутых политик



© 2010 Cisco Systems, Inc. All rights reserved.

Cisco Security Manager 4.0
Корреляция событий и политик

CSM - Event Viewer

File View Help

Views: New Edit Delete

- Predefined Views
  - All Device Events
  - Firewall Traffic Eve
  - Firewall Denied Eve
  - AAA Events
  - NAT Events
  - Botnet Events
  - IPSec VPN Events
  - SSL VPN Events
  - Failover Events
  - All IPS Events
  - IPS Priority Alerts
  - IPS Alert Events
  - IPS Status Events
  - IPS Error Events
  - Unparsed Events
- My Views

Event Monitoring

All Device Events

View Settings

Search within results: Type here to search | last 1 week | Save | Start | Stop | Clear | 20,000

Receive ...	Seve...	Even...	Event Na...	Device	Source	Sourc...	Desti...	Desti...	Action	Risk ...	Description
1/12/10 5:...	Inform...	302015	Built UDP	10.104...	10.104.51.22	udp/514	10.104.49.86	udp/514	built		built outbo...
1/12/10 5:...	Inform...	302015	Bu				10.1.3.31	udp/514	built		built outbo...
1/12/10 5:...	Inform...	302015	Bu				10.76.5.100	udp/514	built		built outbo...
1/12/10 5:...	Inform...	302016	Teardo				10.104.51.22	udp/514	teardown		teardown ...
1/12/10 5:...	Inform...	302016	Teardo				10.104.51.22	udp/514	teardown		teardown ...
1/12/10 5:...	Inform...	302016	Teardo				10.104.51.22	udp/514	teardown		teardown ...
1/12/10 5:...	Inform...	302021	Teardo				10.104.51.22	0	teardown		teardown i...
1/12/10 5:...	Inform...	302020	Built IC				10.104.51.22	0	built		built inbou...
1/12/10 5:...	Inform...	302015	Bu				10.104.49.86	udp/514	built		built outbo...
1/12/10 5:...	Inform...	302015	Bu				10.1.3.31	udp/514	built		built outbo...
1/12/10 5:...	Inform...	302015	Bu				10.76.5.100	udp/514	built		built outbo...
1/12/10 5:...	Inform...	302016	Teardown ...	10.104...	10.104.49.86	udp/514	10.104.51.22	udp/514	teardown		teardown ...
1/12/10 5:...	Inform...	302016	Teardown ...	10.104...	10.1.3.31	udp/514	10.104.51.22	udp/514	teardown		teardown ...
1/12/10 5:...	Inform...	302016	Teardown ...	10.104...	10.76.5.100	udp/514	10.104.51.22	udp/514	teardown		teardown ...
1/12/10 5:...	Inform...	302016	Conn USAGE	10.104...							3 in use, 1...
1/12/10 5:...	Inform...	302015	Built UDP	10.104...	10.104.51.22	udp/514	10.104.49.86	udp/514	built		built outbo...
1/12/10 5:...	Inform...	302015	Built UDP	10.104...	10.104.51.22	udp/514	10.1.3.31	udp/514	built		built outbo...
1/12/10 5:...	Inform...	302015	Built UDP	10.104...	10.104.51.22	udp/514	10.76.5.100	udp/514	built		built outbo...
1/12/10 5:...	Inform...	302016	Teardown ...	10.104...	10.104.49.86	udp/514	10.104.51.22	udp/514	teardown		teardown ...
1/12/10 5:...	Inform...	302016	Teardown ...	10.104...	10.1.3.31	udp/514	10.104.51.22	udp/514	teardown		teardown ...
1/12/10 5:...	Inform...	302016	Teardown ...	10.104...	10.76.5.100	udp/514	10.104.51.22	udp/514	teardown		teardown ...

Filter Event Name is "Built UDP"
Custom Filter...
Clear Event Name Filter
Clear All Filters
Show All Details
Copy
Save
Go To Policy...

Time Slider

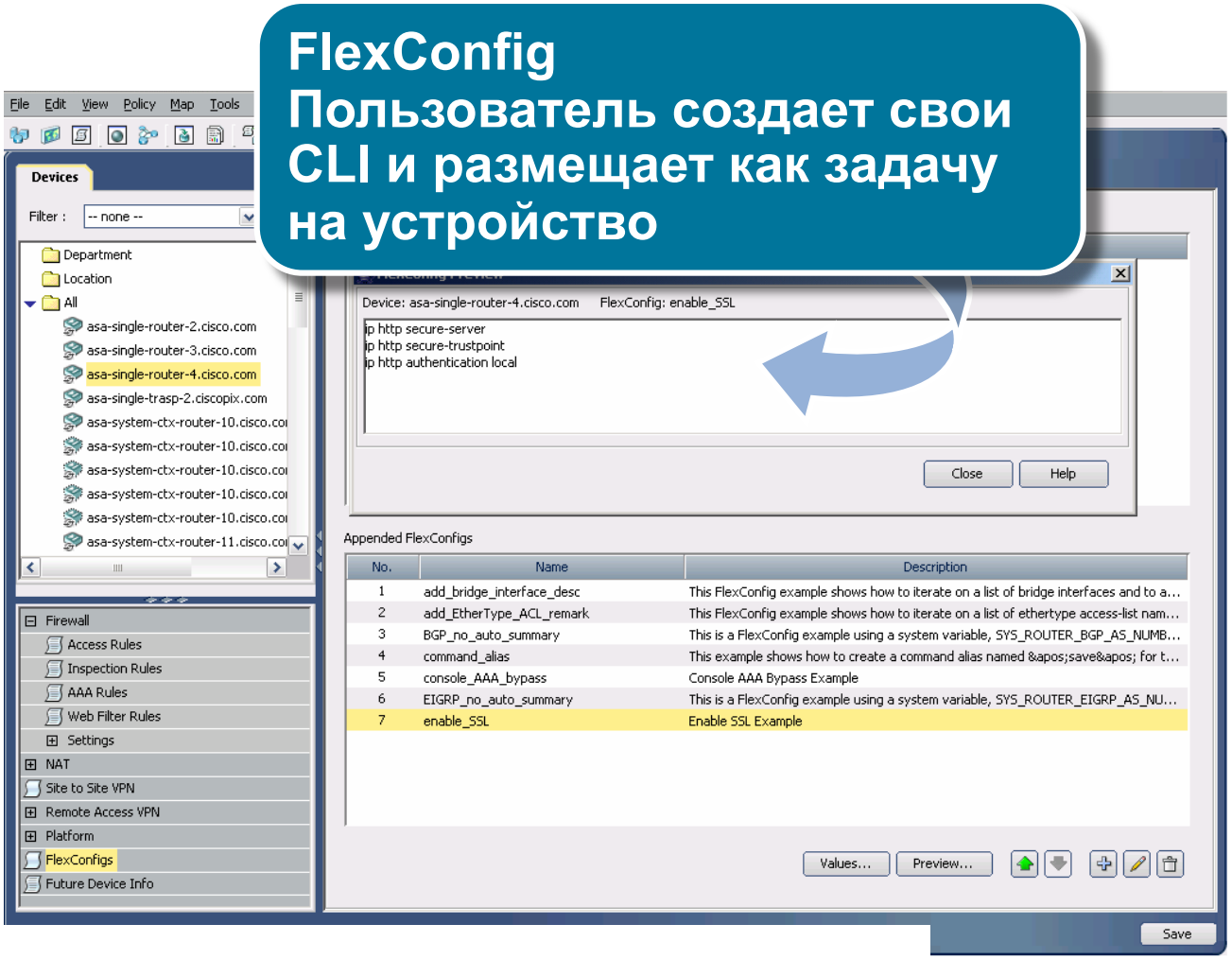
10,000
0
1/8 1/9 1/10 1/11 1/12 1/13 1/14

Event Details

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

FlexConfig

- Скриптовый язык для настройки функций, которые не имеют “родную” поддержку в CSM (в частности полезно для IOS)
- Можно использовать в скриптах информацию об устройстве (интерфейсы, адреса ...)



Гибкость

Индустриальный стандарт, Velocity Template Engine, скриптовый язык, который поддерживает циклы, выражения if/else и переменны

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Сравнение конфигураций

Configuration Archive

Devices Groups

Groups | Search

CSM Config Archive

Created On	Created By	Archival Source	Creation Comment	Transcript

Device : asa-single-router-4.cisco.com

Version ID: 29-Sep-2005 14:10:17

Compare with version: 28-Sep-2005 19:31:07

Config Type: Full Configuration / Delta Configuration

29-Sep-2005 14:10:17	28-Sep-2005 19:31:07
dhcprelay server 1.3.3.1 inside	dhcprelay server 1.3.3.1 inside
dhcprelay server 1.4.4.1 inside	dhcprelay server 1.4.4.1 inside
dhcprelay enable inside	dhcprelay enable inside
dhcprelay setroute inside	dhcprelay setroute inside
dhcprelay timeout 300	dhcprelay timeout 300
ntp authentication-key 1122 md5 *	ntp authentication-key 1122 md5 *
ntp authenticate	ntp authenticate
ntp trusted-key 1122	ntp trusted-key 1122
ntp server 10.1.2.3 key 1122 source inside	ntp server 10.1.2.3 key 1122 source inside
dns retries 5	dns retries 5
dns timeout 10	dns timeout 10
dns domain-lookup inside	dns domain-lookup inside
dns name-server 1.2.2.4	dns name-server 1.2.2.4
dns name-server 0.0.0.0	
request-method rfc connect action reset	
aaa accounting match CSM_AAA_ACCT_1 insi	
aaa authentication match CSM_AAA_AUTHE_1	

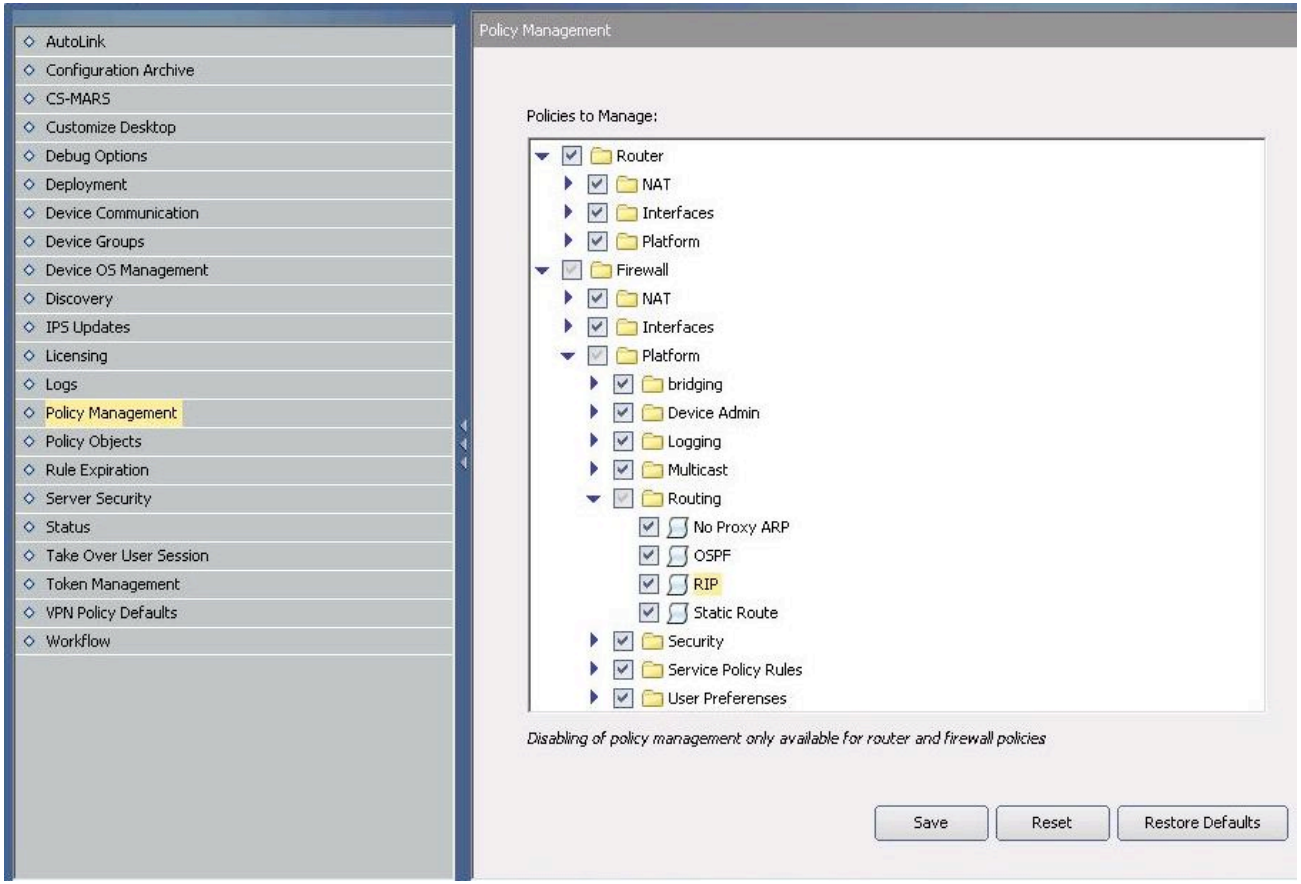
- Запрос и сравнение конфигураций
- Анализ изменений внесенных в конфигурацию не средствами CSM

Close | Help

© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Настройка политик для управления CSM

- Возможно избирательно настроить какие именно политики маршрутизаторов и МСЭ будут управляться CSM



© 2007 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Формализация процесса управления
контроль внесения изменений

Что это такое?

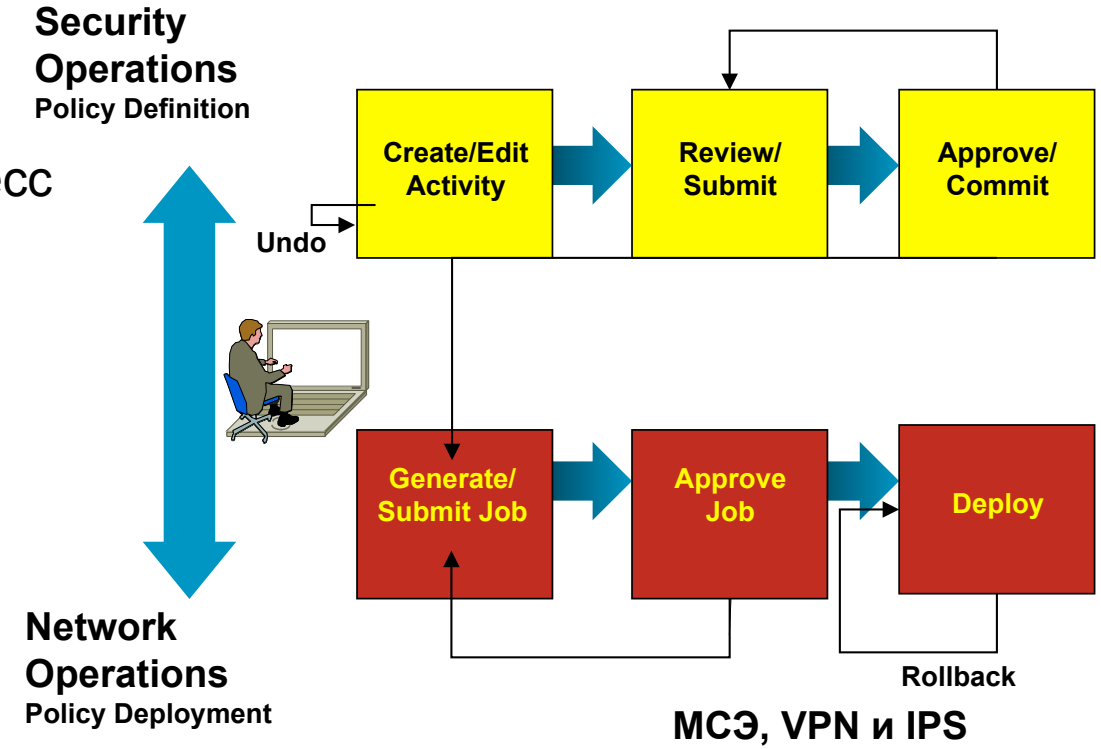
- Структурированный процесс контроля и утверждения изменений политики

Пример

- Кто создает политику?
- Кто утверждает политику?
- Кто применяет политику и когда?

Преимущества

- Эффективное взаимодействие между ролями/отделами



- Кто может изменять политики?
- Кто может просматривать изменения?
- Кто может их утверждать?
- Кто отвечает за применение новых политик?

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

Activity Report

Activity Change Report

Devices

1701-router.cisco.com

FIREWALL-InspectRule

InspectRule

Operation	No	Mandatory	Permit	Source	Destination	Traffic Match	Interface	Inspected Protocol	Category	Enabled
Add	1	true	permit	any	any	default-inspection	Global	[dns(Max length: 512)]	None	true
Add	2	true	permit	any	any	default-inspection	Global	[snmp]	None	true
Add	3	true	permit	any	any	default-inspection	Global	[h323 h225]	Cat-A	true

Operation	No	Mandatory	Permit	Source	Destination	Traffic Match	Interface	Inspected Protocol	Category	Enabled
Delete	~~3~~	~~true~~	~~permit~~	~~any~~	~~any~~	~~default-inspection~~	~~Global~~	~~[h323 h225]~~	~~Cat-A~~	~~true~~

Shared Policies

FIREWALL-InspectRule

Share_Inspect

Parent	Global
Affected Devices	None
New Assignments	Total:1. Devices: pix-515.cisco.com
Unassignments	Total:1. Devices: 1701-router.cisco.com

InspectRule

Operation	No	Mandatory	Permit	Source	Destination	Traffic Match	Interface	Inspected Protocol	Category	Enabled
Modify	1	false	permit	any	any	default-inspection	Global	~~[telnet]~~ [snmp]	None	true
Modify	2	false	permit	any	any	default-inspection	Global	~~[ftp]~~ [h323 h225]	Cat-A	true
Modify	1	true	permit	any	any	default-inspection	Global	~~[ftp strict]~~ [dns(Max length: 512)]	None	true

Operation	No	Mandatory	Permit	Source	Destination	Traffic Match	Interface	Inspected Protocol	Category	Enabled
Delete	~~2~~	~~false~~	~~permit~~	~~any~~	~~any~~	~~default-inspection~~	~~Global~~	~~[h323 h225]~~	~~Cat-A~~	~~true~~

Vms Objects

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

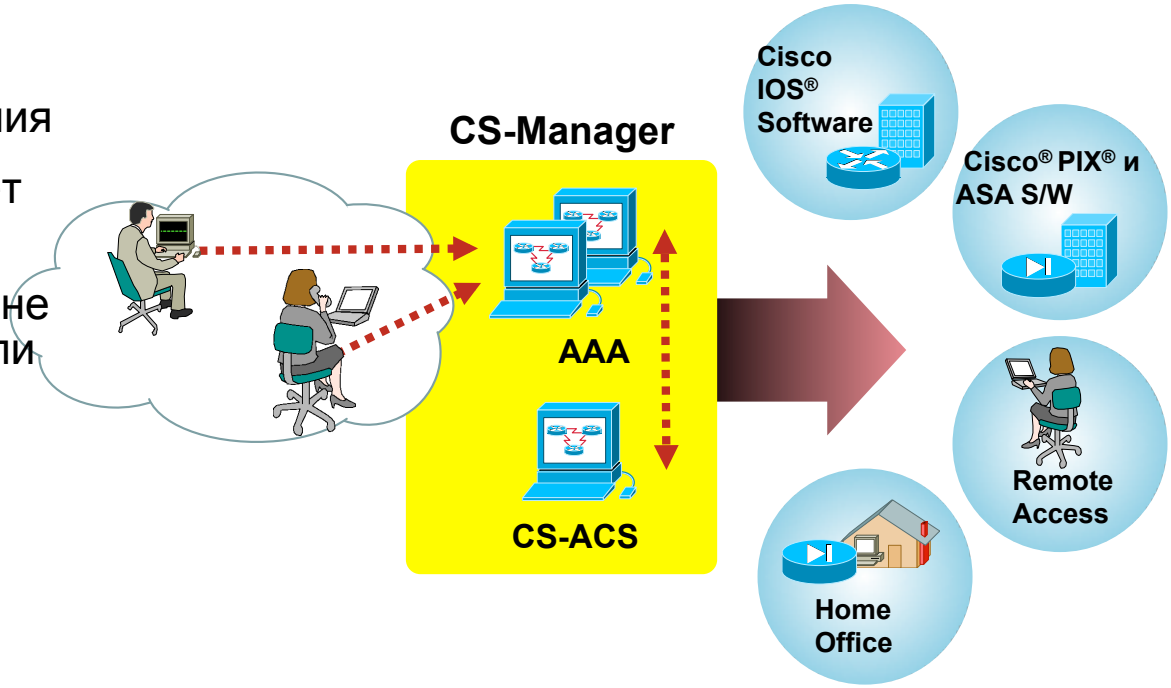
Ролевой доступ

Что это такое?

- Аутентификация администратора перед доступом к системе управления
- Кто и какой тип доступа может иметь к устройствам?
- Авторизация доступа на уровне устройств/ групп устройств или отдельных политик

Пример

- Делегирование административных задач операторам
- Разделение управления и контроля
- Централизованное управление доступом администраторов



© 2010 Cisco Systems, Inc. All rights reserved.

CiscoWorks Network Compliance Manager

Обеспечение соответствия сети требованиям стандартов

© 2010 Cisco Systems, Inc. All rights reserved.

CiscoWorks Network Compliance Manager (NCM)

Мультивендорное решение по управлению изменениями

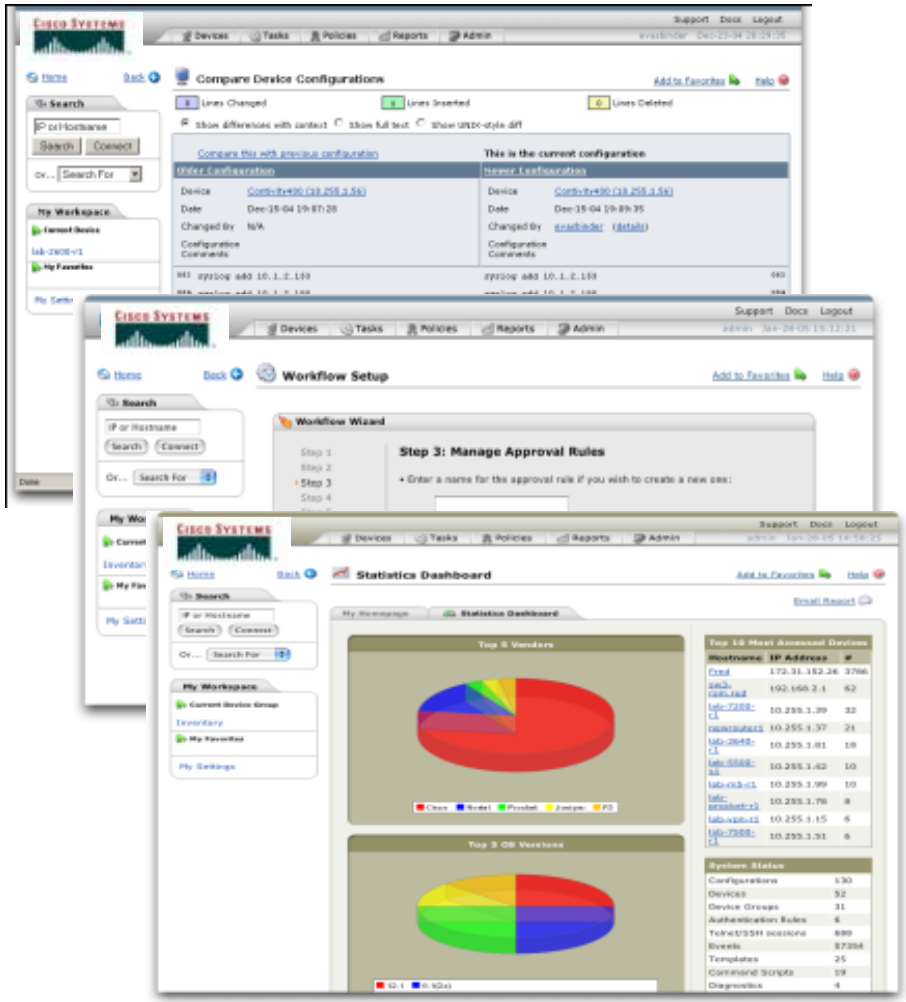
- Обнаружение изменений на сети в реальном режиме времени
- Предварительная проверка изменений перед их внедрением на сети

Аудит и анализ соответствия стандартам и нормативам

- Контроль выполнения стандартов и нормативов на сети
- Оперативная отчетность

Согласование изменений (Workflow)

- Настройка правил согласования
- Возможность настройки сложных правил



© 2010 Cisco Systems, Inc. All rights reserved.

Аудит и анализ соответствия стандартам и нормативам

- Определить нормативные документы, которым должна соответствовать инфраструктура ИТ
- Определить специфические требования для ИС
- Проконсультироваться с аудиторами
- Спроектировать систему контроля
- Внедрить систему
- Аудит инфраструктуры на соответствие стандартам
- Постоянное усовершенствование системы

Самая сложная часть

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

Пример требований - PCI DSS

PCI DSS Стандарт защиты информации в индустрии платежных карт	Перечень требований для повышения уровня безопасности в индустрии платежных карт. разработанный международными платежными системами Visa и MasterCard. Поддерживается AmEx, Diners Club, Discover, JCB. Содержит 12 основных требований, 175 детальных требований
Пример требований	Требование 2.1: Не использовать значения по умолчанию для паролей и других параметров безопасности
Как может быть достигнуто?	Проверка конфигурации на использование стандартных значений ‘public’, ‘private’, ‘cisco’ в SNMP; ‘cisco’, ‘cisco123’, ‘sdm’ для доступа через WEB (например, SDM)

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

Пример корпоративных требований

Управление	“На каждом устройстве должно быть настроено как минимум 2 получателя сообщений Syslog и SNMP trap”
Управление	“Не более 4 получателей Syslog”
Управление	“Не должны использоваться «популярные» значения SNMP community”
Управление	“Для доступа по SNMP должны использоваться ACL”
Безопасность	“На каждом устройстве должны быть настроены AAA/ TACACS и SSHv2”
Безопасность	“AAA/Accounting должен быть включен”
Безопасность	“Должна использоваться опция ‘password 5’, не использоваться пароли в открытом виде”

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

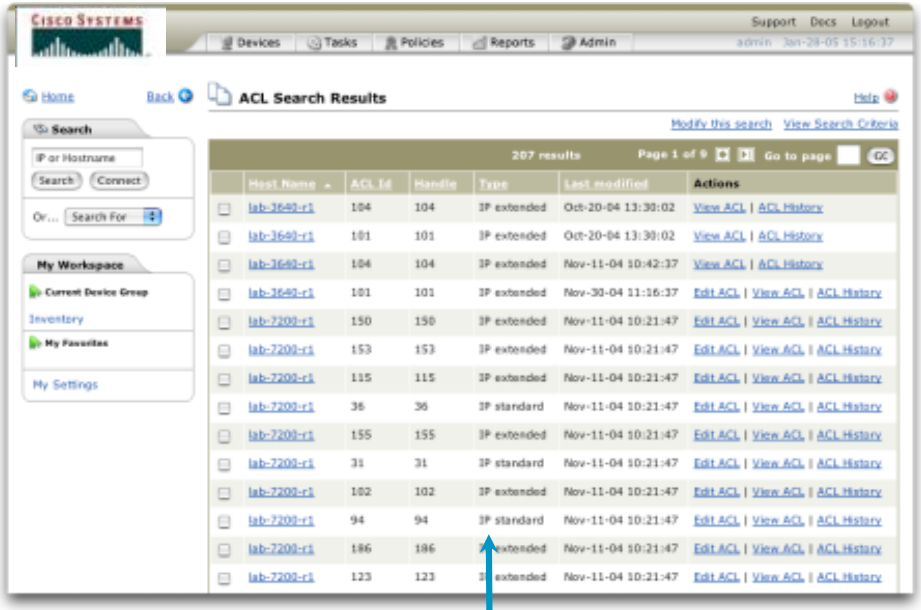
ИБ и NCM

- Поддержка полной истории изменений конфигураций для нужд аудита
- Мониторинг и принудительное применений политик ИБ
- Создание собственных политик ИБ и проверка вносимых изменений на соответствие им еще до применения на устройство
- Разграничение доступа на основе ролей
- Изменений конфигурация с использованием конфиглетов
- Поддержка истории изменений ACL
- Легкое применений изменений в ACL

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

Управление безопасностью

- Централизованное управление версиями ПО
- Telnet/SSH Proxy
  - Единая точка входа
  - Запись полной сессии
  - Точка централизованного контроля привелегий и утверждения изменений
- Управление ACL
  - Просмотр поиск, история изменений
  - Комментарии для ACL
  - Пакетное редактирование ACL для более быстрого реагирования
  - Шаблоны ACL

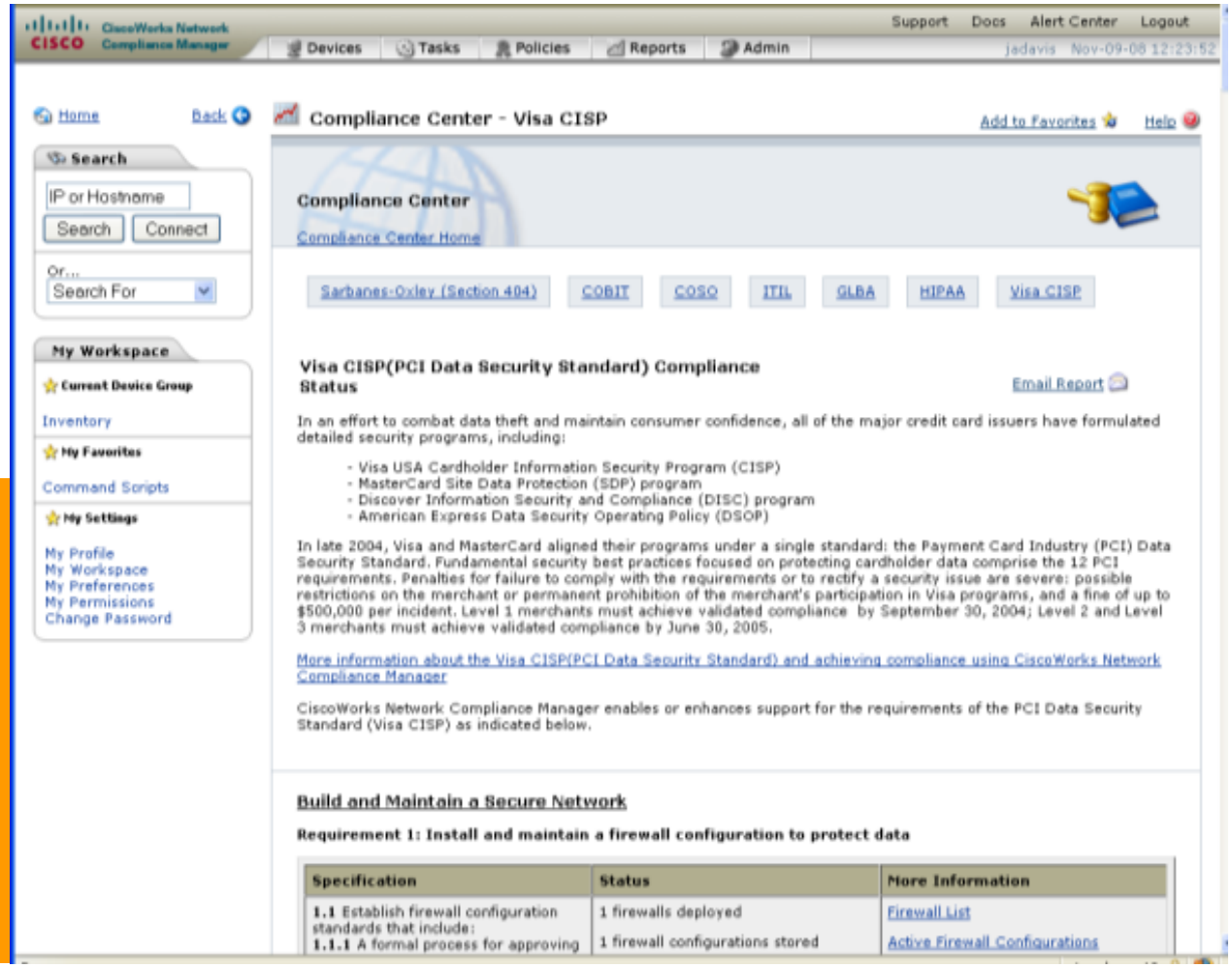


История изменений ACL

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

Стандарты и отчеты

NCM предоставляет готовую отчетность по ряду стандартов



Как только устройство добавлено в систему и по нему получена конфигурация, информация по нему автоматически попадает в отчет.
Вам необходимо нажать одну кнопку...

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

Сравнение CSM и NCM

	CSM	NCM
Поддерживаемые устройства	Только Cisco	Cisco + …
Управление версиями ПО	Да*	Да
Масштабируемость (устройства)	5-5 000	100-25 000
Управление конфигурациями	Да	Да
Оптимизировано для настройки ИБ	Да	Нет
Процедуры утверждения изменений (Workflow)	Да	Да
Аудит на соответствие требованиям	Нет	Да
Аудит вносимых изменений	Ограничено	Да
GUI для управления политиками	Да	Ограничено

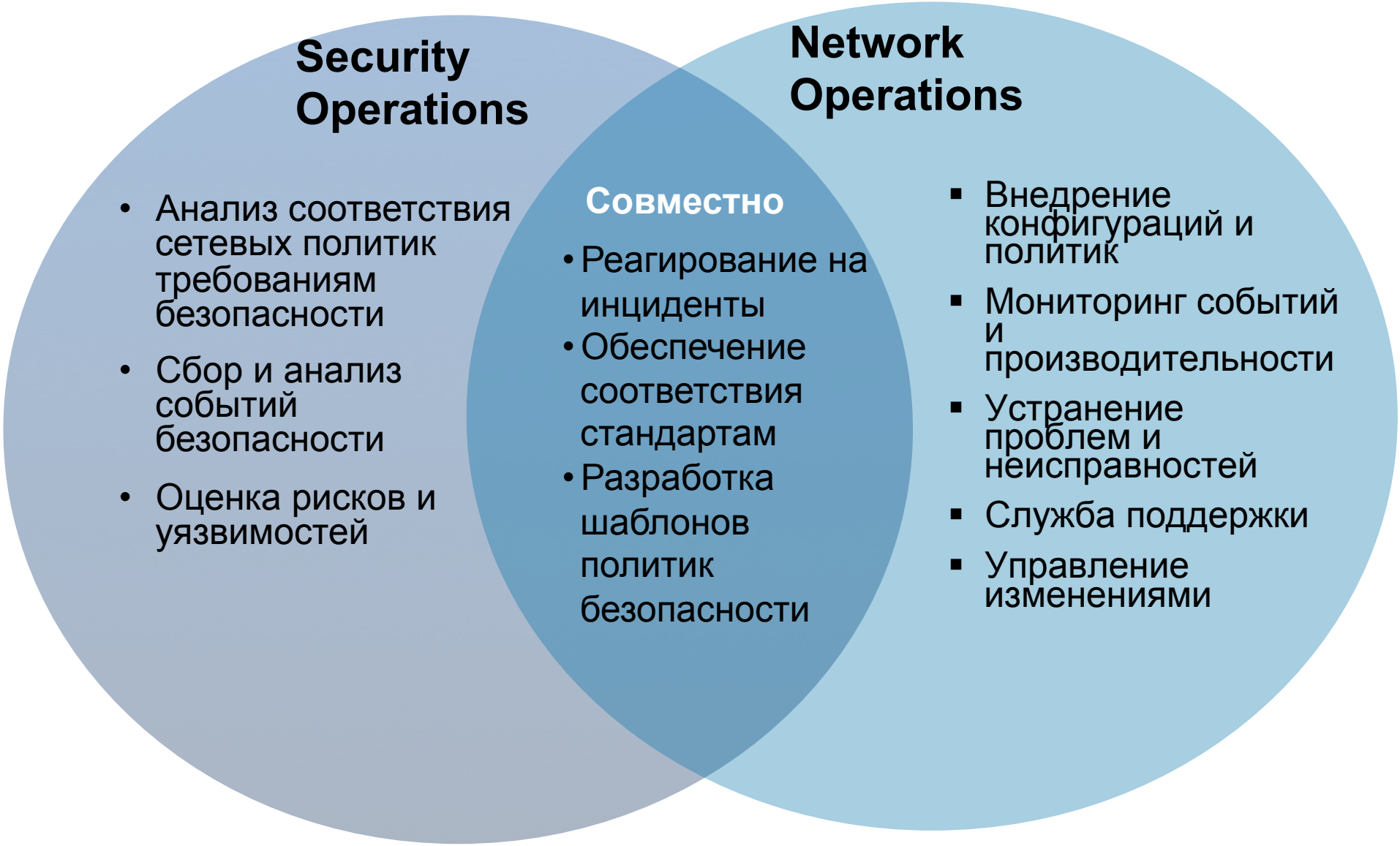
*Посредством RME приложения

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

Практические сценарии совместного использования систем управления сетевым департаментом и службой ИБ

© 2010 Cisco Systems, Inc. All rights reserved.

Разделение полномочий (Вариант А)



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

Разделение полномочий (Вариант А)

Security Operations

- Анализ соответствия сетевых политик требованиям безопасности
- Сбор и анализ событий безопасности
- Оценка рисков и уязвимостей

Совместно

- Реагирование на инциденты
- Обеспечение соответствия стандартам
- Разработка шаблонов политик безопасности

Network Operations

- Внедрение конфигураций и политик
- Мониторинг событий и производительности
- Устранение проблем и неисправностей
- Служба поддержки
- Управление изменениями

MARS

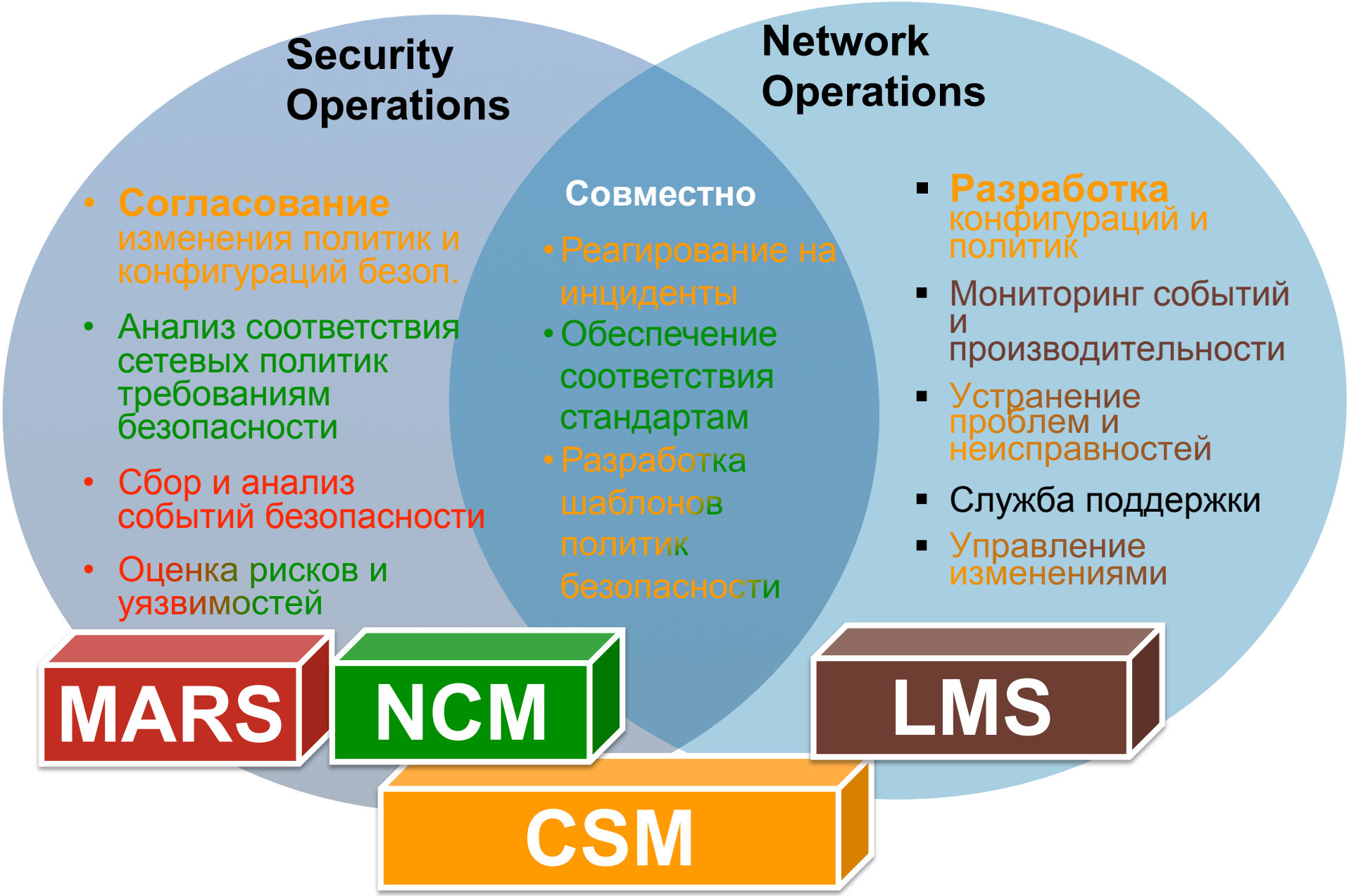
NCM

LMS

CSM

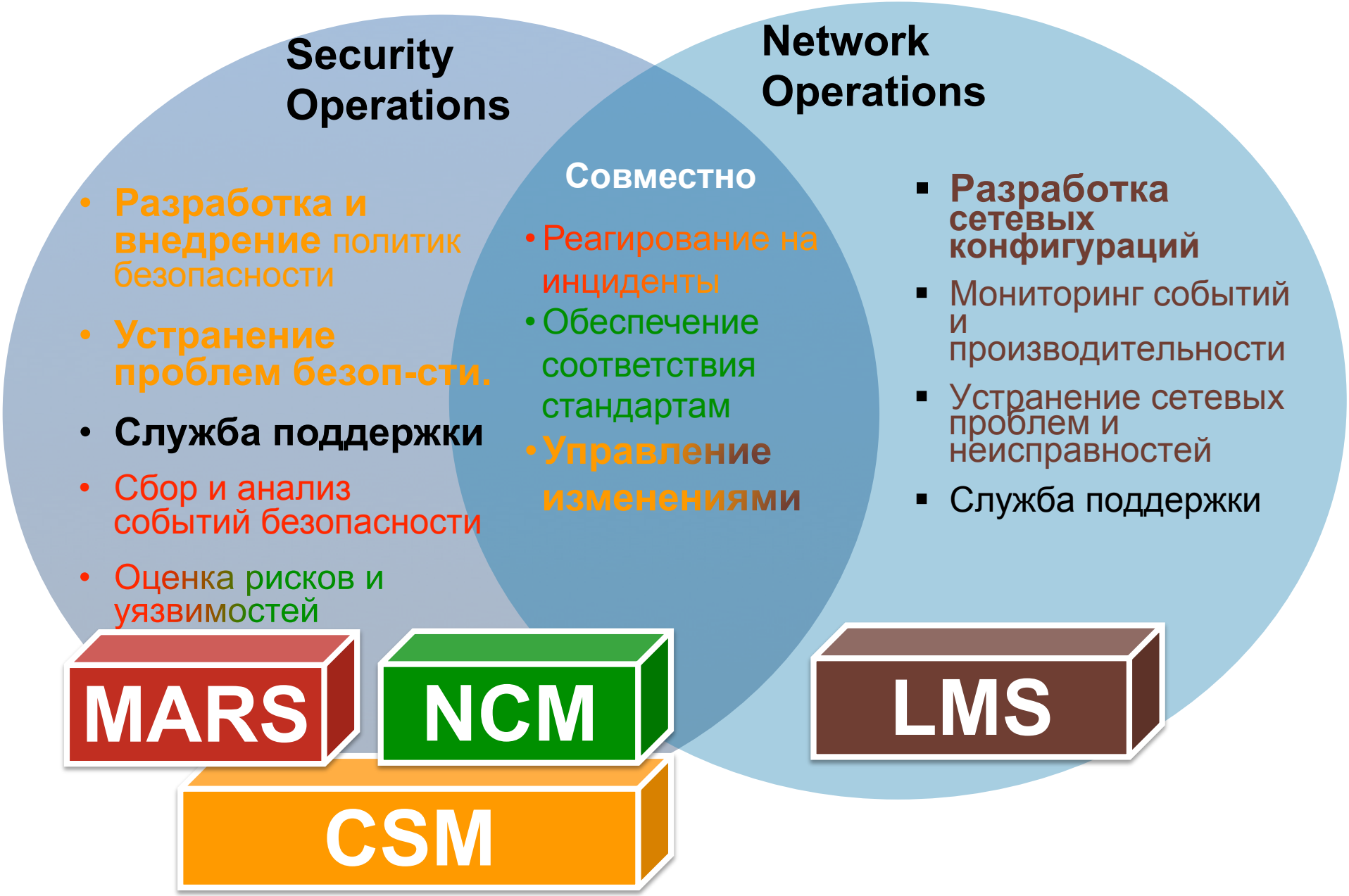
© 2010 Cisco Systems, Inc. All rights reserved. Cisco Public

Разделение полномочий (Вариант Б)



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

Разделение полномочий (Вариант B)



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

Вопросы?

© 2010 Cisco Systems, Inc. All rights reserved.

© 2010 Cisco Systems, Inc. All rights reserved.