

CISCO *Live!*



#CiscoLive



The bridge to possible

Empower IT team to handle Hybrid Workforce with Cisco Best Practices, Tools and Tips

Vijayanand CD (VCD) | Technical Solutions Architect

BRKOPS-1700



#CiscoLive

Cisco Webex App

Questions?

Use Cisco Webex App to chat with the speaker after the session

How

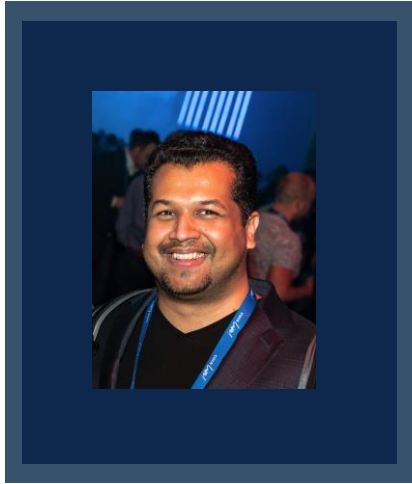
- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 17, 2022.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKOPS-1700>

Speaker Introduction



A student with 20 years of industry experience

16 Years in Cisco & 04 Years with Cisco Partners
Held various roles in Cisco

- Network Consulting Engineer
- On-site Engineer
- Focal Engineer
- Technical Leader
- Consulting System Engineer
- Technical Solutions Architect

Dual CCIE # 20769 (Routing & Switching | Datacenter)
MSc in Mobile Communication and Internet Technologies
MSc in Software and Systems Security*



Agenda

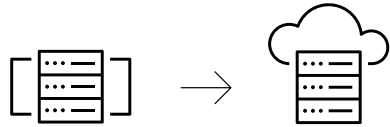
- What is Changing?
- Raising Challenges
- Build an Operational model
- Best Practices, Tips & Tools
- Not a product deep dive session
- Scope is limited to Workforce

What is Hybrid Work?

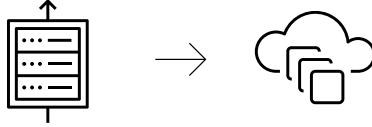
Hybrid Work is an **approach** that designs the work experience around and for the worker, wherever they are. It **empowers people** to work **onsite**, **offsite**, and moving **between locations**. [Cisco]



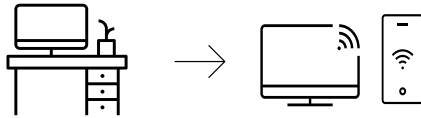
What is Changing?



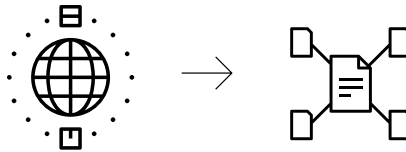
Server farms are shifting to IaaS



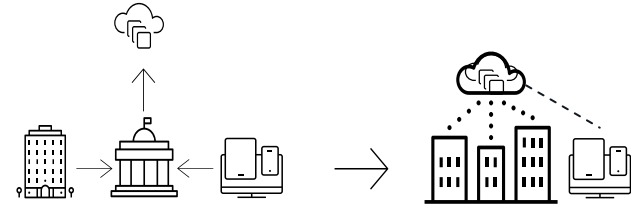
Surge in SaaS based Applications



User work off the network
(Distributed workforce)

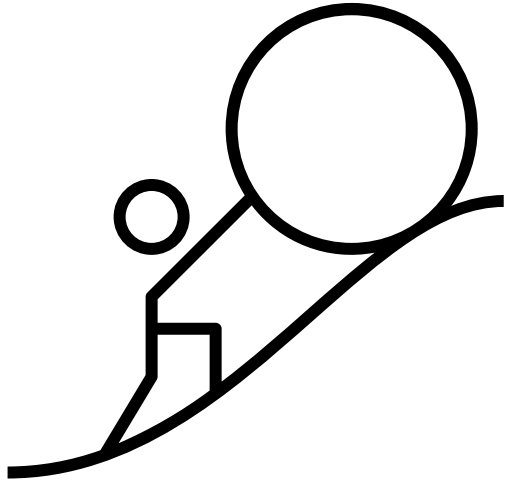


Evolving policies on
digital sovereignty



Traffic flow pattern changed

Raising Challenges



Data assets moving outside the corporate network

- Increasing attack surfaces with BYOD and Mobile workers


Optimal allocation of IT resources

- Limited Hardware resources (and Internet Bandwidth)
- Shift towards Remote IT / Sec Ops

Maintain secure access to business-critical applications

- Traffic hair pinning and Impact on user experience

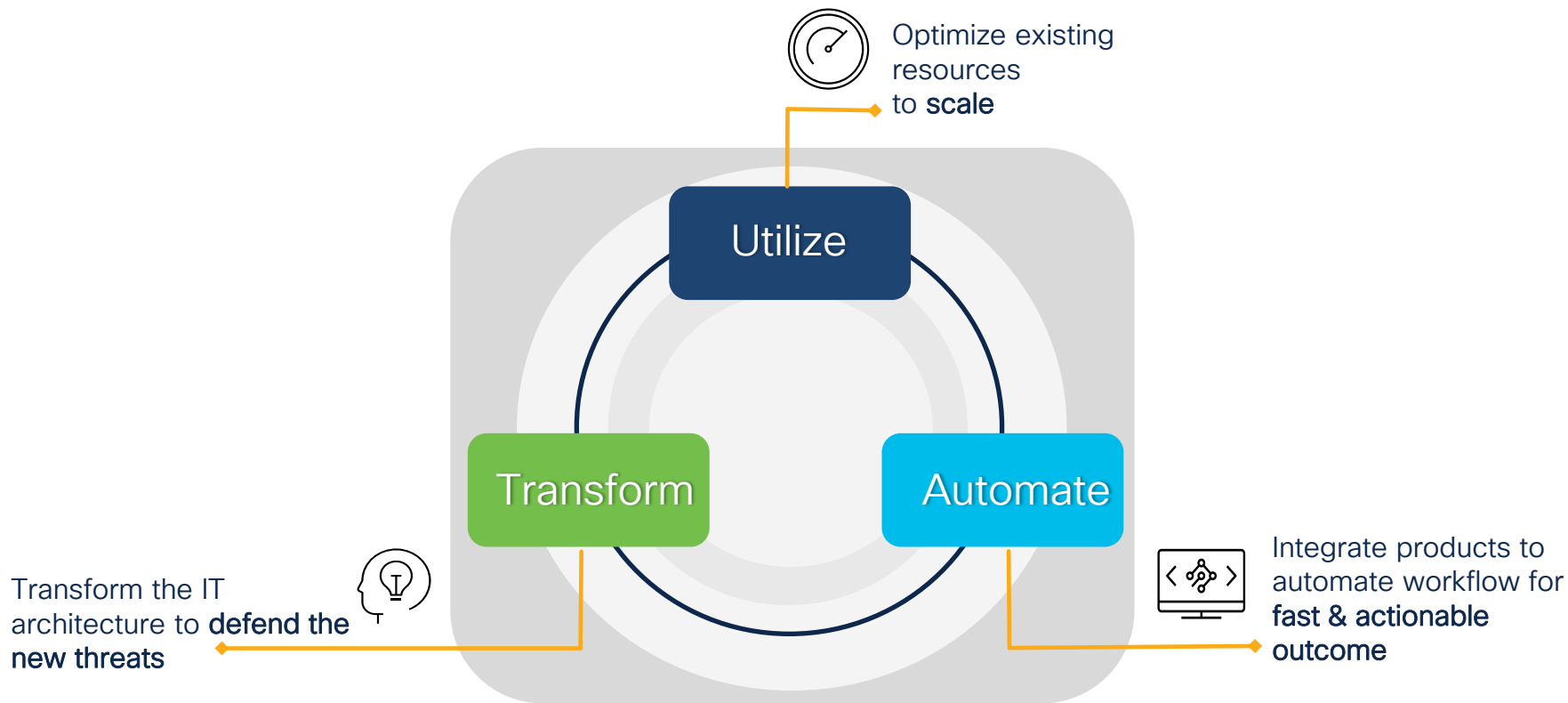
A Problem? or An Opportunity?



*The greatest **danger** in times of turbulence is not the turbulence; it is to act with **yesterday's** logic.*

Peter Drucker

Build an operational model



Hybrid Workforce

Components of a Secure Remote Worker



Users & Devices

Secure Endpoint

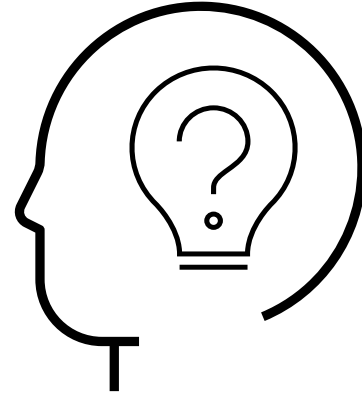
Internet

Secure Transport

Data & Apps

Secure Workload

“Remote Transport”



What is the first thing coming
in our mind ?



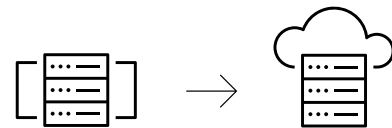
“V P N”

Do we still need Remote Access VPN ?

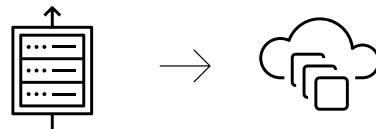
Yes or No?

Not exactly a “Yes” nor a “No” 😊

Are we in a transformation stage?



Server farms are shifting to IaaS



Surge in SaaS based Applications

Secure Transport

Remote Access Virtual Private Network (RA VPN)

- Manage the traffic throughout to avoid high load on headend CPU
- Dedicate devices to server only as VPN termination points
- Direct only **necessary traffic** into the tunnel

of RA VPN sessions + Traffic Load = Impact on Performance



Use **split tunnel** feature as a best practices for performance optimization without sacrificing security

Tip

Only necessary traffic into the tunnel

Optimization

AnyConnect by default will send (secure) all traffic over the tunnel

Split Tunnelling is a method of ***selectively*** forward traffic based on;

- Static Split-tunnel - IPv4/IPv6 Address
- Dynamic Split-tunnel - Domains (FQDNs)
 - **Enhanced Dynamic Split-tunnel**



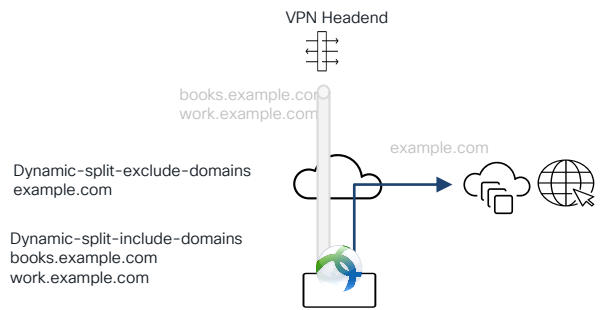
Tools

Cisco Defense Orchestrator (CDO) a cloud-based management solution that allows you to centrally manage security policies and device configurations across multiple Cisco products

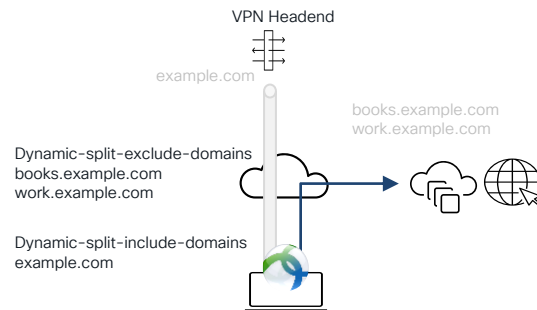
RA VPN Optimization

Enhanced Dynamic Split Tunnel

Enhanced Dynamic Split-tunnel Exclude



Enhanced Dynamic Split-tunnel Include



Dynamic Split-tunnel Exclude + Dynamic Split-tunnel Include = Enhanced Dynamic Split Tunnel

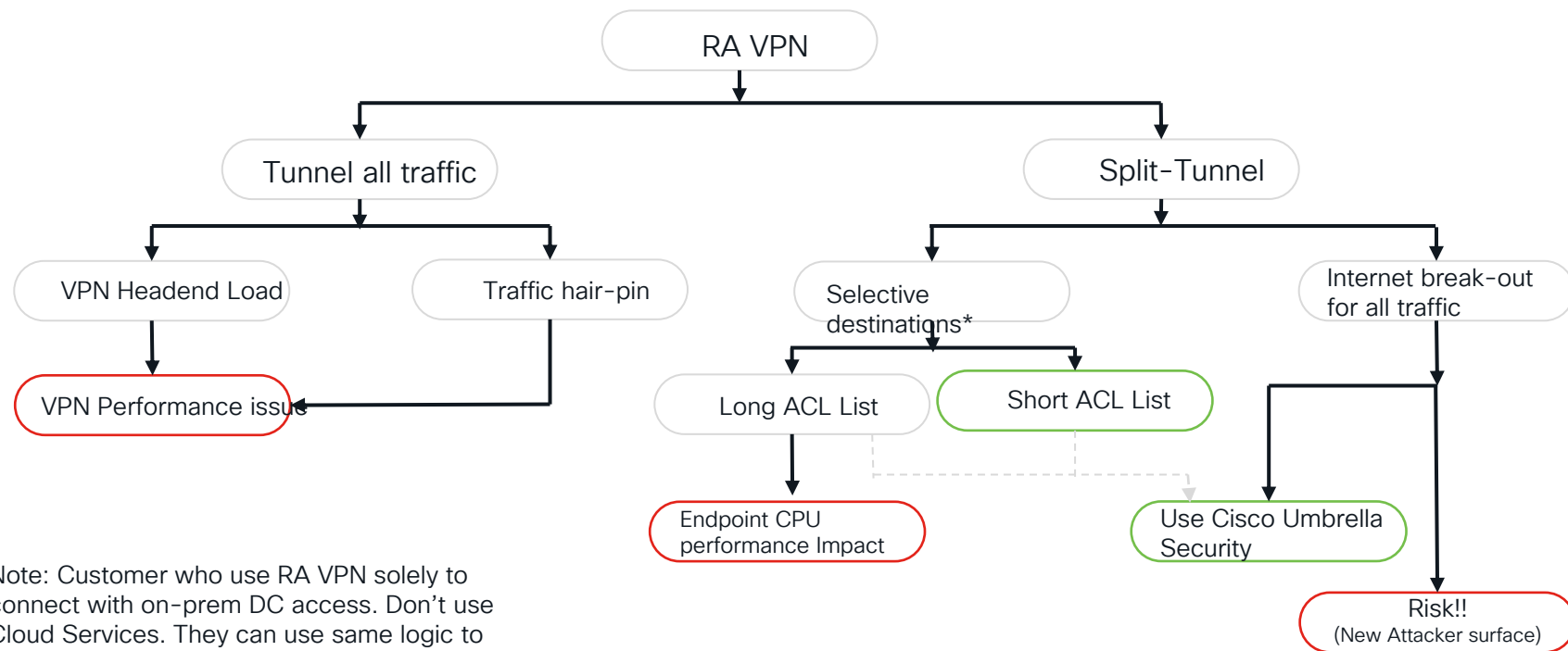


Tip

Do not create long list of destinations. Endpoint device has to perform route lookup to route the traffic. This may have CPU performance issues on endpoint.



VPN tunnel traffic optimization – Mind Map



Note: Customer who use RA VPN solely to connect with on-prem DC access. Don't use Cloud Services. They can use same logic to implement the split-tunnel.

* Must be selective few trusted domain like O365, Webex, Box etc.

How we protect off VPN traffic to internet ?



Secure Transport

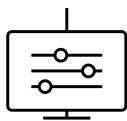
Secure Off VPN traffic with Cisco Umbrella



Add extra layer of security to all Internet-bound traffic



Block malware, phishing and command & control call backs over any port

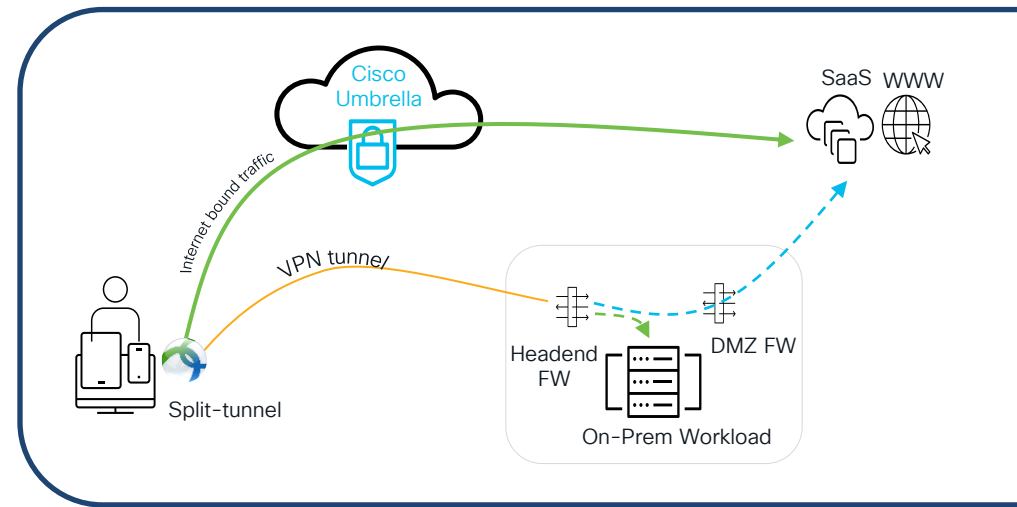


Real-time visibility into all internet activity per hostname



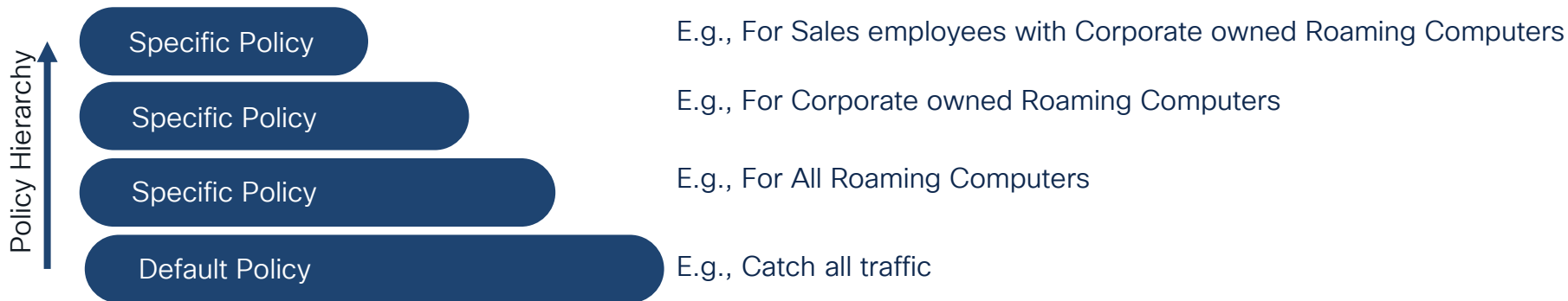
Tip

Use AnyConnect **Network Visibility Module (NVM)** module to enable greater visibility across users, endpoints, and applications, and facilitates analytics on contextual telemetry data



Cisco Umbrella DNS Policies

Layer DNS policies for bottom-up approach



Tip

Use **Tags** to group roaming computers to enforce policies for a group of roaming computers

Note: Tags are only available for roaming computer identity types.

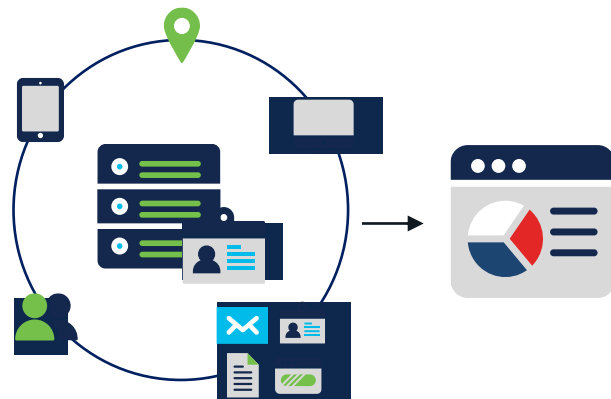
How do we **Monitor** and **Optimize** the traffic on split-tunnel?



Cisco AnyConnect Network Visibility Module (NVM)

Build a holistic view across entire network

- Collect and send data when on premises and/or VPN connected (including split tunneling)
- Very small impact on endpoint due to low level stream level interception
- Get 24-hour rolling cache of flow data when disconnected
- Can exclude selective context variables to meet privacy requirements



Tools

Use **Splunk** which has pre-build AnyConnect NVM App to collect and analyze NVM Telemetry. Also called Cisco Endpoint Security Analytics (CESA).



Recommended Session

BRKSEC-2834 Cisco's Unified Agent: Cisco Secure Client.
Bringing AMP, AnyConnect, Orbital & Umbrella together

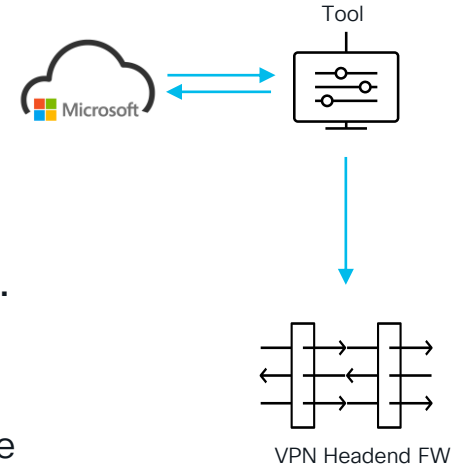
Automate AnyConnect Split-Tunnel

Microsoft Office 365 URLs and IP address may get updated each month

Microsoft provides a JSON-formatted feed of their networks and domains for their various cloud services.

Automate the update process

- Fetch the online services information JSON from Microsoft website
- Use script to parse the JSON into ASA commands
- SSH to an Adaptive Security Appliance and execute the commands



Tools

Use **SecureX** to automate the workflow to fetch JSON and push the URLs & IP addresses into the split-tunnel list in ASA

VPN Capacity Expansion

Dynamically expand ASA headend capacity using Amazon EC2

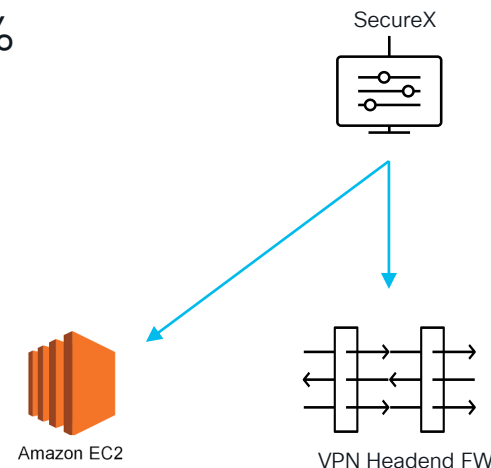
If an existing ASA has VPN user load say over 70%

Logical Workflow Example

```
If = load > 70% then
    spin up new ASAv instance in EC2
```

Optional to update in Webex Teams

```
print = Webex Teams
      "message xxx "
else
    repeat verification after yy time
```



Tip

Use pre-build workflows & atomic actions of SecureX available in GitHub
(<https://ciscosecurity.github.io/sxo-05-security-workflows>)



Transform existing remote access IT infrastructure



To support the hybrid environment - On-premises, Public Cloud, SaaS



Consistence operational model across the hybrid environment



Gain visibility and provide access to all your apps from home, in the office and anywhere

A **zero-trust** approach allows to manage risk across all locations, connections, and devices

Zero Trust with Cisco Secure Access

Establish **Trust** | Enforce **Trust**-based Access | Continuously verify **Trust**

- Is the user who they say they are?
- Do they have access to the right applications?
- Is their device secure?
- Is their device trusted?



CISCO *Live!*



Workforce

Cisco Secure Access by Duo

Establish Trust	Multi Factor Authentication (MFA)
Enforce Trust based Access	Adaptive and role-based access controls
Continues Trust Verification	Duo Device Health App
From	Anywhere

Zero-Trust !!!
Where do I start ????



Zero-Trust - Where do I start?



Start to implement multi-factor authentication (MFA) in VPN with Cisco Secure Access by Duo



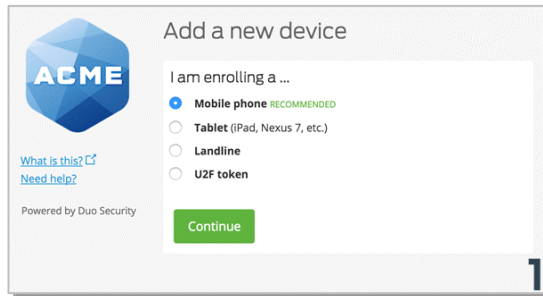
Gain complete visibility into all your devices



Evolve it as a best practice to enforce zero-trust network access (ZTNA) to all employees regardless of their location (office or remote)

Self-Enrollment: Easily enroll users in minutes

- Users easily self-enroll in minutes
- Users leverage their own device
- Enroll thousands of users in hours
- Reduce TCO by enabling the user to easily enroll with no help needed



ACME

Add a new device

I am enrolling a ...

☒ **Mobile phone** RECOMMENDED

☐ Tablet (iPad, Nexus 7, etc.)

☐ Landline

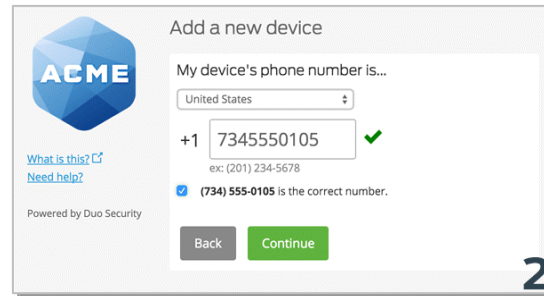
☐ U2F token

[What is this?](#) [Need help?](#)

Powered by Duo Security

Continue

1



ACME

Add a new device

My device's phone number is...

United States

+1 7345550105 ✓

ex: (201) 234-5678

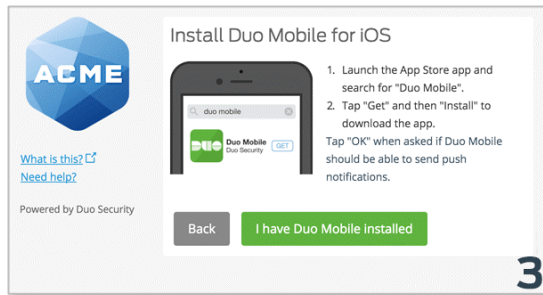
☒ (734) 555-0105 is the correct number.

[What is this?](#) [Need help?](#)

Powered by Duo Security

Back **Continue**

2



ACME

Install Duo Mobile for iOS

1. Launch the App Store app and search for "Duo Mobile".

2. Tap "Get" and then "Install" to download the app.

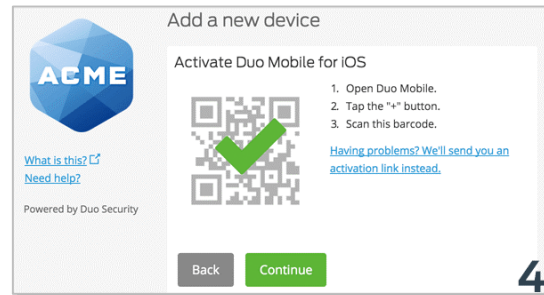
Tap "OK" when asked if Duo Mobile should be able to send push notifications.

[What is this?](#) [Need help?](#)

Powered by Duo Security

Back **I have Duo Mobile installed**

3



ACME

Add a new device

Activate Duo Mobile for iOS

1. Open Duo Mobile.

2. Tap the "+" button.

3. Scan this barcode.

[What is this?](#) [Need help?](#)

Powered by Duo Security

Back **Continue**

4

A Problem?
or
An Opportunity?

Empower IT team



Use best practices and **AnyConnect** capabilities to scale up the resources

Utilize

Transform

Automate



Start Zero Trust journey with Cisco Secure Access by **Duo** layering additional security for Remote access



Use **SecureX** is a cloud-native, built-in platform to integrate your technology for true turnkey interoperability.



In the middle of Difficulty lies Opportunity

Albert Einstein

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.



Learn more with these next steps



Attend / [listen](#) to relevant sessions

SD-WAN is going managed:
is SASE next? - PSOGEN-1028

How to supercharge your Next-Gen
network with AIOps and Managed
Services - BRKNWT-2208

Don't Panic!! The New Hybrid
Workplace can be Operated
and Managed - BRKOPS-2513



Connect with us

Meet us in booth #3562

See a demo of Cisco+ Hybrid
Cloud on the Showcase floor

Book a meeting with our
Engineer, Sanjit Aiyappa (via
our Booth) to discuss Hybrid
Cloud and Sovereign Cloud



Talk to a Cisco+ Hybrid Cloud Partner @ Cisco Live



Booth #1770 & 1200



ConvergeOne

Booth #3444



Booth #1970



Booth #2150



NTT LATAM

Booth #C-35



Booth #3271



PURESTORAGE

Booth #C-29, 1451, 1554



Booth #1756

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with
Cisco Learning Credits

(CLCs) are prepaid training
vouchers redeemed directly
with Cisco.



Learn

Cisco U.

IT learning hub that guides teams
and learners toward their goals

Cisco Digital Learning

Subscription-based product, technology,
and certification training

Cisco Modeling Labs

Network simulation platform for design,
testing, and troubleshooting

Cisco Learning Network

Resource community portal for
certifications and learning



Train

Cisco Training Bootcamps

Intensive team & individual automation
and technology training programs

Cisco Learning Partner Program

Authorized training partners supporting
Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training

Accelerated curriculum of product,
technology, and certification courses



Certify

Cisco Certifications and Specialist Certifications

Award-winning certification
program empowers students
and IT Professionals to advance
their technical careers

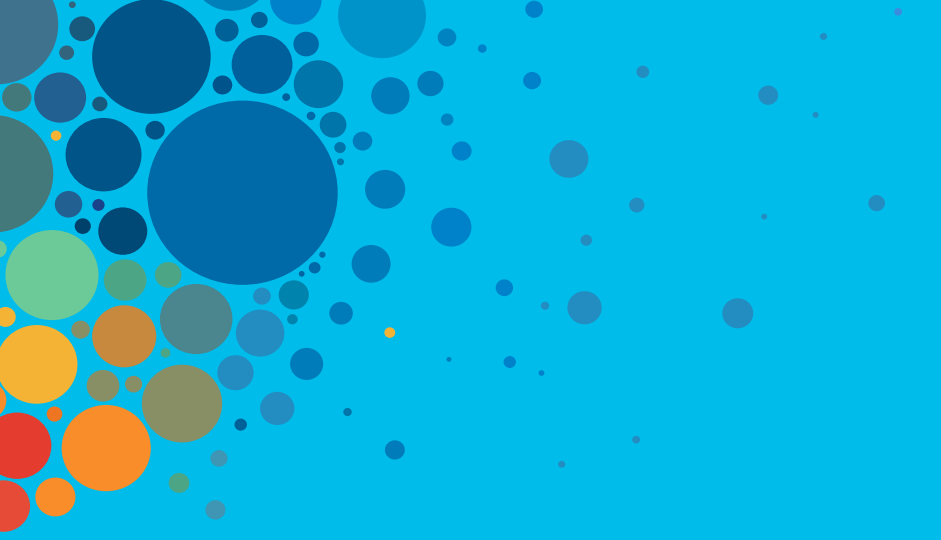
Cisco Guided Study Groups

180-day certification prep program
with learning and support

Cisco Continuing Education Program

Recertification training options
for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**



Continue your education

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



The bridge to possible

Thank you

CISCO *Live!*



#CiscoLive