Teleworker Virtual Series

How to quickly deploy remote work solutions

Teleworkers: We are in this together

Teleworker thoughts/suggestions

Three principles to keep in mind through these challenging times:

✓ Individually take care of yourself, and your families – stay safe, stay healthy and breathe!

✓ Take care of each other – check in with your colleagues and employees so folks know they are not alone

✓ Take care of your customers – whatever it takes. Be confident your teams will do the right thing to get your customers what they need in these ever-changing times.

Teleworker best practices to share

1 It's easy to work a 16-hour day from home - so don’t!

2 Avoid bringing work into the family environment.

3 Manage your home time carefully.

4 Be respectful and patient of other team members' home office environments.

5 Structure your day with breaks.

Deployment options

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

Verify identity of users

Policy Control and Management

ISE

FMC

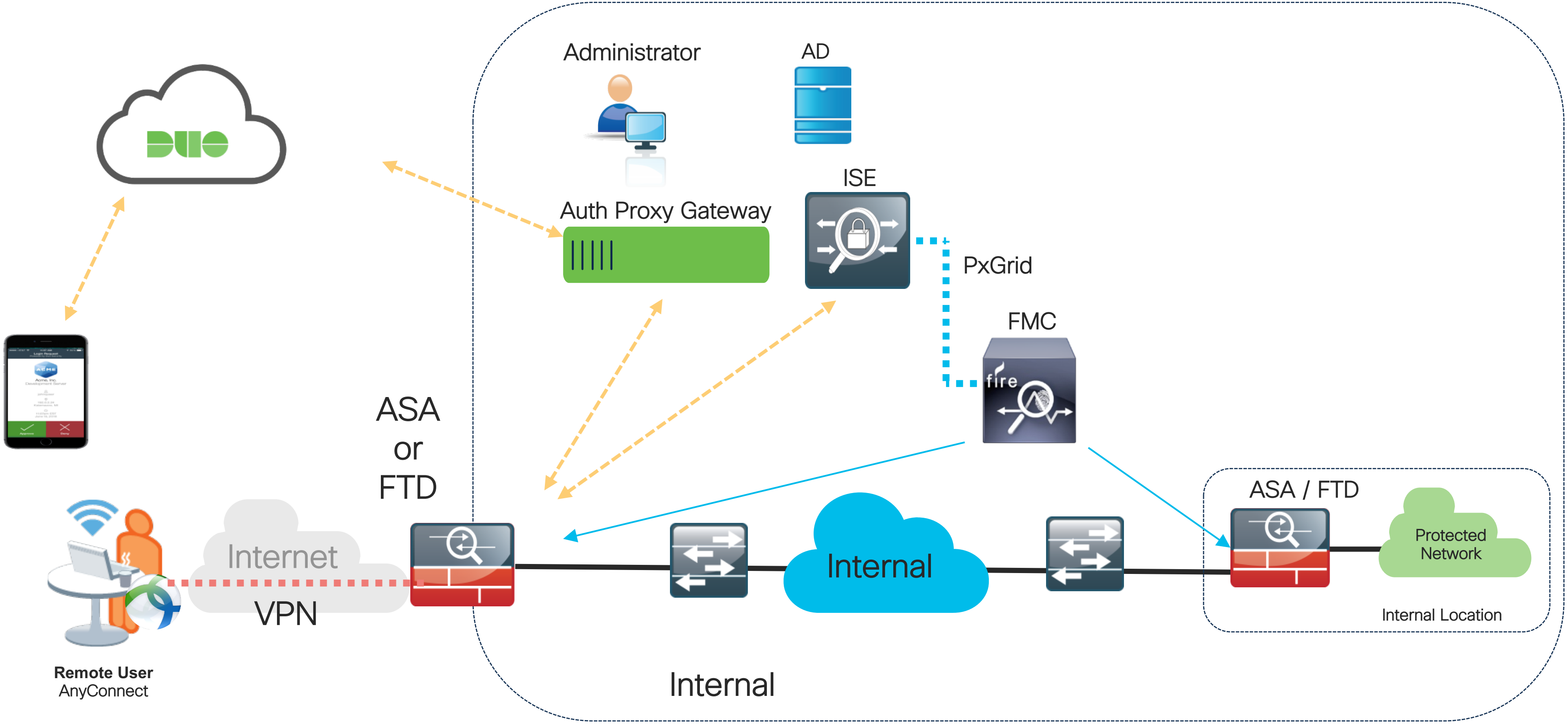
Ensure trustworthiness of devices

Infrastructure

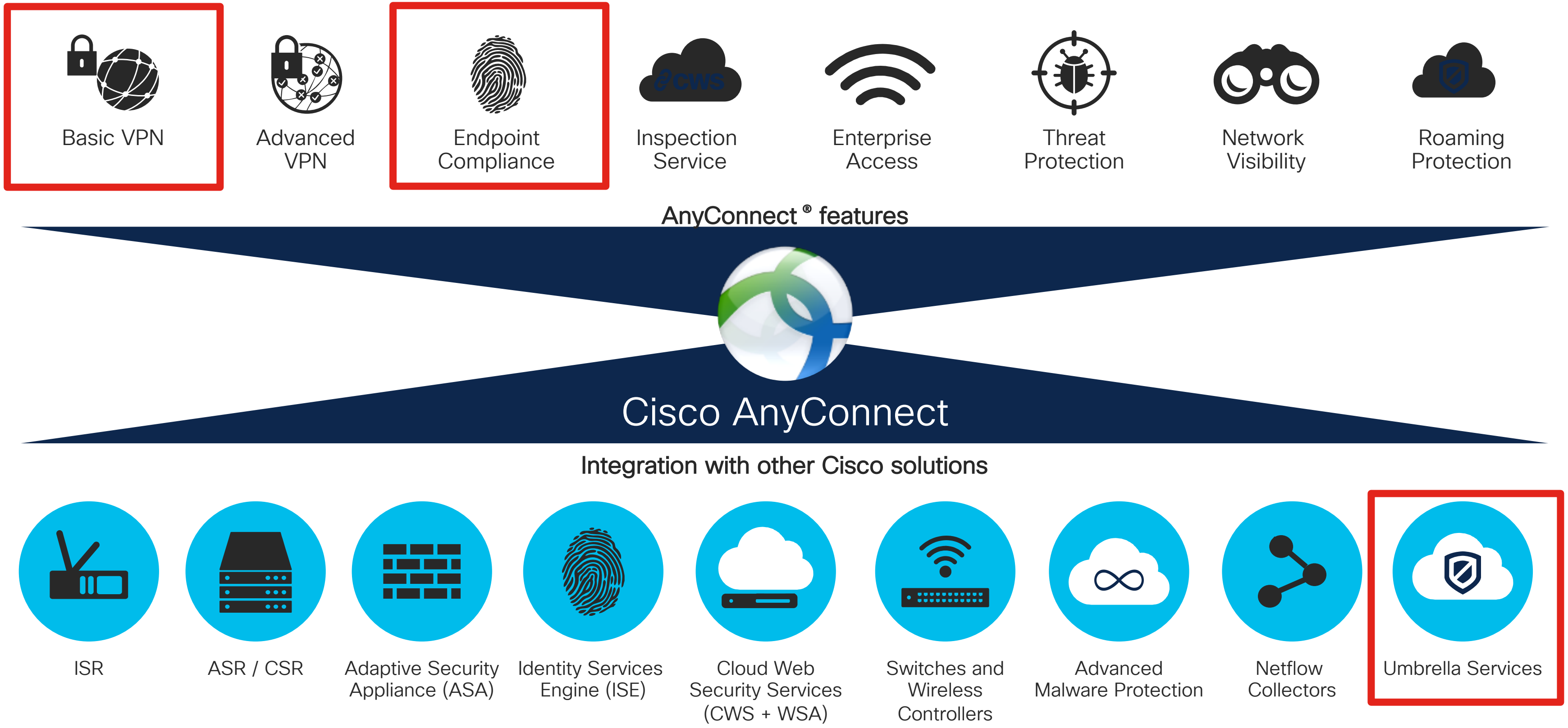
ASA / FTD

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

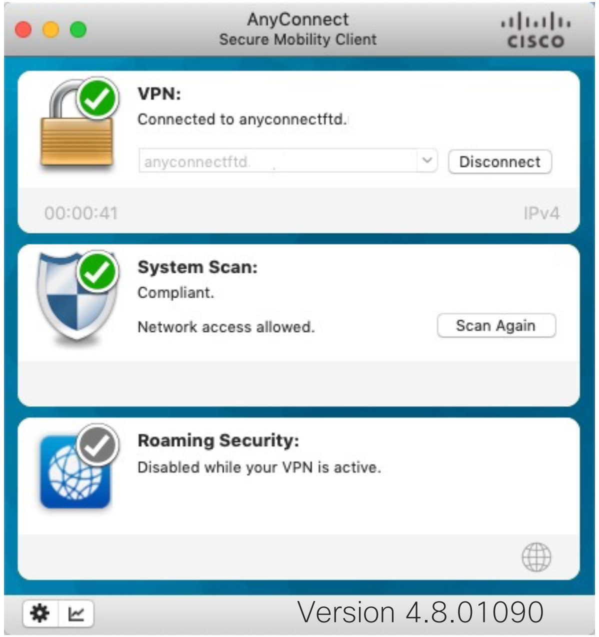
Advanced Malware Protection

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.

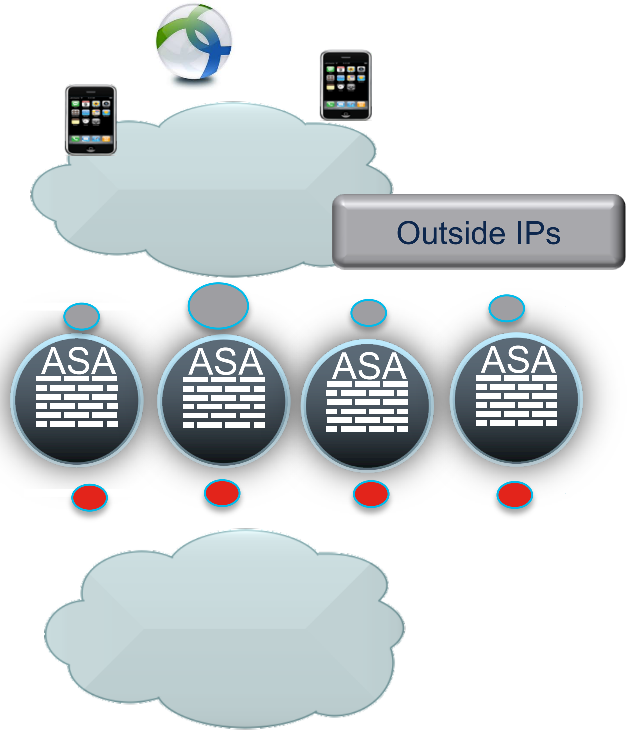
Roaming Security:
Disabled while your VPN is active.

Version 4.8.01090

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

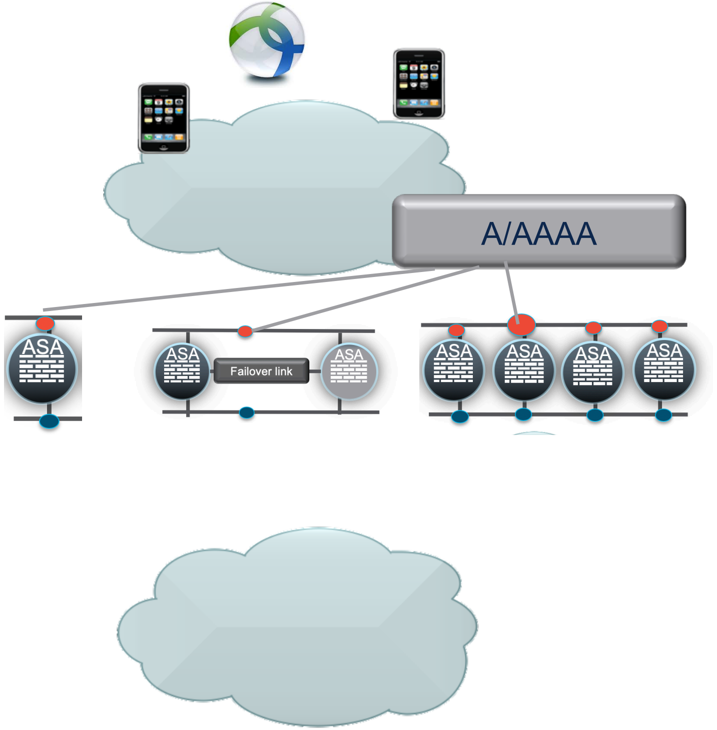
VPN Load Balancing (Native)

- 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)



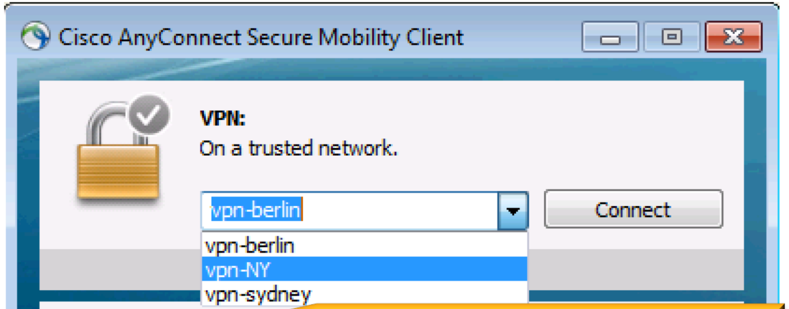
Quick and Ugly Scaling : VPN Load Balancing (DNS)

- 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



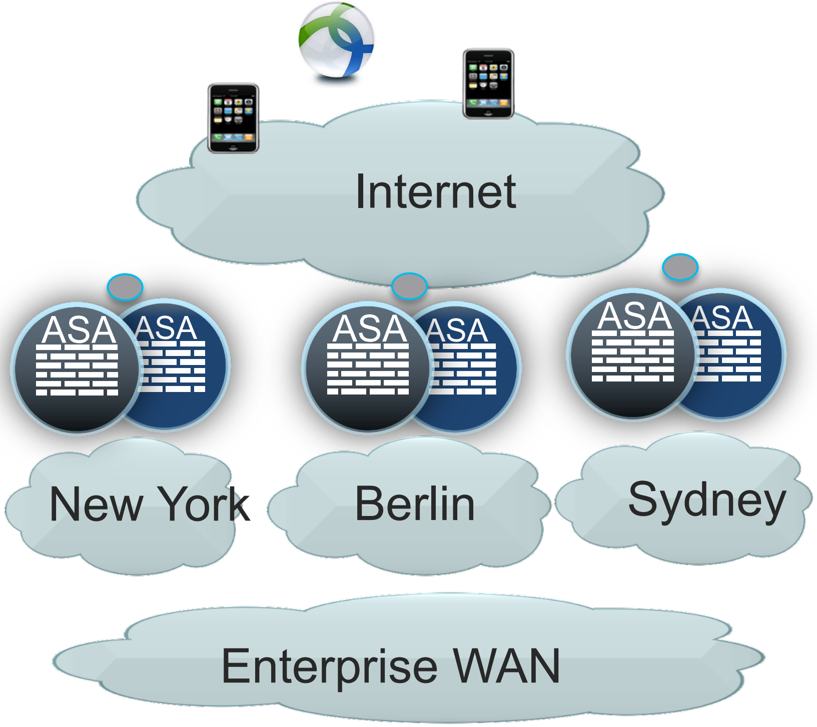
Cisco AnyConnect Secure Mobility Client

VPN:

On a trusted network.

vpn-berlin

AnyConnect Client Profiles (described later)



Office Extend Access Point (OEAP) Solution

Remote Worker Use Case

- Any Cisco Aironet Access Point can function as an ‘Office Extend AP’ (OEAP) – this means if there is inventory of any Aironet AP’s they can be leveraged to provide secure teleworker solution for employees.

- Any controller (virtual or physical) can be used for creating the secure tunnel or a dedicated controller can be set up in DMZ.

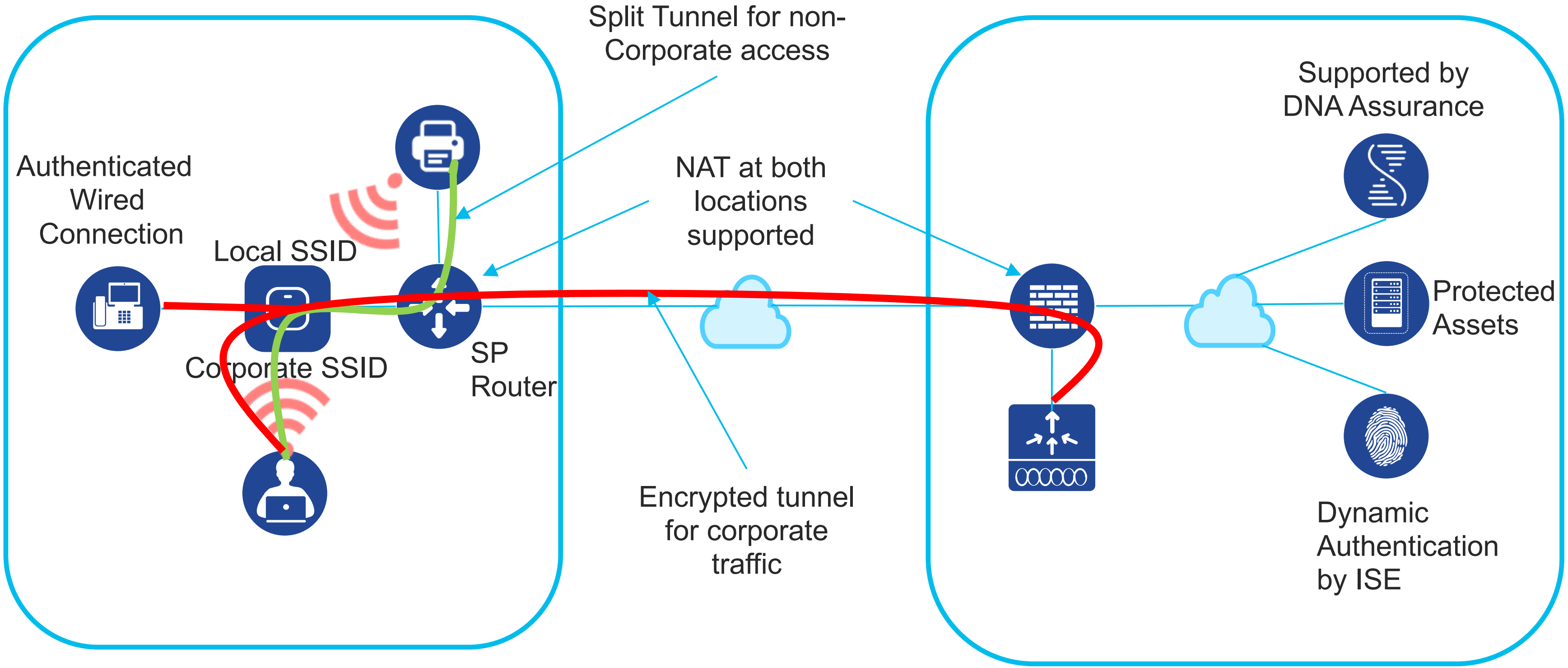
- With OEAP, an employee at home will have access to the Corporate SSID and the corporate network, without having to set up a VPN or have any technical knowledge.

OfficeExtend 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

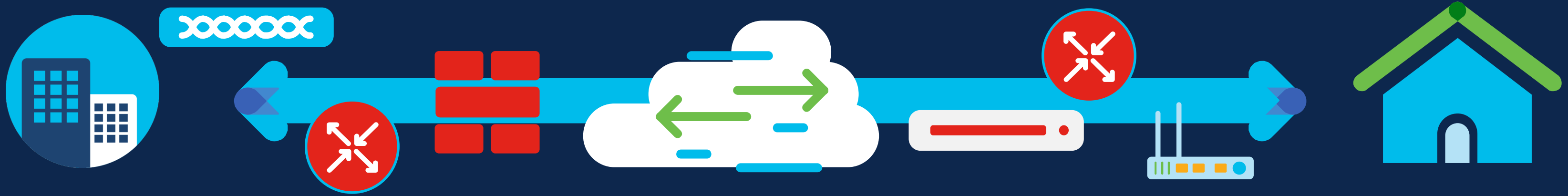
OfficeExtend AP Operation


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

Secure remote work / micro office

You probably have what you need already!

3 Pieces of the Puzzle – What is needed?



Office Environment

Home Environment

1-Any WLC - Physical or Virtual:

(w. sufficient AP licenses)

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

* Can be any AireOS Controller WLC 3504/5520/8540 or even older 5508/8510 running AireOS 8.5 or later

▪Catalyst 9800 appliance or Catalyst 9800-CL in private cloud (OEAP mode supported)

▪ note: AireOS vWLC does not support OEAP

2-Internet Connection

→ Office Internet Connection (where WLC is deployed)

Home Internet Connection →

3-Any Aironet or Catalyst AP:

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

▪ 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

Secure remote work / micro office

Getting Started with OEAP Configuration

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

Reference OEAP CVD Link

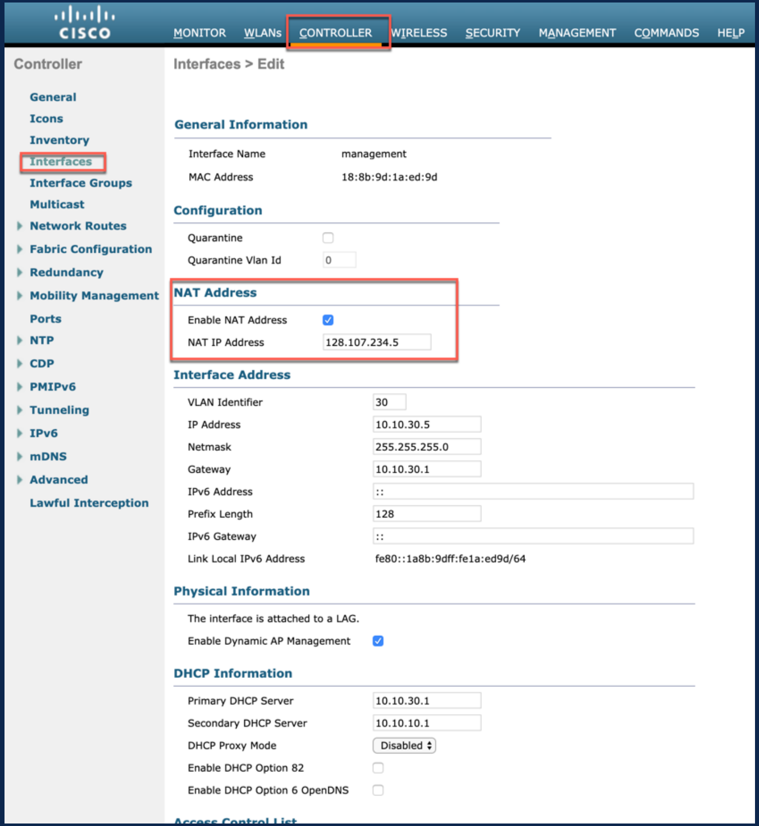
Secure remote work / micro office

Configure WLC

Step 1: Set up either physical or virtual 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 WLC Guided Configuration Walk-through



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
IP Address	10.10.30.5
Netmask	255.255.255.0
Gateway	10.10.30.1
IPv6 Address	::
Prefix Length	128
IPv6 Gateway	::
Link Local IPv6 Address	fe80::1a8b:9dff:fe1a:ed9d/64

Physical Information

The interface is attached to a LAG.

Enable Dynamic AP Management	☑

DHCP Information

Primary DHCP Server	10.10.30.1
Secondary DHCP Server	10.10.10.1
DHCP Proxy Mode	Disabled
Enable DHCP Option 82	□
Enable DHCP Option 6 OpenDNS	□

Access Control List

Secure remote work / micro office

Prime AP: Configuring AP mode to OEAP

Step 1: Have all AP's join a WLC to start so that it's connected and has the 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

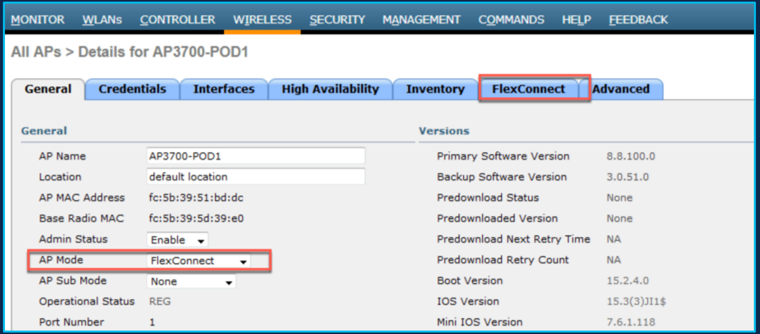
Step 4: Then go to **FlexConnect>OfficeExtend AP** enable OfficeExtend AP by checking the box

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

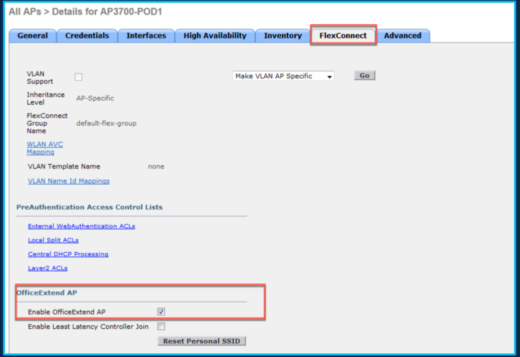
Note: verify which AP's are being sent to the employees. Most AP's use an AC adapter, some AP's might require a power injector or POE to power up the APs

Watch a Prime AP Guided Configuration Walk-through



All APs > Details for AP3700-POD1

General		Versions	
AP Name	AP3700-POD1	Primary Software Version	8.8.100.0
Location	default location	Backup Software Version	3.0.51.0
AP MAC Address	fc:5b:39:51:bd:dc	Predownload Status	None
Base Radio MAC	fc:5b:39:5d:39:e0	Predownloaded Version	None
Admin Status	Enable	Predownload Next Retry Time	NA
AP Mode	FlexConnect	Predownload Retry Count	NA
AP Sub Mode	None	Boot Version	15.2.4.0
Operational Status	REG	IOS Version	15.3(3)JI1$
Port Number	1	Mini IOS Version	7.6.1.118



All APs > Details for AP3700-POD1

VLAN Support □ Make VLAN AP Specific

Inheritance Level AP-Specific

FlexConnect Group Name default-flex-group

WLAN AVC Mapping

VLAN Template Name none

VLAN Name Id Mappings

PreAuthentication Access Control Lists

External WebAuthentication ACLs

Local Split ACLs

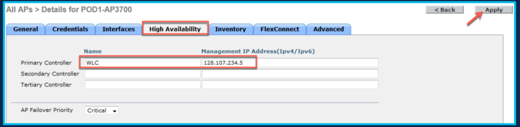
Central DHCP Processing

Layer2 ACLs

OfficeExtend AP

Enable OfficeExtend AP ☑

Enable Least Latency Controller Join □



All APs > Details for POD1-AP3700

	Name	Management IP Address(Ipv4/Ipv6)
Primary Controller	WLC	128.107.234.5
Secondary Controller		
Tertiary Controller		

AP Failover Priority Critical

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

1815i, 1840i, 1852i/E Access points

Customers can leverage the Buy one 1815 access point, get one free offer*

Specialists

*Available in select markets (excluding US and Canada)

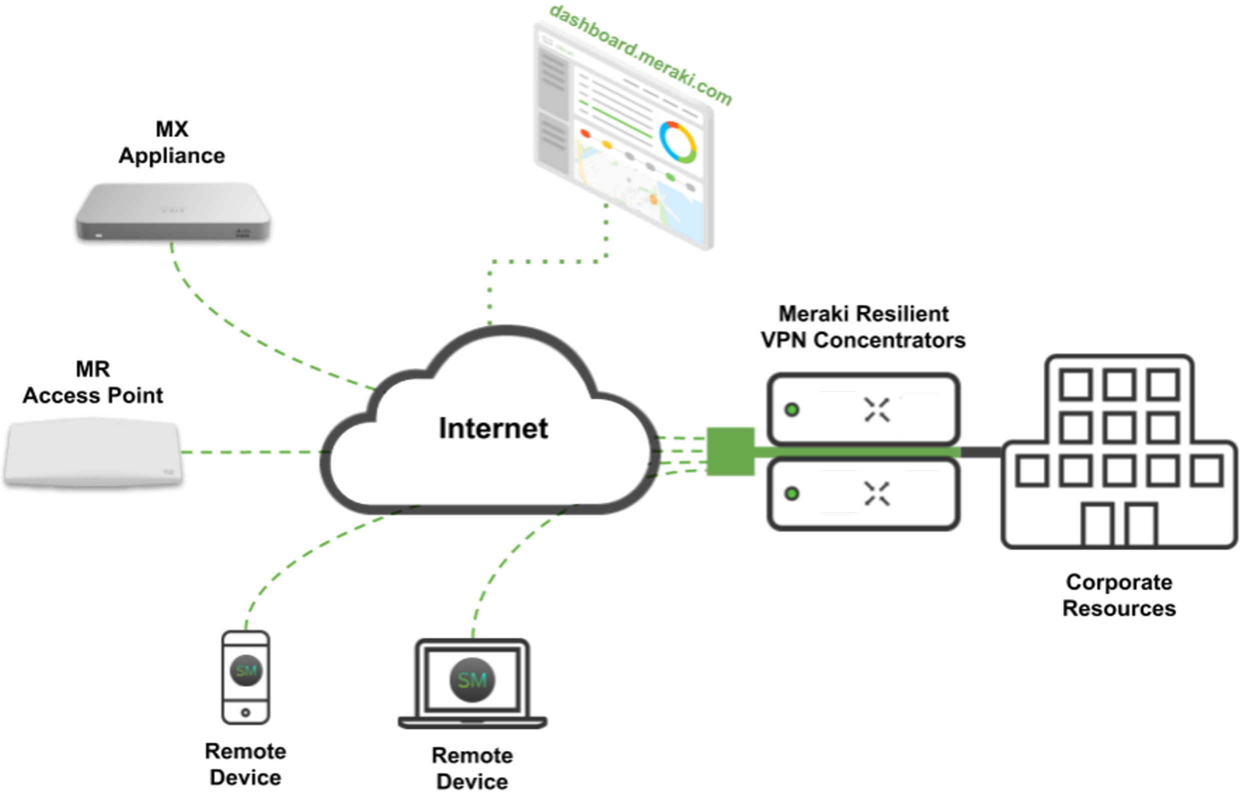
Secure remote work / micro office

Useful Links

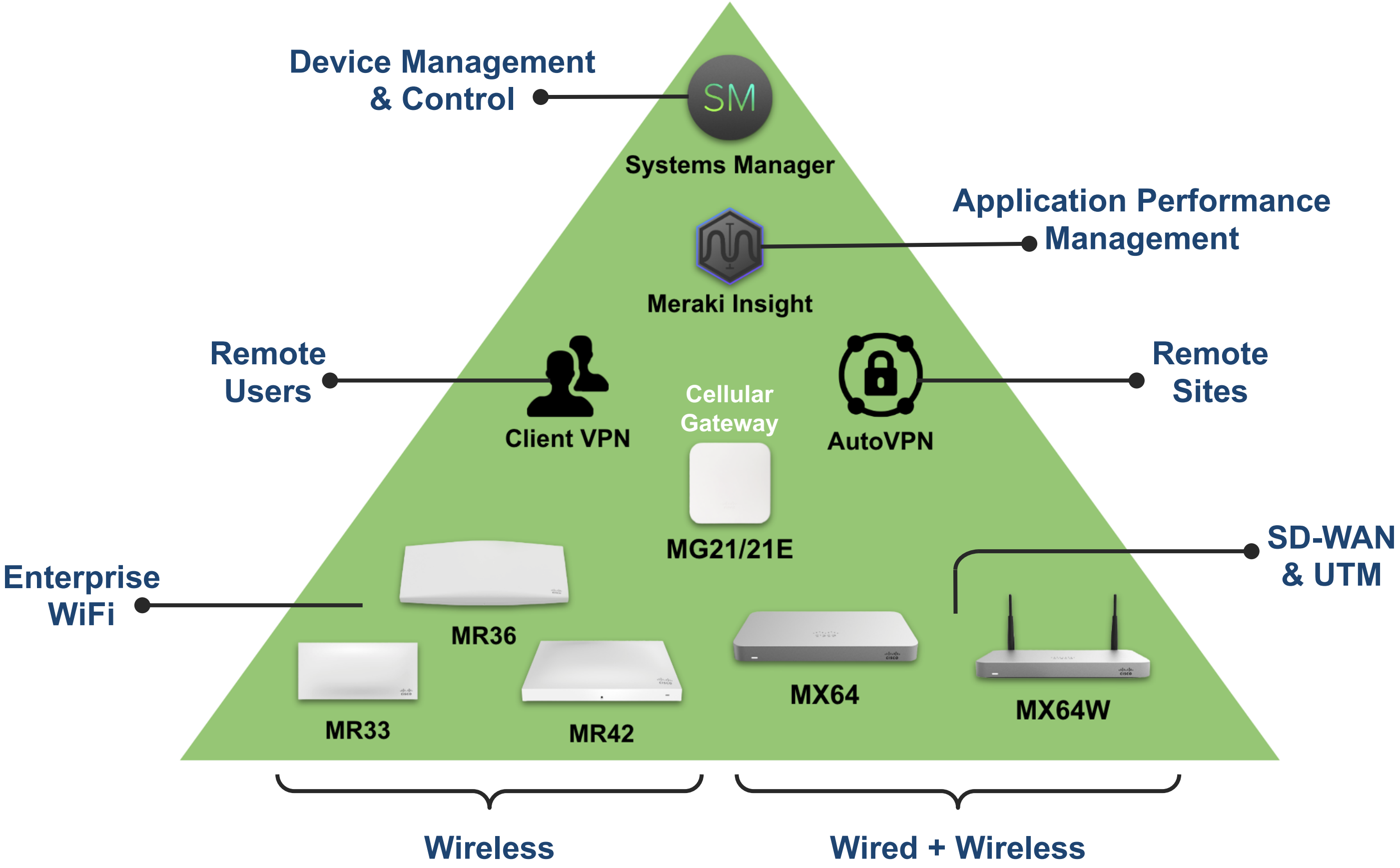
- Customers can leverage the Buy one 1815 access point, get one free offer
- OEAP Configuration Guide (AireOS 8.5): Link
- OEAP Configuration Guide (AireOS 8.8): Link
- OEAP WLC guided configuration video
- OEAP Cisco Validated Design: Link
- 1815t Deployment Guide: Link
- Cisco Wireless Solutions Software Compatibility Matrix: Link
- AP 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

Meraki Teleworker

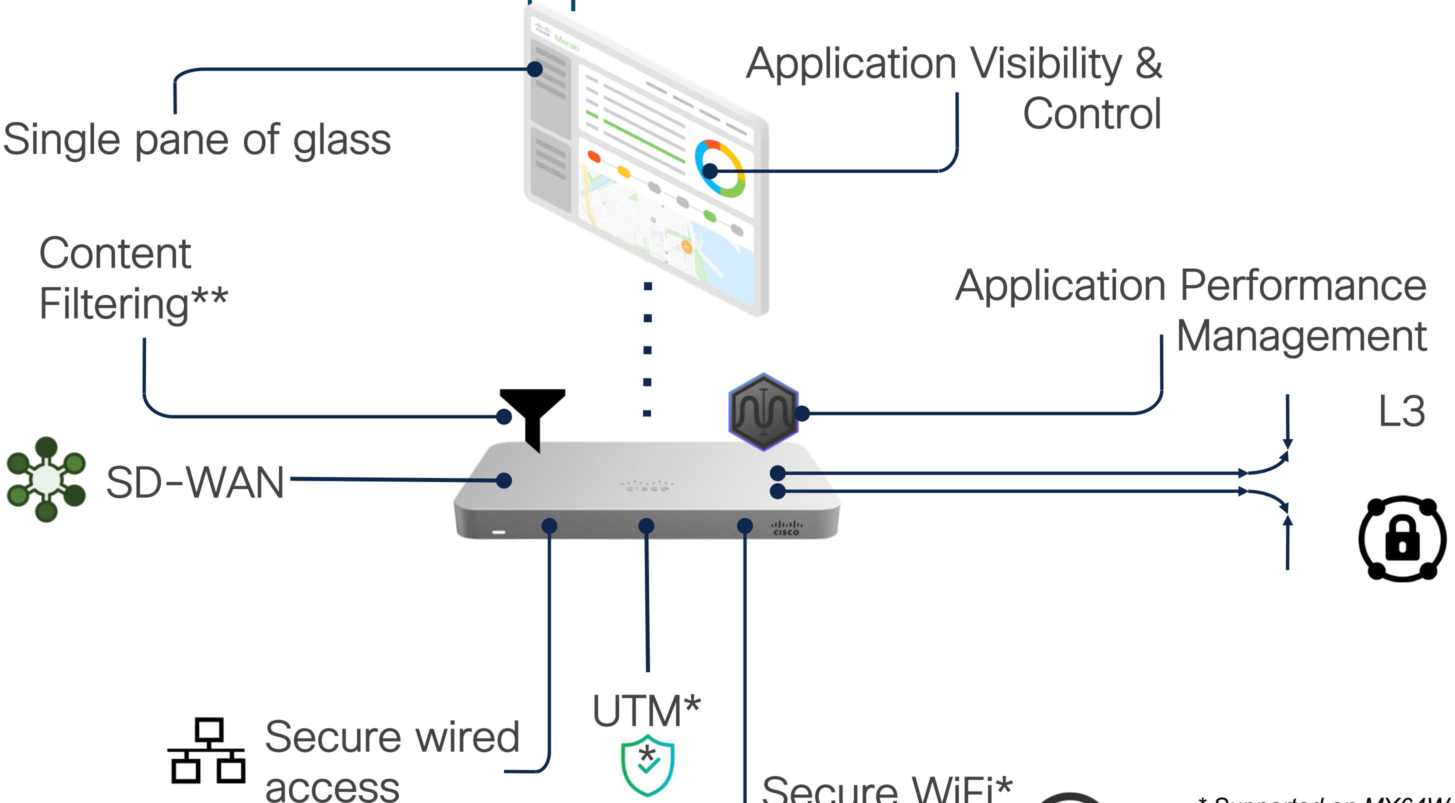
WorkConnect Solution



A solution for all use cases



WorkConnect MX Appliance



Single pane of glass

Application Visibility & Control

Content Filtering**

Application Performance Management

L3

SD-WAN

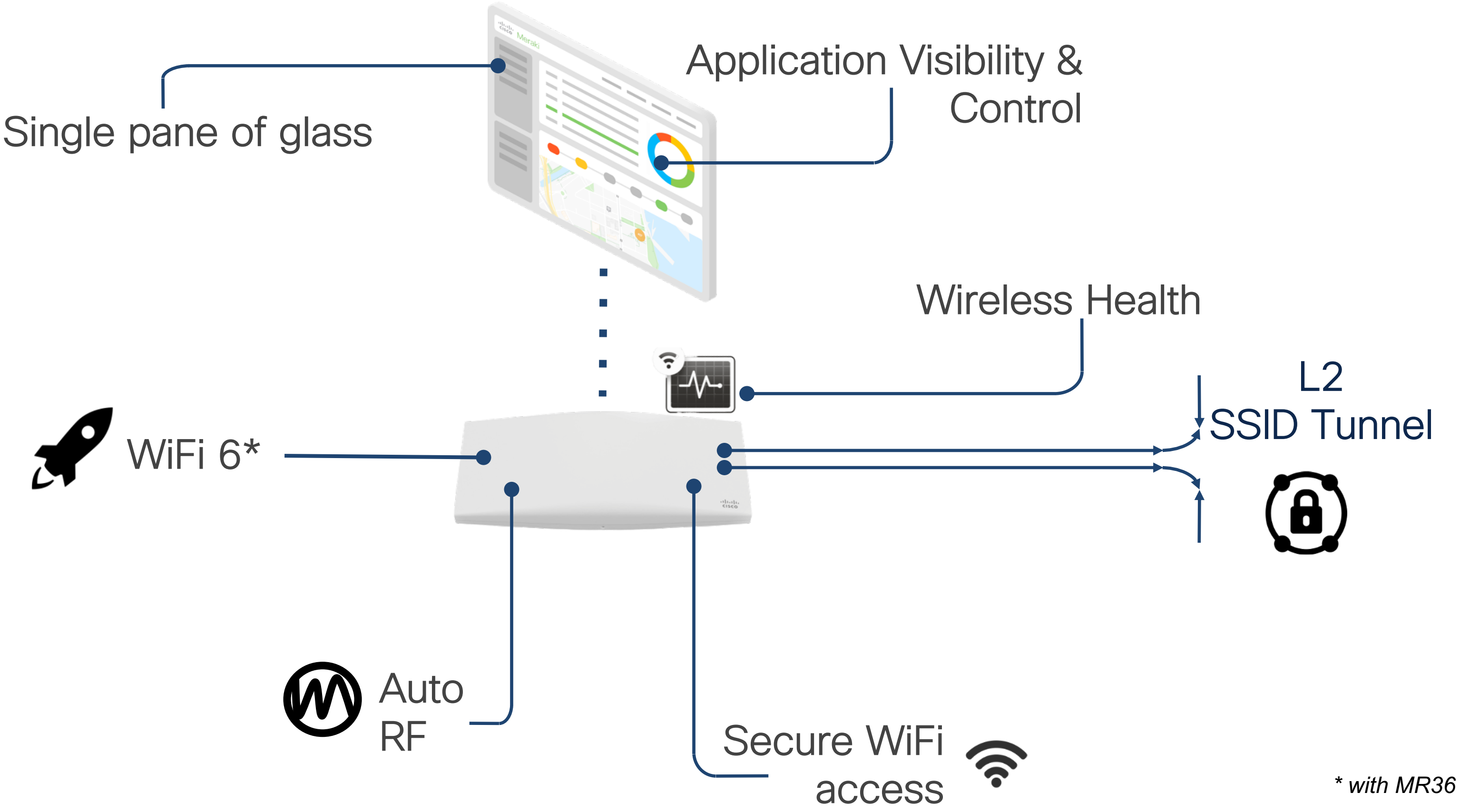
Secure wired access

UTM*

Secure WiFi* access

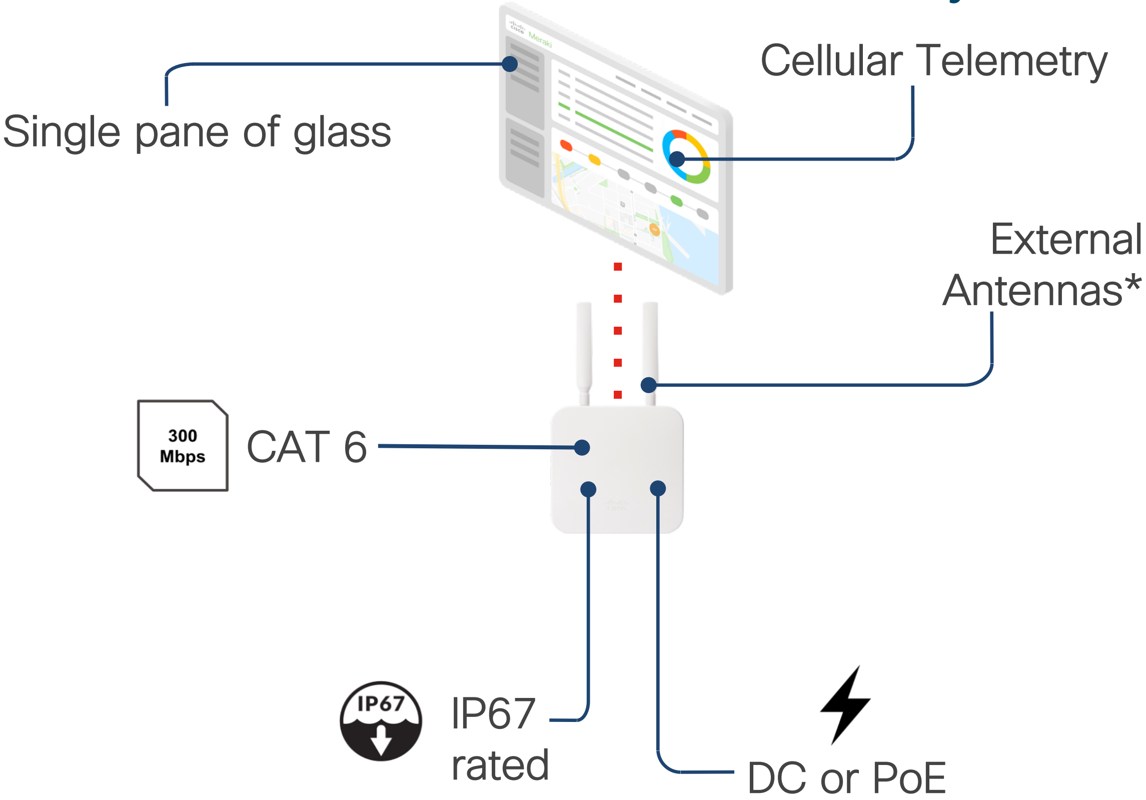
** Supported on MX64W*
*** Requires Advanced Security License*

WorkConnect MR Access Point



* with MR36

WorkConnect MG Cellular Gateway



Single pane of glass

Cellular Telemetry

External Antennas*

300 Mbps

CAT 6

IP67 rated

DC or PoE

* 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

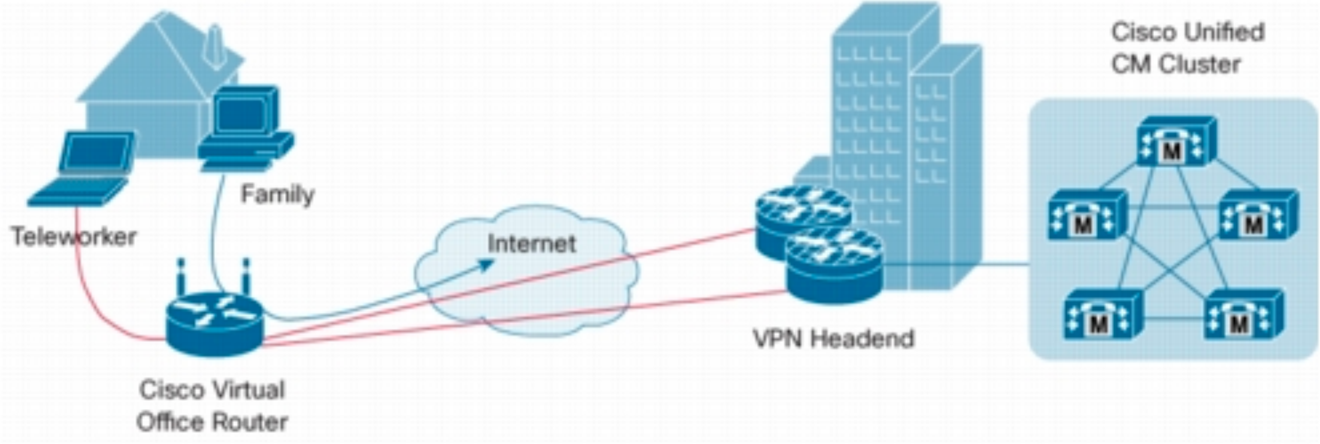
❑ Site to Site VPN
❑ Full/Split tunneling
❑ VPN Firewall
❑ VPN Translation
❑ Include/exclude local networks
❑ Multiple head-ends for resiliency
❑ Zero touch provisioning

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

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.

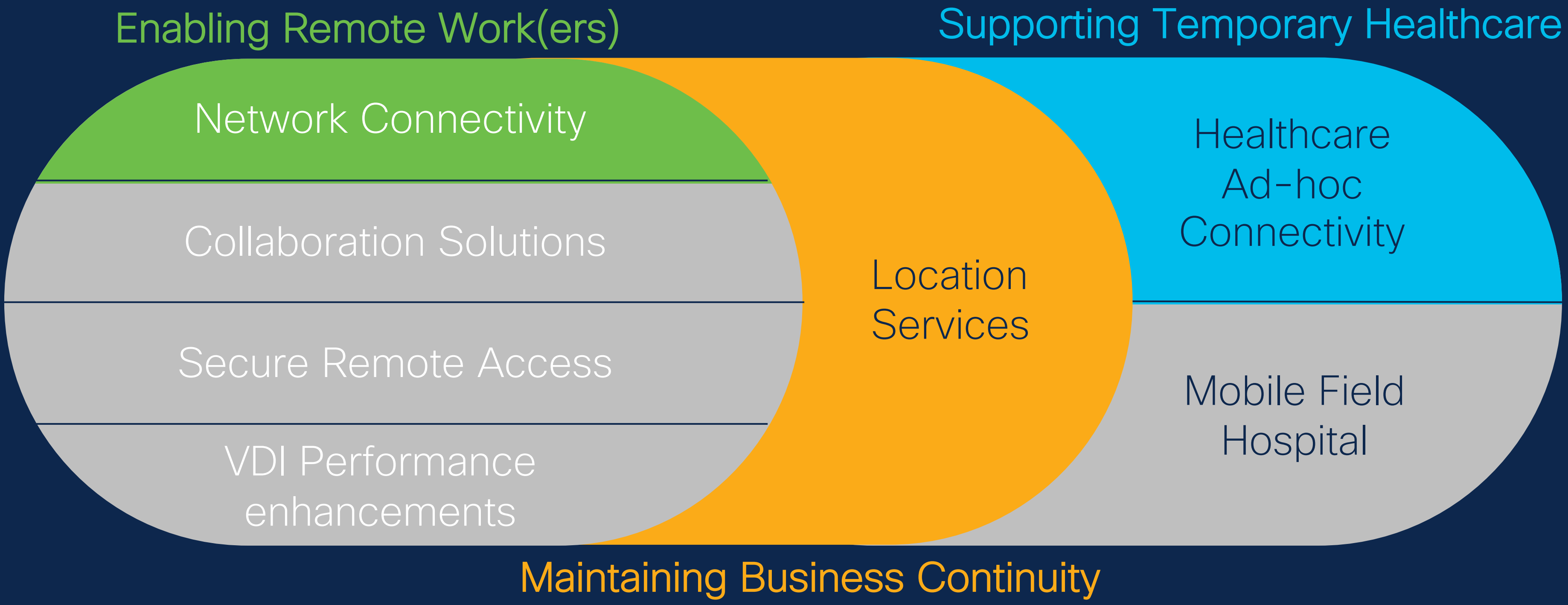
Additional Resources

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

Final Thoughts

Helping maintain business operations



Enabling Remote Work(ers)

Network Connectivity

Collaboration Solutions

Secure Remote Access

VDI Performance enhancements

Location Services

Supporting Temporary Healthcare

Healthcare Ad-hoc Connectivity

Mobile Field Hospital

Maintaining Business Continuity

Click to view Cisco's COVID-19 pandemic page

Continue learning…

Collaboration
Webinars & Demos

Secure your Remote Workforce
Your Questions Answered

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

cisco