# Архитектура и технологии для цифровой эры сетей

Оврашко Андрей
Системный инженер Cisco
aovrashk@cisco.com

# Agenda

1. Цифровая эра – DIGITIZATION
2. Архитектура Cisco Digital Network Architecture (DNA)
3. Сеть как единое «устройство» (SDN подход)
4. Передовые технлогии на сетевых устройствах
5. Сетевые сервисы по требованию (NfV)
6. Услуги безопасности на сетевой инфрастуктуре
7. Cisco ONE – лицензии на софт в бандле с железом

# DIGITIZATION

## Эра «цифровизации»

# “Цифровизация” задает бизнес-приоритеты и ставит новые задачи для ИТ

### Преобразование процессов и бизнес-моделей

Инновации

Ускорение достижения результата

### Поддержка эффективной работы и инноваций

Повышение эффективности

Сохранение кадров

### Персонализация обслуживания

Повышение лояльности

Повышение информированности

**Мобильность**
К 2017 г. объем мобильного трафика превысит объем проводного

**IoT**
К 2020 г. число IoT-устройств утроится

**Аналитика**
75% планируют (или уже инвестируют) в big data

**Облака**
К 2018 г. 80% организаций будут активно использовать SaaS

«Беспроводка»

IP-освещение

Машинное обучение

Коллективная безопасность

# Архитектура цифровых сетей Cisco

## Сеть для развития вашего цифрового бизнеса

# Cisco Digital Network Architecture


Сетевые приложения

**Управление сервисами как из облака**

Политики | Оркестрация

REST API | developer.cisco.com

**Автоматизация**

Абстракция сети
и сквозные политики
контроля

**Аналитика**

Сетевые данные,
Контекстный анализ

Netconf/YANG | CLI | Netflow | Телеметрия

**Виртуализация**

Физическая и виртуальная инфрастуктура | Хостинг приложений

**Интегрированная безопасность**

**NW Sec | TrustSec | NaaS | NaaE | ISE**

Авоматизация и набюдаемость

Безопасность и соответсвие требованиям регуляторов

Возможность заглянуть изнутри и почерпнуть знания для инноваций

# Требования к ИТ

## Автоматизация

- Скорость разворачивания отделений
- Стоимость рабочего места
- Сокращение ИТ трудозатрат
- Скорость и качество решения инцидентов
- Возможность быстрой реакции на инновации

## Безопасность

- Скорость решения последствий инцидентов ИБ
- Готовность к аудитам
- Снижение рисков потерь
- Простота добавления «из конца в конец»
- Наблюдаемость состояния

## Работа с клиентами

- Customer experience
- Remote Expert
- Таргетированный маркетинг
- Гостевой Wi-Fi
- Продуктивность своих сотрудников

**Инновации для трансформации бизнеса**

# Software Defined Networks от Cisco

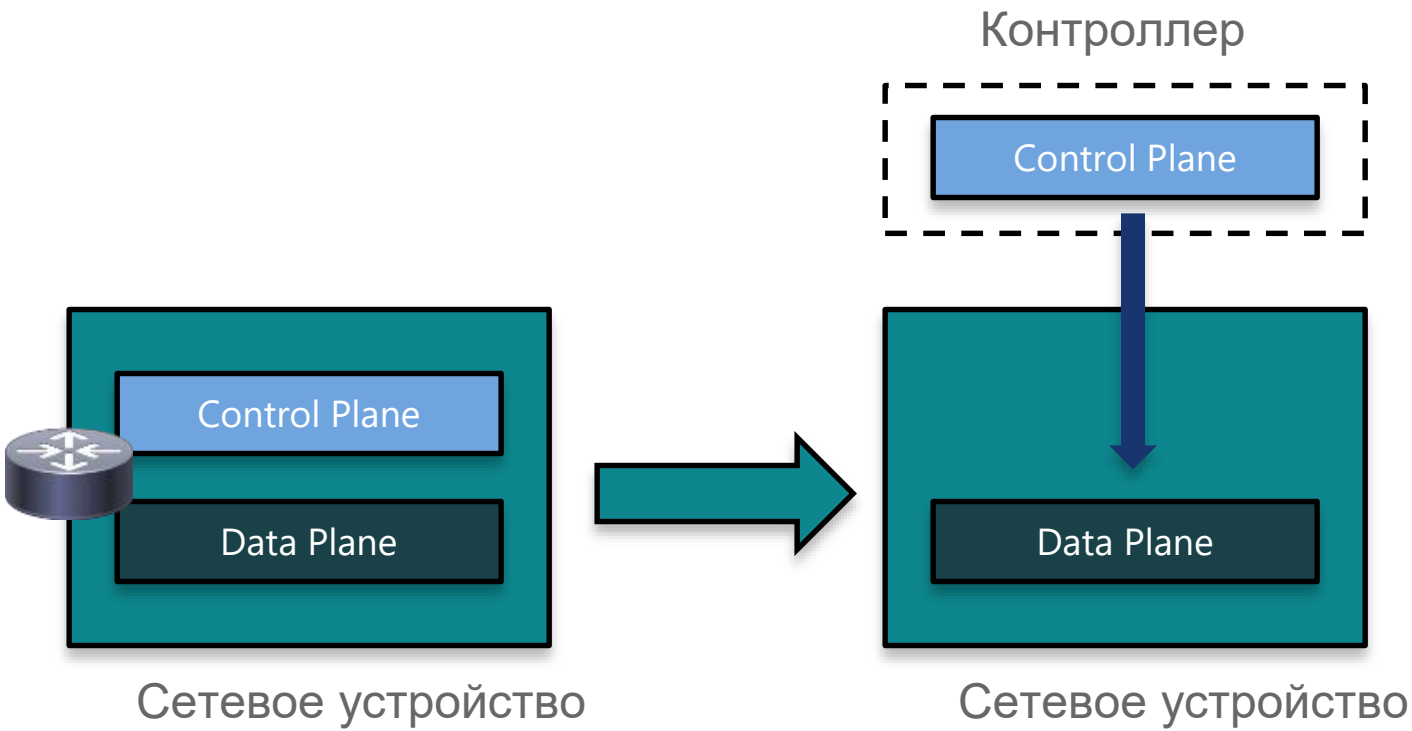
## Программно управляемая автоматизация сети

# Существующая модель управления сетью

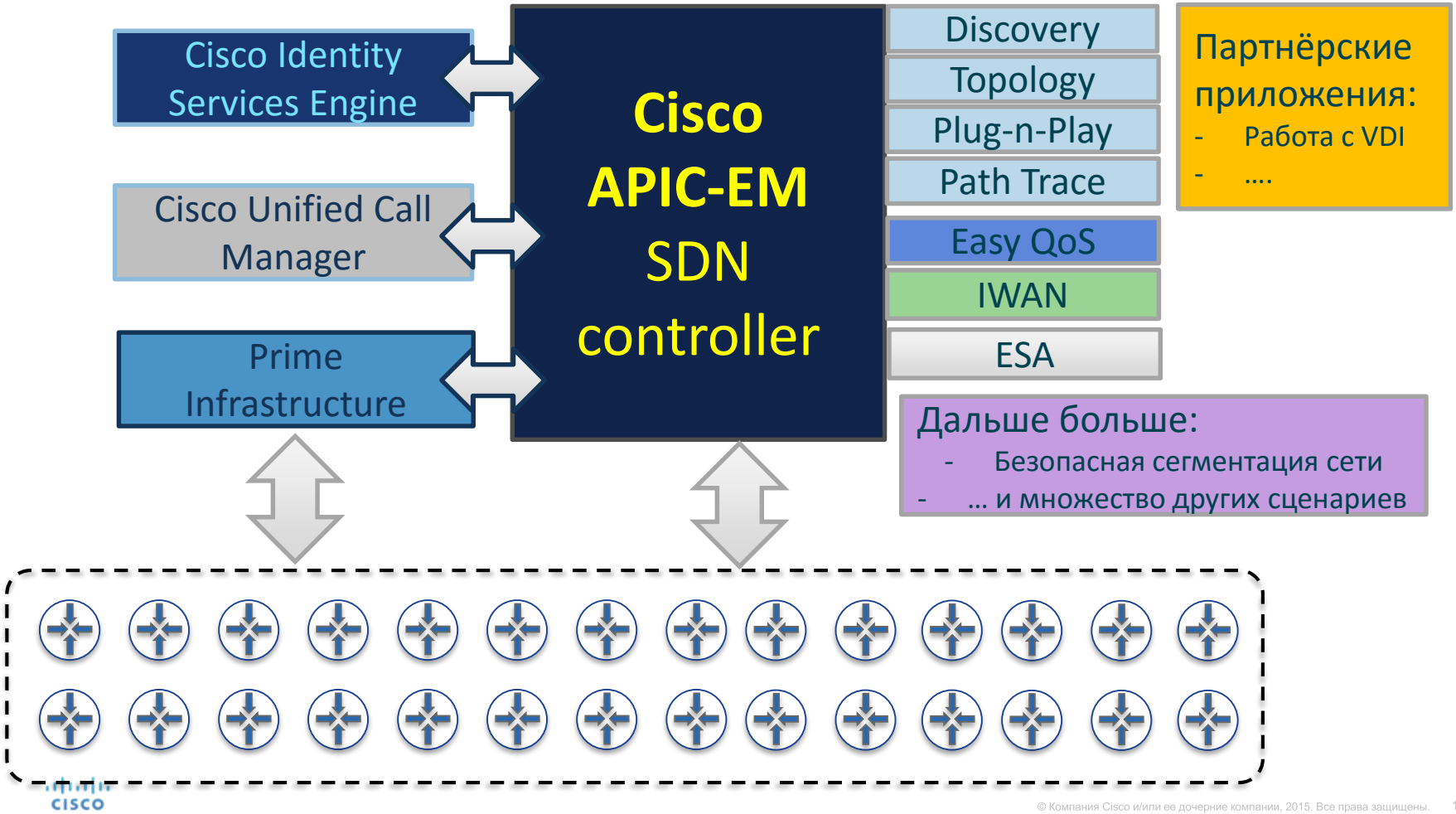
## Ручная настройка каждой отдельной коробки


Настройка функций
Ответ на вопрос: «Как?»

Настройка политик
Ответ на вопрос: **«Зачем?»**




# Происхождение контроллеров



# Модель политик Cisco SDN – от филиала в ЦОД

**СОГЛАСОВАННАЯ ПОЛИТИКА ДЛЯ ОБЛАКА, ЦОД, WAN И УРОВНЯ ДОСТУПА**

**Application Centric Infrastructure**

ЦЕНТР ОБРАБОТКИ ДАННЫХ

SDN CONTROLLER

**Сетевой профиль потока приложений**

SLA, безопасность, QoS, балансировка нагрузки

Облако

ЦОД

APIC EM

СЕТЬ WAN И СЕТЬ ДОСТУПА

**User Centric Infrastructure**

**Сетевой профиль пользователя или объекта**

QoS, безопасность, SLA, устройство, местоположение, роль

WAN

Доступ

**ПРЕИМУЩЕСТВА Cisco**

ПРОЕКТЫ НА ОСНОВЕ ИМЕЮЩЕЙСЯ ИНФРАСТРУКТУРЫ И РАЗРАБОТКИ С НУЛЯ

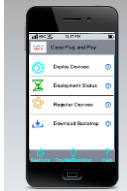
КОМПЛЕКСНОСТЬ

СТРУКТУРА ПОЛИТИК: ОРИЕНТАЦИЯ НА ПОЛЬЗОВАТЕЛЕЙ И ПРИЛОЖЕНИЯ

День 0

# Network Plug and Play (PnP)

## Приложение PnP Helper



[ Дополнительно]

Выполняет начальную загрузку, проверки состояния и возможных неисправностей

Redpark RJ45
Apple 8pin

Redpark RJ45
Apple 30pin

GetConsole
Airconsole2.0
Адаптер Bluetooth

## Облачный сервис переадресации

[ Дополнительно]

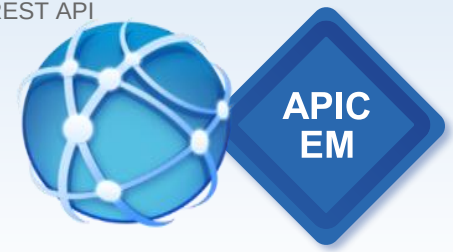
План развития, Фаза 2

## Сервер PnP

Центральный сервер на APIC-EM

Управление узлами, устройствами, образами, лицензиями, рабочим процессом

Предоставление северных интерфейсов REST API




## Протокол PnP

Выполняется между агентом и сервером

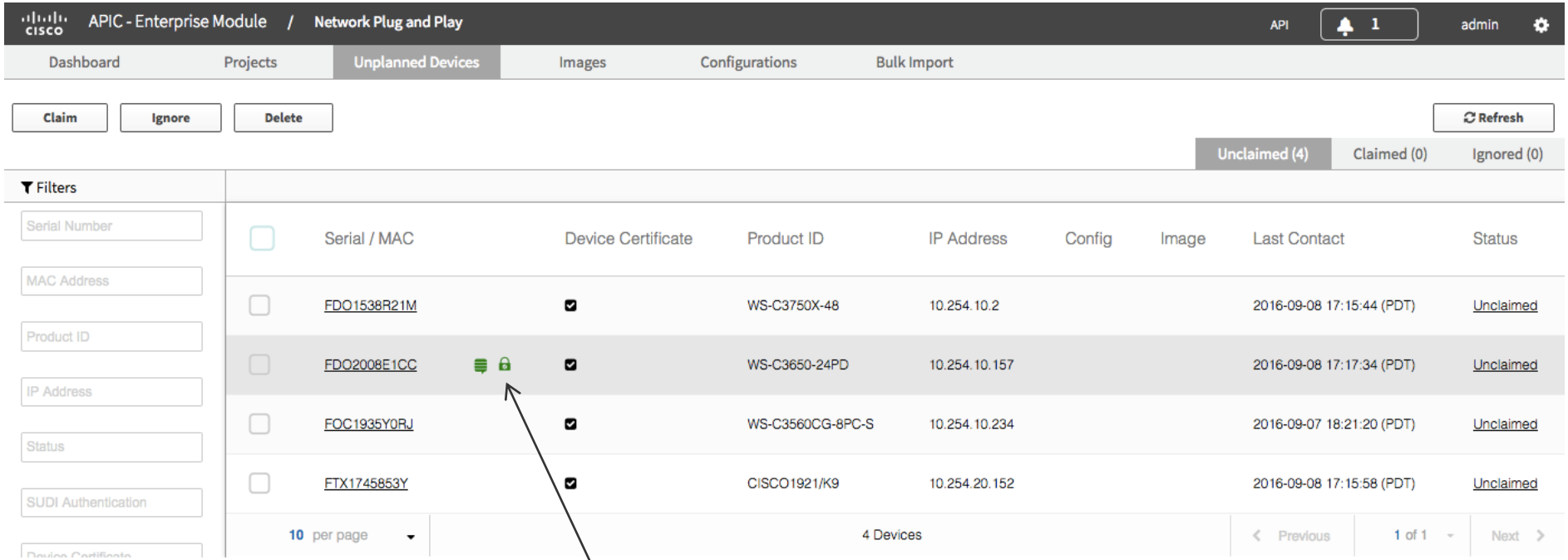
Открытая схема

## Агент PnP

Выполняется на коммутаторах, маршрутизаторах и беспроводных ТД Cisco®

Автоматизирует процесс развертывания

# Идентификатор устройства (SUDI) в схеме работы PnP




«Замочек» показывает, что для подключеня устройства использован Secure Unique Device Identifier

# APIC-EM – как потрогать руками?

**https://sandboxapic.cisco.com**

- Зарегистрируйтесь на Cisco DevNet (http://developer.cisco.com )
- Используйте «песочницу» APIC-EM – всегда включено!
- APIC-EM Login:  username: devnetuser password: Cisco123!

- Сценарии («лабы») для начала работы: http://dcloud.cisco.com




15

# Передовые технологии на сетевых устройствах Cisco

## Путь от сложных задач к простому решению

# «Обычная» нетривиальная задача

**Обеспечить сегментацию в филиальной сети:**

- Растянуть «VLANы» между площадками
- Обеспечить мобильность сотрудников
- Отвязаться от IP-адресации
- Персонализировать доступ
- Создать единую политику
- Централизовано управлять

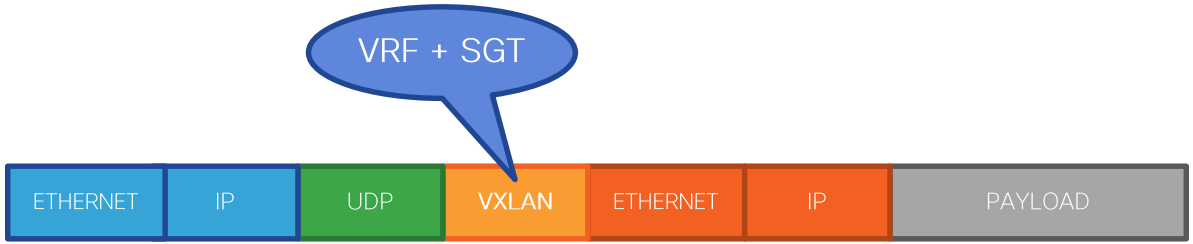
# Персонализация сетевого доступа и правил

## Key Components – Cisco TrustSec

**1. LISP based Control-Plane**

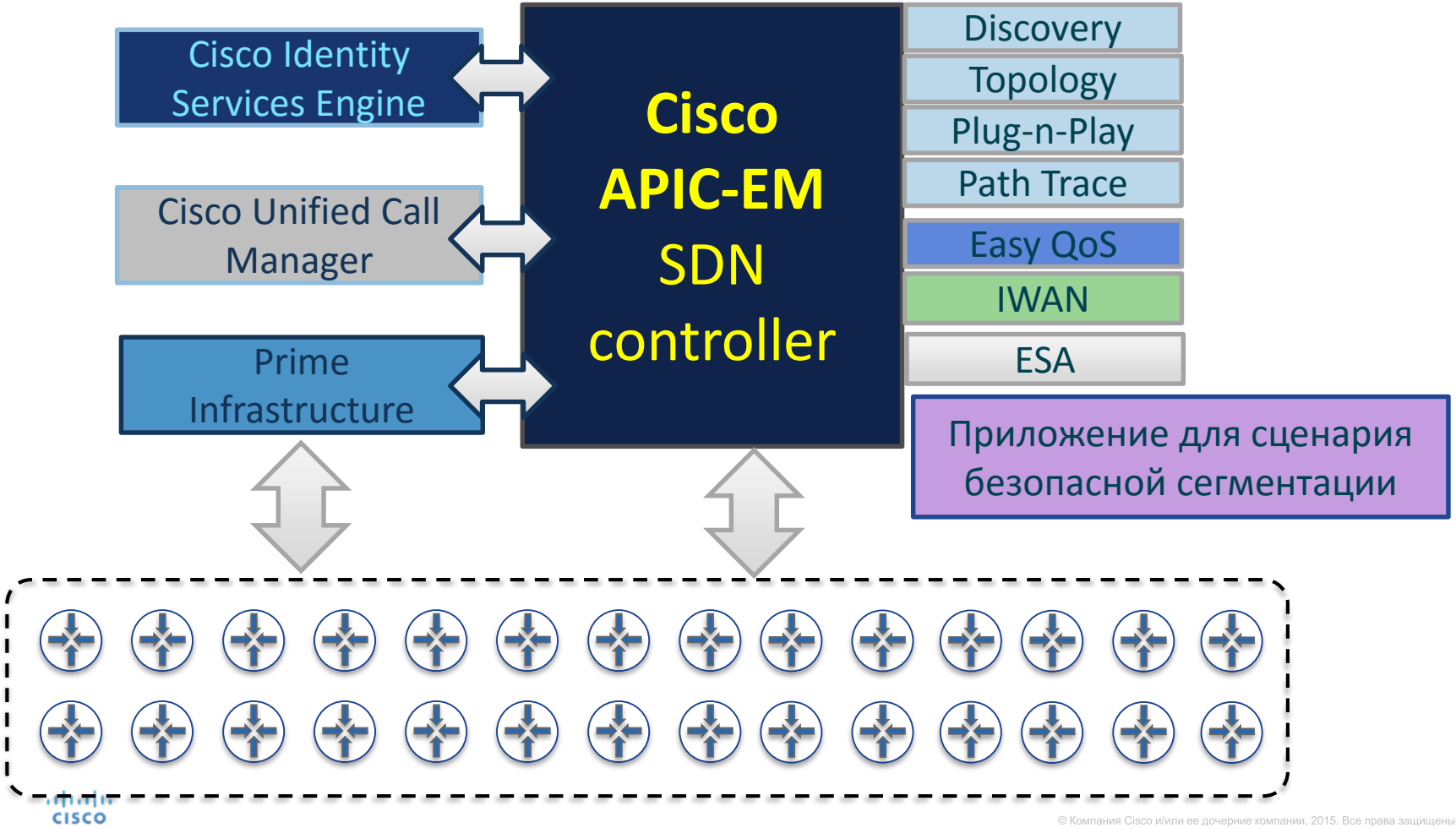
**2. VXLAN based Data-Plane**

**3. Integrated Cisco TrustSec**




Virtual Routing & Forwarding

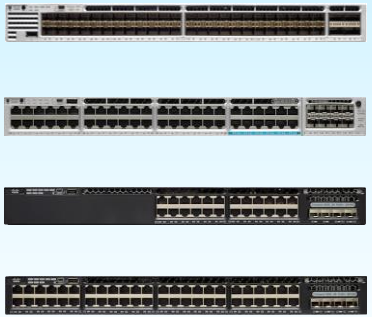
Scalable Group Tagging



# Platform Support

## Multiple Edge, Border & C-Plane Options

### Catalyst 3K



- Catalyst 3650
- Catalyst 3850
- Copper / Fiber
- **IOS-XE 16.3+**

### Catalyst 4K

- Catalyst 4500
- Sup8E
- Sup Uplinks
- **IOS-XE 3.9+**

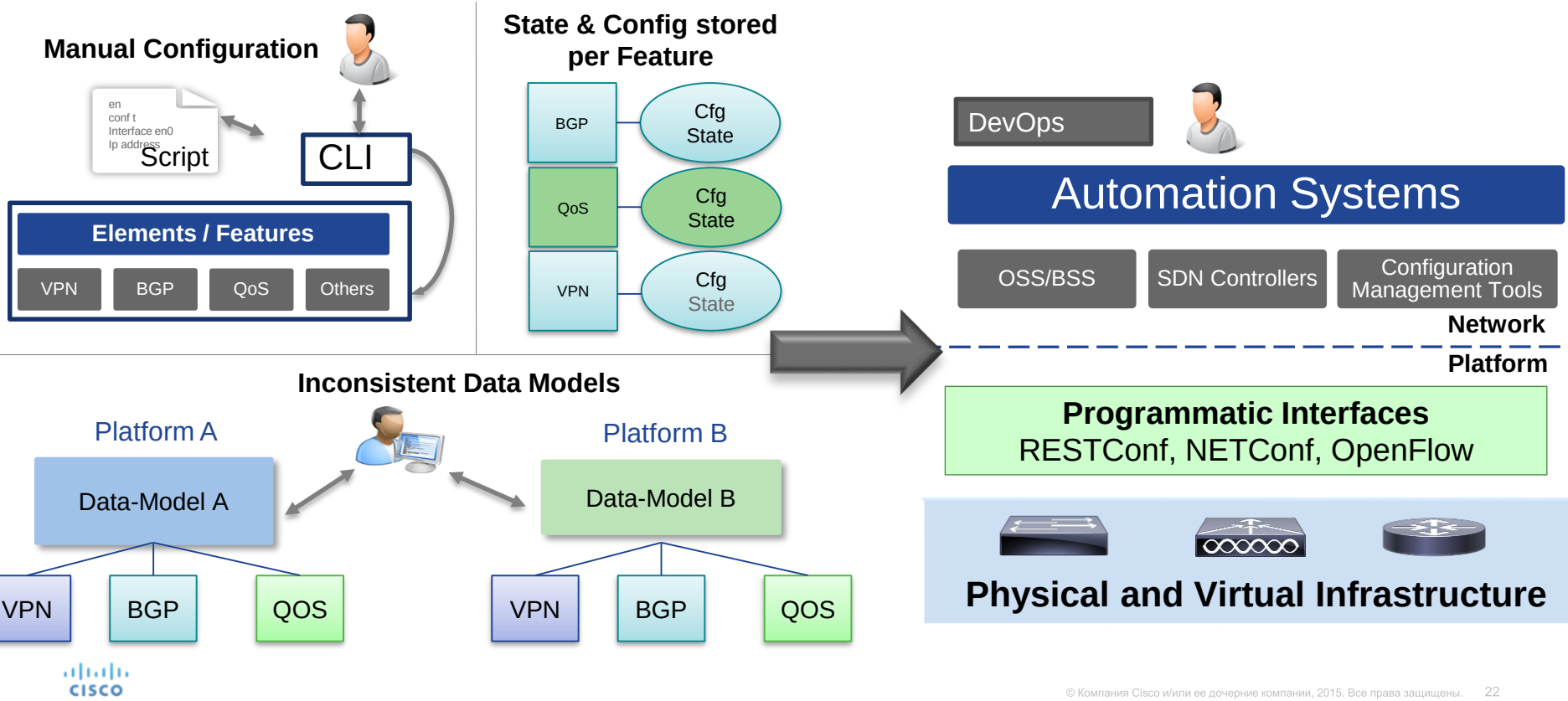
### Catalyst 6K

- Catalyst 6800
- Sup2T / 6T
- 6900 or Newer
- **IOS 15.4SY+**

### Nexus 7K

- Nexus 7700
- Sup2E
- M3 Only
- **NXOS 7.3DX+**

# IOS-XE 16 “Polaris”
## Programmability (NETConf and YANG)



# **Catalyst 3850 & 3650 серии** (IOS-XE 16.x)

– не просто свич

## Protects the Network

**Protections Against Attack**

| | | |
|---|---|---|
| DHCP Snooping | Port Security | uRPF |
| Intrusion Detection | IP Source Guard | ACLs |

Network as an Enforcer | Network as a Sensor


TrustSec


ISE


Stealthwatch


FnF

## Platform Integrity

Secure Boot | Hardware Trust Anchor | Counterfeit Protections | Runtime Defenses | OS Validation | Modern Crypto | Incident Response | No Back Doors

## Security Culture

Supply Chain Management | Open Source Registration | Security Training | Threat Modeling | Product Security Baseline | PSIRT Advisories

VXLAN | LISP | SGT-enforcement | Full NetFlow

# **Catalyst 2960X серии** (IOS 15.x)

## – просто свич, но с продвинутыми возможностями

**Protects the Network**

**Protections Against Attack**

| | | |
|---|---|---|
| DHCP Snooping | Port Security | uRPF |
| Intrusion Detection | IP Source Guard | ACLs |

Network as an Enforcer | Network as a Sensor


TrustSec


ISE


Stealthwatch


FnF

**Platform Integrity**

Secure Boot | Hardware Trust Anchor | Counterfeit Protections | Runtime Defenses | OS Validation | Modern Crypto | Incident Response | No Back Doors

**Security Culture**

Supply Chain Management | Open Source Registration | Security Training | Threat Modeling | Product Security Baseline | PSIRT Advisories

802.1x | SGT-propagation | Full NetFlow

# Интеграция сетевых устройств, системы сбора NetFlow (StealthWatch) и ISE

## Network-as-an-Enforcer (NaaE)

### Monitor

- Оценка «нормального» поведения сети
- Наблюдаемость трафика в реальном времени

### Detect

- Поведенческий анализ
- Распознаване аномального поведения и атак

### Analyze

- Хранение и анализ данных
- Готовность к аудитам
- Поиск первопричин
- Расследоване инцидентов

### Respond

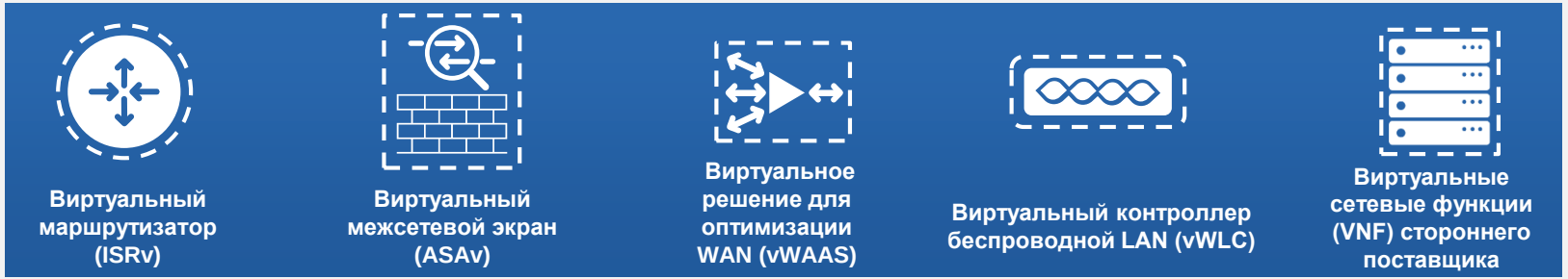
- Скорость поиска проблем и обнаружения атак
- Автоматическа реакция на аномалии и атаки
- «Забрать доступ» или «поместить в карантин»

# Сетевые функции по требованию

## Network Function Virtualization

# Введение: Cisco Enterprise NFV
## Сетевые сервисы за считанные минуты на любой платформе

Enterprise Service Automation (ESA)

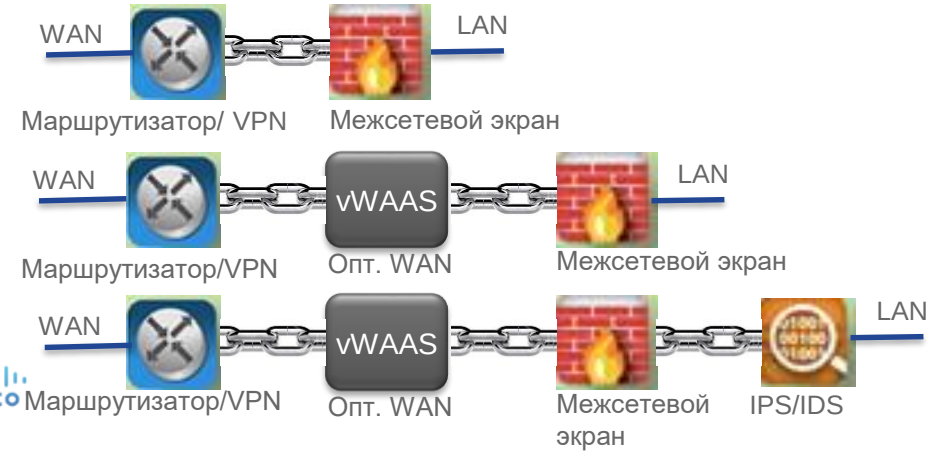


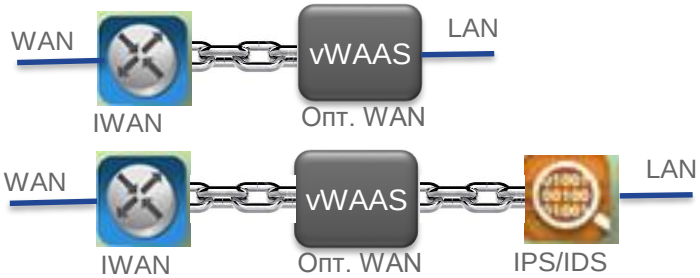

**ПО виртуализации инфраструктуры сетевых функций (NFVIS)**

| | | |
|---|---|---|
| **ISR 4000 + UCS серии E** | **UCS серии C** | **ENCS** |

# Создание цепочек сервисов в решении Enterprise NFV

- Решение позволяет создавать цепочки СЕТЕВЫХ сервисов
- Сетевые функции по требованию
- Централизованное управление через SDN-сценарий Enterprise Service Automation (ESA)



# Безопасность

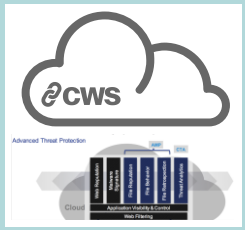

на сетевых устройствах Cisco

и вокруг сетевых устройств Cisco

# Cisco ISR 4000 – платформа сетевой безопансоти

## Protects the Network








## Platform Integrity

Secure Boot | Hardware Trust Anchor | Counterfeit Protections | Runtime Defenses | OS Validation | Modern Crypto | Incident Response

## Security Culture

Supply Chain Management | Open Source Registration | Security Training | Threat Modeling | Product Security Baseline | PSIRT Advisories

# Router security

## Инфрастурктура безопасности вокруг маршрутизаторов

# Интеграция функций безопасности

## Конвергенция сетевых сервисов и функций безопасности

VPN | ZBFW | Snort IPS | Umbrella Branch (OpenDNS) | Stealthwatch Learning Network | Firepower | CWS


**Многоуровневая безопасность**

**Нативная виртуализация сервисов**

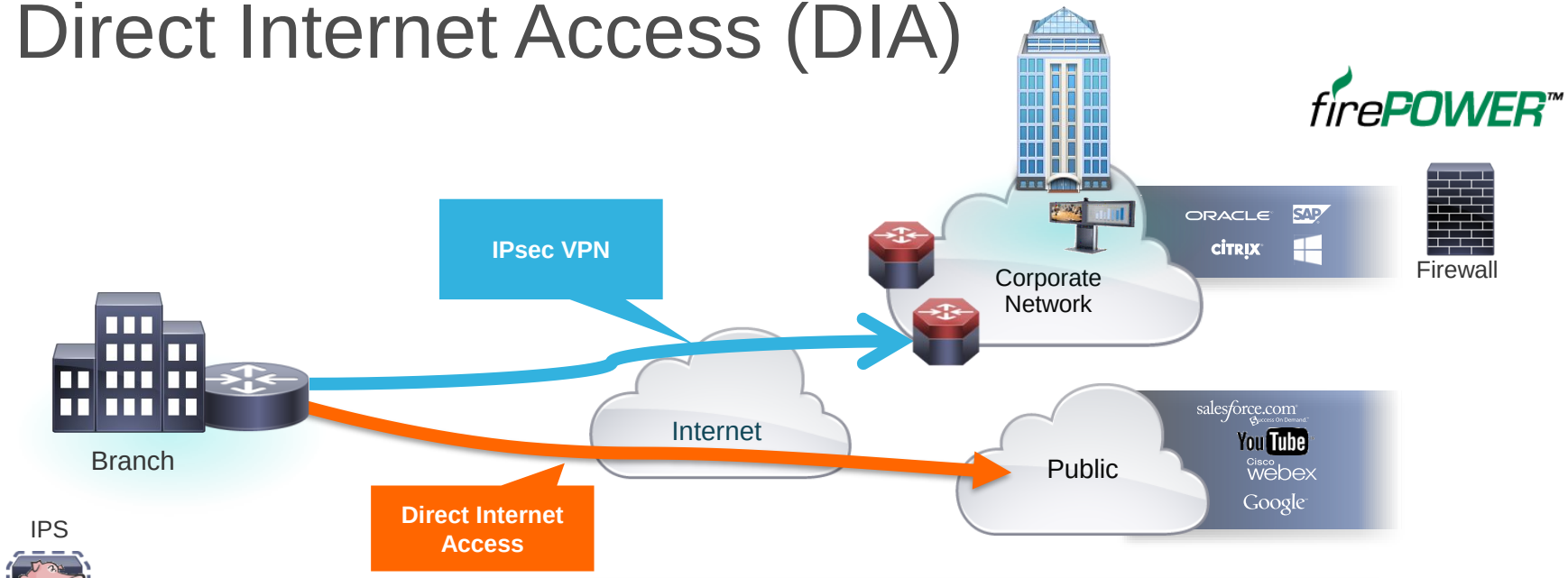
**AVC, WAN Opt, UC, Security**

**Безопасность для соответсвия требованиям внутренних и внешних регуляторов**

**Threat Centric Advanced security**

**Сетевая часть**
**Серверная часть**
**Хранение данных**

# Direct Internet Access (DIA)




IPS

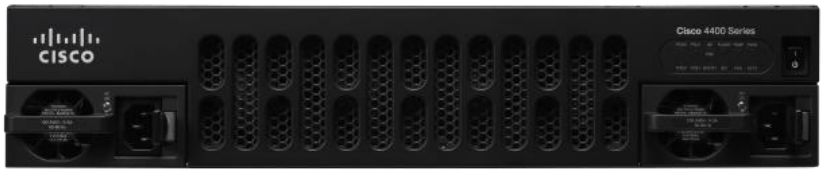
Firewall

Umbrella

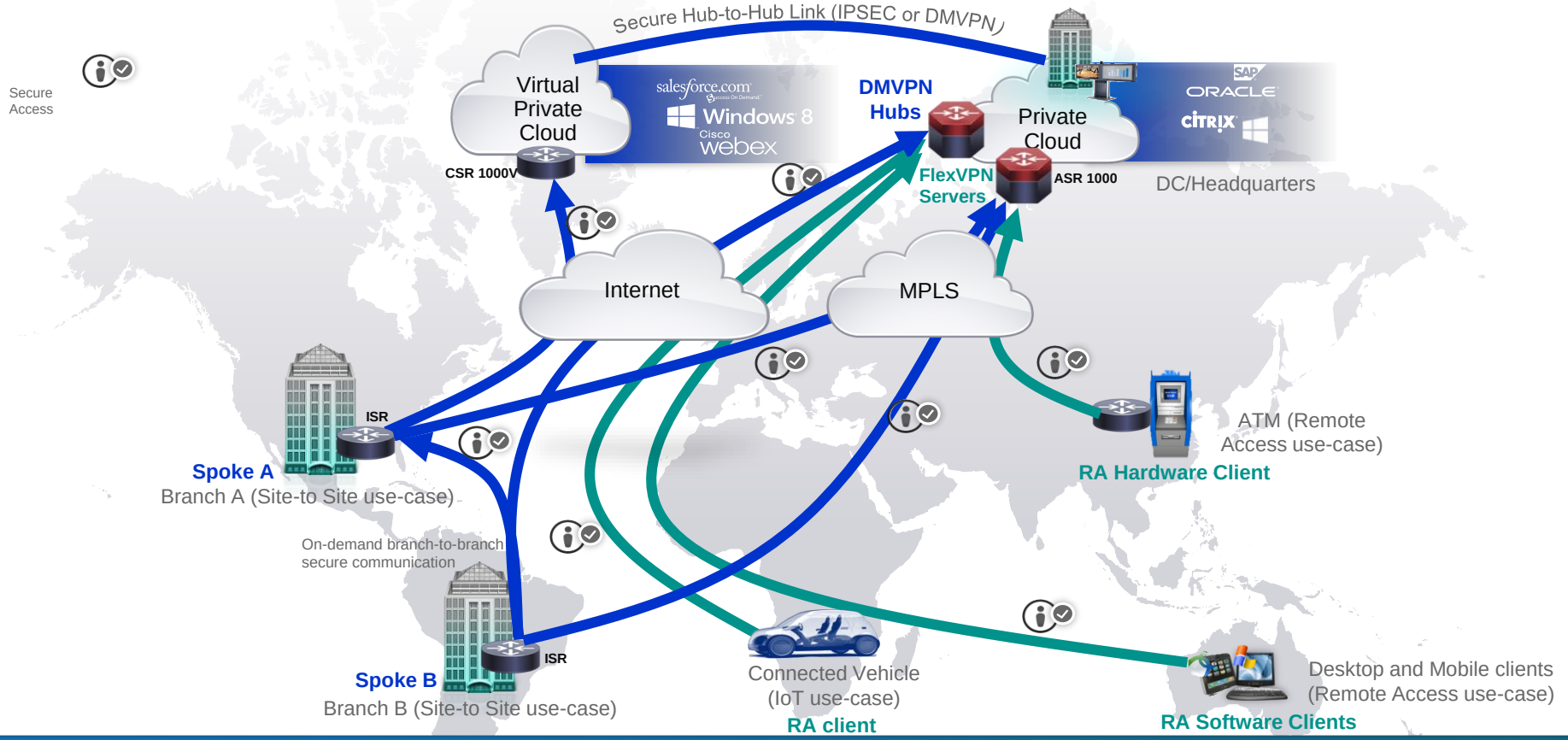
- Безопасный WAN транспорт
- Локальный выход в Internet
- Обнаружение сетевых угроз
- Продуктивность сетевых приложений
- Уменьшение потребления полосы WAN

# Virtual Private Networks (VPN)

VPN — ZBFW — Snort IPS — Umbrella Branch (OpenDNS) — Stealthwatch Learning Network — Firepower — CWS



# Примеры применения DMVPN и FlexVPN решений




**DMVPN:** Secure WAN transport across MPLS and/or Internet for branch-to-branch or branch-to-hub (private cloud / DC access)

**FlexVPN:** Secure access to enterprise network over MPLS and/or Internet for remote users and IoT

# Hub-Spoke + Spoke-Spoke Solutions

## Components and Services Interaction

| Solution | Overlay | Technology | Type | Encryption | PfRv3 | AVC | WAAS | QoS |
|---|---|---|---|---|---|---|---|---|
| IWAN | mGRE | DMVPN | Tunnel | Pair-wise | Yes | Yes | Yes | Adaptive Per-Tunnel |
| DCI | OTV, VXLAN, LISP | MACsec | Tunnel-less | Pair-wise | N/A | N/A | N/A | Per-Interface |
| | | IPsec VPN | Tunnel | Pair-wise | N/A | No | No | Per-Tunnel |
| | | GETVPN | Tunnel-less | Group Key | N/A | N/A | N/A | Egress-Interface |
| MPLS-o-mGRE | mGRE | GETVPN | Tunnel | Group Key | N/A | No | No | Egress-Interface |
| MPLSoDMVPN | mGRE | DMVPN | Tunnel | Pair-wise | N/A | No | No | Per-Tunnel |

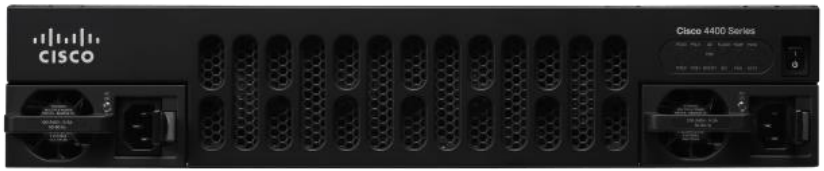
Yes = Supported and Recommended

No = Supported but Not-Recommended

- PfRv3 работает только с DMVPN (единый домен маршрутизации)
- PfRv3 не работает с GETVPN или статическим IPsec VPN
- APIC-EM поддержвает только IWAN – DMVPN, PfR, AVC, etc.

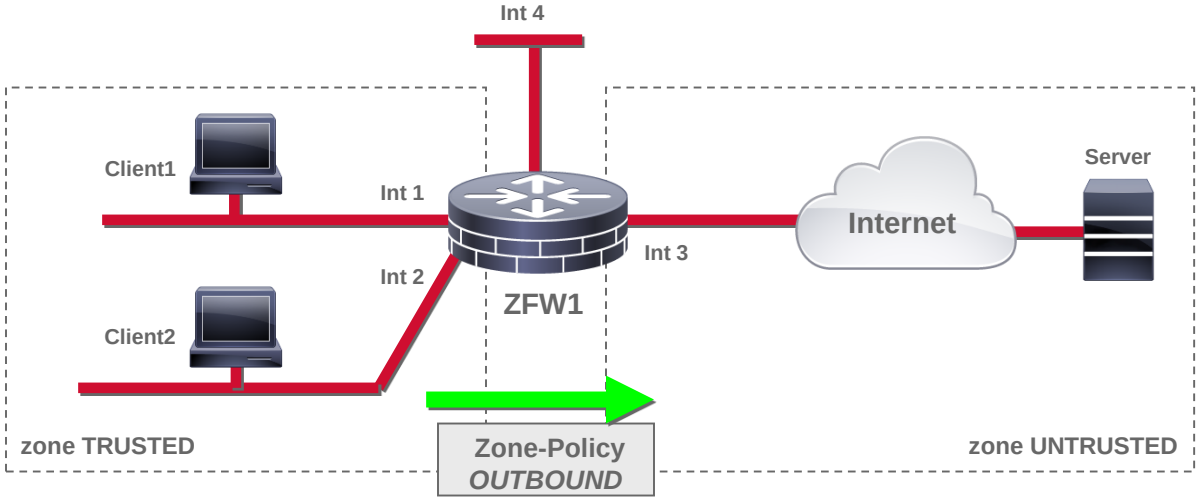
# Zone Based Firewall
(any traffic)

VPN — ZBFW — Snort IPS — Umbrella Branch (OpenDNS) — Stealthwatch Learning Network — Firepower — CWS



# Zone-based Policy Firewall (ZBFW)

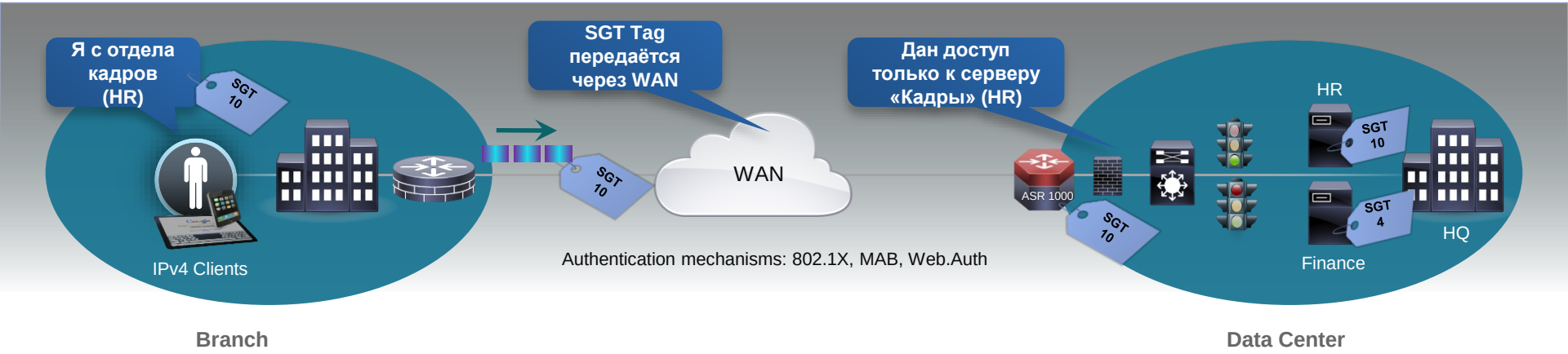
- «Зона»: набор интерфейсов разделяющих общий уровень безопасности “trust level”
- Философия: Фаервольные политики определяют правила для контроля взаимодействия зон (вместо правил между парами интерфейсов)




Полтики ZBFW **однонаправлены**: Источник → Поучатель

# TrustSec + DMVPN

# Дальше больше
## TrustSec SGT поверх DMVPN сети




### Problem Statement

- BYOD support for non-IT standard devices
- Enforcing consistent security policy

### Solution Overview

- Secure Group Tagging (SGT) for Context-aware Firewall enforcement
- Secure Group Tag transport over DMVPN, FlexVPN, GETVPN

### Solution Characteristics

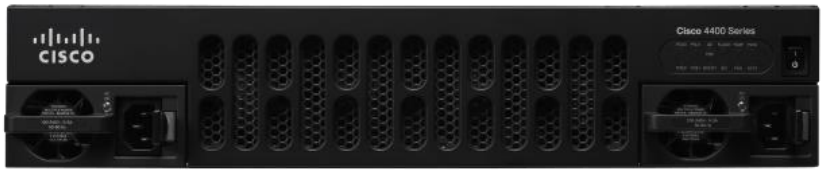
- Secure Identity-based access; keep outsiders out
- Control Access and service levels based on Identity
- Authorized access for users and devices

### Scalability

- 100 Gbps FW (ASR1K with ESP100)
- Support up to 6M Sessions at 350K CPS (ASR1K with ESP100)

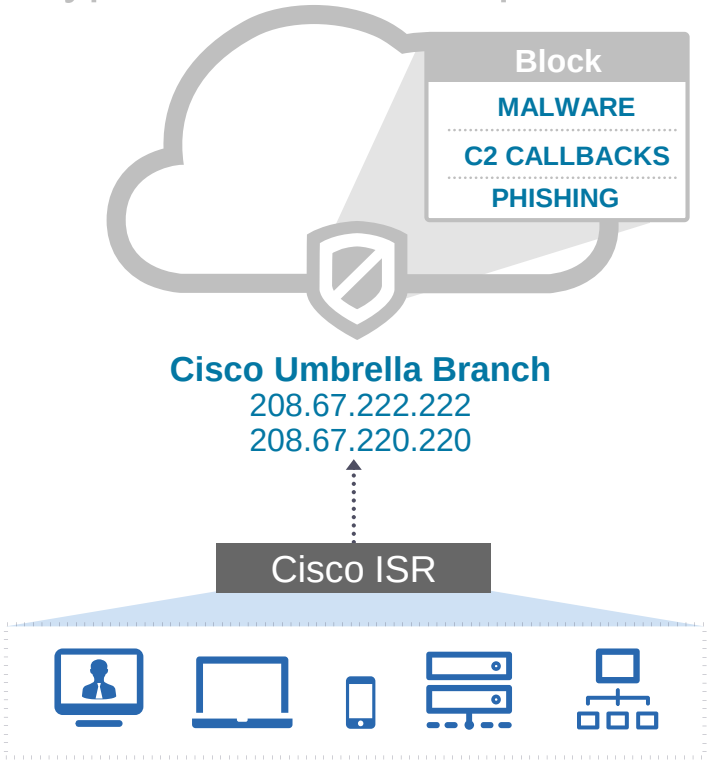
# OpenDNS
(dns)

VPN → ZBFW → Snort IPS → Umbrella Branch (OpenDNS) → Stealthwatch Learning Network → Firepower → CWS



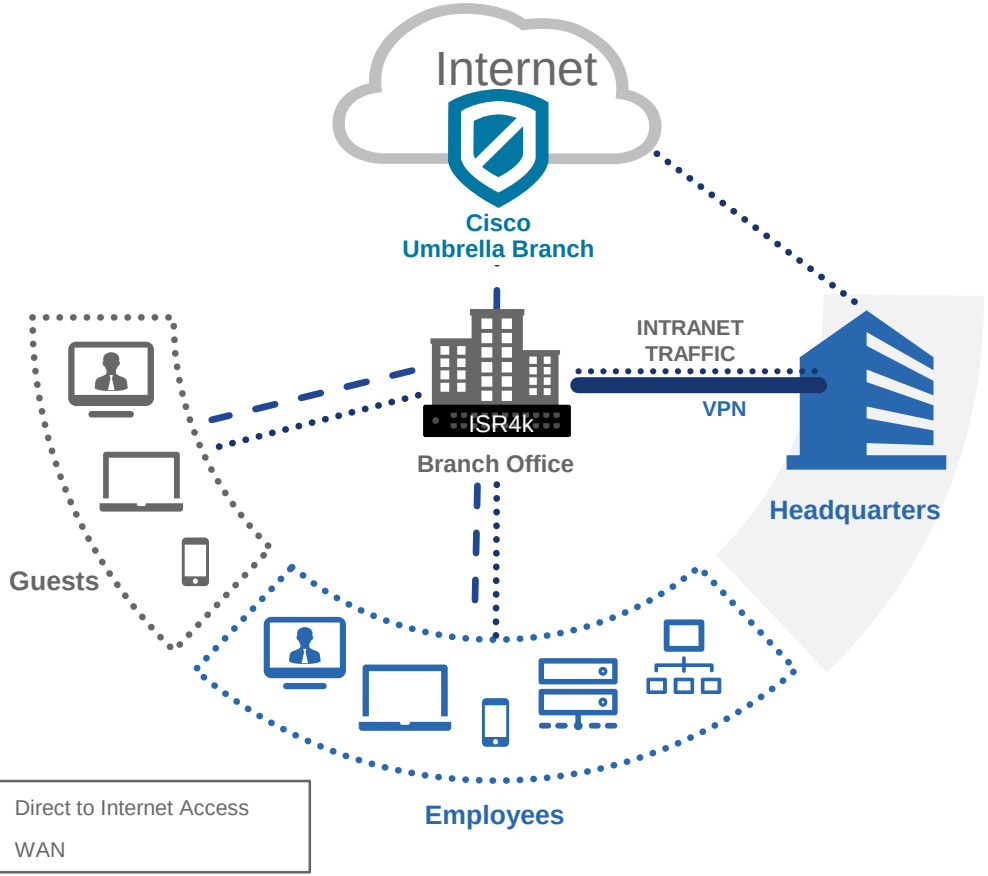
# Cisco Umbrella Branch (a.k.a OpenDNS)

## Первейший уровень защиты филиальной сети




- Visibility & enforcement at the DNS-layer
- Block requests to malicious domains and IPs
- Predictive intelligence: uncover current & emergent threats
- Protect all devices on your branch network against:
  - Malware
  - Phishing
  - C2 callbacks

# Защита гостевого и корпоративного трафика




## SECURITY

- Prevent guest or corporate users from connecting to malicious domains & IPs
- Prevent already-infected devices from connecting to C&C

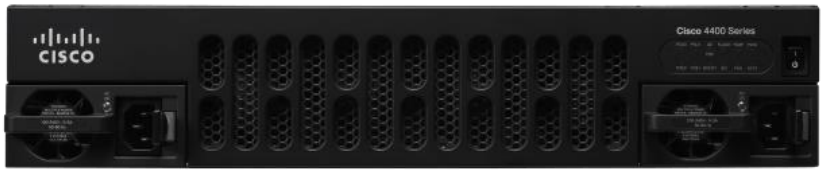
## ACCESS CONTROL

- Guest: Inappropriate content
- Corporate: Loss of productivity

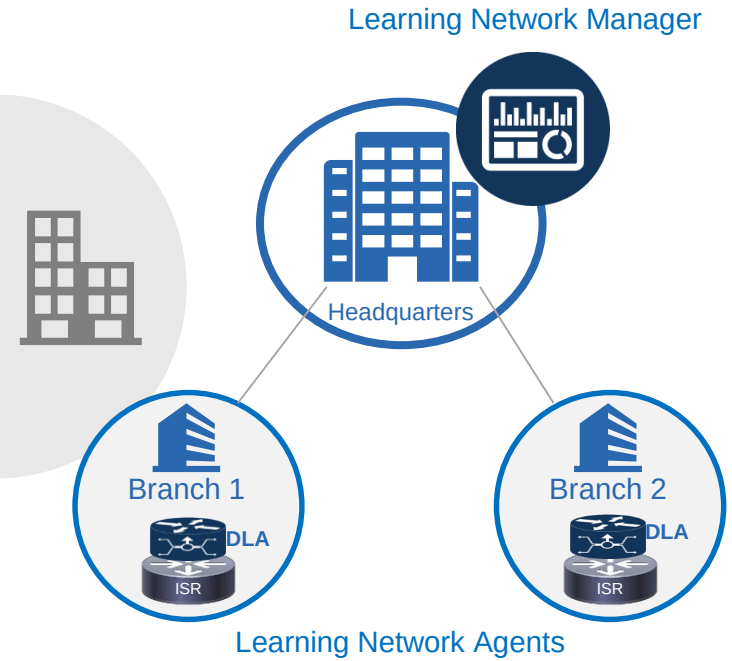
Требуется лицензия SEC/AX
+ подписка на OpenDNS cloud services (1Y or 3Y)

# Stealthwatch
(NetFlow)

VPN — ZBFW — Snort IPS — Umbrella Branch (OpenDNS) — Stealthwatch Learning Network — Firepower — CWS



# Stealthwatch Learning Network License (SLNL)




Привносит возможности **самообучения на платформу Cisco 4000 ISR**

**Не требует настройки** фаервольных правил, сигнатур защиты от malware или настройки списков доступа (ACL)

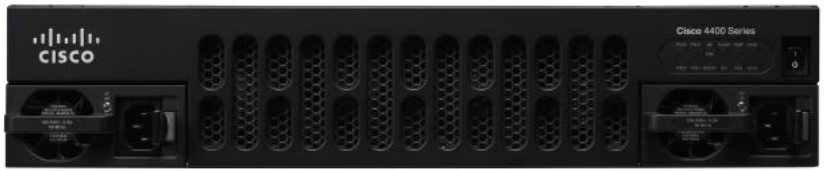
**Использует машинное обучение**, сетевой контекст, перехват пакетов для определения что нормально, а что нет в сетевом поведении

Использует продвинутую сетевую аналитику и моделирование **для определения и блокировки** настоящих аномалей

**Адаптируется** при изменении условий

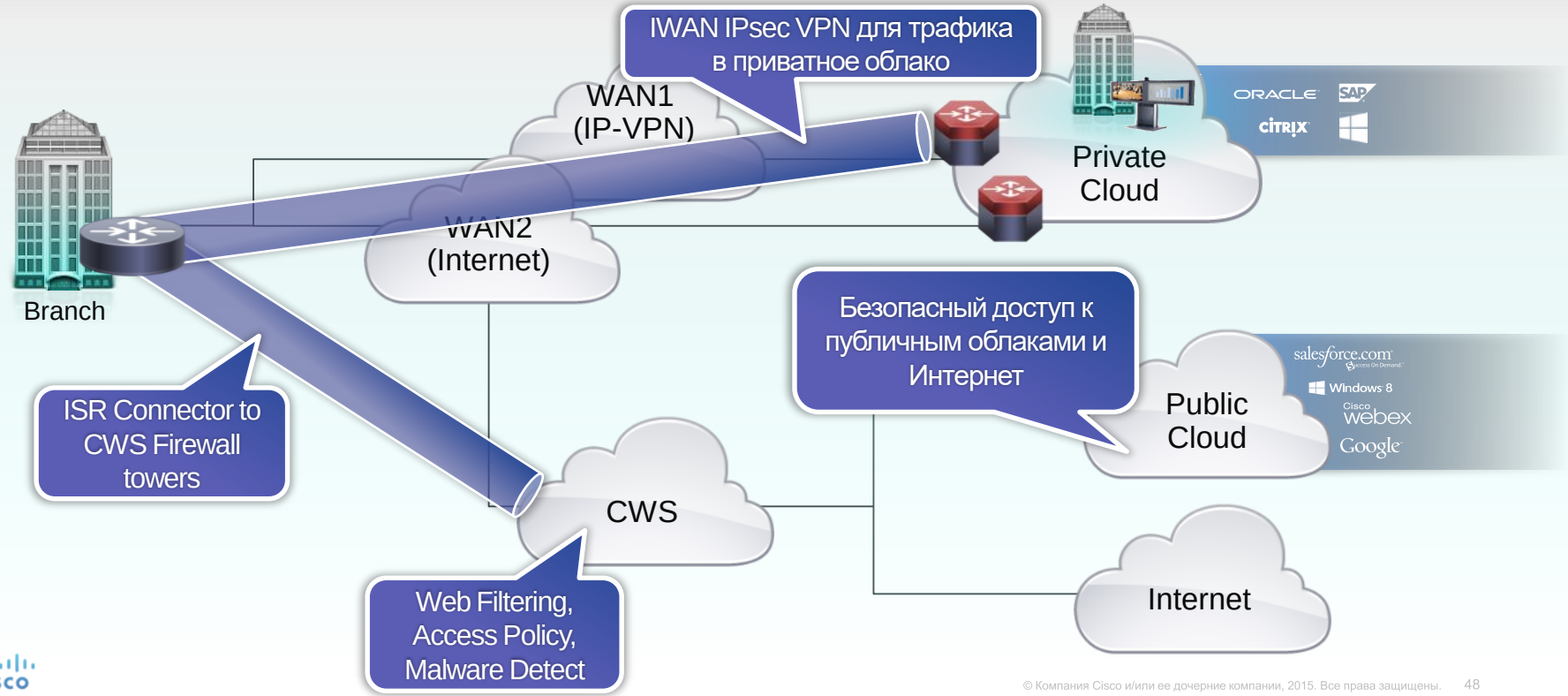
# Cloud Web Security
(http and https)

VPN — ZBFW — Snort IPS — Umbrella Branch (OpenDNS) — Stealthwatch Learning Network — Firepower — CWS

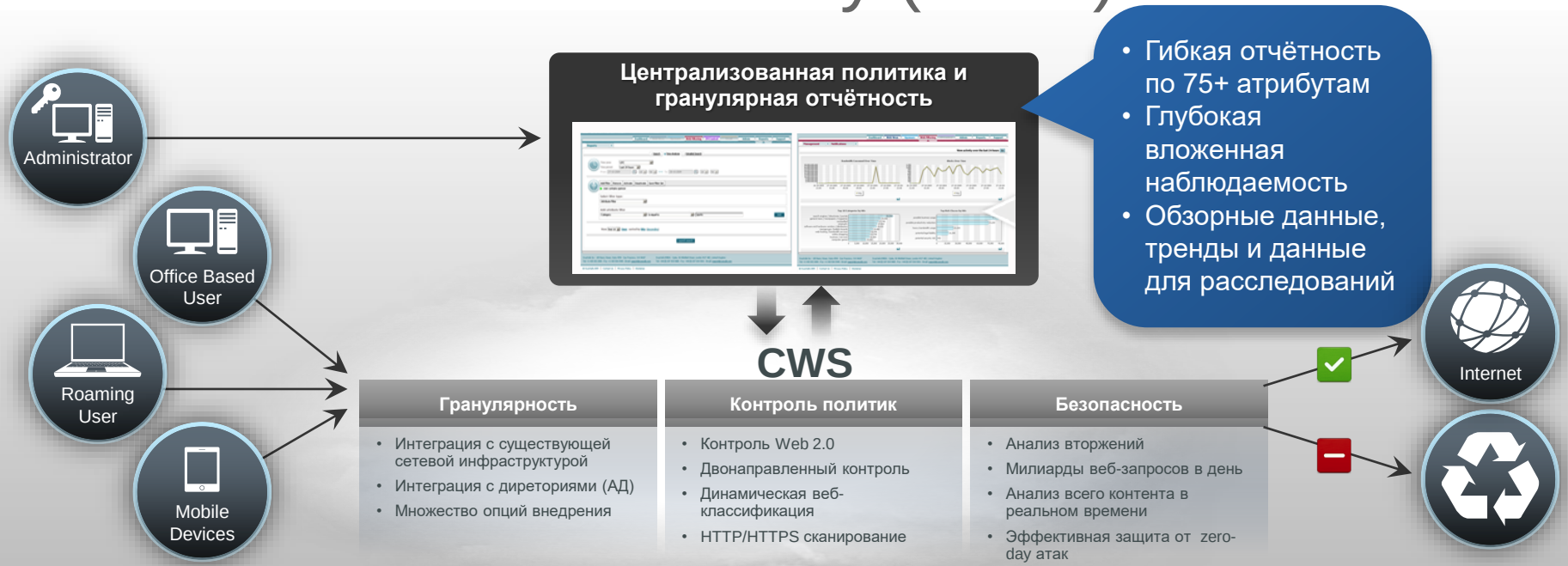


# Безопасность прямого доступа в Интеренет

## Cloud Web Security (CWS)

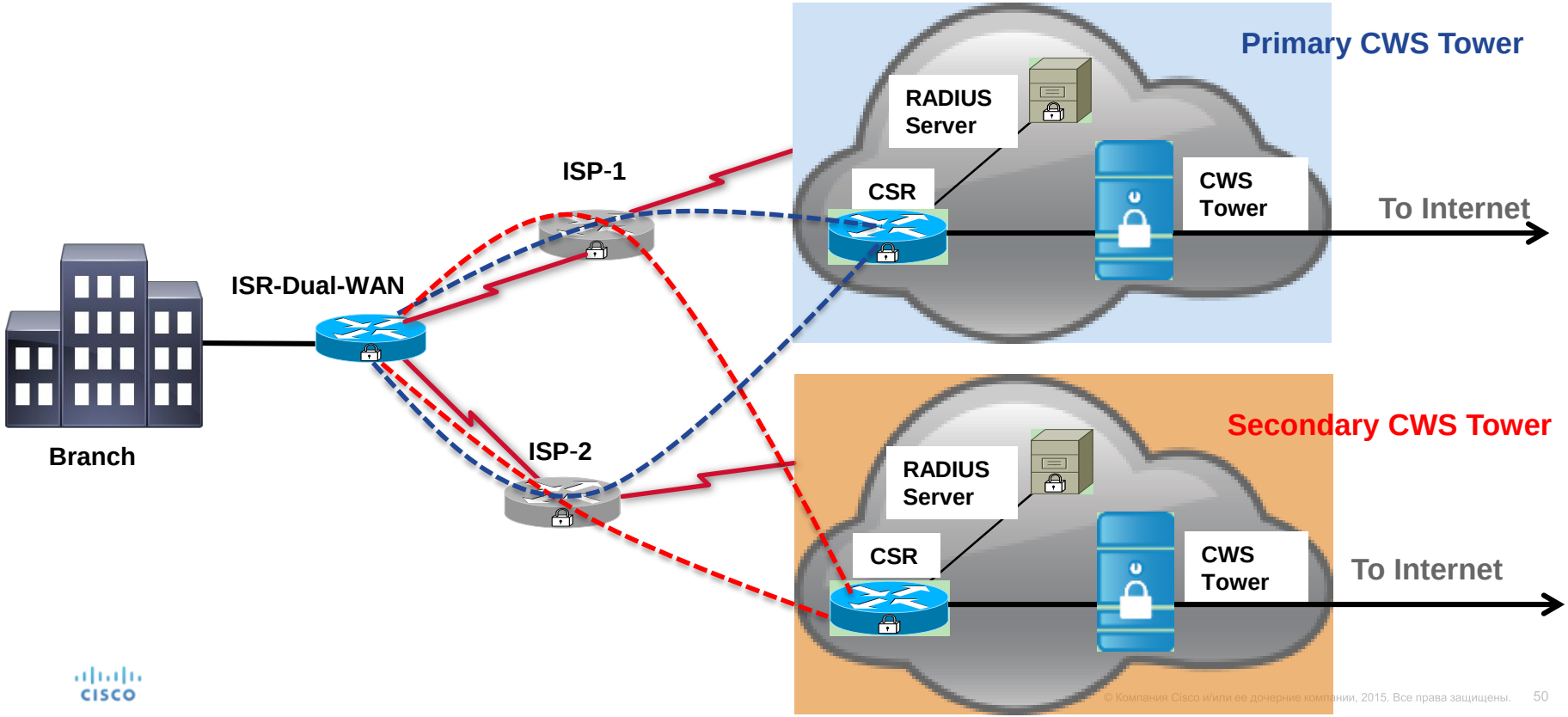


# Cisco Cloud Web Security (CWS)



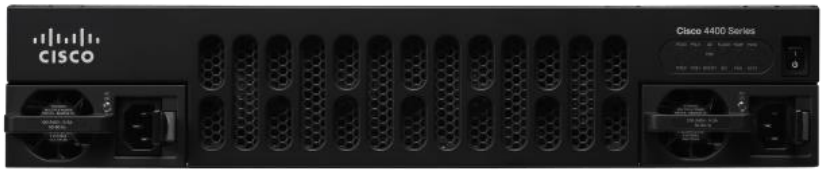

**CWS предоставляет целостную, управляемую, высокопроизводительную веб-безопасность и единую политику вне зависимости где и как пользователи выходят в Интерент**

# ISR 4k и CWS
## перенаправление с туннелированием



# SNORT powered IPS/IDS

VPN — ZBFW — **Snort IPS** — Umbrella Branch (OpenDNS) — Stealthwatch Learning Network — Firepower — CWS



# Snort IDS/IPS

- Больше 4 млн.  загрузок
- 500,000 зарегистрированных пользователей
- Широкоизвестный в мире IPS
- Решение требует:
  - SEC/AX лицензию
  - Подписку на обновление сигнатур (1Y или 3Y)

- Помогает пройти аудиты PCI DSS для филиалов
- Встроенная защита в филиальные роутеры ISR 4000
- Доплняет встроенную безопасность ISR 4000
- Легковесная защита с низкой стоимостью владения (TCO) и автоматизированными обновлениями
- Доступен мониторинг через splunk>

# Snort vs FirePower Thread Defense for ISR

| | Threats | Application visibility and control | Contextual awareness | Impact assessment | Automated IPS tuning | User identities | FireSIGHT |
|---|---|---|---|---|---|---|---|
| Snort IPS | ✓ | | | | | | |
| FirePower IPS and Apps | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

# Snort vs. FirePOWER Threat Defense

| | Snort | FirePOWER |
|---|---|---|
| IDS | Yes | Yes |
| IPS | Yes | Yes |
| Signature set | Snort | FirePOWER |
| Application Control and URL Filtering | No | Yes |
| Next Gen FW | No | Yes |
| SSL Traffic inspection | No | Yes, with the help of SSL decryption appliance |
| Advanced Malware Protection | No | Yes |
| Centralized Management | APIC EM IWAN App (March 2016)<br>Cisco Prime Infrastructure (Nov 2015) | FireSIGHT appliance |
| Centralized Monitoring | No (third-party tools) | FireSIGHT appliance |
| Application/Endpoint visibility and profiling | No | Yes |
| Performance | Less than 1 Gbps | Upto 40 Gbps |
| Compute required | 1 core CPU | 4 vCPUs |

# Community Rule Set vs Subscriber Rule Set

1. Memory – 8 G RAM
2. License – SEC-K9
3. Subscription
4. Container OVA installation
5. Container service activation
6. Enabling IPS/IDS
7. Enable Snort configuration
8. Reporting
9. Signature updates
10. Ability to whitelist

| | **Community Rule Set** | **Subscriber Rule Set** |
|---|---|---|
| Pricing | free | paid |
| Number of rules | 3000+ | 30,000+ |
| Coverage in advance of exploits | No | Yes |
| Signature availability | 30 days later | Fastest access to Talos signature updates |
| Snort Engine “Latest-1” compatibility | 90 days only | |
| SLA | No | |
| Level 3 support | No | Bugzilla |

# FirePOWER Threat Defense for ISR

VPN — ZBFW — Snort IPS — Umbrella Branch (OpenDNS) — Stealthwatch Learning Network — **Firepower** — CWS

# Cisco FirePOWER Threat Defense for ISR

Scalability

New

## Cisco UCS-EN120E

- **SKU:** UCS-EN120E
- **Cores:** 2
- **RAM:** 4-8GB (1DIMM)
- **HDD:** up to 200GB SSD Storage

## Cisco UCS-EN140N

- **SKU:** UCS-EN140N
- **Cores:** 4
- **RAM:** 4-8GB (1DIMM)
- **HDD:** up to 200GB SSD Storage

## Cisco UCS-EN120S

- **SKU:** UCS-EN120S-M2/K9
- **Cores:** 2
- **RAM:** 4-16GB (2 DIMMs)
- **HDD:** 2 hard-drives, available in 2 SAS and SATA options

## Cisco UCS-E140S

- **SKU:** UCS-E140S-M2/K9
- **Cores:** 4
- **RAM:** 8-16GB (2 DIMMs)
- **HDD:** 2 hard-drives, available in 3 SSD, SAS and SATA options

## Cisco UCS-E160D

- **SKU:** UCS-E160D-M2/K9
- **Cores:** 6
- **RAM:** 8-48GB (3 DIMMs)
- **HDD:** 3 hard-drives, available in SSD, SAS and SATA options

## Cisco UCS-E180D

- **SKU:** UCS-E180D-M2/K9
- **Cores:** 8
- **RAM:** 8-48GB (3 DIMMs)
- **HDD:** 3 hard-drives, available in SSD, SAS and SATA options

Feature Richness

* Hard drives Not included

# Говоря о сетевой безопасности филиалов думаем о ISR4000

Cisco ISR 4000 Series

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

# И помним, что безопасность – это не только фаерволл и VPN, это архитектура

Firewall

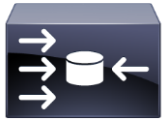
Callmanager

Voice Gateway

Cisco ISR 4000 Series

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

Server



WAN Optimzer & Content Cache

Switch

WLAN-Controller

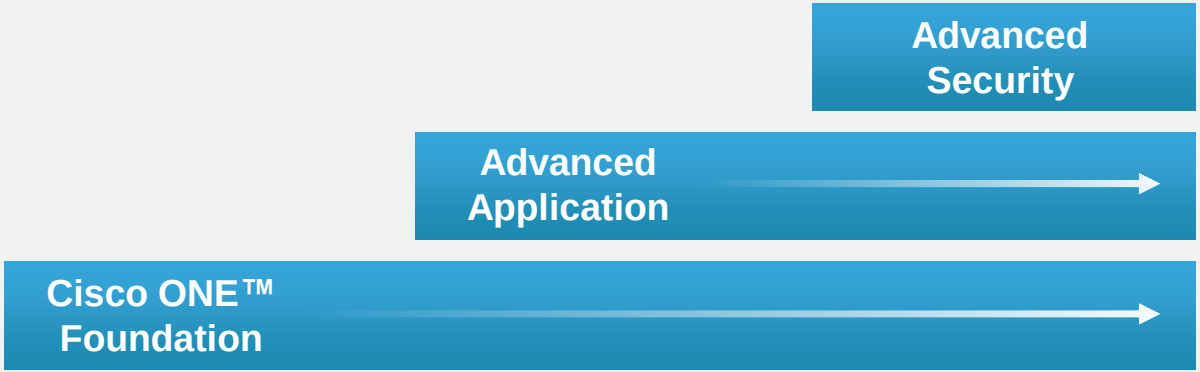
# Оптимизация расходов:
## шаг со стороны вендора

# Cisco ONE

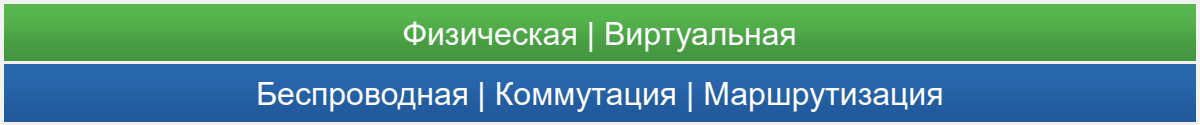
 

# Cisco ONE
# софт с железом – вместе дешевле

## 1 Функциональные возможности ПО




## 2 Платформа




## 3 Модель покупки

- Традиционная
- Подписка
- Корпоративная модель

# Выводы

# Cisco Digital Network Architecture


Сетевые приложения

**Управление сервисами как из облака**

TALOS + CWS + OpenDNS

REST API | developer.cisco.com

**Автоматизация**

SDN-контроллер Cisco
APIC-EM + ESA + Apps

**Аналитика**

StealthWatch + TALOS +
OpenDNS + AMP

Netconf/YANG | CLI | Netflow | Телеметрия

**Виртуализация**

IOS-XE 16.x + ISR 4000 + UCS-E + ECNS

**Интегрированная безопасность**

Полное покрытие архитектуры услугами безопасности

- Авоматизация и набюдаемость
- Безопасность и соответсвие требованиям регуляторов
- Возможность заглянуть изнутри и почерпнуть знания для инноваций

# Выводы

1. **Современная безопасность требует автоматизации всей сети.**
- Вся сеть как «устройство» безопасности
- Сами же устройства также должы уметь обеспечить безопасность

2. **SDN подход незаменим в деле автоматизации и безопасности.**
- Контроллер SDN Cisco APIC-EM бесплатент и доступен каждому
- Есть интересные и полезные бесплатные приложения
- Есть немного платных приложений
- Ждём интересные сценарии в виде последующих приложений

3. **Безопасность – это архитектура.**
- Сеть как составная часть общей архитектуры безопасности
- Комплиментарные решения безопасности вокруг сетевых устройств

4. **Много софта за дёшево – Cisco ONE.**

# Ждём интересные новинки на Cisco Enterprise Networks Forum!

# @ April 2017

# ПРИШЛО САМОЕ ЛУЧШЕЕ ВРЕМЯ

ДЕЛАТЬ УДИВИТЕЛЬНЫЕ ВЕЩИ