Cisco TechTalks

Новая эра корпоративных сетей с Cisco Catalyst 9000

Вебинар #7

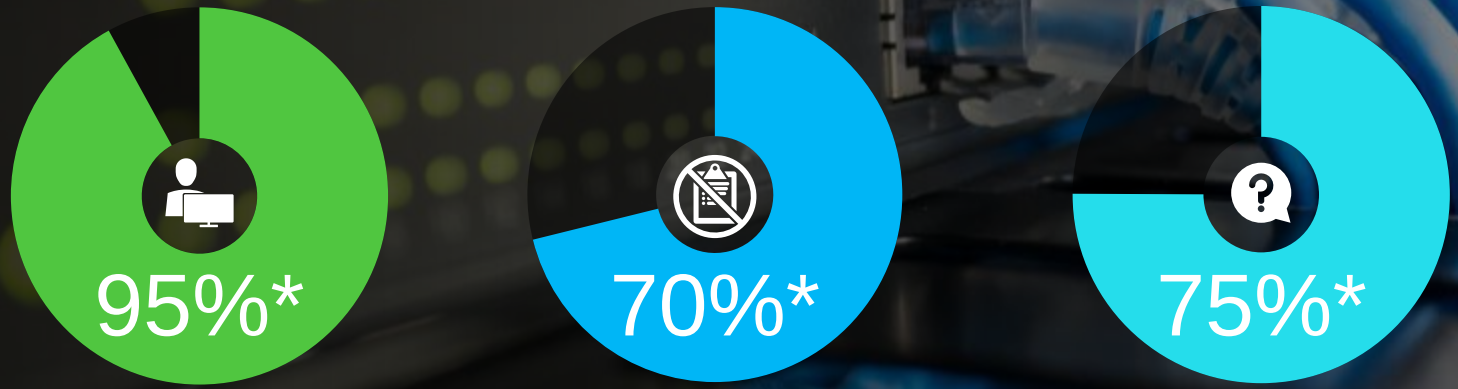
Andrew Ovrashko
System Engineer

22th June 2018

Корпоративные сети сегодня – сложные …

Управление множеством VLAN	Работа с различными сетями	Работа с множеством разных политик - LAN, WLAN, WAN, ЦОД	Масштабирование увеличивает сложность эксплуатации

…и имеют множество эксплуатационных проблем



доля ручного труда при внесении изменений

нарушений политик и правил из-за человеческих ошибок

Операционных расходов приходится на поиск неисправностей и диагностику

Традиционные сети НЕ ГОТОВЫ к быстрым темпам развития потребностей бизнеса

Что изменилось за последнее время?

IT = поддержка бизнеса **–> основа ведения бизнеса**

Сети стали сложнее: Wired + Wireless + Virtual + Remote Access.

Сложность поддержки единых политик по всей сети

Понятие «периметр сети» изменилось.

Больше требований к безопасности. **Сложнее реализация.**

Сетевые сервисы стали сложнее: BYOD, App experience, user mobility.

Значительно возросла нагрузка на IT подразделения.

Что изменится в ближайшее время?

IT персонала меньше, задач больше.

Требования к унификации и единому подходу.

От частных насроек к единым политикам.

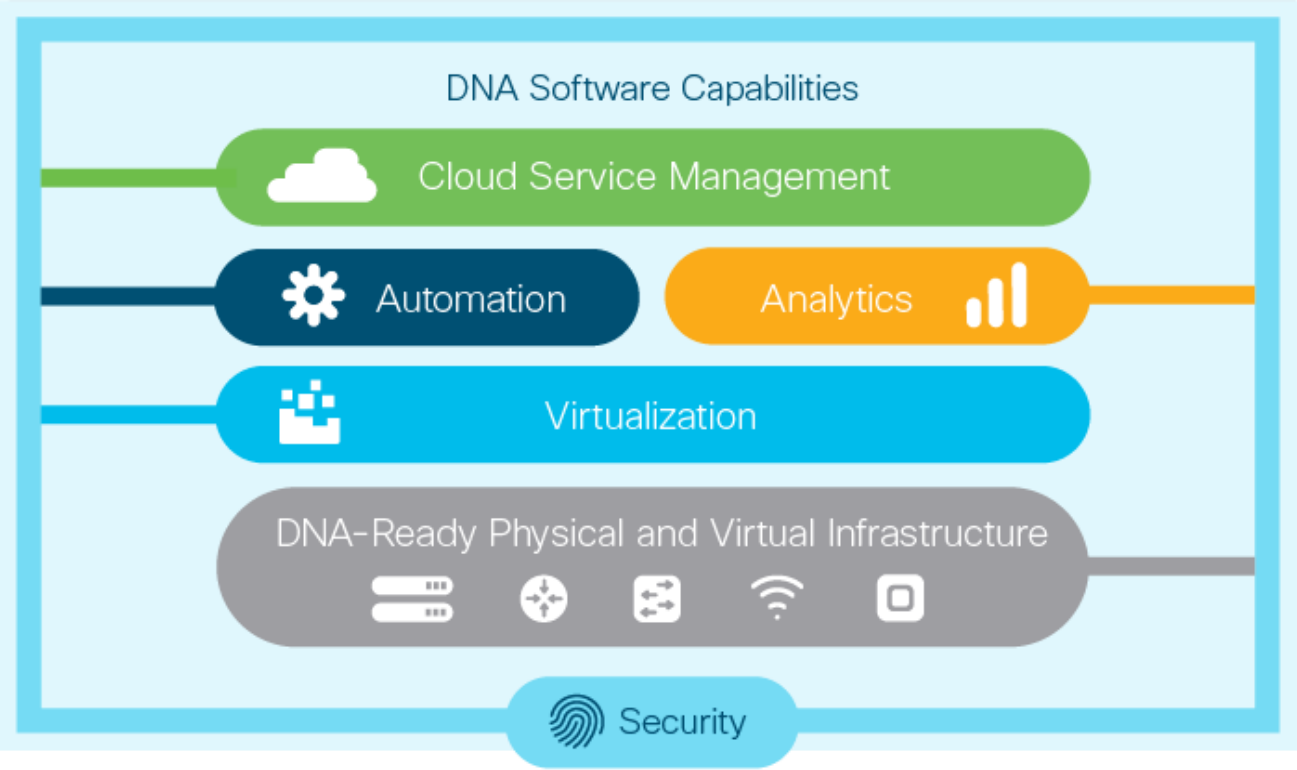
IT SECURITY = MUST HAVE!!

Сложнее угрозы ИБ. Всё больше шифрованного трафика.

Многомерные сети: App, Device, User, Network, Segmentation, IoT, Cloud

Новые подходы к построению сетей: SDN, network Fabric, NaaS/E

Cisco Digital Network Architecture (DNA)

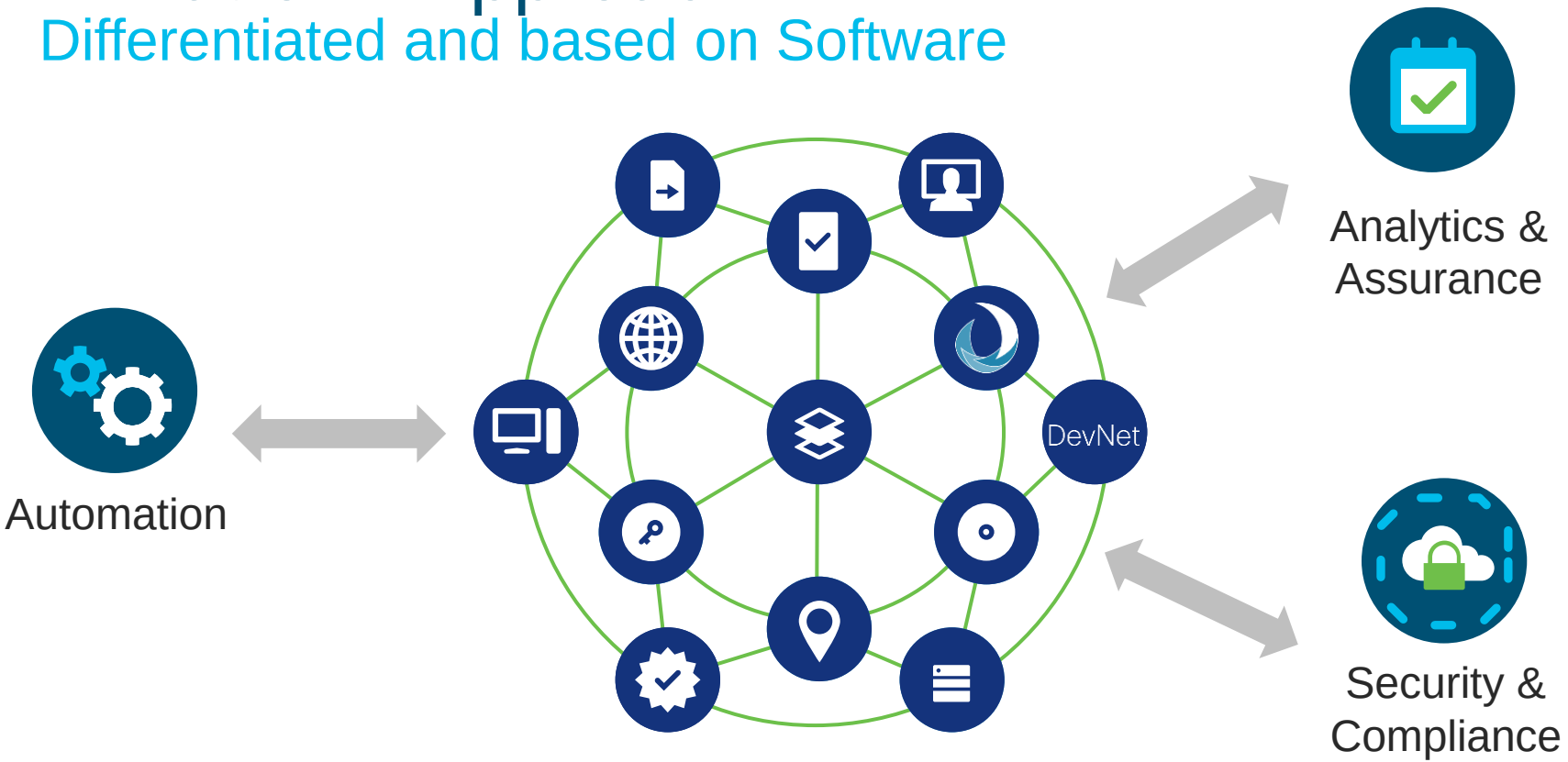


Cisco is rewriting the network playbook

Traditional network	The Network. Intuitive.
Hardware centric	Software driven
Manual	Automated
Fragmented security	Built-in security
Network data	Business insights

Powered by Cisco DNA™

A Platform Approach:
Differentiated and based on Software



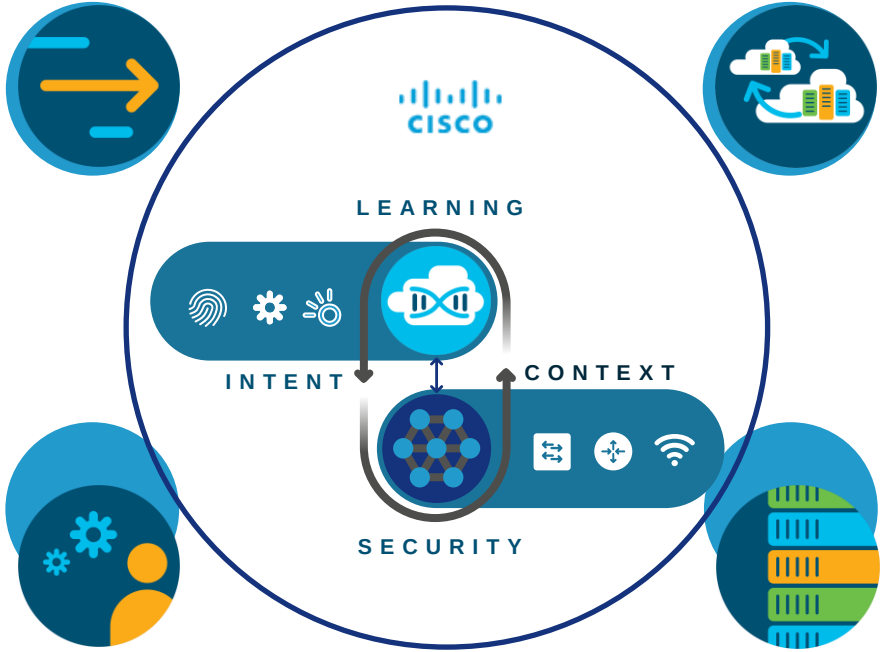
Intent-based network for

WAN

Optimize and secure application performance over any connection to the cloud.

Cloud Edge

Securely connect and protect workloads moving into the cloud and between clouds.



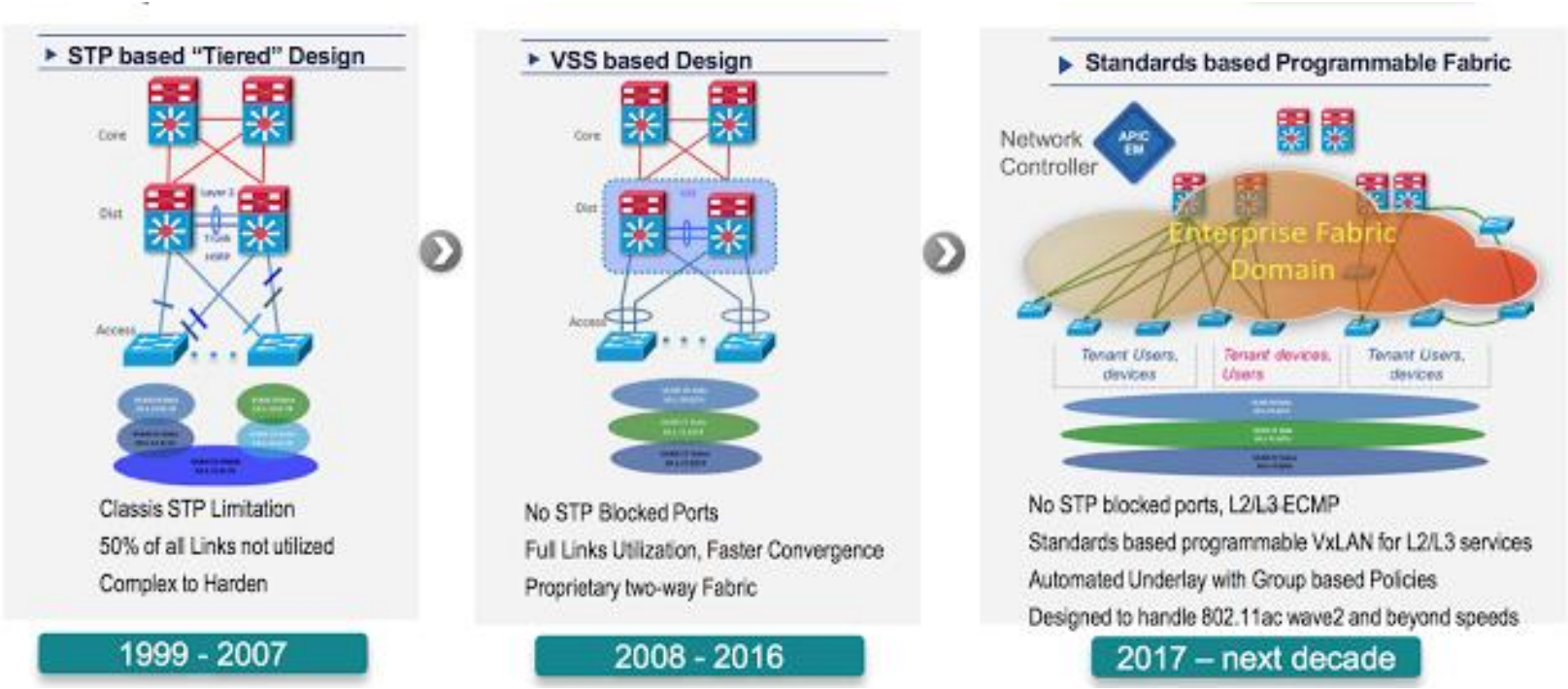
Access

Segment your network and secure user access from the edge to the cloud

Data Center

Run any traditional or cloud native application across any environment

Эволюция сетей



Оверлейный дизайн

Figure 1 *Layer 2 overlay–connectivity logically switched*

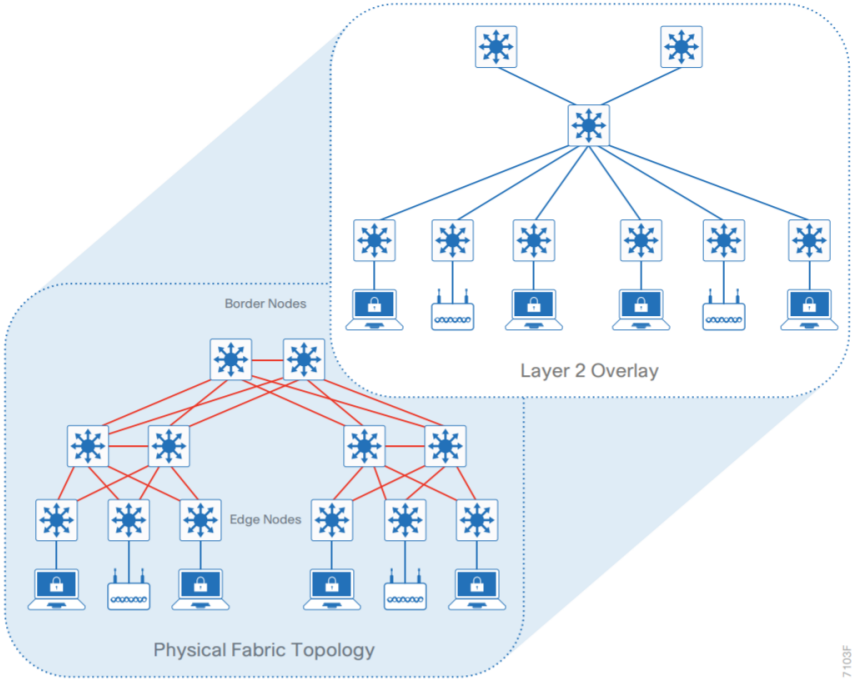
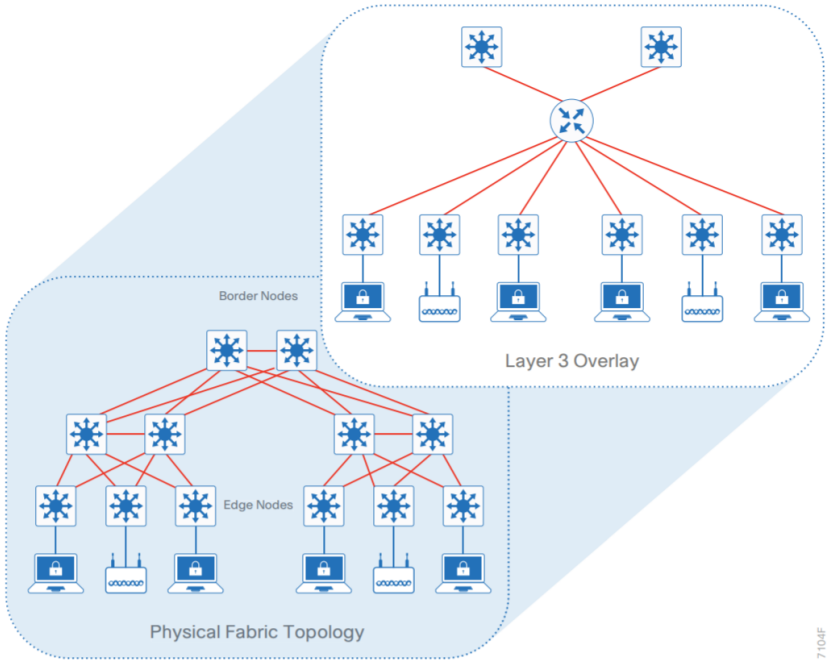
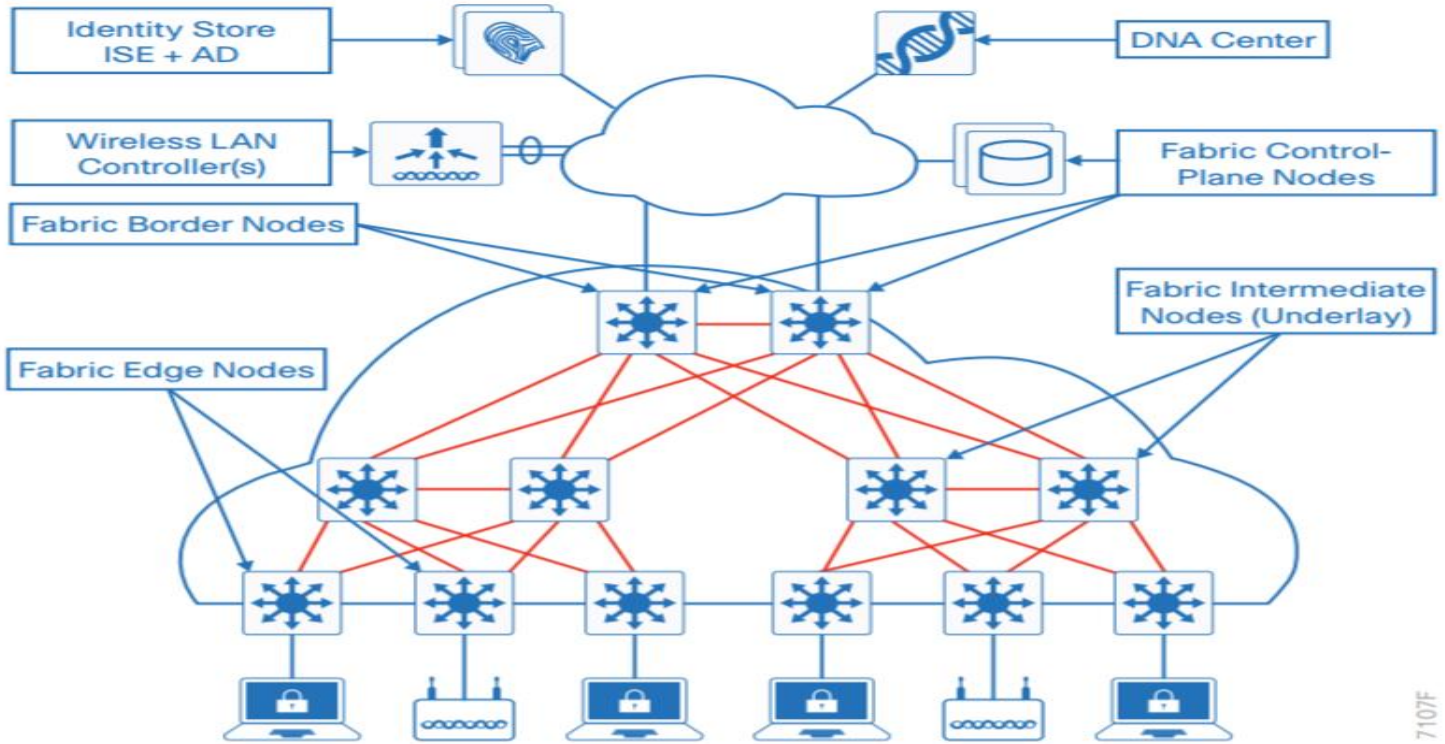


Figure 2 *Layer 3 overlay–connectivity logically routed*

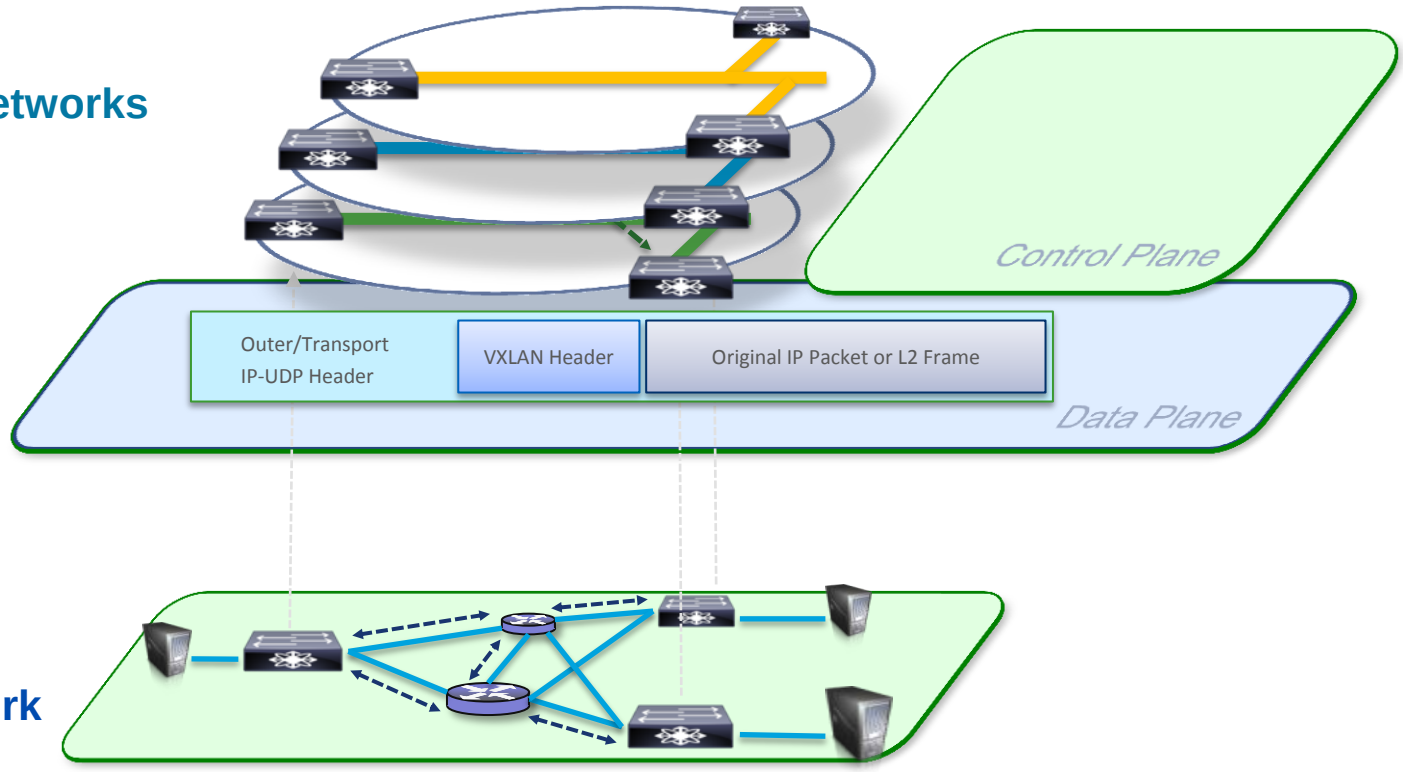


Новая архитектура с использованием «фабрики»

Figure 5 SD-Access solution and fabric components

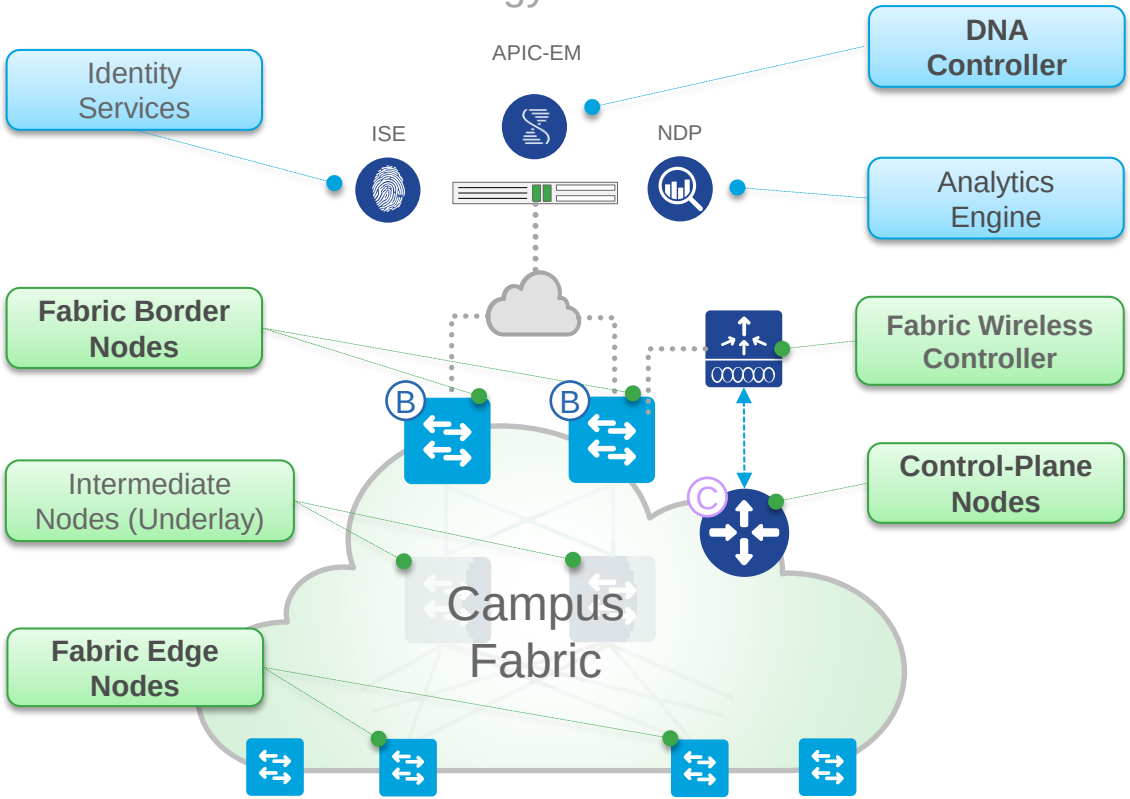


Упрощение части сети до единой «фабрики»



Из чего состоит фабрика SD-Access?

Fabric Roles & Terminology

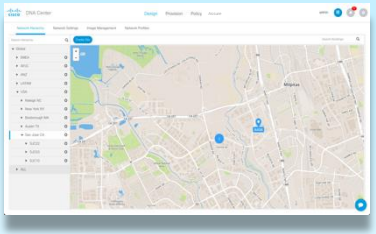


- **DNA Controller** – Enterprise SDN Controller (e.g. DNA Center) provides GUI management and abstraction via Apps that share context
- **Identity Services** – External ID System(s) (e.g. ISE) are leveraged for dynamic Endpoint to Group mapping and Policy definition
- **Analytics Engine** – External Data Collector(s) (e.g. NDP) are leveraged to analyze Endpoint to App flows and monitor fabric status
- **Control-Plane Nodes** – Map System that manages Endpoint to Device relationships
- **Fabric Border Nodes** – A Fabric device (e.g. Core) that connects External L3 network(s) to the SDA Fabric
- **Fabric Edge Nodes** – A Fabric device (e.g. Access or Distribution) that connects Wired Endpoints to the SDA Fabric
- **Fabric Wireless Controller** – A Fabric device (WLC) that connects Wireless Endpoints to the SDA Fabric

DNA Center

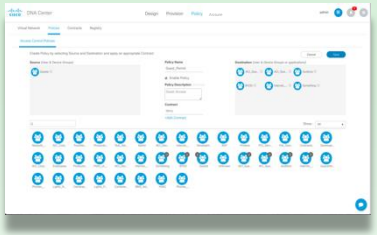
SD-Access 4 Step Workflow

Design



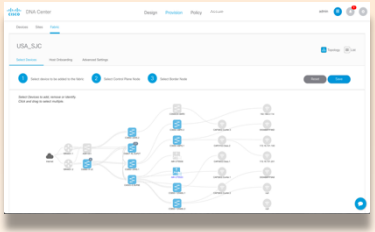
- Global Settings
- Site Profiles
- DDI, SWIM, PNP
- User Access

Policy



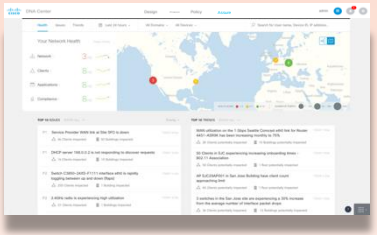
- Virtual Networks
- ISE, AAA, Radius
- Endpoint Groups
- Group Policies

Provision



- Fabric Domains
- CP, Border, Edge
- FEW / OTT WLAN
- External Connect

Assurance



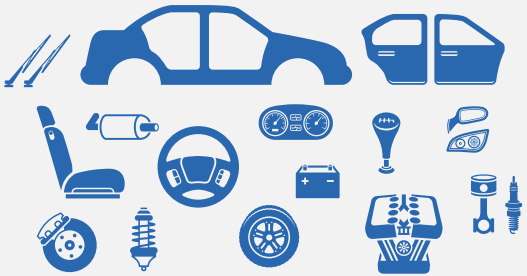
- Network Health
- 360º Views
- FD, Device, Client
- Path Traces

Planning & Preparation

Installation & Integration

Simplification Creates Agility

DO-IT-YOURSELF ASSEMBLY AND INTEGRATION



SDN

READY TO GO

SD-Access

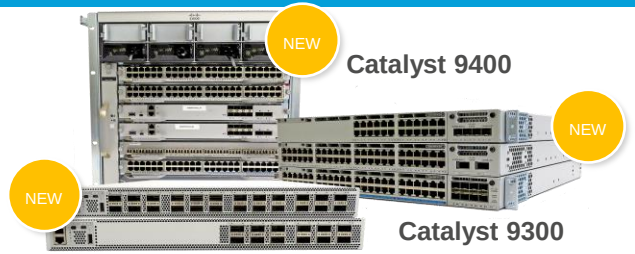
Faster Time to Market and Lower OpEx

Applications Are the Vehicle for Digital Business

SD-Access – поддержка на оборудовании

Полная защита инвестиций

Switching

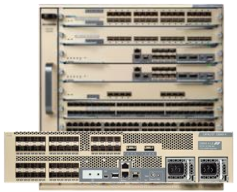


Catalyst 9400

Catalyst 9300

Catalyst 9500

Catalyst 4500E



Catalyst 6K

Nexus 7700

Catalyst 3850 and 3650

Routing

ASR-1000-X

ASR-1000-HX

ISR 4430

ISR 4450

CSRv

Wireless

AIR-CT5520

AIR-CT8540

Wave 2 Aps
(1800, 2800,3800)

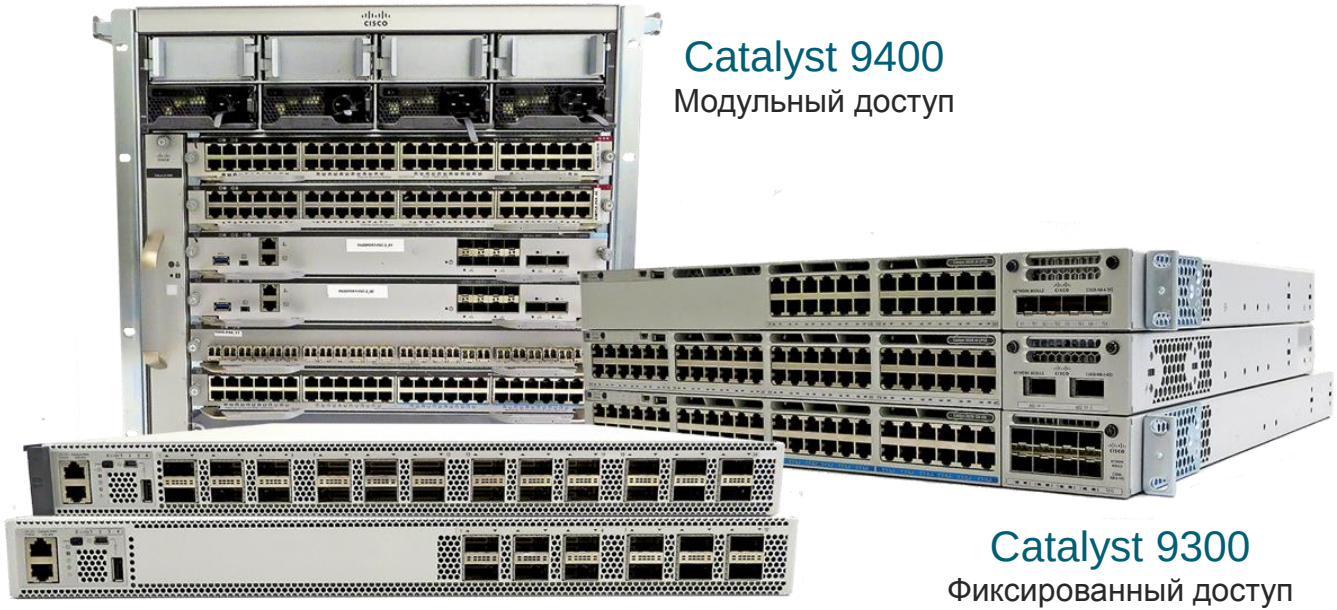
Wave 1 Aps
(1700, 2700,3700)*

Subtended Nodes

CDB

3560-CX

Семейство коммутаторов Catalyst 9K



Catalyst 9400
Модульный доступ

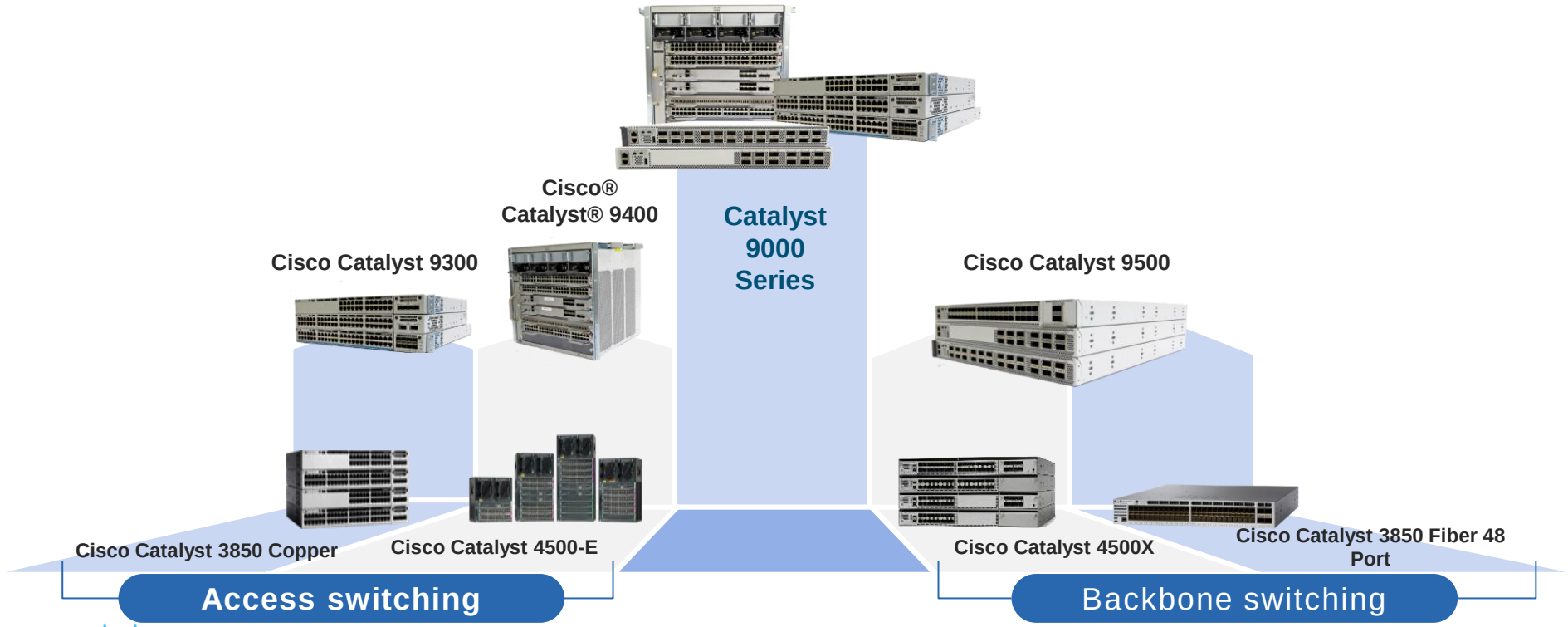
Catalyst 9300
Фиксированный доступ

Catalyst 9500
Фиксированное адро

Cisco Catalyst 9000 инновации
UADP 2.0
Cisco IOS® XE Software
SD-Access
x86 CPU and containers
Encrypted Traffic Analytics
AES256/MACSEC256*
Trustworthy systems
StackWise® Virtual*
IEEE1588 and AVB*
NBAR2
Perpetual/fast PoE
Model-driven programmability
Patching/GIR
Streaming telemetry*

Единое ПО, возможности, лицензирование

Cisco Catalyst 9000 platform transitions



Catalyst 9K: Advantage vs. Essentials

* Future

Advantage

DNA Advantage (Inclusive of DNA Essentials)

3,5,7 Year Terms

Software-defined Access
Policy-based Automation and Assurance, Fabric Enabled Wireless

Assurance & Analytics
Network insights from analytics and machine learning, clients and applications covering on-boarding, connectivity and performance

Security & IoT
Encrypted Traffic Analytics, mDNS GW, NAT/PAT

Telemetry & Visibility
ERSPAN, AVC, NBAR2

Network Advantage (Inclusive of Network Essentials)

Perpetual

Enhanced Security Controls
MACSEC-256

Flexible Network Segmentation
VRF, VXLAN, LISP, Trustsec, SD-Wireless, MPLS L3VPN

IoT & Mobility
CoAP

High Availability & Resiliency
NSF, GIR, Stackwise Virtual, ISSU, Patching

Full Routing Functionality
BGP, HSRP, OSPF, ISIS, HSRP,GLBP

Optimize Bandwidth Utilization with Multicast
MSDP, mVPN, AutoRP, PIM-BIDIR

Essentials

DNA Essentials

3,5,7 Year Terms

Cisco Differentiators
Containers, Python, EEM, ANI, Flexible NetFlow, Wireshark

Basic Automation
Plug and Play, EasyQOS Configuration*

Basic Monitoring Capabilities
EasyQOS Monitoring*, Client and Device 360, PSIRT Compliance*

Element Management
Image and Patch Management, Topology and Discovery

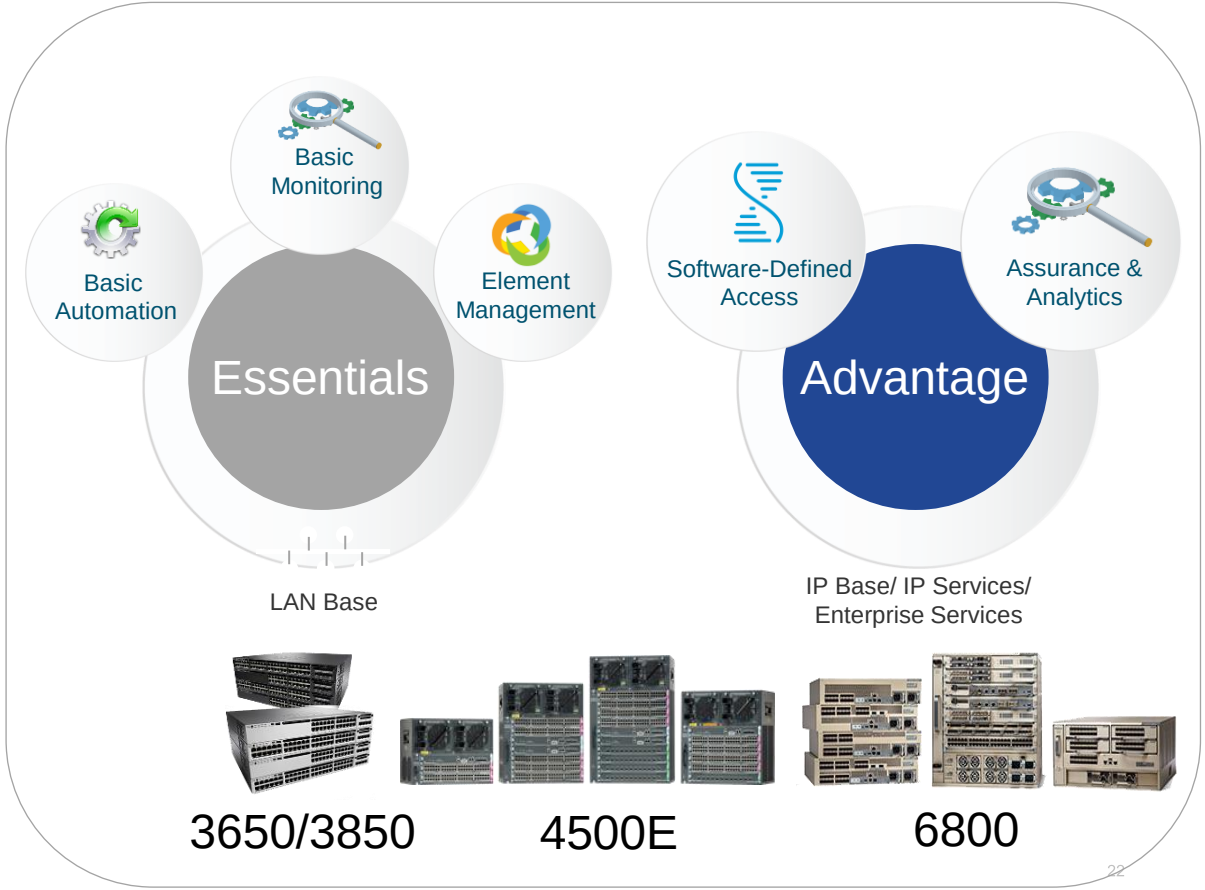
Perpetual

Essential Switch Capabilities
Layer 2, Routed Access, PIM Stub, PVLAN, VRRP, PBR, CDP, QoS, FHS, 802.1x, Macsec-128, CoPP, Trustsec SXP, IP SLA Responder, SSO

Telemetry & Visibility
Sampled NetFlow, SPAN, RSPAN

Inclusive of Switch and DNA Center Capabilities

Introducing DNA Add-on Licenses for 3K, 4K, 6K



Единый софт + программируемые ASIC

- **Full NetFlow** (unsampled)
- Flexible NetFlow (FNF)
- *Trailers:* AVC / SGT
- ETA

- App hosting / **Containers**
- **GIR**
- **Patching** / Fast SW upg

- **MPLS**
- **LISP**
- **VXLAN**

- **SXP classification**
- **TrustSec/SDA scale**
- **SGT-ACL**
- **SD-Access**

- **Advanced NAC**
- **VLAN per MAC**

- **IoT**

- **UPOE 60W (100W)**
- **Fast PoE**
- **Perpetual PoE**

- **C9300: StackPower**

- **Cat9400: ISSU**

- **mGig**

- **MACSEC** на всех портах
- **AES-128**
- **AES-256**

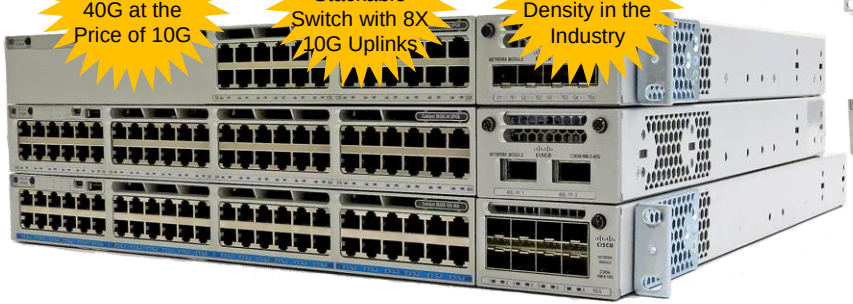
Представляем Catalyst 9300

Новое решение для фиксированного доступа

2.5G at the Price of 1G 40G at the Price of 10G

Only Stackable Switch with 8X 10G Uplinks

Highest 2.5G/mGig Density in the Industry



1G Data

24 Ports

1G UPOE/POE+

mGig UPOE

48 Ports

Modular Fans

Modular Uplinks

8x10G | 2x40G | 4x mGig | 4x1G

Modular Power Supplies

350W | 715W | 1100 W

Catalyst 9K Leadership

- UADP 2.0
- Open IOS-XE
- SD-Access
- X86 CPU & Containers
- Encrypted Traffic Analytics (ETA)*
- 256 bit MACSEC*
- Trustworthy Systems
- StackWise Virtual*
- IEEE1588 & AVB*
- NBAR2
- Perpetual/Fast PoE
- Model Driven Programmability
- Patching/GIR
- Streaming Telemetry*

*not available at FCS

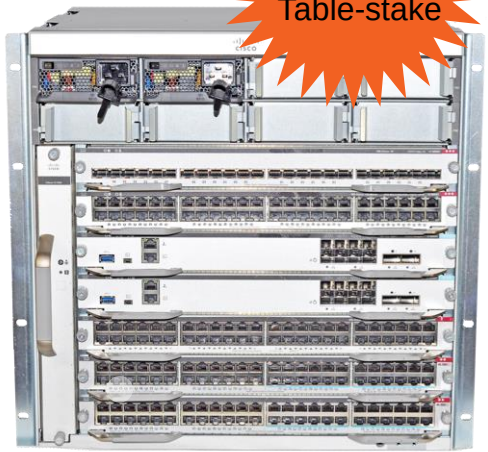
Представляем Catalyst 9400

Новое решение для модульного доступа

Industry's Highest PoE Scale

4-Slot*

Redundancy is now Table-stake



7-Slot

9Tbps System b/w

10-Slot

Catalyst 9K Leadership

- UADP 2.0
- Open IOS-XE
- SD-Access
- X86 CPU & Containers
- Encrypted Traffic Analytics*
- 256 bit MACSEC*
- Trustworthy Systems
- StackWise Virtual*
- IEEE1588 & AVB*
- NBAR2
- Perpetual PoE*
- Model Driven Programmability
- Patching/GIR
- Streaming Telemetry*

Supervisor	Access Linecards	Core Linecards	Power Supply
Sup-1: 80G/Slot Access Optimized Sup-1XL*: 120G/Slot Core Optimized	24xmGig + 24xUPOE* 48xUPoE 48xPoE+* 48xData	24x 10G SFP+* 48x1G SFP* 24x1G SFP*	3200W AC 3200W DC* 2400W AC*

*not available at FCS

C9500 Portfolio

Shipping

C9500-24Q

- 24 x 40G
- QSFP+ Ports
- 4 x UAPD 2.0
- AC/DC* 950 W PS
- N+1 FRU FAN Modules
- USB 3.0 Module
- IOS-XE 16.5.1a

Shipping

C9500-12Q

- 12 x 40G
- QSFP+ Ports
- 2 x UAPD 2.0
- AC/DC* 950 W PS
- N+1 FRU FAN Modules
- USB 3.0 Module
- IOS-XE 16.6.1

Shipping

C9500-40X

- 40 x 1/10G + 8x1/10G or 2x40G
- SFP/SFP+ Ports
- 2 x UAPD 2.0
- AC/DC* 950 W PS
- N+1 FRU FAN Modules
- USB 3.0 Module
- IOS-XE 16.6.1

Mar `18

C9500-16X

- 16 x 1/10G + 8x1/10G or 2x40G
- SFP/SFP+ Ports
- 1 x UAPD 2.0
- AC/DC* 950 W PS
- N+1 FRU FAN Modules
- USB 3.0 Module
- IOS-XE 16.8.1

* Roadmap

C9500H Portfolio

Mar `18

C9500H-32C

- 32 x 100G/40G
- QSFP28 Front Panel Ports
- 2 x UADP 3.0
- AC/DC – 1.6KW PS
- N+1 FRU FAN Modules
- FRU SSD Module
- IOS-XE 16.8.1

Mar `18

C9500H-32QC

- 32 x 40G or 16x100G
- QSFP28 Front Panel Ports
- 1xUADP 3.0
- AC-650W/DC-930W PS
- 1+1 FRU Redundant FAN Modules
- FRU SSD Module
- IOS-XE 16.8.1

Mar `18

C9500H
(48Px10G+4Px100G)

- 48x25G/10G/1G + 4x100G/40G
- SFP+/SFP28/QSFP28 Front Panel Ports
- 1x UADP3.0
- AC – 650W/DC -930W PS
- 1+1 Redundant Fan Trays
- FRU SSD Module
- IOS-XE 16.8.1

Mar `18

C9500H
(24Px10G+4Px100G)

- 24x25G/10G/1G + 4x100G/40G
- SFP+/SFP28/QSFP28 Front Panel Ports
- 1x UADP 3.0
- AC – 650W/DC -930W PS
- 1+1 Redundant Fan Trays
- FRU SSD Module
- IOS-XE 16.8.1

Catalyst 9500 & 9500H

Granular Port Densities for All Campus Sizes

Today
March 2018
Roadmap

Max Port Densities	C9500-16X	C9500-40X	C9500-12Q	C9500-24Q	C9500H (24Px10G+ 4Px100G)	C9500H (48Px10G+ 4Px100G)	C9500H-32QC	C9500H-32C
1G	24	48	12	24	24	48	32	32
10G	24	48	12	24	28	52	32	32
40G	2	2	12	24	4	4	32	32
100G	-	-	-	-	4	4	16	32
10G Breakout	-	-	48	48	40	64	68	108

Double it with SWV

12 – 216 Ports in 1 RU

Granular Port Densities

Port Speeds from 1G to 100G

Ready for Deployments

For supported pluggables, breakouts etc. visit http://switching.cisco.com/roadmaps

Сценарии использования Cisco и Business Impact

Безопасность

- Ролевой доступ к сети (Network Access Control).
- Сегментация сети (микро- и макро-) в зависимости от роли.
- Полная интеграция Cisco сети и Cisco безопасности + eco-partners.

Мониторинг

- Продвинтутый мониторинг агрегированной сетевой статистики (NetFlow) с машинным обучением и множеством готовых шаблонов.
- Обнаружение malware в шифрованном трафике.
- Network Data Platform как часть Cisco DNA Center.

Автоматизация

- Простота внедрения сети любого масштаба
- Многомерные инструменты (network, user, app, compliance) траблшутинга
- Business insights

Наиболее интересные сценарии применения Cisco Catalyst 9k

- #1 TrustSec with Scalable Group Tag (SGT)
- #2 DEFence rediness CONditions (DEFCON) with Scalable Group Tag (SGT)
- #3 Rapid Threat Containment (RTC)
- #4 Encrypted Traffic Analytics (ETA)
- #5 VLAN per MAC
- #6 MACSec
- #7 Sofware Defined Access (SDA)
- #8 Application Visibility and Control (AVC)
- #9 Readiness for innovations

Сегментация сети

Зачем нужна сегментация сети:

- ❑ Уменьшение доменов отказа
(network broadcast domain, troubleshooting domain)
- ❑ Удобство построения политики доступа между сегментами
(списки контроля доступа, ACL)
- ❑ Уменьшение доменов поражения угрозами ИБ

Зачем нужна динамическая микросегментация сети:

- ➢ Простота создания политик по схеме «сегмент=пользователь(группа)»
(RBAC, Role Based Access Control)
- ➢ Динамика позволяет не только автоматически дать доступ, но и забрать
(RADIUS CoA[Change of Authorization]; NaaE [Network-as-Enforcer], RTC [Rapid Threat Containment])
- ➢ Аутентификация пользователей и их устройств в конкретном месте и времени
(CBAC, Context Based Access Control)

Сценарии использования Cisco и Business Impact

#1 TrustSec with Scalable Group Tag (SGT)

Case / issue:

- Сотрудники ждут очереди для перехода между командами, потому что Helpdesk перегружен запросами

Root cause:

- Текущие списки доступа (ACL) привязаны к IP-адресации
- Каждый сайт – свой уникальный IP-pool, количество сетей – мультипликатор политик доступа (ACL)

[45 групп сотрудников] X [20 сайтов] = **900 разных ACL (!!!)**

Group Policy based segmentation

Solution:

- Переход на SGT даст возможность иметь всего 45 ACL (по одной для группы)
- Возможно частичное и/или стадийное внедрение с сохранением текущей парадигмы с ACL
- Возможны гибридные схемы со старым и сторонним оборудованием (есть ограничения и нюансы)

Business impact: **HIGH**

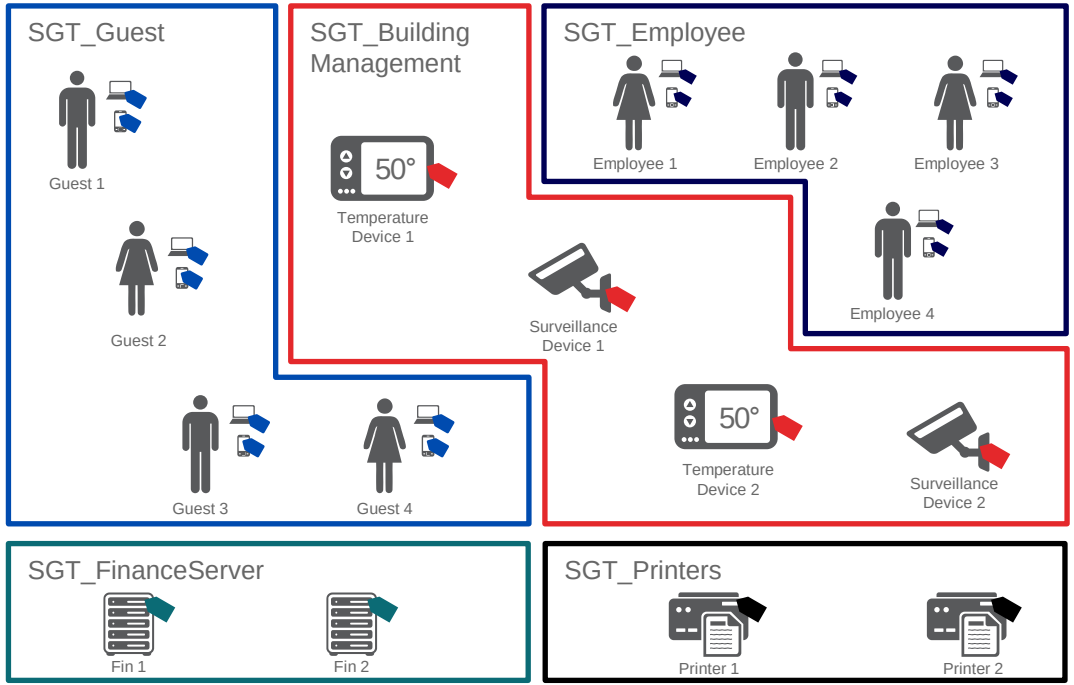
- Agile IT
- Повышение общего уровня информационной безопасности
- Полная наблюдаемость сетевых взаимодействий, простота поддержки и аудита
- Однозначно определённая политика безопасности

/24

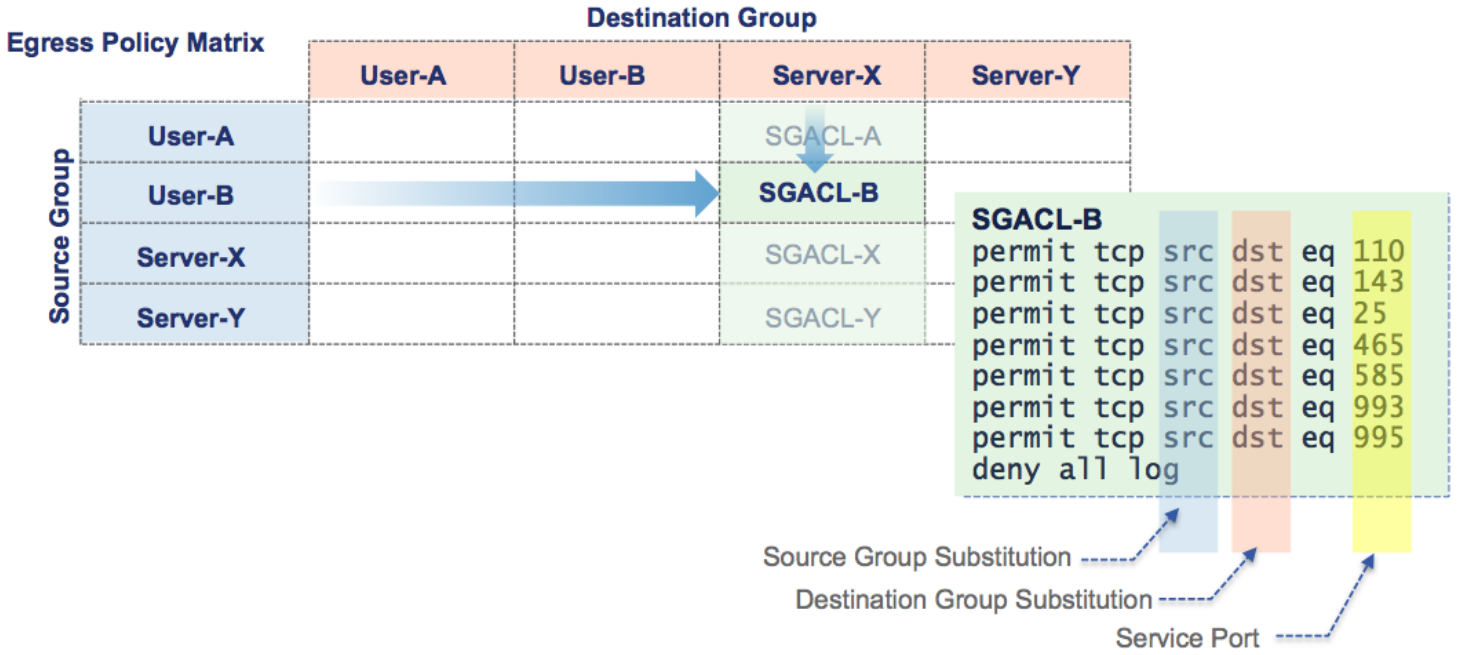
Decoupling policy from subnet

ISE обеспечивает **сегментацию** сети

- Для любых пользователей и устройств
- В качестве инструмента могут быть **любые сетевые устройства** (файерволы, коммутаторы, маршрутизаторы, WiFI…)



Security Group Access Control Lists



Сценарии использования Cisco и Business Impact

#2 DEFence rediness CONditions (DEFCON) with Scalable Group Tag (SGT)

Case / issue:
Необходимо быстро (почти мгновенно) изменить права доступа по всей сети, например в случае вирусной эпидемии, но в текущих реалиях это невозможно, так как требует изменения множества ACL

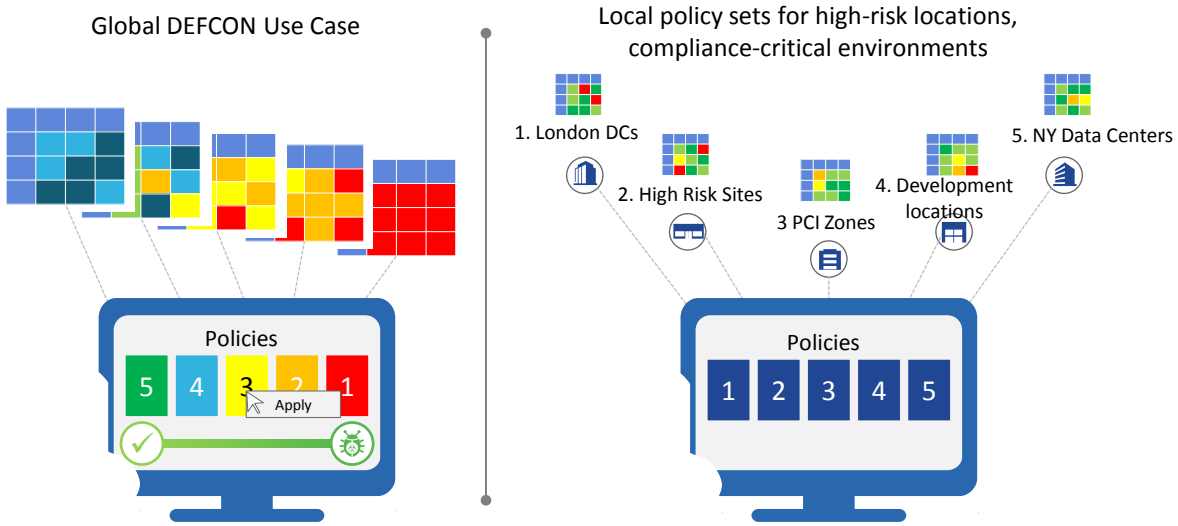
Root cause:
- Текущие списки доступа (ACL) привязаны к IP-адресации
- Каждый сайт – свой уникальный IP-pool
- Нет единой, полностью детерминированной, матрицы доступа

«Красная кнопка»
План «Б»

Solution:
- Политики доступа по SGT привязаны к единой (!) матрице доступа между группами
- DefCon подход предусматривает, что таких «единых матриц» доступа может быть несколько – каждая для своего случая.
- Переключение между матрицами доступа «мирного времени» и «состояния войны» практически мгновенное
- Интеграция с эко-партнёрами по pxGrid (McAfee, Splunk etc.)

Business impact: **HIGH**
- Уменьшение влияния брешей ИБ (минимизация охвата поражения в результате реализации угроз ИБ)
- Business continuity (возможность изолировать LoB приложения от источников угроз)
- Скорость реализации экстренной реакции [переход на «План Б» за считанные минуты]

Политики безопасности с учетом уровня угрозы



DEFCON (аббревиатура, англ. *DEFense readiness CONdition* — готовность обороны) — шкала готовности вооружённых сил Соединённых Штатов Америки. Стандартный протокол в мирное время — DEFCON 5. DEFCON 1 соответствует ожиданию немедленной полномасштабной атаки

Политики DefCon для сети

Multiple levels of policy sets
Applied globally

Standard Policy

Source \ Destination	LoB 1 Employee	LoB 2 Employee	Partner 1	Partner 2	PCI Server	Shared Apps	LoB 1 Apps	LoB 2 Apps
LoB 1 Employee	✓	–	–	–	–	✓	✓	–
LoB 2 Employee	–	✓	–	–	–	✓	–	✓
Partner 1	–	–	✓	–	–	✓	–	–
Partner 2	–	–	–	✓	–	✓	–	–
POS Terminal	–	–	–	–	✓	–	–	–

Ограничение распространения

DEFCON3 Policy

Source \ Destination	LoB 1 Employee	LoB 2 Employee	Partner 1	Partner 2	PCI Server	Shared Apps	LoB 1 Apps	LoB 2 Apps
LoB 1 Employee	–	–	–	–	–	✓	✓	–
LoB 2 Employee	–	–	–	–	–	✓	–	✓
Partner 1	–	–	✓	–	–	–	–	–
Partner 2	–	–	–	✓	–	✓	–	–
POS Terminal	–	–	–	–	✓	–	–	–

Сценарии использования Cisco и Business Impact

#3 Rapid Threat Containment (RTC)

Case / issue:
Необходимо быстро и автоматически изолировать заражённых пользователей (например, при выявлении обращения к командным центрам бот-нетов)

Root cause:
- Продукты ИБ и контроль сетевого доступа не связаны
- Множество клиентов без каких либо агентов на ОС (виртуалки, BYOD, *nix OS)
- Множество клиентов сети не в домене (виртуалки, BYOD, *nix OS)

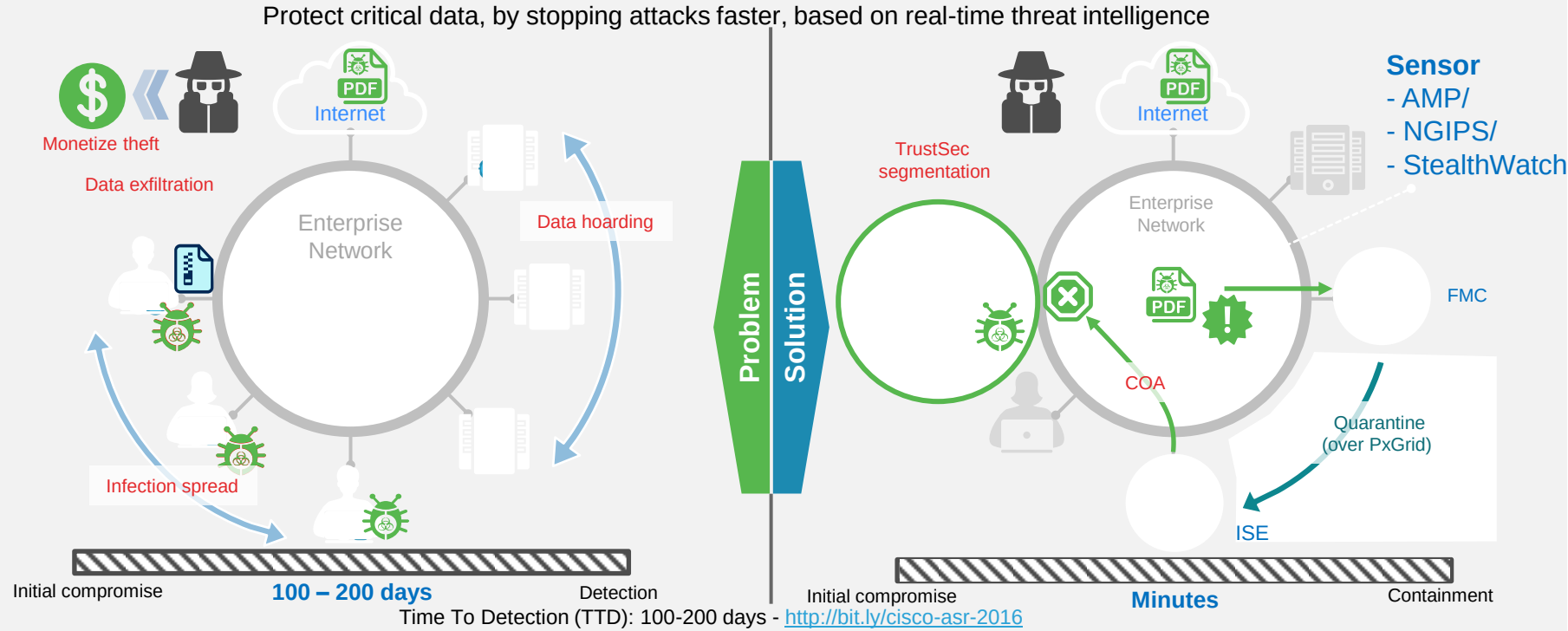
Solution:
- Автоматизация взаимодействия инструментов ИБ и систем контроля доступа к сети (RTC)
- Реакция на события от продуктов ИБ Cisco (AMP, StealthWatch, FirePower)
- Интеграция с эко-партнёрами по pxGrid (McAfee, Splunk и многие другие.)

Связка сети и безопасности

Business impact: **HIGH**
- Уменьшение влияния брешей ИБ (минимизация охвата поражения до единичного хоста)
- Business continuity (точечная изоляция/карантин)
- Не требует вмешательства администратора (24X7)
- Дополнительная ценность от уже купленных продуктов ИБ и мониторинга

Объединяем все вместе Rapid Threat Containment (RTC)

Быстрое реагирование



Сценарии использования Cisco и Business Impact

#4 Encrypted Traffic Analytics (ETA) with StealthWatch

Encrypted Traffic Analytics

Case / issue:

- В сети множество шифрованного трафика и его доля растёт из года в год
- Это слепая зона для всех продуктов безопасности

Root cause:

- Malware зачастую использует шифрованные коммуникации (SSL/TLS).
- Без расшифровки трафика понять malware или не-malware трафик в текущих реалиях нет возможности
- Поставить агентское ПО (чтобы увидеть трафик до шифрования) на каждый хост (VMs, BYOD) нет возможности
- SSL offload адресует только часть трафика (много SSL/TLS шифрования, трафик malware)

Solution:

- Переход на свичи, которые могут экспортровать NetFlow в Stealthwatch
- Переход на свичи с поддержкой ETA (не все NetFlow устройства поддерживают ETA)
- Управление автоматической реакцией через ISE - Rapid Threat Containment (RTC)

Business impact: **HIGH**

- Бесклиентская защита сети
- Полная наблюдаемость **всех** сетевых endpoint (виртуалок, устройств за хабами и тп)
- Операционная эффективность (нет необходимости заставлять пользователей вводить виртуалки в домен или вручную ставить агентское ПО)
- Обнаружение malware там, где раньше его нельзя было обнаружить **с эффективностью более 99% (!!) и false positive <0.1%**

Что позволяет обнаруживать NetFlow?

Сканирование сети

Сканирование TCP, UDP, портов по множеству узлов

Обнаружение ботнетов

Когда внутренний узел общается с внешним сервером C&C в течение длительного периода времени

Отказ в обслуживании

SYN Half Open; ICMP/UDP/Port Flood

Фрагментированные атаки

Узел отправляет необычный фрагментированный трафик

Изменение репутации узла

Потенциально скомпрометированные внутренние узлы или получение ненормального скана или иные аномалии

Распространение червей

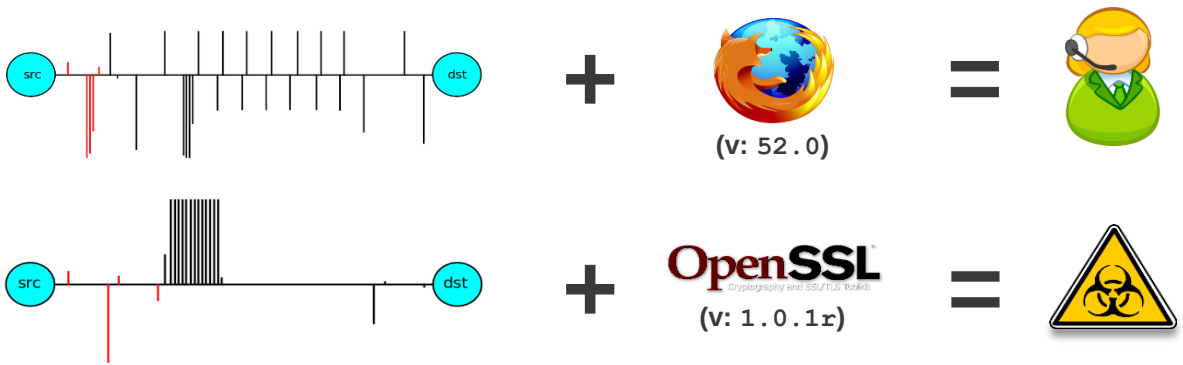
Инфицированный узел сканирует сеть и соединяется с узлами по сети; другие узлы начинают повторять эти действия

Утечки данных

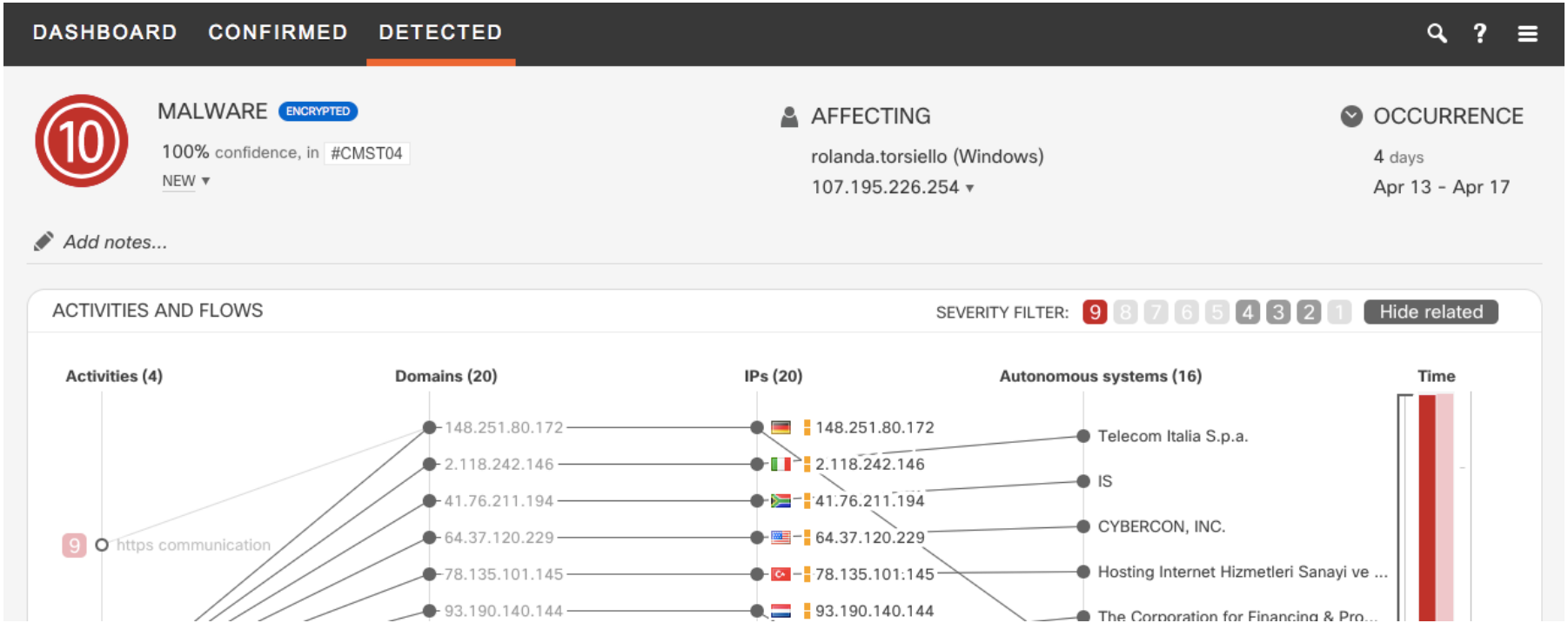
Большой объем исходящего трафика VS. дневной квоты

Как узнать в шифрованном трафике «зло»?

- 6 лет сбора статистики + машинное обучение + аналитика
- 180 патентов
- **Множество методов и техник**
- Точность 99%
- Ложных срабатываний 0,01%



Encrypted Traffic Analytics: Example Incident

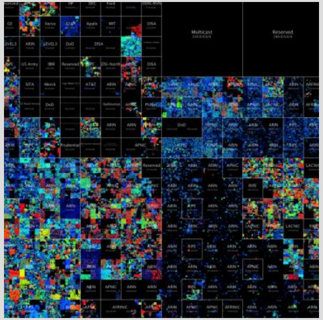


How do we inspect encrypted traffic?

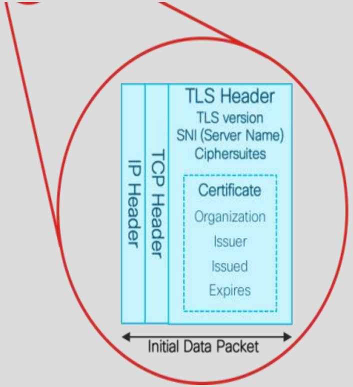
Global risk map	Initial Data Packet	Sequence of Packet Lengths and Times

Who's who of the Internet's dark side

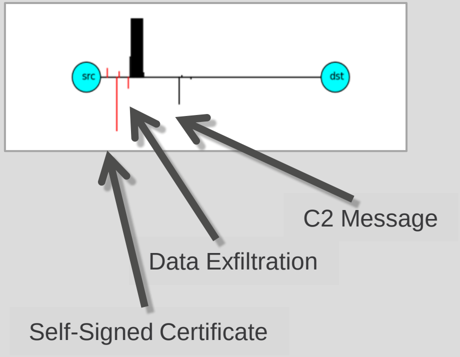
Make the most of the unencrypted fields



Broad behavioral information about the servers on the Internet.

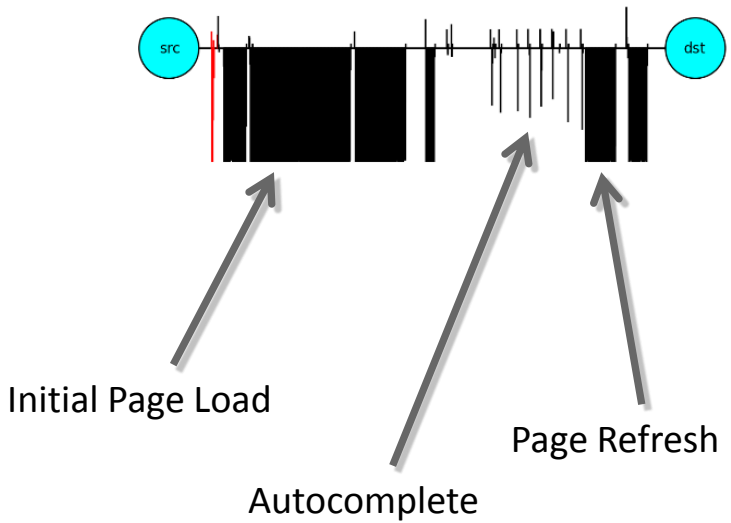


Identify the content type through the size and timing of packets

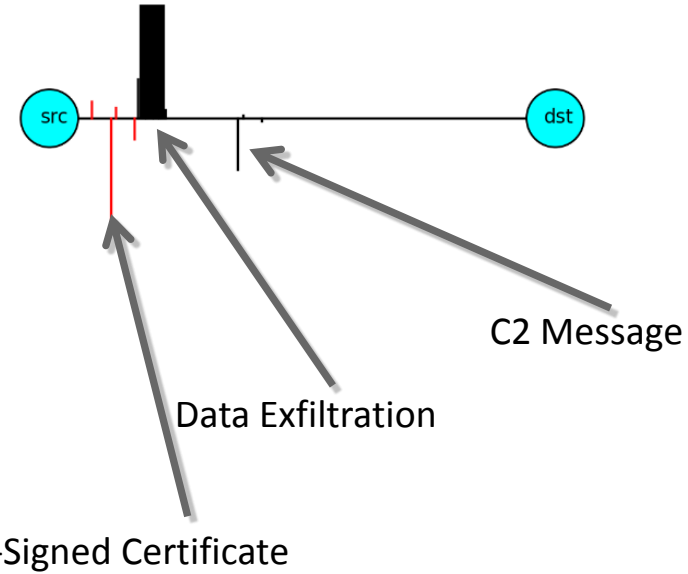


Behavioral Patterns w.r.t. Packet Lengths/Times

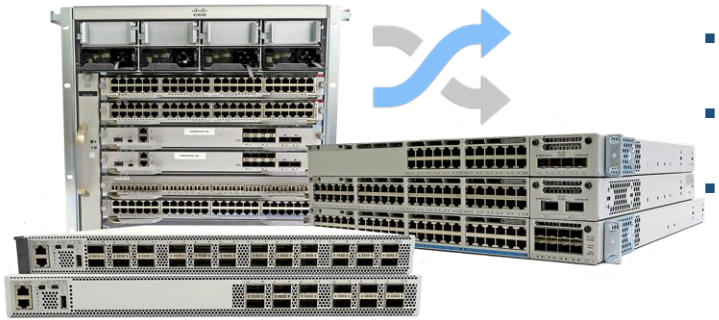
Google Search



Bestafera



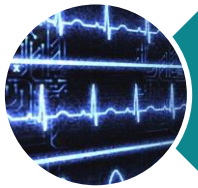
Эксклюзивная поддержка ETA на Catalyst 9K



Специализированная телеметрия

- **Netflow Data:** SrcIP, DstIP, SrcPort, DstPort, Proto, #Bytes, #Packets
- **Intraflow Data:** Sequence of Packet Lengths & Times (SPLT), Byte Distribution, …
- **TLS Metadata:** Extensions, Ciphersuites, SNI, Certificate Strings, …

Основная задача

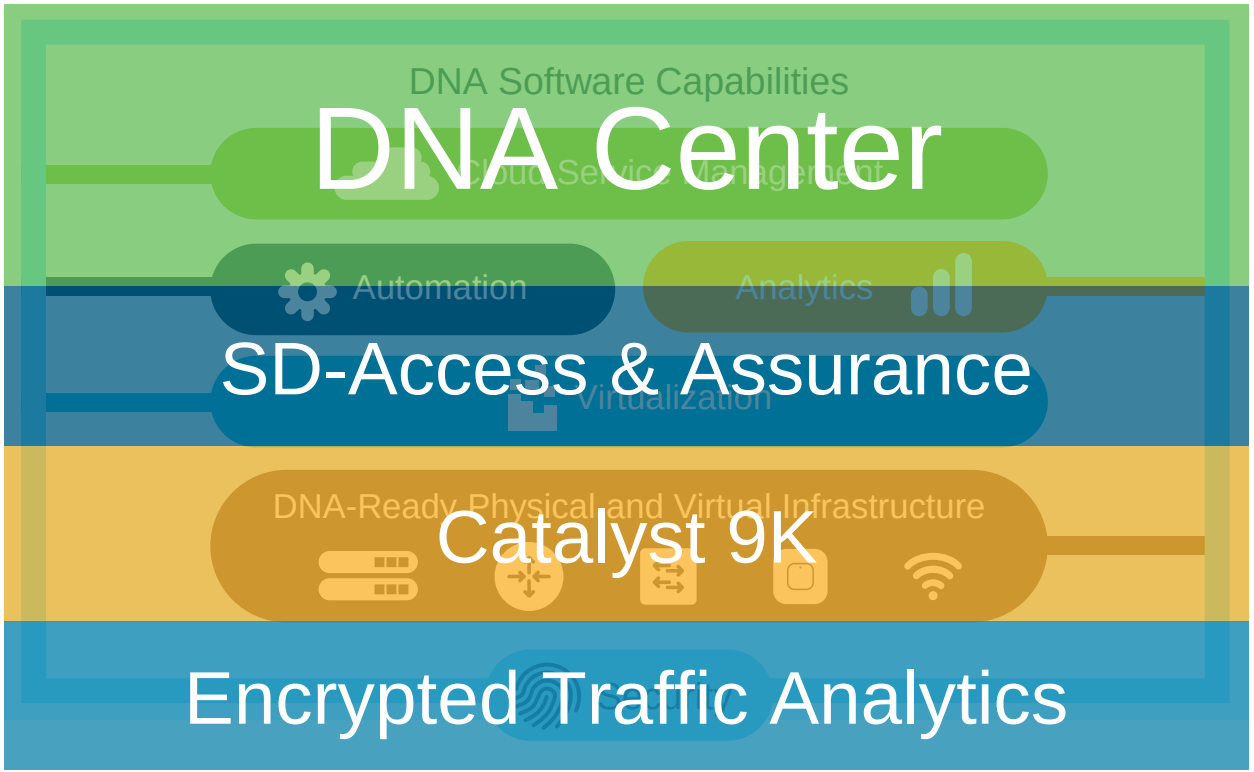


Обнаружение угроз в зашифрованном трафике

Вторичная задача

Аудит использования криптографии

Digital Network Architecture – What's New



[Q1] Можно ли купить Cat9k без подписки DNA?

- Нет. Обязательная покупка минимум 3 летней подписки DNA.
- Подписка предоставляет ongoing access to innovations (AVC, ETA, …)
- Даже с подпиской стоимость владения выходит дешевле

- В зависимости от необходимого функционала есть выбор:

DNA Essential (активирует также вечную лицензию Network Essential)

DNA Advantage (активирует также вечную лицензию Network Advantage)

C1 (DNA-Adv + ISE-Base + ISE-Plus + StealthWatch)

[Q2] Что будет когда подписка кончится?

- Всё будет работать как и раньше (Right-to-Use)
- Останется полное право пользоваться функционалом постоянных лицензий Network Essential/Advantage
- Если нужен функционал с подписок – надо купить подписку DNA

- На данный момент функционал не контролируется (RTU)
- Никто не обещает что так будет всегда (читать соглашение EULA)

[Q3] Мне нужны DNA-Advantage не везде, но пока не знаю точно где?

- Cisco Smart Licensing позволяет перемещать лицензии по устройствам в пределах одного Smart Account
- Перемещение в пределах группы совместимых устройств

- На данный момент функционал не контролируется (RTU)
- Никто не обещает что так будет всегда (читать соглашение EULA)