Проводные и беспроводные решения Cisco для организации удаленного домашнего офиса

Юрий Довгань

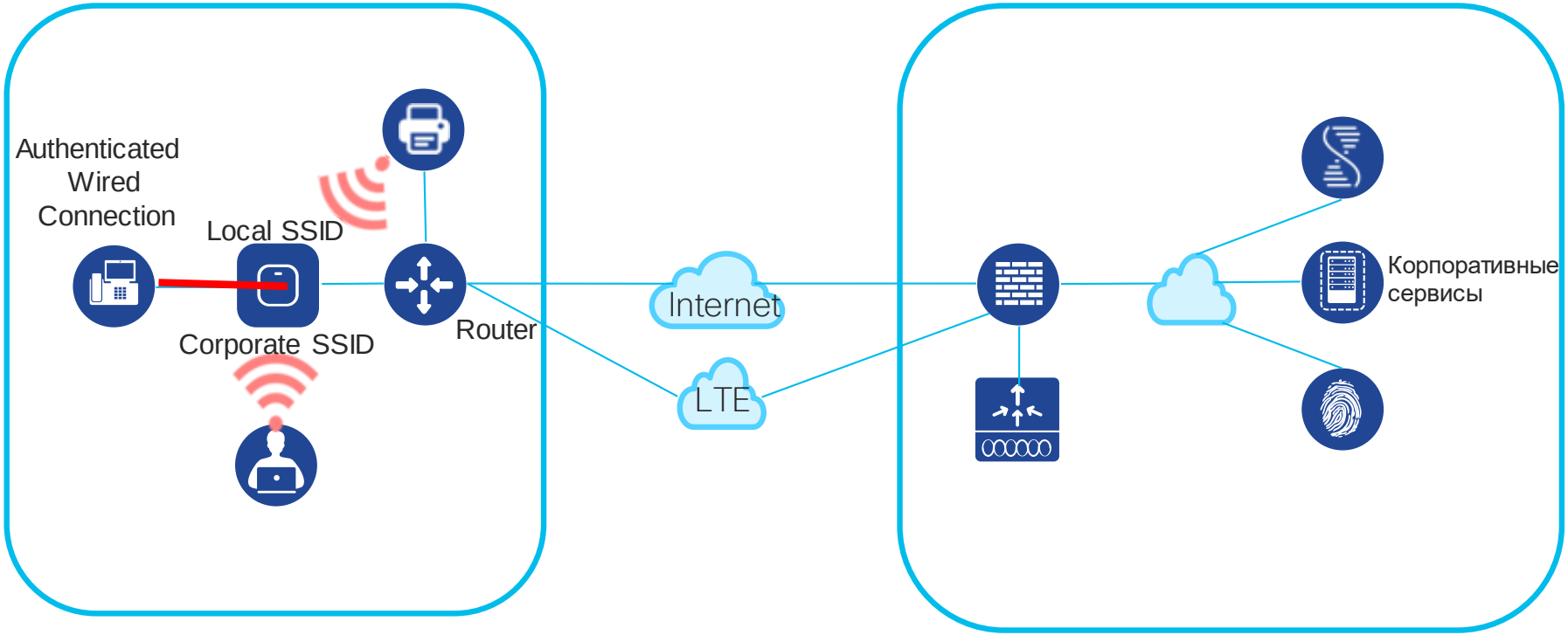
Системный инженер

ydovgan@cisco.com

Удаленный домашний офис: требования

1. Быстрое и прозрачное для сотрудника внедрение офиса (Zero Touch Provisioning)
2. Безопасность: конфиденциальность передаваемых данных (Auto-VPN), проверка аутентичности устройства, защита от атак (NGFW, DNS Security etc.) при прямом выходе в Интернет
3. Пользовательский опыт при доступе к корпоративным ресурсам (отказоустойчивость каналов, выбор оптимального канала, работа SaaS приложений)
4. Беспроводной доступ с разделением корпоративных и домашних сервисов
5. Подключение и аутентификация корпоративных устройств: IP-телефон, видеотерминал. PoE, 802.1x, QoS.

Архитектура подключения удаленного домашнего офиса



Варианты внедрений

Teleworker Options

Cisco SD-WAN

Поддержка платформ:
- ISR1000
- ISR 4000/ASR1000
- Cloud or On-Prem

Преимущества:
ZTP, Automation, SLA-routing, WAN-optimization, SaaS-optimization, Security

VPN remote Access

Platform Support:
- AnyConnect VPN
- ISE (AAA)
- NGFW or ASA
- Duo (optional for dual auth)

OEAP Cisco Controller On-Prem Solution

Поддержка платформ(вар. 1)
- WLC
- AP3500 and newer

Поддержка платформ(вар. 2)
- WLC
- OEAP600, AP1810, AP1815T

Преимущества:
- Existing APs reuse
- Remote Ethernet with option 2

Meraki Teleworker Cloud Based Solution

Поддержка платформ:
- Meraki MX series Security Appliance
- Meraki Z3/Z3C Teleworker Gateway
- Meraki MR series

Преимущества:
- Cloud managed
- Simple and fast configuration
- Zero-touch deployment
- Use existing MR's if available
- Integrated cellular on C models
- Enhanced Security on MX models (AMP, Sourcefire IDS/IPS, Content Filtering, Umbrella)
- Application performance monitoring on MX models (Meraki Insight)

CVO Router

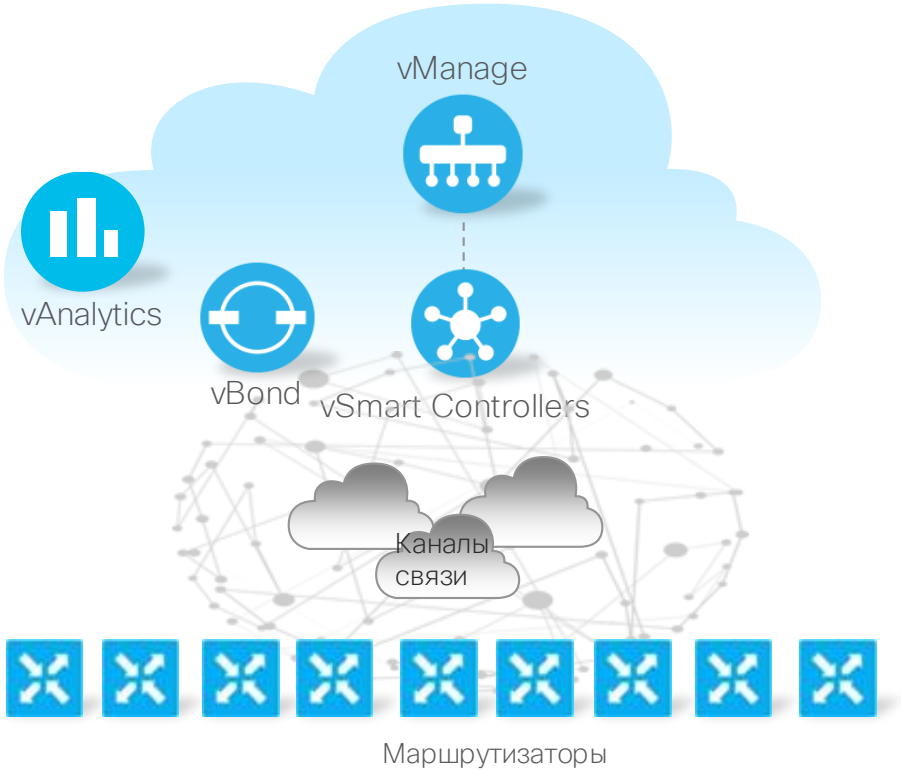
Поддержка платформ
- Cisco Integrated Services Router (ISR) G2
- Cisco Unified IP Phone (optional)
- Head-end with a VPN router

Преимущества:
- Enhanced security
- Remote wired/wireless access to corporate resources

Cisco SD-WAN

Обзор решения Cisco SD-WAN

Применение SDN принципов к распределенным сетям

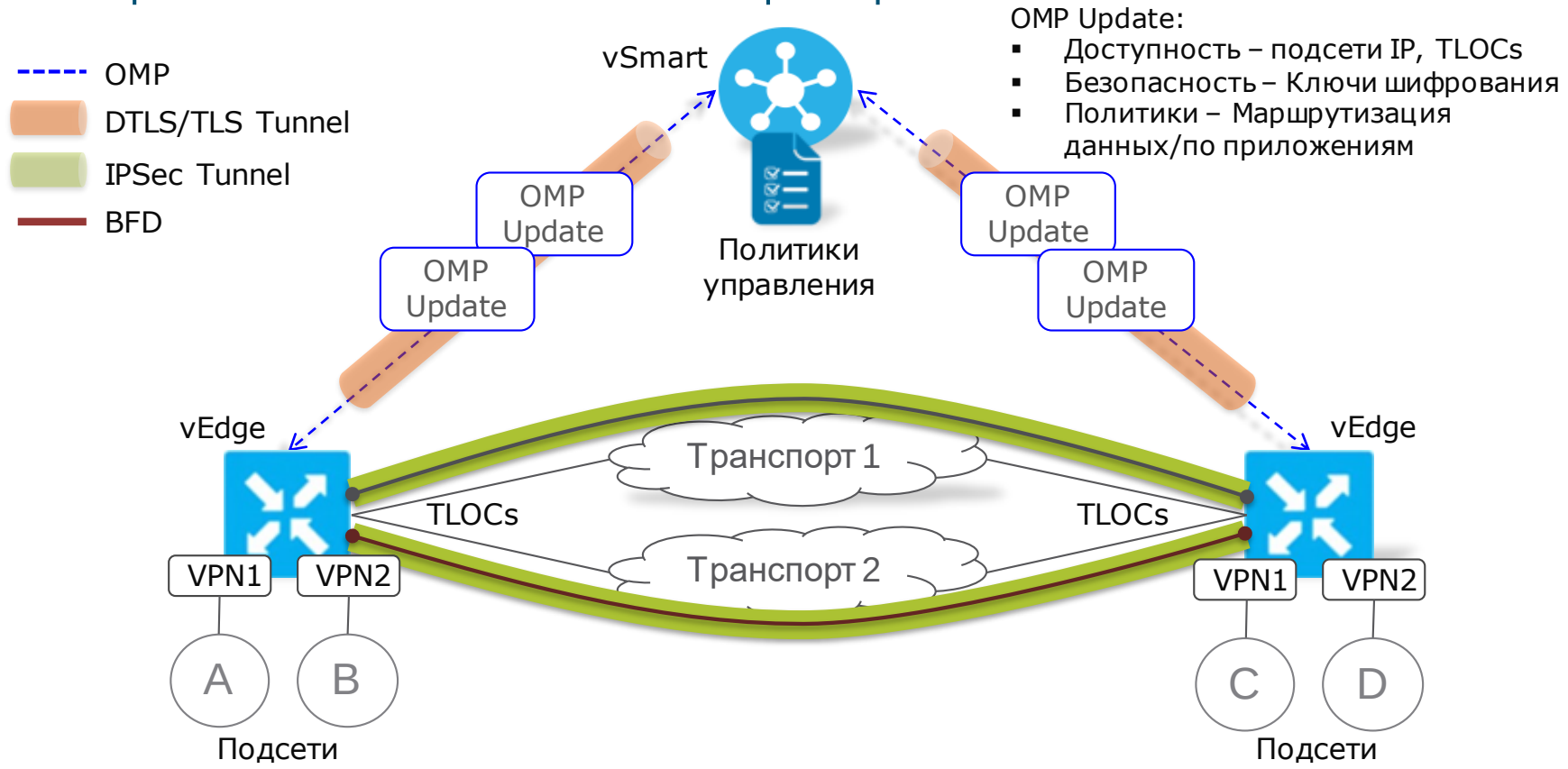


Администрирование/ Оркестрация

Плоскость управления (Control Plane)

Плоскость передачи данных (Data Plane)

Как работает SD-WAN фабрика



Платформы для Cisco SD-WAN

Только SD-WAN

vEdge 100

50-100M

vEdge 1000

175-300M

vEdge 2000

vEdge 5000

1-2G

ISR 1100-4G

125-220M

ISR 1100-6G

300-550M

SD-WAN с сервисами

ISR 1000

Next-gen Performance Flexibility

50-200M

ISR 4000

Modular Integrated services

ASR 1000

High-performance with redundancy

1.6-19G (Basic)
0.7-9G (Medium)

Виртуализация

ENCS 5100

ENCS 5400

Публичные и частные облака

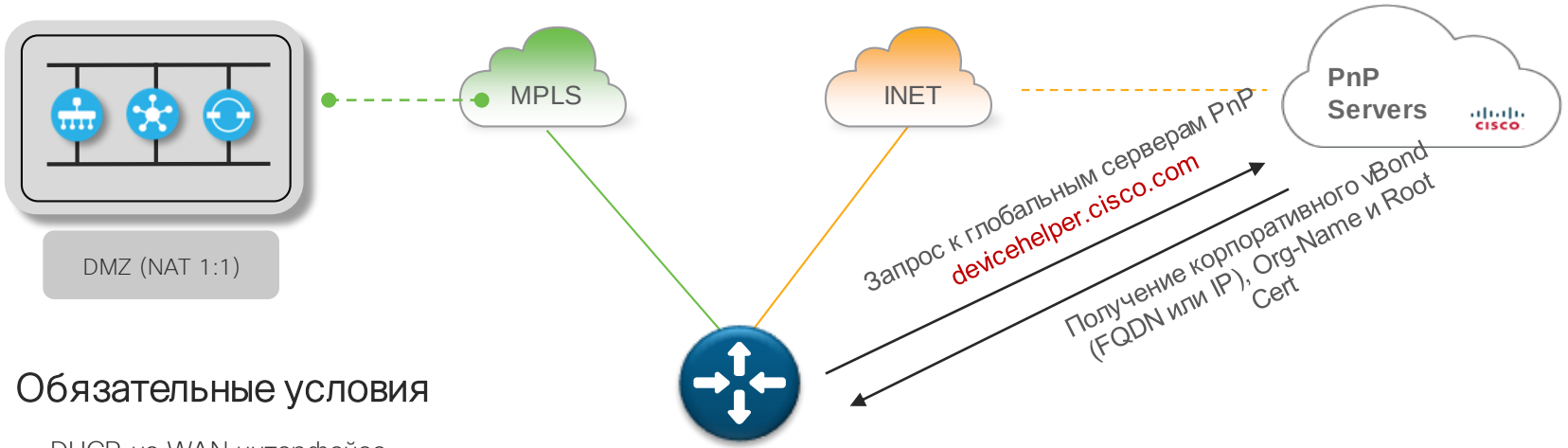
amazon web services

KVM

Microsoft Azure

vmware ESXi

Вариант 1. ZTP используя глобальный PnP

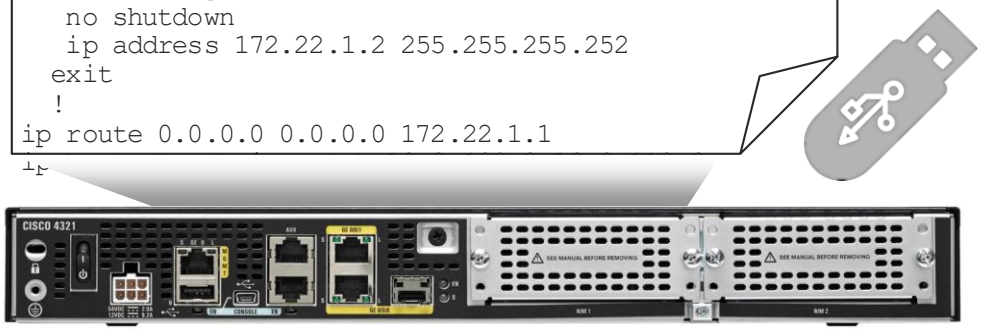


Обязательные условия

- DHCP на WAN интерфейсе
- DNS сервер и доступность devicehelper.cisco.com

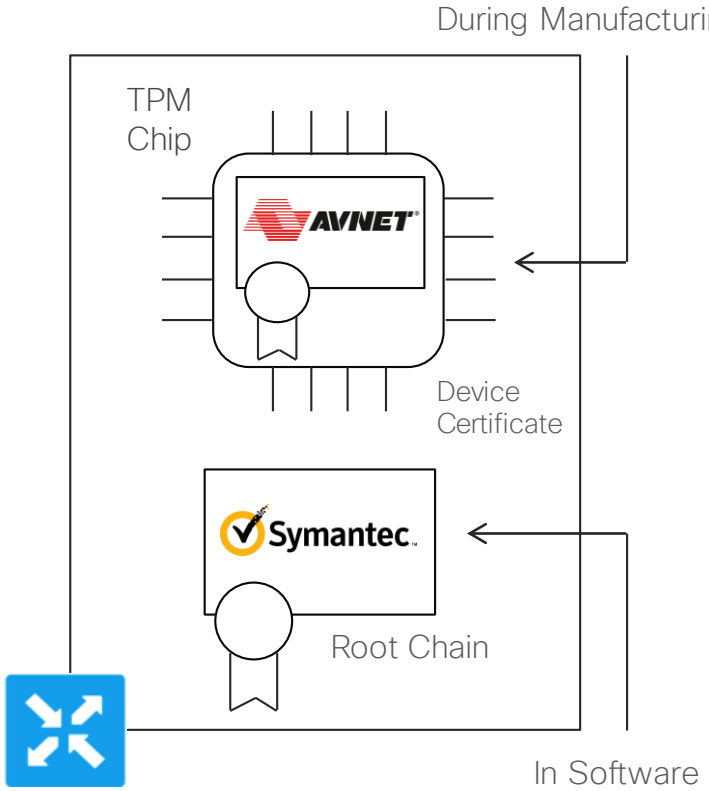
Вариант 2. ZTP со статичным IP или без Интернет

```
#cloud-boothook
  system
   personality            vedge
   device-model           vedge-ISR-4321
   host-name              wan-edge-br1-1-isr4321
   system-ip              10.255.255.31
   site-id                1
   organization-name      "Cisco SD-WAN PoV Kiev"
   console-baud-rate      9600
   vbond vbond.cisco.lab port 12346
   !
   !
  !
interface GigabitEthernet0/0/0
   no shutdown
   ip address 172.22.1.2 255.255.255.252
  exit
  !
ip route 0.0.0.0 0.0.0.0 172.22.1.1
```



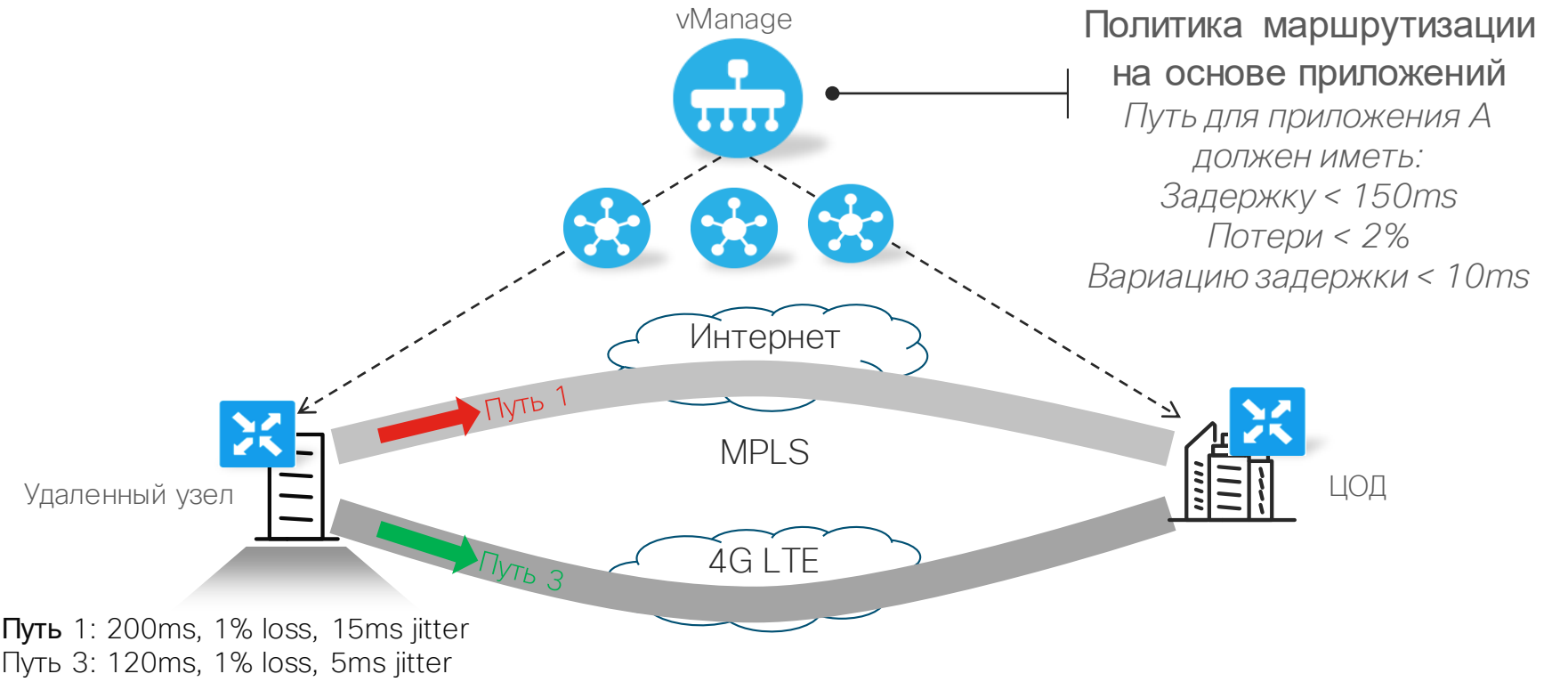
- При загрузке, маршрутизатор ищет на bootflash: или usbflash: файл с именем **ciscosdwan.cfg**
- Конфигурационный файл с базовыми настройками интерфейсов, Root CA, Organization Name, vBond адресами передается в PnP процесс
- Поддерживается только начиная с SD-WAN IOS-XE 16.10
  - 16.10.1
  - 16.10.2

SD-WAN Router Identity

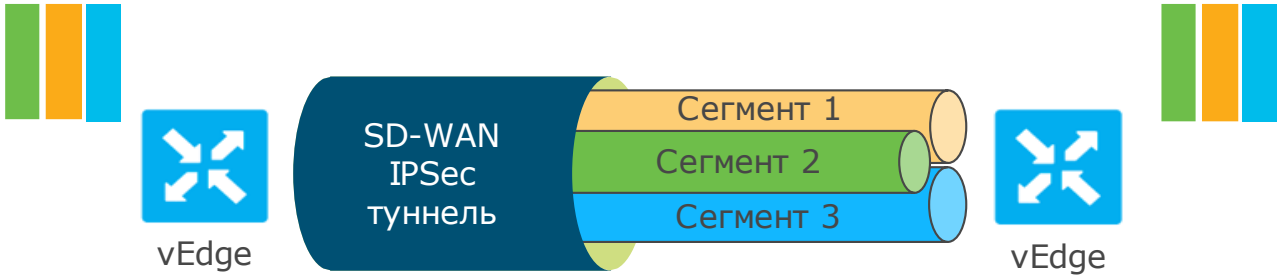


- Each physical vEdge router is uniquely identified by the chassis ID and certificate serial number
- Certificate is stored in on-board Temper Proof Module (TPM)
  - Installed during manufacturing process
- Certificate is signed by Avnet root CA
  - Trusted by Control Plane elements
- Symantec root CA chain of trust is used to validate Control Plane elements
- Alternatively, Enterprise root CA chain of trust can be used to validate Control Plane elements
  - Can be automatically installed during ZTP

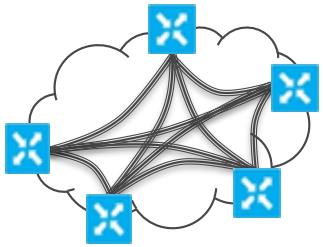
Обеспечение SLA для критичных приложений



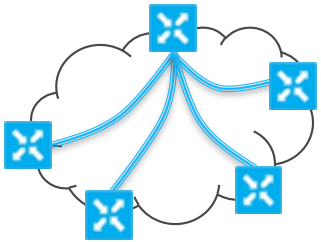
Безопасная сегментация



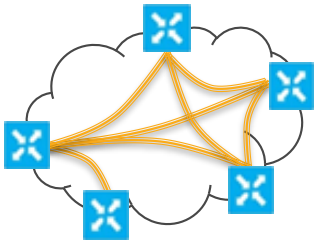
Уникальная топология для каждого VPN



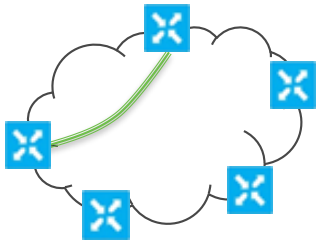
Full Mesh топология



Централизованная
Hub-and-Spoke

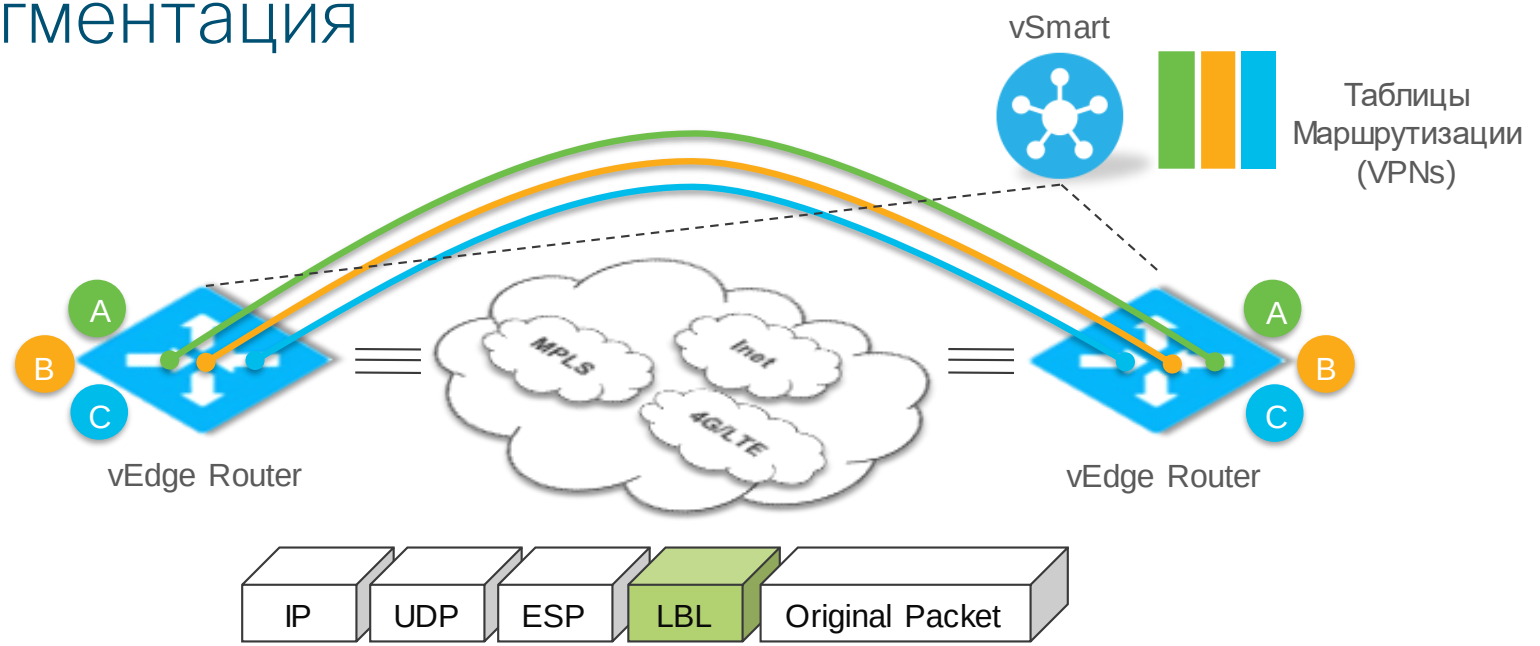


Частично связанная
Partial Mesh



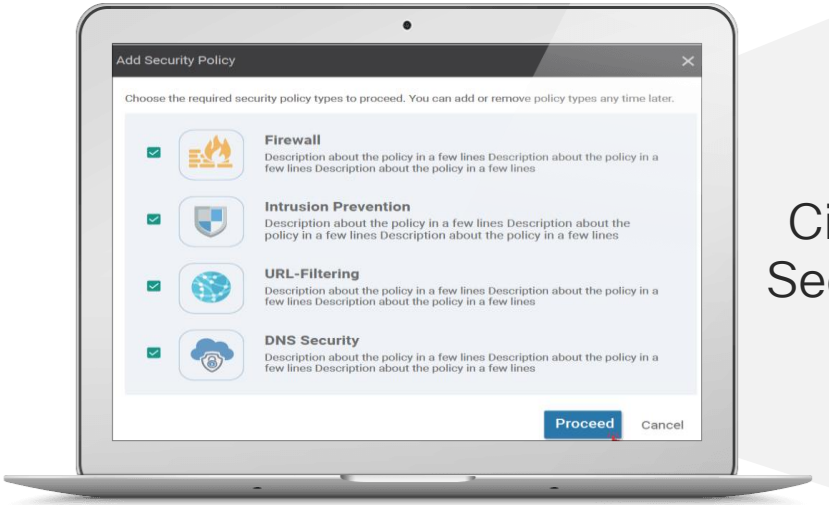
Точка-точка
Point-to-Point

Сегментация



- Сегментированная связность через фабрику без зависимости от типа транспорта
- Интерфейсы и sub-интерфейсы (802.1Q теги) are mapped into VPNs
- vEdge/cEdge роутер поддерживает таблицу маршрутизации для каждого VPN для полной изоляции плоскости управления
- Метки (Labels) используются на уровне data plane для разделения трафика

Комбинируем лучшие технологии безопасности и SD-WAN



Cisco SD-WAN

Cisco Security

Enterprise Firewall
+1400 layer 7 apps classified

Intrusion Protection System
Most widely deployed IPS engine in the world

URL-Filtering
Web reputation score using 82+ web categories

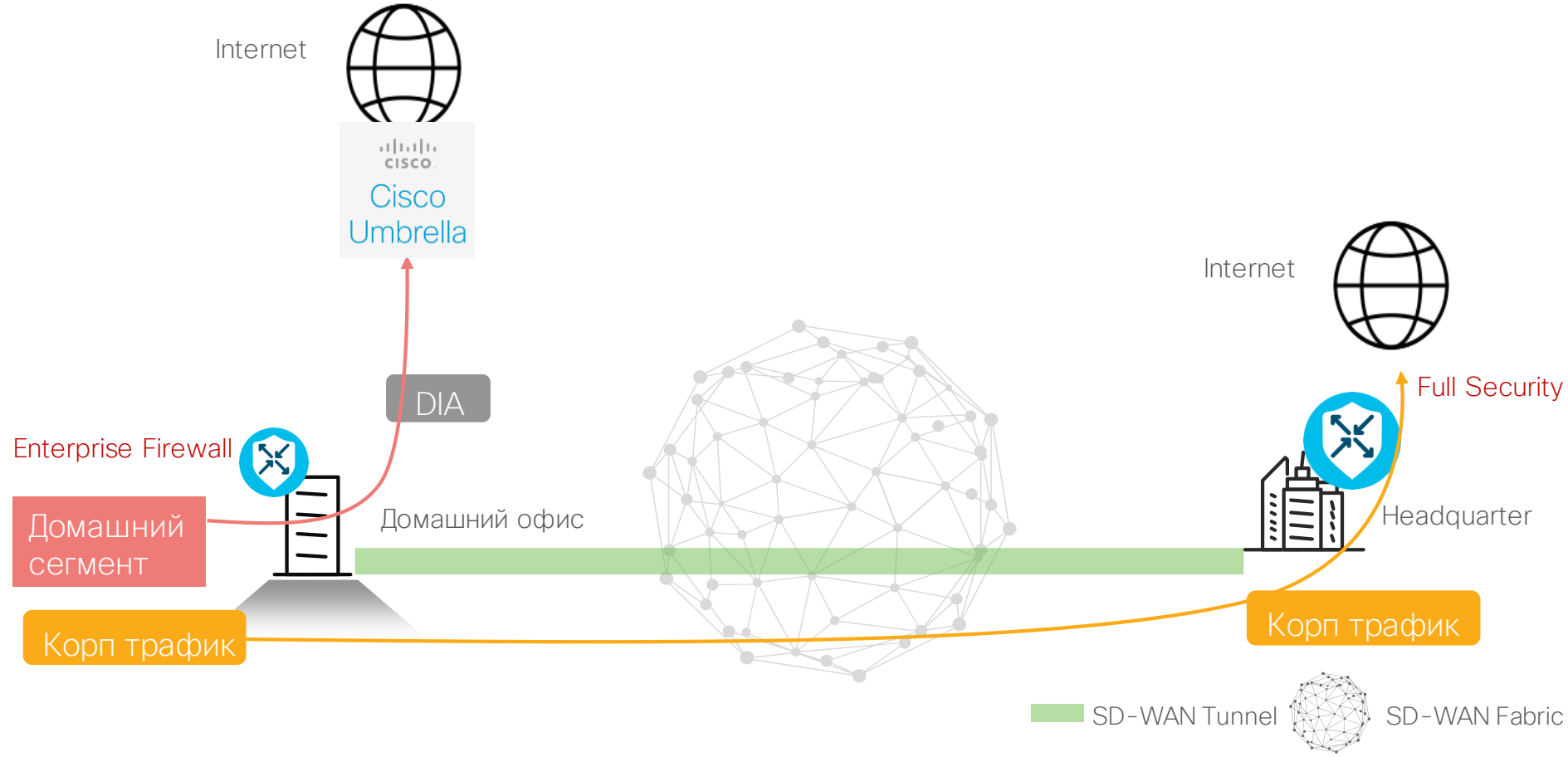
Adv. Malware Protection*
With File Reputation and Sandboxing

Simplified Cloud Security
Easy Deployment for Cisco Umbrella

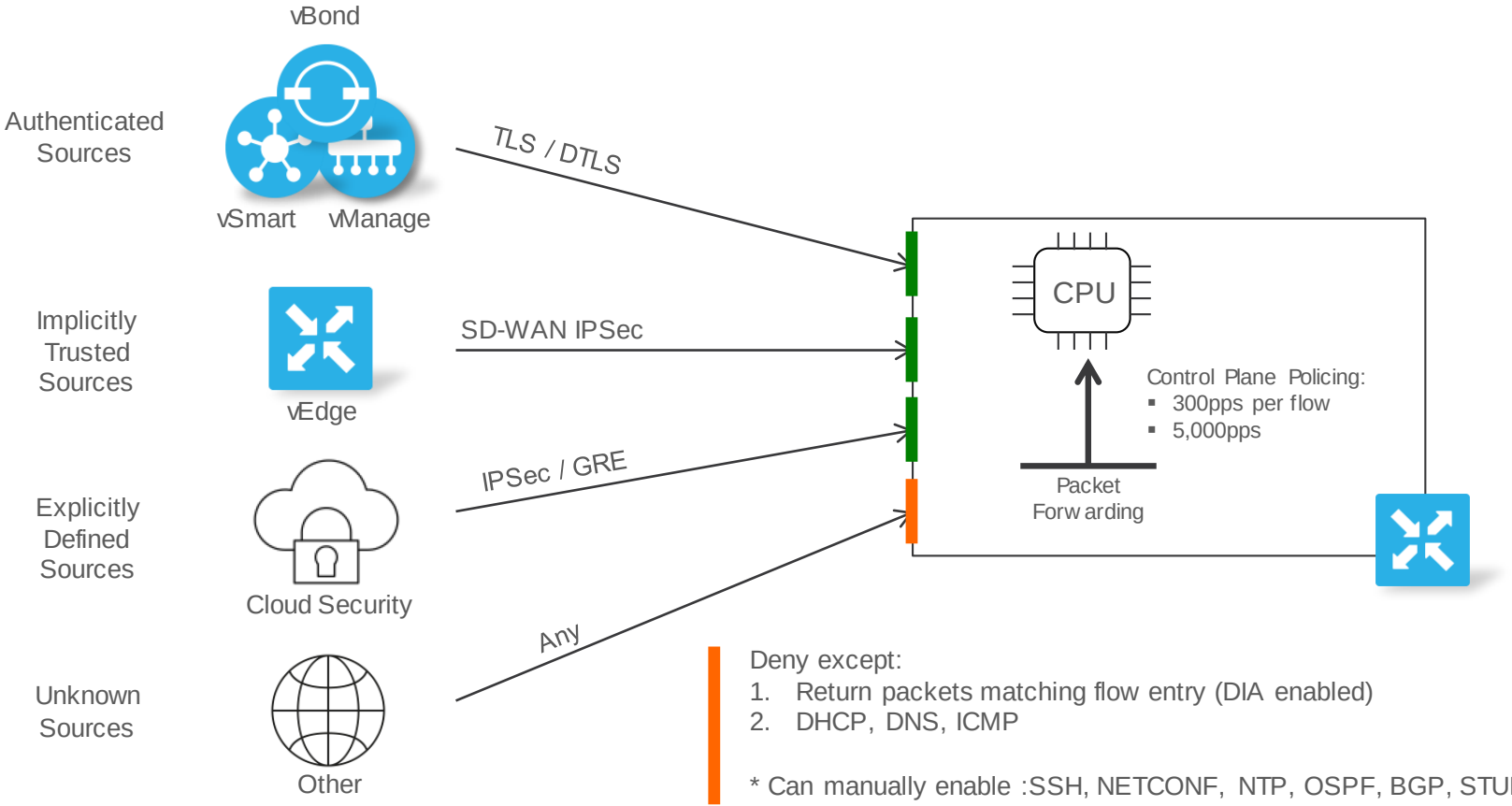
Hours instead of weeks and months

*Roadmap Mar '19

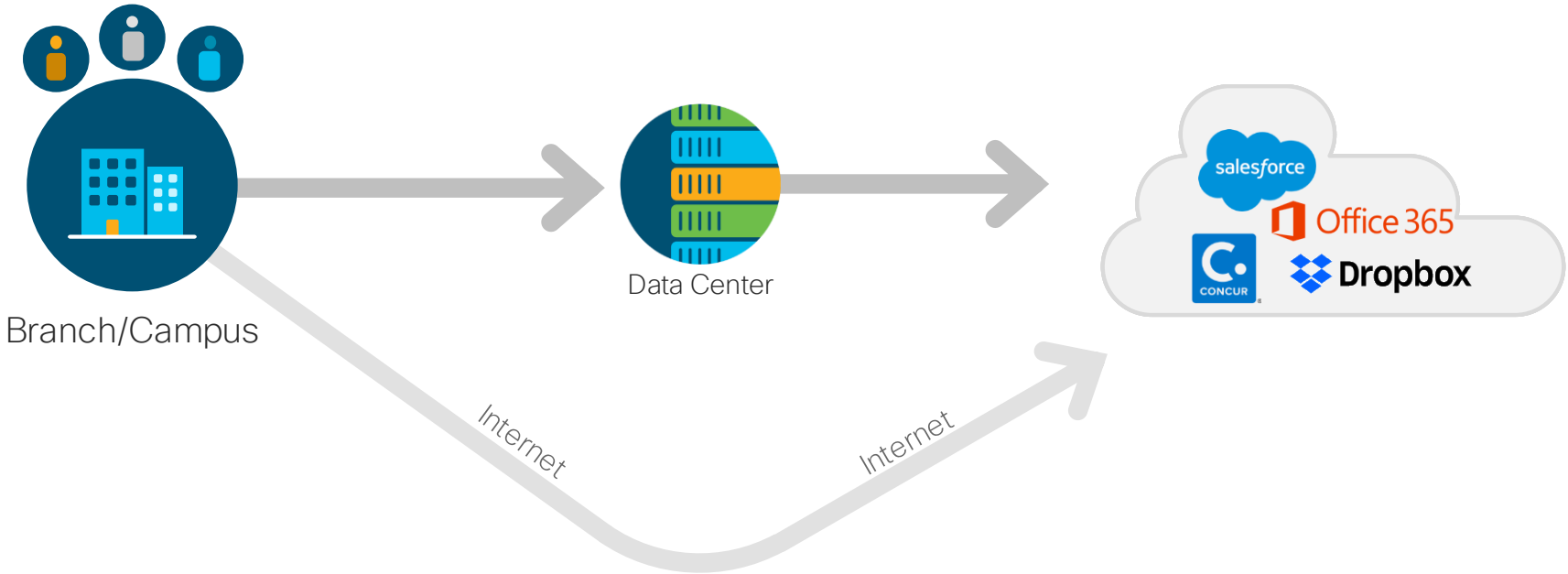
Сегментация домашнего и корпоративного доступа. Защита от атак из интернет



DDoS Protection for SD-WAN Routers



Cloud-on-Ramp for SaaS



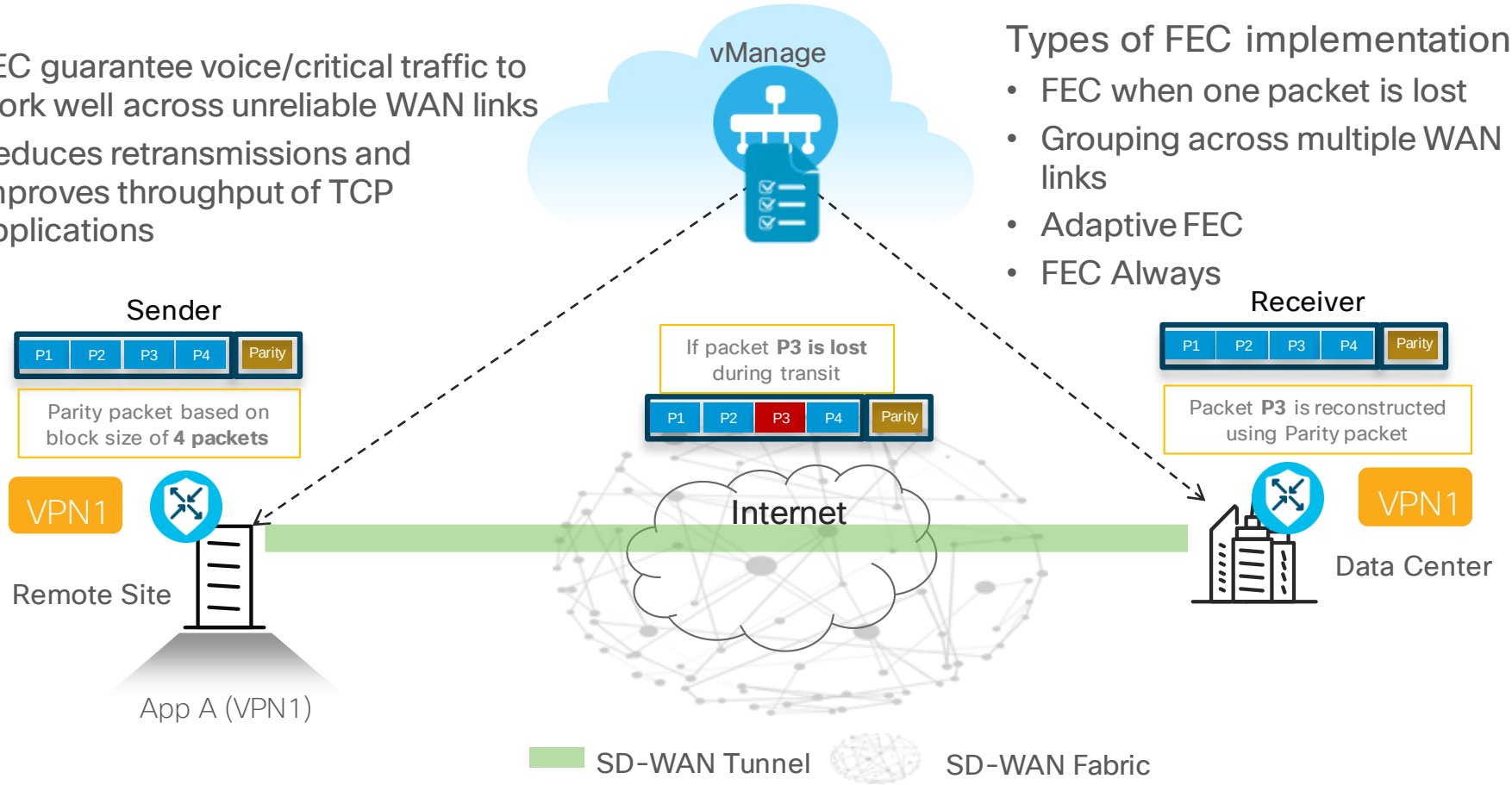
Локальный выход в Интернет (DIA) для SaaS
Поиск оптимального пути к серверу SaaS приложения
Контроль канала до облака
Контроль отклика приложения

Защита от потерь пакетов – Forward Error Correction

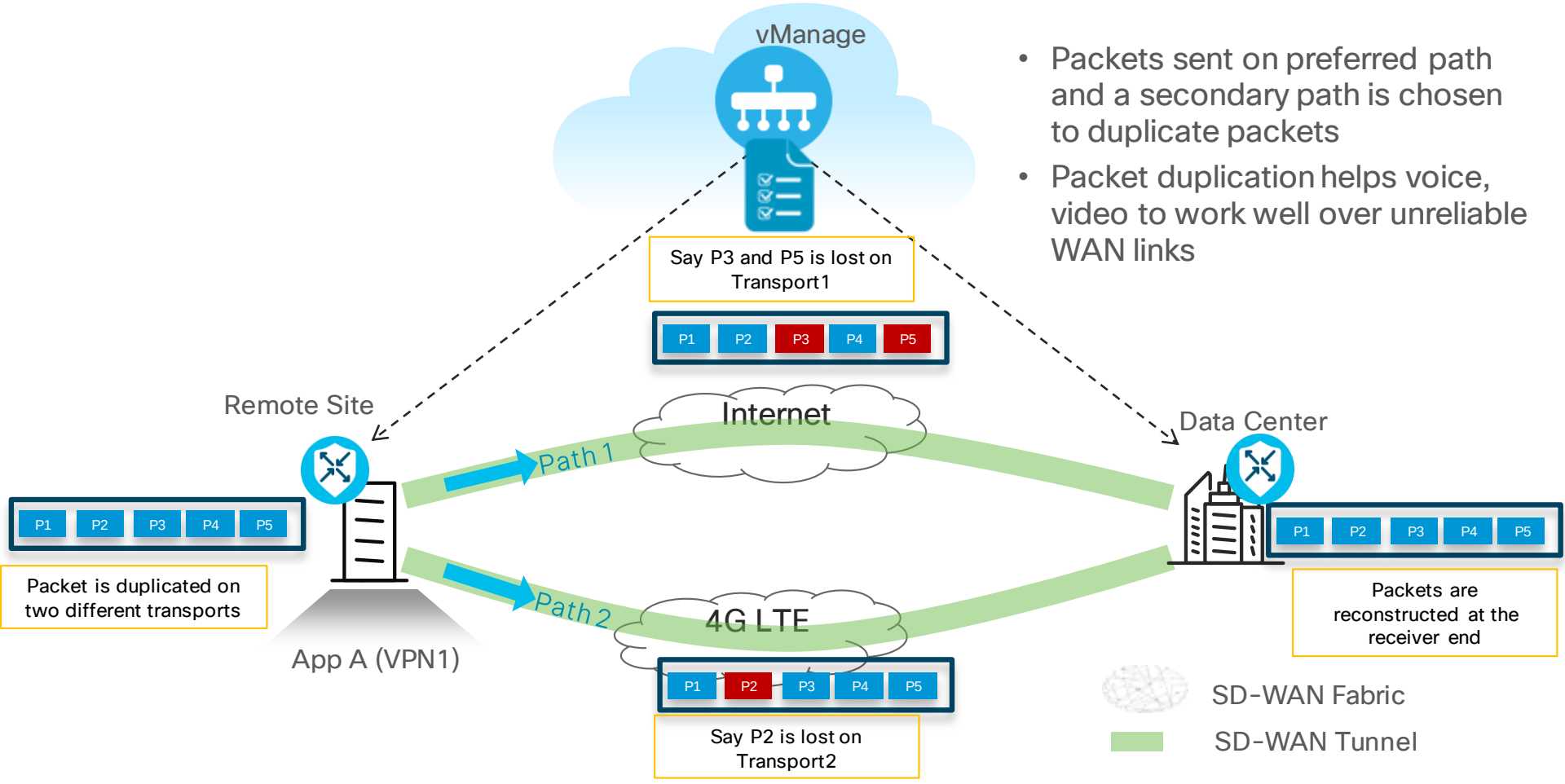
- FEC guarantee voice/critical traffic to work well across unreliable WAN links
- Reduces retransmissions and improves throughput of TCP applications

Types of FEC implementation

- FEC when one packet is lost
- Grouping across multiple WAN links
- Adaptive FEC
- FEC Always



Работа на плохих каналах: пакетная дупликация



- Packets sent on preferred path and a secondary path is chosen to duplicate packets
- Packet duplication helps voice, video to work well over unreliable WAN links

Решение Office Extend Access Point (OEAP)

Remote Worker Use Case

- Любая Cisco Aironet Точка доступа может работать как ‘Office Extend AP’ (OEAP) – это означает, что если есть парк оборудования точек доступа, они могут использоваться для организации удаленных домашних офисов.

- Любой контроллер (виртуальный или физический) может использоваться для подключений OEAP точек или выделенный контроллер устанавливается в DMZ.

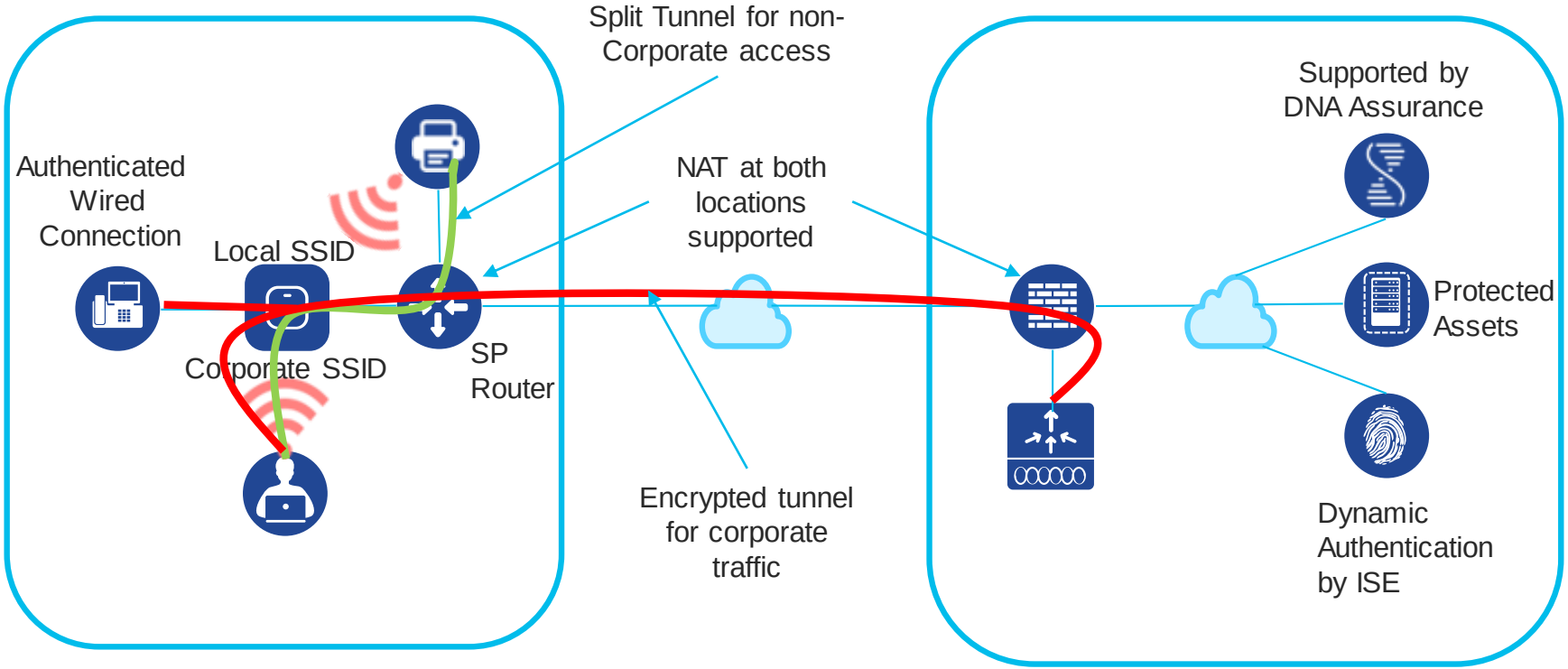
- С решением OEAP, сотрудник дома будет иметь доступк к корпоративному SSID и корпоративной сети, без необходимости устанавливать VPN и иметь технические знания.

OfficeExtend функции

Наверняка уже есть необходимые компоненты для внедрения

Simple Centralized Configuration	
QoS	Application Visibility allows detection tagging of configured business traffic QoS allows the prioritization of the tagged business traffic
Encryption	DTLS Encryption over the wire (commonly used in VPN traffic) 802.1x with AES encryption over the air protects data
Split Tunnel	Allows the use of local printers etc. if configured Allows non-essential traffic to be dropped locally reducing the demand to office
SSIDs	One local Multiple Corporate SSIDs
NAT support	Works with AP and or WLC behind NAT
AP Support	Most all APs can do OEAP APs with Aux ports or teleworker APs with multiple ports allow for authenticated wired traffic Can use PoE or local AC power adaptor depending on AP types.
DNA Center Assurance	AI support of trends and issues ML for diagnostics

OfficeExtend: работа точек доступа

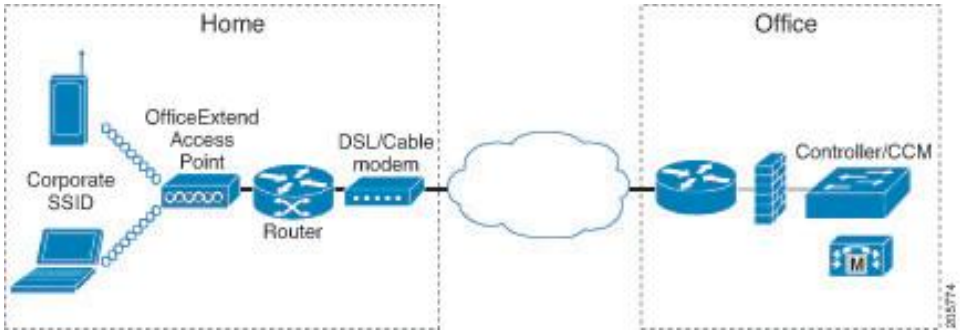


Расширяем беспроводное покрытие до дома

- Equipment needed?
  - WLC in DMZ –
    - Can be any AirOS Controller WLC 3504/5520/8540 or even older 2504/5508/8510 running AirOS 8.5 or later
    - 9800 appliance or 9800-CL in private cloud (OEAP mode supported) – IOS XE
  - AP at teleworker site
    - Purpose built 1815T teleworker AP AireOS 8.5 and Later, also IOS-XE
    - Any Aironet 11n – AP16xx/26xx/36xx; AireOS 7.4 to AireOS 8.5 not on IOS-XE
    - 11ac Wave 1 – AP17xx/27xx/37xx AireOS 8.3 and later, also IOS-XE
    - 11ac Wave 2 AP's- AP18xx/28xx/38xx) AireOS 8.3 and later also IOS-XE
    - 11ax AP's – C9115, C9117, C9120, C9130 AireOS 8.10 also IOS-XE 16.12.2s

    Compatibility Matrix: https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html
  - WLC AP License/DNA License
- Steps Needed
  - Configure WLC
  - Onboard AP
  - Provide AP to teleworker to connect at their site

  Reference: OEAP Deployment



Next-Generation Wave 2 802.11ac OfficeExtend Access Point

Cisco Aironet® 1815t

Teleworker or Micro-branch deployments, providing **wired and wireless corporate access** to remote workers

Simultaneous **Dual Radio, Dual Band 2x2:2 with 802.11ac Wave 2**, including MU-MIMO

Elegant design with integrated antennas for optimal wireless coverage and convenient cable management.

3 x GigE Ethernet Ports, 1 x uplink GigE port
Up to 2 ports can be tunneled back to Wireless LAN Controller

AC Adapter included

Full PoE out (803.af) on LAN 1 port

Basic OEAP Configuration Tips

- WLC requires a public routable IP address so remote APs can reach WLC from their home network (can be in DMZ)
- That public IP can be added as a NAT IP on WLC management interface
- Some ports like CAPWAP, radius etc. needs to be open on Firewall as the OEAP controllers located in the DMZ need to communicate using a number of services such as RADIUS, TACACS+,NTP,FTP and CAPWAP
- For non OEAP models AP (for e.g. 1600/2600/3600/2700/3700/3800 etc admin needs to change the AP mode to FlexConnect and then enable OEAP option.
- Prime the OEAPs to join the WLC i.e. configure OEAP with WLC management public IP address

Reference OEAP Cisco Validated Design

https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-CiscoOfficeExtendDesignGuide-AUG14.pdf

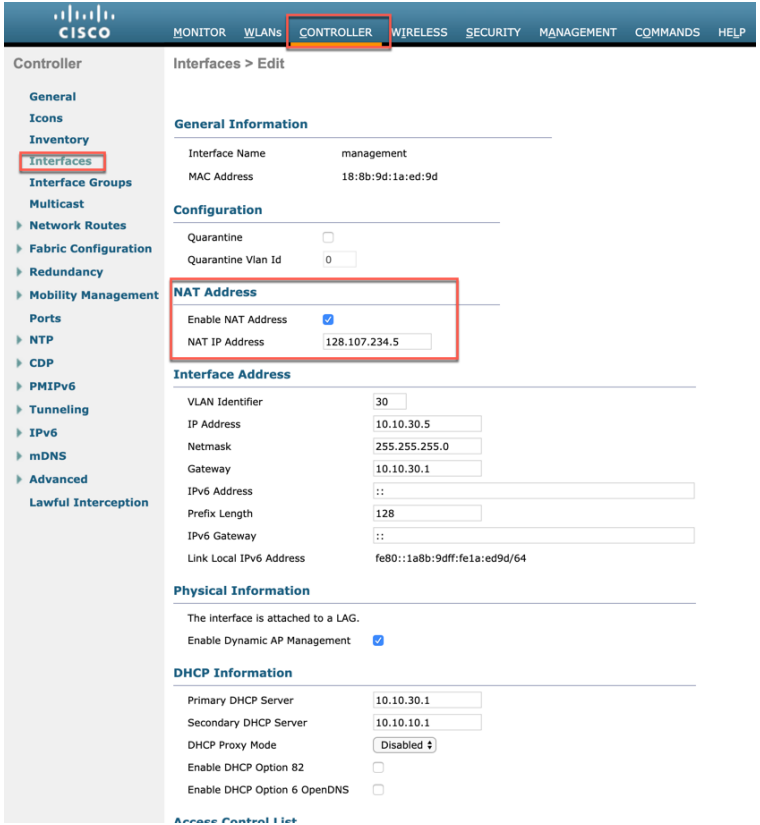
Secure remote work / micro office

Configure AireOS WLC

Step 1: Set up a controller to be used in DMZ
Step 2: Configure Management
In Controller > Interfaces, click the management interface

Step3: Select Enable NAT Address.
Step4: In the NAT IP Address box, enter the publicly reachable IP address, and then click Apply. (Example: 128.107.234.5)

Watch a AireOS WLC Guided Configuration Walk-through



1 Secure remote work / micro office

1: Have all AP's join a WLC to start so that it's connected and has Stepthe latest code

Step 2: From WIRELESS >All APs Select the AP which needs to be converted to OEAP

Step 3: From General tab change the AP mode to FlexConnect

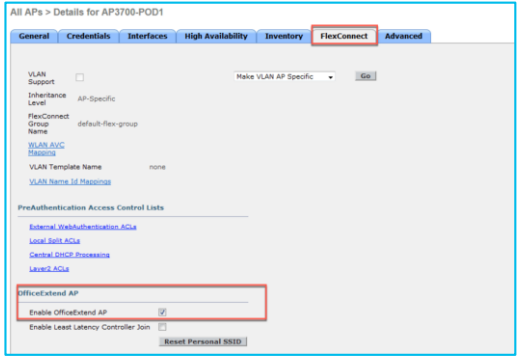
Step 4: Then go to **FlexConnect>OfficeExtend AP** enable OfficeExtend AP by checking the box

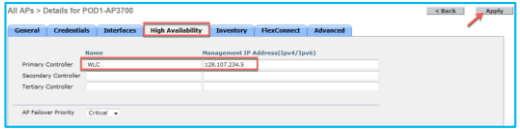
Step 5: Also, configure the high Availability by providing the WLC name and IP address in Primary Controller option and click **Apply.**

Now admin can take out the AP and give it to the remote worker where he connects it to the home router

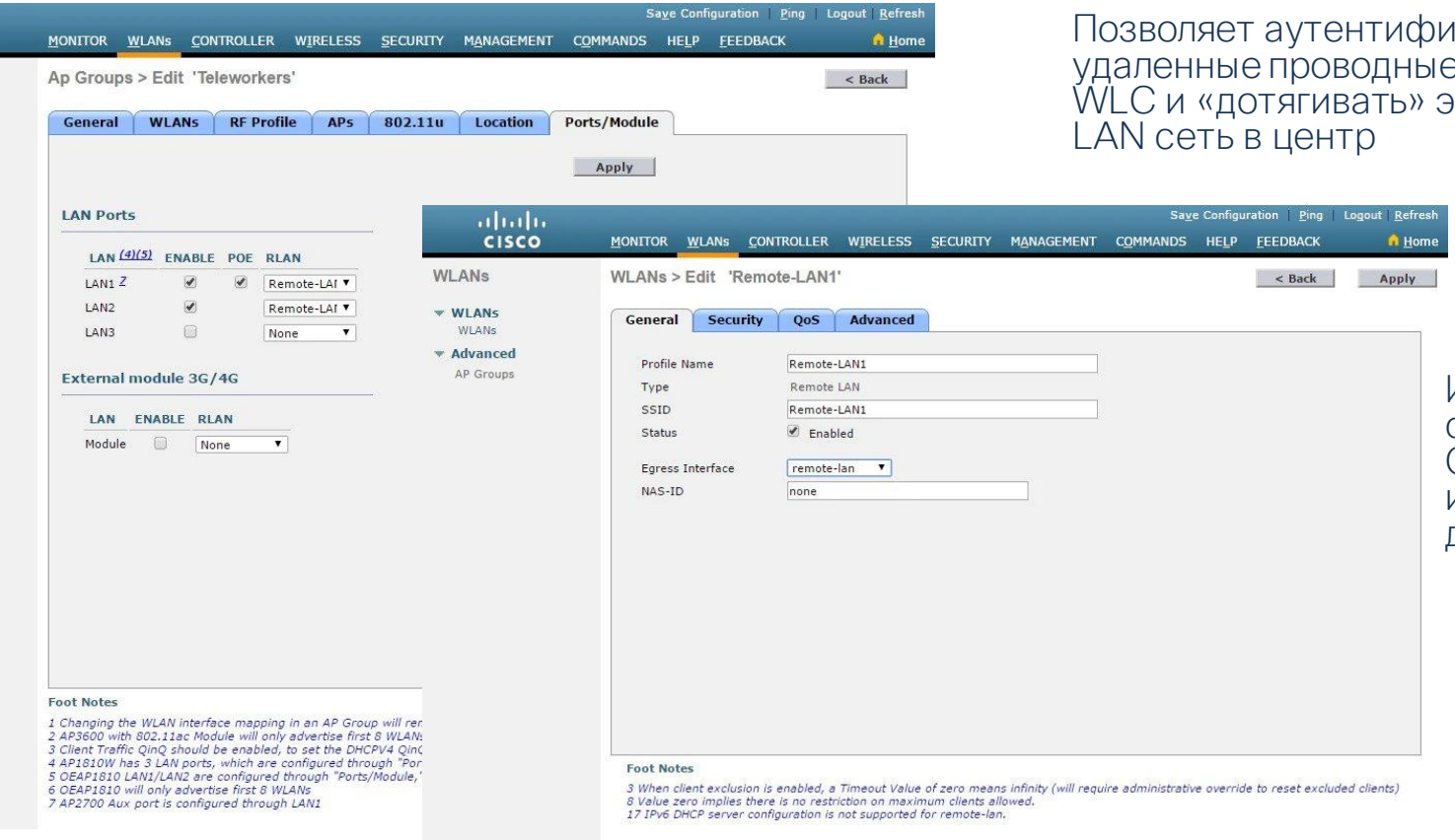
Note: verify which AP's are being sent to the employees. Most AP's use an AC adapter, some AP's might require a power injector or POE to power up the APs

Watch a Prime AP Guided Configuration Walk-through





Remote LAN



Позволяет аутентифицировать удаленные проводные устройства на WLC и «дотягивать» эту удаленную LAN сеть в центр

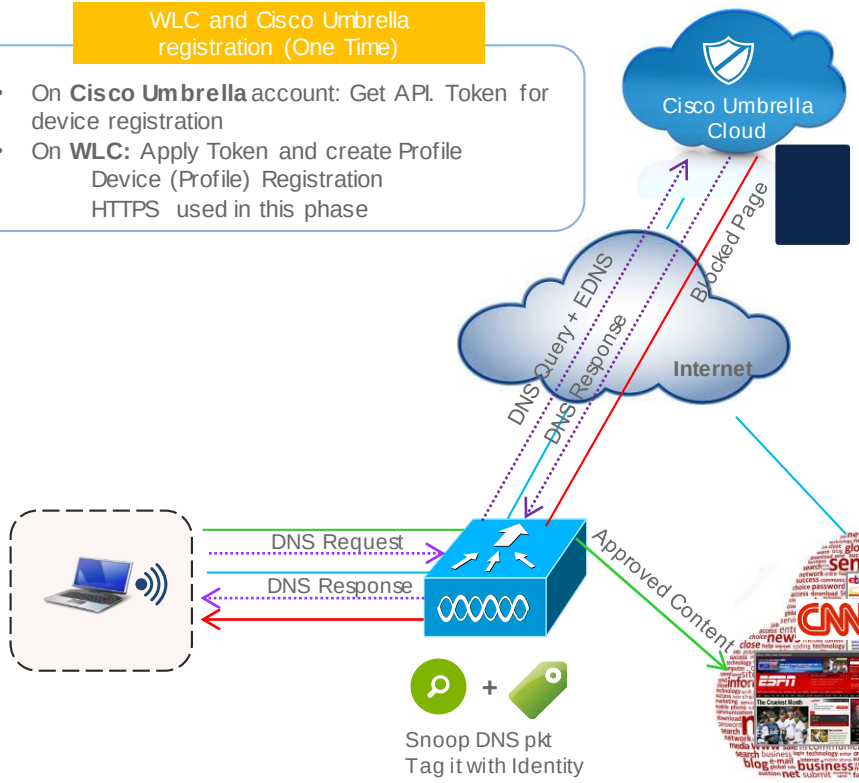
Используются порты на специализированных OEAP точках или AUX порты на других точках

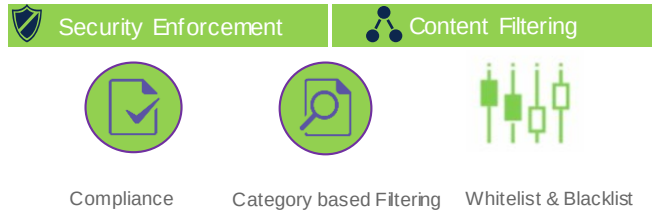
Интеграция OEAP и Umbrella

Cisco Umbrella- WLC Packet Flow

WLC and Cisco Umbrella registration (One Time)

- On **Cisco Umbrella** account: Get API. Token for device registration
- On **WLC:** Apply Token and create Profile
  Device (Profile) Registration
  HTTPS used in this phase





Wireless client traffic flow

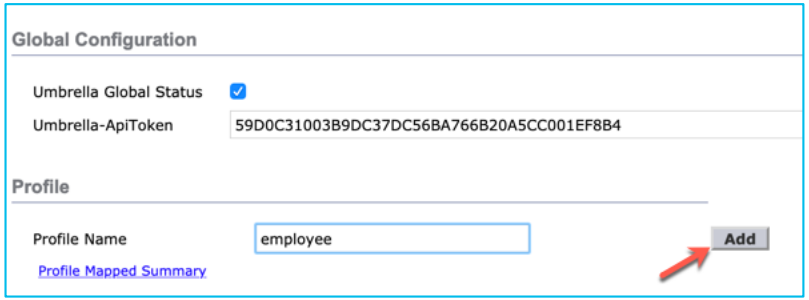
- Client sends DNS query
- WLC snoops DNS query, forwards it with EDNS
- Cisco Umbrella applies Profile specific Policy
- Sends DNS response to WLC
- WLC forwards the response to client

OpenDNS- Profile Creation on WLC

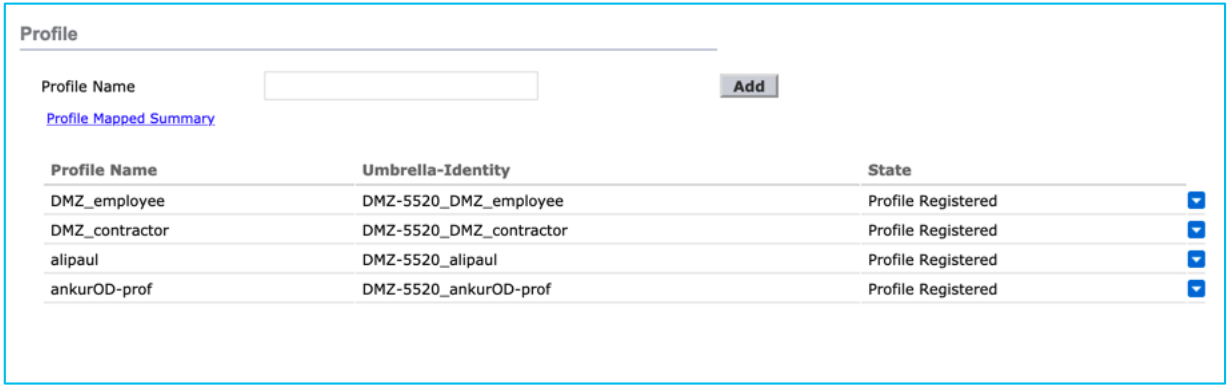
Step1: From WLC main menu go to **Security>Umbrella>General**

- Enable Umbrella Global Status by checking the box
- Add the API Token ********8E17EB6ABBCA001EF8B4**
  (This API token we acquired from the Umbrella account)
- Click **Apply**

Step 2: Then configure a profile and hit **Add**

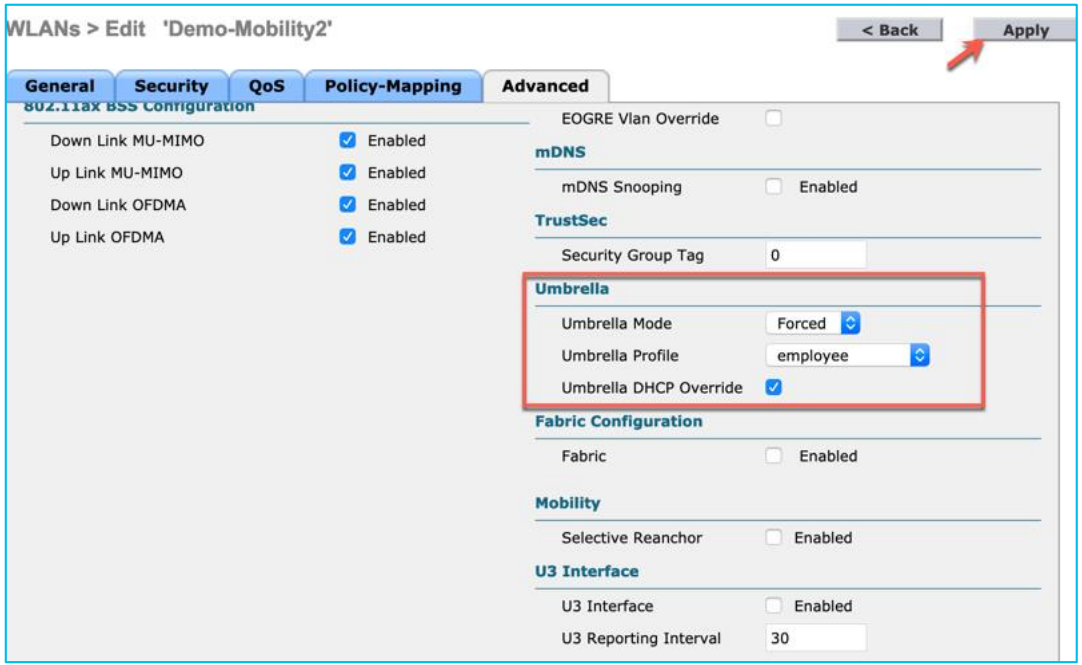


Step 3: Confirm that the profiles get registered



Configuring Umbrella on WLAN

Step1: From WLC main menu navigate to **WLAN > Advanced > Umbrella section select Umbrella mode "Forced" Click Apply.**



Варианты для быстрого внедрения OEAP на период карантина

1 Secure remote work / micro office

Offers

AireOS and IOS-XE WLCs

Leverage WLC evaluation license
Supports maximum WLC platform AP Limit
Duration: 90 Days (AireOS), 60 Days (IOS-XE)

No AP Count license required for Mobility Express or Autonomous Mode APs

Setup evaluation license in AireOS or IOS-XE

Free 9800-CL WLC

With a 90-day evaluation license
Supports maximum WLC platform AP Limit
No AP Count license required for Mobility Express or Autonomous Mode Aps

Download WLC controller for cloud .ova file here

Setup evaluation license in IOS-XE

Secure remote work / micro office

- Wireless OEAP TDM presentation: Link
- OEAP Configuration Guide (AireOS 8.5): Link
- OEAP Configuration Guide (AireOS 8.8): Link
- OEAP WLC guided configuration video
- OEAP Cisco Validated Design: Link
- 1815t Deployment Guide: Link

- Wireless OEAP Cheatsheet: Link
- Cisco Wireless Solutions Software Compatibility Matrix: Link

- AP at teleworker site

AP Models	OEAP	RLAN/Aux port	9800	AireOs
91xx	Supported	N/A (AP does not have Aux Ports)	17.2	8.5.161.0/8.10.112.0
Wave 2 Aps (including 4800)	Supported	28xx/38xx/1850/1815t/1815w supports RLAN	17.2	8.5.161.0/8.10.112.0
Wave 1	Supported	N/A (AP does not have Aux Ports)	17.2	8.5.161.0/8.10.112.0

Useful Links

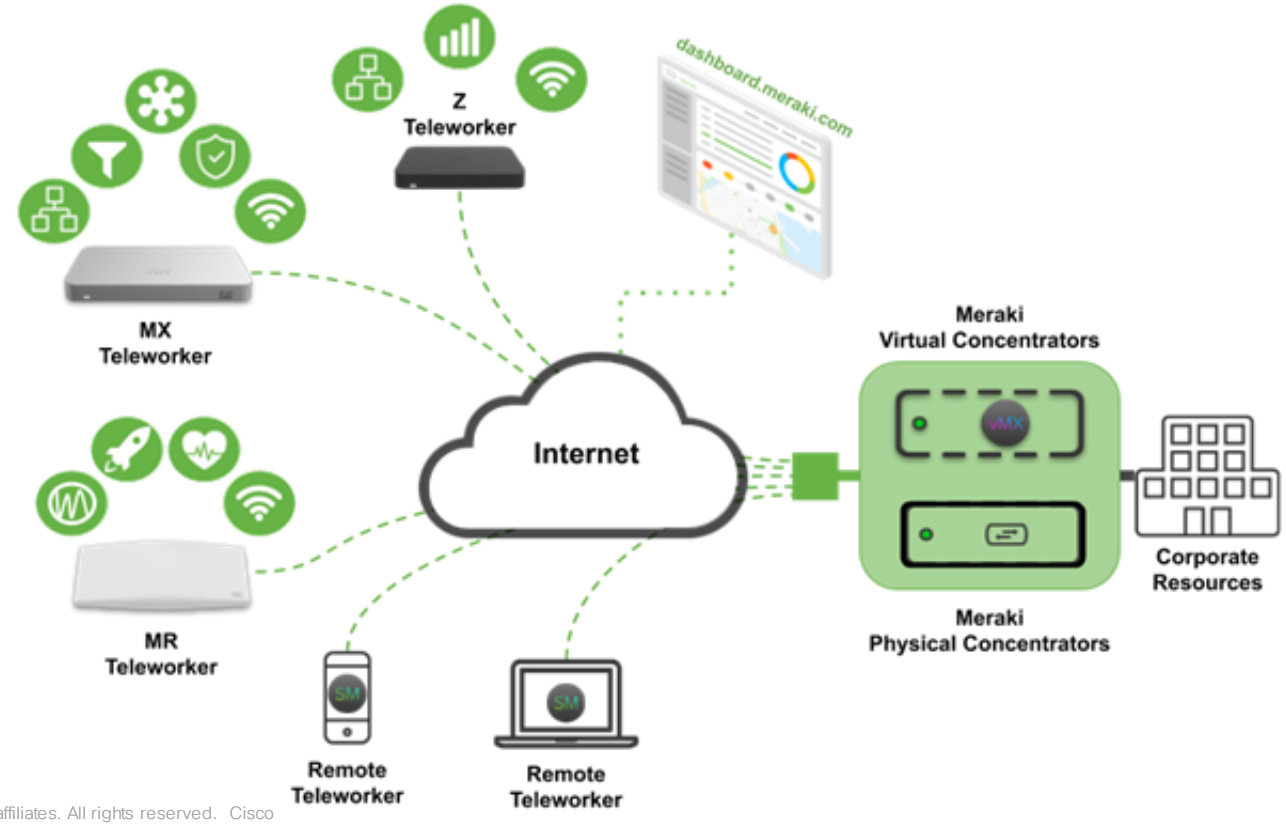
- OEAP Configuration Guide (AireOS 8.5): https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-5/config-guide/b_cg85/configuring_officeextend_access_points.html?bookSearch=true
- OEAP Configuration Guide (AireOS 8.8): https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-8/config-guide/b_cg88/configuring_officeextend_access_points.html?bookSearch=true
- OEAP Configuration Guide (AireOS 8.10): https://www.cisco.com/c/en/us/td/docs/wireless/controller/8-10/config-guide/b_cg810/configuring_officeextend_access_points.html?bookSearch=true
- OEAP CVD: https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Aug2014/CVD-CiscoOfficeExtendDesignGuide-AUG14.pdf
- 1815t Deployment Guide: https://www.cisco.com/c/dam/m/zh_cn/solutions/enterprise-networks/mobility-express/office-extend/office-extend-deployment-guide.pdf
- Catalyst 9800 Configuration guides: https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-installation-and-configuration-guides-list.html
- Compatibility Matrix: https://www.cisco.com/c/en/us/td/docs/wireless/compatibility/matrix/compatibility-matrix.html

AP at teleworker site

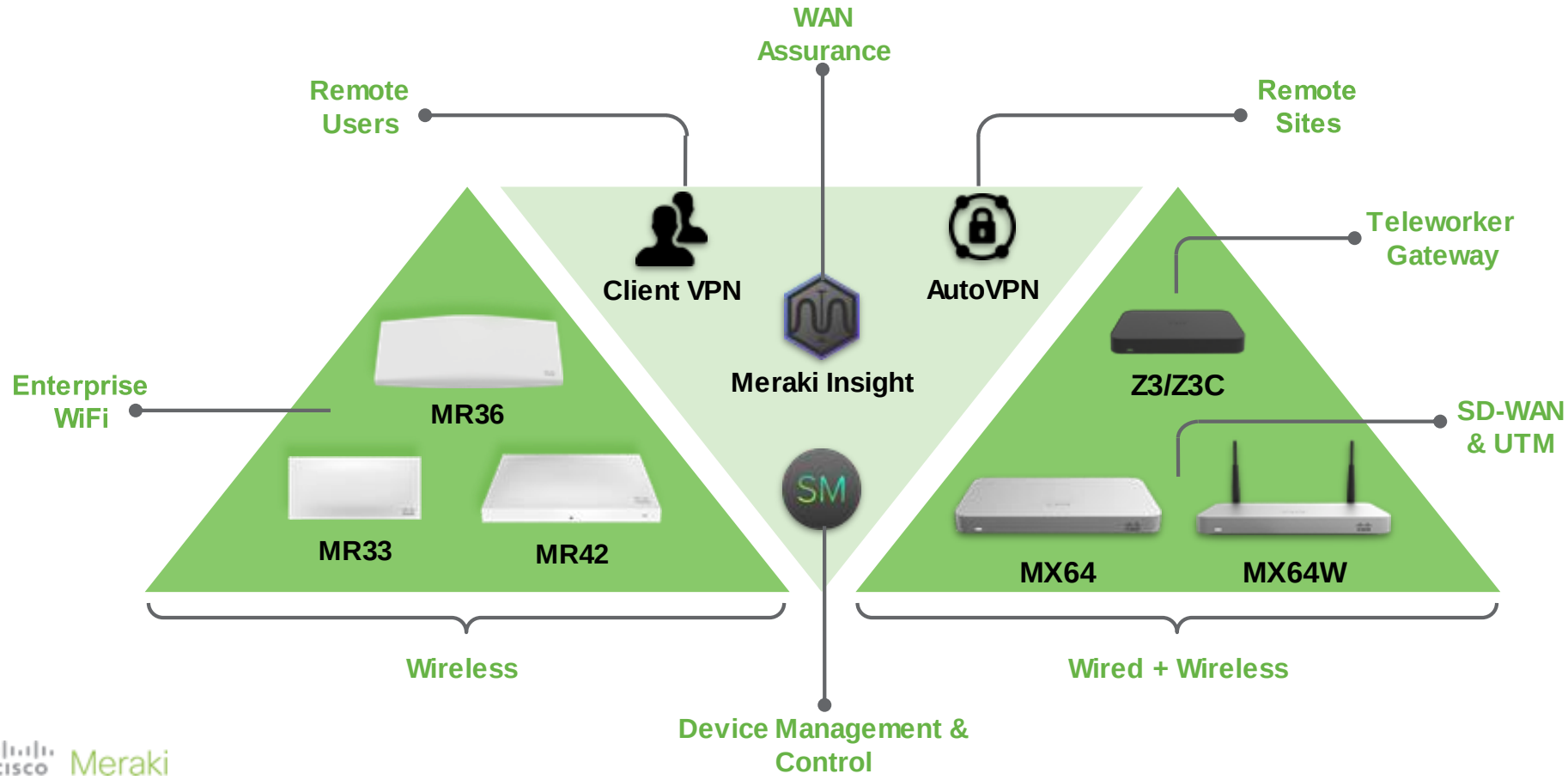
- Purpose built 1815T teleworker AP AireOS 8.5 and Later, also Cisco IOS -XE
- Any Aironet 11n - AP16xx/26xx/36xx; AireOS 7.4 to AireOS 8.5 not on Cisco IOS XE
- 11ac Wave 1 - AP17xx/27xx/37xx AireOS 8.3 and later, also Cisco IOS XE
- 11ac Wave 2 AP's- AP18xx/28xx/38xx) AireOS 8.3 and later also Cisco IOS XE
- 11ax AP's – C9115, C9117, C9120, C9130 AireOS 8.10 also Cisco IOS XE 16.12.2s

Удаленный домашний офис на базе решений Meraki

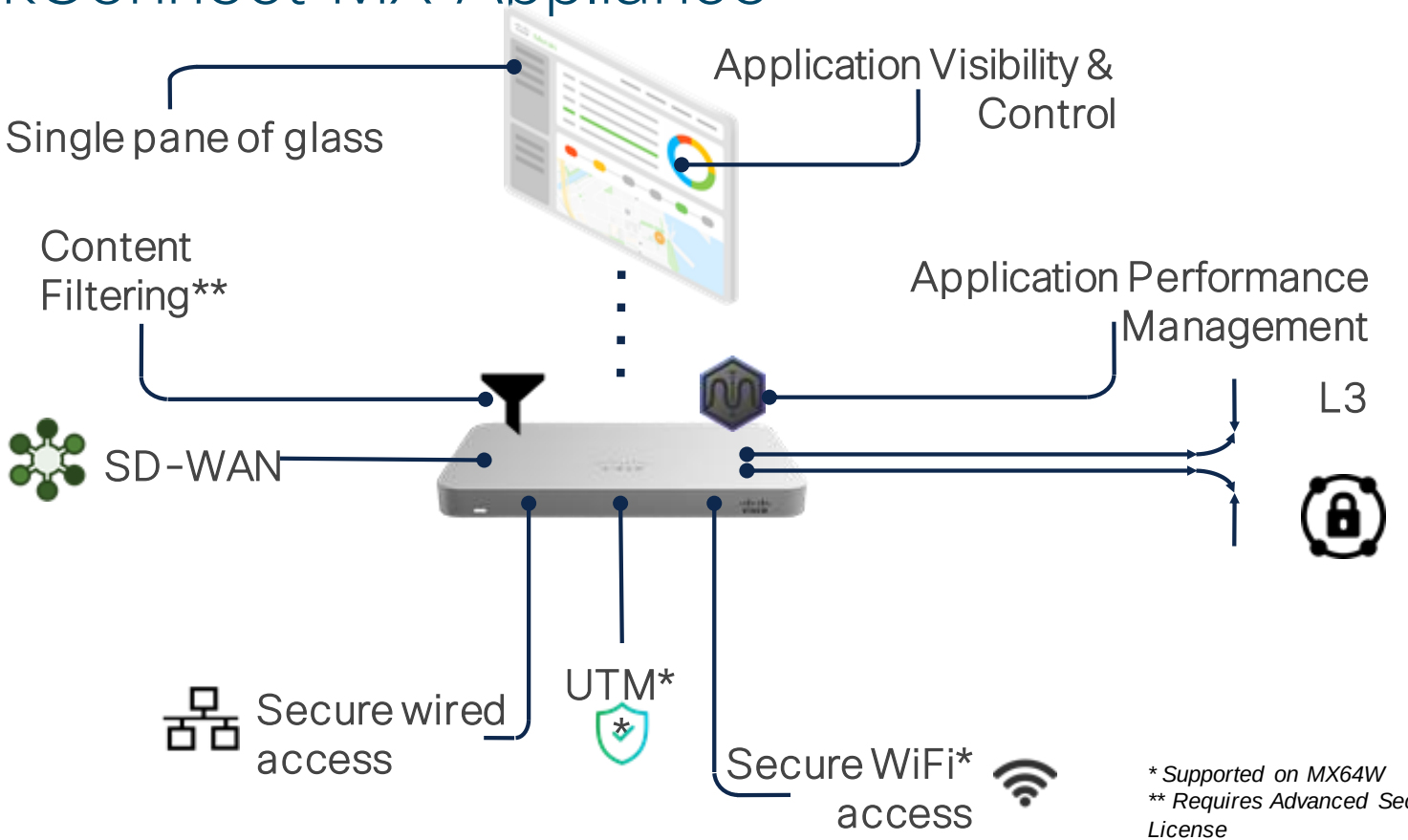
Meraki Remote Work Solutions



A solution for all use cases



WorkConnect MX Appliance

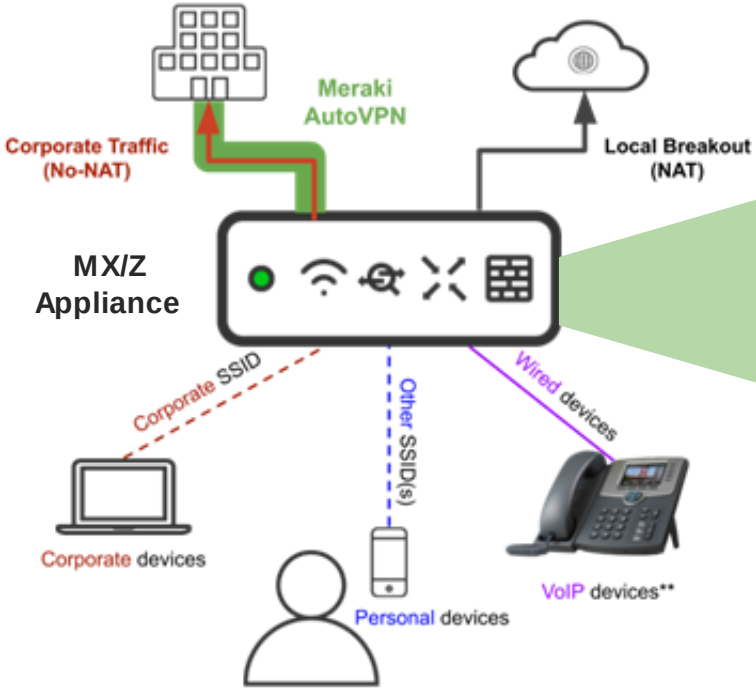


** Supported on MX64W*
*** Requires Advanced Security License*

MX/Z Teleworker

	Z3	Z3C	MX64	MX64W
WAN Ports	1		1 or 2	
LAN Ports	4		4 or 3	
PoE Ports	1		None	
Cellular Primary	Must add MG21/MG21E		Must add MG21/MG21E	
Cellular Backup	Via USB dongle	Integrated	Via USB dongle	
WiFi	Integrated		N/A	Integrated
Throughput	100mbps		250mbps	
SD-WAN	N/A		Supported	
UTM	N/A		Supported with Advanced Security license	
Content Filtering	N/A		Supported with Advanced Security license	

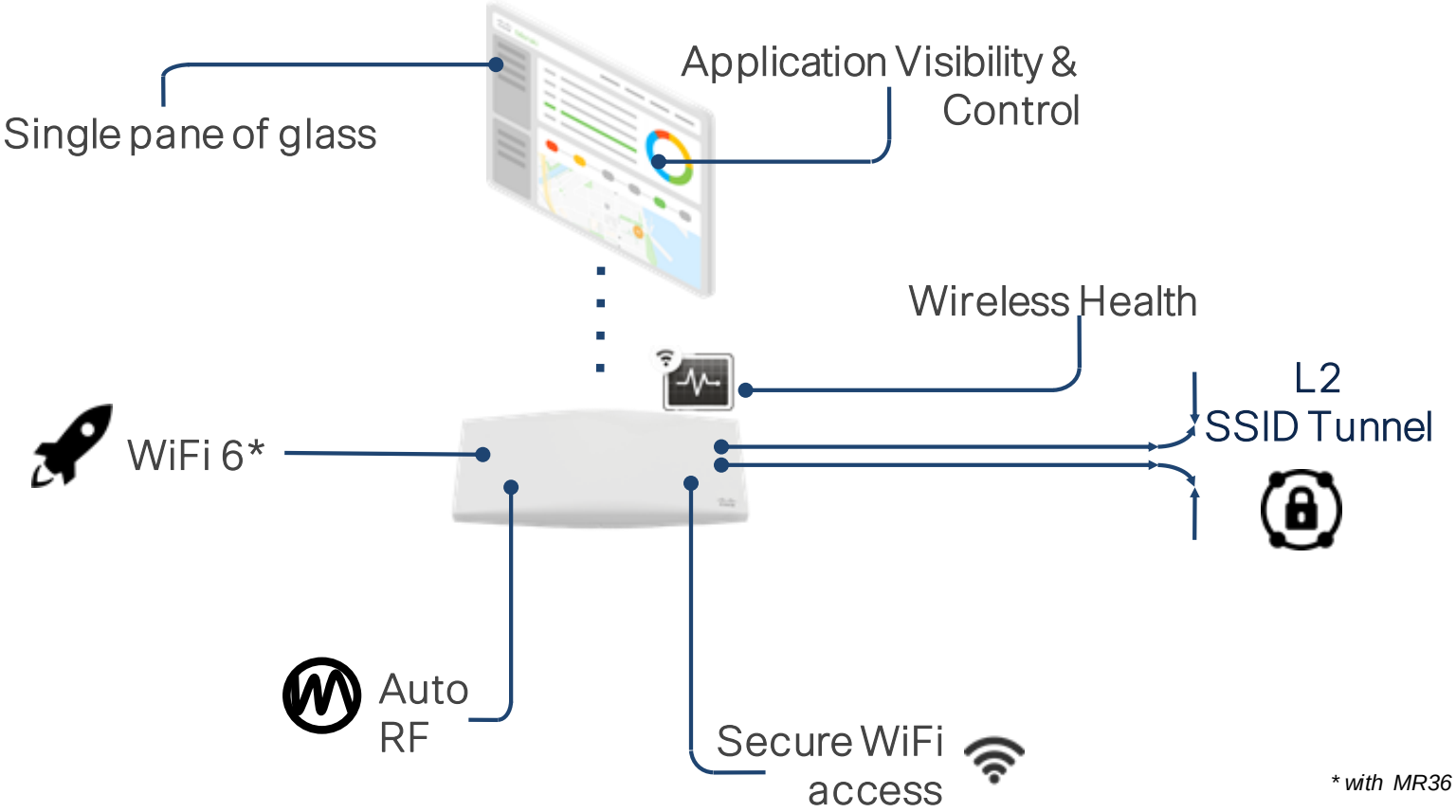
SoHo Teleworker Solution with MX/Z Appliance



- Dual Radio WiFi*
- PSK or Radius Authentication
- Multiple LAN Ports
- SD-WAN***
- Full/Split Tunneling
- UTM & Content Filtering****
- Zero touch provisioning

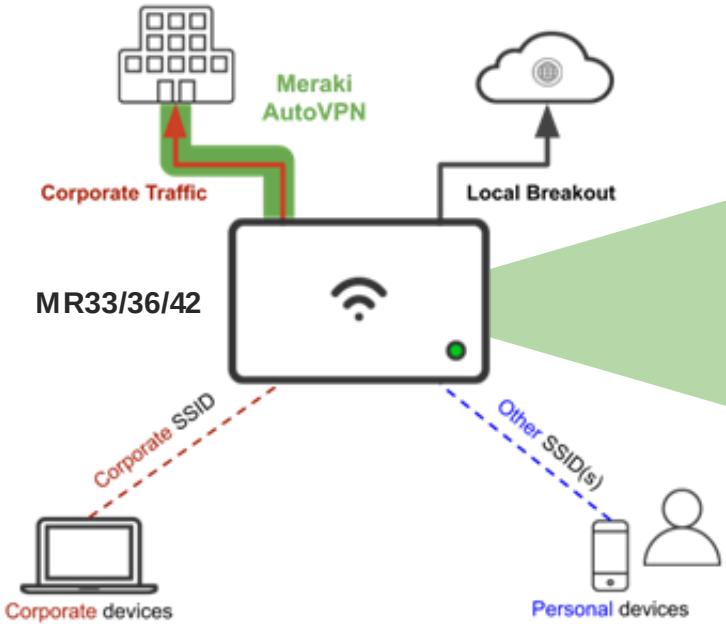
** on Z3/Z3C/MX64W*
*** On Z3/Z3C otherwise requires a PoE injector*
**** on MX64/64W*
***** Requires MX with Advanced Security license*

WorkConnect MR Access Point



** with MR36*

SoHo Teleworker Solution with MR Access Points



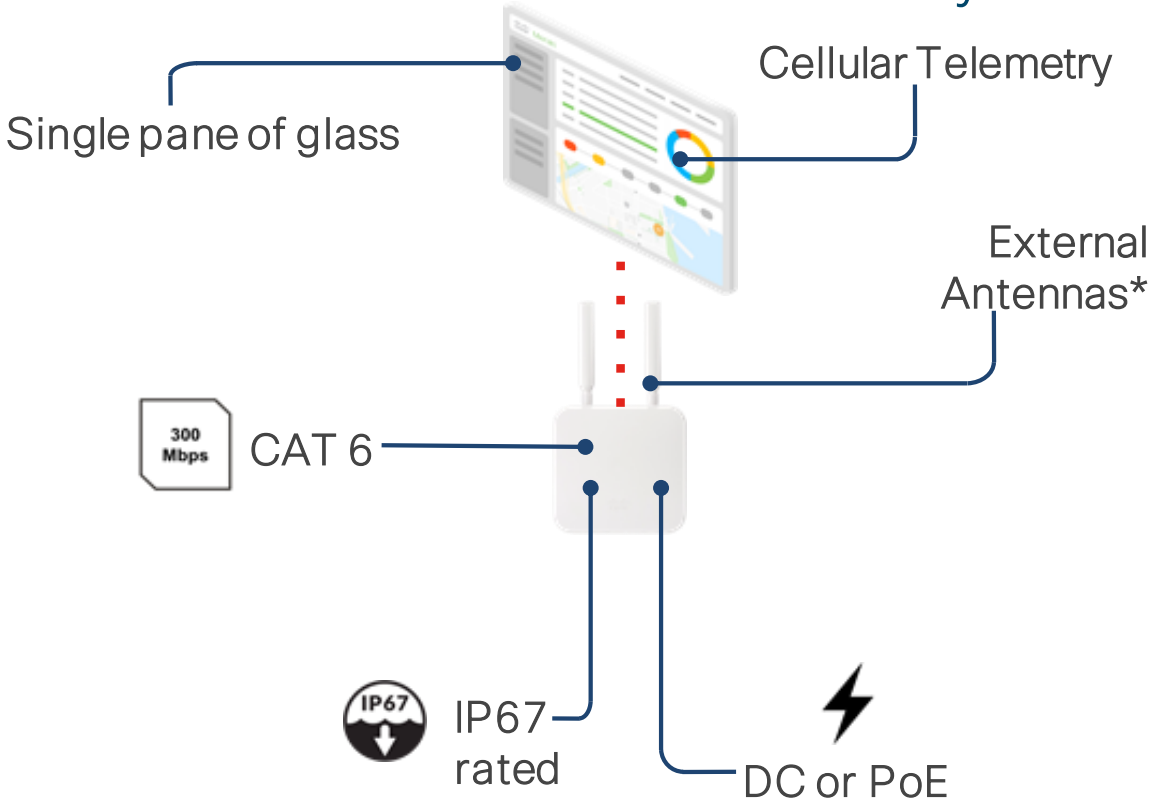
- 802.11ac wave 2 and WiFi 6*
- PSK or Radius Authentication
- GigE uplink
- Full/Split tunneling
- Layer 7 Firewall
- DC or PoE**
- Content Filtering***
- Zero touch provisioning

** on MR36*
*** Requires an adaptor or PoE injector*
**** Requires Advanced license*

MR Comparison Chart

	MR33	MR36	MR42
Uplink	1 x GigE	1 x GigE	1 x GigE
Radio	2.4GHz 5GHz Dedicated Security Radio Bluetooth	2.4GHz 5GHz Dedicated Security Radio Bluetooth	2.4GHz 5GHz Dedicated Security Radio Bluetooth
Hardware Features	2x2 MU-MIMO 802.11ac Wave 2	2x2:2 UL/DL MU-MIMO 802.11ax	3x3 MU-MIMO 802.11ac Wave 2
Aggregate Frame Rate	1.3 Gbps	1.7 Gbps	1.9 Gbps
VPN Throughput	~ 50 Mbps	~ 75 Mbps	~ 50 mbps
Umbrella Integration	Supported with Advanced License	Supported with Advanced License	Supported with Advanced License

WorkConnect MG Cellular Gateway



** with MG21E*

Meraki – VPN

Client VPN

- ❑ Clientless VPN
- ❑ No need to install any software
- ❑ Supported natively on all operating systems
- ❑ Multiple authentication options
- ❑ Two factor authentication
- ❑ Split traffic

AutoVPN

- ❑ Site to Site VPN
- ❑ Full/Split tunneling
- ❑ VPN Firewall
- ❑ VPN Translation
- ❑ Include/exclude local networks
- ❑ Multiple head-ends for resiliency
- ❑ Zero touch provisioning

https://documentation.meraki.com/MX/Client_VPN/Client_VPN_Overview

Meraki Systems Manager

Systems Manager

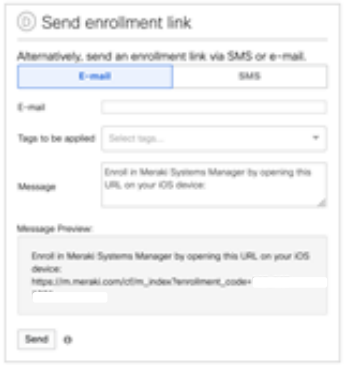
- Easy enrollment via email or SMS or simply via a mobile browser
- Push apps or content
- Restrict usage
- Monitor devices regardless of their location or connection type
- Real time visibility
- Dynamic policies using Sentry
- Hassle free VPN & WiFi provisioning
- Security posture
- Manage hardware and software inventory
- Protect devices, enforce encryption and remote wipe

Enroll Corporate devices with Sys Mgr

Web Browser

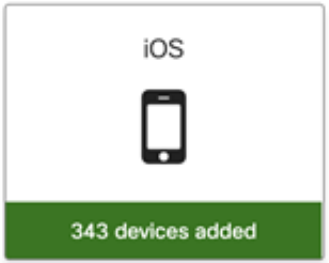
Mobile App

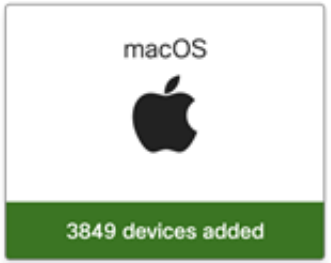
Device Configurator

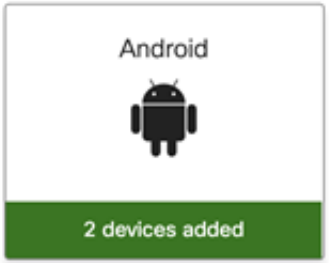


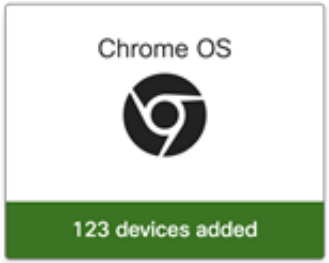
Email / SMS

Manage Hardware and Software Inventory

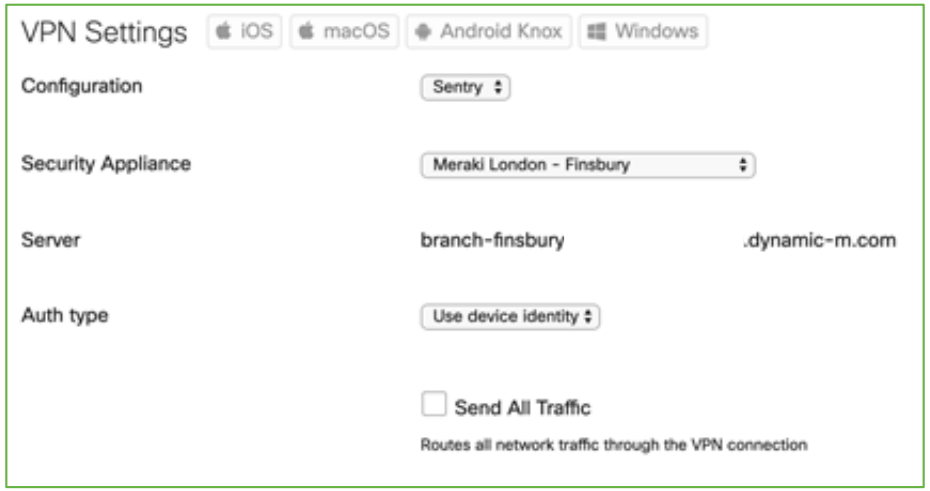


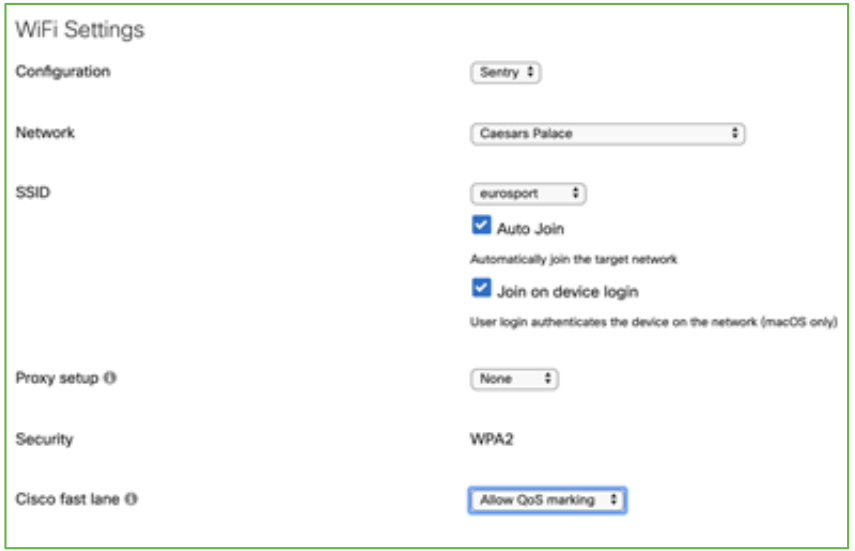




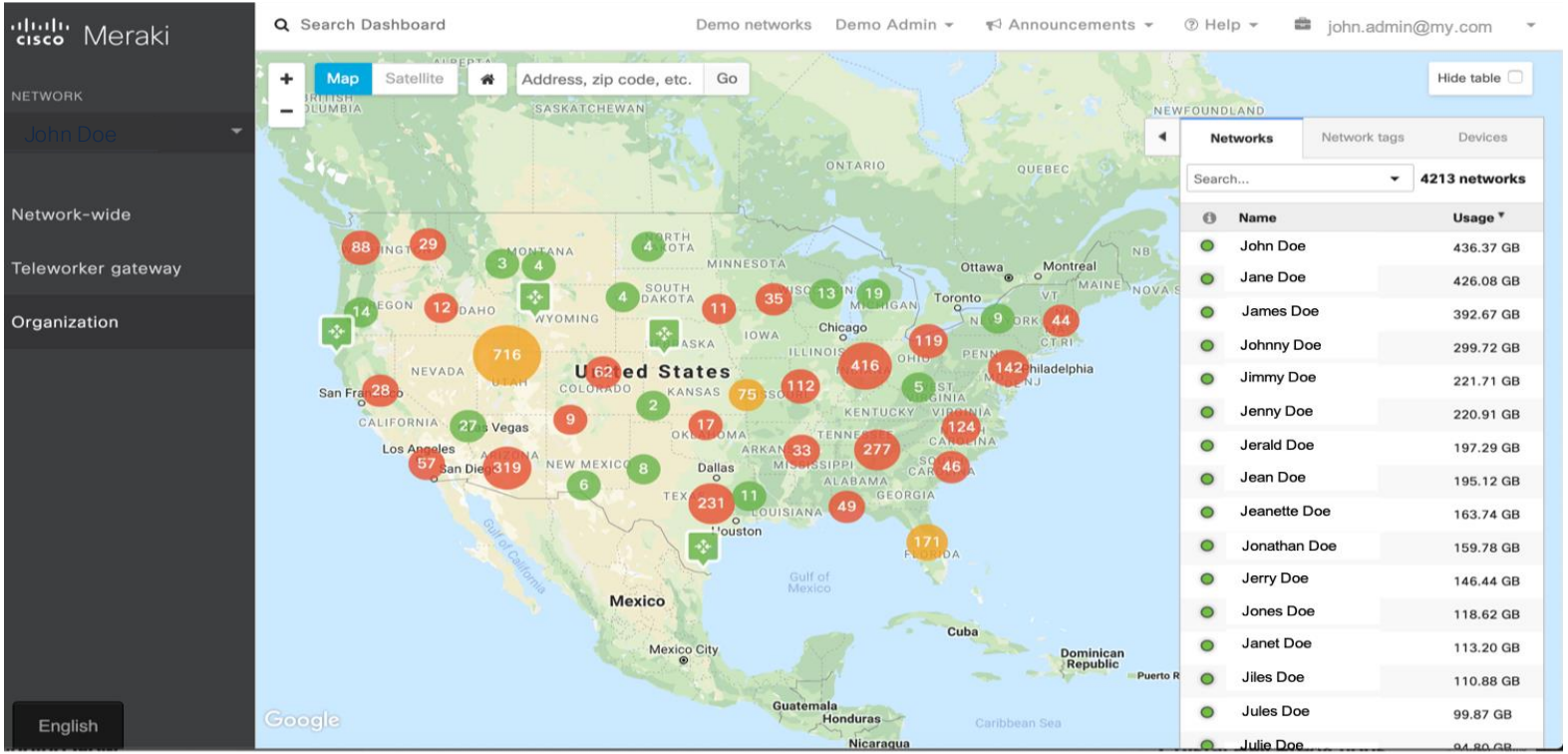


Provision VPN and WiFi





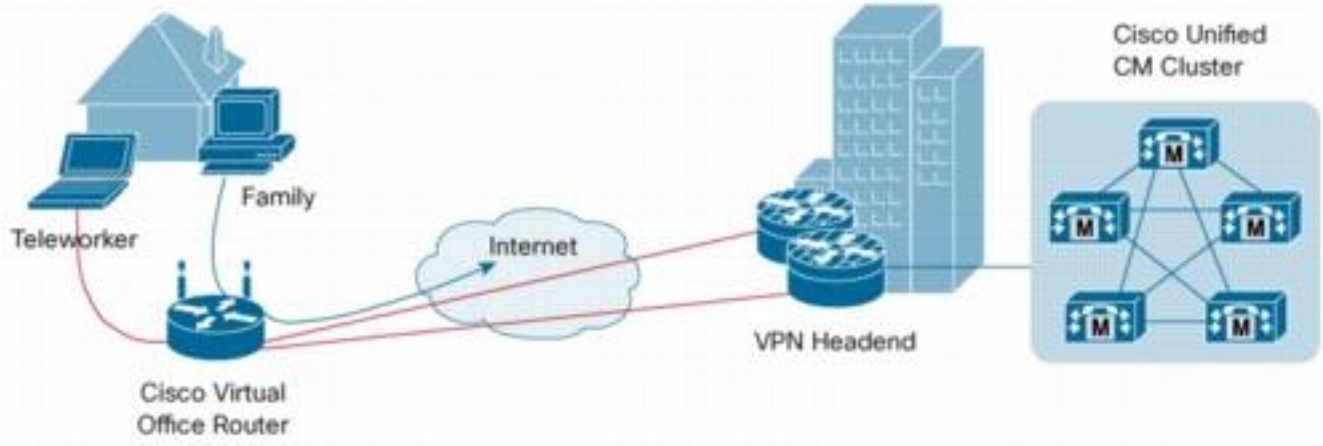
Demo: https://meraki.cisco.com/form/demo



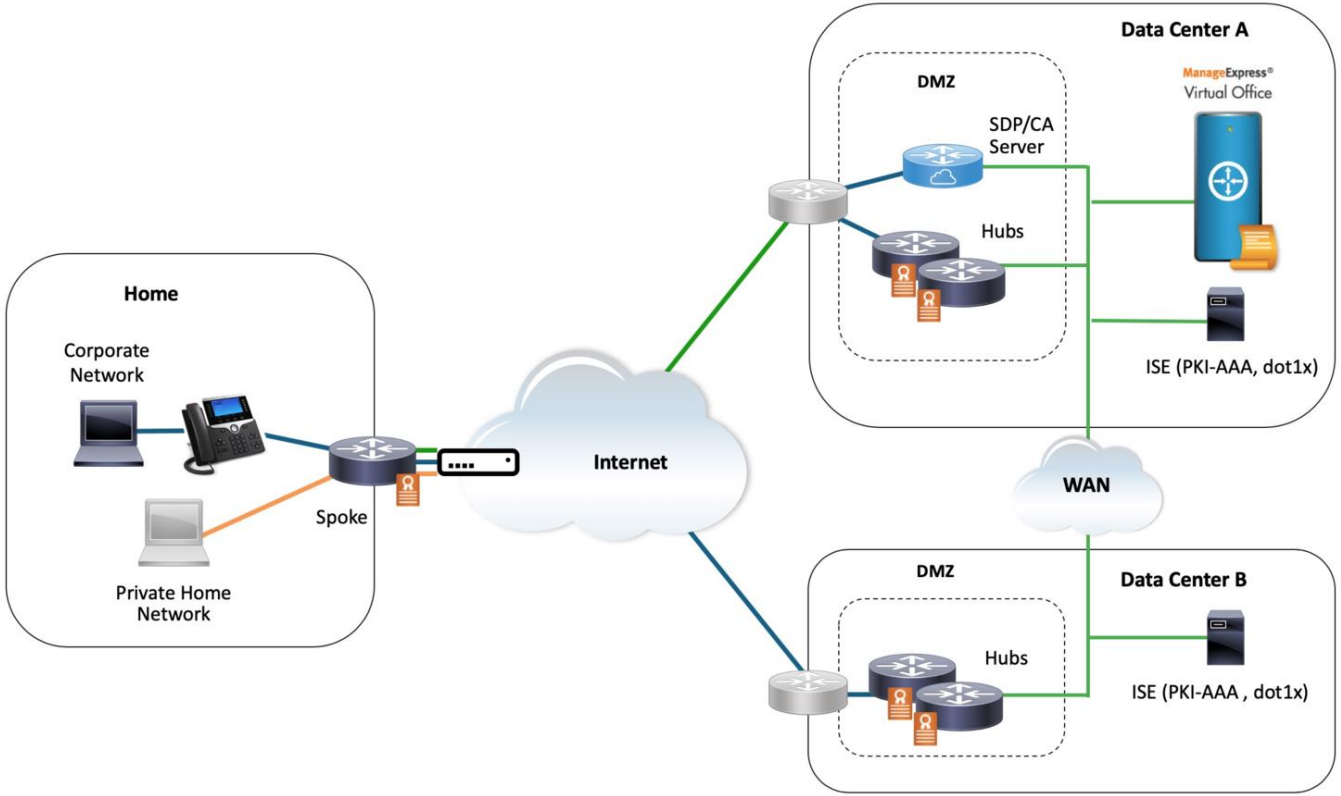
Решение Cisco Virtual Office (CVO)

Обзор CVO

CVO facilitates the deployment of voice, video, wireless, and security technologies as services that can be incrementally enabled on the CPE in response to changing business requirements.



Архитектура CVO



Virtual office / Teleworker

3 Pieces of the Puzzle – What is needed?

Data center

1 - Support for full IP phone, wireless, data, and video services over an encrypted VPN

- CVO Controllers with Zero-Touch deployment and management
  - Licenses : CVO-1100-4P-CFG, CVO-1100-8P-CFG
- VPN Headend : ISR4K for Secure device provisioning, ASR1K Series

2 - Internet Connection

- Headend Internet Connection
- Home Internet Connection

Virtual Office Environment

3 - Cisco Virtual Office Router:

- Remote Router with Wireless:
  - SD-WAN ready Cisco ISR1K : C1121-8PLTEPW$*, C1111-4PW, C1111-8PW, C1117-4PW
  - SEC license needed for CVO deployment to enable zone-based firewall, easyVPN, DMVPN capabilities
- See bundle options in following slides

* SKU based on Wi-Fi domain

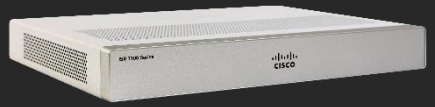
Suitable for midsize and large organizations looking to provide teleworkers, small offices, and mobile users with office-like experiences combining voice, video, wireless, and real-time data applications in a secure environment

Gigabit-Plus LTE Connectivity to On-Demand Locations
ISR 1121 + 4G/LTE (5Ge) Advanced Pro Module

SD-WAN Ready

- Router
- Security
- Switch Ports
- Wireless (Wi-Fi)
- Cellular (1.2 Gbps LTE Advanced Pro)

C1121X-8PLTEPWY*



+

P-LTEAP18-GL**

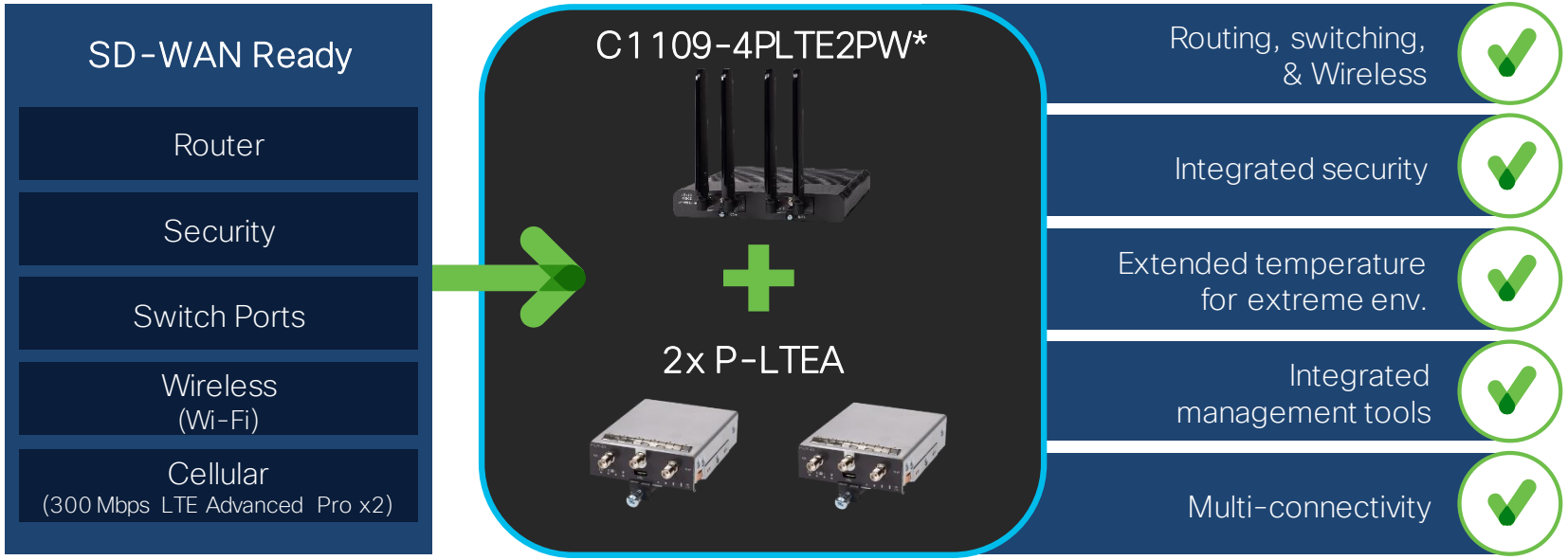
- Routing, switching, and wireless
- Integrated security
- Speed and performance
- Integrated management tools
- Multi-connectivity

PID	LTE Bands
P-LTEAP18-GL	1, 2, 3, 4, 5, 7, 8, 12, 13, 14, 17, 18, 19, 20, 25, 26, 28, 29, 30, 32, 38, 39, 40, 41, 42, 43, 46, 48, 66, 71

** P-LTEAP18-GL available Europe & US only. For global CAT6 LTE options please visit ISR1K Datasheet

C1121X-8PLTEPWY*
* Wi-Fi domain WY; Y = A, E, B, Z

Active/Active LTE Advanced Connectivity to On-Demand Locations
ISR 1109 with Dual-Pluggables



PID	LTE Bands
P-LTEA-EA	1-5, 7, 12, 13, 20, 25, 26, 29, 30, and 41
P-LTEA-LA	1, 3, 5, 7, 8, 18, 19, 21, 28, 38, 39, 40, and 41

C1109-4PLTE2PW*
* Wi-Fi domain W* =A, B, D, E, Q, R, Z

1

Secure Connectivity to Remote Teleworkers
ISR 1111 with Integrated 4G LTE Advanced

SD-WAN Ready

- Router
- Security
- Switch Ports
- Wireless (Wi-Fi)
- Cellular (300 Mbps LTE Advanced)

C1117-4PW
C1111-4PW / C1111-8PW

- Routing, switching, and wireless
- Integrated security
- Speed and performance
- Integrated management tools
- Multi-connectivity

PID	LTE Bands
C1111-xPLTEEA	1-5, 7, 12, 13, 20, 25, 26, 29, 30, and 41
C1111-xPLTELA	1, 3, 5, 7, 8, 18, 19, 21, 28, 38, 39, 40, and 41

C1111-xPLTExAW*
* Wi-Fi domain W* = A, B, D, E, F, H, N, Q, S, Z

Предложения для построения удаленных офисов

Teleworker Bundles

ISR1000-4P-TWPM20
ISR1000-8P-TWPM20

(14% Off on HW)*

Use cases : Home Office

- SD-WAN Ready ISR1K
  - SKU Options : C1121-8PLTEPW$*, C1111-4PW, C1111-8PW, C1117-4PW
  - Wi-Fi domain: W$; $ = A, E, B, Z
- Free Virtual Office License
  - SKU : CVO-1100-4P-CFG, CVO-1100-8P-CFG
- Cellular Modules
  - SKU Options : P-LTEAP18-GL, P-LTEA-EA, P-LTE
- Add-on SD-WAN subscriptions (L-LIC-DNA-ADD)

Microbranch Bundle

ISR1000-4P-MBPM20
ISR1000-8P-MBPM20

(14% Off on HW)

Use cases : Health Camps / Relief Camps / Support center/ Urgent Care

- SD-WAN Ready ISR1K
  - SKU Options : C1121X-8PLTEPW$*, C1109-4PLTE2PWB, C1111-xPLTExAW*
  - Wi-Fi domain: W$; $ = A, E, B, Z
- Cellular Modules
  - SKU Options : P-LTEAP18-GL, P-LTEA-EA, P-LTE
- SD-WAN subscriptions (Optional – As part of bundle)

Benefits of CVO

1

Scalability

Allows consistent secure access for users at corporate headquarters, remote sites, home offices, and public hotspots.

2

Secure, zero-touch deployment

Quickly proliferate deployments to remote sites with no IT staff. Automation of ongoing operations through central network management, using push technology, to simplify administration and keep costs low.

3

Application performance

Delivers application performance required for latency and bandwidth-sensitive voice, video, and real-time data applications: This capability calls for advanced integration of VPN technologies with quality of service (QoS), IP Multicast, voice, and video services.

4

Secure access and control

Maintain complete control over the entities attempting to access the network at remote, off-campus locations where ascertaining physical identity is not possible. Limit access to certain devices or users, separate domains for employees and guests and families, and the ability to allow employees to use resources in untrusted domains without compromising security.

Additional Resources

https://www.cisco.com/c/en/us/solutions/enterprise-networks/virtual-office/index.html

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/virtual-office/guide_c07-683001.html

Дополнительные ресурсы

Additional Resources

Additional Webinars:

- https://www.cisco.com/c/m/en_us/covid19/atx-webinars.html

Cisco Covid-19 Response Landing Page:

- http://www.cisco.com/covid19

OEAP Configuration Video:

- https://youtu.be/MfdemAD0vos

Mail List for Teleworker Specific Technical Questions:

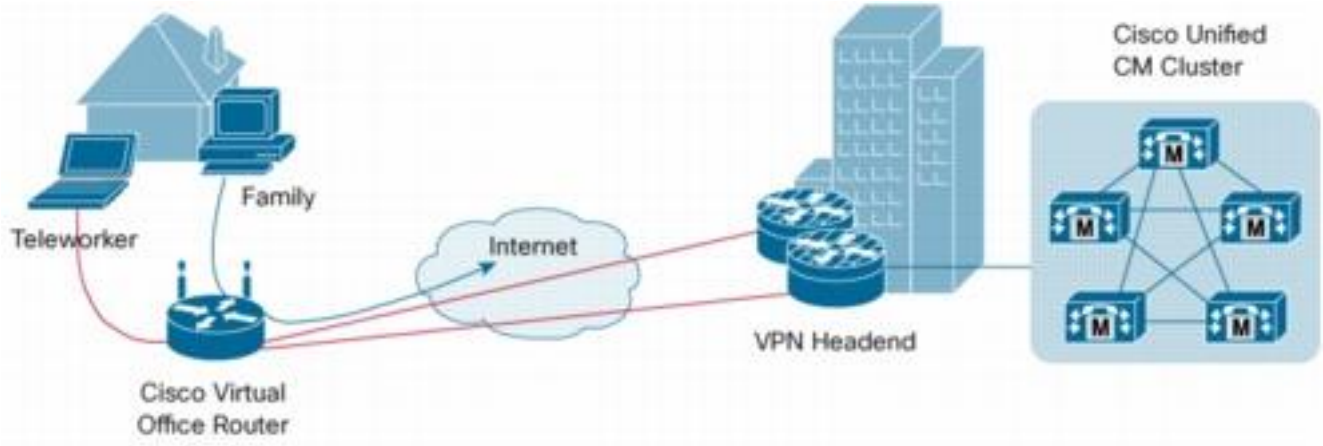
- teleworker_qa@external.cisco.com

Final Thoughts

Cisco Virtual Office (CVO) Solution

CVO Overview

CVO facilitates the deployment of voice, video, wireless, and security technologies as services that can be incrementally enabled on the CPE in response to changing business requirements.



Benefits of CVO

1

Scalability

Allows consistent secure access for users at corporate headquarters, remote sites, home offices, and public hotspots.

2

Secure, zero-touch deployment

Quickly proliferate deployments to remote sites with no IT staff. Automation of ongoing operations through central network management, using push technology, to simplify administration and keep costs low.

3

Application performance

Delivers application performance required for latency and bandwidth-sensitive voice, video, and real-time data applications: This capability calls for advanced integration of VPN technologies with quality of service (QoS), IP Multicast, voice, and video services.

4

Secure access and control

Maintain complete control over the entities attempting to access the network at remote, off-campus locations where ascertaining physical identity is not possible. Limit access to certain devices or users, separate domains for employees and guests and families, and the ability to allow employees to use resources in untrusted domains without compromising security.

Additional Resources

https://www.cisco.com/c/en/us/solutions/enterprise-networks/virtual-office/index.html

https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/virtual-office/guide_c07-683001.html