Cisco TechClub
Webináře

Jak jednoduše a zároveň bezpečně připojit zaměstnance z home office do firemní sítě?

VPN Remote Access, OfficeExtend AP (OEAP), Meraki Teleworker

Jaroslav Čížek, Jiří Tesař, Andrej Jeleník

Duben 2020

Agenda

- Úvod – přehled možností
- VPN Remote Access
- OfficeExtend Access Point (OEAP)
- Meraki Teleworker
- Shrnutí

Network Connectivity – Teleworker Options

VPN remote Access

Platform Support:

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

Benefits

- Highly secure access across popular PC and mobile devices
- Consistent user experience
- Intelligent, dependable, and always-on connectivity

OEAP Cisco Controller On-Prem Solution

Platform Support (Option 1):

- WLC
- AP3500 and newer

Platform Support (Option 2)

- WLC
- OEAP600, AP1810, AP1815T

Benefits

- Repurpose existing AP's
- Remote Ethernet available with Option 2

Meraki Teleworker Cloud Based Solution

Platform Support:

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

Benefits:

- 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

Platform Support

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

Benefits:

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

VPN Remote Access

Solution Components

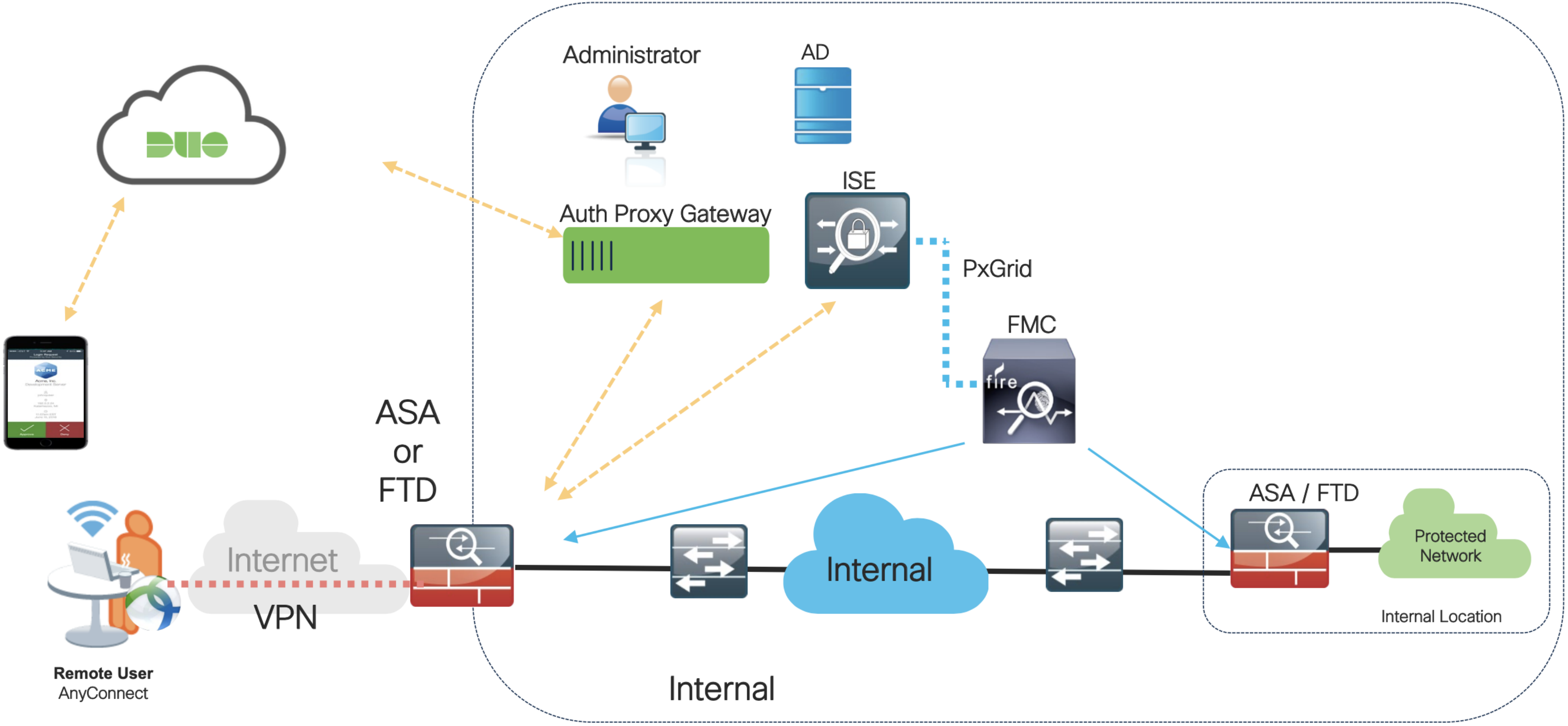
Establish Trust

Enforce Trust-Based Access

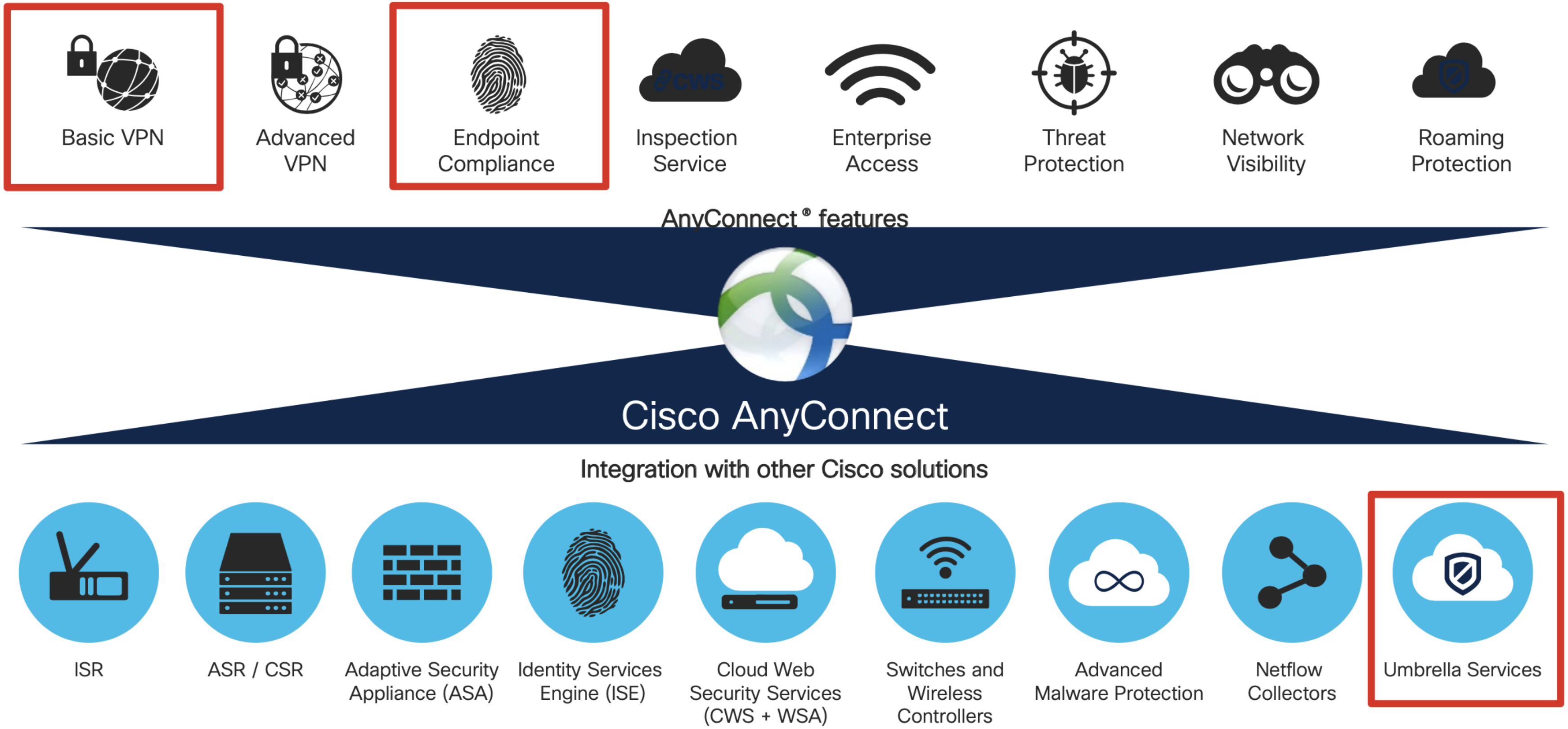
Continuous Trust Verification

Multi Factor Authentication	DUO	Verify identity of users
Policy Control and Management	ISE FMC	Ensure trustworthiness of devices
Infrastructure	ASA / FTD	Enforce risk-based and adaptive access policies

Big Picture Architecture



Cisco AnyConnect® – Way more than VPN



Basic VPN

Advanced VPN

Endpoint Compliance

Inspection Service

Enterprise Access

Threat Protection

Network Visibility

Roaming Protection

AnyConnect® features

Cisco AnyConnect

Integration with other Cisco solutions

ISR

ASR / CSR

Adaptive Security Appliance (ASA)

Identity Services Engine (ISE)

Cloud Web Security Services (CWS + WSA)

Switches and Wireless Controllers

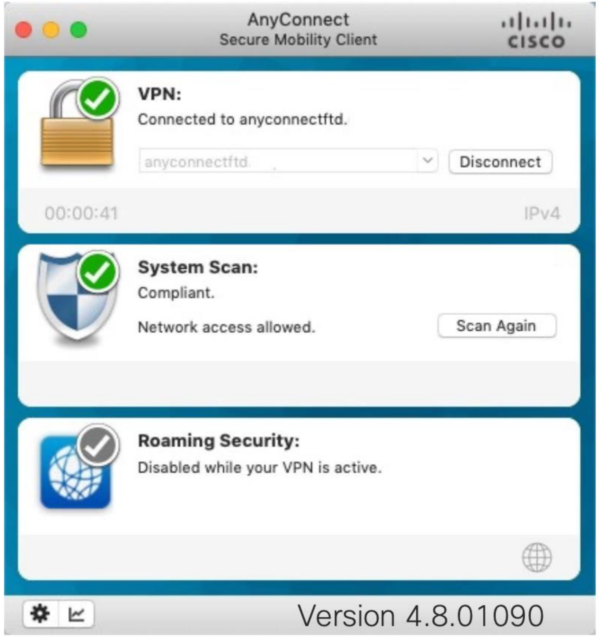
Advanced Malware Protection

Netflow Collectors

Umbrella Services

AnyConnect Secure Mobility Client

- TLS/IPSec IKEv2 Client
- IPv4, IPv6
- Windows, MAC OS X, Linux Intel
- Mobile devices IOS/Android
- Strong and NG encryption
- Authentication Options
- Consistent User Experience
- And more…



AnyConnect
Secure Mobility Client

VPN:
Connected to anyconnectftd.

anyconnectftd

00:00:41 IPv4

System Scan:
Compliant.
Network access allowed.

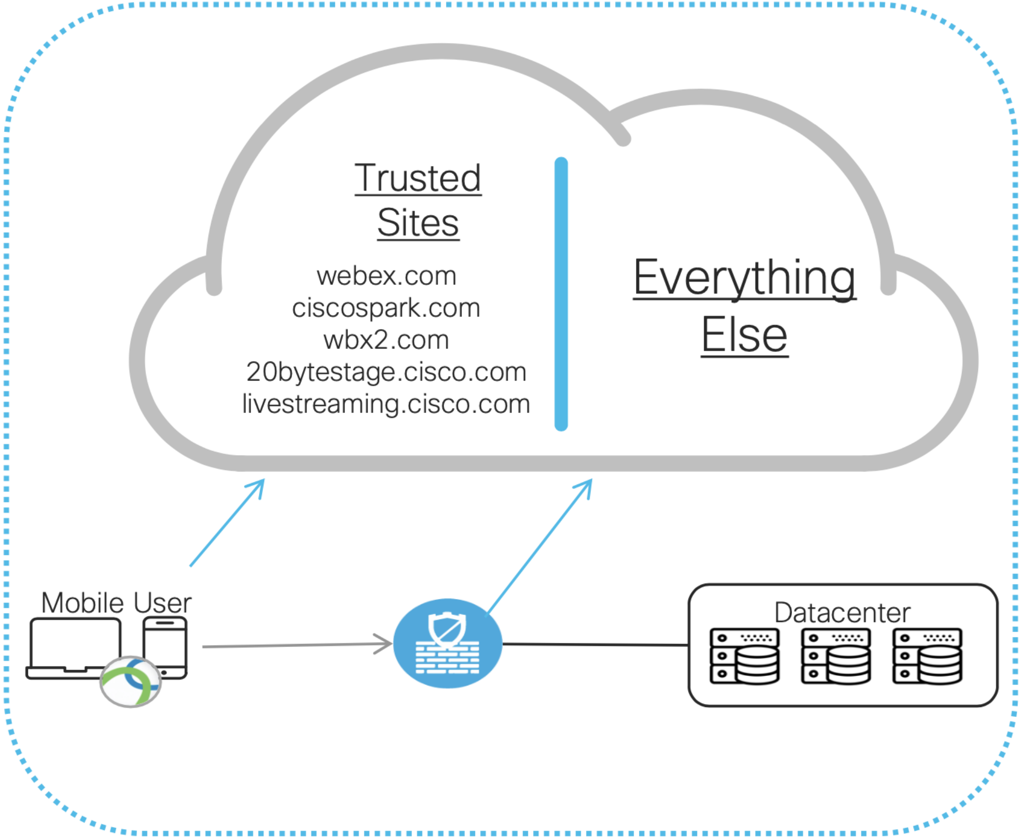
Roaming Security:
Disabled while your VPN is active.

Version 4.8.01090

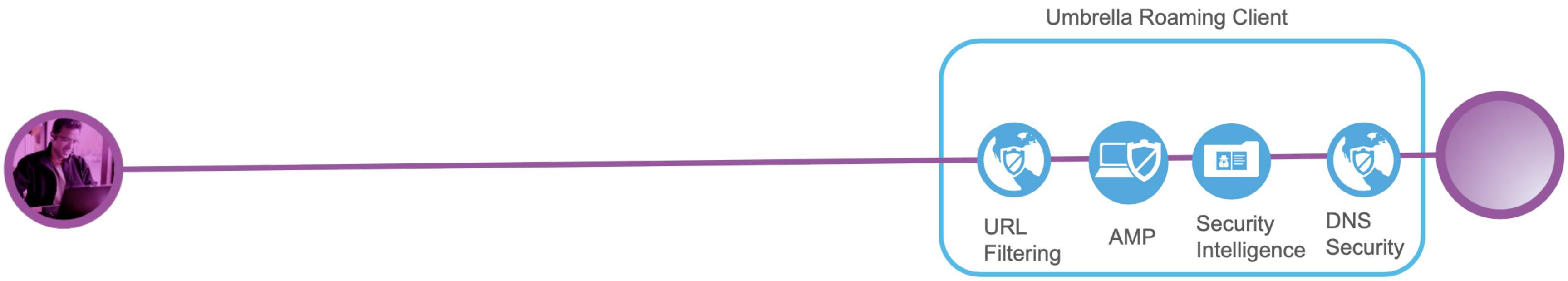
https://www.cisco.com/c/en/us/products/collateral/security/anyconnect-secure-mobility-client/datasheet-c78-733184.html

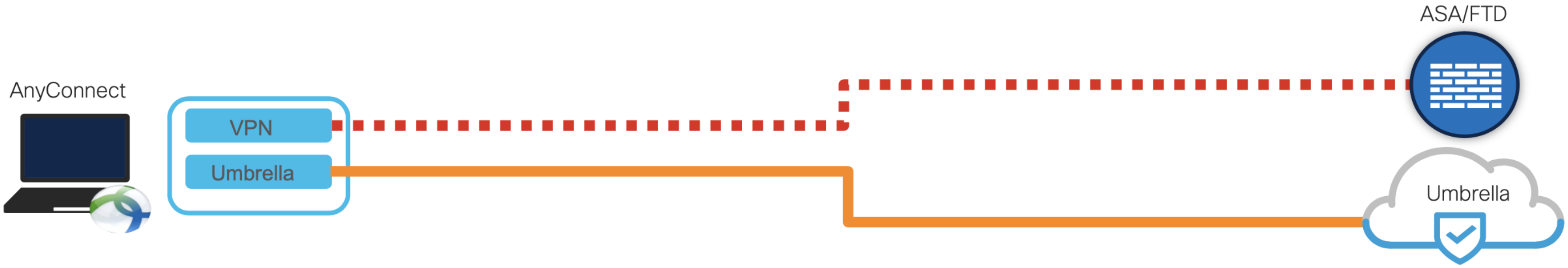
AnyConnect Dynamic Split Tunnels

- Allows applications to be dynamically excluded from the AnyConnect VPN tunnel by specifying a list of domain names.
- AnyConnect will dynamically identify IP addresses associated with these domains, and exclude them from the VPN tunnel
- This allows trusted cloud and web applications to be offloaded from TIC access points.



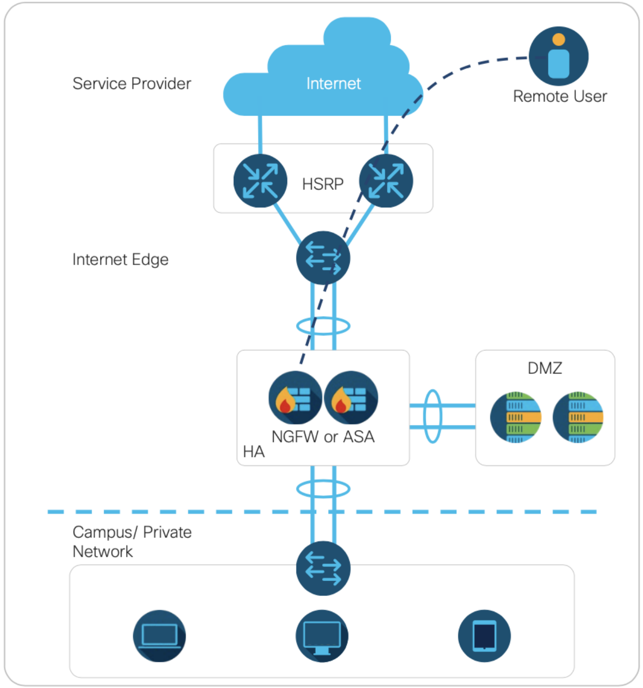
Typical Endpoint Requirements





FTD For Remote Access VPN

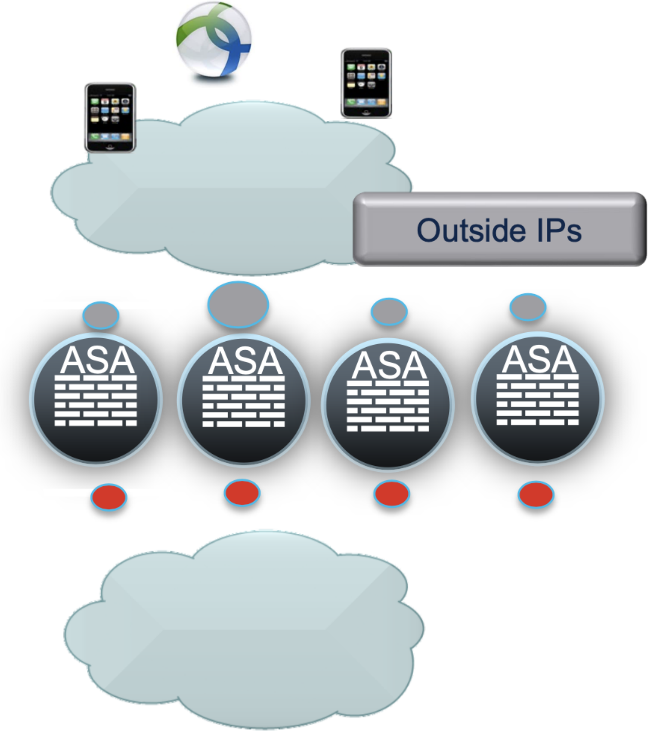
Key Functions	Key Capabilities
Resilience (and scalability)	VPN load balancing
Advanced Access Control	IPSEC and SSL
Block access to malicious IP's, URL's, DNS	**Talos Security Intelligence**
Dynamic NAT/PAT and Static NAT	AD, LDAP and Radius
Remote Access VPN	IKEv1 and IKEv2
Site to Site VPN	RADIUS CoA
Detecting malicious network traffic	**Snort IPS**
Visibility and tracking of file transfers, Blocking of malicious files	**Advanced Malware Protection**
Dynamic analysis of unknown files	**Threat Grid Integration**



Use-case: RAVPN

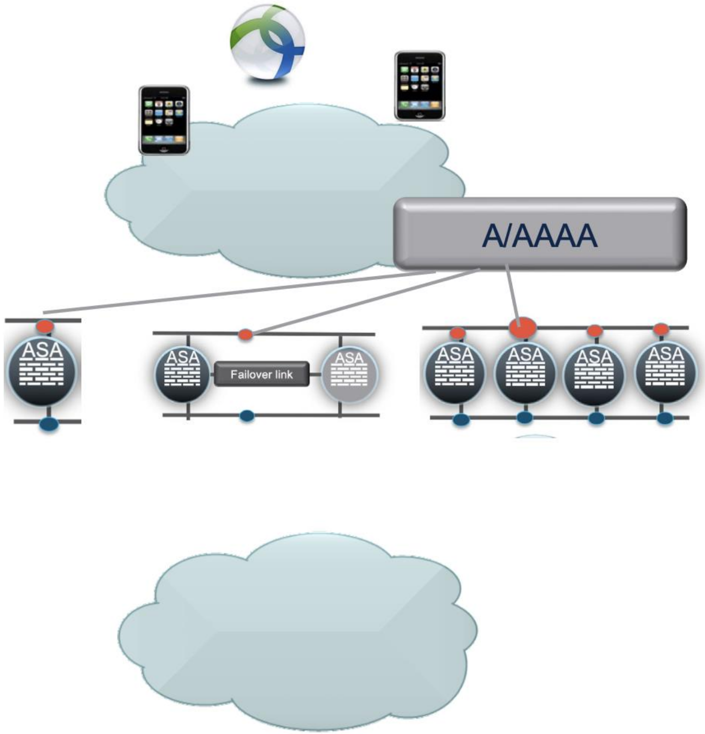
VPN Load Balancing (Native)

- Multiple ASAs in a VPN Cluster
  - **Not the same as ASA Clustering** technology (which does not support remote access VPN)
- Each ASA has separate config and IPs
- ASA ”master” also owns the shared virtual IP
- AnyConnect Client connects to master and is redirected to “least loaded” ASA
- No configuration or state-synch
- Unfortunately rarely used...
  - Lack of seamless failover?
  - ...but, allows for different hardware/software across ASAs (easy upgrading/expansion)
  - Very stable (old technology)



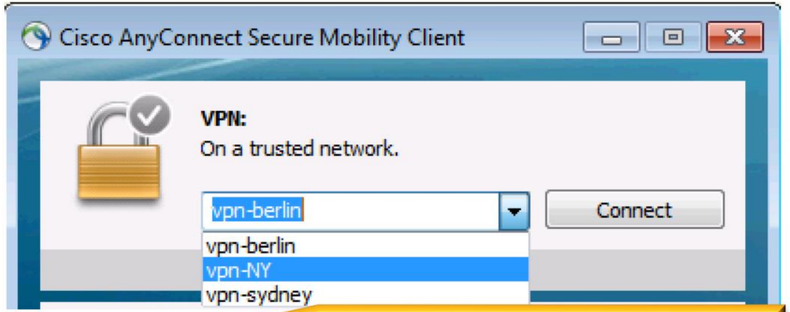
Quick and Ugly Scaling : VPN Load Balancing (DNS)

- Supported by most DNS servers...
- VPN gateway (e.g. vpn.labrats.se) resolved to different A/AAAA
- could be separate VPN load balancing clusters, or HA-pairs, or individual ASAs/FTDs
- avoid certificate warnings!
  - same cert / private key for all ASAs
  - wild card cert. *.vpn.labrats.se
  - use vpn.labrats.se in SAN field of all certs
- Note: No automatic failover! Client may need to manually reconnect



“Manual Scaling” – Let user decide!

- Let user choose gateway
  - From dropdown
  - Each gateway may have predefined backups
    - backup not automatically chosen if failure due to oversubscription
- Can push different profiles to diff users

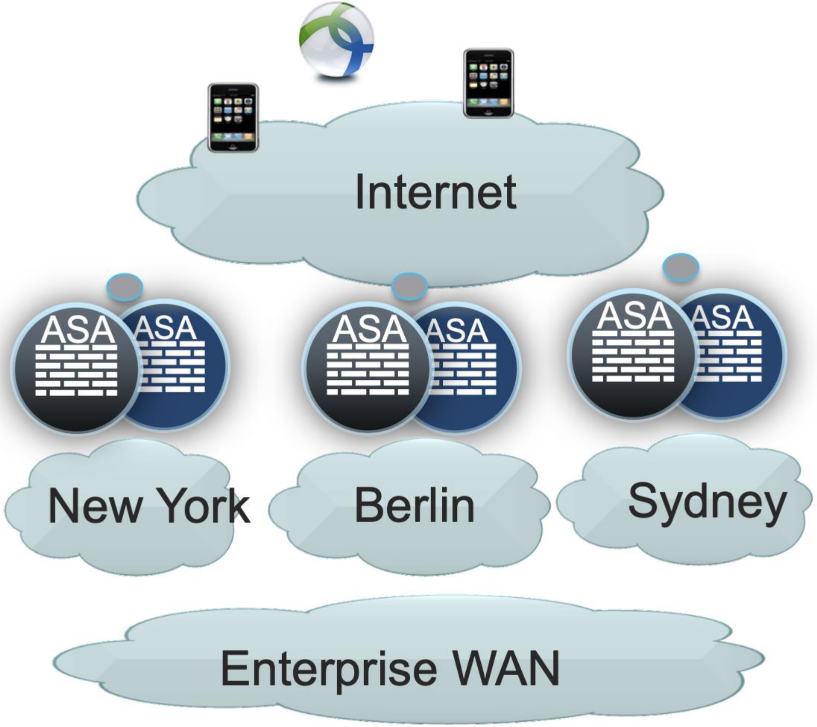


Cisco AnyConnect Secure Mobility Client

VPN:
On a trusted network.

vpn-berlin

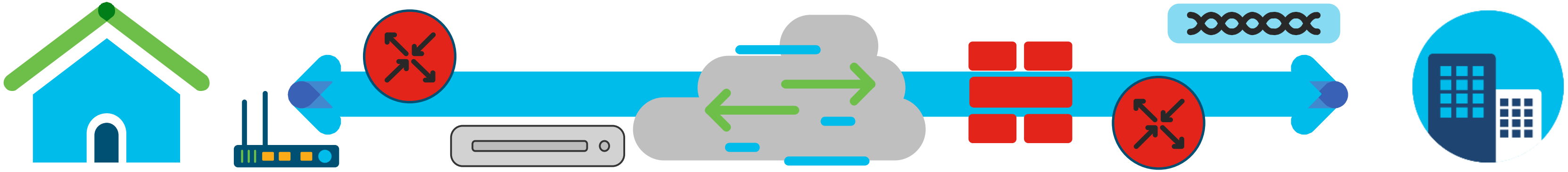
AnyConnect Client Profiles (described later)



OfficeExtend Access Point (OEAP) Teleworker Solution

Secure Teleworker / Micro office - OEAP

3 Pieces of the Puzzle – What is needed?



Home Environment

1-Any Aironet or Catalyst AP:

Any Cisco Catalyst or Aironet AP going 3 generations back can be used:

- 11ax: 91xx
- 11ac W2: 18xx/28xx/38xx/48xx
- 11ac W1: 17xx/27xx/37xx
- 11n: 16xx/26xx/36xx

- *Purpose built 1815T teleworker AP AireOS 8.5 and Later, also IOS XE; Recommended 8.5.161.0/8.10.112.0, 17.2*
- *Any Aironet 11n – AP16xx/26xx/36xx; AireOS 7.4 to AireOS 8.5*
- *11ac Wave 1 – AP17xx/27xx/37xx AireOS 8.3 and later, also IOS XE; Recommended 8.5.161.0/8.10.112.0, 17.2*
- *11ac Wave 2 AP's- AP18xx/28xx/38xx) AireOS 8.3 and later also IOS XE; Recommended 8.5.161.0/8.10.112.0, 17.2*
- *11ax AP's – C9115, C9117, C9120, C9130 AireOS 8.10 also IOS XE 17.2; Recommended 8.5.161.0/8.10.112.0, 17.2*

2-Internet Connection

Office Internet Connection (where WLC is deployed)

Home Internet Connection

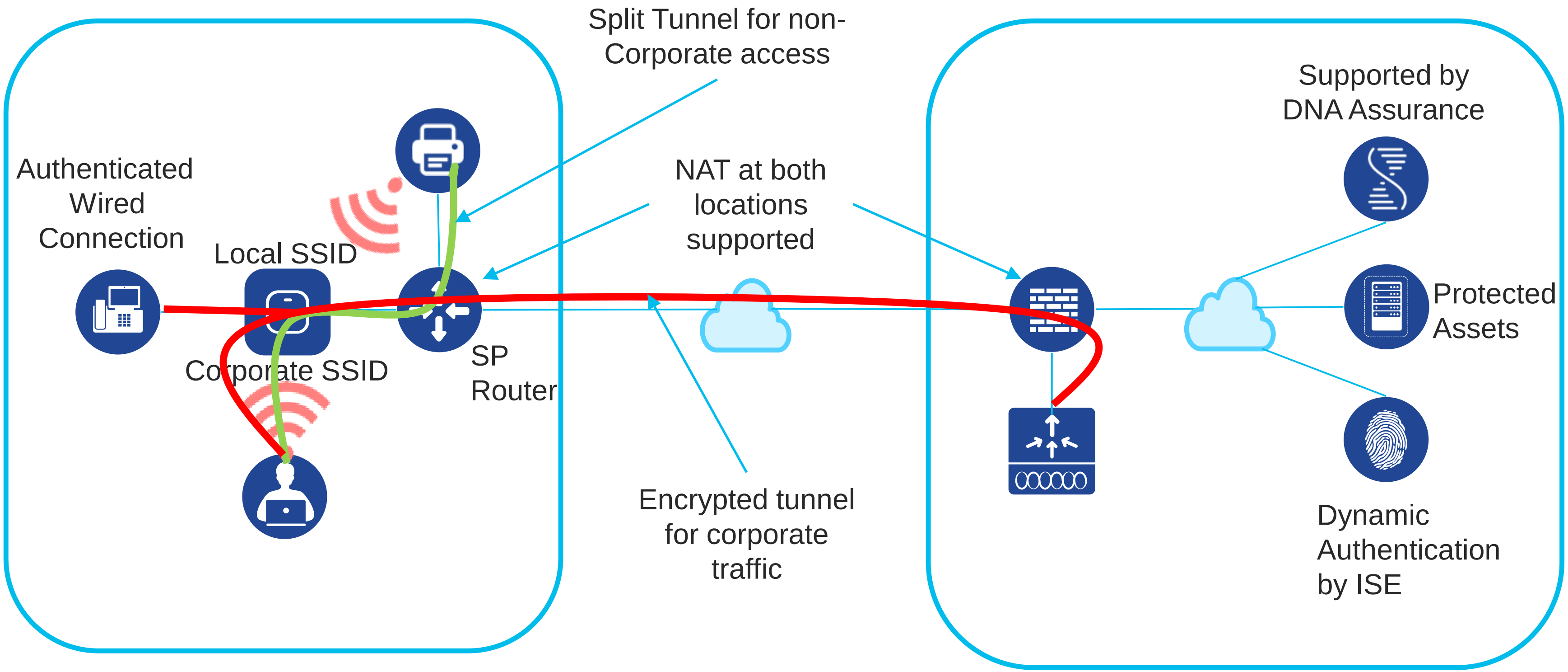
Office Environment

3 -Any WLC - Physical or Virtual: (w. sufficient AP licenses)

- Cisco IOS XE: Virtual: Catalyst 9800-CL (free download), Catalyst 9800-L, 9800-40, 9800-80
- AireOS: 2504/3504/55xx/85xx

- *Can be any AireOS Controller WLC 3504/5520/8540 or even older 508/8510 running AireOS 8.5 or later*
- *note: AireOS vWLC does not support OEAP*

OfficeExtend AP – Operation
Expanding Wireless Coverage


Split Tunnel for non-Corporate access
Authenticated Wired Connection
Local SSID
NAT at both locations supported
Supported by DNA Assurance
Corporate SSID
SP Router
Protected Assets
Encrypted tunnel for corporate traffic
Dynamic Authentication by ISE

OfficeExtend AP - Features

Most likely already own the components for this

✓ 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

Cisco AP1815T - 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

OfficeExtend AP – Basic 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. 1600/2600/3600/2700/3700/3800/4800 etc. – admin needs to change the AP mode to FlexConnect and then enable OEAP option.

- Pre-configure the OEAPs to join the WLC i.e. configure OEAP with WLC management public IP address

Reference OEAP Cisco Validated Design Link

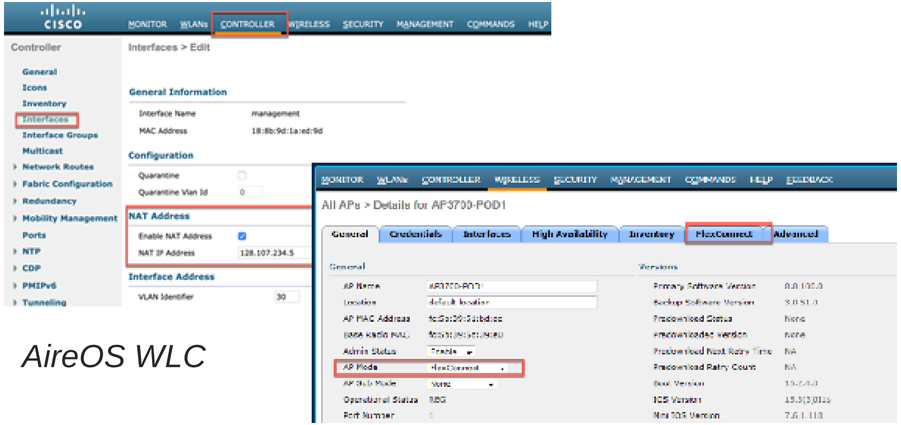
OfficeExtend AP – AireOS and IOS-XE/C9800 Configuration Video

- AireOS WLC Guided Configuration Walk-through

  Watch an AireOS WLC Guided Configuration Walk-through

- IOS-XE/C9800 WLC Guided Configuration Walk-through

  Watch a C9800 WLC Guided configuration Walk-through



CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP
Controller
General
Icons
Inventory
Interfaces
Interface Groups
Multicast
Network Routes
Fabric Configuration
Redundancy
Mobility Management
Ports
NTP
CDP
PMIPv6
Tunneling
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
General Credentials Interfaces High Availability Inventory FlexConnect Advanced

Interfaces > Edit

General Information

Interface Name management
MAC Address 18:8b:9d:1a:ed:9d

Configuration

Quarantine □
Quarantine Vlan Id 0

NAT Address

Enable NAT Address ☑
NAT IP Address 128.107.234.5

Interface Address

VLAN Identifier 30

All APs > Details for AP3700-POD1

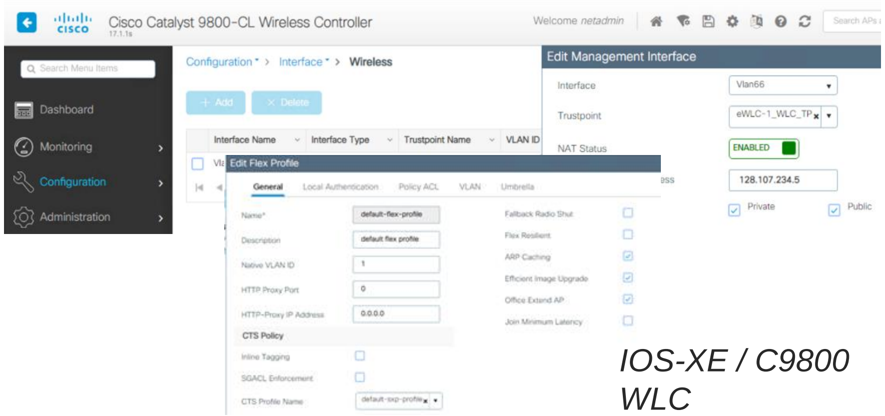
General

AP Name AP3700-POD1
Location default location
AP MAC Address fc:5b:39:53:bd:cc
Base Radio MAC fc:5b:39:5d:39:e0
Admin Status Enable
AP Mode FlexConnect
AP Sub Mode None
Operational Status REG
Port Number 1

Versions

Primary Software Version 8.8.100.0
Backup Software Version 8.0.51.0
Predownload Status None
Predownloaded Version None
Predownload Next Retry Time NA
Predownload Retry Count NA
Boot Version 15.2.4.0
IOS Version 15.3(3)JD1
Mini IOS Version 7.6.1.118

AireOS WLC



Configuration > Interface > Wireless

Edit Management Interface

Interface Vlan66
Trustpoint eWLC-1_WLC_TP
NAT Status ENABLED
128.107.234.5
☑ Private ☑ Public

Edit Flex Profile

Name* default-flex-profile
Description default flex profile
Native VLAN ID 1
HTTP Proxy Port 0
HTTP-Proxy IP Address 0.0.0.0

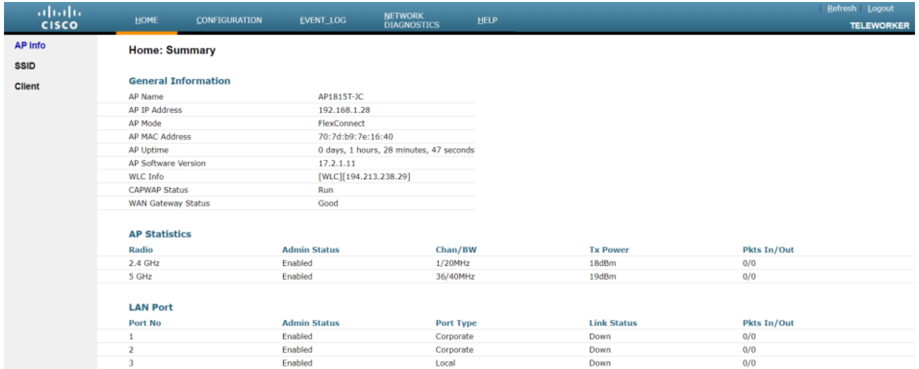
CTS Policy

Inline Tagging □
SGACL Enforcement □
CTS Profile Name default-sxp-profile

Fallback Radio Shut □
Flex Resilient □
ARP Caching ☑
Efficient Image Upgrade ☑
Office Extend AP ☑
Join Minimum Latency □

IOS-XE / C9800 WLC

OfficeExtend AP – Local AP Web GUI



Home: Summary

General Information

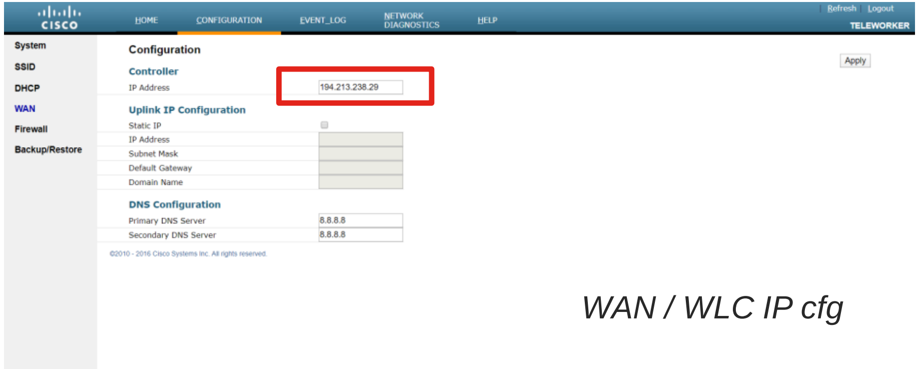
AP Name	AP1815T-JC
AP IP Address	192.168.1.28
AP Mode	FlexConnect
AP MAC Address	70:7d:b9:7e:16:40
AP Uptime	0 days, 1 hours, 28 minutes, 47 seconds
AP Software Version	17.2.1.11
WLC Info	[WLC][194.213.238.29]
CAPWAP Status	Run
WAN Gateway Status	Good

AP Statistics

Radio	Admin Status	Chan/BW	Tx Power	Pkts In/Out
2.4 GHz	Enabled	1/20MHz	18dBm	0/0
5 GHz	Enabled	36/40MHz	19dBm	0/0

LAN Port

Port No	Admin Status	Port Type	Link Status	Pkts In/Out
1	Enabled	Corporate	Down	0/0
2	Enabled	Corporate	Down	0/0
3	Enabled	Local	Down	0/0



Configuration

Controller

IP Address	194.213.238.29

Uplink IP Configuration

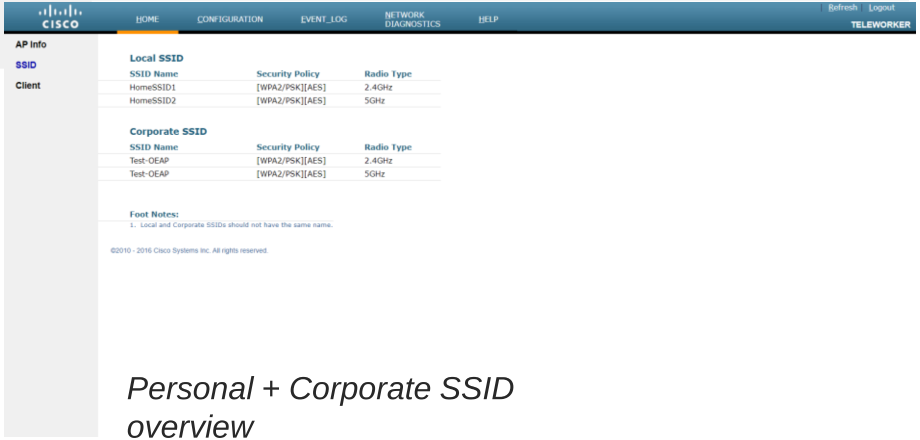
Static IP	□
IP Address	
Subnet Mask	
Default Gateway	
Domain Name	

DNS Configuration

Primary DNS Server	8.8.8.8
Secondary DNS Server	8.8.8.8

©2010 - 2016 Cisco Systems Inc. All rights reserved.

WAN / WLC IP cfg



Local SSID

SSID Name	Security Policy	Radio Type
HomeSSID1	[WPA2/PSK][AES]	2.4GHz
HomeSSID2	[WPA2/PSK][AES]	5GHz

Corporate SSID

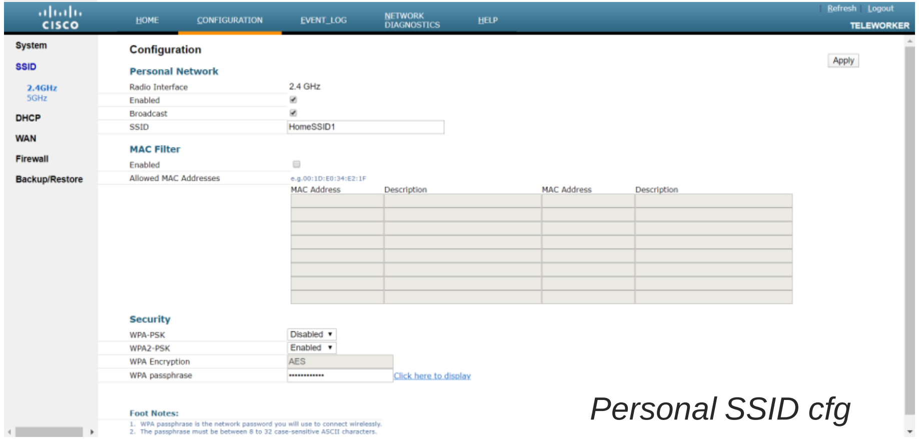
SSID Name	Security Policy	Radio Type
Test-OEAP	[WPA2/PSK][AES]	2.4GHz
Test-OEAP	[WPA2/PSK][AES]	5GHz

Foot Notes:

1. Local and Corporate SSIDs should not have the same name.

©2010 - 2016 Cisco Systems Inc. All rights reserved.

Personal + Corporate SSID overview



Configuration

Personal Network

Radio Interface	2.4 GHz
Enabled	☑
Broadcast	☑
SSID	HomeSSID1

MAC Filter

Enabled	□
Allowed MAC Addresses	e.g.00:1D:E0:34:E2:1F

MAC Address	Description	MAC Address	Description

Security

WPA-PSK	Disabled ▾
WPA2-PSK	Enabled ▾
WPA Encryption	AES
WPA passphrase	•••••••••••• Click here to display

Foot Notes:

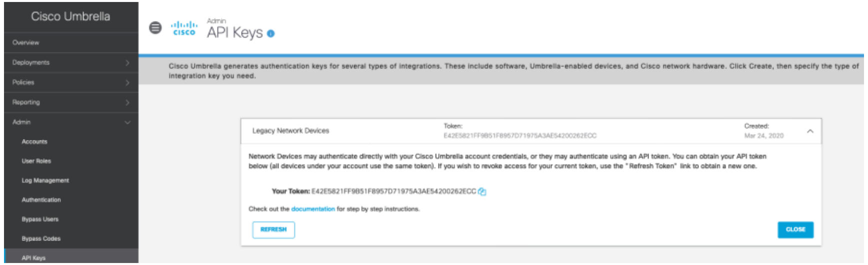
1. WPA passphrase is the network password you will use to connect wirelessly.
2. The passphrase must be between 8 to 32 case-sensitive ASCII characters.

Personal SSID cfg

Cisco Public

OfficeExtend AP – Optional Umbrella Integration

- Integration with Umbrella can be enabled to further enhance the security of the users



Cisco Umbrella generates authentication keys for several types of integrations. These include software, Umbrella-enabled devices, and Cisco network hardware. Click Create, then specify the type of integration key you need.

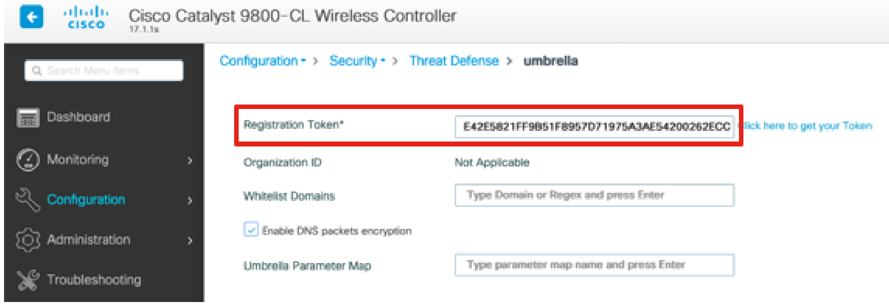
Legacy Network Devices
Token: E42E5821FF9B51F8957D71975A3AE54200262ECC
Created: Mar 24, 2020

Network Devices may authenticate directly with your Cisco Umbrella account credentials, or they may authenticate using an API token. You can obtain your API token below (all devices under your account use the same token). If you wish to revoke access for your current token, use the "Refresh Token" link to obtain a new one.

Your Token: E42E5821FF9B51F8957D71975A3AE54200262ECC

Check out the documentation for step by step instructions.

Cisco Umbrella


Cisco Catalyst 9800-CL Wireless Controller
17.1.1s
Search Menu Items
Dashboard
Monitoring
Configuration
Administration
Troubleshooting
Configuration › Security › Threat Defense › umbrella
click here to get your Token

Registration Token* E42E5821FF9B51F8957D71975A3AE54200262ECC

Organization ID Not Applicable

Whitelist Domains Type Domain or Regex and press Enter

☑ Enable DNS packets encryption

Umbrella Parameter Map Type parameter map name and press Enter

Cisco C9800 Umbrella cfg

OfficeExtend AP – Links and Supported Versions

- 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
- Cisco Wireless Solutions Software Compatibility Matrix: Link

AP Models	OEAP	RLAN/Aux port	9800	AireOs
91xx	Supported	N/A (AP does not have Aux Ports)	17.2	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

OfficeExtend AP – FAQ

Question: Do we need to connect to the controller locally first and then send it to the user?
Answer: You don't need to collect it locally first. If you prime it locally, you don’t have to download the code across internet which might be slow

Question: Why would customer want to use OEAP, which requires AP, vs. Cisco AnyConnect VPN with BYOD AP?
Answer: OEAP allows you to have multiple devices and do encryption on the AP and not on the device itself; it also allow you to run "home" SSIDs and accommodate those users

Question: Will OEAP solution work with external antenna AP models?
Answer: Works with both internal and External Antennas

Question: What is OEAP performance with DTLS Data encryption
Answer: It depends on the AP model – expect ~tens of Mbps on low-end models (for example AP1815T)

Question : Which protocol number is used over the WAN?
Answer: 5246 and 5247 capwap port and paylod is encrypted with DTLS

Question : Is Umbrella supported on OEAP?
Answer: Yes, Umbrella is supported on OEAP for central switched WLANs not on local SSID

OfficeExtend AP - 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 from CCO

Setup evaluation license in IOS-XE

Cisco Meraki

Teleworker

Andrej Jeleník - Systems Engineer

Cisco Czech Republic

Meraki Products

MR - Meraki Wireless (Access Points)

MX - Meraki UTM / SD-WAN

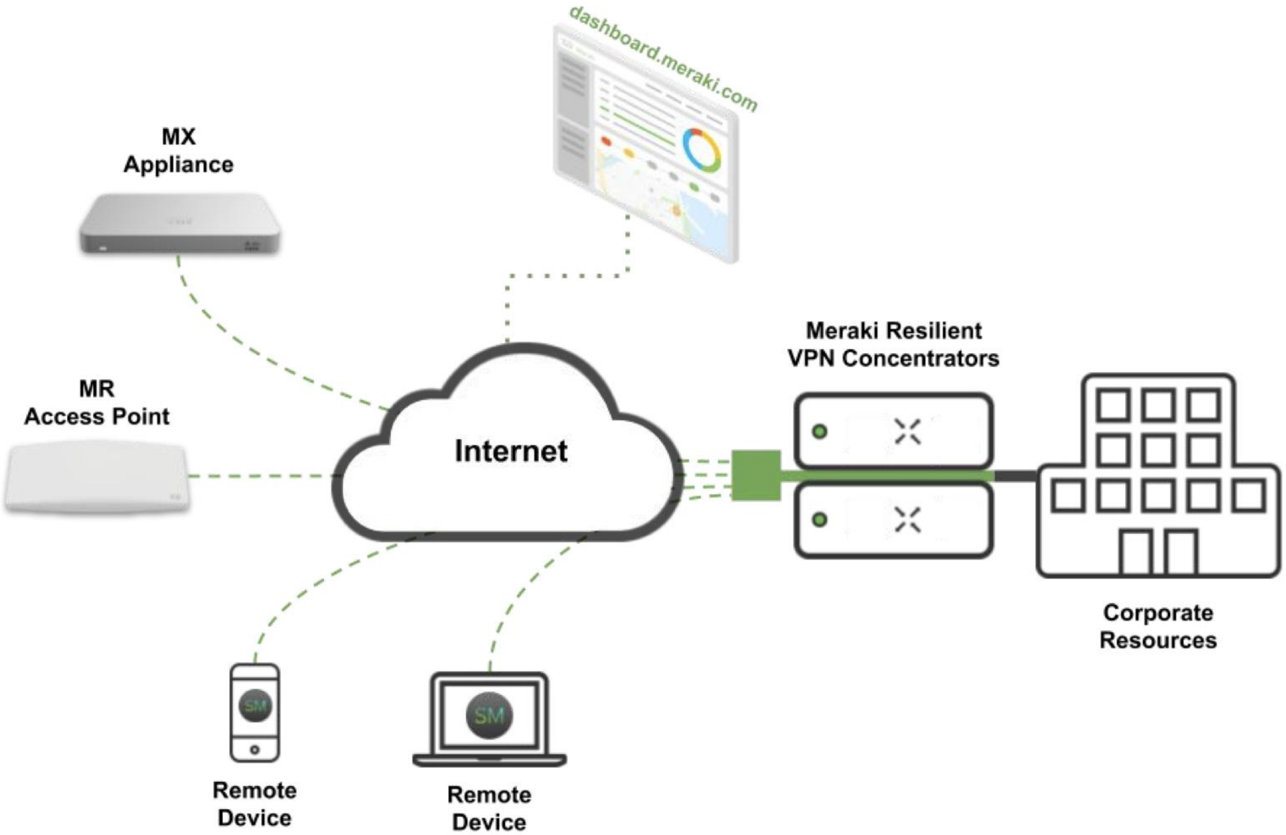
MS - Meraki Switching

MI - Meraki Insight Intelligence

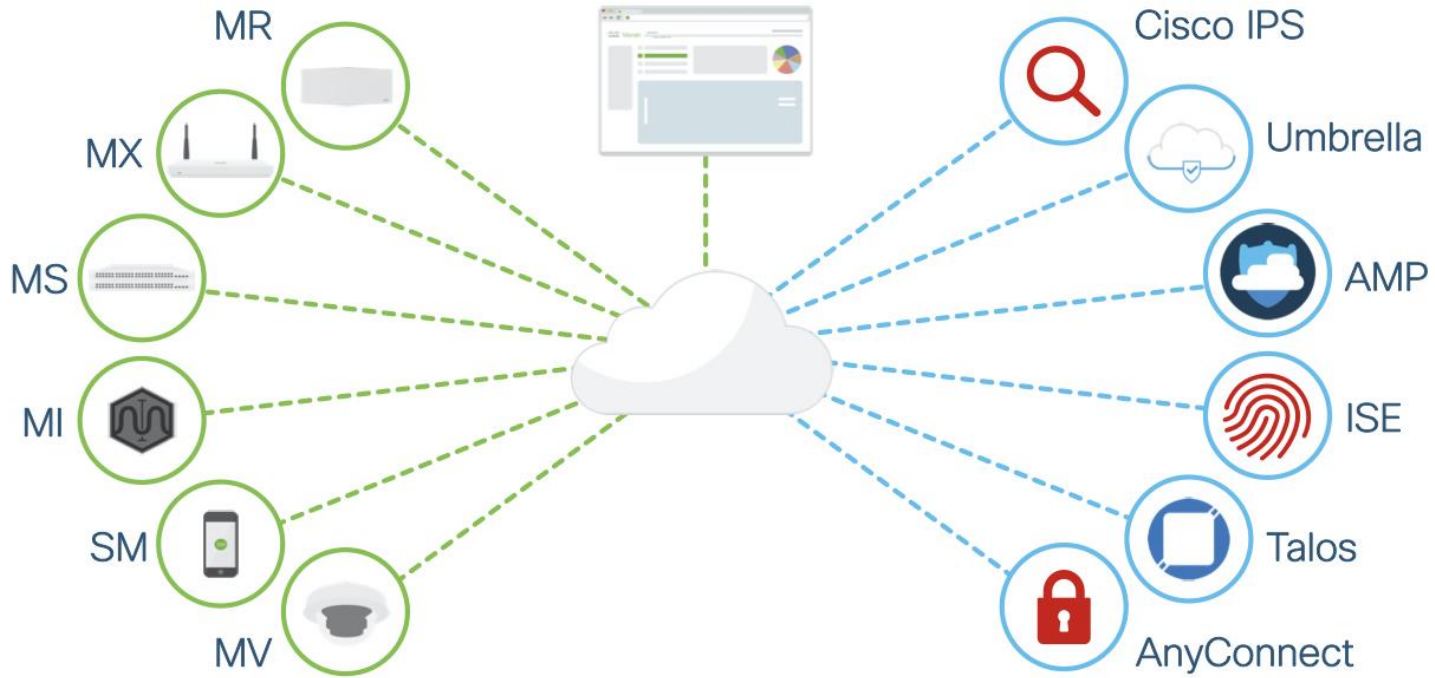
SM - Meraki Cloud based MDM

MV - Meraki Security Cameras

Solutions

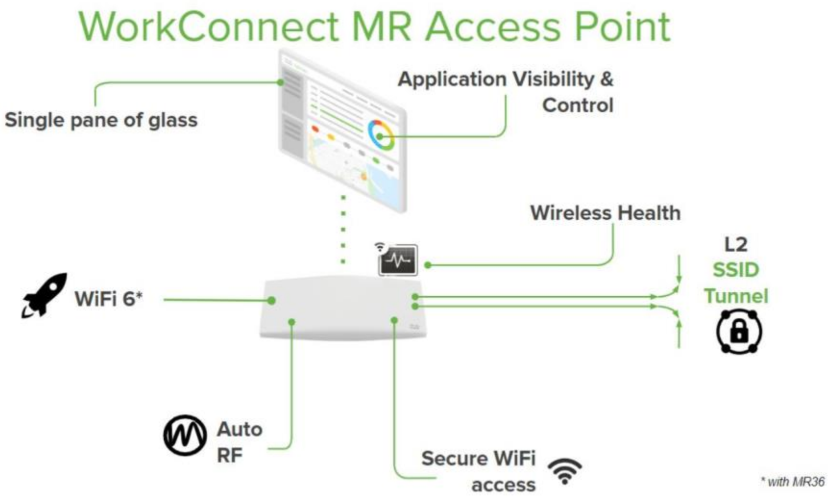

dashboard.meraki.com
MX
Appliance
MR
Access Point
Internet
Meraki Resilient
VPN Concentrators
Corporate
Resources
SM
SM
Remote
Device
Remote
Device

Meraki with Cisco



Meraki Cloud Managed Wireless

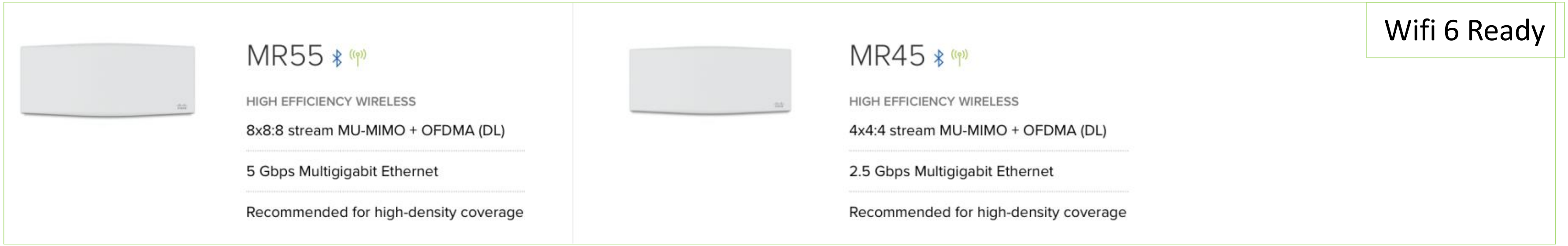
MR



- **Requirement**: MX at customer's HQ in Concentrator Mode (NAT Mode unsupported)
- Cisco Meraki access points are built from the highest grade components and carefully optimized for a seamless user experience. The outcome: faster connections, greater user capacity, more coverage, and fewer support calls.
- Positioning:
  - Customers that want to have the same SSID configurations they have on their corporate offices (same SSID name, same authentication process etc.).
  - With MR's, you can have the Meraki-Corp SSID at home. Plug and play!

Meraki MR - Access Point models

https://meraki.cisco.com/products/wireless#models



Wifi 6 Ready

MR55

HIGH EFFICIENCY WIRELESS

8x8:8 stream MU-MIMO + OFDMA (DL)

5 Gbps Multigigabit Ethernet

Recommended for high-density coverage

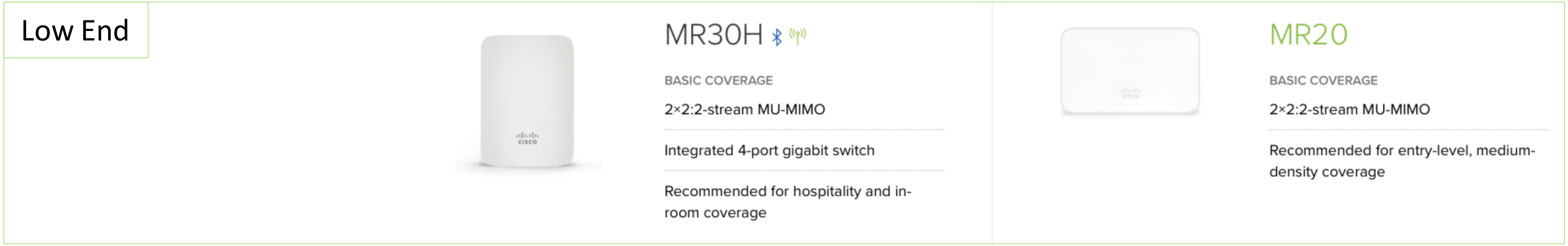
MR45

HIGH EFFICIENCY WIRELESS

4x4:4 stream MU-MIMO + OFDMA (DL)

2.5 Gbps Multigigabit Ethernet

Recommended for high-density coverage



Low End

MR30H

BASIC COVERAGE

2×2:2-stream MU-MIMO

Integrated 4-port gigabit switch

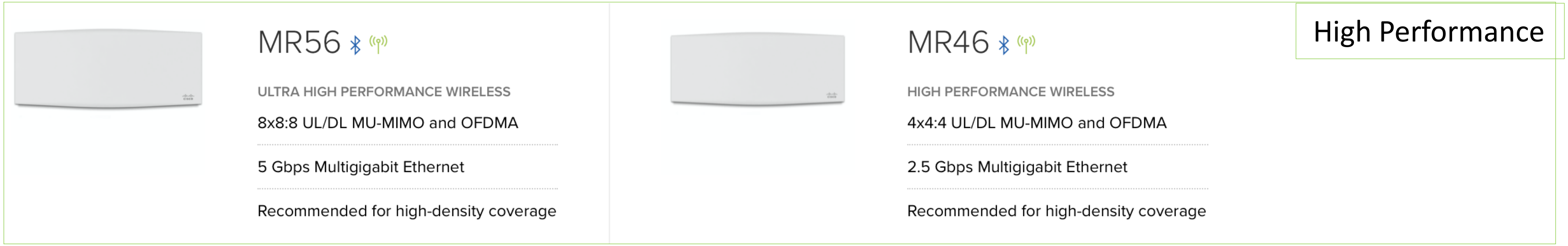
Recommended for hospitality and in-room coverage

MR20

BASIC COVERAGE

2×2:2-stream MU-MIMO

Recommended for entry-level, medium-density coverage



High Performance

MR56

ULTRA HIGH PERFORMANCE WIRELESS

8x8:8 UL/DL MU-MIMO and OFDMA

5 Gbps Multigigabit Ethernet

Recommended for high-density coverage

MR46

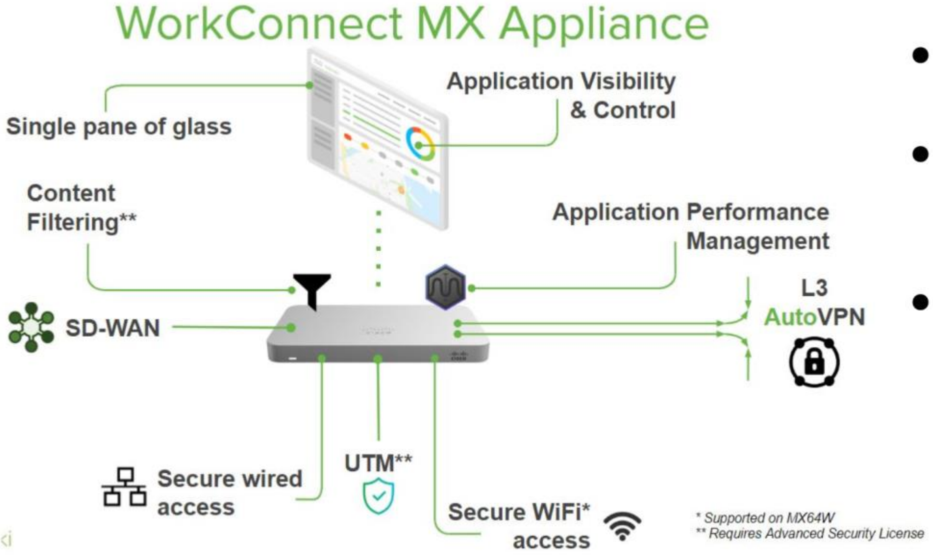
HIGH PERFORMANCE WIRELESS

4x4:4 UL/DL MU-MIMO and OFDMA

2.5 Gbps Multigigabit Ethernet

Recommended for high-density coverage

MX



WorkConnect MX Appliance

* Supported on MX64W
** Requires Advanced Security License

- Cisco Meraki Security Appliances can be remotely deployed in minutes using zero-touch cloud provisioning.
- Security settings are simple to synchronize across thousands of sites using templates.
- Auto VPN technology securely connects branches in 3 clicks, through an intuitive, web-based dashboard.
- Positioning:
  - Customers interested on remote connectivity;
  - SD-WAN to ensure application performance;
  - Content-filtering, Threat Prevention (IDS/IPS), Advanced Malware Protection (AMP) included with Adv. Security License

MX Portfolio

Teleworker

Z3

Z3C

5 users
802.11ac Wave 2 Wireless & PoE
FW throughput: 100 Mbps
CAT 3 LTE (Z3C)

Small Branch

MX64

~50 users
802.11ac Wireless*
FW throughput: 250 Mbps

MX67/68

~50 users
802.11ac **Wave 2*** & PoE
FW throughput: **450 Mbps**

MX67C/68CW

~50 users
802.11ac **Wave 2*** & PoE
FW throughput: **450 Mbps**
CAT 6 LTE

Medium Branch

MX84

~200 users
FW throughput: 500 Mbps

MX100

~500 users
FW throughput: 750 Mbps

Large Branch, Campus or Concentrator

MX250

~2,000 users
FW throughput: 4 Gbps

MX450

~10,00 users
FW throughput: 6 Gbps

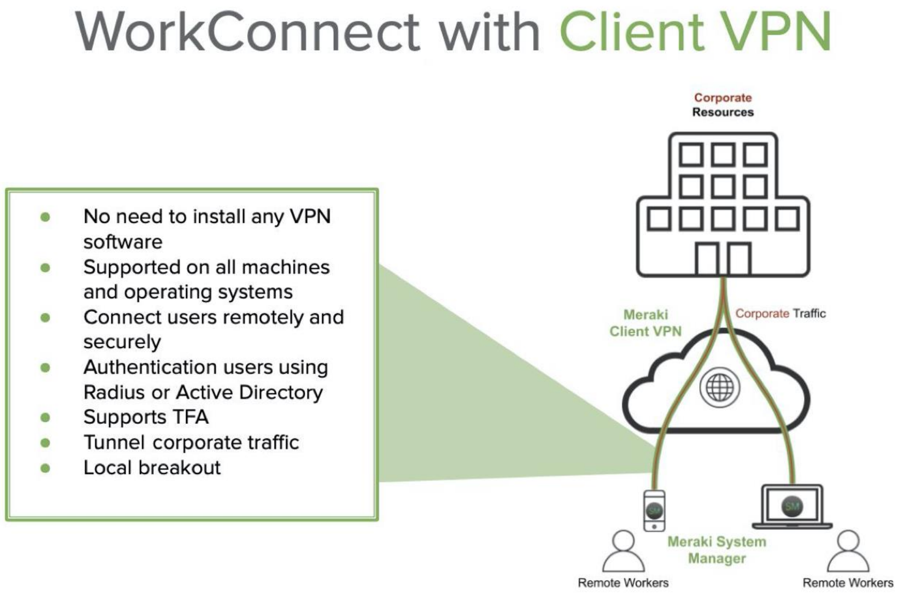
Virtual

vMX100 for AWS & Azure

FW throughput: 750 Mbps
VPN & SD-WAN features

**Available with wireless models (MX64W, MX67W, MX68W, MX68CW)*

Client VPN



WorkConnect with Client VPN

- No need to install any VPN software
- Supported on all machines and operating systems
- Connect users remotely and securely
- Authentication users using Radius or Active Directory
- Supports TFA
- Tunnel corporate traffic
- Local breakout

- **Requirement**: MX at customer's HQ.
- Customers that don't want to ship equipment to the remote worker's address.
- Full-tunnel only
- Pros:
  - Included with MX license;
  - No hardware at remote worker location;
- Cons:
  - Roll-out can be cumbersome due to amount of distributed endpoints and different operating systems.
  - Systems Manager customers can leverage SM to overcome this issue, by pushing the VPN profile. Better together!

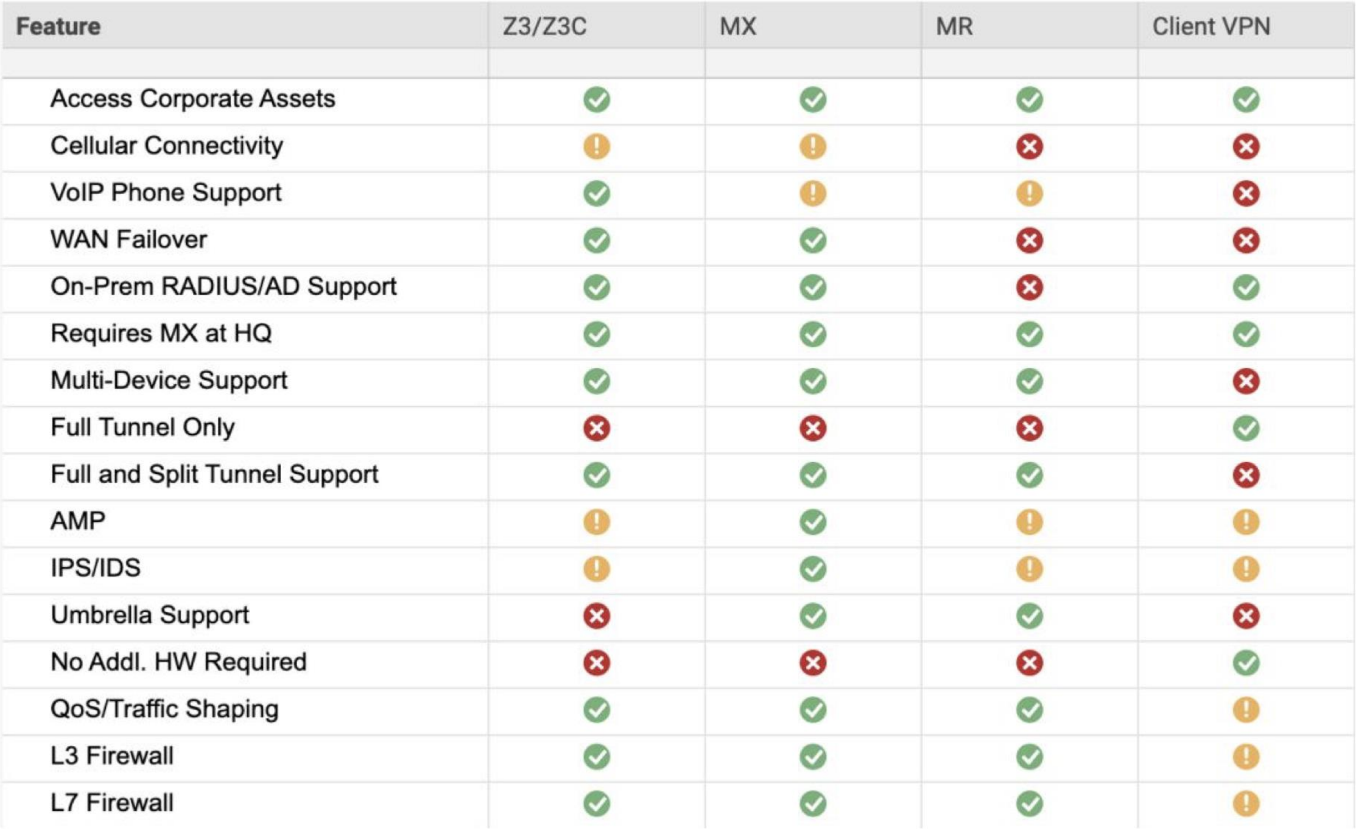
Z3

- **Requirement**: MX at customer's HQ
- The Cisco Meraki Z3 is a teleworking-focused appliance suited for home office deployments. The Z3 includes integrated wireless, cellular failover (on Z3C), and PoE for devices like VoIP phones.
- Positioning:
  - Customers have existing MX at HQ
  - Each remote user will have IP phone
  - Cellular failover is critical
  - Customer wants to use wireless devices in addition to IP phone
  - Want to connect multiple devices
  - VPN throughput limited to 50Mbps
- Recommendations: larger MX at HQ -- MX250 or MX450
- Notes: use of IPS/IDS and AMP is limited to “Full Tunnel” when setting up Z3, meaning that the MX @ HQ will provide these services. The Z3 does not provide local IPS/IDS or AMP

Models

	Z3 	Z3C
Recommended use cases	Teleworker with VoIP or PoE, IoT, and M2M	Teleworker with VoIP or PoE, IoT, and M2M
Recommended clients	Up to 5 devices	Up to 5 devices
Stateful Firewall Throughput	100 Mbps	100 Mbps
Maximum VPN Throughput	50 Mbps	50 Mbps
WAN Interfaces	1 x GbE RJ45 1 x USB (cellular failover[1])	1 x GbE RJ45 1 x Integrated CAT 3 LTE Cellular Modem (cellular failover) 1 x USB (cellular failover[1])
LAN Interfaces	4 x GbE	4 x GbE
PoE	1 x PoE enabled port (802.3af, 15.5W)	1 x PoE enabled port (802.3af, 15.5W)

Security features comparison



Feature	Z3/Z3C	MX	MR	Client VPN
Access Corporate Assets	✓	✓	✓	✓
Cellular Connectivity	!	!	✗	✗
VoIP Phone Support	✓	!	!	✗
WAN Failover	✓	✓	✗	✗
On-Prem RADIUS/AD Support	✓	✓	✗	✓
Requires MX at HQ	✓	✓	✓	✓
Multi-Device Support	✓	✓	✓	✗
Full Tunnel Only	✗	✗	✗	✓
Full and Split Tunnel Support	✓	✓	✓	✗
AMP	!	✓	!	!
IPS/IDS	!	✓	!	!
Umbrella Support	✗	✓	✓	✗
No Addl. HW Required	✗	✗	✗	✓
QoS/Traffic Shaping	✓	✓	✓	!
L3 Firewall	✓	✓	✓	!
L7 Firewall	✓	✓	✓	!

Cisco Meraki Teleworker Solutions

MX

- All-in-one security appliance
- Cellular backup options
- Wireless models available

Z3

- Designed for tabletop teleworker
- PoE+ port for phones
- 802.1X port security

MR

- **Requirement**: Hub MX in concentrator mode
- No local security

CLIENT VPN

- Can be deployed manually or using **Meraki Systems Manager (MDM)**
- Direct VPN for mobile workers

HOW TO SIZE YOUR HUB

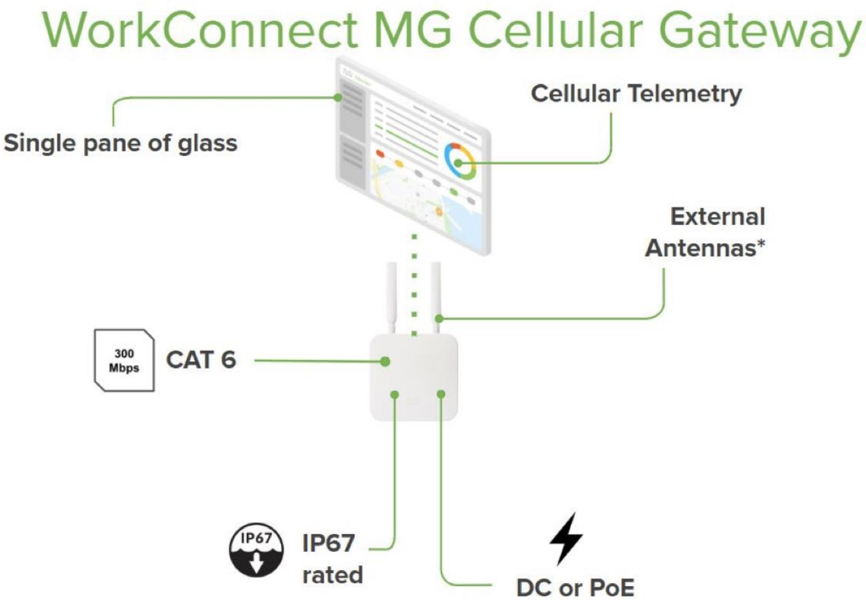
	MX84	MX100	MX250
Clients	200	500	2,000
T.	320 Mb	650 Mb	2 Gb
VPN Tunnels	100	250	3,000
VPN T.	250 Mb	500 Mb	1 Gb

Ask us how *Meraki Insight (**MI**)* can help monitor application, VoIP, and WAN performance.

Need cellular? The *Meraki Gateway (**MG**)* has you covered!

meraki.cisco.com/products

MG



- Cisco Meraki MG Cellular Gateways seamlessly transpose a wireless cellular signal to wired Ethernet for primary or failover connectivity.
- **Requirement**: The customer must have an existing edge device (e.g. MX).
- Positioning:
  - Locations without a wired Internet Service Provider;
  - The cellular signal (coverage) is not strong enough (e.g. basements, rural areas etc.)

The MG21 and MG21E

- Integrated CAT6 modem with up to 300Mbps
- DC / PoE power in
- 2x Ethernet ports for HA
- Nano SIM card slot
- IP67 rated
- Multi-surface mounting bracket (wall, ceiling, and tabletop)
- LTE connectivity out-of-the-box
- External antennas*
  - Dipole included
  - Patch available as an accessory
- API support

Shrnutí, Q&A

Network Connectivity – Teleworker Options

VPN remote Access

Platform Support:

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

Benefits

- Highly secure access across popular PC and mobile devices
- Consistent user experience
- Intelligent, dependable, and always-on connectivity

OEAP Cisco Controller On-Prem Solution

Platform Support (Option 1):

- WLC
- AP3500 and newer

Platform Support (Option 2)

- WLC
- OEAP600, AP1810, AP1815T

Benefits

- Repurpose existing AP's
- Remote Ethernet available with Option 2

Meraki Teleworker Cloud Based Solution

Platform Support:

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

Benefits:

- 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

Platform Support

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

Benefits:

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

Teleworker best practices to share

1 **It's easy to work a 16-hour day from home – so don't!**
Schedule your day. Establish some structure by knowing when you want to start and finish. It's easy to keep working or return to work late in the evening, as you have everything you need right there. But it's healthier to maintain set work hours.

2 **Avoid bringing work into the family environment.**
If you have deadlines, escalations and other intense situations, be aware of the impact it can have on your family members. They may see or overhear you handling difficult issues and, as a result, they might internalize that stress or worry.

3 **Manage your home time carefully.**
Staying at home makes it easier to engage in family time. But it's important to manage it so you don't get burned out by being home all day (and night).

4 **Be respectful and patient of other team members' home office environments.**
Some folks will have home offices that are well established, with a professional look and configuration. Others, who are new to working from home, may not. Some may struggle to carve out a workspace in their homes or need to share that work environment with a spouse or significant other, which can cause background noise and distractions. If you hear a dog bark or a baby cry, please be patient with them.

5 **Structure your day with breaks.** Walk the block, smell the roses, or do a call from the garden. If the walls start closing in, change your scenery:

- Schedule lunch and eat it away from your office.
- Don't forget to exercise. it's a great way to clear out the mental cobwebs and re-energize your body.
- Schedule quick 15-minute calls with colleagues or friends. Talking to them not only refreshes your brain but is great therapy

Nadcházející webináře

07.05.2020 Cisco technologie pro řešení podnikových WAN sítí

Rychlý technologický vývoj se nevyhýbá ani oblasti podnikových WAN sítí. V tomto webináři si představíme nové platformy Cisco směrovačů pro výstavbu podnikových WAN sítí, poskytneme celkový přehled aktuálního produktového portfolia Cisco směrovačů a rovněž budou diskutovány principy DNA licenčního modelu pro Cisco WAN sítě.

Přednášející: Miroslav Brzek

05.05.2020 Přehled nových funkcí a vlastností nástrojů pro vzdálenou spolupráci

Ani aktuální nestandardní situace nezastavila inovace v oblasti týmové a vzdálené spolupráce. V tomto webináři ze série Tech Club Vás seznámíme s přehledem nových funkcí a vlastností, ale také s novinkami, které se teprve připravují. Zaměříme se především na software klienty a jejich rozhraní. Kromě toho také projdeme unified aplikace, embedované webové aplikace a streaming na sociální sítě, např. na YouTube či na Facebook.

Přednášející: Ivan Sýkora

Více informací na webu Cisco Tech Club Webinářů

CISCO