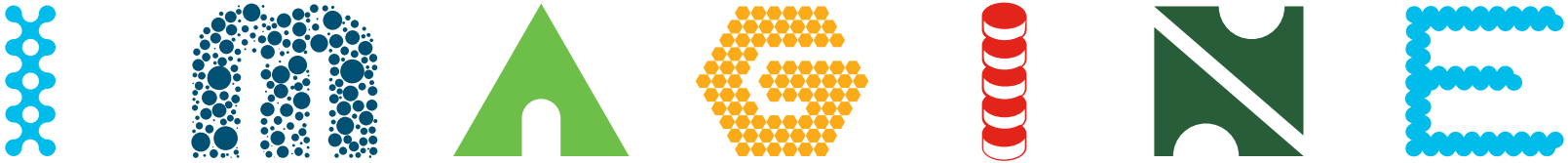
Cisco live!

January 28 - February 1, 2019 - Barcelona

cisco

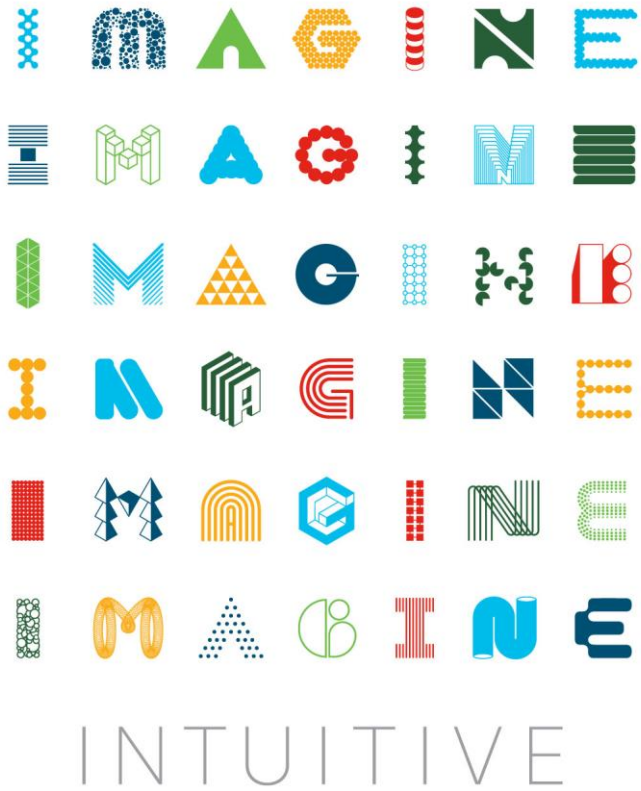


INTUITIVE

BRKSEC-3001

Advanced IKEv2 Protocol

Jay Young, CCIE - Technical Leader, Services



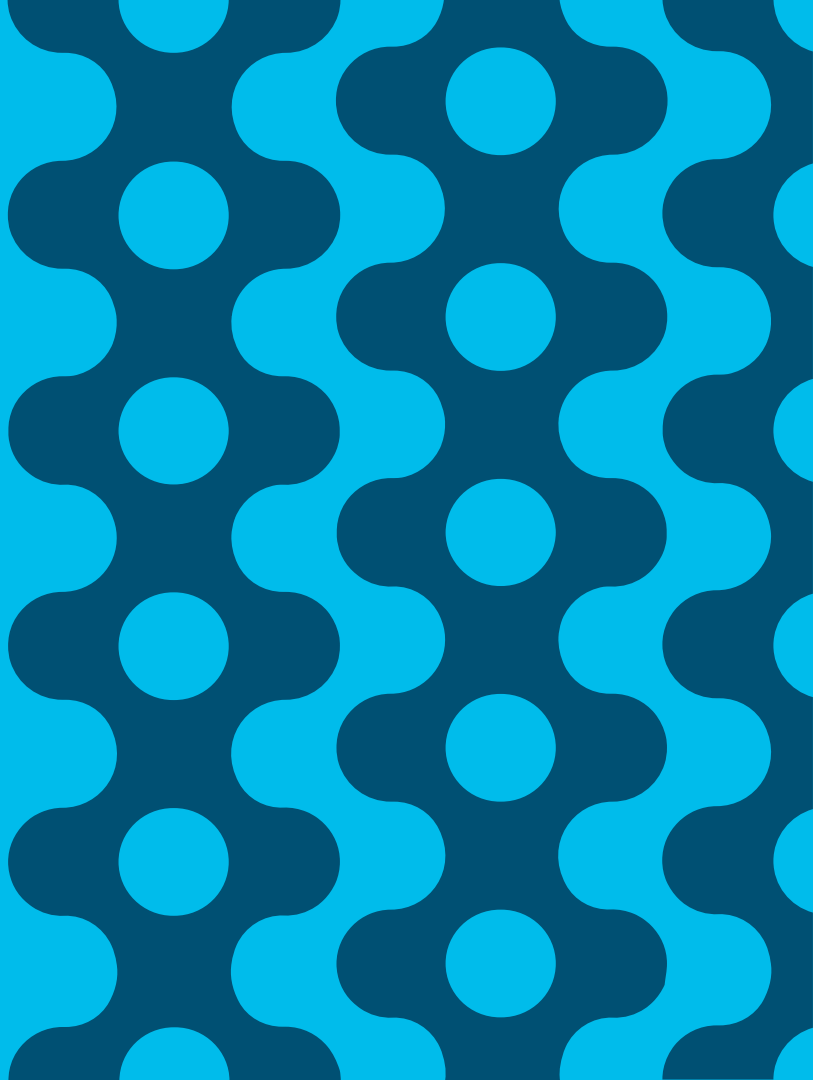
Cisco live!

Agenda

- IP Security overview
- IKEv1 – Protocol Overview
- IKEv1 – Everything is good, right?
- IKEv2 – Protocol Overview & Comparison
- Summary

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IP Security Overview



Lets jump in our time machine back to 1998

- A need for a standard secure method to communicate over the Internet
- Architecture needed:
  - Multiple Strong Authentication Methods
  - Anti-clogging (DoS)
  - Prevent Connection Hijacking
    - Linking key exchange with authentication
  - Prevent Man-in-the-middle attacks
    - Interception, insertion, deletion, replay, redirection
  - Encryption
  - Integrity

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IP security overview

- A collection of 12 RFCs published to define IP Security (IPsec)
- Some were very high level architectural designs
- Some were very low on roles, responsibilities and functions
- Numerous other RFCs defined to add shortcomings

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IP Security Overview

Key Exchange

RFC2412
OAKLEY

Architecture

RFC2408
ISAKMP

RFC2401
Sec Arch for IP

RFC2411
IPsec Doc

Cipher/Hash

RFC2403
HMAC-MD5

RFC2410
ESP-NULL

RFC2404
HMAC-SHA-1

RFC2405
ESP w/ DES

Traffic Encapsulation Protocols

RFC2406
ESP

RFC2402
AH

Protocol Definition

RFC2407
IPsec DOI

RFC2409
IKEv1

+many more minor additions

NAT-T
RFC3947+3948

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

ISAKMP

- ISAKMP defines two phases:
- Phase 1
  - Used for control plane
  - Establish secure channel between peers
  - Prove identities
  - Negotiate data plane security settings
- Phase 2
  - Used for data plane
  - Transports the protected data

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – Protocol Overview

IKEv1

There are two different ‘modes’ for building Phase 1

Main Mode

- 6 packet exchange
- Full Identity protection (protects against passive surveillance)
- Better Anti-DoS protection

Aggressive Mode

- 3 packet exchange
- Identities passed in the clear
- Responder must authenticate himself first
- PSK can be retrieved by an offline brute-force attack
- Trivial to DoS
- Faster session establishment

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1- Main Mode (message 1 and 2)

- The first two messages are used to negotiate the following cryptographic attributes:
  - Authentication method*
  - Encryption cipher*
  - Integrity hash*
  - Lifetime of Security Association
  - Diffie-Hellman Key Exchange Group *
- Initiator proposes a list of combinations of the starred (*) above
- Responder picks one of the combinations proposed
- Lifetime is MIN(initiator, responder)
- NOT encrypted – Peer NOT authenticated yet

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1- Main Mode (message 3 and 4)

- Exchange Diffie-Hellman key values
- Exchange Nonce values
- Detect if NAT is used between peers
- Suggest trusted certificate authorities (CA)
- After this exchange, further communication is encrypted and secure.
- Peer **NOT** authenticated yet.

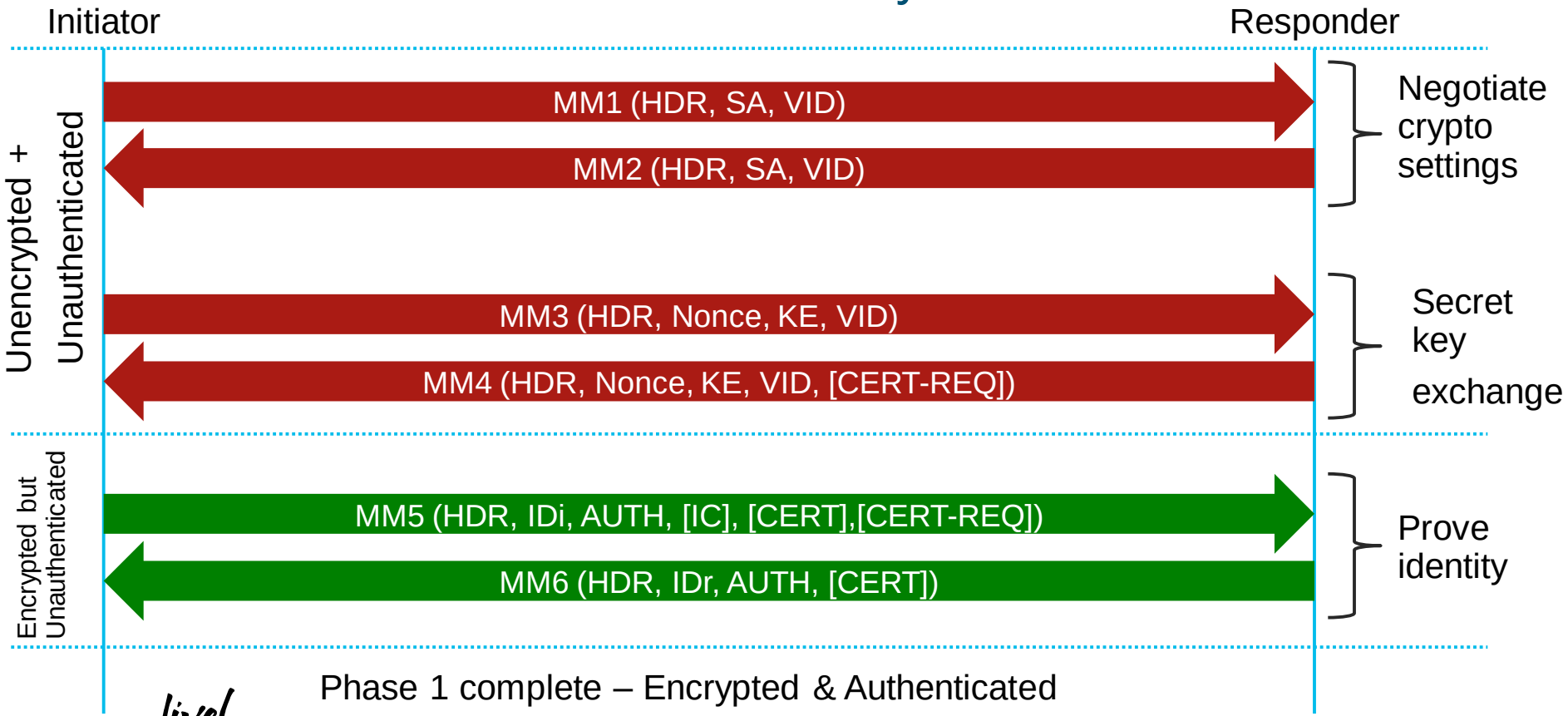
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1- Main Mode (message 5 and 6)

- Exchange certificate
- Prove identity using Pre-Shared Key or Certificate
- Cryptographically validate previous messages – prevents session hijack
- Switched to UDP/4500 if NAT had been detected in MM3+4
- Encrypted – Peer is proving identity.

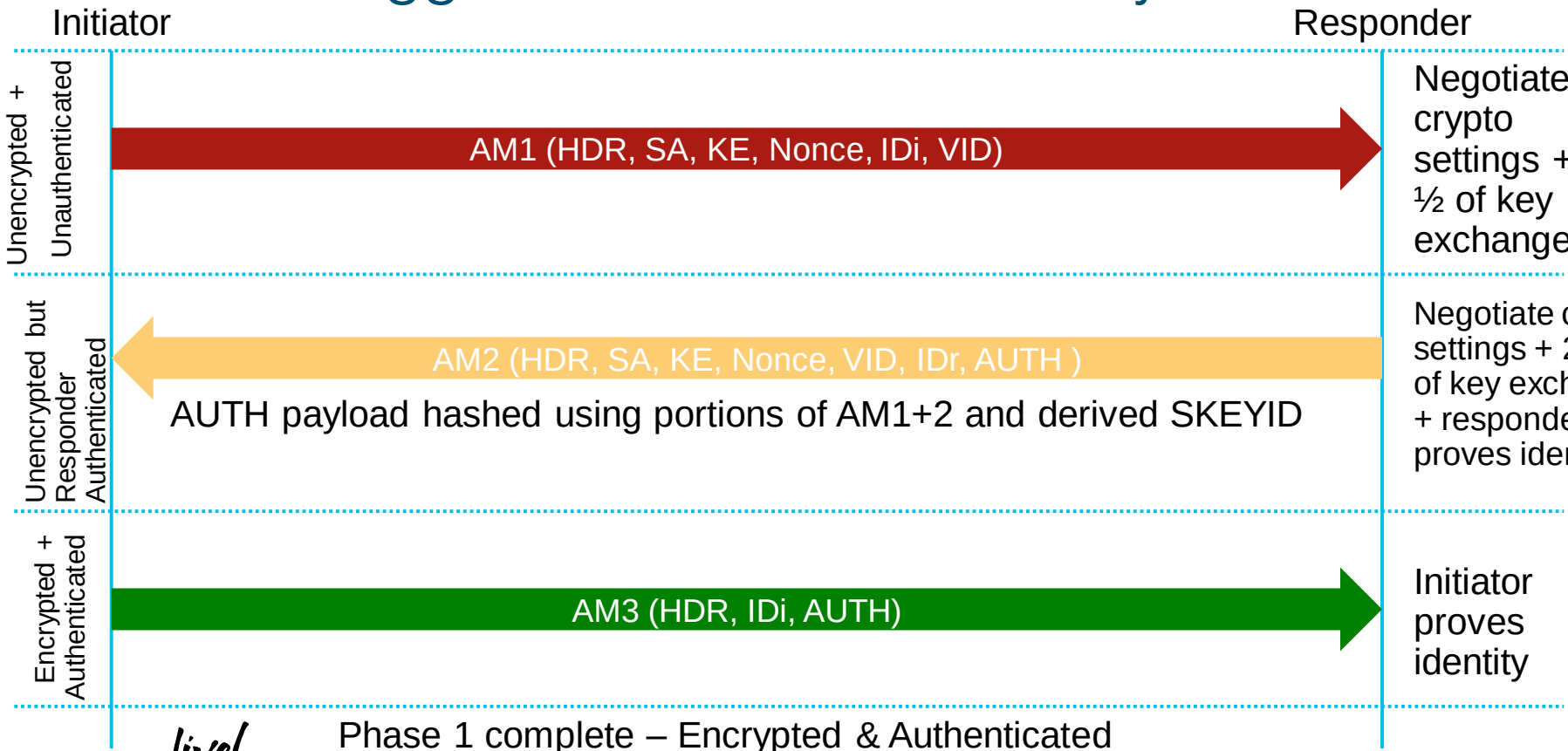
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – Main Mode Summary



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – Aggressive Mode Summary



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – Phase 1

- 1st Phase is already built: it provides security and proof with whom you are communicating with
- The following operations occur over this Phase 1 SA:
  - Dead Peer Detections (keepalive messages)
  - Negotiation and Establishment of ESP and AH SAs (Phase 2)
  - Notifications (Teardown/Deletion)
  - Xauth (Username/Password Authentication) – Remote access
  - Mode_CFG (IP address assignment, DNS, etc.) – Remote access
- In most deployments Phase 2 is IPsec, but other DOIs exist (e.g. GDOI).

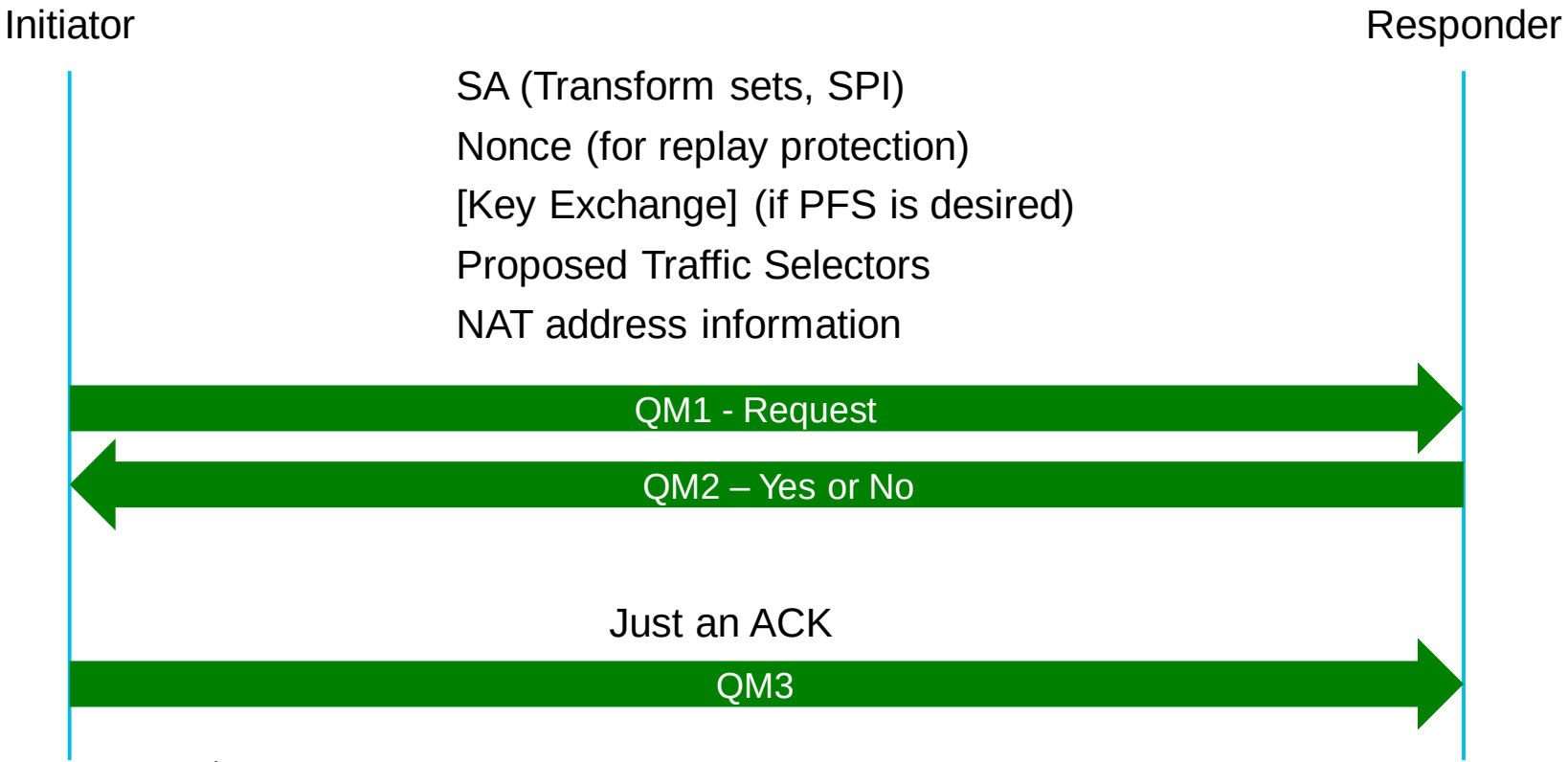
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – Quick Mode Phase 2

- Quick mode allows the establishment of an IPsec SA in three messages
- Things negotiated:
  - Traffic to be protected
  - How to be encapsulated
  - How to be encrypted
  - How to provide integrity
  - How long the SA is valid for in time and volume of data
  - If Perfect Forward Secrecy (PFS) is required

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1- Quick Mode Summary



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – Everything's good, right?

IKEv1 – Challenges

- NAT breaks things™
- What do you mean certificates don't scale?
- So many keys which one do I use?

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – NAT breaks things™

- IPsec uses IP protocol 50 (ESP) and 51 (AH)
- 1:1 NAT
  - AH can't work – Integrity check performed over IP address fields + payload
  - ESP can work – Integrity check performed only over payload
- N:1 Port Address Translation (PAT)
  - Rule of Thumb – Only TCP and UDP can reliably be NATted
- ESP doesn't have ports ∴ ESP can't work through PAT

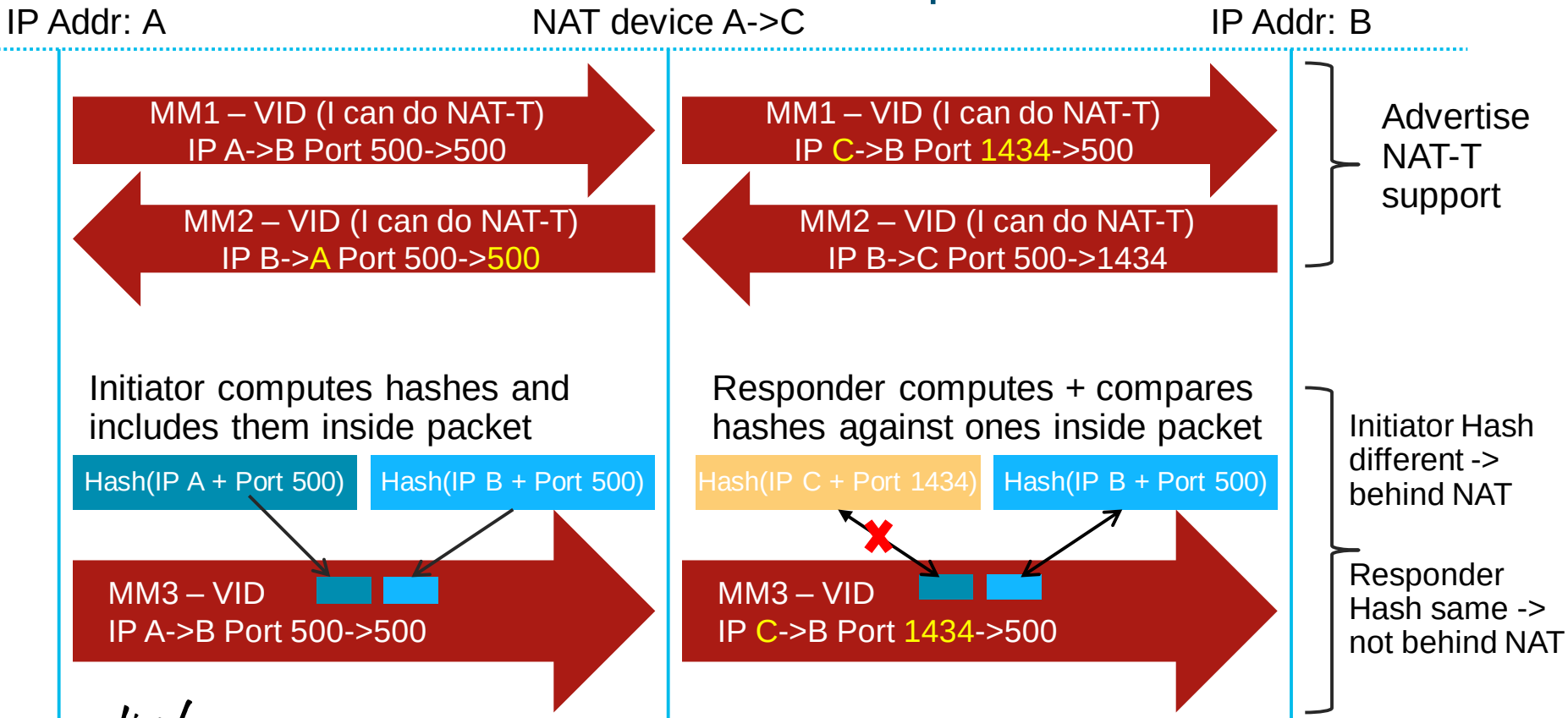
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – NAT-T

- **Solution**: Encapsulate ESP packets within UDP when going through NAT
- NAT/PAT devices only see UDP packets.
- Port 4500 is reserved for IPsec over UDP
- Support for NAT-T was added with RFC 3947 and 3948

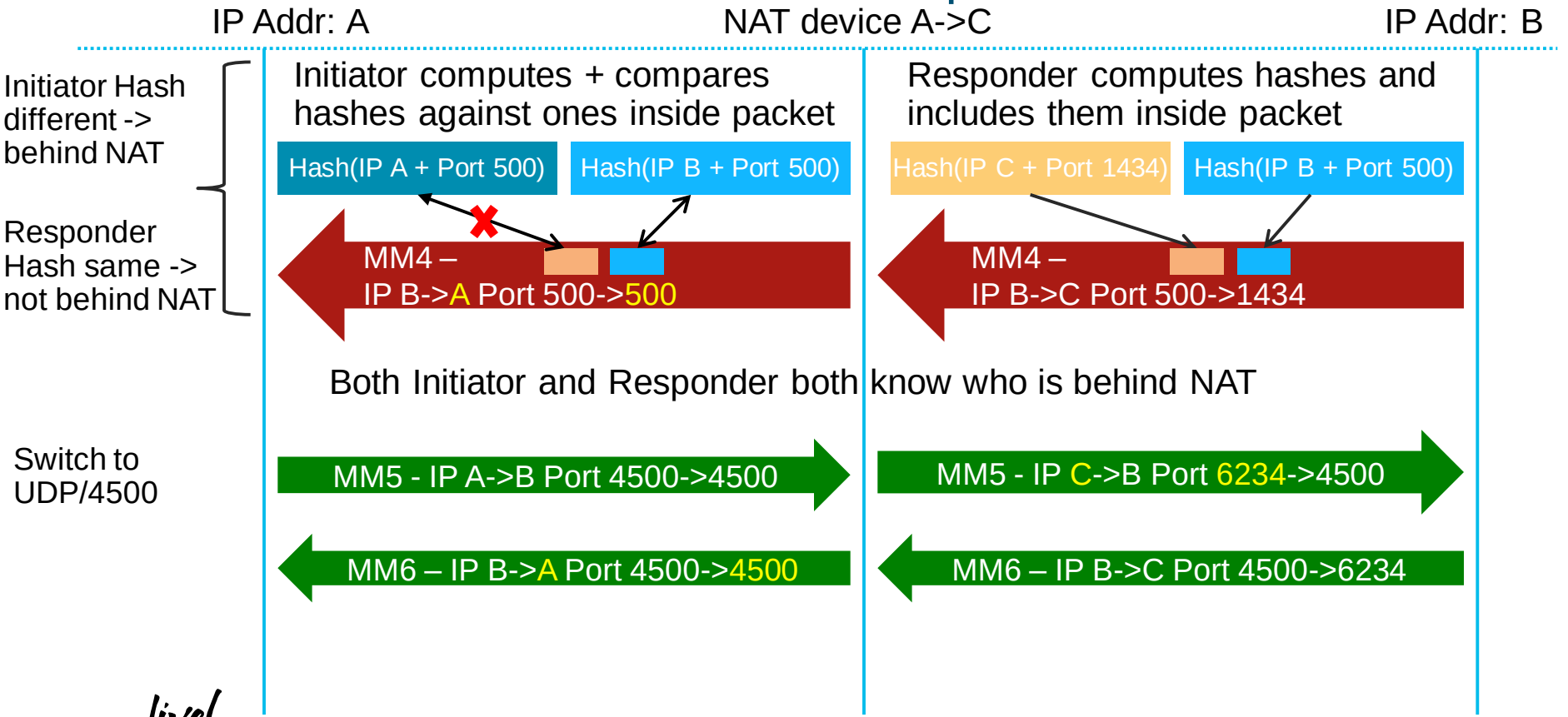
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – Determine if NAT is in path



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – Determine if NAT is in path



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – NAT-T

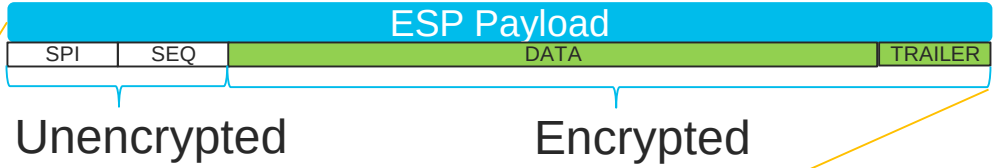
- Normal Case without NAT:
  - UDP/500 for control channel
  - ESP or AH for data channel

- **Problem**: Stateful firewalls (NAT devices) can prevent the control channel communication due to inactivity even when data channel is actively used.

- NAT Case:
  - Send both control channel and data channel over UDP/4500

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – NAT-T



IP Addr: A

NAT device A->C

IP Addr: B

Data Traffic

ESP Payload

IP A->B | UDP Port 4500->4500 | ESP Payload

IP C->B | UDP Port 6234->4500 | ESP Payload

Control Traffic

0000 + IKE Message

IP A->B | UDP Port 4500->4500 | 0000 + IKE Message

IP C->B | UDP Port 6234->4500 | 0000 + IKE Message

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

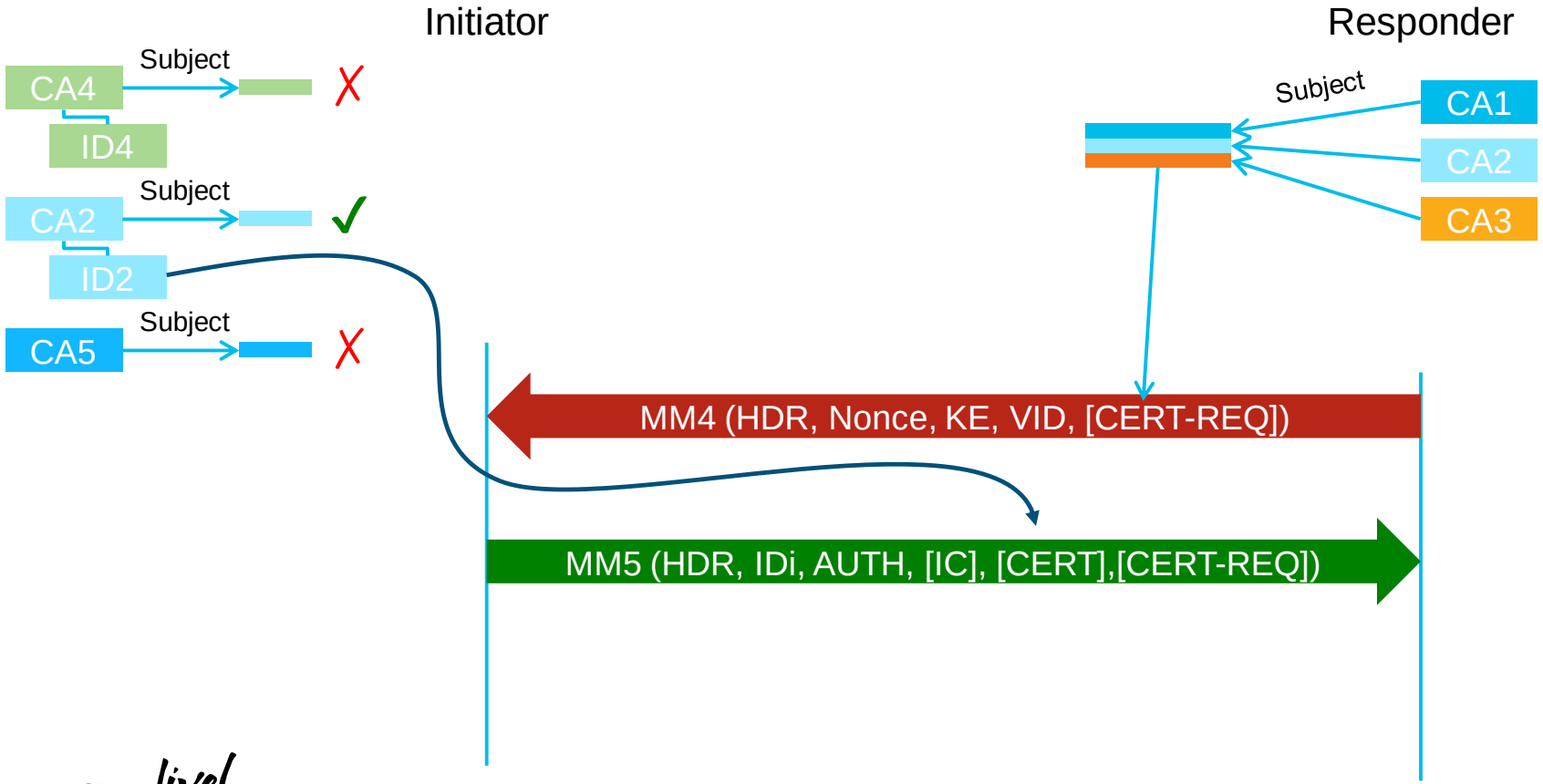
IKEv1 – Certificates

- Authentication can use certificates
- **Problem 1**: Peer must know which CAs are trusted by peer
- Explicit configuration doesn't scale

- **Solution 1**: RFC4945 – Prior to AUTH provide a list of trusted CAs to peer
  - In MM4 – Responder sends list of CA he trusts
  - In MM5 – Initiator sends list of CA he trusts.

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

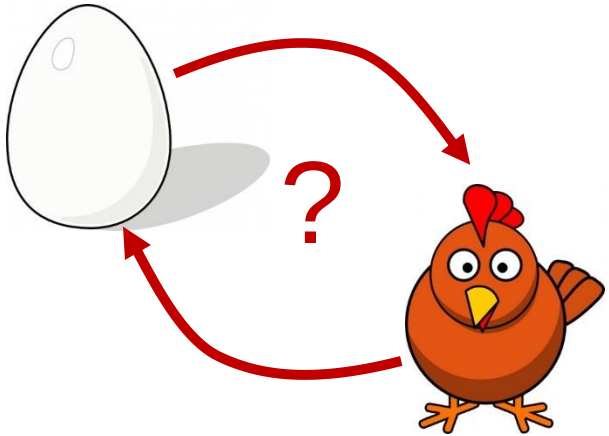
IKEv1 – Certificates



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 – Pre-shared-keys

- Keys are linked to an identity
  - IP address, FQDN, Email, Distinguished Name
- Identities are shared in MM5 and MM6
- The PSK is part of key generation
- Crypto keys are generated in MM3 and MM4
- PSK lookup can ONLY be done on IP address
- If remote devices have dynamic addresses, then use wildcard key (not best practice)
- Workaround: Use Aggressive mode
  - Caveat: Aggressive mode is less secure



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

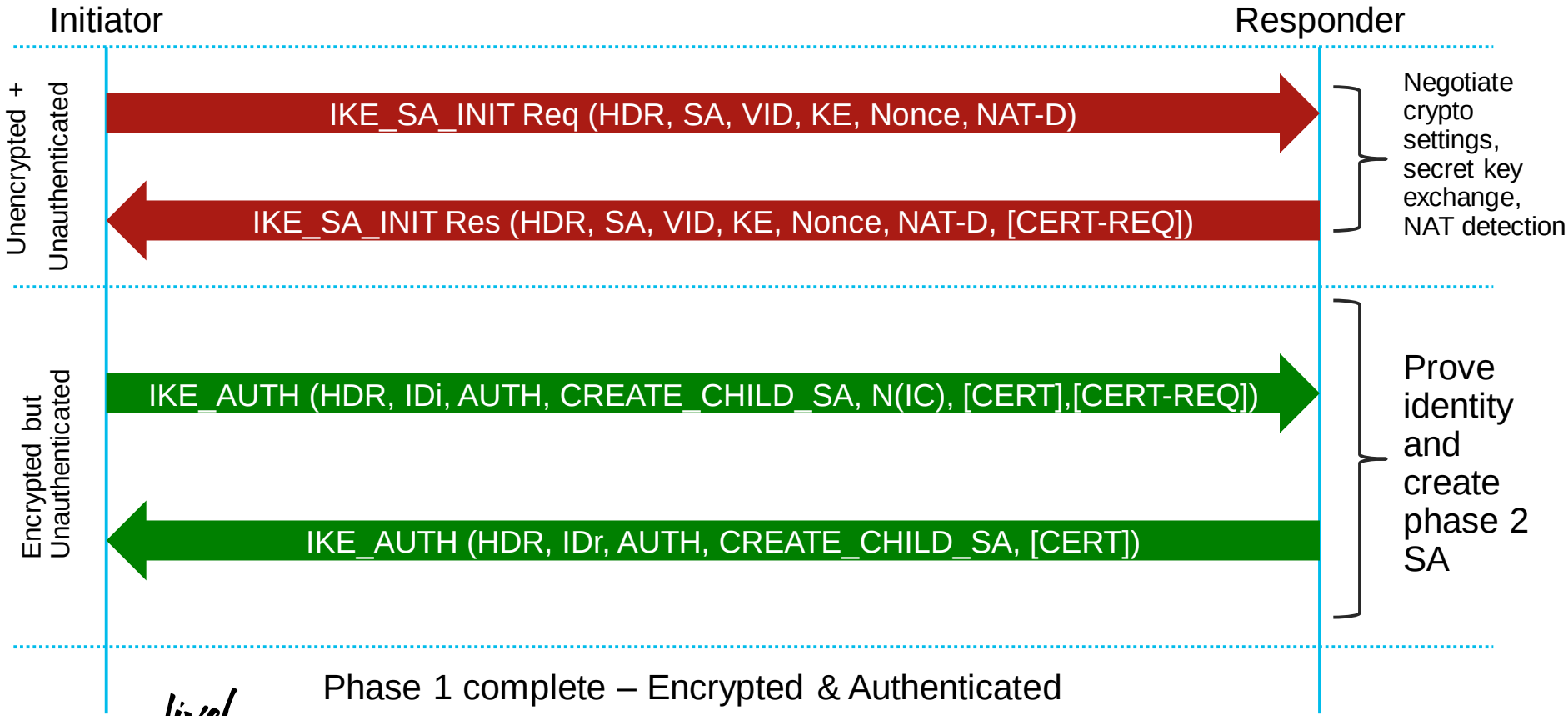
IKEv2 – Overview (Finally!)

IKEv2 – Goals (What did we learn)

- Define IKEv2 in one document rather than a combination of many
- Reduce setup latency by reducing number of messages
- More secure
- Always provide identity protection (No Aggressive mode)
- PSK is not used in crypto key generation*
- Provide additional authentication mechanisms (EAP)
- Allow more flexible authentication choices (asymmetrical)
- Exchange of routes and attributes
- Reduce number of options/methods – simplify implementations

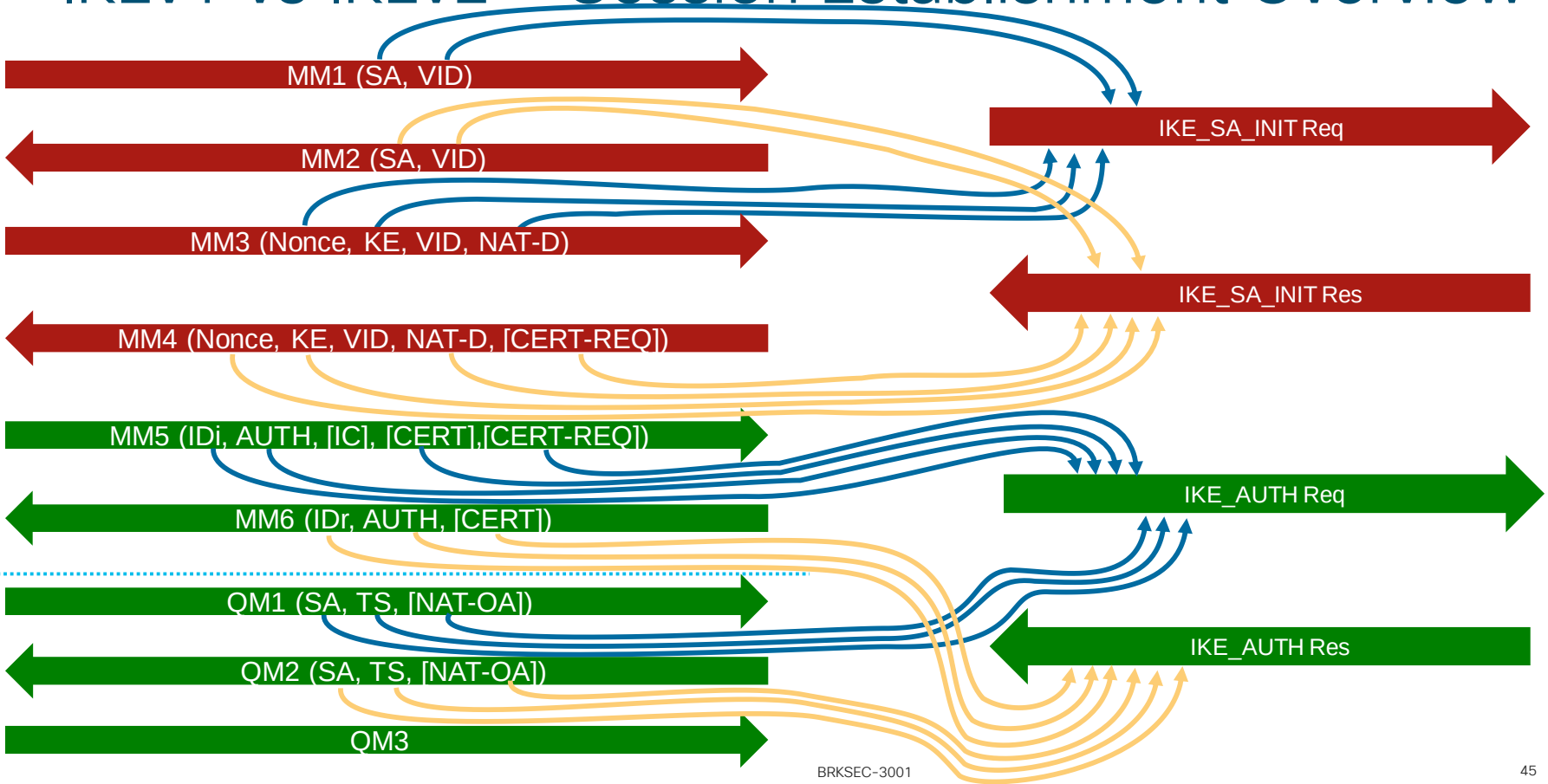
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2 – Session Establishment Overview

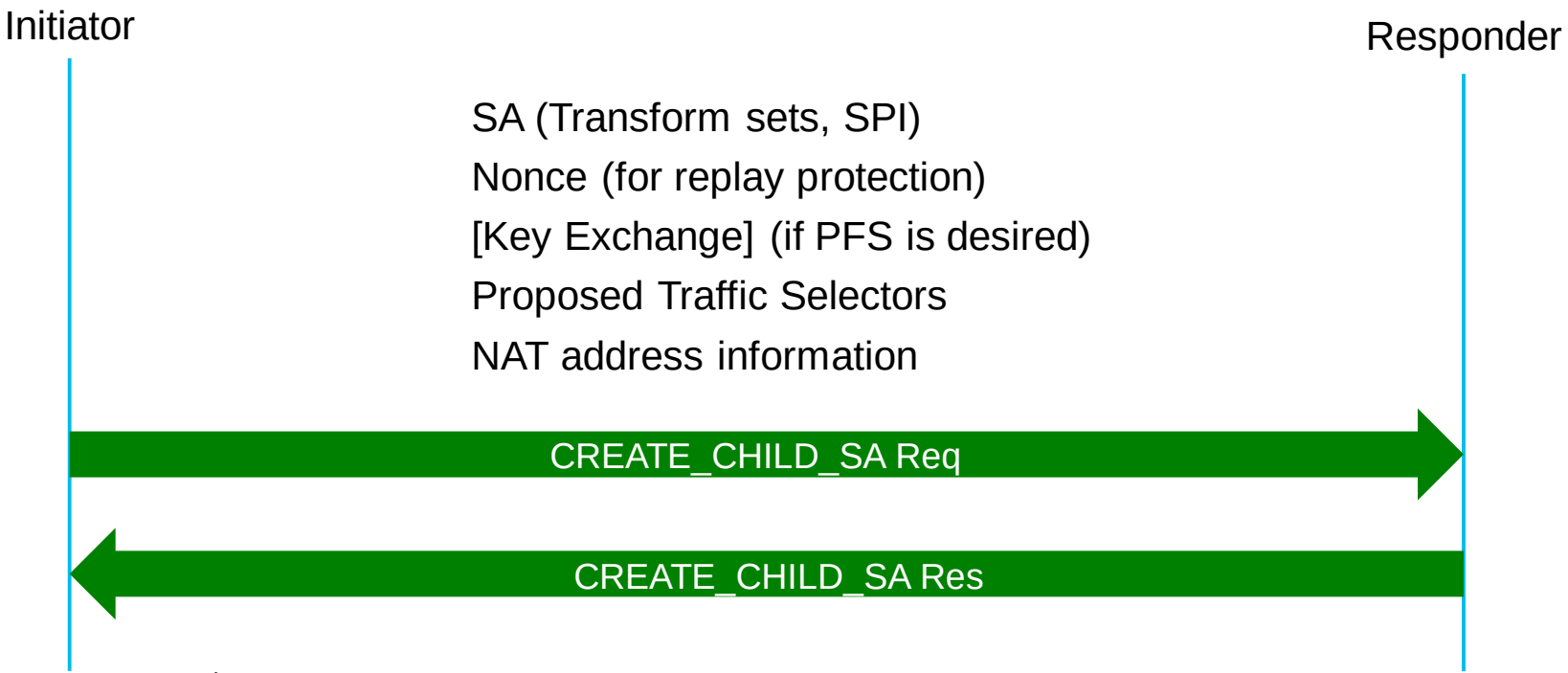


© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv1 vs IKEv2 – Session Establishment Overview

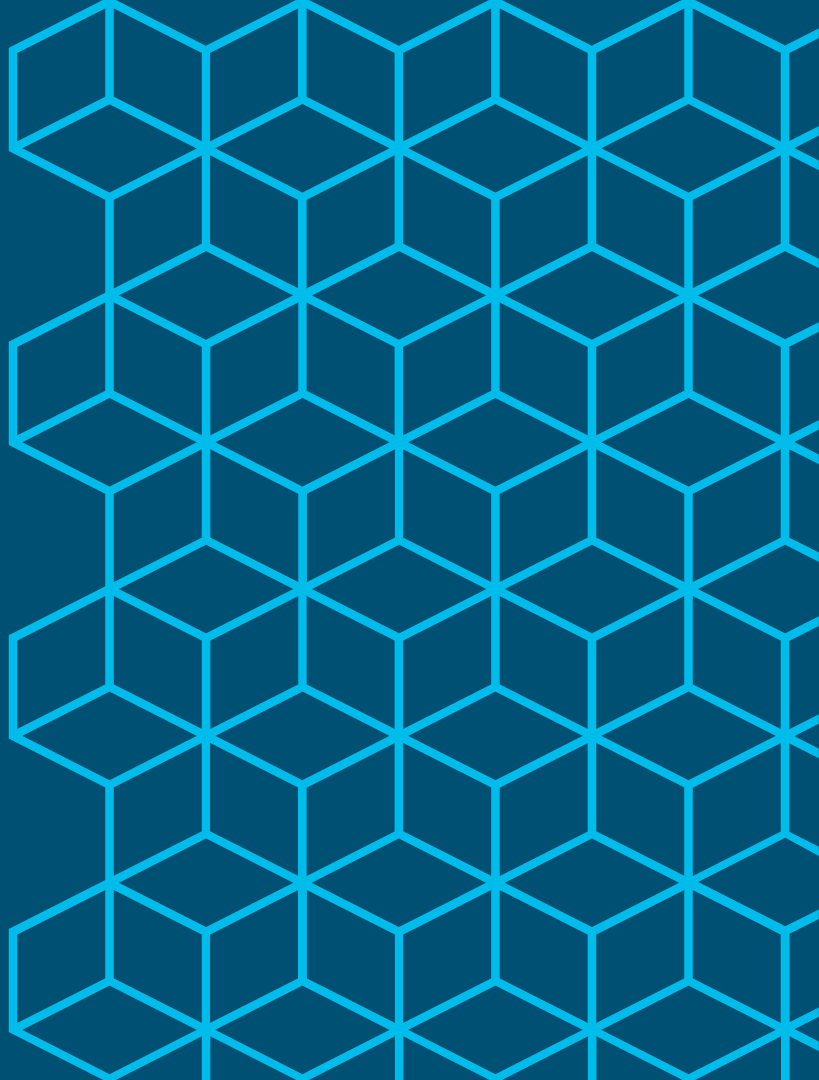


IKEv2 – 2nd Child SA Establishment



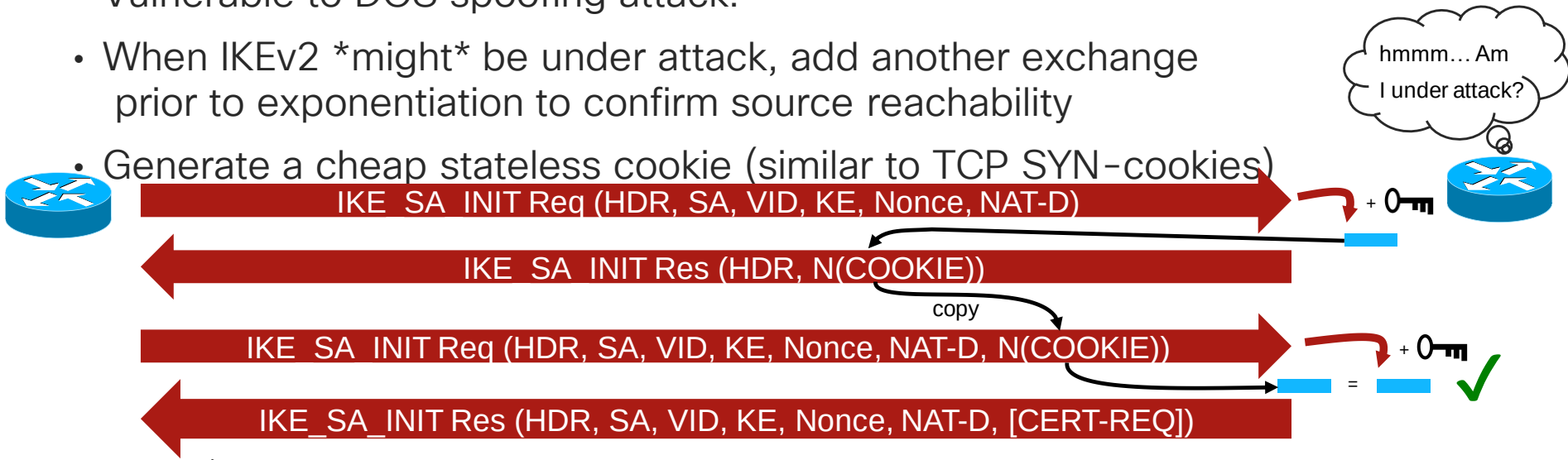
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Wow!
IKEv2 is super fast!
well.....



IKEv2 – Faster exchange right?

- "It depends!"
- Exponentiation is done after 1st packet
- Vulnerable to DOS spoofing attack!
- When IKEv2 *might* be under attack, add another exchange prior to exponentiation to confirm source reachability
- Generate a cheap stateless cookie (similar to TCP SYN-cookies)



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2 – Faster exchange right? Part 2

- Key establishment is done in first two packets.
- Initiator must guess which DH group his peer will accept
- If wrong/unacceptable group is sent, responder will hint and say ‘try again’

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

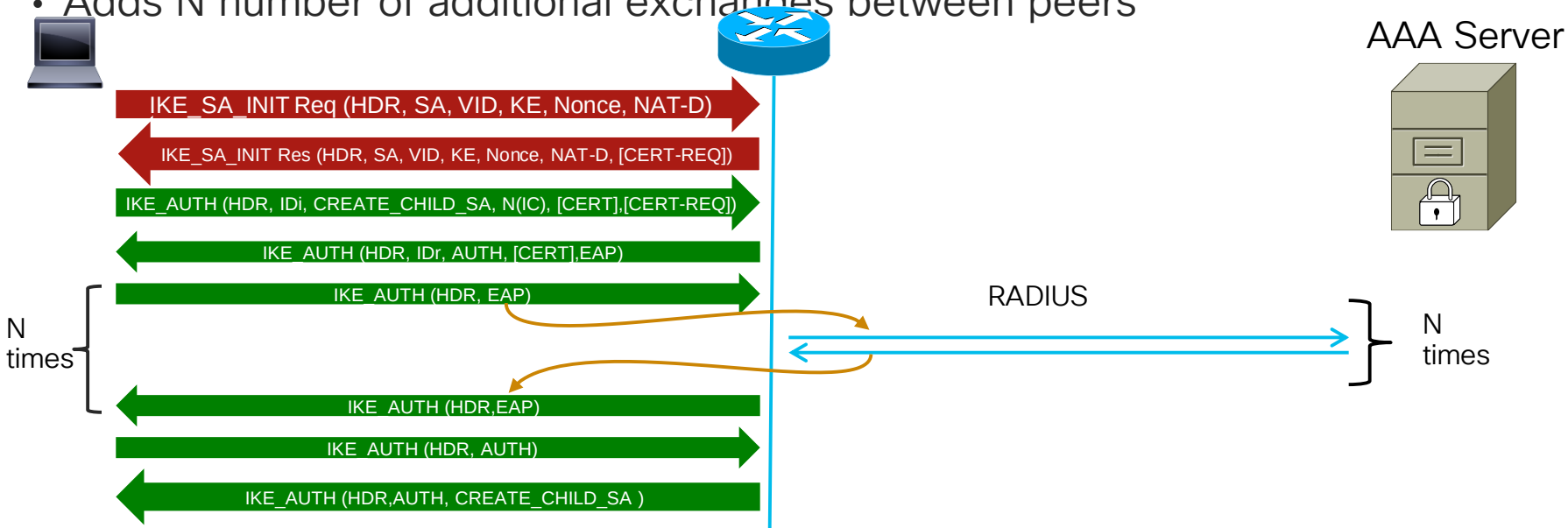
IKEv2 – Faster exchange right? Part 3

- EAP authentication of client
- EAP messages are carried within IKE_AUTH messages
- Adds multiple IKE exchanges back and forth between client and NAS
- N x exchanges – Depends on EAP method

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2 – EAP Authentication

- EAP authentication of client.
- Adds N number of additional exchanges between peers



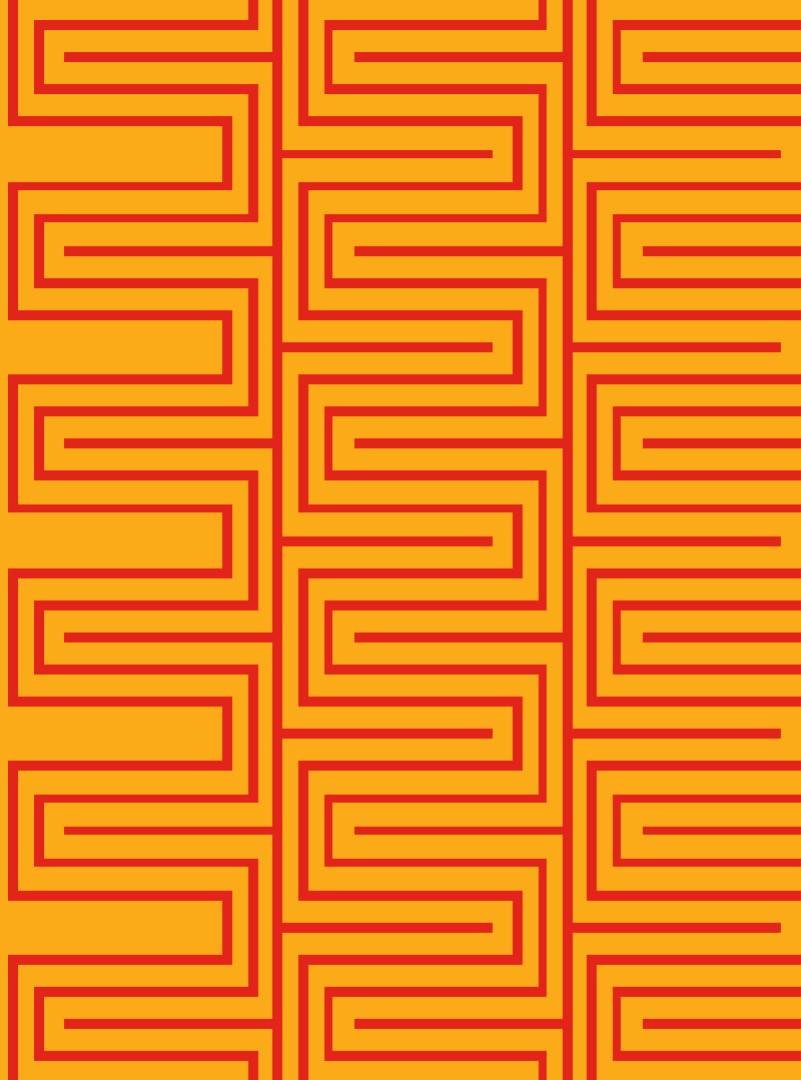
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2 – Faster exchange right? Part 4

- 4 packets for basic exchange
- +2 for Anti-spoofing (if detected)
- +2 for incorrect DH group
- +(2 x N) exchanges for EAP Authentication

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2’s shiny new abilities



IKEv2 – More Secure!!!!!

- Reuses encapsulation model from ESP for all IKEv2 messages
- Certificate Request are obfuscated
- Support for combined mode ciphers (AEAD)
- EAP versus XAUTH
  - No need for a group pre-shared-key
  - NAS never sees user/password in clear
- Initiator must prove identity first (except w/ EAP)
- Suite-B support – Next Gen Encryption
- Session keys are not based on PSK
  - Allows for scalable AAA based PSK lookup

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2 – Flexible Authentication Methods

- Unlike IKEv1, authentication is done uni-directionally in IKEv2
- Different pre-shared-keys can be used for local and remote
- Different authentication methods can be used for local and remote
- Example on IOS:

```
crypto ikev2 profile Profile1
 identity local fqdn hub.example.com
 authentication remote pre-share
 authentication remote eap
 authentication local rsa-sig
```

Peer can use either:

EAP

Pre-Shared-Key

We will use certificate

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2 – Attribute Exchange

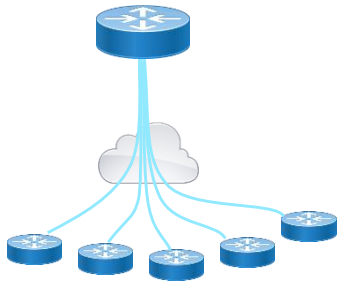
- Config Request/Reply – Solicited
  - Remote access use case:
    - IP address
    - DNS
    - WINS
    - Split-tunnel
- Config Set/Ack – Unsolicited
  - IKEv2 routing
  - Version info
  - Extensible for future

Typical DMVPN Tunnel Deployment

Every 5 seconds send:

74 byte EIGRP hello packet

168 byte ESP packet



175 MegaBytes per spoke, per month

$$$$$ if on metered ISP (4G, Satellite)

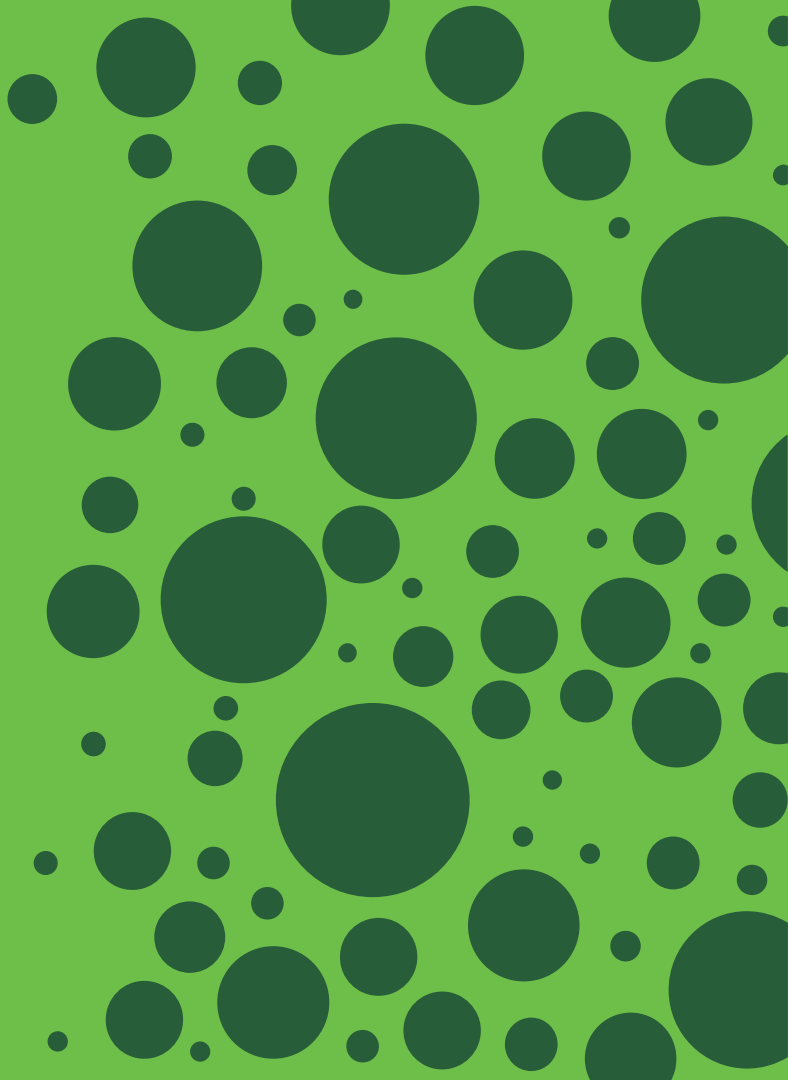
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2 – Fragmentation

- Large IKE messages make large UDP datagrams
- Packets get fragmented at IP layer
- Filtering/Blocking of fragments causes protocol failure
- **Solution**: Fragment at Application layer
- IKEv1 – Proprietary
  - Encrypt then segment across multiple UDP packets
- IKEv2 – Standard, RFC7383
  - Segment then encrypt

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Where to use?



ASA/FTD

- Can terminate both IKEv1 and IKEv2 site-to-site
- AnyConnect can use SSL or IKEv2/IPsec
- 3rd party IKEv2 remote access clients
- Support for Virtual Tunnel Interfaces*
- Support for policy based VPN (crypto map)

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN – Simplified IOS(-XE) implementation

- Smart defaults
- Virtual Tunnel Interface based (point-to-point)
- Interoperability
- Unified configuration
- Multiple redundancy options
- Simple config for basic topology
  - Customizable for complex network requirements
- More explicit and easier to understand debugs

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Almost everything is already taken care for you!

```
hostname site1
!
interface Tunnel0
  ip address 10.1.12.1 255.255.255.0
  tunnel source Ethernet0/1
  tunnel destination 172.18.3.52
  tunnel protection ipsec profile ipsecProf1
!
crypto ipsec profile ipsecProf1
  set ikev2-profile ikev2Prof1
!
crypto ikev2 profile ikev2Prof1
 match identity remote address 172.18.3.52 255.255.255.255
 authentication local pre-share key key2
 authentication remote pre-share key key1
```

Just provide:

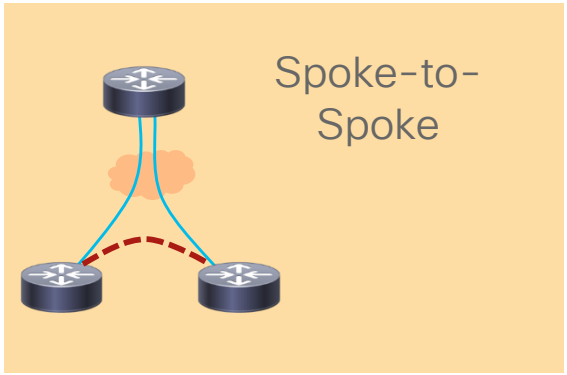
Who to connect to

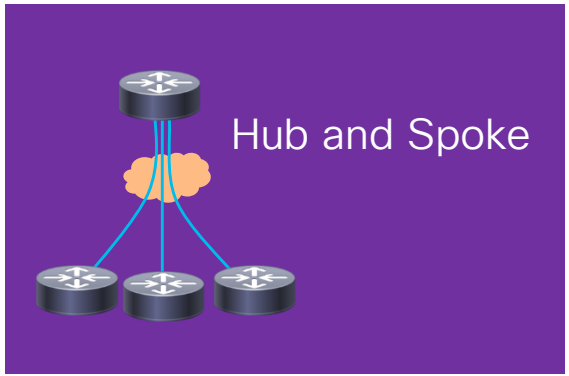
&

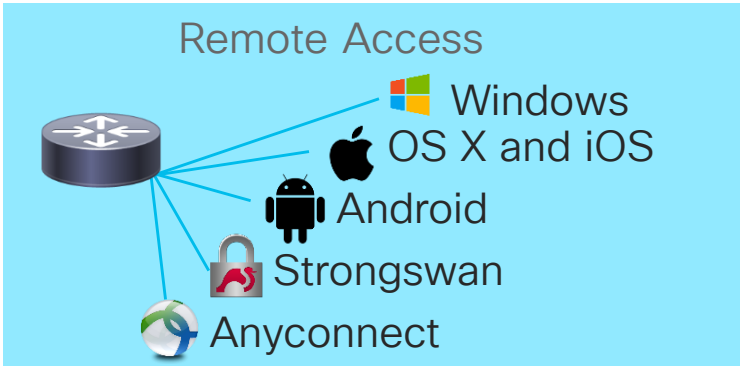
Password

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

FlexVPN Supported Deployment models:







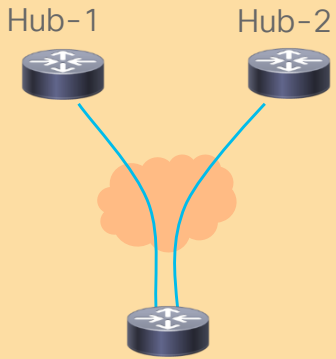
IKEv2 also supported with:

- DMVPN/iWAN 2.x
- Crypto maps
- GET-VPN (G-IKEv2)

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

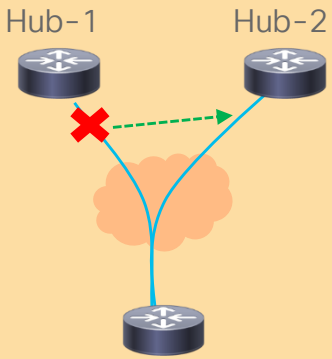
FlexVPN Redundancy models

Always On



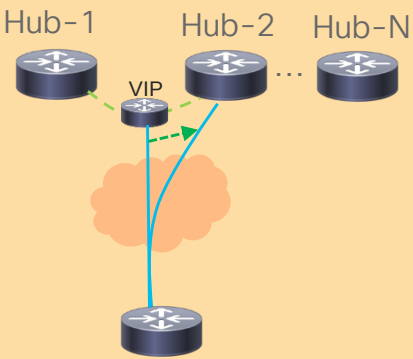
- Two Tunnels
- Routing Protocol
- Route around issue

Backup Peer



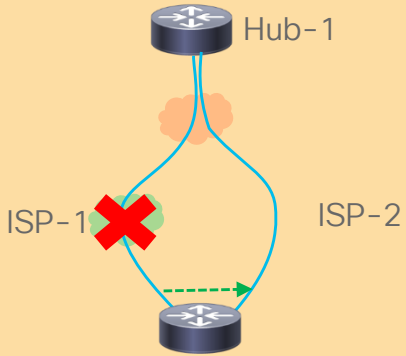
- One Tunnel
- Detect failure
- Contact backup

HSRP/IKEv2 Load Balancing Cluster



- One Tunnel
- Connect to Master
- Redirected to node

Tunnel Source Pivot



- One Tunnel
- 2 ISPs
- Change source of tunnel

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

IKEv2 – IOS better debugs

- Debugs are well structured and explicit
- Mirrors the protocol flow
- Delineates the transitions in Finite State Machine

```
IKEv2:(SESSION ID = 3,SA ID = 1):Sending Packet [To 172.20.5.43:500/From 172.18.3.52:500/VRF i0:f0]
Initiator SPI : 3D336F01678C442D - Responder SPI : 0000000000000000 Message id: 0
IKEv2 IKE_SA_INIT Exchange REQUEST
Payload contents:
 SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)  NOTIFY(NAT_DETECTION_DESTINATION_IP)
…
IKEv2:(SESSION ID = 3,SA ID = 1):Received Packet [From 172.20.5.43:500/To 172.18.3.52:500/VRF i0:f0]
Initiator SPI : 3D336F01678C442D - Responder SPI : 57A175F05AE0C0DC Message id: 0
IKEv2 IKE_SA_INIT Exchange RESPONSE
Payload contents:
 SA KE N VID VID NOTIFY(NAT_DETECTION_SOURCE_IP)  NOTIFY(NAT_DETECTION_DESTINATION_IP)
```


© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

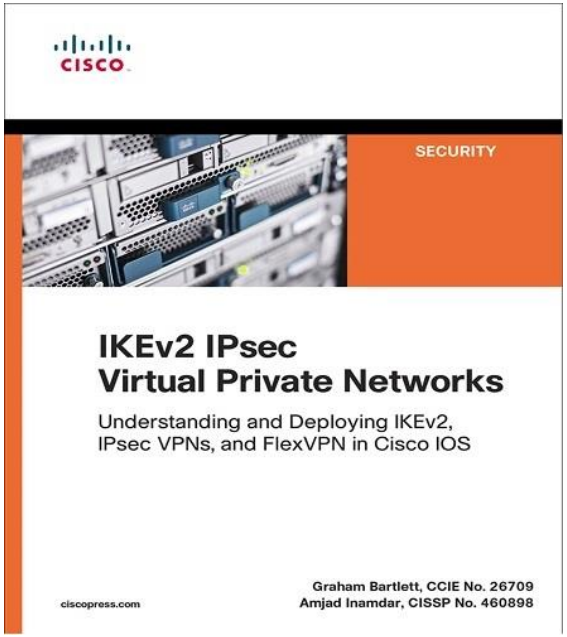
Related Sessions

- BRKSEC-2881 – Designing Remote-Access and Site-to-Site IPSec Networks with FlexVPN
  - Piotr Kupisiewicz – Cisco Services Customer Support Engineer
  - Today 1PM

- BRKSEC-3054 – IOS FlexVPN Remote Access, IoT and Site-to-Site advanced Crypto VPN Designs
  - Frederic Detienne – Cisco Services Distinguished Engineer
  - Piotr Kupisiewicz – Cisco Services Customer Support Engineer
  - Was on Monday – Checkout slides and recording

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco Press Book 'IKEv2 IPsec VPNs' by Amjad Inamdar & Graham Bartlett



https://www.amazon.com/IKEv2-IPsec-Virtual-Private Networks/dp/1587144603/

Listed in the CCIE Security reading list
https://learningnetwork.cisco.com/community/certifications/ccie_security/written_exam/study-material

Customer Reviews ★★★★★

One of the best technical books I've read
This book is the IKEv2 VPN equivalent of Jeff Doyle's Routing TCP/IP Vol 1 & 2 - a must read for any network security engineer wanting to design and build secure VPN's. One of the best technical books I've read.

Superb book and well worth the money for anyone even thinking about Cisco crypto
This book is the most comprehensive book on IKEv2 for Cisco network engineers that you will find and is all about real-world scenarios.

Definitive guide on modern IPsec VPN theory and practice
Many times I wish I had a book like this to help distill many complex IETF RFCs into "plain English" and provide practical and actionable security best practices.

Highly recommended for anyone on the CCIE Security track or anyone
If you need to really understand IKEv2 and FlexVPN, this is the book that will get you there. Be warned, it's not for the faint of heart ...

The best book on IKEv2 IPsec VPNs
The book is awesome! I appreciate authors' work on presenting deeply technical topics in extremely easy to understand manner.

Finally, all you need to know about FLEX in one place!
Well written , concise and accurate. An absolute must for anyone designing, supporting or troubleshooting IKEv2 VPNs. You too can become a FLEX expert!

Most comprehensive VPN reference
This the most comprehensive book on IKEv2 and IPSec I have come across. If anyone is interested in Cisco VPN solutions, this is the book to look for.

Extremely well written book on Nextgen Crypto VPN technologies
The authors have immense experience in the domain which is very evident in the way every topic is explained brilliantly. A must have book if you are into Security.!

Brilliant
It's well worth the money. I feel like I know the subject thoroughly now. I don't usually leave reviews but was motivated to in this instance. Good job, highly recommended.

Great Book
Very in depth and detail explanations. It has greatly enhanced my understanding of IKEv2, IPSec, and Cisco's implementations.

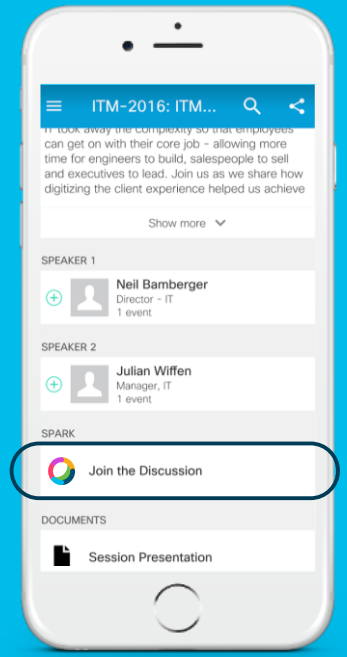
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Summary

Summary

- IKEv1 works well, but needed many add-ons to shine
- IKEv2 built those add-ons into standard
- IKEv2 easier to understand + troubleshoot
- IKEv2 has better security model + SuiteB support
- v1 and v2 are incompatible
- IOS (FlexVPN) simplifies config, allows vendor interoperability and highly scalable

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public



cs.co/ciscolivebot#BRKSEC-3001

Cisco Webex Teams

Questions?

Use Cisco Webex Teams (formerly Cisco Spark) to chat with the speaker after the session

How

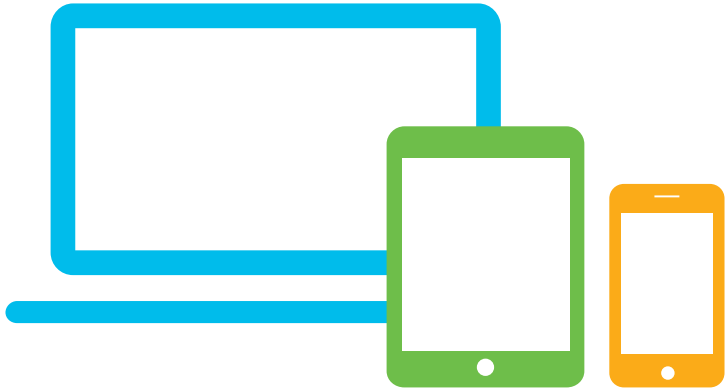
1. Find this session in the Cisco Events Mobile App
2. Click “Join the Discussion”
3. Install Webex Teams or go directly to the team space
4. Enter messages/questions in the team space

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Complete your online session survey

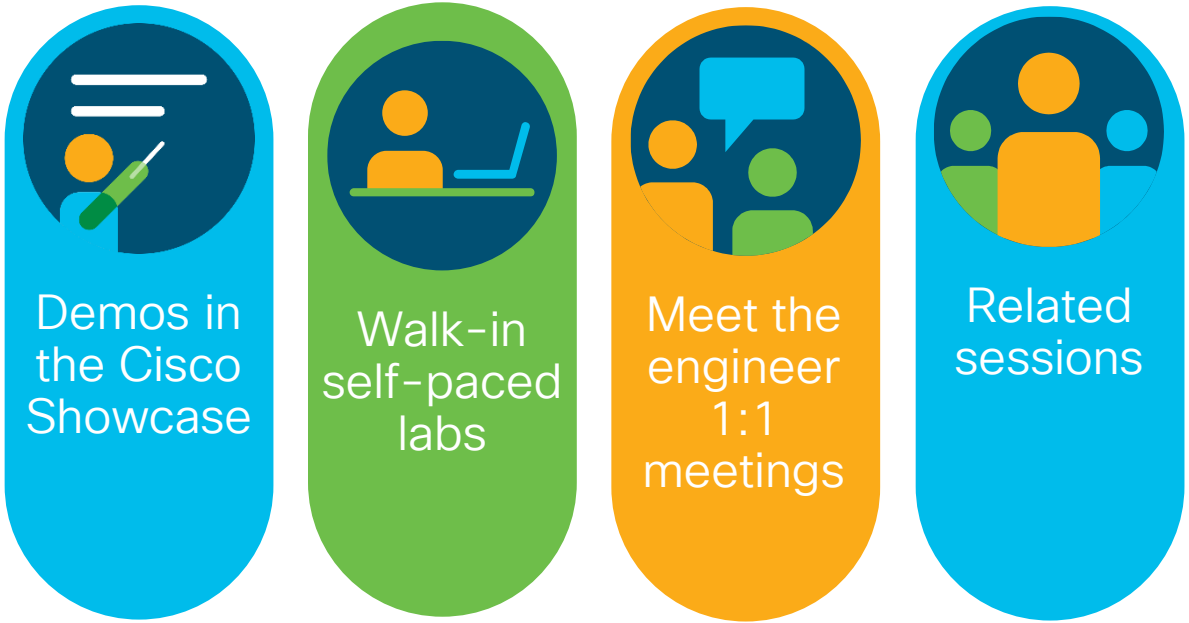
- Please complete your Online Session Survey after each session
- Complete 4 Session Surveys & the Overall Conference Survey (available from Thursday) to receive your Cisco Live T-shirt
- All surveys can be completed via the Cisco Events Mobile App or the Communication Stations

Don't forget: Cisco Live sessions will be available for viewing on demand after the event at ciscolive.cisco.com



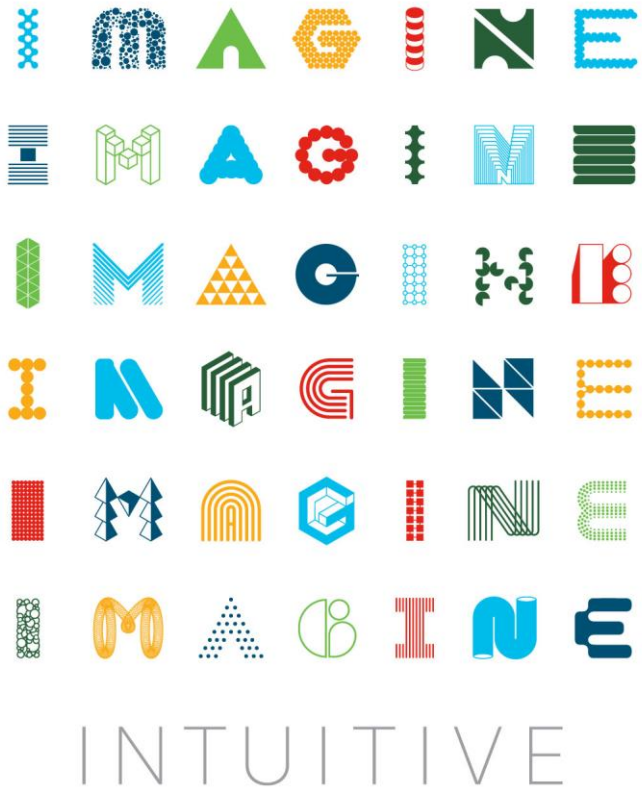
© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Continue Your Education



© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Thank you



INTUITIVE

Cybersecurity Cisco education offerings

Course	Description	Cisco Certification
Understanding Cisco Cybersecurity Fundamentals (SFUND)	The SECFND course provides understanding of cybersecurity's basic principles, foundational knowledge, and core skills needed to build a foundation for understanding more advanced cybersecurity material & skills.	CCNA® Cyber Ops
Implementing Cisco Cybersecurity Operations (SECOPS)	This course prepares candidates to begin a career within a Security Operations Center (SOC), working with Cybersecurity Analysts at the associate level.	CCNA® Cyber Ops
Cisco Security Product Training Courses	Official deep-dive, hands-on product training on Cisco's latest security products, including NGFW, ASA, NGIPS, AMP, Identity Services Engine, Email and Web Security Appliances, and much more.	

For more details, please visit: www.cisco.com/go/securitytraining or http://learningnetwork.cisco.com
Questions? Visit the Learning@Cisco Booth

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cybersecurity Cisco education offerings

Course	Description	Cisco Certification
CCIE Security 5.0		CCIE® Security
Implementing Cisco Edge Network Security Solutions (SENSS) Implementing Cisco Threat Control Solutions (SITCS) v1.5 Implementing Cisco Secure Access Solutions (SISAS) Implementing Cisco Secure Mobility Solutions (SIMOS)	Configure Cisco perimeter edge security solutions utilizing Cisco Switches, Cisco Routers, and Cisco Adaptive Security Appliance (ASA) Firewalls Implement Cisco's Next Generation Firewall (NGFW), FirePOWER NGIPS (Next Generation IPS), Cisco AMP (Advanced Malware Protection), as well as Web Security, Email Security and Cloud Web Security Deploy Cisco's Identity Services Engine and 802.1X secure network access Protect data traversing a public or shared infrastructure such as the Internet by implementing and maintaining Cisco VPN solutions	CCNP® Security
Implementing Cisco Network Security (IINS 3.0)	Focuses on the design, implementation, and monitoring of a comprehensive security policy, using Cisco IOS security features	CCNA® Security

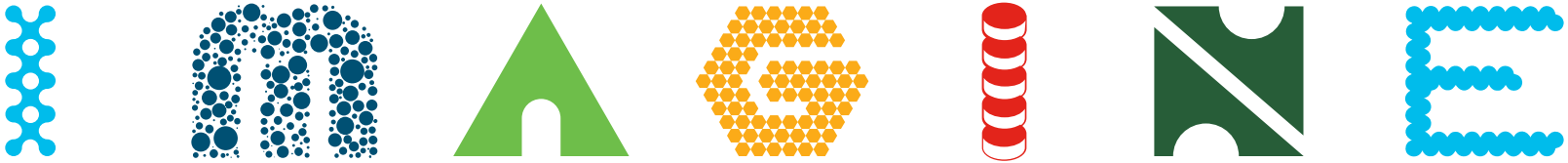
For more details, please visit: www.cisco.com/go/securitytraining or http://learningnetwork.cisco.com
Questions? Visit the Learning@Cisco Booth

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco live!

January 28 - February 1, 2019 - Barcelona

cisco



INTUITIVE