Cisco Expo 2011

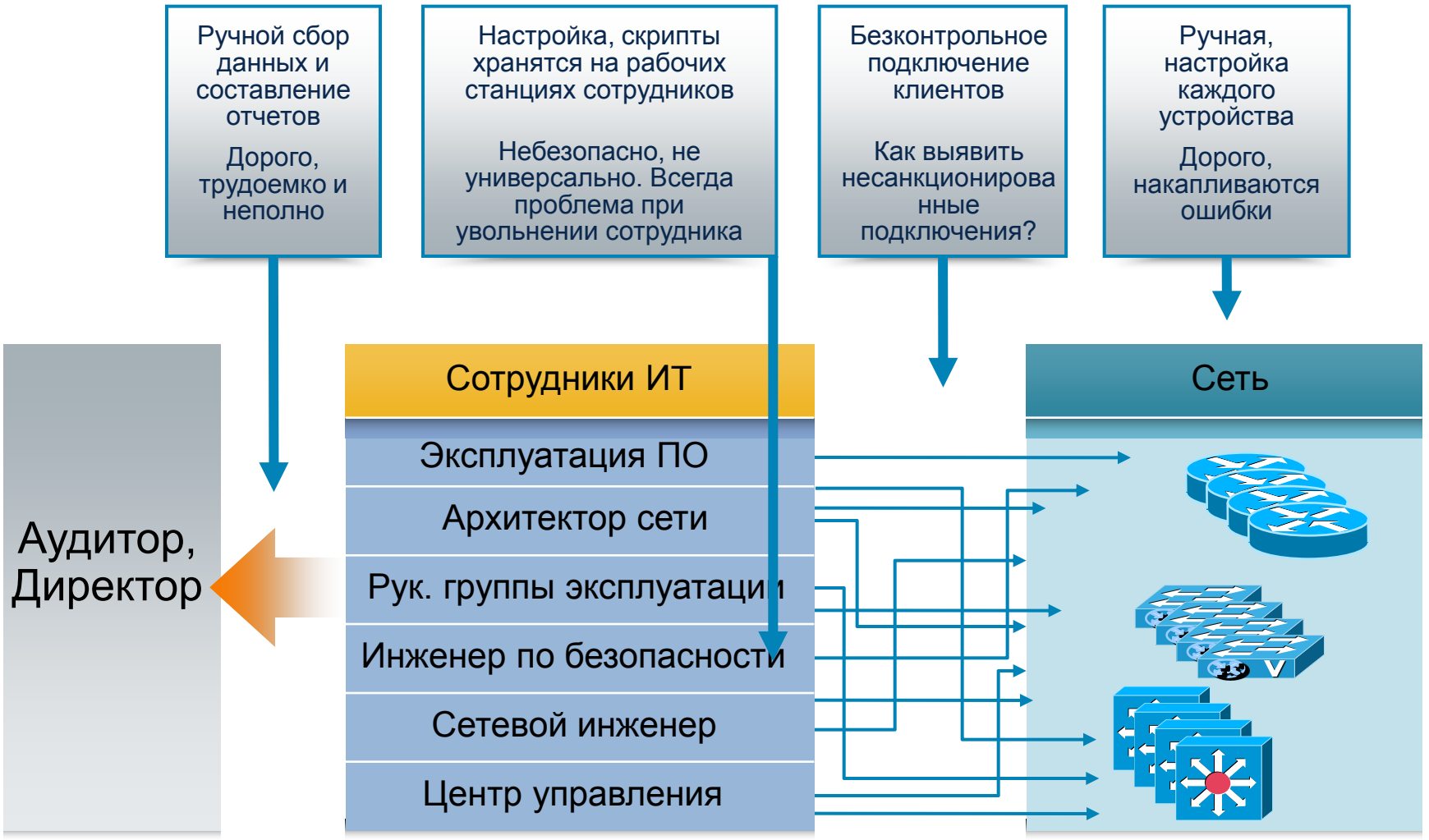
Инструменты контроля сетевого окружения.

CiscoWorks NCM как средство аудита

Патенко Владислав, инженер-консультант

vpatenko@cisco.com

Проблемы при настройке оборудования вручную



Следствия управления сетью вручную

Увеличение количества отказов	80% отказов и проблем с безопасностью связаны с неконтролируемой настройкой сети
Понижение доступности сети	80% бюджета на увеличение доступности сети расходуется реактивно
Большие трудозатраты на управление	45% времени инженеров израсходуются на настройку оборудования вручную
Сложный контроль соответствия политикам	5-кратное увеличение стоимости и трудозатрат на контроль соответствия политикам

Источник: Опрос заказчиков компанией Cisco

CiscoWorks Network Compliance Manager

Одно из лучших в мире решений по управлению изменениями

- Обнаружение изменений на сети в реальном режиме времени
- Предварительная проверка изменений перед их внедрением на сети
- Контроль за выполнением корпоративных правил и политик

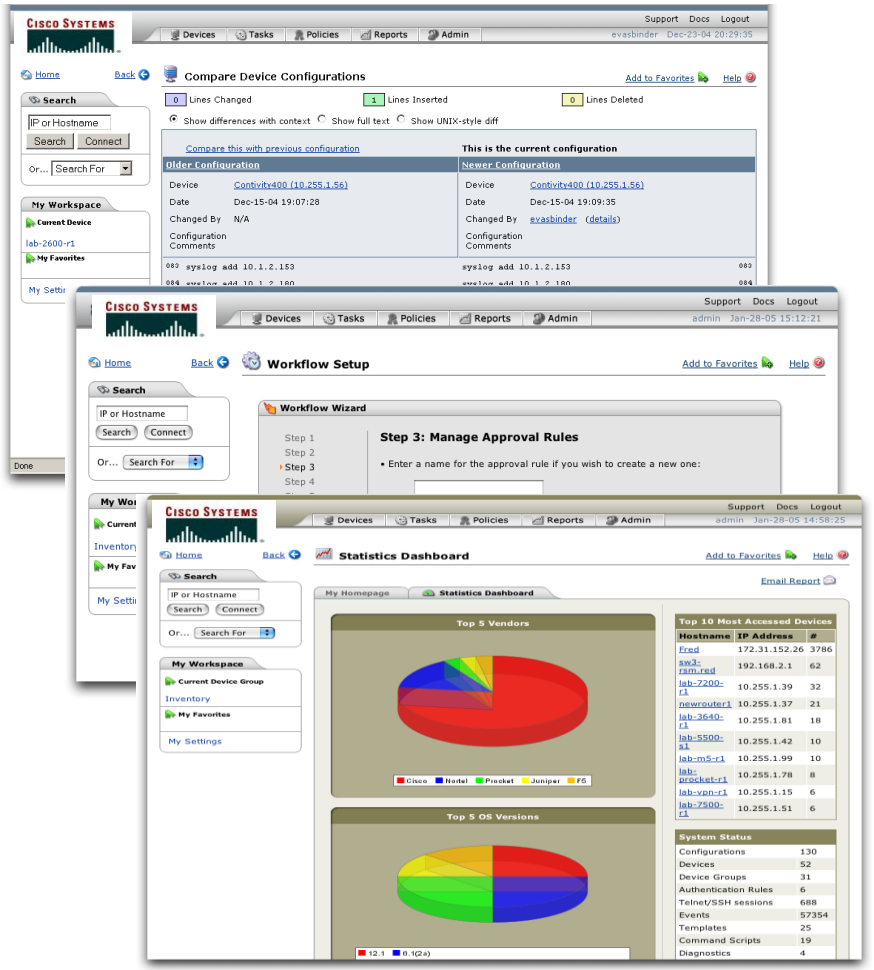
Аудит и анализ соответствия политиками компании

- Внедрение политик и правил на сети
- Автоматическая генерация отчетов по соответствию международным рекомендациям (SOX, VISA CISP, HIPAA, GLBA, ITIL, CobiT, COSO)

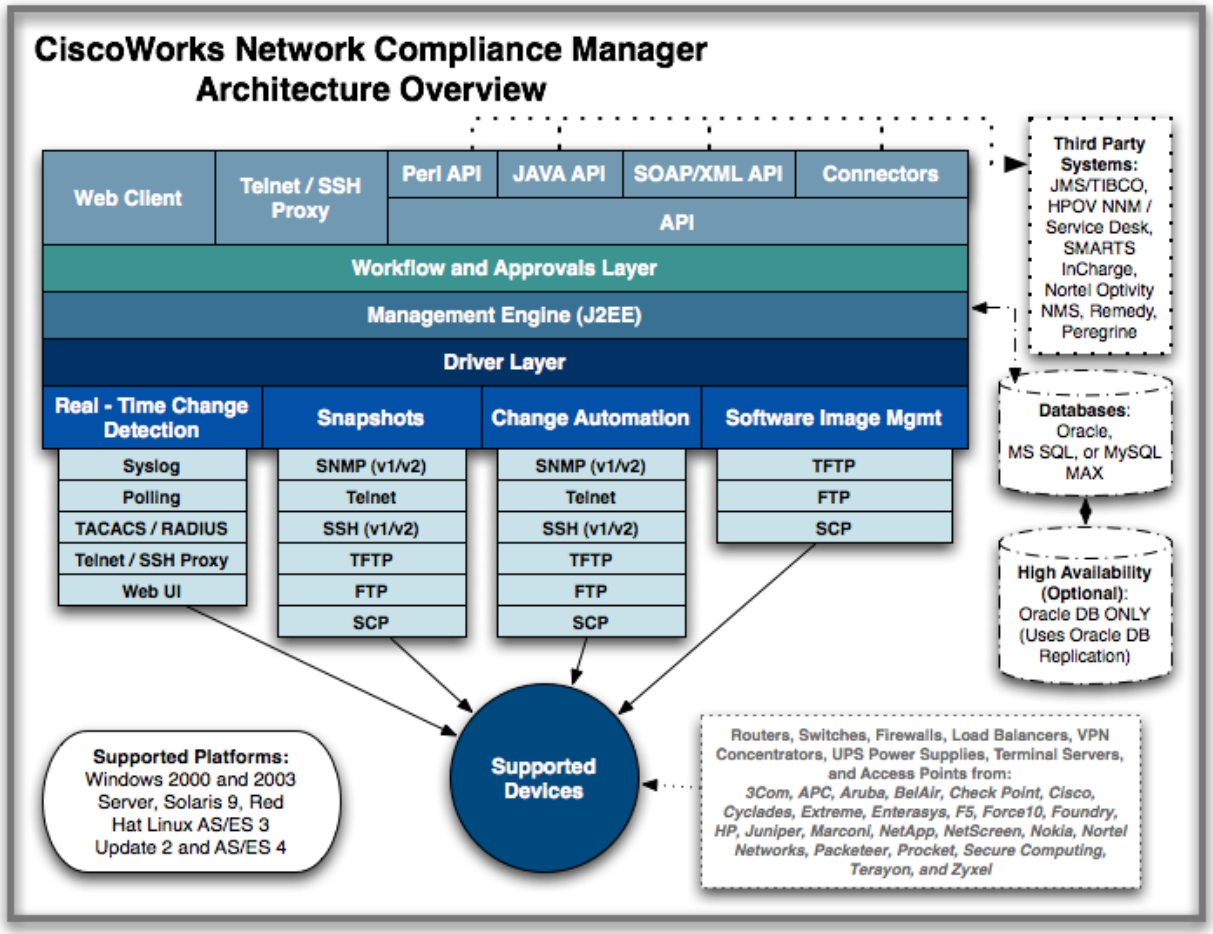
Согласование изменений

- Настройка правил согласования
- Возможность настройки сложных правил

Отчетность



Обзор архитектуры



Безопасность

- Контроль доступа на уровне каждого устройства
- Контроль доступа на уровне задач/скриптов
- Шифрование данных

Интеграция с LDAP и AAA

- LDAP / Active Directory
- RADIUS / TACACS
- SecureID

Высокая доступность

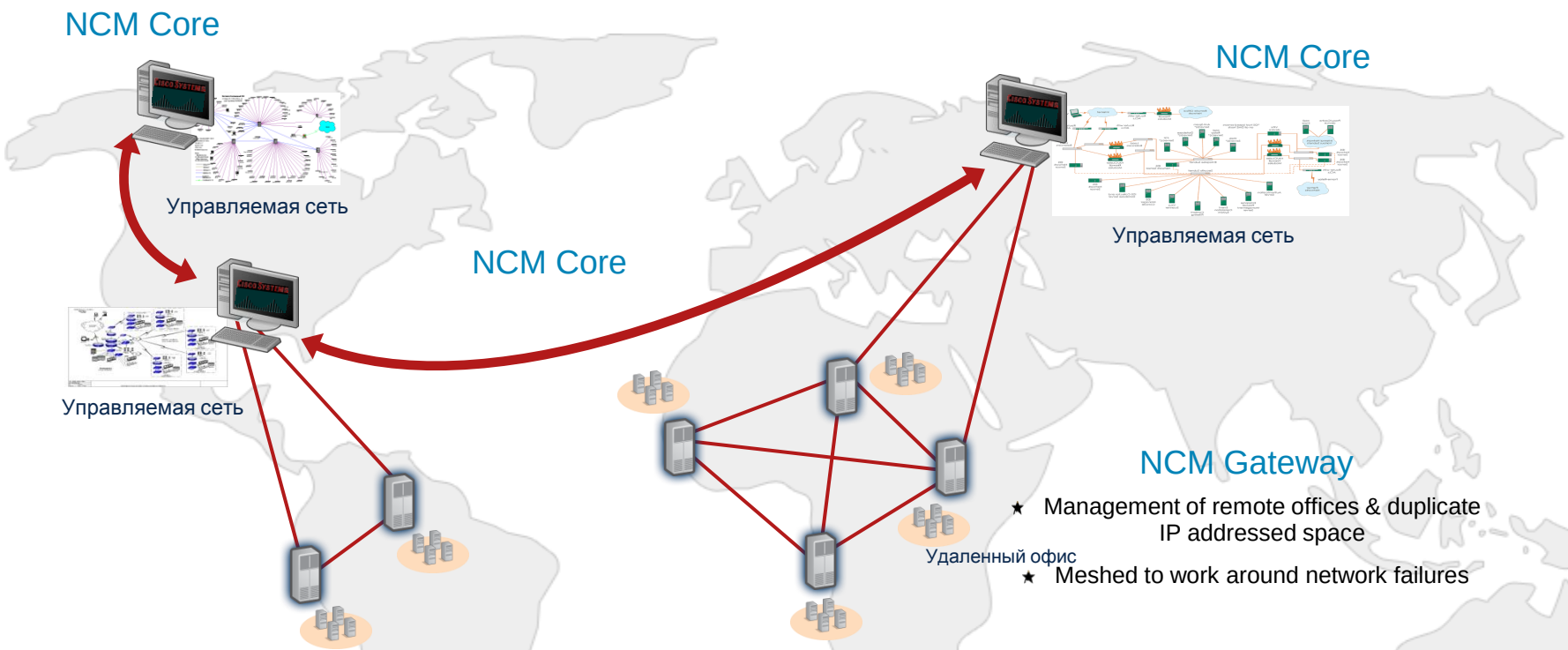
- High Availability Replication
- Satellite Off-loading
- Кластеры Microsoft и Veritas (Solaris)

Расширения

- APIs (Perl, Java, Web Services (XML)
- Открытая схема БД
- Интеграция с CiscoWorks и другими NMS

Возможности по отказоустойчивости

Конфигурация Active/Active через репликацию базы данных



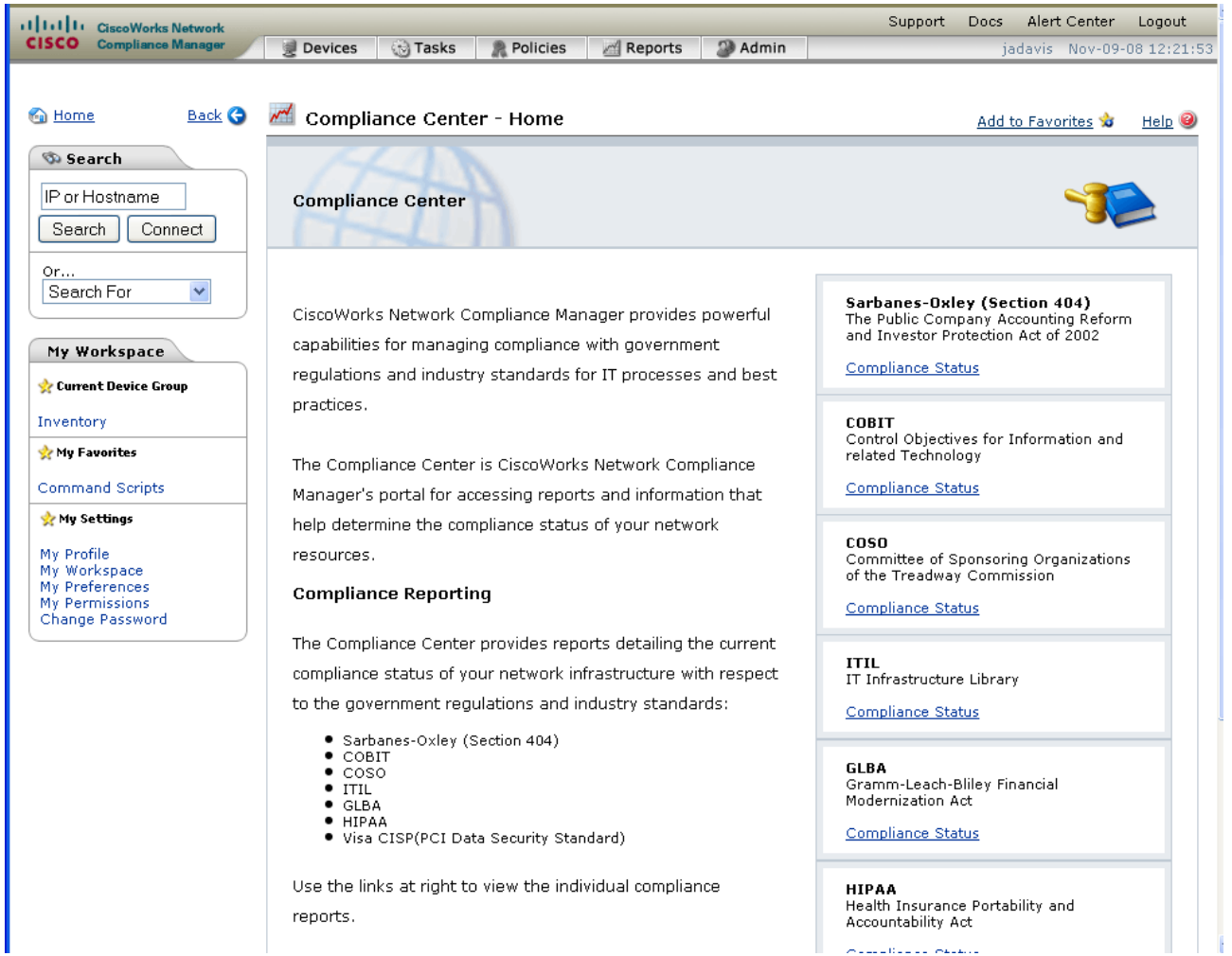
Отказоустойчивость NCM

- Синхронизация данных между всеми NCM Core в реальном времени
- Удаленное управление и восстановление систем
- Полная репликация данных

Компоненты	Ключевые возможности
★ Core ★ HA ★ Gateway	★ Безопасность, масштабируемость ★ Нет единой точки отказа ★ Удаленное управление устройствами— даже в сетях с дублированием IP адресов

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...

Home | Back

Compliance Center - Visa CISP

Add to Favorites | Help

Search
IP or Hostname
Search | Connect
Or...
Search For

My Workspace
Current Device Group
Inventory
My Favorites
Command Scripts
My Settings
My Profile
My Workspace
My Preferences
My Permissions
Change Password

Compliance Center

Compliance Center Home

Sarbanes-Oxley (Section 404) | COBIT | COSO | ITIL | GLBA | HIPAA | Visa CISP

Visa CISP(PCI Data Security Standard) Compliance Status

Email Report

In an effort to combat data theft and maintain consumer confidence, all of the major credit card issuers have formulated detailed security programs, including:

- Visa USA Cardholder Information Security Program (CISP)
- MasterCard Site Data Protection (SDP) program
- Discover Information Security and Compliance (DISC) program
- American Express Data Security Operating Policy (DSOP)

In late 2004, Visa and MasterCard aligned their programs under a single standard: the Payment Card Industry (PCI) Data Security Standard. Fundamental security best practices focused on protecting cardholder data comprise the 12 PCI requirements. Penalties for failure to comply with the requirements or to rectify a security issue are severe: possible restrictions on the merchant or permanent prohibition of the merchant's participation in Visa programs, and a fine of up to $500,000 per incident. Level 1 merchants must achieve validated compliance by September 30, 2004; Level 2 and Level 3 merchants must achieve validated compliance by June 30, 2005.

More information about the Visa CISP(PCI Data Security Standard) and achieving compliance using CiscoWorks Network Compliance Manager

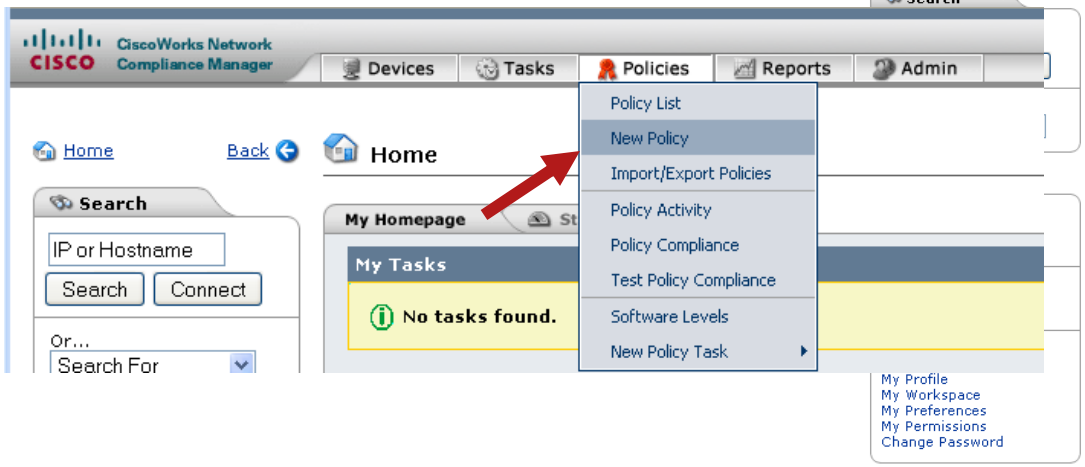
CiscoWorks Network Compliance Manager enables or enhances support for the requirements of the PCI Data Security Standard (Visa CISP) as indicated below.

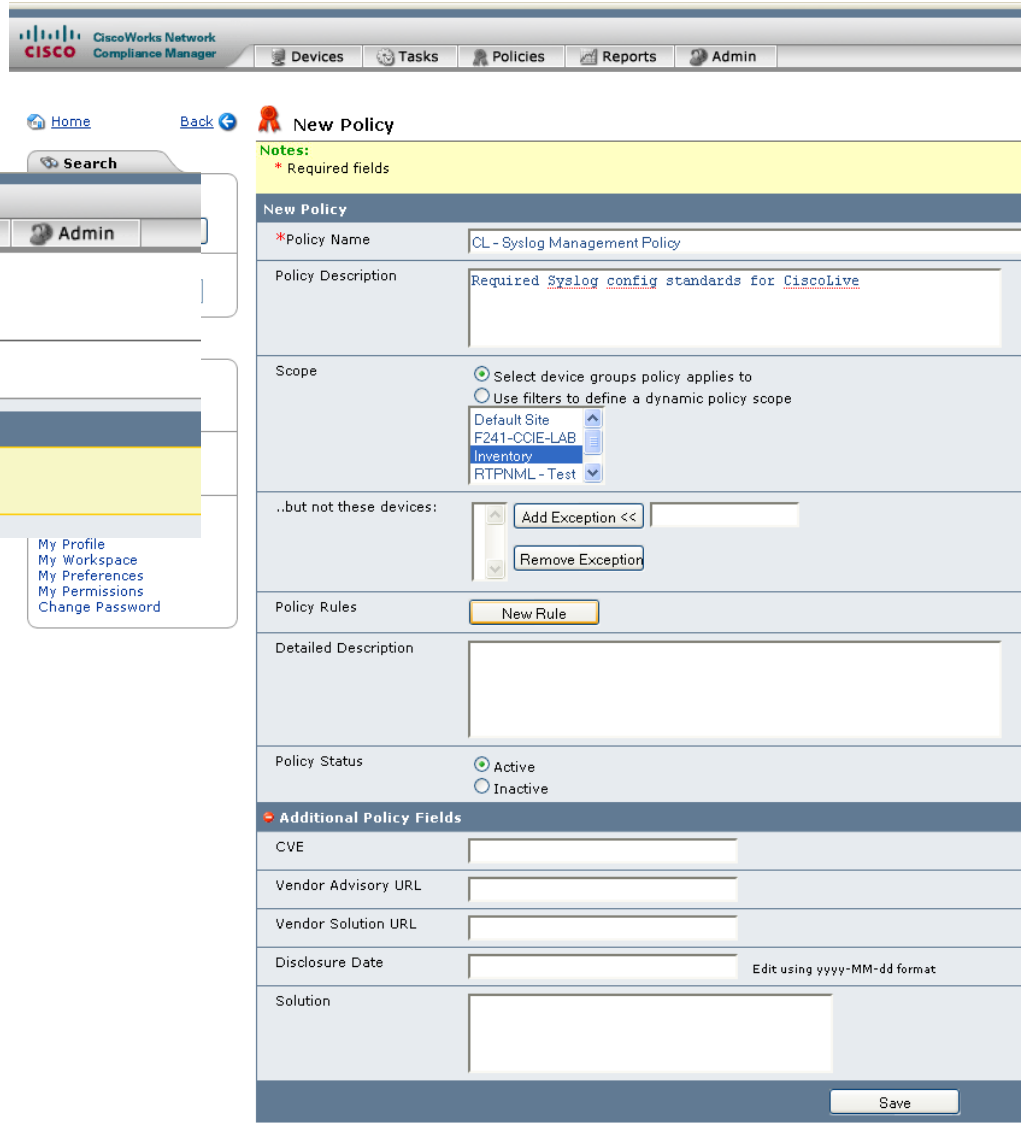
Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect data

Specification	Status	More Information
1.1 Establish firewall configuration standards that include: **1.1.1** A formal process for approving and testing all external network connections and changes to the firewall configuration **1.1.2** A current network diagram with all connections to cardholder data, including any wireless networks **1.1.3** Requirements for a firewall at each Internet connection and between any DMZ and the Intranet **1.1.4** Description of groups, roles, and responsibilities for logical management of network components **1.1.5** Documented list of services/ports necessary for business **1.1.6** Justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN **1.1.7** Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented **1.1.8** Periodic review of firewall/router rule sets **1.1.9** Configuration standards for routers	1 firewalls deployed 1 firewall configurations stored 0 firewall configuration changes in the last 7 days 18 routers deployed 339 router configurations stored 5 router configuration changes in the last 7 days 16 configuration policies in place 59 violations of NSA Router Security Best Practices policy in last 7 days 0 approved firewall changes in the last 7 days 0 unapproved firewall changes in the last 7 days	Firewall List Active Firewall Configurations Firewall Configuration Changes Router List Active Router Configurations Router Configuration Changes Configuration Policies NSA Router Security Best Practices Violation Events Approved Firewall Changes Unapproved Firewall Changes
1.2 Build a firewall configuration that denies all traffic from "untrusted" networks/hosts, **except for**: **1.2.1** Web protocols - HTTP (port 80) and Secure	0 firewalls in configuration policy non-compliance 0 firewall configuration non-compliance events in the	Non-Compliant Firewalls

Как создать правило для проверки политики?





Определите название политики, правило, группу устройств через меню “New Policy”

Back

Edit Policy Rule

Notes:
* Required fields

Edit Policy Rule

*Rule Name: Minimum 2 Syslog receivers

*Rule Type: (•) Configuration ( ) Diagnostics ( ) Software

Rule Description:
Every IOS device must have a minimum of 2 Syslog event message receivers

Applies to devices with these drivers

( ) All Device Families

Device Family: Cisco IOS

(•) All applicable drivers

( ) Select specific drivers

- Cisco switches, Catalyst 2900XL & 3500XL series, IOS version 11.x
- Cisco switches, Catalyst 2950, 2970, 3550, 3750 & 8500 series, IOS version 12.x
- Cisco routers, 3600 series, IOS version 11.x
- Cisco routers, 7200 & 7500 series, IOS version 11.x

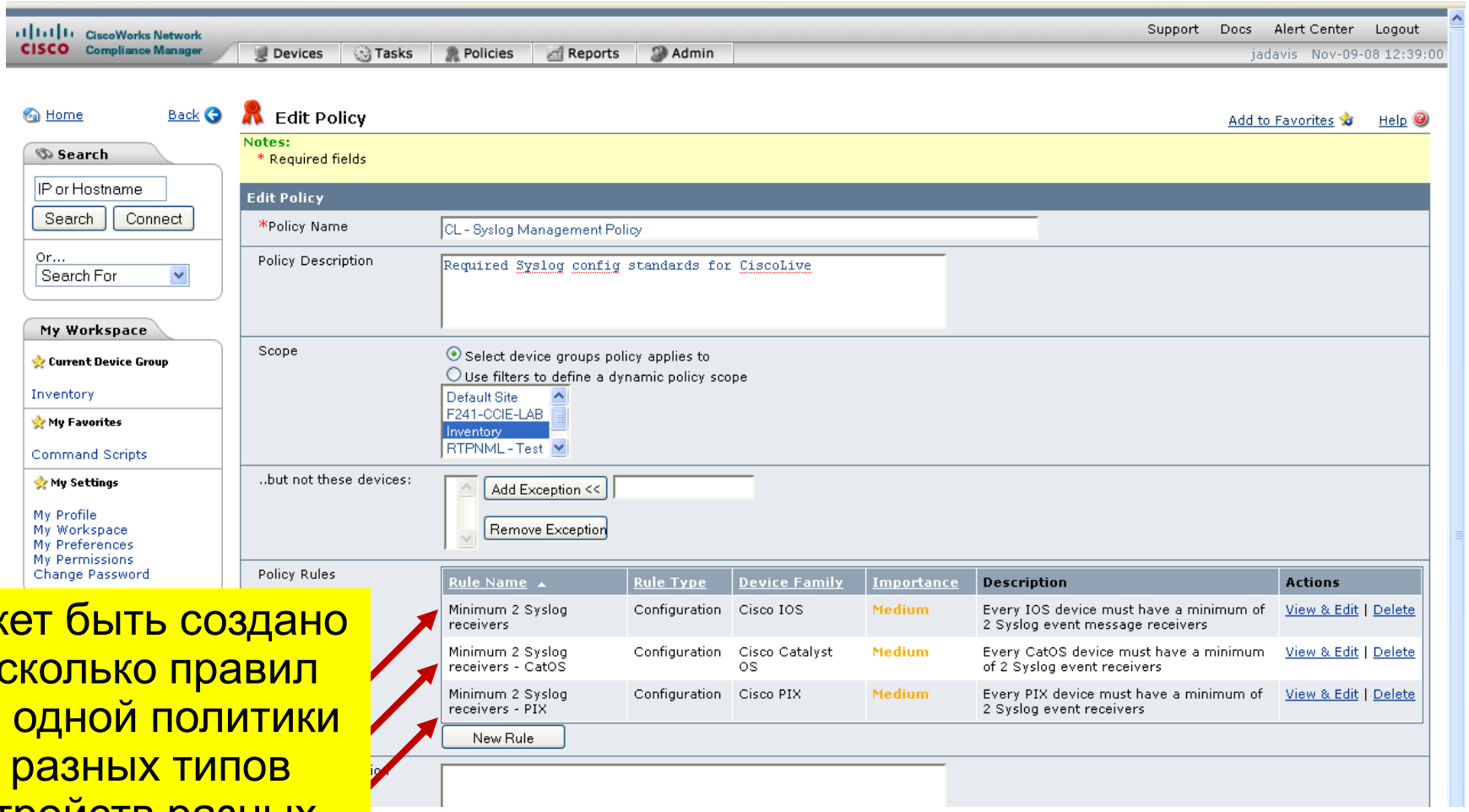
Define Text Block: [ ] Set Text Blocks to be used by rule conditions.

Tip: Use to check each single interface in IOS.

Rule Conditions

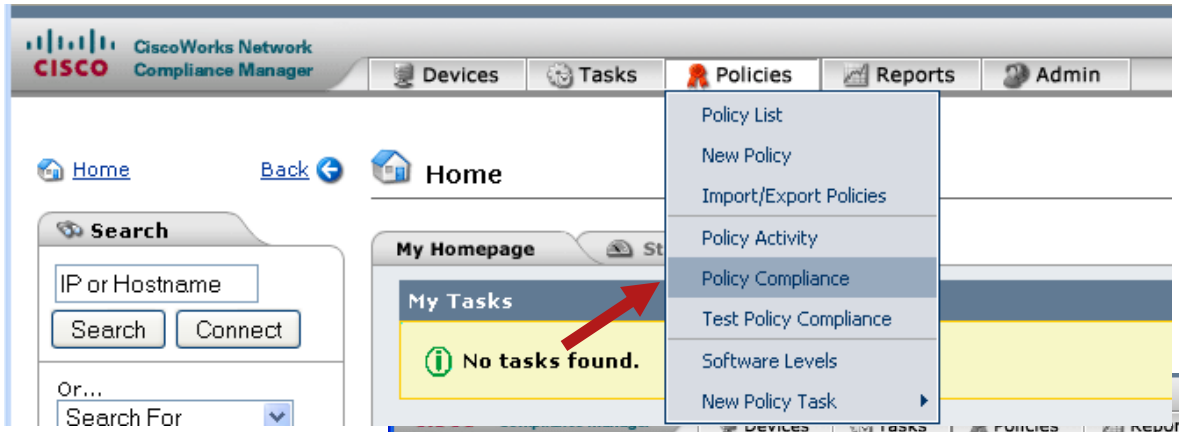
Conditions

A X [✓] Regular Expression [get help defining patterns.]

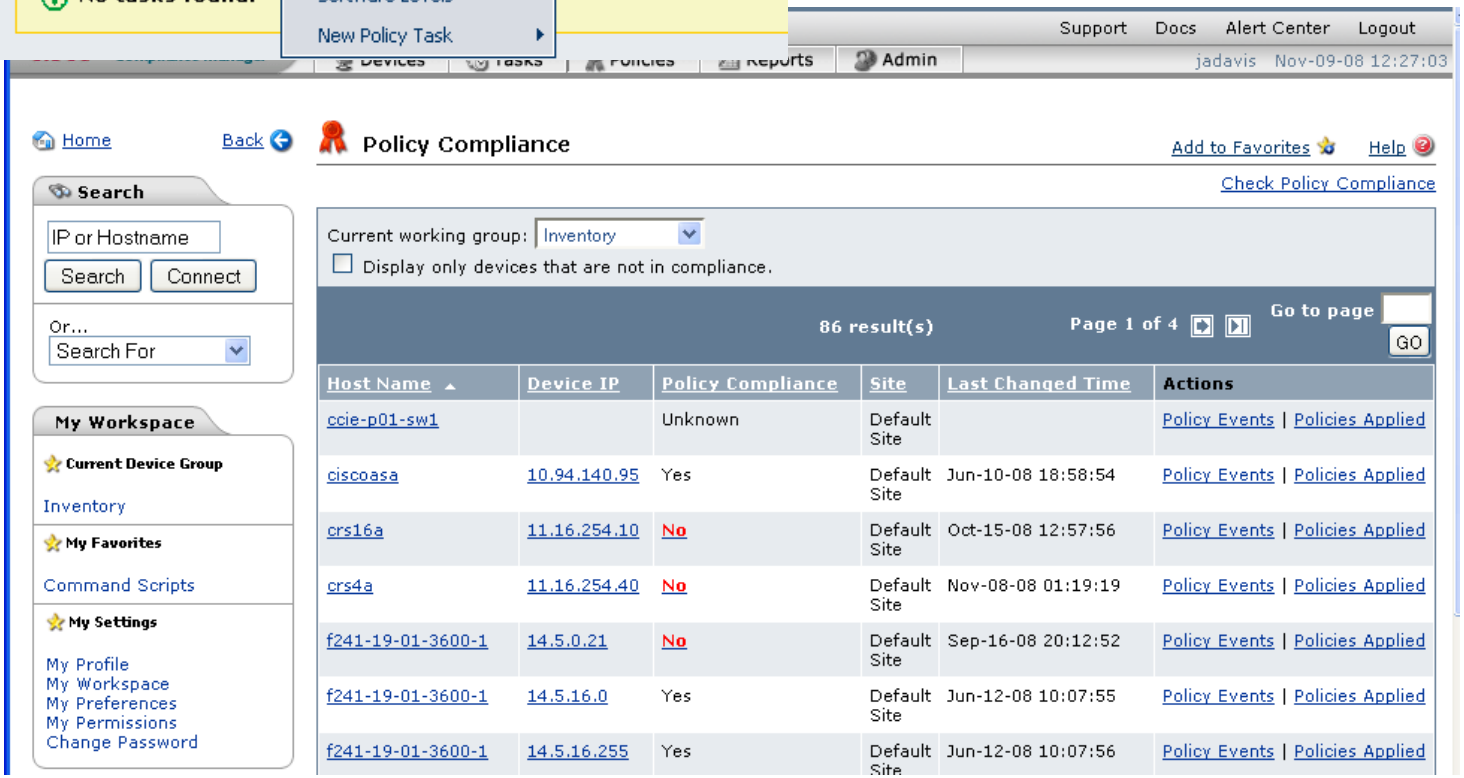


Может быть создано несколько правил для одной политики и разных типов устройств разных производителей.

Отчет по соответствию политикам



Просмотр периодических отчетов по соответствию политикам



NCM Alert Center

Что это такое?

Дополнительная услуга, которая позволяет пользователям NCM оперативно получать информацию о возможных ошибках и уязвимостях в функциях обеспечения безопасности

Предоставляемые функции:

Security Alerts – оповещения о возможных ошибках транслируются в политики NCM

Shared Product Extensions – получение и использование скриптов и новых политик

Functionality Updates – новые возможности появляются без ожидания выхода новой версии ПО

NCM Alert Center
На связи с Cisco

Автоматическое получение данных об уязвимостях

- Своевременное получение данных

Получение готовых политик

- Данные об уязвимостях в виде готовых политик
- Пользователь может выбрать политики, которые должны работать на сети

Быстрый поиск и исправление проблемы

- Автоматический поиск всех устройств с уязвимостями и вывод отчета
- NCM обеспечит исправление проблемы

Автоматическое извещение о проблемах

- Извещение о появлении новых проблем или новых устройств, установленных на сети со старыми проблемами

CiscoWorks LMS или NCM?

- NCM частично пересекается с LMS (инвентарные данные, управление конфигурациями и ПО)
- Преимущества NCM:
  - Поддержка 30+ производителей – CiscoWorks работает только с оборудованием Cisco
  - Масштабирование – архитектура NCM позволяет работать с гораздо большими сетями
  - Отчетность – в стандартной поставки предоставляются готовые отчеты по PCI DSS, ITIL, COBIT ...
  - Workflow – возможность создания алгоритмов согласования изменений
  - API – гибкие возможности по интеграции (SOAP, PERL, другие)
- Решения интегрируются и дополняют друг друга

Cisco Expo 2011

Инструменты контроля сетевого окружения.

Cisco NAM как средство оценки производительности

Патенко Владислав, инженер-консультант

vpatenko@cisco.com

Обзор функциональности Cisco NAM

Контроль производительности приложений

- Мониторинг времени отклика приложений
- Анализ результатов оптимизации WAN
- Анализ качества голосового трафика

Анализ трафика

- Анализ трафика по приложениям, устройствам, DSCP/QoS, VLAN, VRF
- Анализ сети с наличием VM

Диагностика

- Захват пакетов, декодирование, фильтрация и поиск ошибок
- Статистика по портам и интерфейсам

Cisco Nexus 1010 Appliance

Cisco Nexus 70xx series

Cisco Catalyst 65xx series

Cisco 76xx series

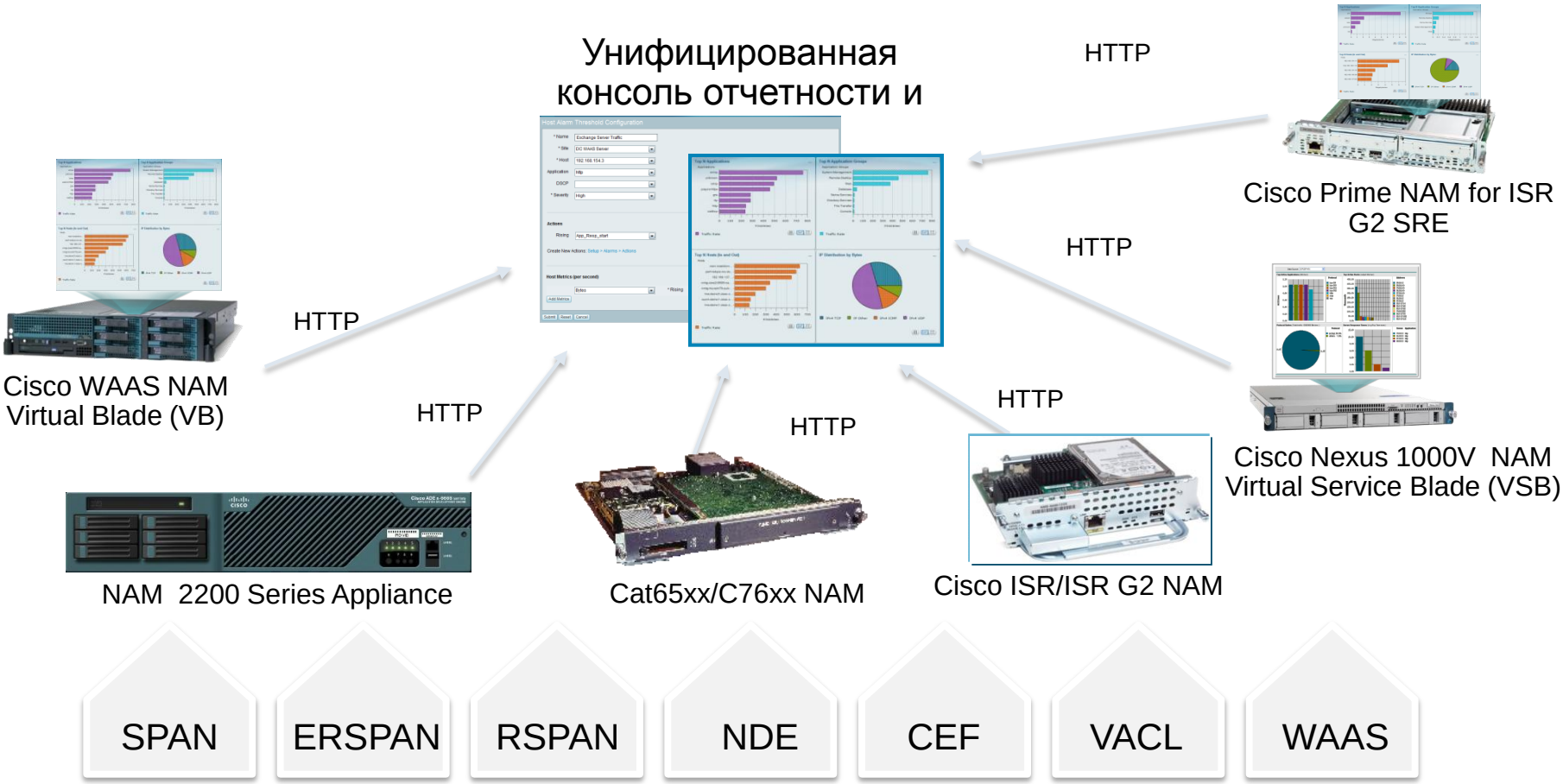
Cisco ISR / ISR G2

Cisco WAAS Appliances

Cisco Catalyst 4K series

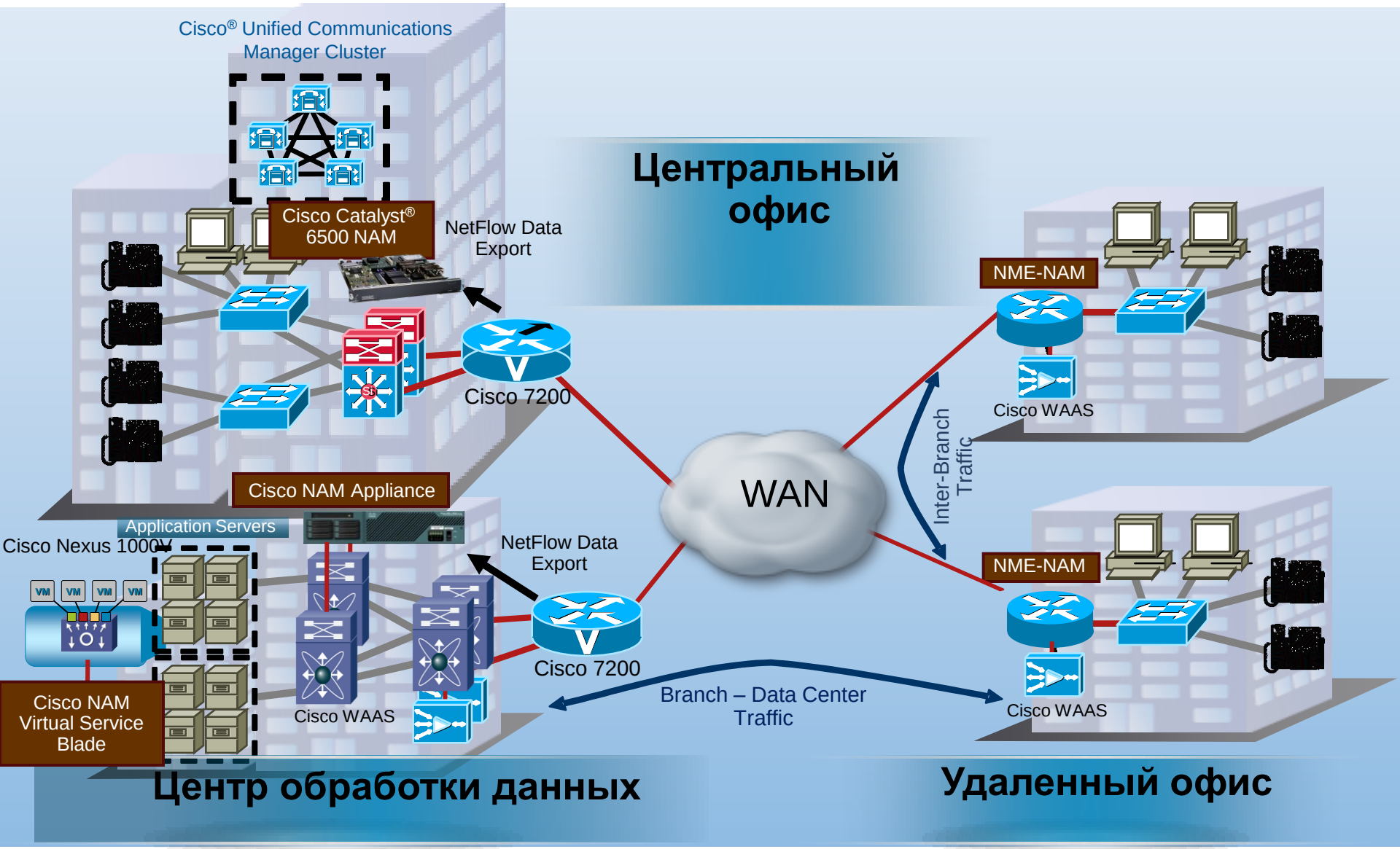
Гибкость в выборе платформы

Платформы и источники трафика

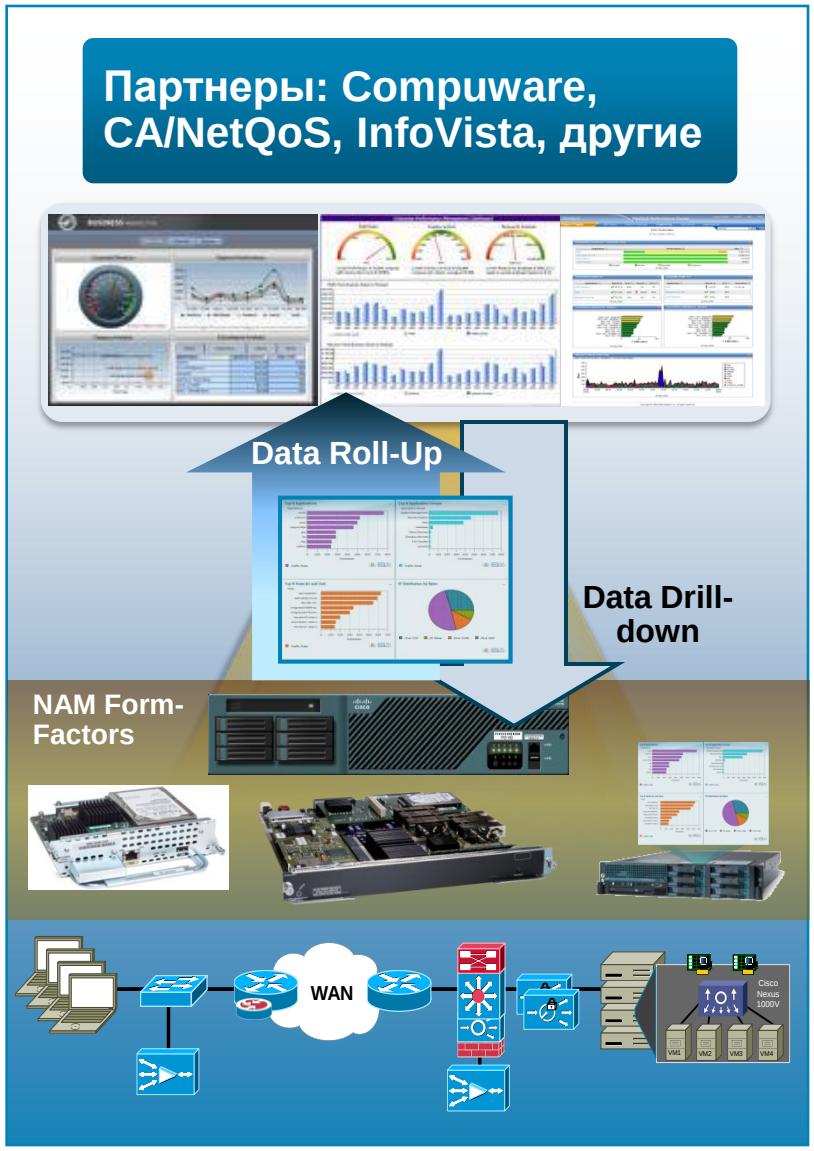


Унифицированная консоль управления и мониторинга одинаковая на всех платформах.

Возможные точки контроля
С учетом существующих архитектурных решений Cisco



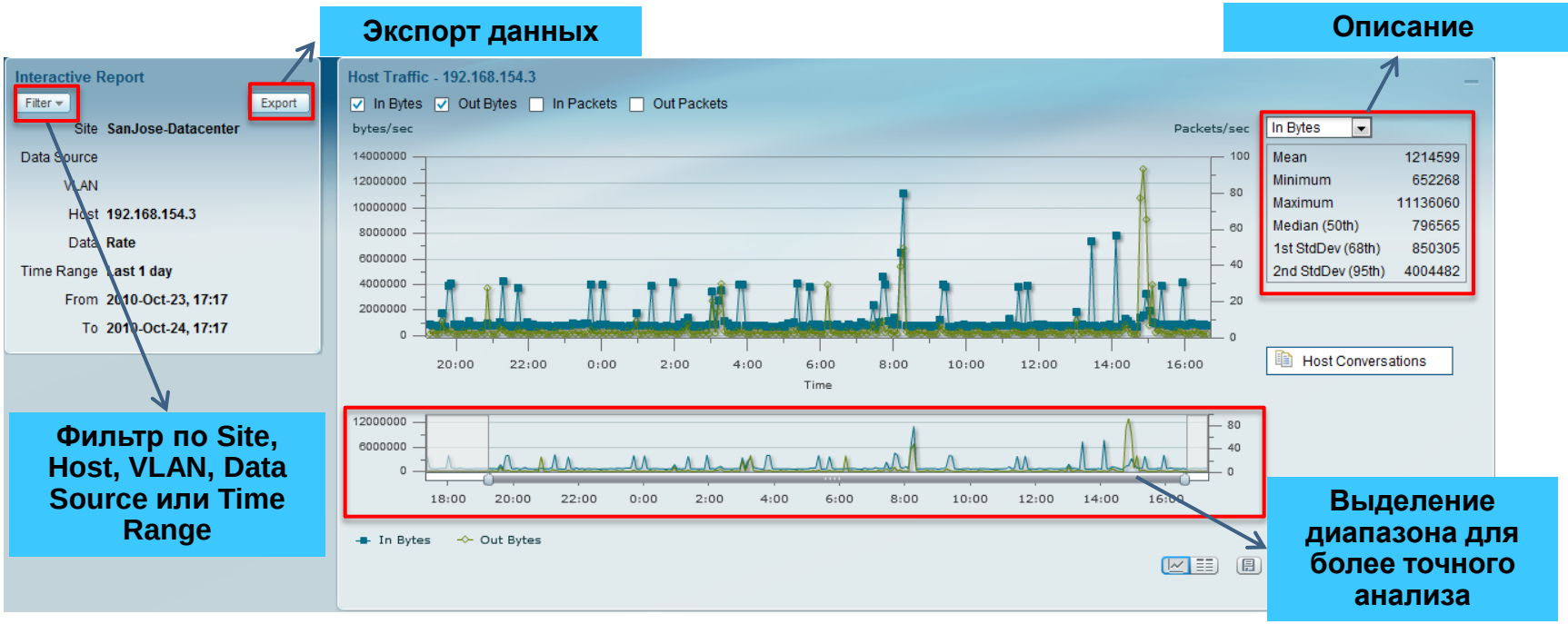
Централизованные системы отчетности



- Консолидация данных для контроля производительности сети
- Возможность получения детальных отчетов с NAM до уровня содержимого пакетов
- Диагностика

Интерактивная отчетность

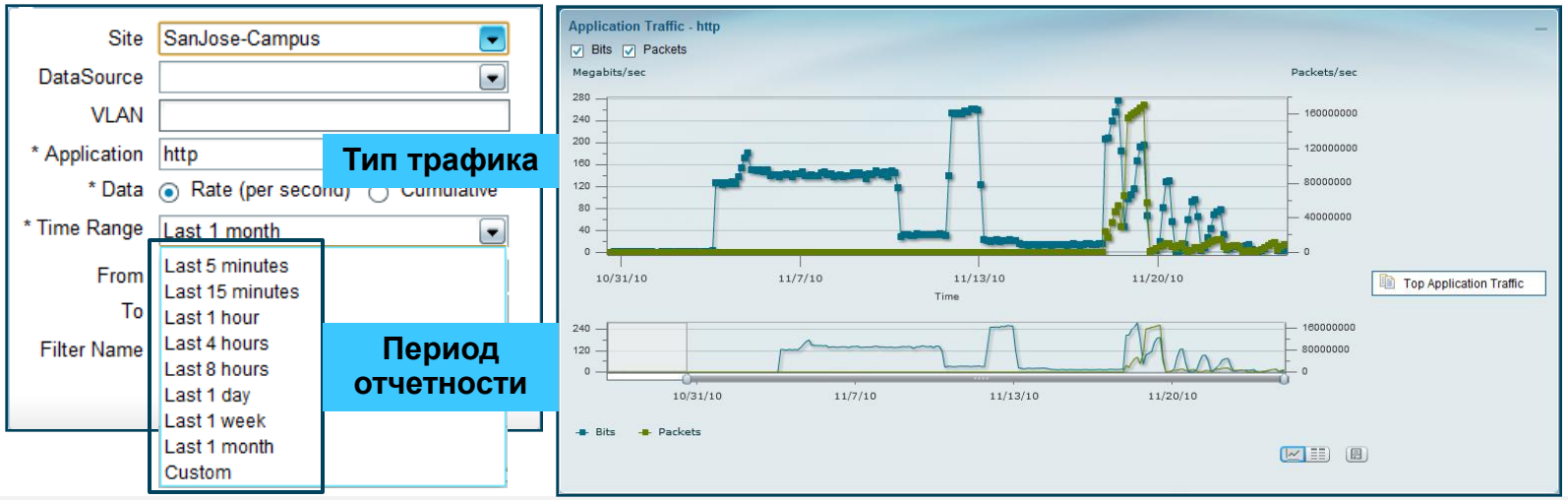
Быстрый доступ к важной информации



- Уменьшение времени идентификации и решения проблемы:
  - Выделение требуемого диапазона (zoom) и получение детализации
  - Гибкие фильтры
  - Визуальная корреляция данных
- Идентификация повторяющихся проблем и сохранение фильтров
- Экспорт данных для более детального анализа другими инструментами

Анализ исторических данных

Данные хранятся в встроенной базе данных



Функция:

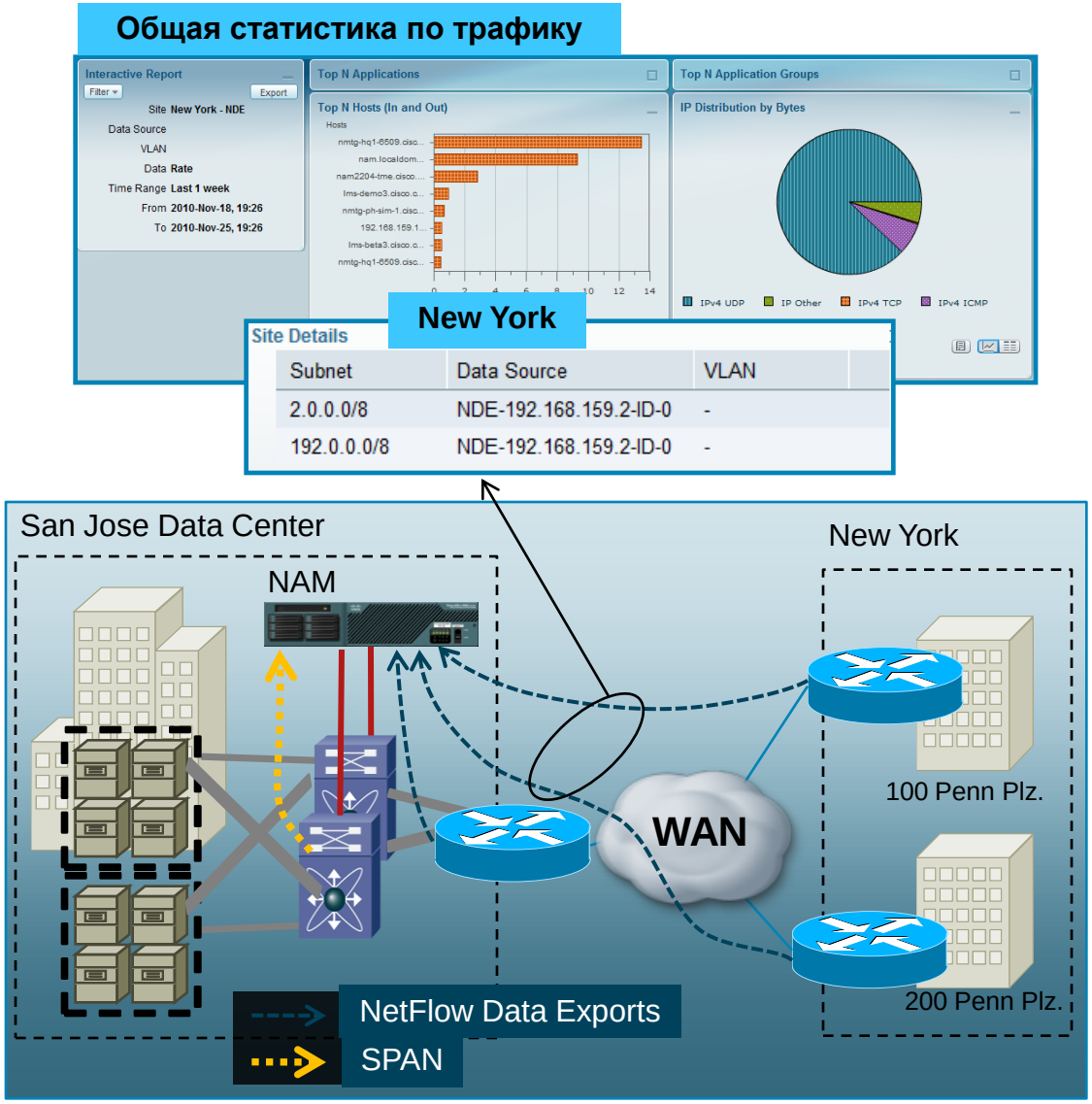
- Хранение всех данных до 72 часов с гранулярностью 1-5 мин и более длительный период с большей гранулярностью (1-2 часа)
- Интуитивно понятный интерфейс для дальнейшего анализа данных

Возможности:

- Анализ тенденций для диагностики проблем с производительностью
- Уменьшение времени поиска проблемы с доступом к детальным данных за последние 72 часа
- Надежный источник данных для принятия решений по оптимизации сети или настройке приложений.

Мониторинг удаленных офисов

Отражает топологию сети



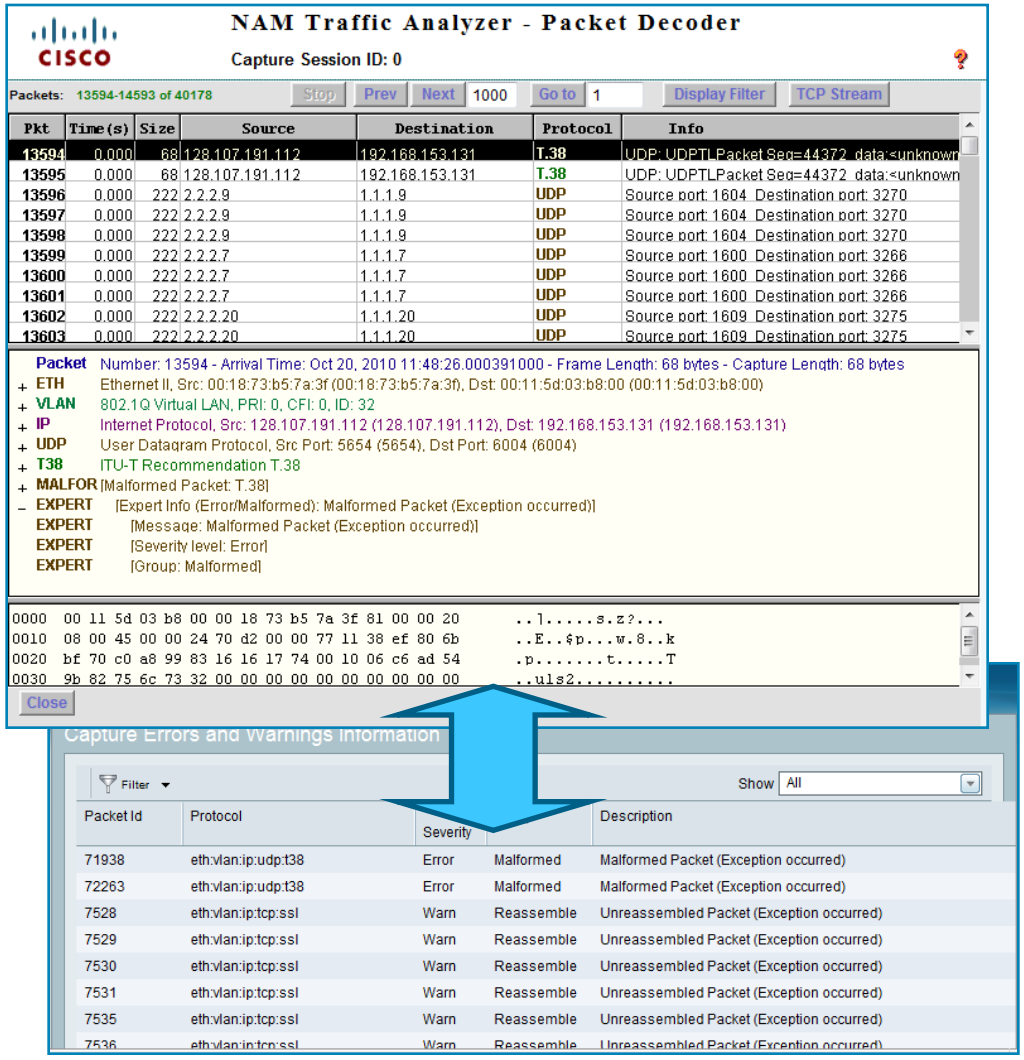
Функции:

- Создание офиса (Site) как группы узлов по IP адресу или сети, источника данных или VLAN
- Группировка данных по офису в одном окне (тип трафика, качество голоса, время отклика приложений, оптимизация WAN)

Возможности:

- Гибкая отчетность с группировкой данных по офисам, подразделениям
- Превентивное извещение о проблеме по граничным значениям для каждого офиса

Сканирование ошибок пакетов
Highlights observed Protocol/Packet level Anomalies



Функции:

- Анализ пакета и подсветка аномальных пакетов
- Получение детализации по пакетов одним щелчком мыши

Возможности:

- Повышение эффективности работы службы эксплуатации – возможность записи трафика по событию
- Подсветка ошибок позволяет сэкономить время на анализе данных

Анализ времени отклика приложения
Аналитика для анализа TCP- приложений

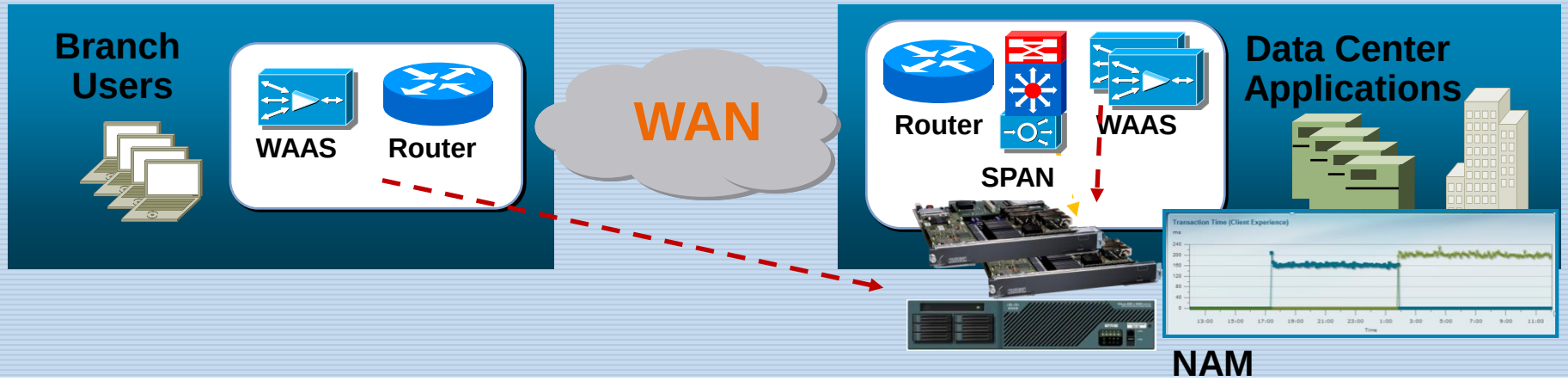
- **Детальная статистика по сессиям и транзакциям – более 45 параметров**

- Data-transfer time
- Transaction time
- Connection duration
- Number of bytes and packets retransmitted
- Retransmission delay
- Acknowledgement delay
- Number of open connections
- Number of closed connections
- Number of refused connections
- Number of unresponsive connections
- And more…

Мощное средство для мониторинга приложений

Контроль эффективности оптимизации WAN

Интегрированное решение с Cisco WAAS



Функции:

- Отчетность по производительности приложений в реальной режиме времени на всех сегментах WAAS
- Детальные отчеты по времени отклика приложений, загрузке каналов, и другим параметрам
- Статистика по оптимизированным и неоптимизированным приложениям

Возможности:

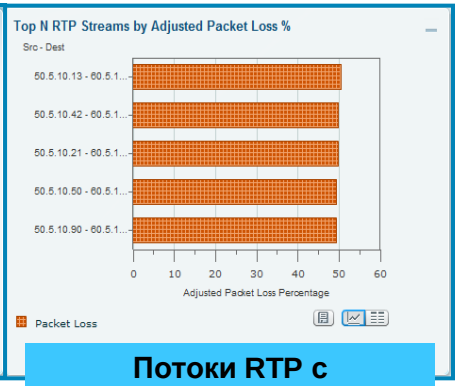
- Идентификация приложений для оптимизации
- Учет эффективности работы Cisco WAAS
- Увеличение эффективности работы служб эксплуатации по решению проблем

Анализ качества голосового трафика

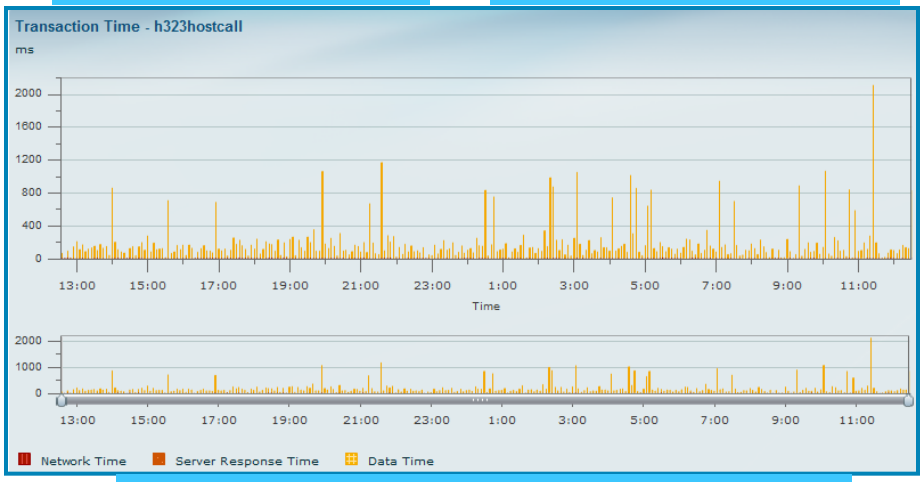
Мониторинг и диагностика в реальном режиме времени

- Мониторинг MOS (базируется на рекомендациях ITU-T G.107)
- Анализ потоков RTP в реальном режиме времени
- Быстрый поиск проблемных направлений
- Диагностика проблем с производительностью с использованием статистики по интерфейсам, DSCP, детальный анализ пакетов
- Время отклика для сигнальных протоколов на базе TCP, например SCCP, SIP

Устройства (телефоны) с низким MOS



Потоки RTP с наибольшей потерей пакетов (%)

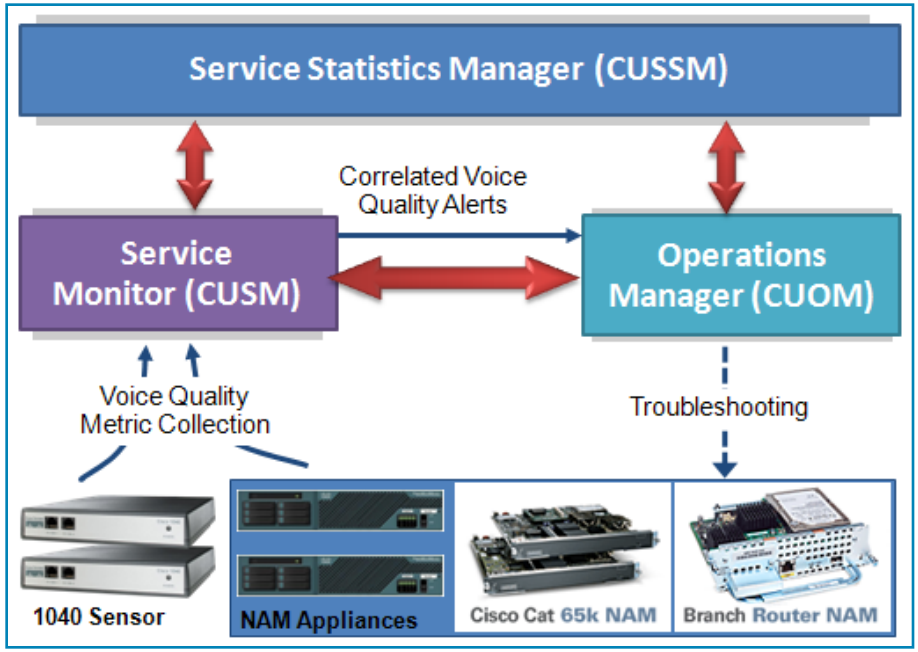


Время транзакции H.323 - последние 24 часа

Централизованная отчетность по качеству голосового трафика

Интеграция с Cisco Unified Communication Management Suite

- В реальном режиме времени по всей сети
- Превентивные извещения по проблемам с качеством голосовых услуг
- Детальная информация с NAM для диагностики
- Масштабируемые и гибкое решение – возможность снять статичтику в любой точке сети



Cisco NAM дополняет CUCMS для получение комплексного решения по мониторингу услуг передачи голоса

Контроль виртуальных машин

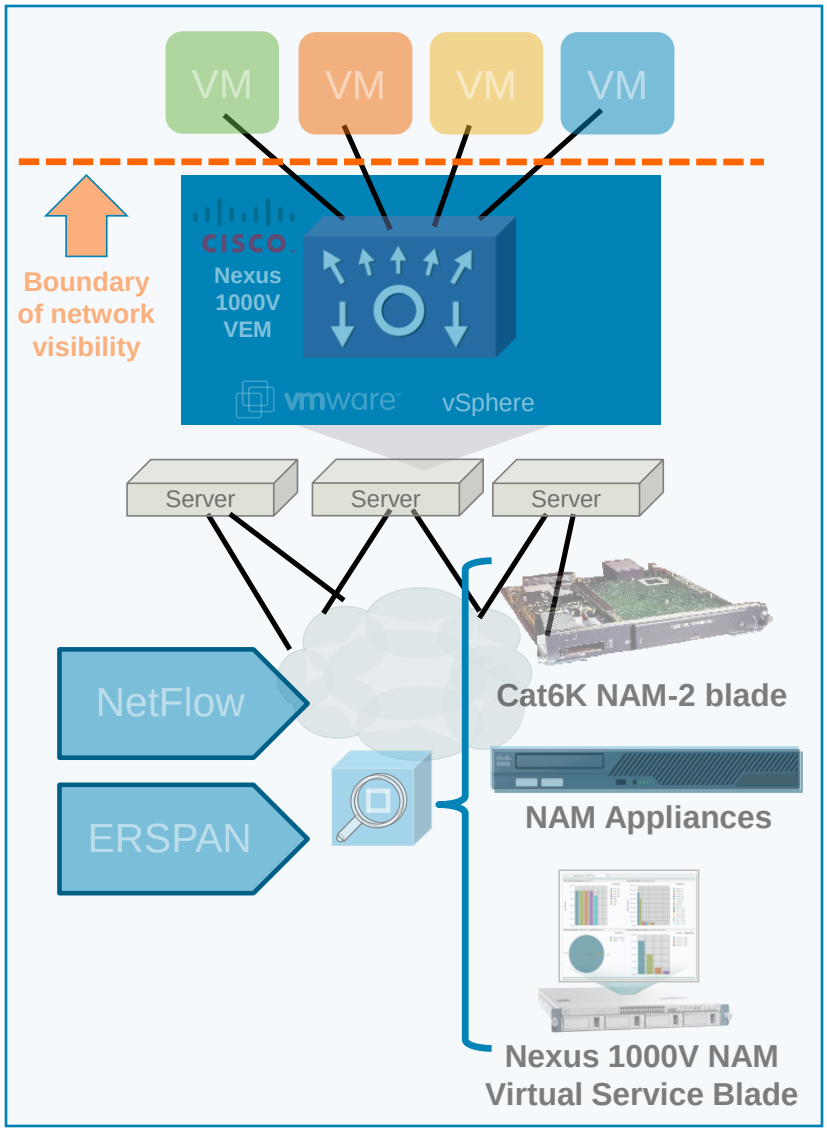
Интеграция NAM и коммутатора Nexus 1000V

Функции:

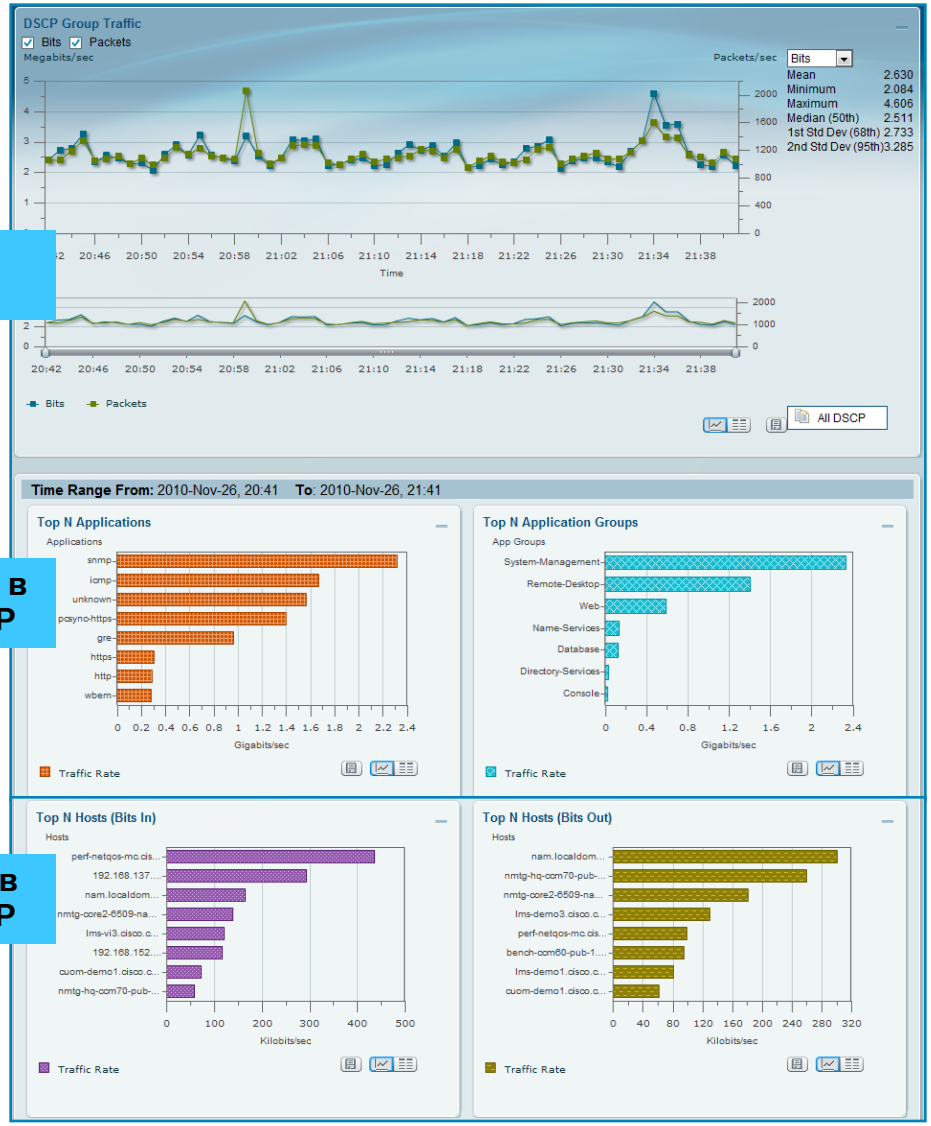
- Детальный анализ трафика по виртуальной машине, VLAN, DSCP, приложению , и т.д.
- Статистика как по физическим, так и виртуальным серверам
- Мониторинг виртуальных интерфейсов
- Мониторинг виртуальной машины во время миграции с VMotion

Возможности:

- Гибкие возможности по визуализации трафика с виртуальных машин
- Учет проблем с производительностью из-за миграции или изменений конфигурации.



Анализ DiffServ



Трафик с DSCP0

Приложения в группе DSCP

Устройства в группе DSCP

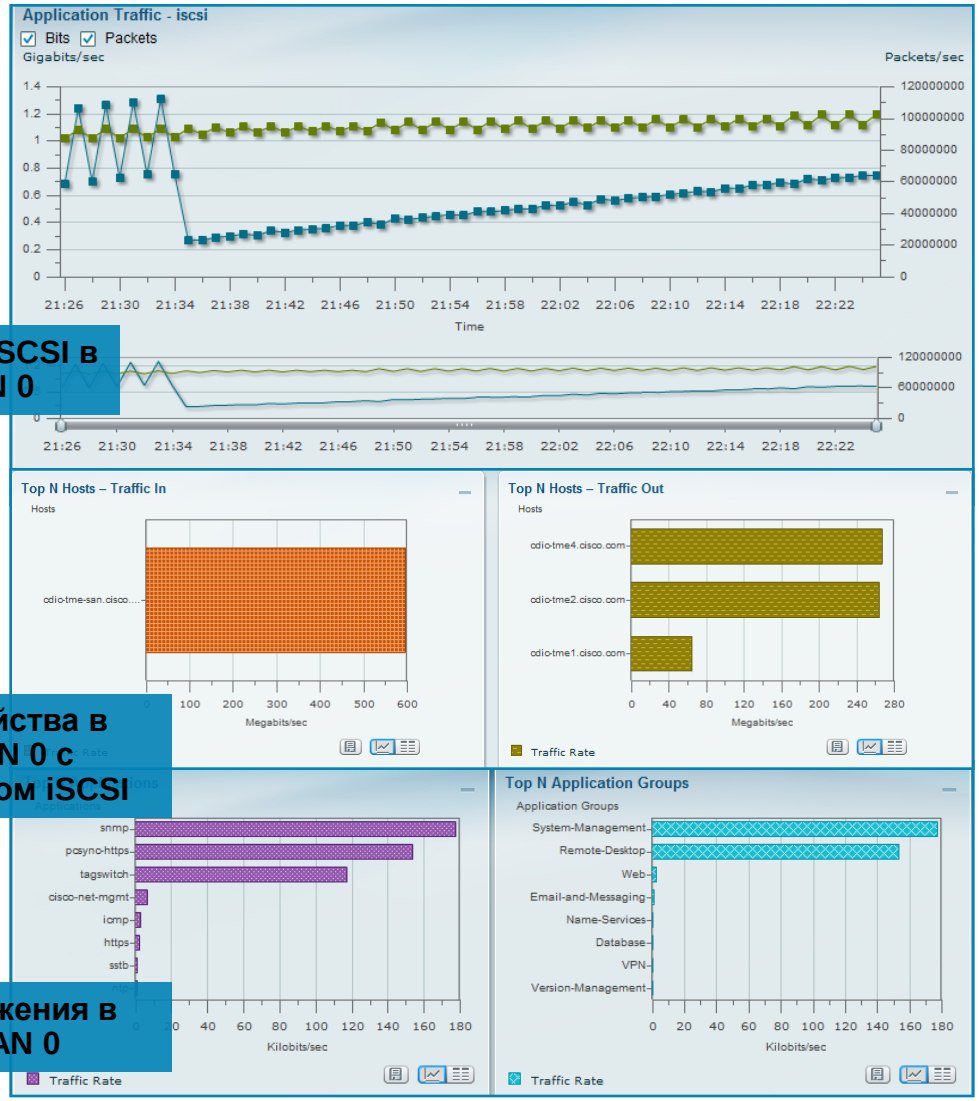
Функция:

- Визуализация трафика по узлам и приложениям для каждого DSCP
- Агрегация трафика по каждому DSCP

Возможности:

- Проверка правильности планирования и внедрения QoS
- Определение неучтенного трафика, или трафика с неправильным DSCP

Анализ трафика VLAN



Трафик iSCSI в VLAN 0

Устройства в VLAN 0 с трафиком iSCSI

Приложения в VLAN 0

Функции:

- Просмотр всех VLAN по количеству трафика
- Анализ трафика VLAN :
  - Приложения
  - Узлы
  - Потоки
  - Качество голоса
  - Время отклика приложений

Возможности:

- Мониторинг трафика в каждом контролируемом VLAN
- Поиск некорректных назначений виртуальных машин (интерфейсов) и VLAN

Дополнительная информация

- Документация, презентации, описания

  NAM: http://www.cisco.com/go/nam

  NCM: http://www.cisco.com/go/ncm

- Демонстрационные версии

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

Вопросы и Ответы

Мы хотели бы узнать Ваше мнение

Пожалуйста, заполните анкету