



Cisco Expo 2009

Управление конфигурациями сетевых устройств и их соответствием нормативам и стандартам



Владислав Патенко

Системный инженер-консультант по системам управления

Содержание

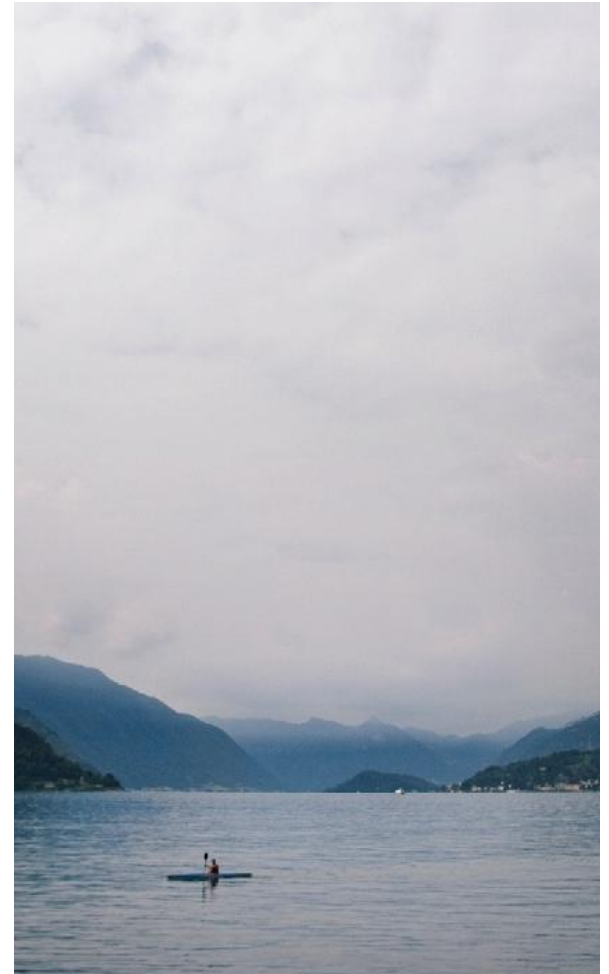
1. Зачем необходим контроль конфигурации оборудования?
2. Примеры нормативных требований
3. Как обеспечить контроль соответствия стандартам?
4. Комплексное решение - PACE
5. Обзор Cisco Network Compliance Manager
6. Функции контроля соответствия стандартам в CiscoWorks LAN Management Solution

Когда задача становится актуальной?

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

Результаты аудита сетей:

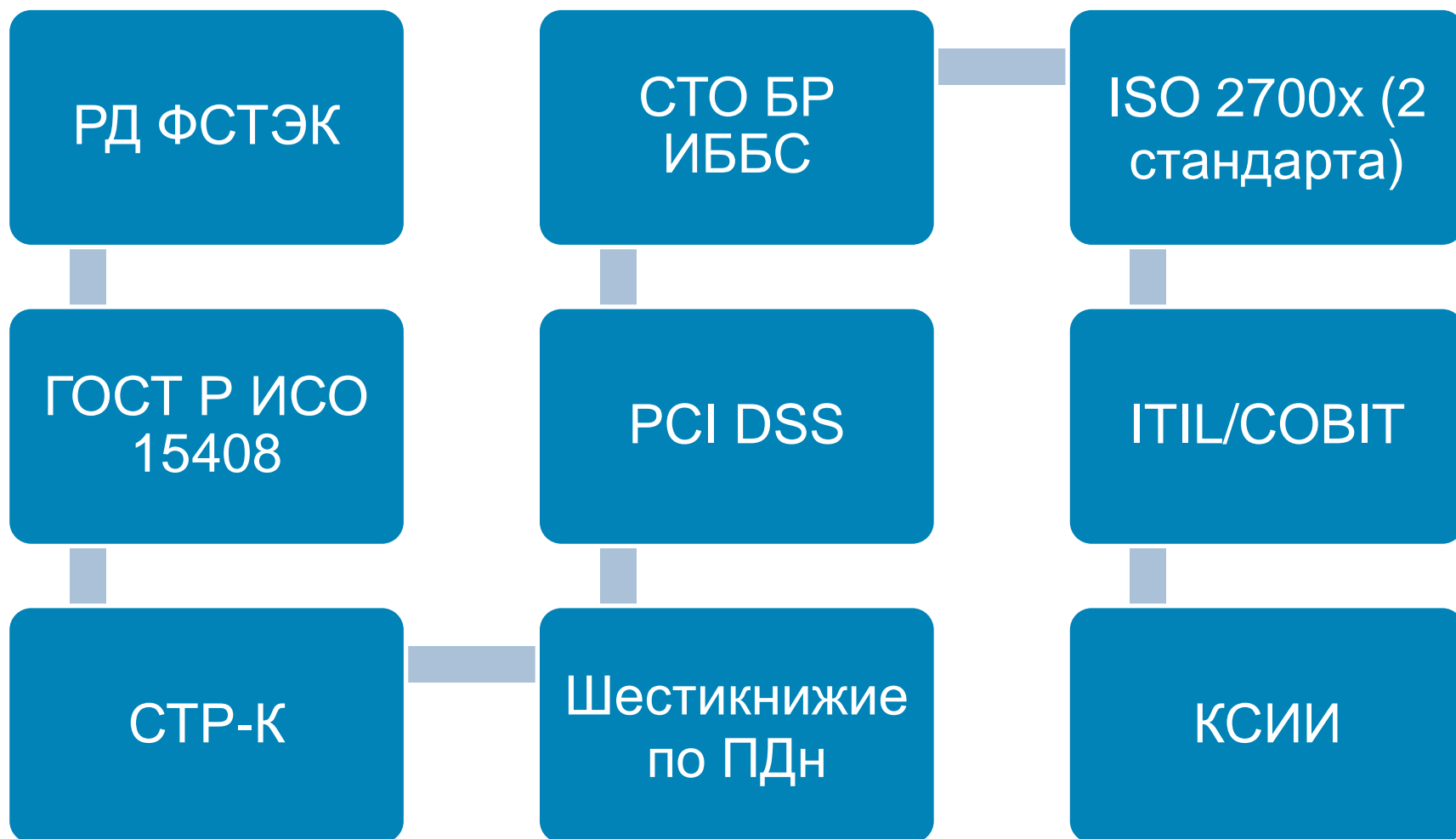
- 47% изменений не учтены
- 60% простоев связаны с человеческими ошибками



Нормативные документы



Распространенные в РФ требования ИБ



...

Пример требований - PCI DSS

<p>PCI DSS</p> <p>Стандарт защиты информации в индустрии платежных карт</p>	<p>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</p>
<p>Пример требований</p>	<p>Требование 2.1: Не использовать значения по умолчанию для паролей и других параметров безопасности</p>
<p>Как может быть достигнуто?</p>	<p>Проверка конфигурации на использование стандартных значений 'public', 'private', 'cisco' в SNMP; 'cisco', 'cisco123', 'sdm' для доступа через WEB (например, SDM)</p>

Пример требований - ITIL

<p>ITIL IT Infrastructure Library</p>	<p>Набор рекомендаций к процессам управления ИТ услугами, инфраструктурой, внедрения и эксплуатации. Разработаны по заказу Британского правительства</p> <p>Опубликован в нескольких книгах.</p>
<p>Пример требований</p>	<p>“7.9.1 Система управления конфигурациями. Система управления конфигурациями должна обеспечивать контроль доступа к информации”</p>
<p>Как может быть достигнуто?</p>	<p>Настройка и проверка использования AAA в конфигурации оборудования и RBAC в информационных системах</p>

Пример требований - COBIT

<p>COBIT</p> <p>Control Objectives for Information and related Technology</p>	<p>Набор рекомендаций для ИТ, созданный организацией Information Systems Audit and Control Association (ISACA) и IT Governance Institute (ITGI) в 1992. COBIT предоставляет руководителям, аудиторам и пользователям ИТ набор измерений, индикаторов, процессов и лучшие практики, который помогают измерить и оптимизировать эффективность работы ИТ.</p>
<p>Пример требования</p>	<p>DS4 постоянная проверка доступности сервиса.</p>
<p>Как может быть достигнуто?</p>	<p>Использовать средство контроля услуг IPSLA . Контроль состояния интерфейсов через отсылку SNMP trap и syslog. Запуск периодических текстов на оборудовании (EEM, Gold и другие механизмы)</p>

Пример корпоративных требований

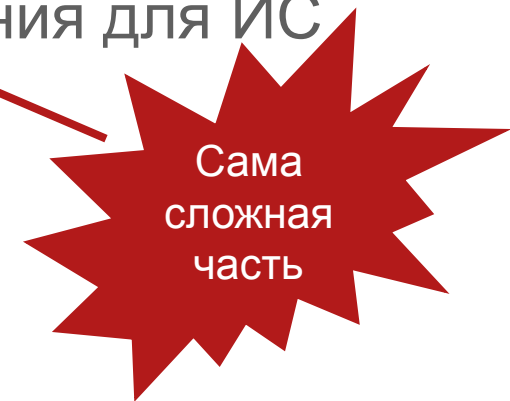
Управление	“На каждом устройстве должно быть настроено как минимум 2 получателя сообщений Syslog и SNMP trap”
Управление	“Не более 4 получателей Syslog”
Управление	“Не должны использоваться «популярные» значения SNMP community”
Управление	“Для доступа по SNMP должны использоваться ACL”
Безопасность	“На 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”

Как обеспечить контроль соответствия стандартам?



С чего начать?

1. Определить нормативные документы, которым должна соответствовать инфраструктура ИТ
2. Определить специфические требования для ИС
3. Проконсультироваться с аудиторами
4. Спроектировать систему контроля
5. Внедрить систему
6. Аудит инфраструктуры на соответствие стандартам
7. Постоянное усовершенствование системы



Что значит процесс контроля для служб ИТ?

1. Постоянный сбор данных

- Инвентарной информации
- Конфигурации устройств

Много людей останавливаются на этом этапе

2. Проверка характеристик функционирования устройств

3. Средства управления должны обеспечивать:

- Сбор
- Проверка данных
- Отчетность
- Ежедневно, в постоянном режиме



Какие решения предлагает Cisco?

1. CiscoWorks Network Compliance Manager (NCM)

Поддержка разных производителей

Поставляется с настройками для некоторых стандартов

2. EMC VoyenceControl

Альтернатива NCM

3. CiscoWorks LAN Management Solution (LMS)

Решение часто уже установлено у пользователей

Может выполнять простые функции контроля файлов конфигурации

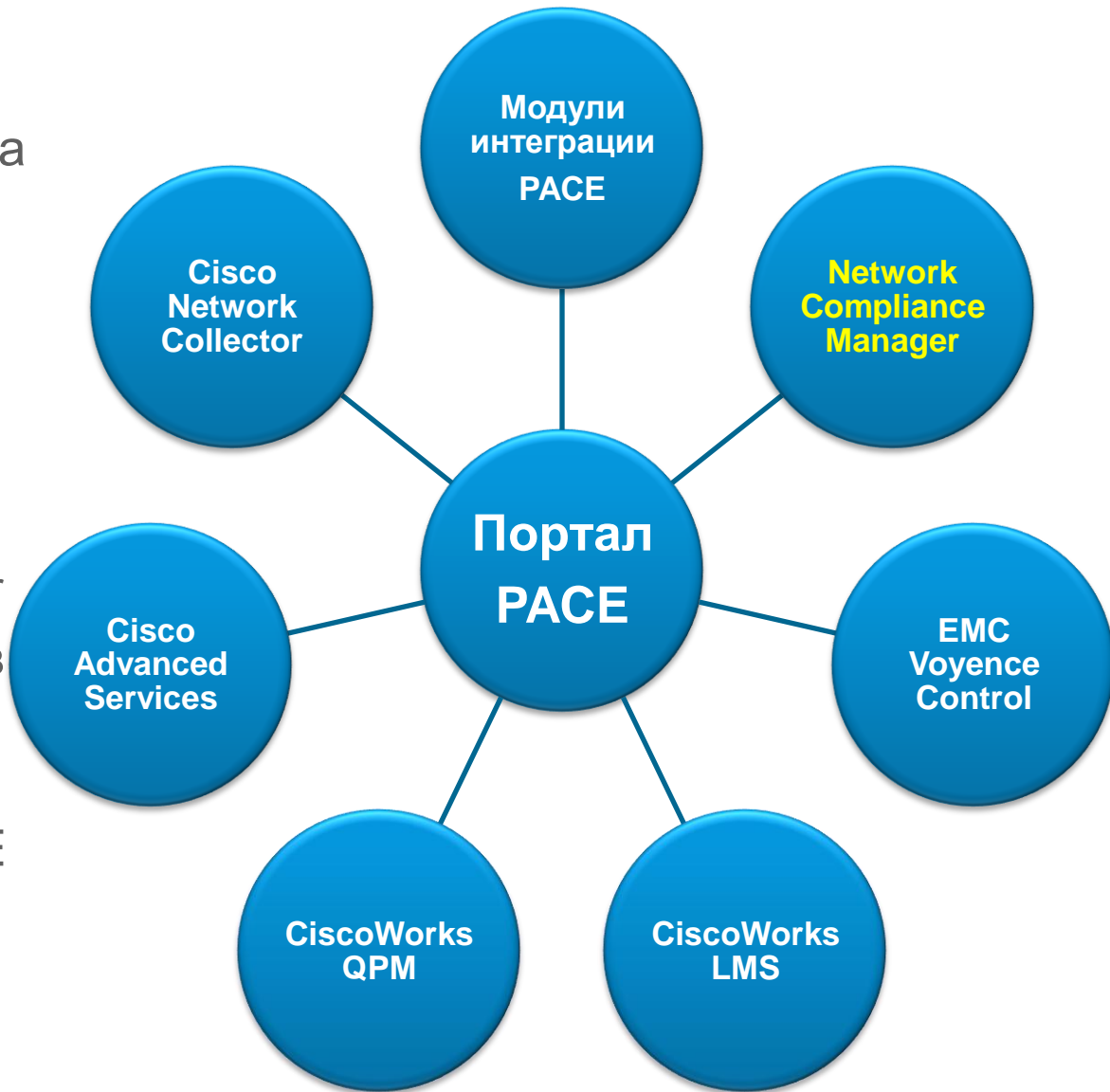
PACE 2.0. Обзор решения

PACE Portal – единая точка получения данных с систем

- CiscoWorks LMS
- Network Compliance Manager
- QoS Policy Manager
- Cisco Network Collector

Поставляется бесплатно в составе NCM

Услуги Cisco AS – опциональная часть PACE



Обзор Cisco Network Compliance Manager



CiscoWorks Network Compliance Manager (NCM)

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

Аудит и анализ соответствия стандартам и нормативам

- Контроль выполнения стандартов и нормативов на сети
- Оперативная отчетность

Согласование изменений

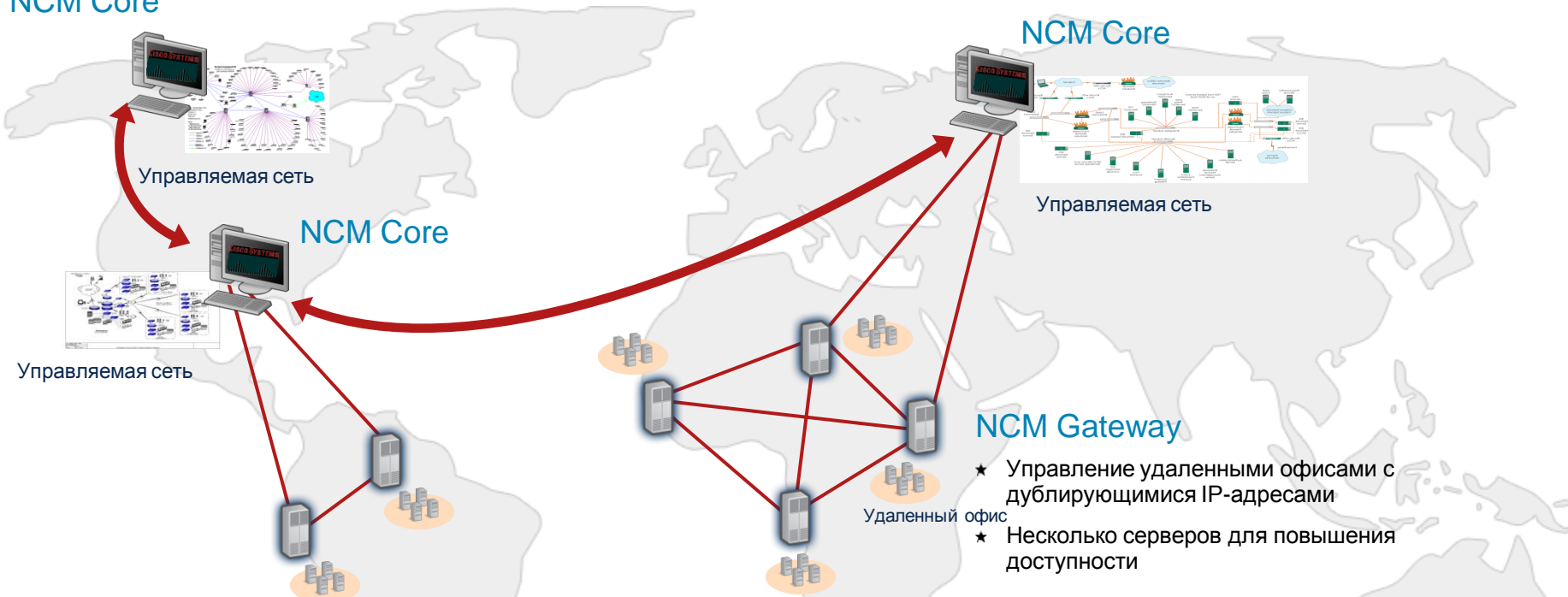
- Настройка правил согласования
- Возможность настройки сложных правил

The image displays three overlapping screenshots of the CiscoWorks Network Compliance Manager (NCM) web interface. The top screenshot shows the 'Compare Device Configurations' page, comparing an older configuration with the current one for device Contivik400. The middle screenshot shows the 'Workflow Setup' page, specifically the 'Step 3: Manage Approval Rules' section. The bottom screenshot shows the 'Statistics Dashboard' with various charts and tables, including 'Top 5 Vendors', 'Top 10 Most Accessed Devices', and 'System Status'.

Возможности по отказоустойчивости

Конфигурация Active/Active через репликацию базы данных

NCM Core



Управляемая сеть

NCM Core

NCM Core

Управляемая сеть

NCM Gateway

- ★ Управление удаленными офисами с дублирующимися IP-адресами
- ★ Несколько серверов для повышения доступности

Удаленный офис

Отказоустойчивость NCM

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

Компоненты

- ★ Core
- ★ HA
- ★ Gateway

Ключевые возможности

- ★ Безопасность, масштабируемость
- ★ Нет единой точки отказа
- ★ Удаленное управление устройствами— даже в сетях с дублированием IP адресов

NCM: Поддерживаемые платформы

Поддерживаемые серверные платформы:

- Windows Server
- Solaris
- Linux RedHat ES/AS
- SUSE Enterprise Linux

Поддерживаемые СУБД:

- Oracle
- MySQL
- Microsoft SQL

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...

The screenshot displays the CiscoWorks Network Compliance Manager (NCM) interface. At the top, there is a navigation bar with tabs for 'Devices', 'Tasks', 'Policies', 'Reports', and 'Admin'. The user is logged in as 'jadavis' on 'Nov-09-08 12:21:53'. The main content area is titled 'Compliance Center - Home' and features a search bar with 'IP or Hostname' and 'Search' and 'Connect' buttons. Below the search bar is a 'My Workspace' sidebar with links to 'Current Device Group', 'Inventory', 'My Favorites', 'Command Scripts', and 'My Settings'. The main content area is titled 'Compliance Center' and contains introductory text, a 'Compliance Reporting' section with a bulleted list of standards, and a vertical list of standard-specific links on the right side.

Compliance Center - Home

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

CiscoWorks Network Compliance Manager provides powerful capabilities for managing compliance with government regulations and industry standards for IT processes and best practices.

The Compliance Center is CiscoWorks Network Compliance Manager's portal for accessing reports and information that help determine the compliance status of your network resources.

Compliance Reporting

The Compliance Center provides reports detailing the current compliance status of your network infrastructure with respect to the government regulations and industry standards:

- Sarbanes-Oxley (Section 404)
- COBIT
- COSO
- ITIL
- GLBA
- HIPAA
- Visa CISP(PCI Data Security Standard)

Use the links at right to view the individual compliance reports.

Sarbanes-Oxley (Section 404)
The Public Company Accounting Reform and Investor Protection Act of 2002
[Compliance Status](#)

COBIT
Control Objectives for Information and related Technology
[Compliance Status](#)

COSO
Committee of Sponsoring Organizations of the Treadway Commission
[Compliance Status](#)

ITIL
IT Infrastructure Library
[Compliance Status](#)

GLBA
Gramm-Leach-Bliley Financial Modernization Act
[Compliance Status](#)

HIPAA
Health Insurance Portability and Accountability Act
[Compliance Status](#)

Стандарты и отчеты

Пример отчета по PCI DSS

The screenshot displays the CiscoWorks Network Compliance Manager interface. The top navigation bar includes links for Support, Docs, Alert Center, and Logout, along with user information (jadavis) and a timestamp (Nov-09-08 12:23:52). The main content area is titled "Compliance Center - Visa CISP" and features a search bar, a "Compliance Center Home" link, and several compliance standards tabs: Sarbanes-Oxley (Section 404), COBIT, COSO, ITIL, GLBA, HIPAA, and Visa CISP. The "Visa CISP(PCI Data Security Standard) Compliance Status" section includes an "Email Report" link and a detailed description of the standard. Below this, a section titled "Build and Maintain a Secure Network" lists "Requirement 1: Install and maintain a firewall configuration to protect data". A table provides a summary of the compliance status for this requirement.

Specification	Status	More Information
1.1 Establish firewall configuration standards that include:	1 firewalls deployed	Firewall List
1.1.1 A formal process for approving	1 firewall configurations stored	Active Firewall Configurations

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

Как создать правило для проверки?

The image shows two screenshots from the CiscoWorks Network Compliance Manager interface. The left screenshot shows the 'Policies' menu with 'New Policy' highlighted by a red arrow. The right screenshot shows the 'New Policy' configuration form with the following details:

- Policy Name:** CL - Syslog Management Policy
- Policy Description:** Required Syslog config standards for CiscoLive
- Scope:** Select device groups policy applies to (selected), Use filters to define a dynamic policy scope (unselected). Device groups include Default Site, F241-CCIE-LAB, Inventory, and RTPNML - Test.
- Policy Rules:** New Rule button
- Policy Status:** Active (selected), Inactive (unselected)
- Additional Policy Fields:** CVE, Vendor Advisory URL, Vendor Solution URL, Disclosure Date (with format hint: Edit using yyyy-MM-dd format), Solution.

Save button at the bottom right.

Определите название политики, правило, группу устройств через меню "New Policy"

[Back](#)

Edit Policy Rule

[Ad](#)

Notes:
* Required fields

Edit Policy Rule

*Rule Name

*Rule Type Configuration Diagnostics Software

Rule Description

Applies to devices with these drivers

All Device Families

Device Family

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

Regular Expression [\[get help defining patterns.\]](#)

Home Back

Edit Policy

Add to Favorites Help

Search

IP or Hostname

Or...

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

Notes:
 * Required fields

Edit Policy

*Policy Name

Policy Description

Scope
 Select device groups policy applies to
 Use filters to define a dynamic policy scope

Default Site

..but not these devices:

Policy Rules

Rule Name	Rule Type	Device Family	Importance	Description	Actions
Minimum 2 Syslog receivers	Configuration	Cisco IOS	Medium	Every IOS device must have a minimum of 2 Syslog event message receivers	View & Edit Delete
Minimum 2 Syslog receivers - CatOS	Configuration	Cisco Catalyst OS	Medium	Every CatOS device must have a minimum of 2 Syslog event receivers	View & Edit Delete
Minimum 2 Syslog receivers - PIX	Configuration	Cisco PIX	Medium	Every PIX device must have a minimum of 2 Syslog event receivers	View & Edit Delete

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

Отчет по соответствию политикам

The screenshot shows the CiscoWorks Network Compliance Manager interface. The top navigation bar includes 'Devices', 'Tasks', 'Policies', 'Reports', and 'Admin'. The 'Policies' menu is open, showing options like 'Policy List', 'New Policy', 'Import/Export Policies', 'Policy Activity', 'Policy Compliance', 'Test Policy Compliance', 'Software Levels', and 'New Policy Task'. A red arrow points to the 'Policy Compliance' option. Below the menu, a 'My Tasks' section displays 'No tasks found.' with an information icon.

Просмотр периодических отчетов по соответствию политикам

The screenshot shows the 'Policy Compliance' report page. The page title is 'Policy Compliance'. The current working group is 'Inventory'. There is a checkbox for 'Display only devices that are not in compliance.' The report shows 86 results, displayed as Page 1 of 4. The table below lists the devices and their compliance status.

Host Name	Device IP	Policy Compliance	Site	Last Changed Time	Actions
ccie-p01-sw1		Unknown	Default Site		Policy Events Policies Applied
ciscoasa	10.94.140.95	Yes	Default Site	Jun-10-08 18:58:54	Policy Events Policies Applied
crs16a	11.16.254.10	No	Default Site	Oct-15-08 12:57:56	Policy Events Policies Applied
crs4a	11.16.254.40	No	Default Site	Nov-08-08 01:19:19	Policy Events Policies Applied
f241-19-01-3600-1	14.5.0.21	No	Default Site	Sep-16-08 20:12:52	Policy Events Policies Applied
f241-19-01-3600-1	14.5.16.0	Yes	Default Site	Jun-12-08 10:07:55	Policy Events Policies Applied
f241-19-01-3600-1	14.5.16.255	Yes	Default Site	Jun-12-08 10:07:56	Policy Events Policies Applied

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

Функции контроля соответствия стандартам в CiscoWorks LMS



CiscoWorks LMS/RME



CiscoWorks LMS Portal (rtpnmiz-lms31)

Welcome jadavis

Home | Logout | Help | About

My Portal Public Private



09 Nov 2008, 18:18 EST

Functional	System	Network	DFM	CM	RME	IPM	CS	HUM	
------------	--------	---------	-----	----	-----	-----	----	-----	--

CiscoView

- Chassis View
- Mini RMON
- Administration

CiscoWorks Assistant

- Home
- Workflows
- Administration

Common Services

- Home
- Server
- Software Center
- Device and Credentials
- Groups

Device Diagnostic Tools

- Device Troubleshooting
- Device Center

RME

- Home
- Devices
- Config Management
 - Archive Management
 - Config Editor
 - NetConfig
 - Compliance Mgmt
- Software Management
- Job Management
- Reports
- Tools
- Administration
- Shortcuts

Campus Manager

- Home
- User Tracking
- Visualization
- Configuration
- Reports
- Job Management
- Administration

Device Fault Manager

Health and Utilization Monitor

- Poller and Template Management
 - Threshold Management
- Reports
- Admin

Internetwork Performance Monitor

- Collector Management
- Reports
- Admin

LMS Workflows Demo

CiscoWorks Product Updates

Setup Center

- Server Setup
- Server Settings

External Links

- Cisco.com Resources
- CiscoWorks Resources
- Third Party
- Custom Tools



CiscoWorks LMS/RME

Resource Manager Essentials

Home | Devices | **Config Mgmt** | Software Mgmt | Job Mgmt | Reports | Tools | Admin

Archive Mgmt | Config Editor | Net Config | **Compliance Mgmt**

You Are Here > Config Mgmt > Compliance Mgmt > Template Mgmt

TOC

- **Template Mgmt**
- .. Compliance Check
- .. Direct Deploy
- .. Compliance/Deploy Jobs

Baseline Templates

Showing 5 records

<input type="checkbox"/>	Name ▲	Device Type	Description	Created on
1. <input type="checkbox"/>	NSA_Router_Security	Routers,Cisco Interfaces and Modules	The NSA Router Security Recommendations	Jul 03 2008 07:34:10
2. <input type="checkbox"/>	TemplateExample1	Routers	Basic template example with Regular expression	Jun 30 2008 12:19:26
3. <input type="checkbox"/>	TemplateExample2	Routers	Advanced template example with Submode and Parent_child options	Jun 30 2008 12:19:26
<input type="checkbox"/>	TemplateExample3	Routers	Advanced template example with prerequisite option	Jun 30 2008 12:19:26
<input type="checkbox"/>	TemplateExample4	Routers	Advanced template example with ordered set option	Jun 30 2008 12:19:26

Edit | Export | Delete | Create | Import

Можно создать или импортировать новый шаблон. Несколько шаблонов доступны в стандартном пакете

Mode: ADDING
 1. Select Mode

 2. Add Template Details

Add Template Details

Baseline Templates

Conditional Block

 Check for compliance only if the following condition is satisfied

 Global

 SubMode

Cli Commands

```
#To check for existence of command enter
#+ <command>
# To check for non existence of command enter
#- <command>
# Commands without + or - are considered as comments
```

Для гибкости
используется regex

Compliance Block

 Global

 Use the SubMode of above condition

 SubMode

Cli Commands *

```
#To check for existence of command enter
#+ <command>
# To check for non existence of command enter
#- <command>
# Commands without + or - are considered as comments
- snmp-server community public [#((ro)|(rw)|(RO)|RW)]#]
- snmp-server community private [#((ro)|(rw)|(RO)|RW)]#]
```

 Order Sensitive

[Preview](#)
[Reset](#)
[Help](#)

* - Required

- Step 2 of 2 -

[<Back](#)
[Next>](#)
[Finish](#)
[Cancel](#)

Определите команды для проверки:
Со знаком '+' должны присутствовать
Со знаком '-' должны отсутствовать

Нажмите кнопку Finish

CiscoWorks LMS/RME

Выполнение проверки соответствия шаблону

Resource Manager Essentials

Home | Devices | Config Mgmt | Software Mgmt | Job Mgmt | Reports | Tools | Admin

Archive Mgmt | Config Editor | NetConfig | Compliance Mgmt

You Are Here > Config Mgmt > Compliance Mgmt > Compliance Check

1

TOC

- .. Template Mgmt
- .. Compliance Check**
- .. Direct Deploy
- .. Compliance/Deploy Jobs

2

	Name	Device Type	Description	Created on
1.	<input checked="" type="radio"/> No_poor_SNMP_strings	Routers,Switches and Hubs		Nov 09 2008 18:37:52
2.	<input type="radio"/> NSA_Router_Security	Routers,Cisco Interfaces and Modules	The NSA Router Security Recommendations	Jul 03 2008 07:34:10
3.	<input type="radio"/> TemplateExample1	Routers	Basic template example with Regular expression	Jun 30 2008 12:19:26
4.	<input type="radio"/> TemplateExample2	Routers	Advanced template example with Submode and Parent_child options	Jun 30 2008 12:19:26
5.	<input type="radio"/> TemplateExample3	Routers	Advanced template example with prerequisite option	Jun 30 2008 12:19:26
6.	<input type="radio"/> TemplateExample4	Routers	Advanced template example with ordered set option	Jun 30 2008 12:19:26

Showing 6 records

3

Compliance Check

После определения шаблона

1. Выберите 'Compliance Check' из меню,
2. Выберите шаблон,
3. Нажмите кнопку 'Compliance Check'

CiscoWorks LMS/RME

The screenshot shows the CiscoWorks LMS/RME interface. At the top, there is a navigation bar with the Cisco logo and the title 'Resource Manager Essentials'. Below this is a menu with options: Home, Devices, Config Mgmt, Software Mgmt, Job Mgmt, Reports, Tools, and Admin. A breadcrumb trail indicates the current location: 'You Are Here > Config Mgmt > Compliance Mgmt > Compliance/Deploy Jobs'. On the left, a 'TOC' (Table of Contents) sidebar lists: Template Mgmt, Compliance Check, Direct Deploy, and Compliance/Deploy Jobs (which is highlighted). The main content area is titled 'Baseline Jobs' and displays a table with 2 records. The first record is highlighted with a red arrow pointing to the 'Compliant/Deployed Device(s)' column, which shows '40 out of 41 Compliant'. The second record shows '0 out of 15 Compliant'. Below the table are buttons for 'Deploy', 'Retry', and 'Delete'.

Job ID	Description	Compliant/Deployed Device(s)	Status
1. 1050	CL - check for easy SNMP strings	40 out of 41 Compliant	Successful
	or_Check_1	0 out of 15 Compliant	Successful

После выполнения задачи результат будет доступен в меню 'Compliance/Deploy Jobs'.

Проверяются конфигурации, хранящиеся в архиве – задача выполняется без задержек.

Нажмите на ссылку-результат для просмотра деталей.

Baseline Compliance Report - Mozilla Firefox

http://rtpnmlz-lms31:1741/rme/dcmaBLAuditReport.do?jobId=1050

Baseline Compliance Report

CISCO Generated on Nov 09 2008 18:40:53

Go to: <<Select an Item>>

- <<Select an Item>>
- Compliant Devices
- Non-Compliant Devices**
- Excluded Devices

Template Name: No_poor_SNMP_strings

Number of Compliant device(s): 40

Number of Non-Compliant device(s): 1

Number of Excluded device(s): 0

Compliance Details

Compliant Devices

Device Name	Latest Version	Created On
14.5.5.51	1	Jul 03 2008 05:36:02
14.5.5.52	1	Jul 03 2008 05:35:31
14.5.5.53	1	Jul 03 2008 05:35:38
f241-19-01-2800-3	1	Jul 01 2008 14:48:04

Выберите нужный отчет

f241-19-03-2900-6	1	Jul 01 2008 14:46:39
f241-19-03-2900-9	1	Jul 01 2008 14:47:03
f241-19-03-2948g-1	1	Jul 01 2008 14:42:18
f241-19-03-3700-1	1	Jul 01 2008 14:48:33

Back to Top

Non-Compliant Devices

Device Name	Latest Version	Created On	Command(s) to Deploy
rtpnml-7606	1	Jul 01 2008 14:43:11	-snmp-server community ***** RO

Back to Top

Excluded Devices

No records.

Нажав на номер версии можно посмотреть детали конфигурации

Система предоставляет возможность выполнить команду на устройстве для устранения несоответствия конфигурации шаблону

CiscoWorks LMS или NCM?

1. NCM частично пересекается с LMS по функционалу в приложении RME (инвентарные данные, управление конфигурациями и ПО)
2. 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)
3. Решения дополняют друг друга в PACE

Пример проекта внедрения Network Compliance Manager



Этап 1

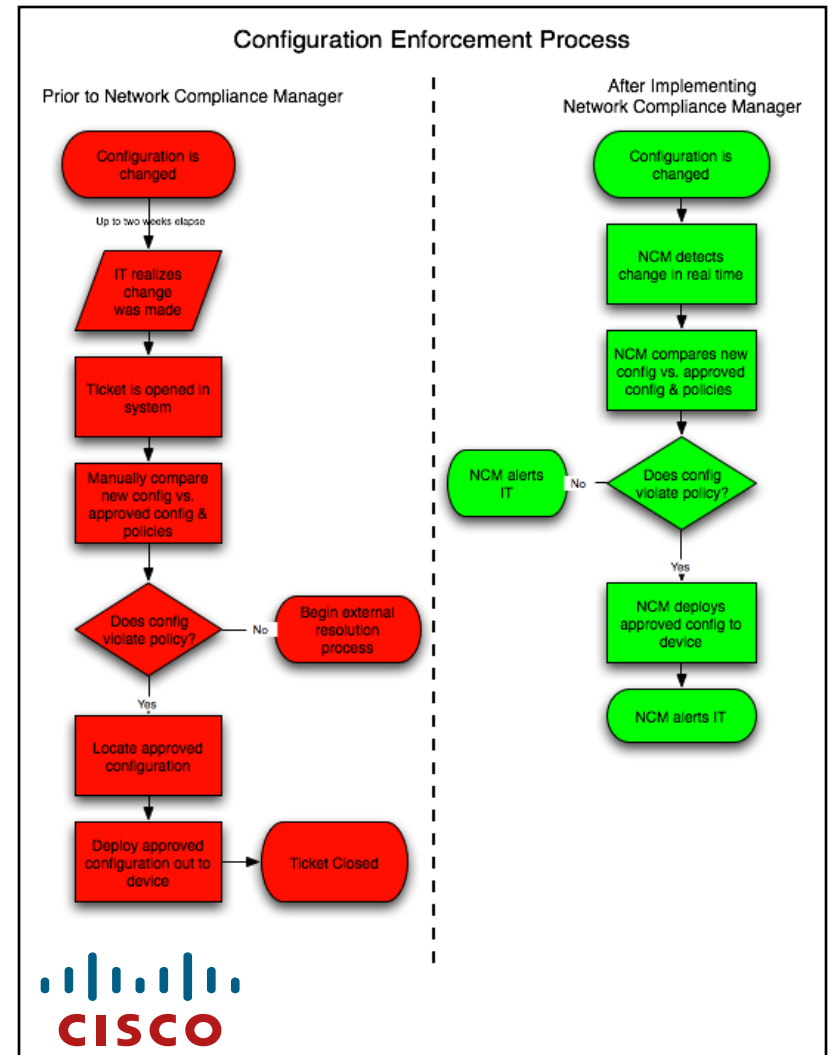
Решение по аудиту сети

1. Минимум трудозатрат для первых результатов
2-6 месяцев
Позволяет изучить возможности решения
2. Результат:
Мониторинг соответствия политикам
Контроль изменения конфигураций
Оперативная отчетность по ошибкам/дырам IOS

Этап 2

Контроль изменений

1. 4-9 месяцев
2. Внедрение процесса согласования и контроля изменений из централизованной системы
3. Унификация конфигураций
4. Интеграция с существующими системами управления изменениями



Этап 3

Автоматизация процессов

1. Обычно последний этап внедрения
2. Настройка NCM для автоматического исправления ошибок
3. Настройка NCM для проведения диагностики оборудования
4. Полная интеграция с другими системами (Service Desk, Управление инцидентами)

Рекомендации

- Унифицируйте конфигурации устройств для уменьшения время восстановления после отказов
- Контролируйте процесс внесения изменений для повышения доступности и безопасности работы сети
- Следите за текущими версиями программного обеспечения для уменьшения количества ошибок и возможных отказов
- Своевременно производите замену оборудования, которое больше не производится и не поддерживается, - это значительно уменьшит время возможных простоев

Вопросы и Ответы

Мы хотели бы узнать Ваше мнение

Пожалуйста,
заполните анкету





CISCO