Pig-in-the-middle

TLS/QUIC Decryption, Encrypted Visibility Engine (and much more ☺)
Deep Dive on Cisco Secure Firewall

Christopher Grabowski
Technical Marketing Engineering
Technical Leader

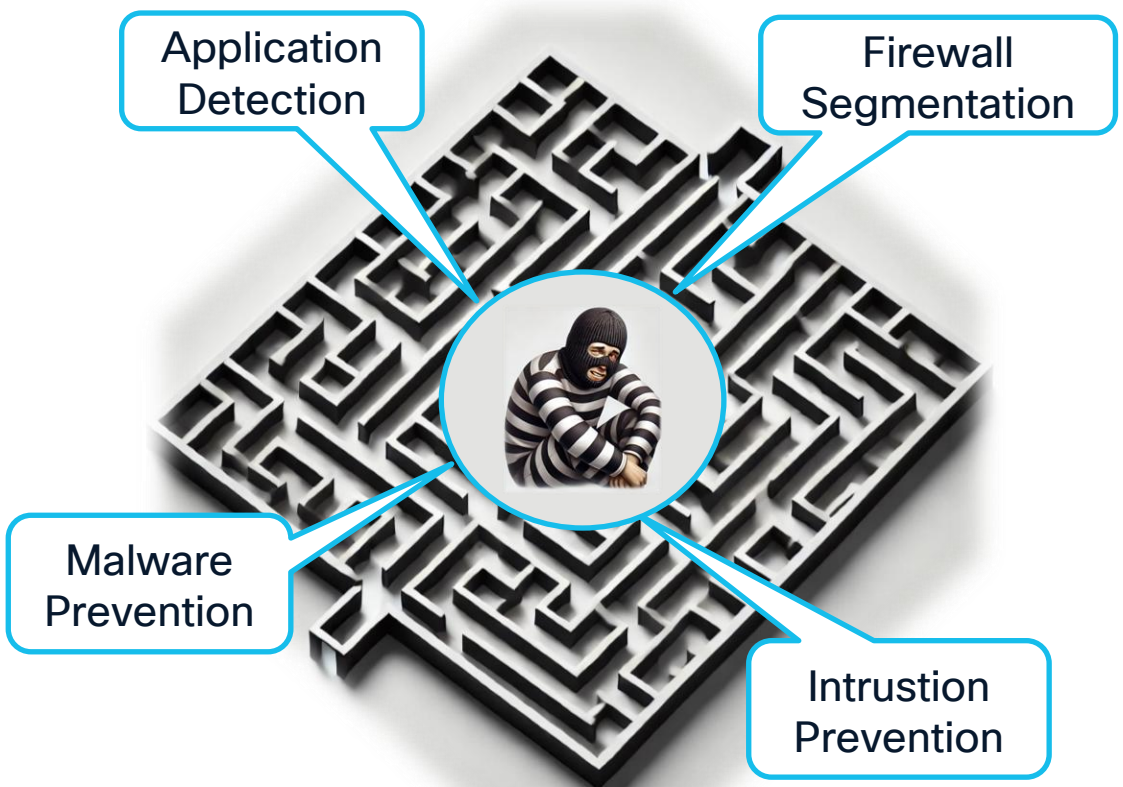
Session ID: BRKSEC-3320

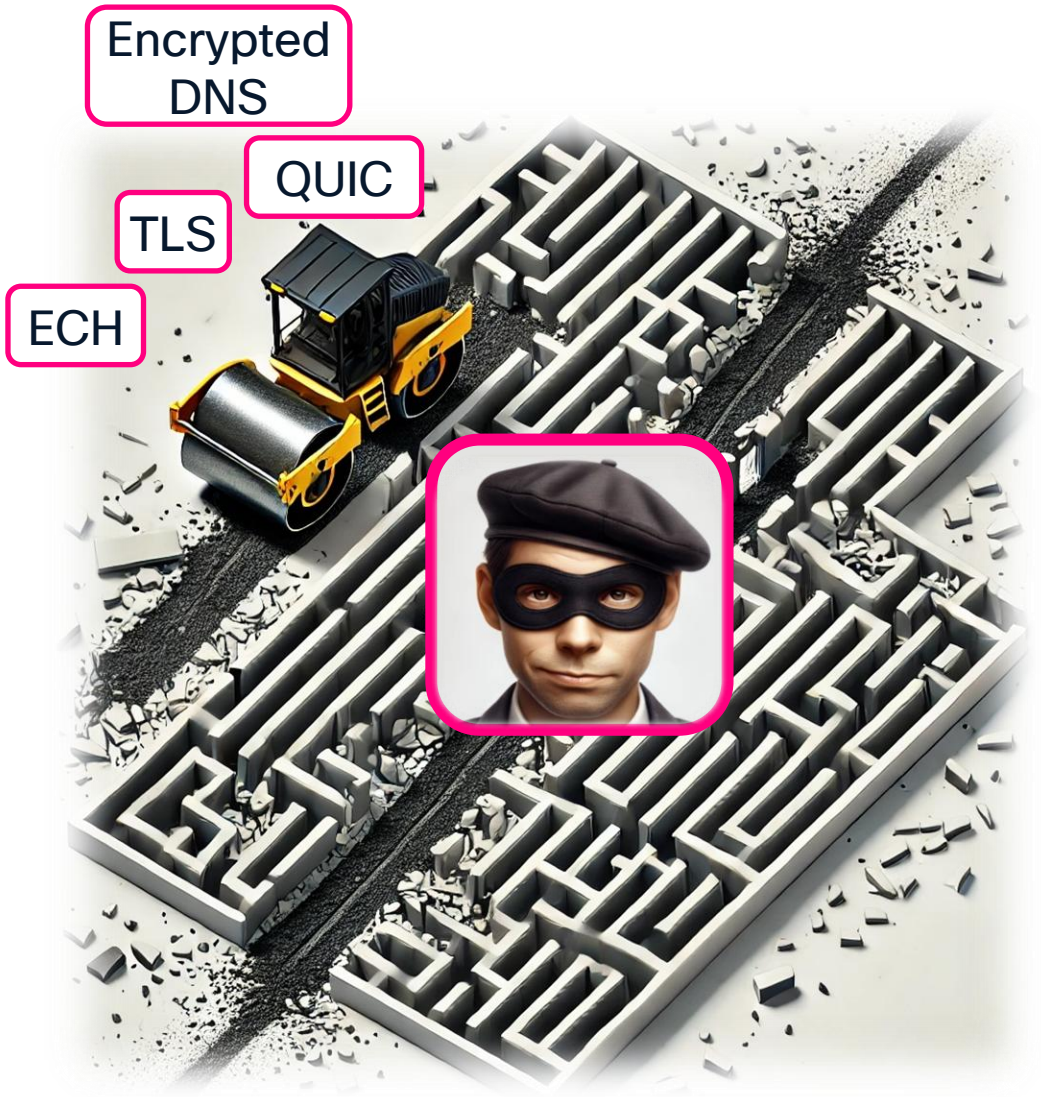
“The F-117 Nighthawk was a ‘silver bullet’, able to effortlessly penetrate the best-defended air spaces in the world by virtue of stealth”

Major Robert ‘Robson’ Donaldson describes taking the stealth fighter to war during Operation Desert Storm against Iraq.

With the evolving encryption stack, we may be soon finding ourselves staring at the radar – and realizing (OR NOT) it has gone dumb…

Security is just an obstacle course for an attacker





© 2025 Cisco and/or its affiliates. All rights reserved.

Without visibility, there is no security – the new encryption stack is making us blind

THE CHALLENGE: Security is Going Dark

- 50% of internet traffic now uses QUIC (bypasses TCP)
- Encrypted Client Hello (ECH) disables NGFW capabilities
- Certificate lifetimes dropping to 47 days by 2029
- Quantum computers will break current encryptions

THE SOLUTION: Cisco Secure Firewall Innovations

- ✓ QUIC decryption (GA) – inspect UDP-based encrypted traffic
- ✓ EVE (ML Engine) – detects threats and Apps without decryption
- ✓ Shadow Traffic Detection – find evasion attempts
- ✓ PQC ready hardware and automation enhancements

YOUR OUTCOMES TODAY

- ➢ Maintain visibility despite encryption trends
- ➢ Simplify decryption policy and automate certificate lifecycle
- ➢ Build awareness and sharpen your crypto-skills
- ➢ Plan ahead and build your readiness roadmap

© 2025 Cisco and/or its affiliates. All rights reserved.

Agenda

01 Introduction

02 TLS Handshake Walkthrough

03 The New Decryption UI

04 QUIC and EVE Updates

05 Detecting Shadow Traffic

06 Encrypted Client Hello

07 Certificate Management

08 Post Quantum vs. TLS

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Cisco Webex App

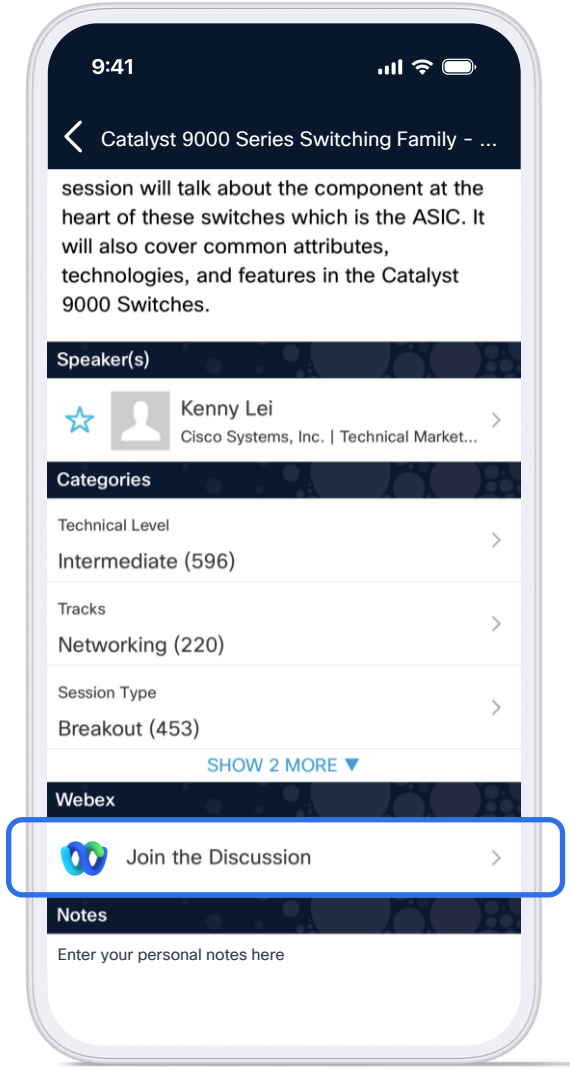
Questions?

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 14 November 2025.



https://ciscolive.ciscoevents.com/
ciscolivebot/**#BRKSEC-3320**

© 2025 Cisco and/or its affiliates. All rights reserved.

Your Speaker

- Based in Warsaw, Poland
- With Cisco since May 2012
- Started with TAC Security, then Advanced Services, now Technical Marketing Engineer
- Focusing on Identity Firewall, Integrations and TLS Decryption
- Enjoys cooking and spending time with the family

Christopher Grabowski
Technical Marketing Engineer
CCIE Security #42466

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

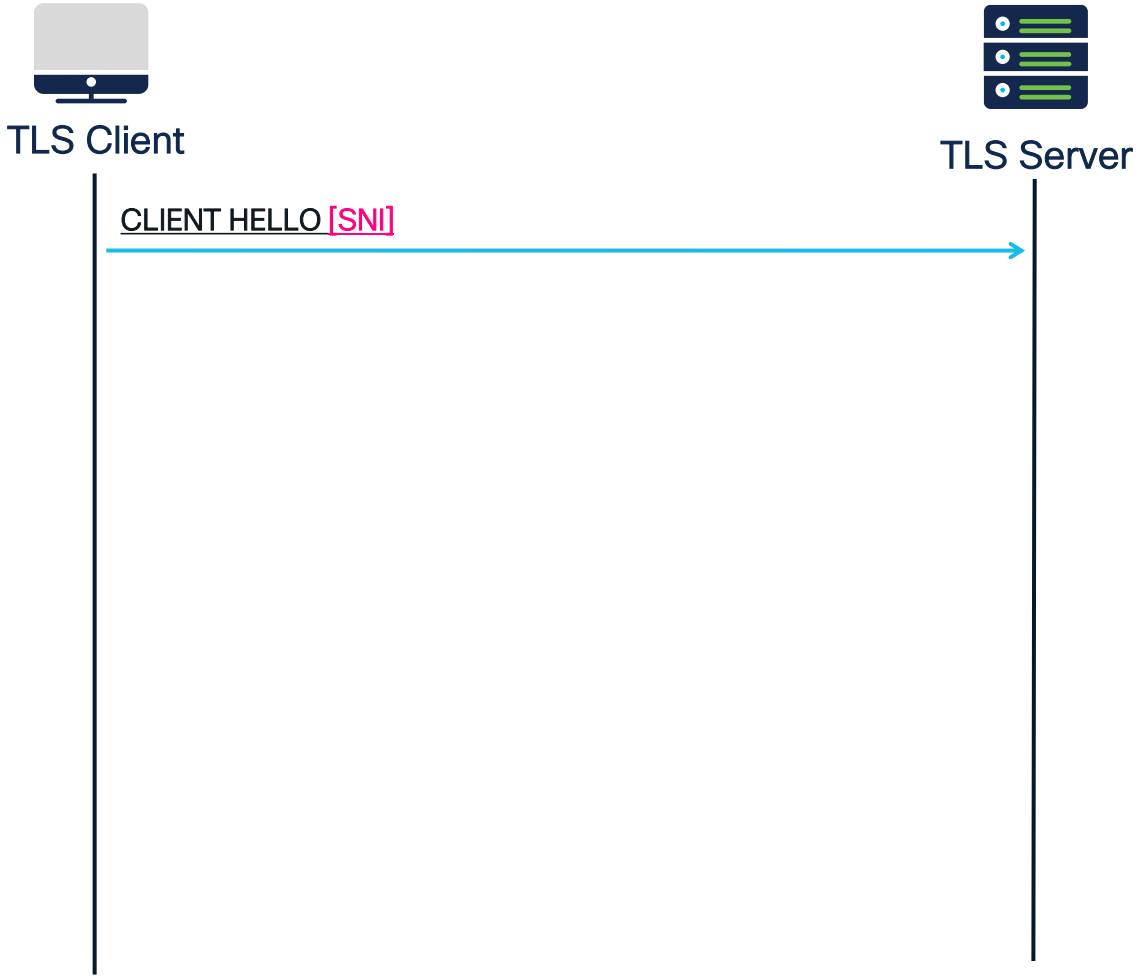
WARNING !

This presentation may cause elevated geek levels over an extended period of time

VIEWER DISCRETION IS ADVISED

TLS Handshake

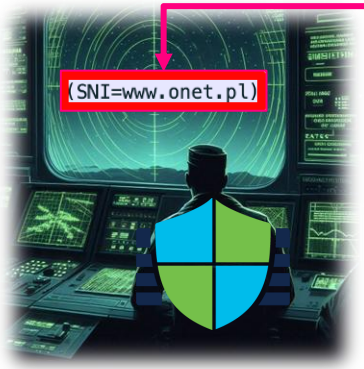
TLS 1.3 Handshake At a Glance



© 2025 Cisco and/or its affiliates. All rights reserved.

Firewall enforcement heavily relies on this single TLS extension

	Time	Source	SPORT	Destination	DPORT	Protocol	Length	Info
1	0.000000	172.16.136.96	49934	18.239.83.46	443	TCP	66	49934 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.000500	18.239.83.46	443	172.16.136.96	49934	TCP	66	443 → 49934 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
3	0.000547	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=1 Ack=1 Win=2097408 Len=0
4	0.000780	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	585	Client Hello (SNI=www.onet.pl)



URL Category and Reputation

Selective TLS/QUIC decryption

Advanced inspection:
- IPS
- Malware protection
- TID (URLs, Hashes)

Security Intelligence URLs

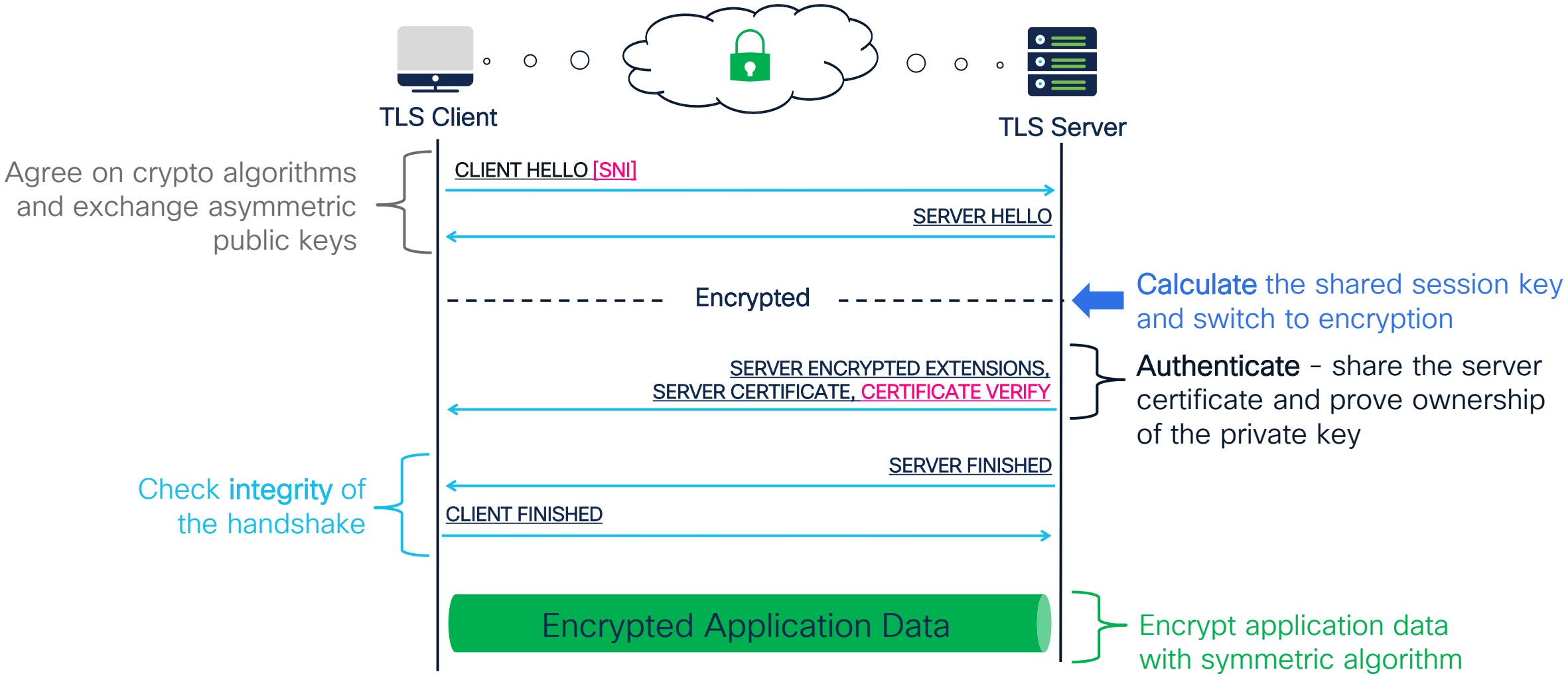
AppID

TLS Server Identity Probe

(Prevent SNI spoofing and improve decryption accuracy)

© 2025 Cisco and/or its affiliates. All rights reserved.

TLS 1.3 Handshake At a Glance



© 2025 Cisco and/or its affiliates. All rights reserved.

How quickly does Snort stop inspecting connections?

With decryption enabled, Snort continued inspection (column available in 7.7+) for 10s of packets.

Event Type	Action	Source IP	Destination IP	Destination Port / ICMP Code	TLS Client SNI	Inspected Packets	TLS Actual Action	EVE Process Name
Connection	Allow	172.16.136.96	18.239.83.82	**443** (https) / tcp	www.onet.pl	21	Decrypt (Resign)	chromium browser
Connection	Allow	172.16.136.96	18.239.83.82	**443** (https) / tcp	www.onet.pl	76	Decrypt (Resign)	chromium browser

Without decryption, the inspection stops after only 4 packets

Event Type	Action	Source IP	Destination IP	Destination Port / ICMP Code	TLS Client SNI	Inspected Packets	TLS Actual Action	EVE Process Name
Connection	Allow	172.16.136.96	18.239.83.46	**443** (https) / tcp	www.onet.pl	4	Do Not Decrypt	chromium browser
Connection	Allow	172.16.136.96	18.239.83.46	**443** (https) / tcp	www.onet.pl	4	Do Not Decrypt	chromium browser

... and the firewall looks at the TCP handshake the initial TLS message from the client:

	Time	Source	SPORT	Destination	DPORT	Protocol	Length	Info
1	0.000000	172.16.136.96	49934	18.239.83.46	443	TCP	66	49934 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.000500	18.239.83.46	443	172.16.136.96	49934	TCP	66	443 → 49934 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
3	0.000547	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=1 Ack=1 Win=2097408 Len=0
4	0.000780	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	585	Client Hello (SNI=www.onet.pl)

© 2025 Cisco and/or its affiliates. All rights reserved.

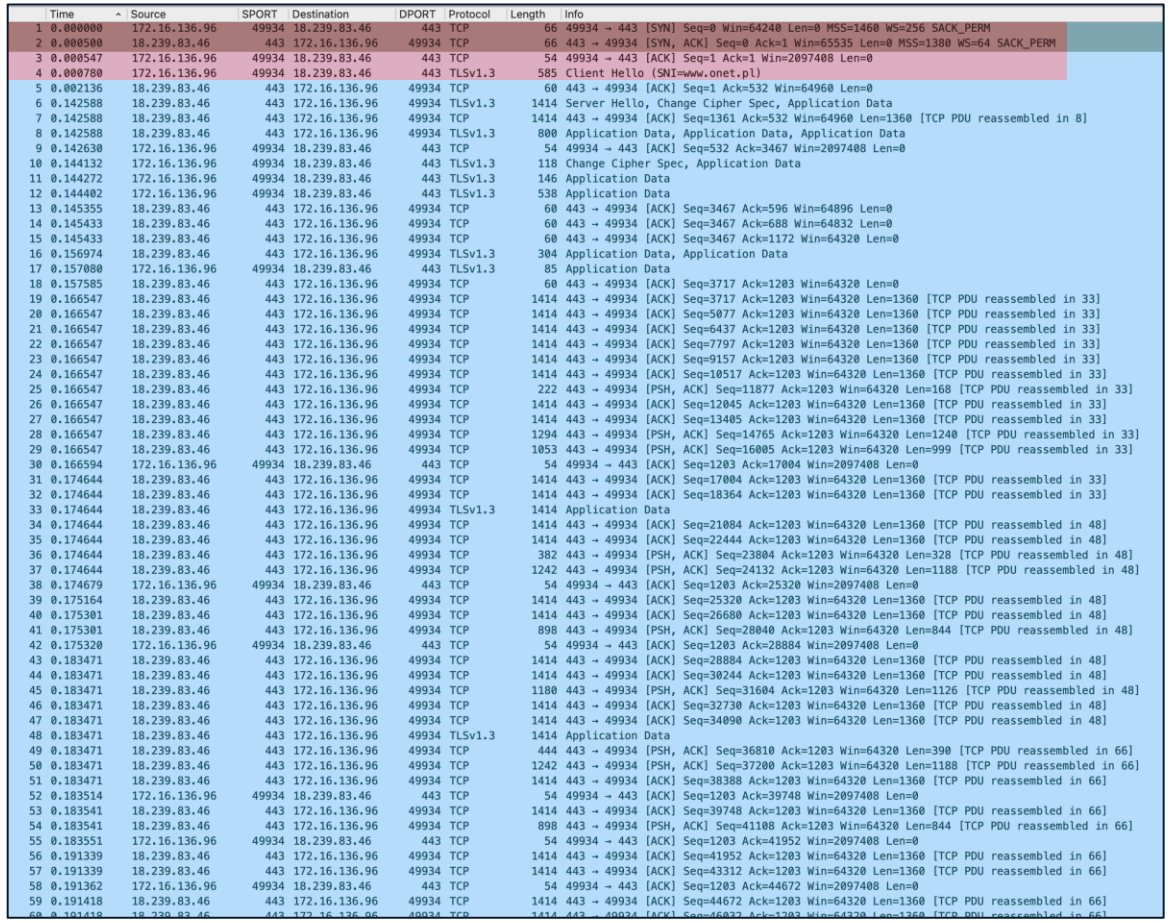
cisco

Without decryption, we are essentially blind after the initial handshake...

Inspection scope without TLS/QUIC decryption.

(4 packets ...)

Wireshark packet capture (HTTPs connection to https://onet.pl)



	Time	Source	SPORT	Destination	DPORT	Protocol	Length	Info
1	0.000000	172.16.136.96	49934	18.239.83.46	443	TCP	66	49934 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.000500	18.239.83.46	443	172.16.136.96	49934	TCP	66	443 → 49934 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=64 SACK_PERM
3	0.000547	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=1 Ack=1 Win=2097408 Len=0
4	0.000780	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	585	Client Hello (SNI=www.onet.pl)
5	0.002136	18.239.83.46	443	172.16.136.96	49934	TCP	60	443 → 49934 [ACK] Seq=1 Ack=532 Win=64960 Len=0
6	0.142588	18.239.83.46	443	172.16.136.96	49934	TLSv1.3	1414	Server Hello, Change Cipher Spec, Application Data
7	0.142588	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=1361 Ack=532 Win=64960 Len=1360 [TCP PDU reassembled in 8]
8	0.142588	18.239.83.46	443	172.16.136.96	49934	TLSv1.3	800	Application Data, Application Data, Application Data
9	0.142630	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=532 Ack=3467 Win=2097408 Len=0
10	0.144132	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	118	Change Cipher Spec, Application Data
11	0.144272	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	146	Application Data
12	0.144402	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	538	Application Data
13	0.145355	18.239.83.46	443	172.16.136.96	49934	TCP	60	443 → 49934 [ACK] Seq=3467 Ack=596 Win=64896 Len=0
14	0.145433	18.239.83.46	443	172.16.136.96	49934	TCP	60	443 → 49934 [ACK] Seq=3467 Ack=688 Win=64832 Len=0
15	0.145433	18.239.83.46	443	172.16.136.96	49934	TCP	60	443 → 49934 [ACK] Seq=3467 Ack=1172 Win=64320 Len=0
16	0.156974	18.239.83.46	443	172.16.136.96	49934	TLSv1.3	304	Application Data, Application Data
17	0.157080	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	85	Application Data
18	0.157585	18.239.83.46	443	172.16.136.96	49934	TCP	60	443 → 49934 [ACK] Seq=3717 Ack=1203 Win=64320 Len=0
19	0.166547	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=3717 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33]
20	0.166547	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=5077 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33]
21	0.166547	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=6437 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33]
22	0.166547	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=7797 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33]
23	0.166547	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=9157 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33]
24	0.166547	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=10517 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33]
25	0.166547	18.239.83.46	443	172.16.136.96	49934	TCP	222	443 → 49934 [PSH, ACK] Seq=11877 Ack=1203 Win=64320 Len=168 [TCP PDU reassembled in 33]
26	0.166547	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=12045 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33]
27	0.166547	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=13405 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33]
28	0.166547	18.239.83.46	443	172.16.136.96	49934	TCP	1294	443 → 49934 [PSH, ACK] Seq=14765 Ack=1203 Win=64320 Len=1240 [TCP PDU reassembled in 33]
29	0.166547	18.239.83.46	443	172.16.136.96	49934	TCP	1053	443 → 49934 [PSH, ACK] Seq=16005 Ack=1203 Win=64320 Len=999 [TCP PDU reassembled in 33]
30	0.166594	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=1203 Ack=17004 Win=2097408 Len=0
31	0.174644	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=17004 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33]
32	0.174644	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=18364 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 33]
33	0.174644	18.239.83.46	443	172.16.136.96	49934	TLSv1.3	1414	Application Data
34	0.174644	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=21084 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48]
35	0.174644	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=22444 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48]
36	0.174644	18.239.83.46	443	172.16.136.96	49934	TCP	382	443 → 49934 [PSH, ACK] Seq=23804 Ack=1203 Win=64320 Len=328 [TCP PDU reassembled in 48]
37	0.174644	18.239.83.46	443	172.16.136.96	49934	TCP	1242	443 → 49934 [PSH, ACK] Seq=24132 Ack=1203 Win=64320 Len=1188 [TCP PDU reassembled in 48]
38	0.174679	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=1203 Ack=25320 Win=2097408 Len=0
39	0.175164	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=25320 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48]
40	0.175301	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=26680 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48]
41	0.175301	18.239.83.46	443	172.16.136.96	49934	TCP	898	443 → 49934 [PSH, ACK] Seq=28040 Ack=1203 Win=64320 Len=844 [TCP PDU reassembled in 48]
42	0.175320	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=1203 Ack=28884 Win=2097408 Len=0
43	0.183471	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=28884 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48]
44	0.183471	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=30244 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48]
45	0.183471	18.239.83.46	443	172.16.136.96	49934	TCP	1180	443 → 49934 [PSH, ACK] Seq=31604 Ack=1203 Win=64320 Len=1126 [TCP PDU reassembled in 48]
46	0.183471	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=32730 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48]
47	0.183471	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=34090 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 48]
48	0.183471	18.239.83.46	443	172.16.136.96	49934	TLSv1.3	1414	Application Data
49	0.183471	18.239.83.46	443	172.16.136.96	49934	TCP	444	443 → 49934 [PSH, ACK] Seq=36810 Ack=1203 Win=64320 Len=390 [TCP PDU reassembled in 66]
50	0.183471	18.239.83.46	443	172.16.136.96	49934	TCP	1242	443 → 49934 [PSH, ACK] Seq=37200 Ack=1203 Win=64320 Len=1188 [TCP PDU reassembled in 66]
51	0.183471	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=38388 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 66]
52	0.183514	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=1203 Ack=39748 Win=2097408 Len=0
53	0.183541	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=39748 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 66]
54	0.183541	18.239.83.46	443	172.16.136.96	49934	TCP	898	443 → 49934 [PSH, ACK] Seq=41108 Ack=1203 Win=64320 Len=844 [TCP PDU reassembled in 66]
55	0.183551	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=1203 Ack=41952 Win=2097408 Len=0
56	0.191339	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=41952 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 66]
57	0.191339	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=43312 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 66]
58	0.191362	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=1203 Ack=44672 Win=2097408 Len=0
59	0.191418	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=44672 Ack=1203 Win=64320 Len=1360 [TCP PDU reassembled in 66]

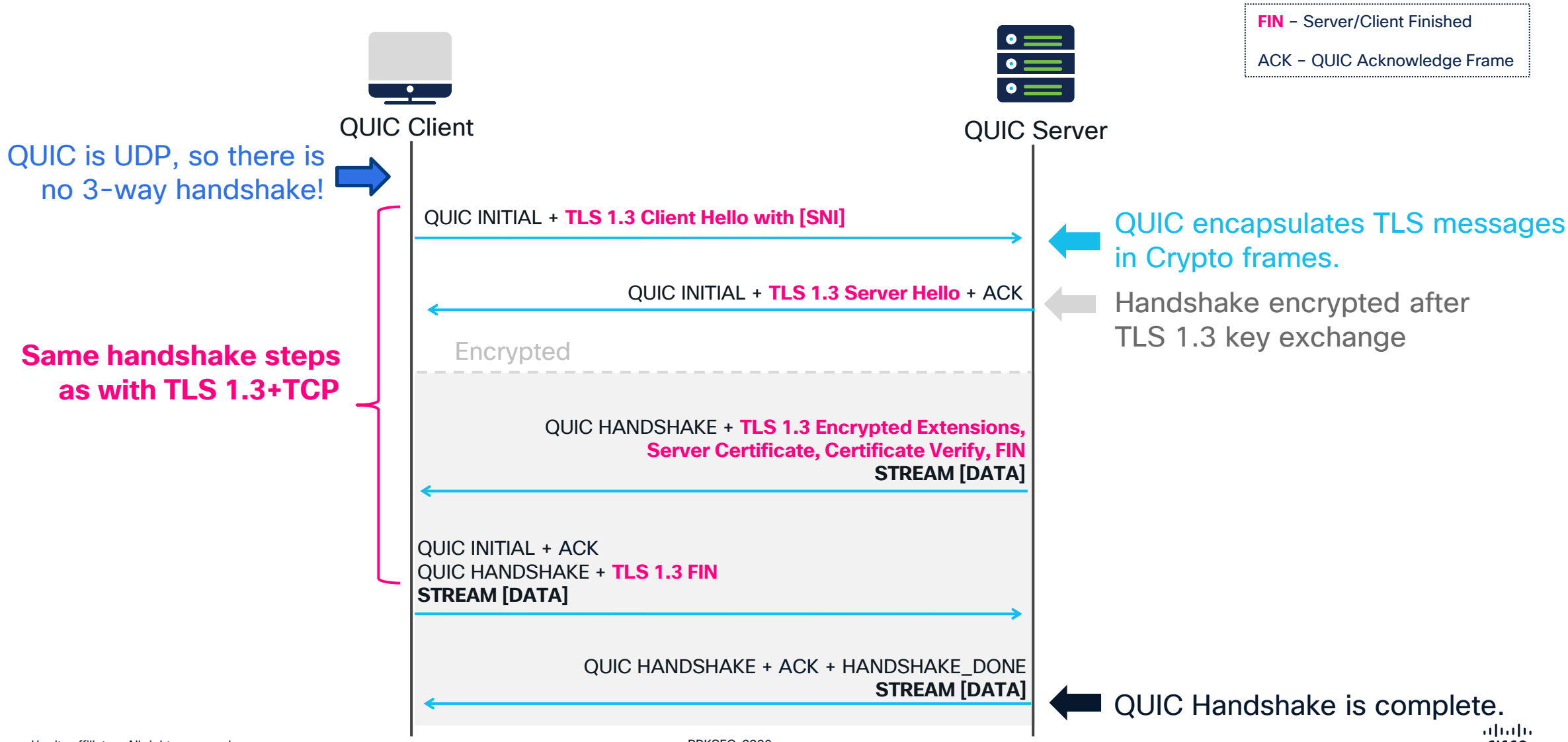
With decryption, Snort disengages after preempting all checks.

(as many packets as needed)

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Understanding a QUIC session handshake



© 2025 Cisco and/or its affiliates. All rights reserved.

TLS Handshake – Key Takeaways

- SNI is visible in cleartext and drives 80%+ of security stack decisions
- TLS 1.3 and QUIC protect most of the handshake, but SNI remains exposed
- Without decryption, inspection drops after ~4 packets (vs. full session with decryption)
- QUIC uses TLS 1.3 natively, eliminates TCP 3-way handshake and has its own flow control

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Revamped Decryption User Interface

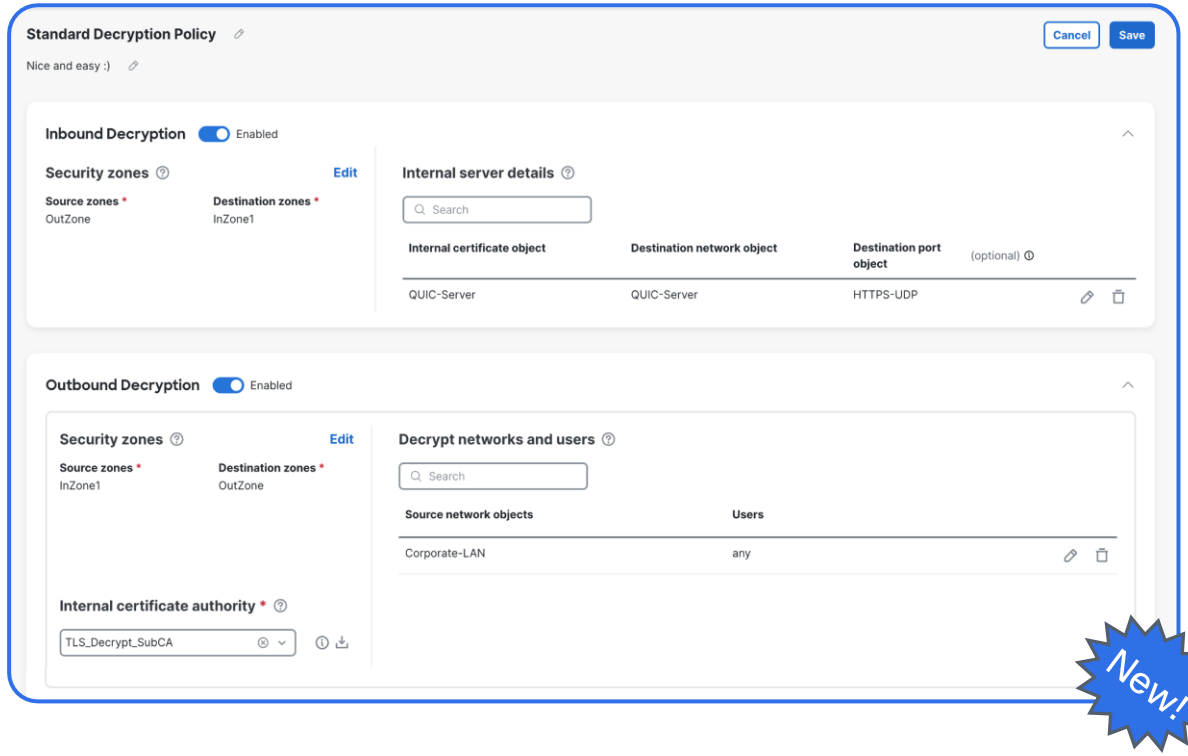
The New Simplified Decryption Configuration Workflow

Rule-based Decryption Policy

#	Name	Dest Networks	Applications	Categories	SSL	Action
Administrator Rules						
This category is empty						
Standard Rules						
1	Inbound-Decrypt-1160dfefd2	QUIC-Server	*any*	*any*	1 Cert Status selection	Decrypt - Replace Cert
2	Block-Certificate-Status	*any*	*any*	*any*	3 Cert Status selections	Block with reset
3	Block-TLS-Version	*any*	*any*	*any*	3 Protocol Versions	Block with reset
4	Bypass-Trusted-Connections	*any*	*any*	Any (Except Uncatego	1 Client Threat selection	Do not decrypt
5	Bypass-Undecryptable-Sites (Disabled)	*any*	*any*	*any*	1 DN selection	Do not decrypt
6	Bypass-Apps	*any*	YouTube YouTube Kids YouTube Music YouTube TV (6 more...)	*any*	*any*	Do not decrypt
7	Bypass-Undecryptable-Apps	*any*	Tags: undecryptable	*any*	*any*	Do not decrypt
8	Bypass-Categories	*any*	*any*	Finance (Any reputatio Health and Medicine (Online Trading (Any re	*any*	Do not decrypt
9	Outbound-Decrypt-8fda97de48	*any*	*any*	*any*	*any*	Decrypt - Resign
Root Rules						
This category is empty						
Default Action						Do not decrypt

Traditional, granular mode for specialized configurations.

Standard Decryption Policy



No ruleset to manage, simple guided configuration with predefined bypasses!

© 2025 Cisco and/or its affiliates. All rights reserved.

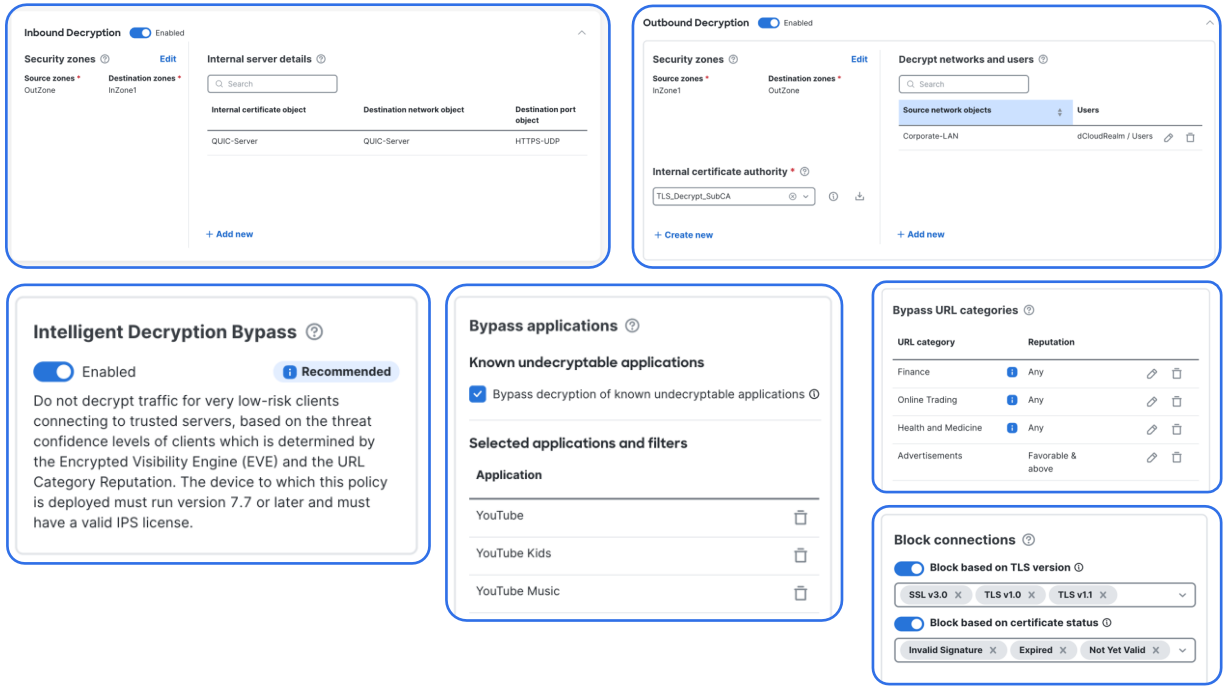
The New Simplified Decryption Configuration Workflow

Rule-based Decryption Policy

Custom DND Exceptions for Inbound	(IP/Port based)
Known Key – Server Protection	(IP/Port based)
Custom DND Exceptions / Bypass for Outbound	(IP/Port based)
Custom DND Exceptions for Outbound (Specific: URLs, DNs, Applications)	
Do Not Decrypt (DND) Undecryptable, Pinned, Legaly Prohibited (URL Categories, Application Groups, DN Lists)	
Key Resign – Outbound Client Protection (URL Categories, Application Groups)	
Default Do Not Decrypt	

- Classic, **granular rule-by-rule control**
- **Requires careful rule ordering** to avoid decryption conflicts
- Recommended for **complex and exceptional use-cases**

Standard Decryption Policy

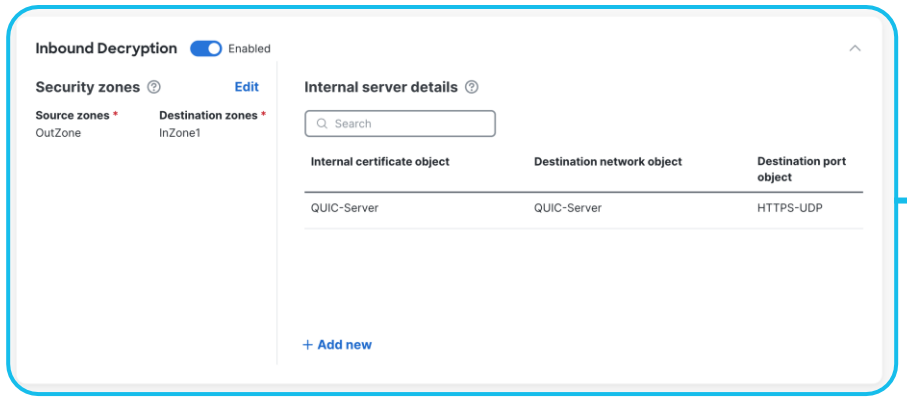


- **Single-page** setup with a clear, **intuitive workflow**
- Organised, **tiled layout** for inbound, outbound, bypass, and block policies
- Rule order automatically managed – **focus on intent, not sequence**

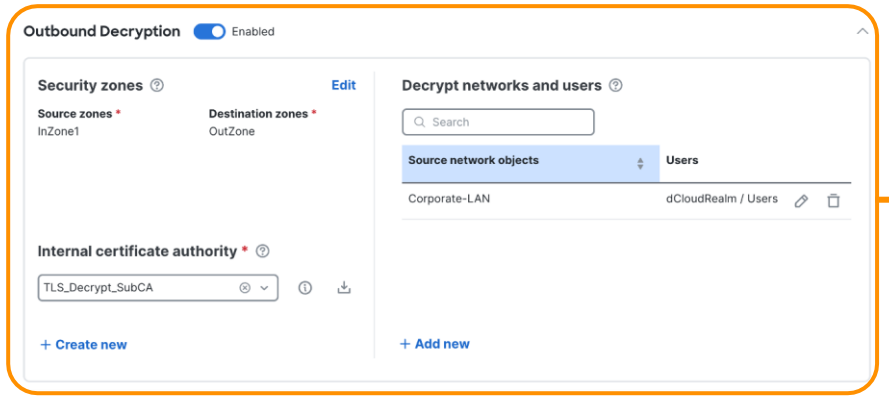
© 2025 Cisco and/or its affiliates. All rights reserved.

Decryption Policy in 4 Simple Steps

Step1: Specify your servers for decryption



Step 2: Set protected networks and users



TLS Handshake

Automatic ordering

Inbound Decryption

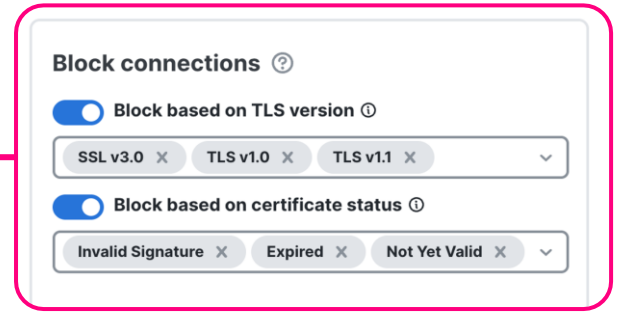
Block Insecure Handshake

Bypass Decryption

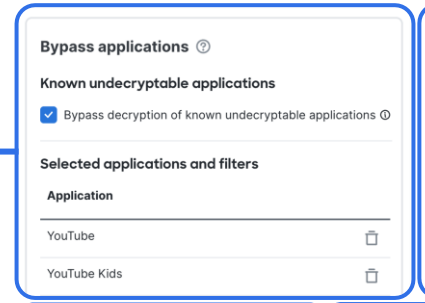
Outbound Decryption

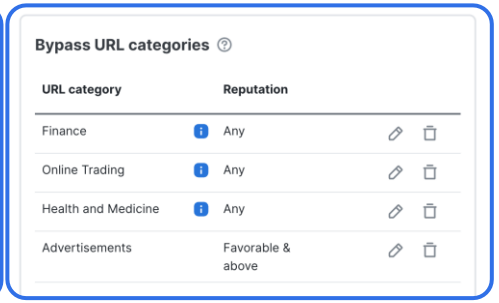
Decryption verdict

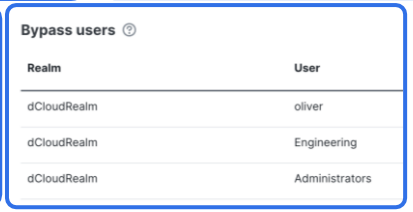
Step 4: Block weak ciphers and bad certificates



Step 3: Exempt Apps, URLs, Users etc...







© 2025 Cisco and/or its affiliates. All rights reserved.

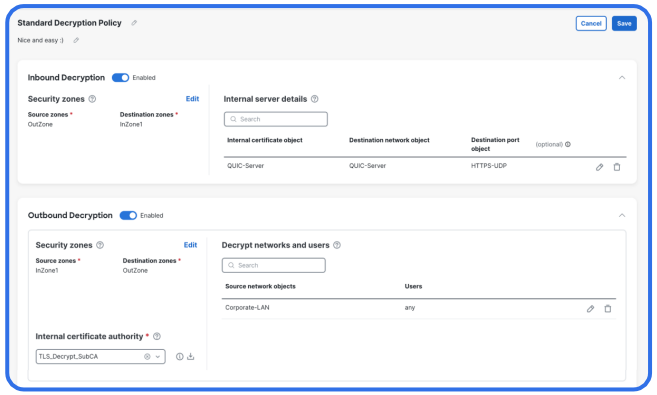
DEMO:

Simplified Decryption User Interface

© 2025 Cisco and/or its affiliates. All rights reserved.

New Decryption UI – Key Takeaways

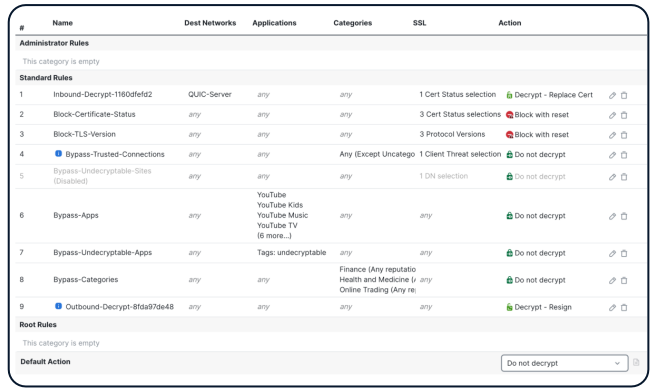
- **Start your journey with the Standard Decryption Policy** – intuitive, fast, and powerful
- Enjoy **90% of the capabilities** with a fraction of the setup effort – don't worry about the rule order, centrally manage exemptions (Apps, URLs, Users)
- Advanced and brown field stay with the **Rule-Based Policy for complex** conditional logic
- Convert **Standard to Rule-Based if needed** in one step



Standard Decryption Policy

Convert Policy Mode

(one way road)



Rule-based Decryption Policy

© 2025 Cisco and/or its affiliates. All rights reserved.

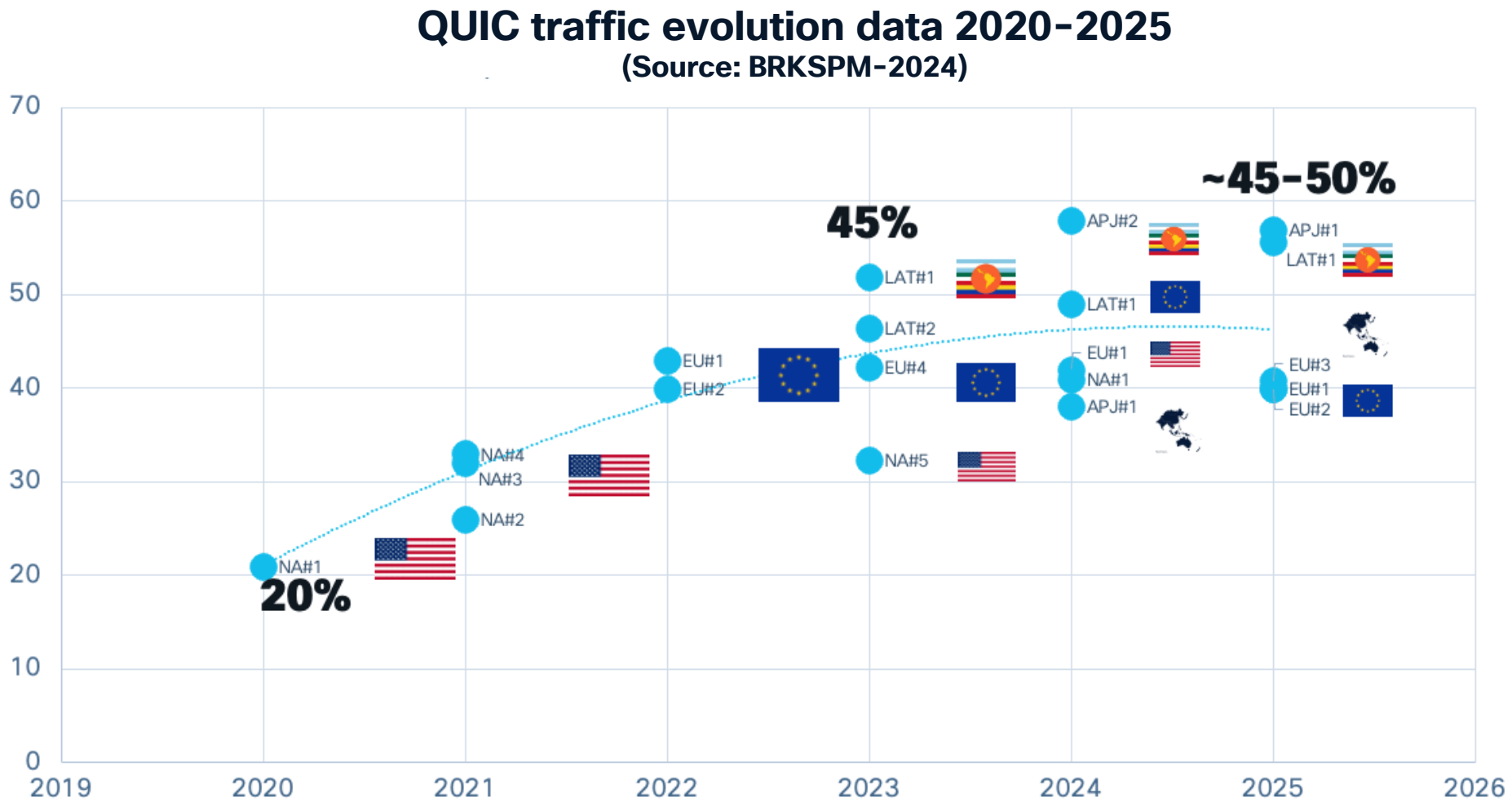
Convert Decryption Policy to Rule-Based

Cisco Secure Firewall 10.0

QUIC Update

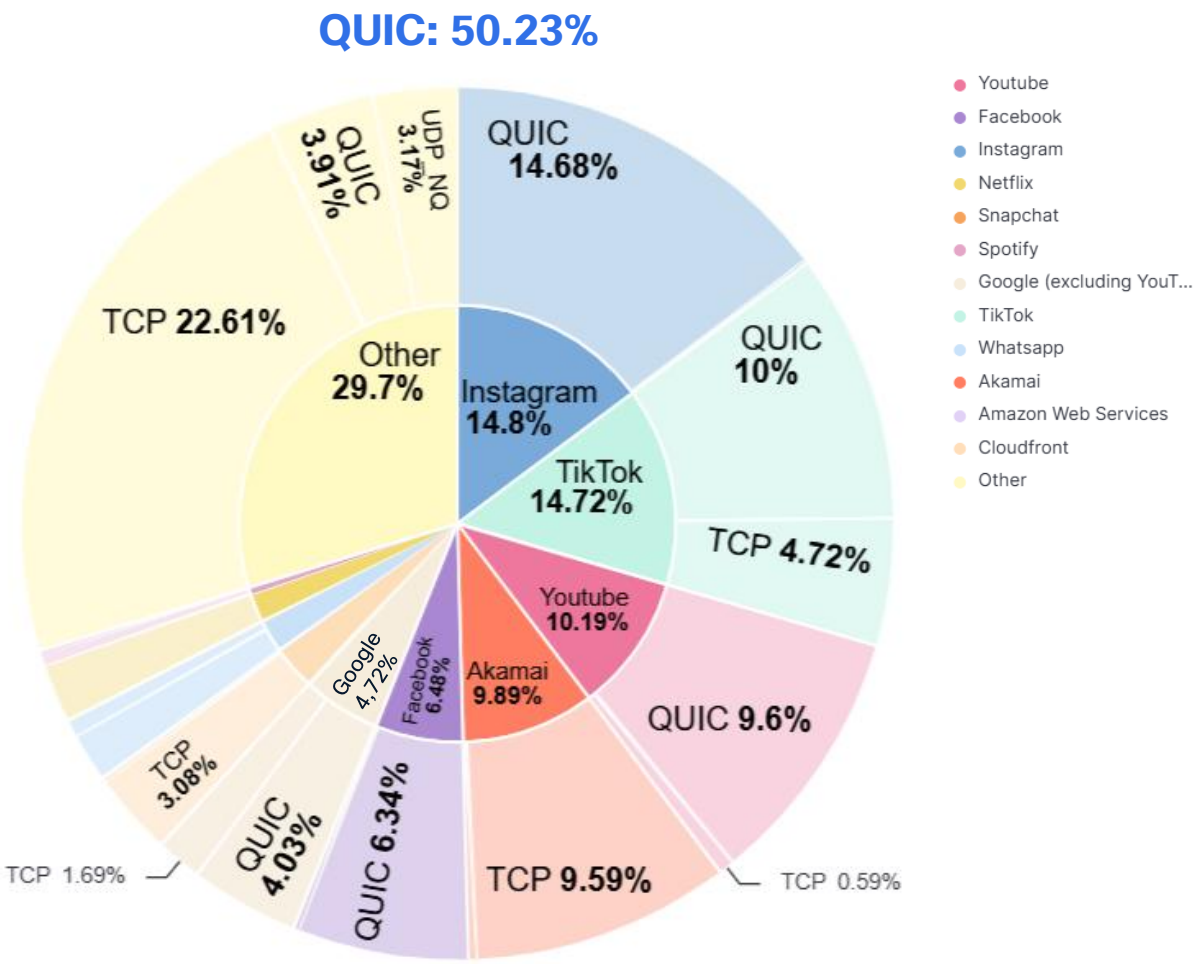
QUIC is no longer a niche protocol

For more stats on QUIC check: BRKSPM-2024

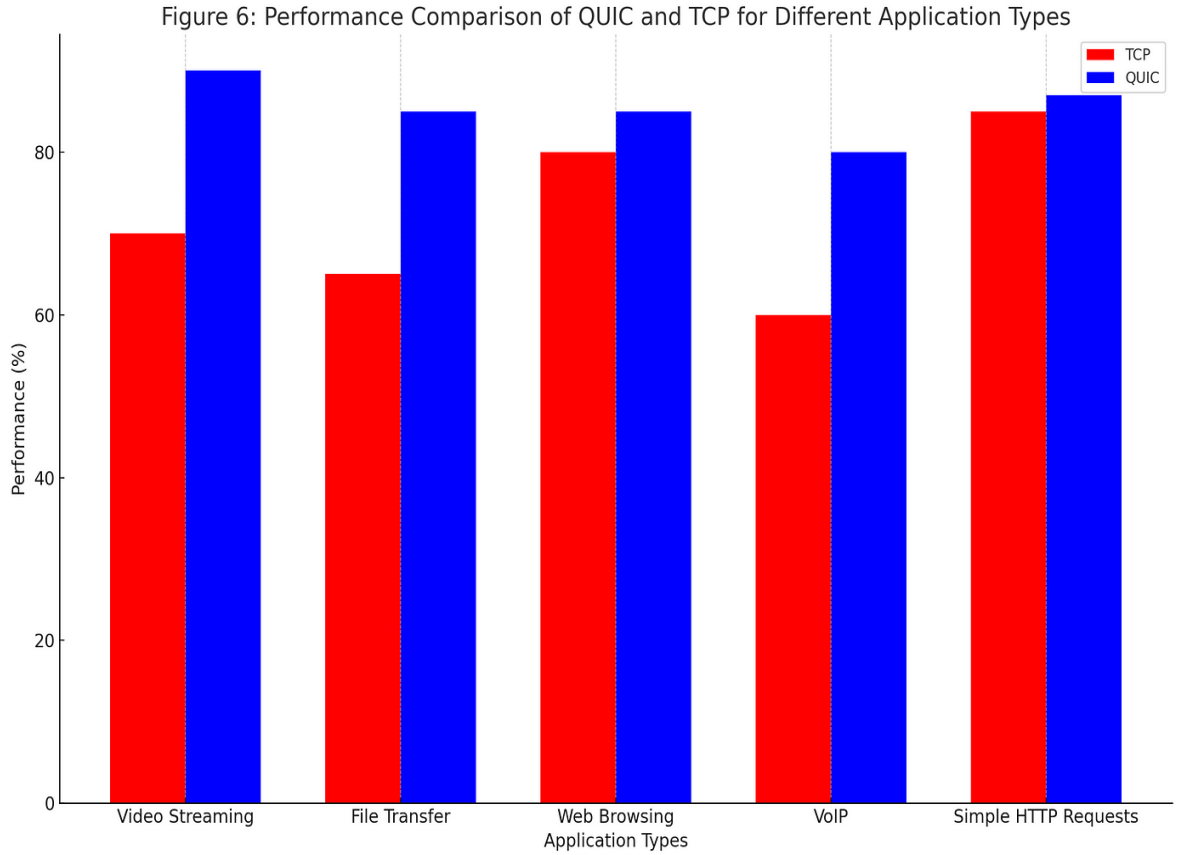


© 2025 Cisco and/or its affiliates. All rights reserved.

The benefits of QUIC make it the first-choice protocol



Europe 2025 (Service Provider Network)

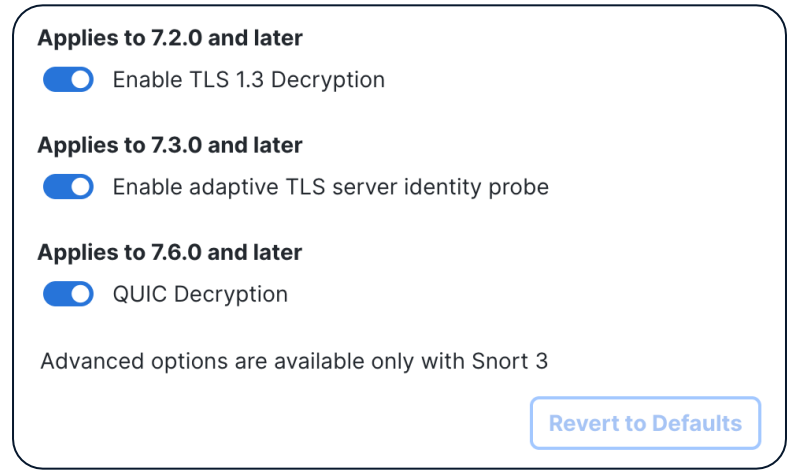


© 2025 Cisco and/or its affiliates. All rights reserved.

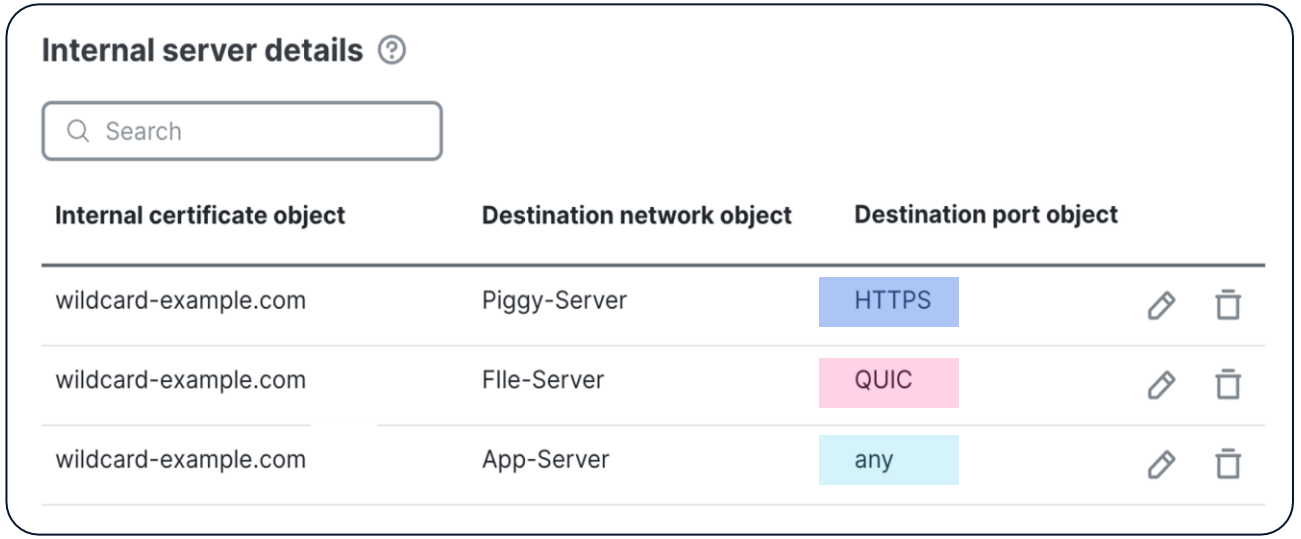
cisco

QUIC Decryption on Cisco Secure Firewall

- QUIC uses TLS 1.3 for negotiation – we follow the same decryption logic as with TLS
- QUIC is general availability in 10.0 – one click to enable



- Seamless use in the decryption policy determined by selected port object:
  - TCP – matches TLS connections
  - UDP – matches QUIC connections only
  - Any – matches both QUIC and TLS connections

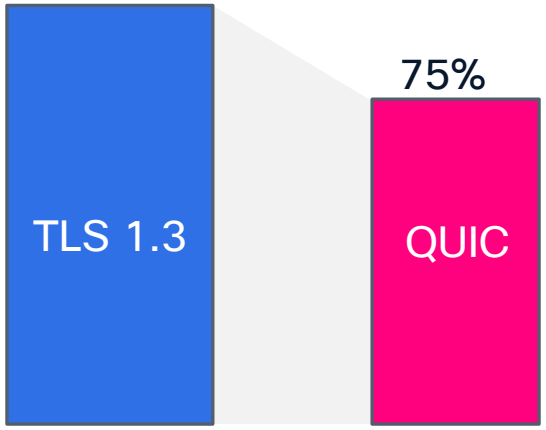


© 2025 Cisco and/or its affiliates. All rights reserved.

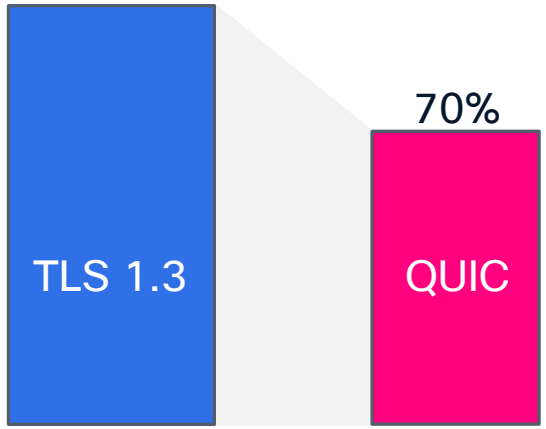
QUIC Decryption Considerations

- **Inbound decryption**
  - Supported for all browsers
  - Tested servers: NGINX, NGNIXProxy, NGTCP/2, angie, aioquic, tquic, quiche, HA-Proxy, Caddy, OLS, H2O
  - Tested clients: Curl, NGTCP/2, aioquic, neqo, quiche, tquic, msquic, HA-Proxy, Caddy, OLS, H2O
- **Outbound decryption** supported on Firefox and Safari; Chromium blocks trusted CA store for certificate check in QUIC connections
- **Cluster and high availability** – decrypted session states are not synchronized – existing flows must re-establish upon switchover (same behavior as with TLS)
- **QUICv2 support planned in CY26**

Decryption Throughput*



Decryption New Conn/Sec*



* – average expected results; actual performance may vary by hardware model and traffic profile

© 2025 Cisco and/or its affiliates. All rights reserved.

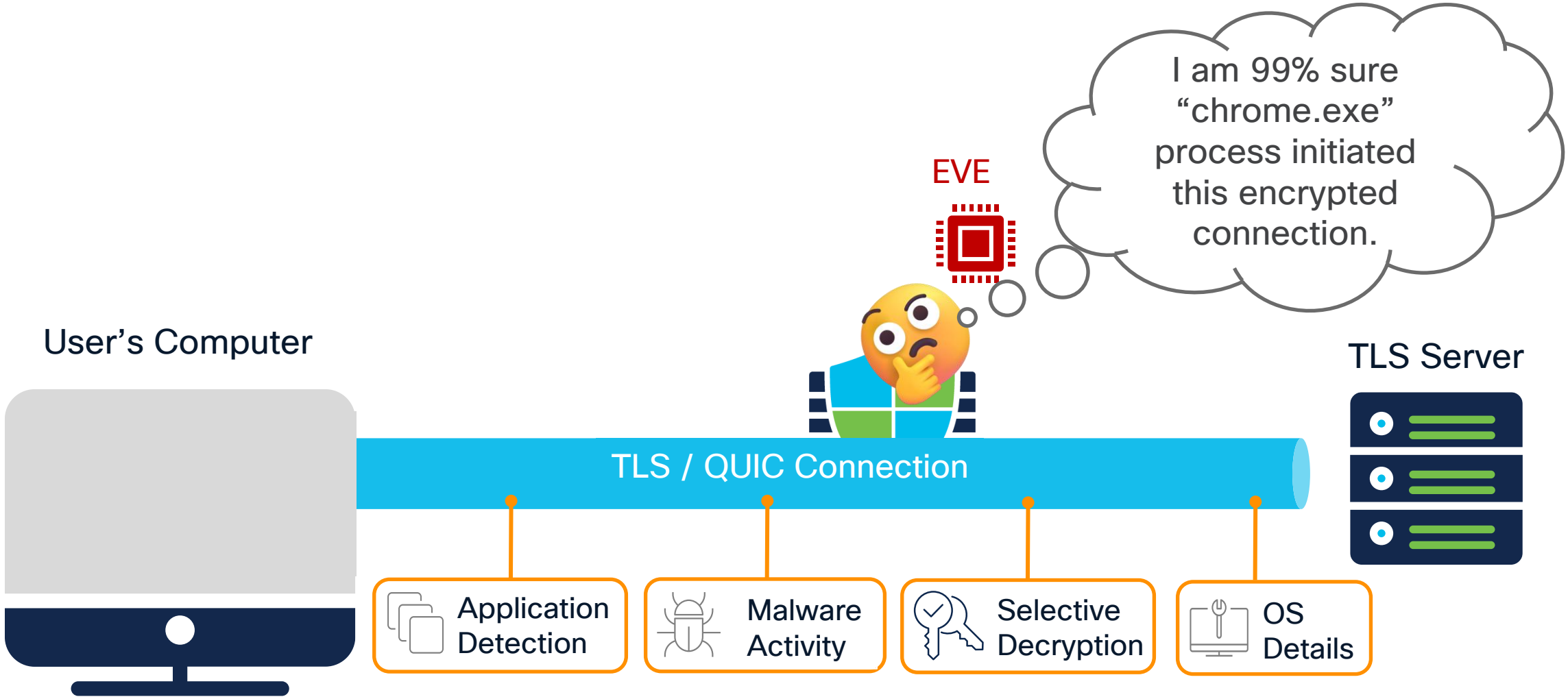
QUIC – Key Takeways

- **QUIC is now mainstream** (50% adoption) - performance benefits make it the first-choice protocol for modern applications - block major
- **QUIC decryption is production-ready** – General availability on Cisco Secure Firewall 10.0, same decryption principles as with TLS 1.3
- **Performance trade-off is reasonable** – 70-75% performance of TLS 1.3 decryption.
- **Inbound use-case fully supported –** protect your QUIC servers today!
- **Outbound use-case is tricky, consider 3 options:**
  - **Block QUIC traffic with AppID –** most secure and performant; may break some Apps
  - **Decrypt all outbound QUIC –** works for Firefox and Safari; triggers downgrade on Chromium; may break some apps
  - **Selective decryption + blocking with AppID –** requires ongoing monitoring and tweaking - consider blocking or excluding major contributors from your QUIC decryption policy (YouTube, Tik-Tok, Instagram, Facebook).

© 2025 Cisco and/or its affiliates. All rights reserved.

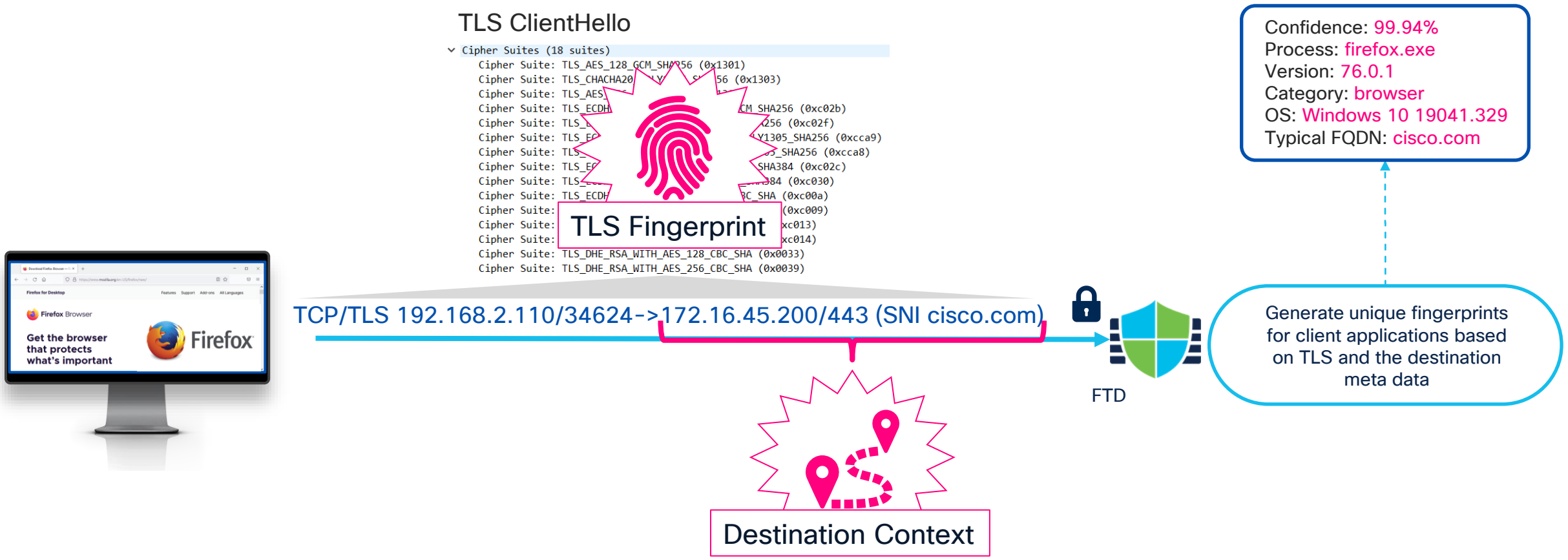
Encrypted Visibility Engine

What Does Encrypted Visibility Engine Provide?



© 2025 Cisco and/or its affiliates. All rights reserved.

Encrypted Visibility Engine Relies on TLS Fingerprints and Destination Context



© 2025 Cisco and/or its affiliates. All rights reserved.

EVE evaluates a single packet in TLS/QUIC handshake – independently from decryption setup

	Time	Source	SPORT	Destination	DPORT	Protocol	Length	Info
1	0.000000	172.16.136.96	49934	18.239.83.46	443	TCP	66	49934 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.000500	18.239.83.46	443	172.16.136.96	49934	TCP	66	443 → 49934 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1380 WS=64 SACK_PERM
3	0.000547	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=1 Ack=1 Win=2097408 Len=0
4	0.000780	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	585	Client Hello (SNI=www.onet.pl)
5	0.002136	18.239.83.46	443	172.16.136.96	49934	TCP	60	443 → 49934 [ACK] Seq=1 Ack=532 Win=64960 Len=0
6	0.142588	18.239.83.46	443	172.16.136.96	49934	TLSv1.3	1414	Server Hello, Change Cipher Spec, Application Data
7	0.142588	18.239.83.46	443	172.16.136.96	49934	TCP	1414	443 → 49934 [ACK] Seq=1361 Ack=532 Win=64960 Len=1360 [TCP PDU reassembled in 8]
8	0.142588	18.239.83.46	443	172.16.136.96	49934	TLSv1.3	800	Application Data, Application Data, Application Data
9	0.142630	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=532 Ack=3467 Win=2097408 Len=0
10	0.144132	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	118	Change Cipher Spec, Application Data
11	0.144272	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	146	Application Data
12	0.144402	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	538	Application Data
13	0.145355	18.239.83.46	443	172.16.136.96	49934	TCP	60	443 → 49934 [ACK] Seq=3467 Ack=596 Win=64896 Len=0
14	0.145433	18.239.83.46	443	172.16.136.96	49934	TCP	60	443 → 49934 [ACK] Seq=3467 Ack=688 Win=64832 Len=0
15	0.145433	18.239.83.46	443	172.16.136.96	49934	TCP	60	443 → 49934 [ACK] Seq=3467 Ack=1172 Win=64320 Len=0
16	0.156974	18.239.83.46	443	172.16.136.96	49934	TLSv1.3	304	Application Data, Application Data

QUIC looks at TLS Client Hello packet only.

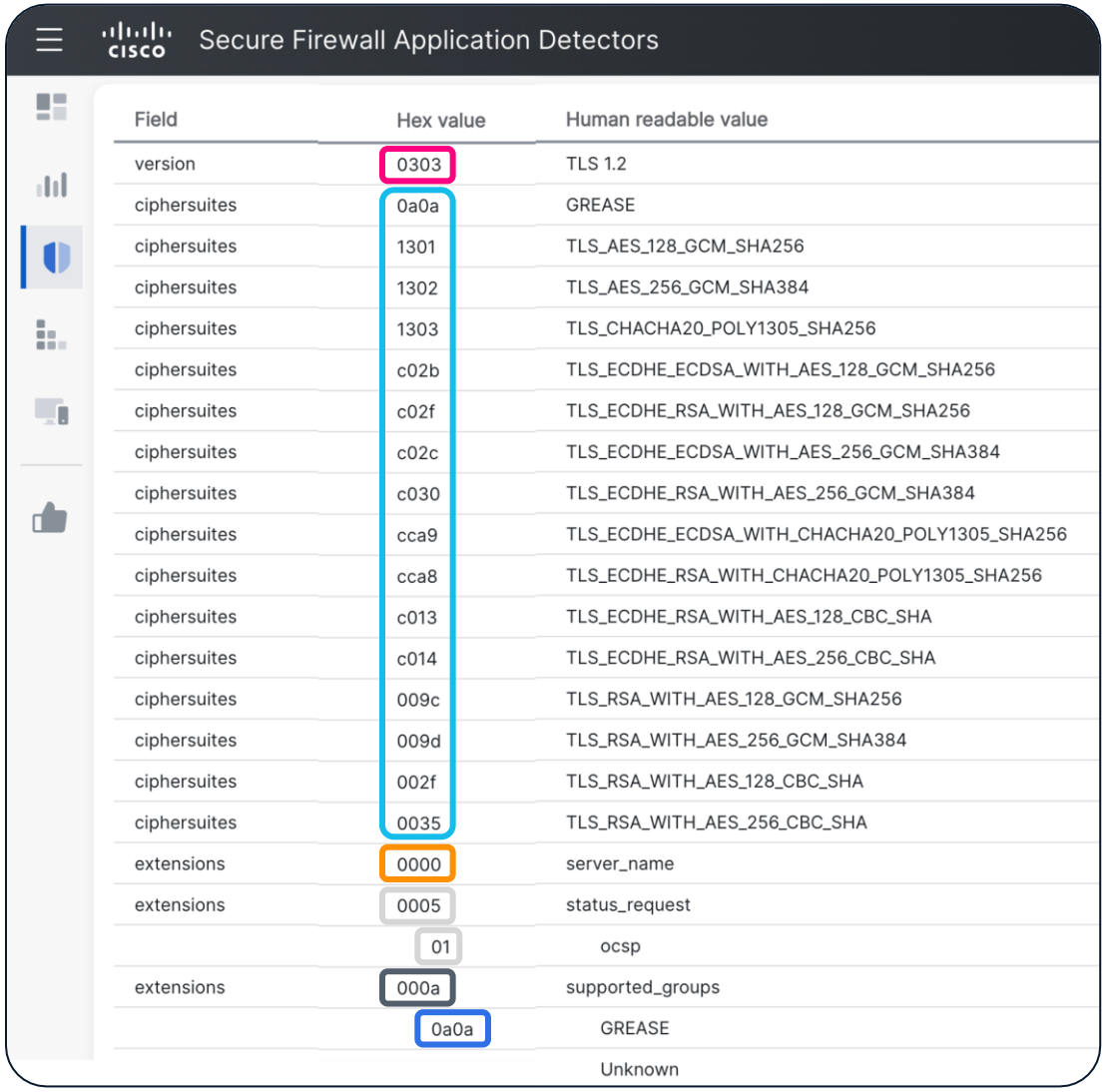
Decryption disabled

Decryption enabled

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

How do we calculate the TLS fingerprint



Field	Hex value	Human readable value
version	0303	TLS 1.2
ciphersuites	0a0a	GREASE
ciphersuites	1301	TLS_AES_128_GCM_SHA256
ciphersuites	1302	TLS_AES_256_GCM_SHA384
ciphersuites	1303	TLS_CHACHA20_POLY1305_SHA256
ciphersuites	c02b	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
ciphersuites	c02f	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
ciphersuites	c02c	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
ciphersuites	c030	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
ciphersuites	cca9	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
ciphersuites	cca8	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
ciphersuites	c013	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
ciphersuites	c014	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
ciphersuites	009c	TLS_RSA_WITH_AES_128_GCM_SHA256
ciphersuites	009d	TLS_RSA_WITH_AES_256_GCM_SHA384
ciphersuites	002f	TLS_RSA_WITH_AES_128_CBC_SHA
ciphersuites	0035	TLS_RSA_WITH_AES_256_CBC_SHA
extensions	0000	server_name
extensions	0005	status_request
	01	ocsp
extensions	000a	supported_groups
	0a0a	GREASE
		Unknown

TLS Fingerprint:

tls/1/(0303)(0a0a130113021303c02bc02fc02cc030cca9cca8c013c014009c009d002f0035)[(0000)(000500050100

(0303) **Version**

(0a0a130113021303c02bc02fc02cc030cca9cca8c013c014009c009d002f0035) **Ciphers**

[**EXTENSIONS:**

(0000) **server_name**

(0005000501000000000) **status_request**

(000a000c000a0a0a11ec001d00170018) supported_groups

(000b00020100) ec_point_formats

(000d00120010040308040401) signature_algorithms

(0010000e000c026832086874) ALPNs

(0012) signed_cert_timestamp

(0017) master_secret

(0033)

(0a0a) GREASE

(0a0a) GREASE

(44cd) UNKNOWN

(fe0d) encrypted_client_hello

(ff01) renegotiation info

]

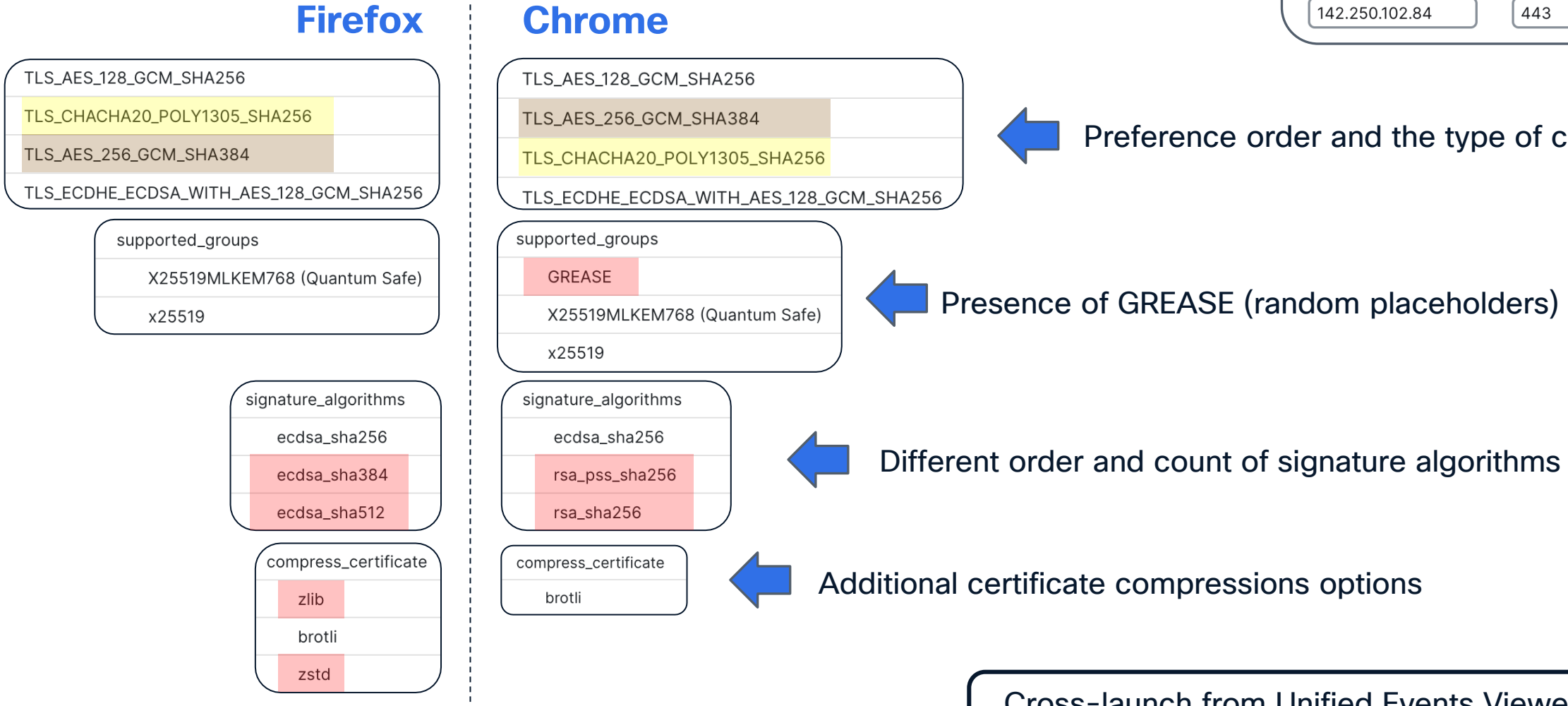
Billions of possible combinations

© 2025 Cisco and/or its affiliates. All rights reserved.

One Destination, Many Fingerprints

Destination

VDB Version	Server Name
latest	accounts.google.com
IP Address	**Port**
142.250.102.84	443



... and many, many more!

Cross-launch from Unified Events Viewer
or navigate to: https://appid.cisco.com/eve

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

The Power of the Destination Context

Fingerprint

tls/1/(0303)(0a0a130113021303c02bc02fc02cc030cca9cca8c013c014009c009d002f0035)[((

73.10% of connections with this fingerprint in EVE's database originated from the Chromium Browser

IP Address

142.250.102.84

Server Name

accounts.google.com

Port

443

Out of those 73.10% connections:

- **99.71%** reached out to "accounts.google.com"
- **100%** connected to 142.250.102.84
- **73.11%** used port 443

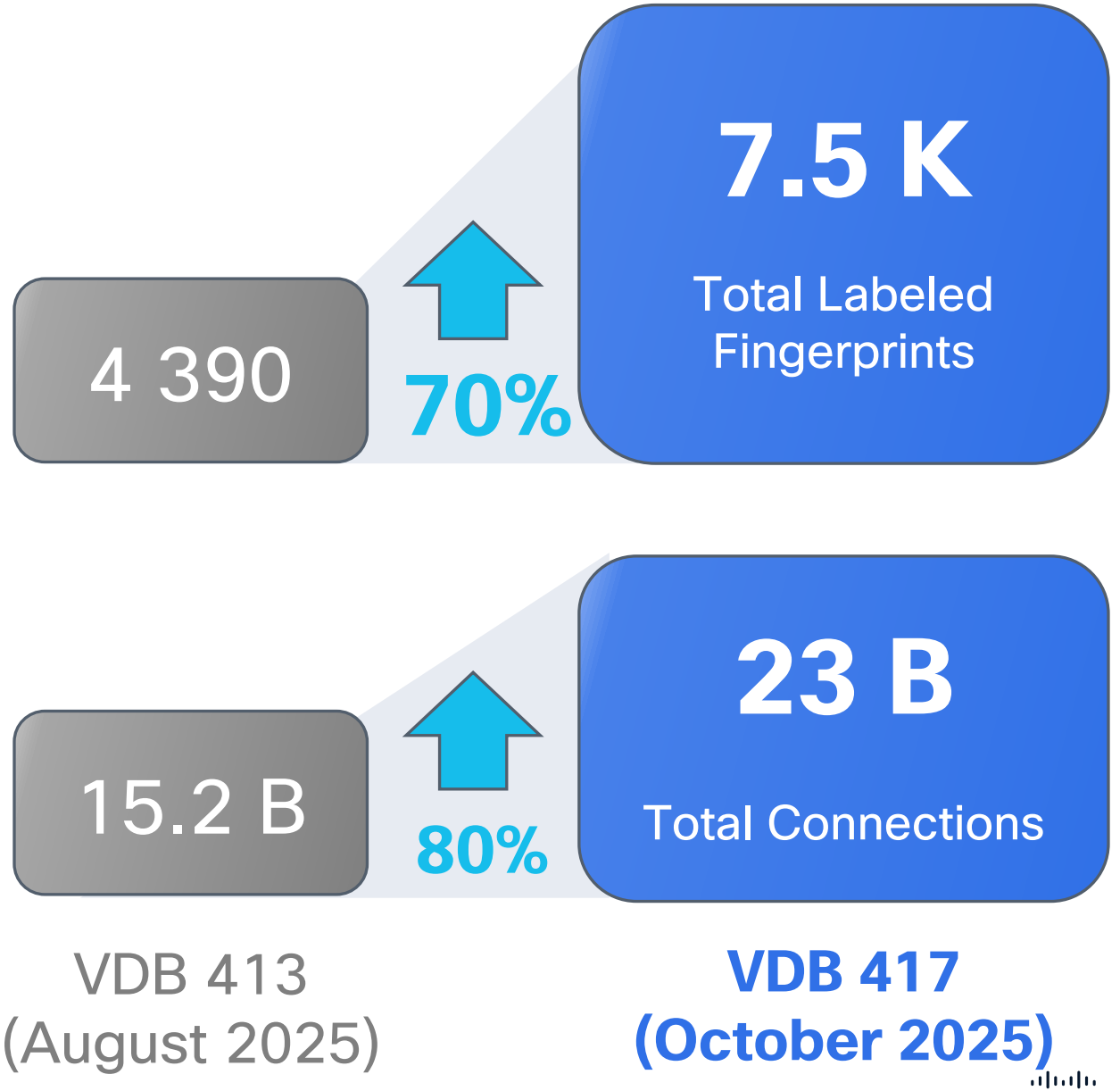
Process Name	Prevalence	Server Name	IP Address	Port
chromium browser	0.7310	0.9971	1.0000	0.7311
slack	0.0834	0.0000	0.0000	0.0835
microsoft visual studio	0.0822	0.0000	0.0000	0.0822
miro	0.0281	0.0011	0.0000	0.0281
figma	0.0269	0.0000	0.0000	0.0269
spotify	0.0221	0.0000	0.0000	0.0221
microsoft teams	0.0137	0.0000	0.0000	0.0137
github desktop	0.0058	0.0000	0.0000	0.0058

The other processes (slack, miro, figma etc...) produced similar TLS fingerprints, however **connected to different IPs, Domains and ports.**

© 2025 Cisco and/or its affiliates. All rights reserved.

EVE training set enhanced with customer data

- Increased EVE accuracy:
  - **70%** more **labeled fingerprints** (processes)
  - **2 x** more **recognized OS'es**
- Training set enriched with **Cisco XDR endpoints data**
- Significant ramp up in the size of the training data set – **1 billion sessions per day** from anonymized real user flows



© 2025 Cisco and/or its affiliates. All rights reserved.

Encrypted Visibility Engine - Key Takeaways

- **EVE complements, not replaces decryption** – use both together for comprehensive security

- **Detects application/OS and malware activity** looking at a single TLS/QUIC packet - **minimal performance impact, no decryption required**

- **Optimise performance with Intelligent Decryption bypass** – EVE's Client Threat Score + URL Reputations

- **Continously trained and improved on real world connections** – remember to keep VDB up-to-date

- **AppID and URL filtering for QUIC in Access Control Policy requires EVE enabed** – EVE is the decoder for QUIC Initial packets providing SNI

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Shadow Traffic

Shadow Traffic Detection

Clear way to detect and monitor Shadow Traffic

Help administrators promptly react to unsanctioned connections

Combined powers of AppID, EVE and TLS/QUIC decryption.

Designed to avoid network monitoring and traffic analysis by advanced firewalls.

80+ evasive anonymizers, VPN clients, multi-hop proxies.

Hide real intention of user connectivity.

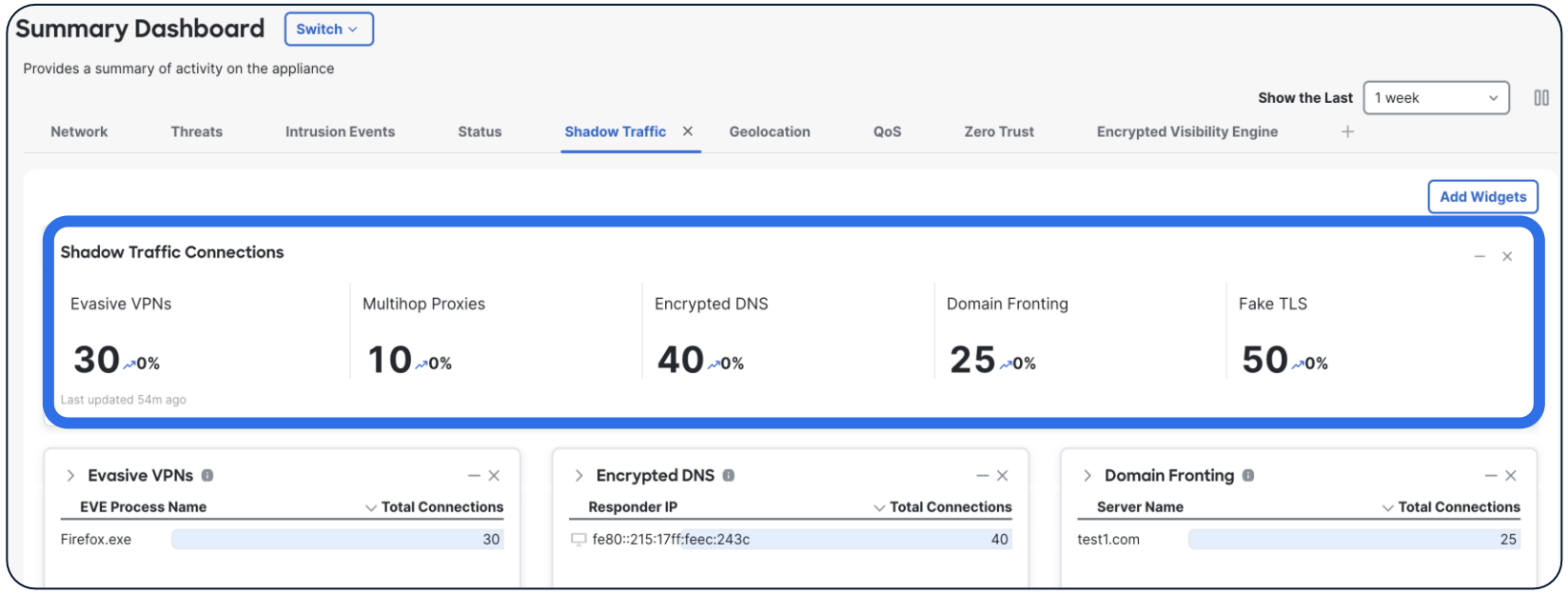
Fake TLS connections, encrypted DNS, hiding behind benign sites.

© 2025 Cisco and/or its affiliates. All rights reserved.

Detecting Shadow Traffic in Firewall Management Center

A new dashboard presents Shadow Traffic detected in firewall protected network divided into five categories:

- Evasive VPNs
- Encrypted DNS
- Domain Fronting
- Multi-hop Proxies
- Fake TLS



Firewall **detects and flags suspicious connections** showing the signs of evasion in a new column: **Shadow Traffic Type**.

Event Type	Action	Client Application	Web Application	Destination IP	Destination Port / ICMP Code	Shadow Traffic Type	TLS Client SNI
Connection	Allow	SSL client	XVPN	35.205.176.240	**443** (https) / tcp	Evasive VPN	8v9m.com
Connection	Allow	X-VPN	Web Browsing	130.211.50.202	**20005** / tcp	Evasive VPN	
Connection	Allow	X-VPN	Web Browsing	35.205.250.171	**20005** / tcp	Evasive VPN	
Connection	Allow	Firefox	DNS over HTTPS	172.64.41.4	**443** (https) / tcp	Encrypted DNS	mozilla.cloudflare-dns.com
Connection	Allow	Firefox	DNS over HTTPS	172.64.41.4	**443** (https) / tcp	Encrypted DNS	mozilla.cloudflare-dns.com
Connection	Allow	Tor		185.220.101.192	**443** (https) / tcp	Evasive VPN, Multihop Proxy	www.4vg22c3cybm7v6bqyf...
Connection	Allow	Tor		64.65.0.11	**443** (https) / tcp	Evasive VPN, Multihop Proxy	www.sr33qfglszbztrvgyt3b...

© 2025 Cisco and/or its affiliates. All rights reserved.

DEMO:

Detecting Shadow Traffic

© 2025 Cisco and/or its affiliates. All rights reserved.

Five Flavors of Shadow Traffic

Shadow Traffic Connections

Evasive VPNs	Multihop Proxies	Encrypted DNS	Domain Fronting	Fake TLS
30 ↗0%	10 ↗0%	40 ↗0%	25 ↗0%	50 ↗0%

Last updated 54m ago

Evasive VPNs

Known evasive VPN applications attempting to bypass firewall controls.

70+ VPN Apps

HMA Monster VPN CyberGhost

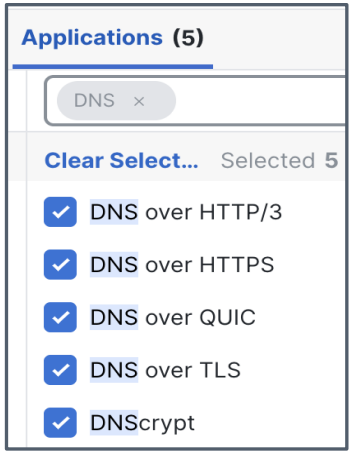
Multi-hop Proxies

Attempts to anonymize network activity.

Tor ...and more!

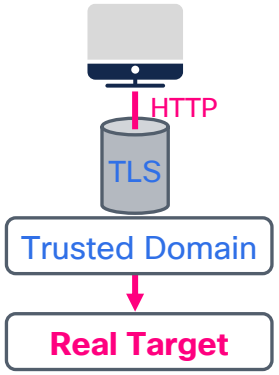
Encrypted DNS:

Covert domain resolution tunneling.



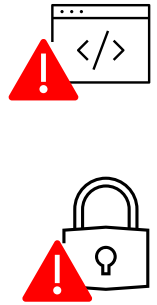
Domain Fronting:

HTTP header hostname and SNI/certificate mismatch – disguise true destination.



Fake TLS:

Non-standard or insecure TLS/QUIC cipher suites or domain faking.



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Synergy and benefits of AppID and EVE working together

Detection engine	Evasive VPNs	Multi-hop Proxy	Encrypted DNS	Domain Fronting	Fake TLS
EVE	✓	✓	✓	✗	✓
AppID	✓	✓	✓	✓*	✗

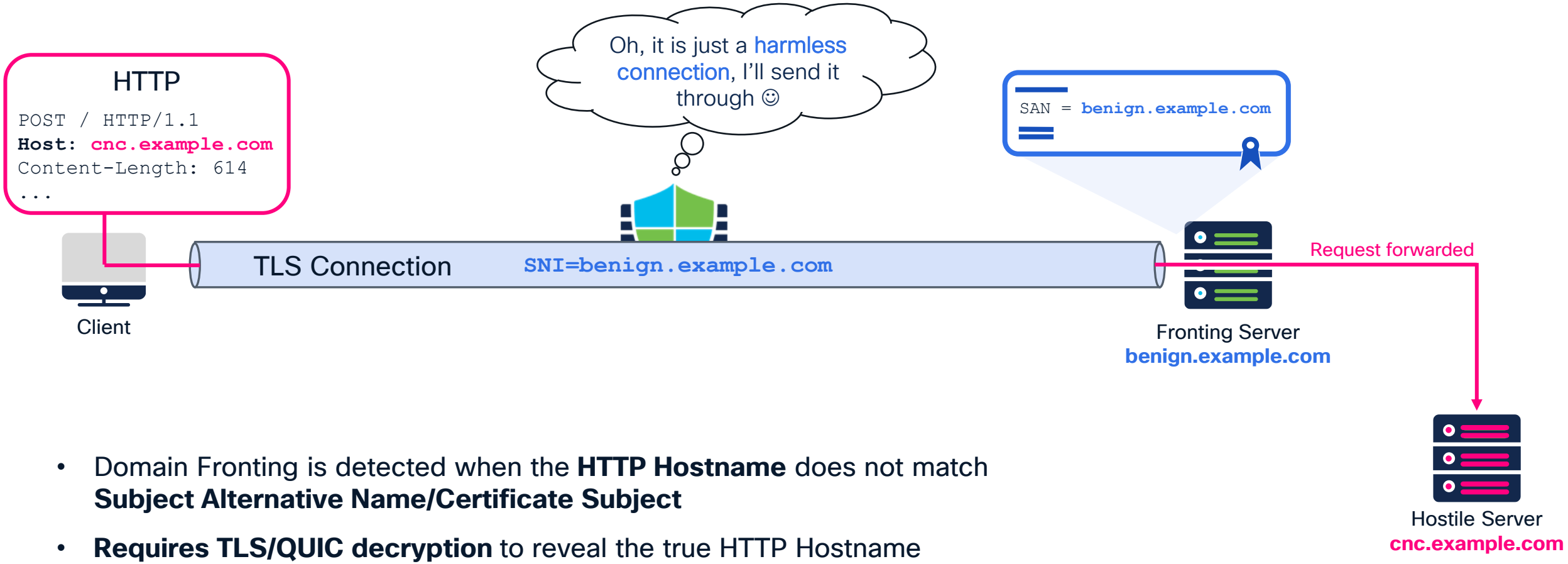
Shadow traffic detection leverage both **machine learning** and traditional **signature-based** engines:

- EVE extends visibility into encrypted traffic identifying client processes and source OS
- AppID provides granular application detection with deep inspection in unencrypted or decrypted traffic.
- Domain Fronting (*) requires TLS/QUIC decryption to compare TLS endpoint with the real HTTP request

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Domain Fronting – Hide Behind Legitimate TLS Connection



- Domain Fronting is detected when the **HTTP Hostname** does not match **Subject Alternative Name/Certificate Subject**
- **Requires TLS/QUIC decryption** to reveal the true HTTP Hostname

© 2025 Cisco and/or its affiliates. All rights reserved.

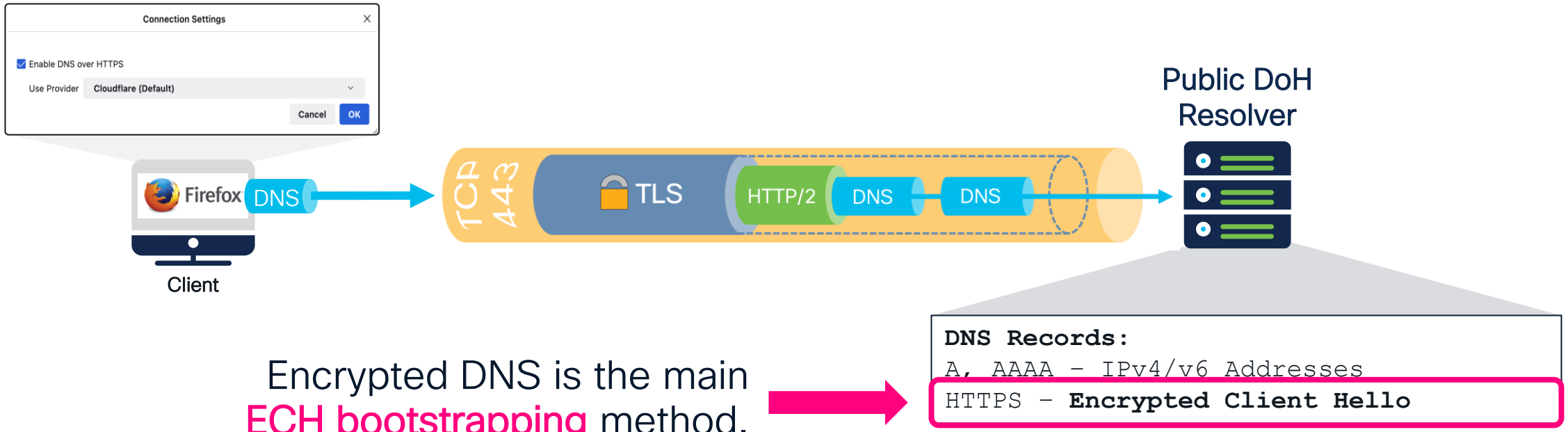
DEMO:

Domain Fronting

© 2025 Cisco and/or its affiliates. All rights reserved.

Encrypted DNS Challenges

- The web browser bypasses OS DNS stack
- Avoids DNS based corporate security controls and logging
- Delegates DNS control to a content provider (e.g. Cloudflare)



Encrypted DNS is the main ECH bootstrapping method.

© 2025 Cisco and/or its affiliates. All rights reserved.

Shadow Traffic – Key Takeaways

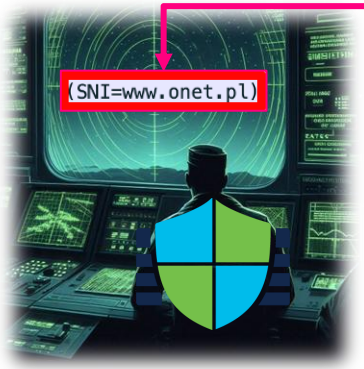
- **EVE + AppID + Decryption working together** to detect 80+ evasive tools, domain fronting and fake TLS
- **Evasive tools evolve constantly** – configure restrictive policy with and monitor closely for Shadow Traffic (assume something sneaks out sooner or later)
- **Enable EVE and Shadow Traffic detection** – review regularly and identify endpoints/users attempting to bypass your controls
- **Educate your users** and ensure your organization's **Security Policy sanctions use of evasive software**
- **Do not block "DNS Crypt" if you use Umbrella** – this AppID matches Cisco Umbrella services

© 2025 Cisco and/or its affiliates. All rights reserved.

Encrypted Client Hello

Firewall enforcement heavily relies on this single TLS extension

	Time	Source	SPORT	Destination	DPORT	Protocol	Length	Info
1	0.000000	172.16.136.96	49934	18.239.83.46	443	TCP	66	49934 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
2	0.000500	18.239.83.46	443	172.16.136.96	49934	TCP	66	443 → 49934 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=
3	0.000547	172.16.136.96	49934	18.239.83.46	443	TCP	54	49934 → 443 [ACK] Seq=1 Ack=1 Win=2097408 Len=0
4	0.000780	172.16.136.96	49934	18.239.83.46	443	TLSv1.3	585	Client Hello (SNI=www.onet.pl)



URL Category and Reputation

Selective TLS/QUIC decryption

Advanced inspection:
- IPS
- Malware protection
- TID (URLs, Hashes)

Security Intelligence URLs

AppID

TLS Server Identity Probe

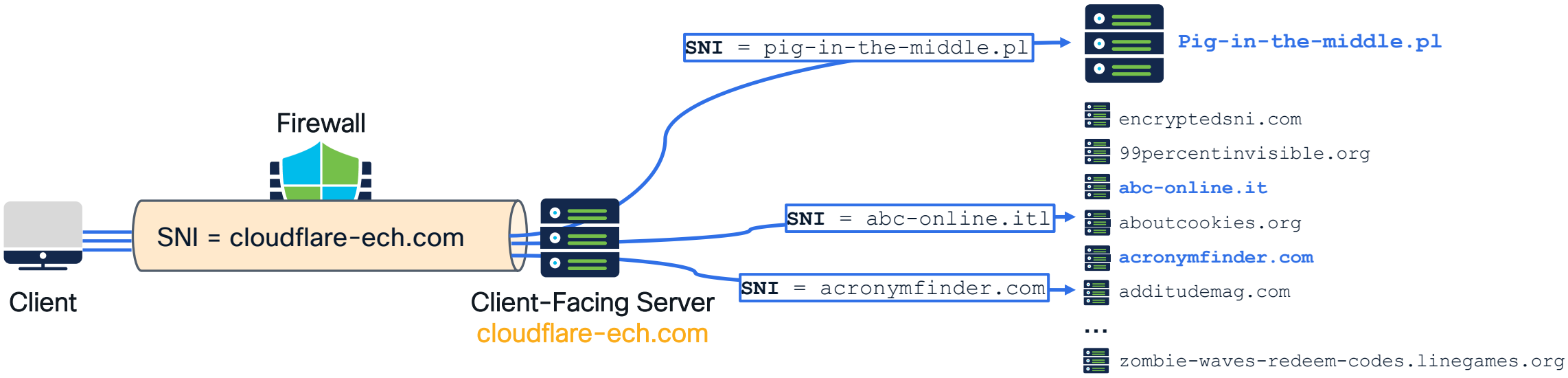
© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

What is Encrypted Client Hello (ECH)?

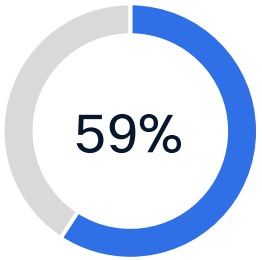
Learn more: RSAC 2025 “ECH: Hello to Enhanced Privacy or Goodbye to Visibility?”

- ECH is the last piece of the puzzle to close SNI security gap – HPKE, Encrypted DNS, service bindings for DNS ... and more!
- You can still recognize the Service Provider hosting the real destination – e.g. Clourflare, Akamai, Fastly etc...
- ECH requires bootstrap configuration from the Service Provider

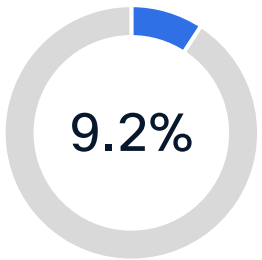


© 2025 Cisco and/or its affiliates. All rights reserved.

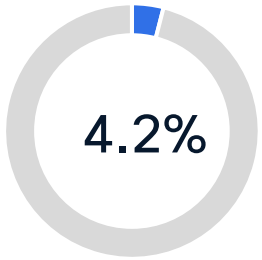
Why should we care?



of **browsers** support ECH[1]



Of top **1M sites** have ECH enabled[2]



Of top **10K sites** have ECH enabled[3]

- The **ECH infrastructure is ready and fully operational** on both the user (browsers) and the CDN side.
- Most web browsers support ECH and actively send **fake ECH extensions to GREASE the Internet**.
- Cloudflare is the first CDN to **fully support Encrypted Client Hello** and the destination for almost all ECH traffic
- ECH is at its final draft 25 – expected to be ratified **any day now**...

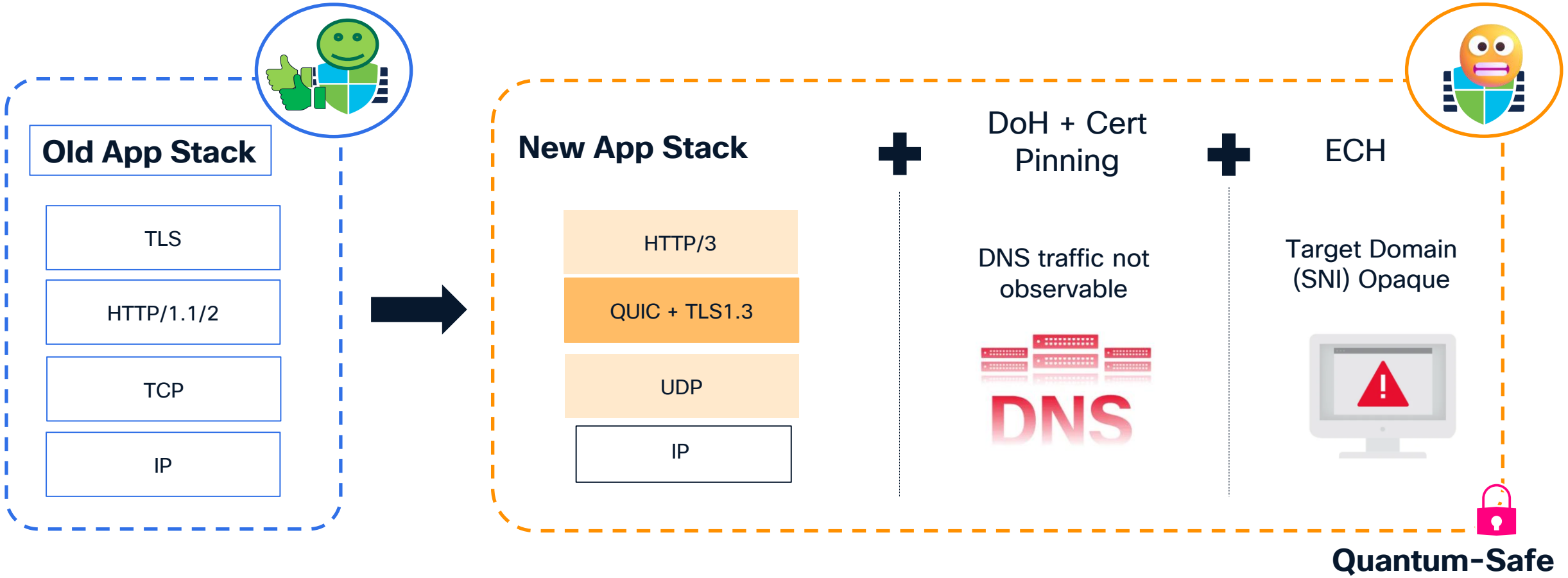
Prepare for :

- Impairment of existing network-centric security stack – firewall, IPS, etc...
- Malware, C2, exfiltration (etc...) hiding under the radar

[1] - https://www.stetic.com/market-share/browser/
[2] - https://portal.onersac.com/library/B00507DF8D944ED79CA2D5EA1FD168E8
[3] - https://divested.dev/misc/ech.txt

© 2025 Cisco and/or its affiliates. All rights reserved.

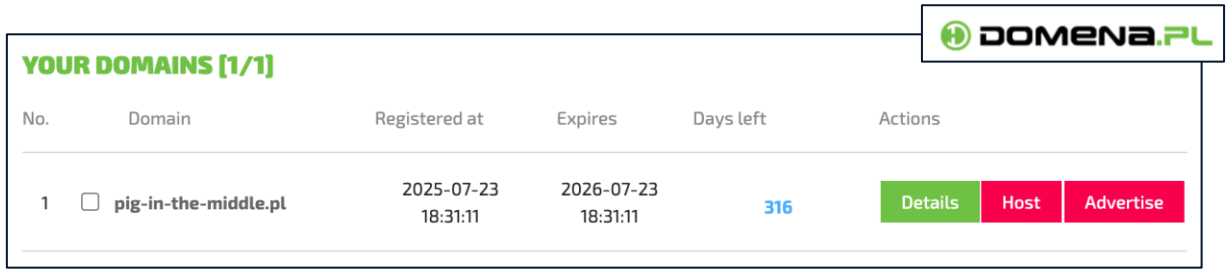
The “nightmare” crypto stack is here...



© 2025 Cisco and/or its affiliates. All rights reserved.

...and you can set it up in three simple steps...

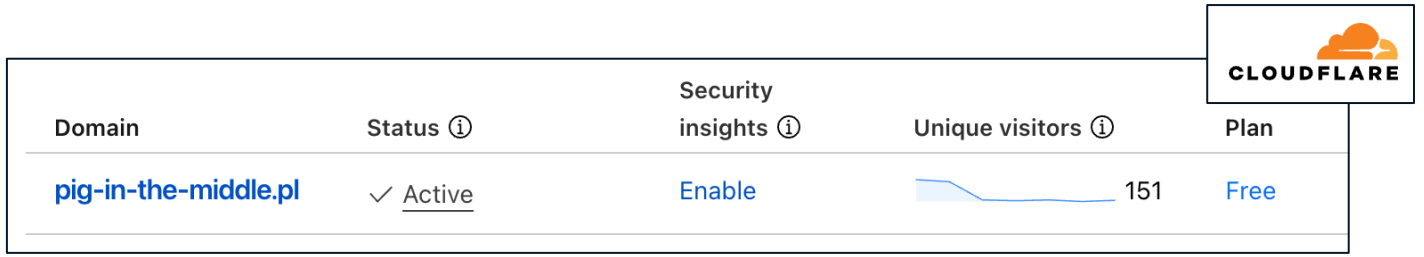
1. Register a domain.



2. Set up your web server.

```
server {
    listen 443 quic reuseport;
    listen 443 default_server ssl;
    http2 on; http3 on; http3_hq on;
    server_name pig-in-the-middle.pl;
    quic_retry on;
    ssl_early_data on;
    ssl_certificate /etc/letsencrypt/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/privkey.pem;
}
```

3. Sign-up for a free plan* at Cloudflare and delegate your domain.



* - ECH cannot be disabled in Cloudflare's free plan – potentially hiding thousands of web pages behind **cloudflare-ech.com**.

© 2025 Cisco and/or its affiliates. All rights reserved.

...et voila!

QUIC Protocol – Certificate Pinned

No.	Time	Source	SPORT	Destination	DPORT	Protocol	Length	Info
196	05:00:02.478506	2a01:110f:4404:3400:451d:2176:7833:79a2	54251	2a06:98c1:52::4	443	QUIC	1294	Initial, DCID=51caa96f95cefdf1da9f0982, SCID=92f450, PKN: 1, CRYPTO
1673	05:00:06.014693	2a01:110f:4404:3400:451d:2176:7833:79a2	54258	2606:4700:3030::6815:1001	443	QUIC	1294	Initial, DCID=a658f1d5031e05a9, SCID=35bab5, PKN: 1, CRYPTO

Encrypted

DNS

```
TLSv1.3 Record Layer: Handshake Protocol: Client Hello
  Handshake Protocol: Client Hello
    Handshake Type: Client Hello (1)
    Length: 1788
    Version: TLS 1.2 (0x0303)
      [Expert Info (Chat/Deprecated): This legacy_version field MUST be ignored. The supported_versions extension is present and MUST be used instead.]
    Random: 81eb04265af6f7eb56550f9feb0ad2418fd6a28b59a929d9dc4db01bae6b49aa
    Session ID Length: 0
    Cipher Suites Length: 6
    Cipher Suites (3 suites)
    Compression Methods Length: 1
    Compression Methods (1 method)
    Extensions Length: 1741
    Extension: key_share (len=1327) X25519MLKEM768, x25519, secp256r1
    Extension: psk_key_exchange_modes (len=2)
    Extension: delegated_credentials (len=10)
    Extension: extended_master_secret (len=0)
    Extension: record_size_limit (len=2)
    Extension: supported_versions (len=3) TLS 1.3
    Extension: signature_algorithms (len=24)
    Extension: server_name (len=23) name=cloudflare-ech.com
    Extension: renegotiation_info (len=1)
    Extension: status_request (len=5)
    Extension: encrypted_client_hello (len=249)
```

PQC Keyshare

ECH

ECH

Nothing here ☹

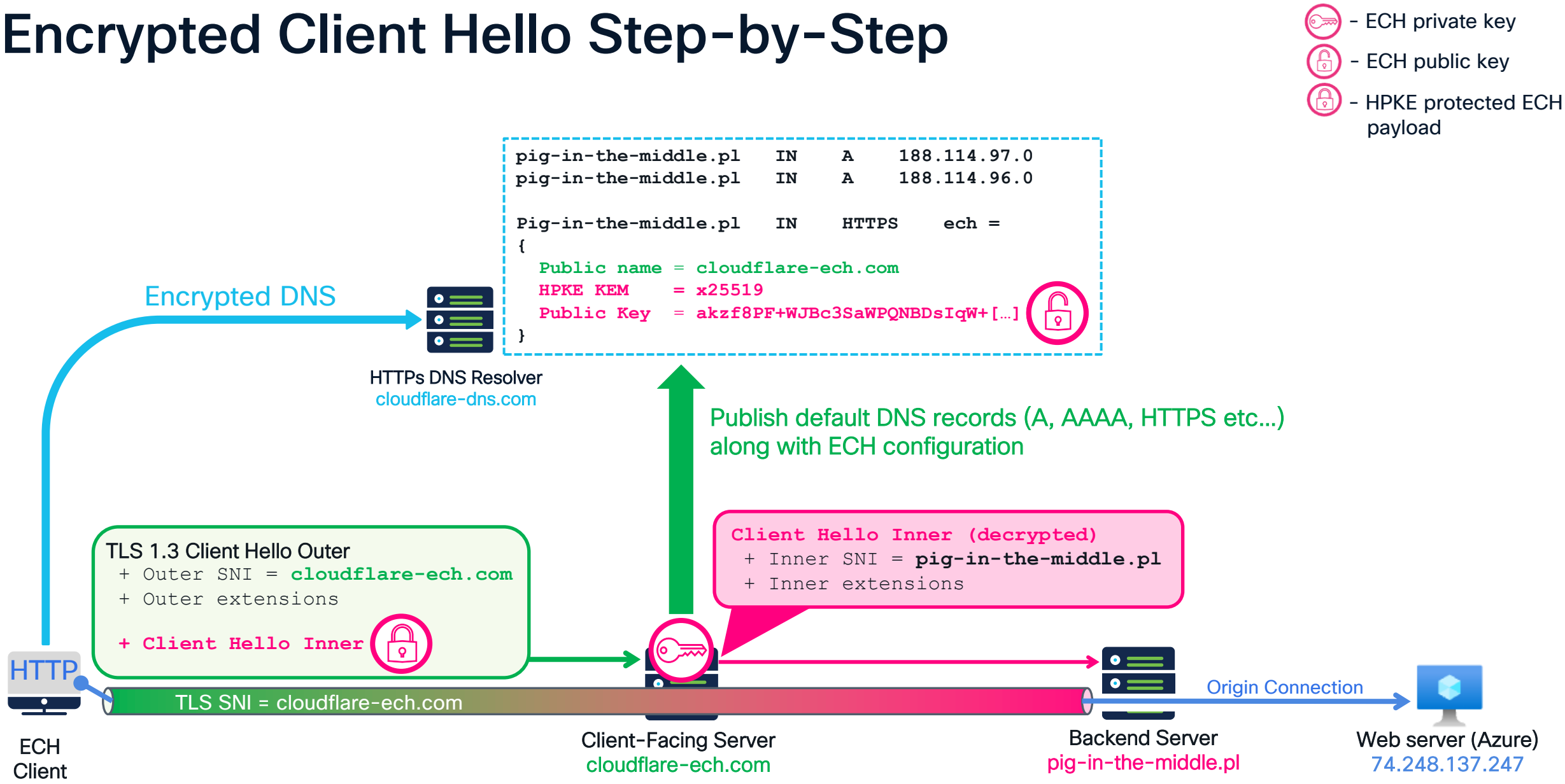
	Date/Time	Event Type	Initiator IP	Responder IP	Responder Port	Action	Application	Client Application	Initiator Port	URL	Web Application
⊞	Sep 5, 2025, 05:02:12	Connect...	2a01:110f:...	2a06:98c1:...	443	Allow	QUIC	QUIC client	54251		Unknown
⊞	Sep 5, 2025, 05:02:12	Connect...	2a01:110f:...	2606:470...	443	Allow	QUIC	QUIC client	54258		Unknown

© 2025 Cisco and/or its affiliates. All rights reserved.

* – certificate pinning only for QUIC traffic. If Firefox falls back to TLS, OS trusted RootCAs accepted

cisco

Encrypted Client Hello Step-by-Step



© 2025 Cisco and/or its affiliates. All rights reserved.

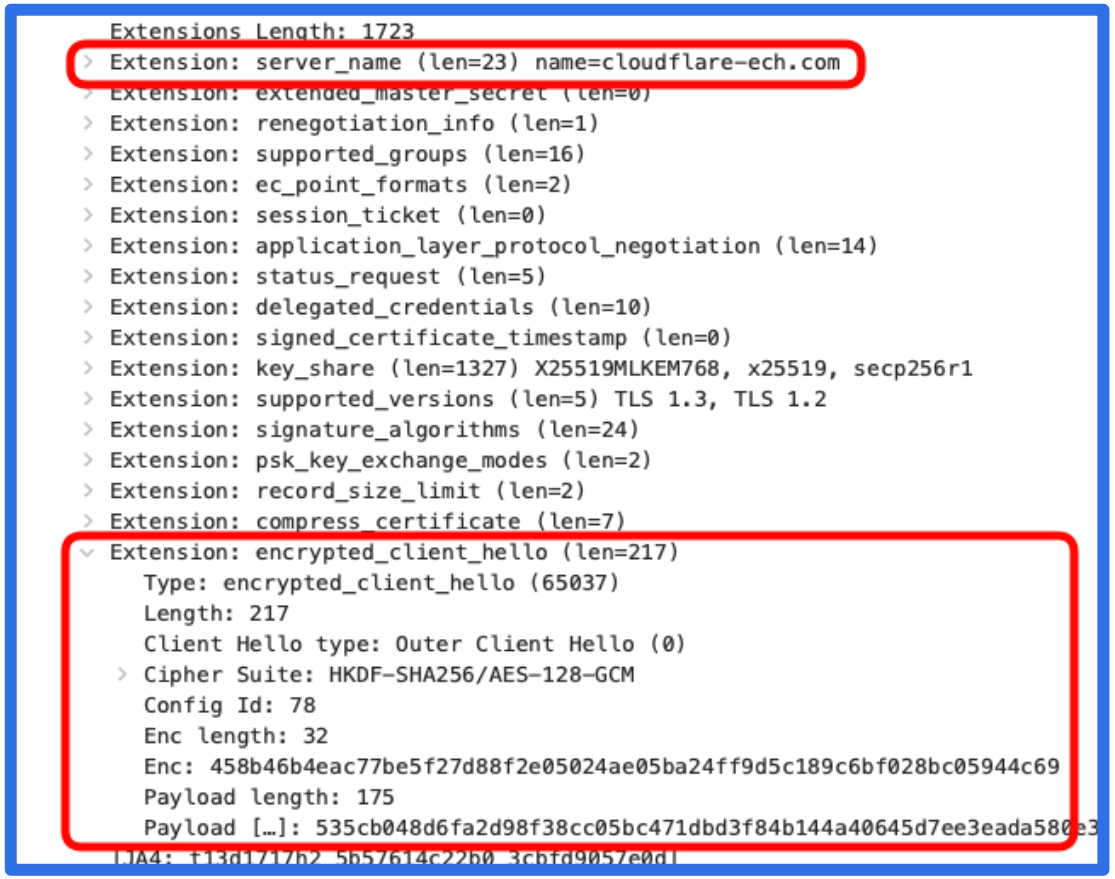
DEMO:

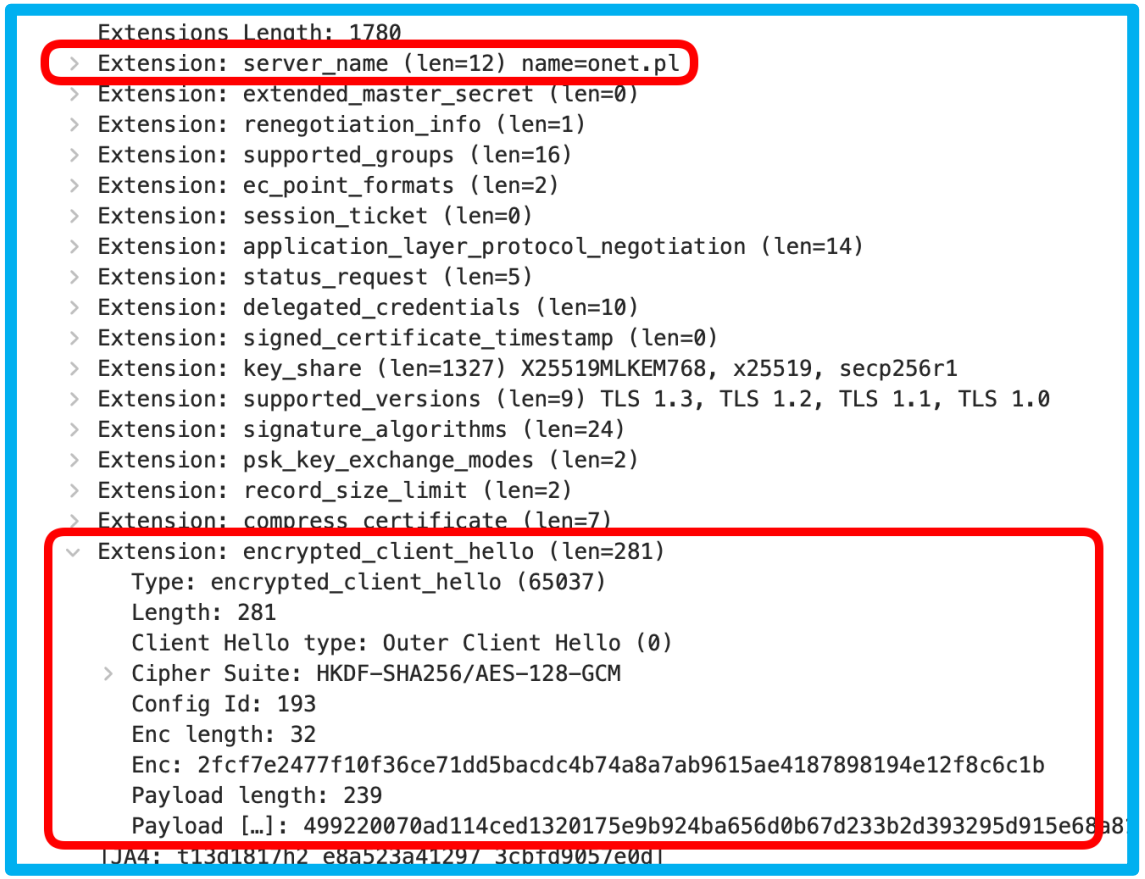
Observing the ECH connection in Wireshark

© 2025 Cisco and/or its affiliates. All rights reserved.

Can a firewall block ECH connections?

Can you tell which of the below is FAKE?





© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Can a firewall figure out if server accepted ECH?

Server's acceptance of ECH proposal encoded in the last 8 bytes of Random value...

Real ECH - Server Hello

```
Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 1210
  Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 1206
    Version: TLS 1.2 (0x0303)
      Random: 5164dec3639e45dbbb1e2ad875b6c56c8f652f3003348a5[illegible]7bd627f7136f77b3
      Session ID Length: 32
      Session ID: c38222699a03fb7e17659e1c95264e9fbdab19c4131a2a0a546ccb9d4b0af626
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Compression Method: null (0)
      Extensions Length: 1134
    Extension: key_share (len=1124) X25519MLKEM768
    Extension: supported_versions (len=2) TLS 1.3
    [JA3S Fullstring: 771,4865,51-43]
```

Fake ECH - Server Hello

```
Transport Layer Security
  TLSv1.3 Record Layer: Handshake Protocol: Server Hello
    Content Type: Handshake (22)
    Version: TLS 1.2 (0x0303)
    Length: 1210
  Handshake Protocol: Server Hello
      Handshake Type: Server Hello (2)
      Length: 1206
    Version: TLS 1.2 (0x0303)
      Random: 4e347c055d50c51dcfe89fde91e218e48226fb7ce41c73d[illegible]75b6b05e58ed9648
      Session ID Length: 32
      Session ID: 4d7cec89f7e13c3f1b3790b278cc414a610265547111d63128dc267ca1983cab
      Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
      Compression Method: null (0)
      Extensions Length: 1134
    Extension: supported_versions (len=2) TLS 1.3
    Extension: key_share (len=1124) X25519MLKEM768
    [JA3S Fullstring: 771,4865,43-51]
```

The server response does not explicitly acknowledge acceptance of ECH by the standard

(this prevents Middleboxes from detecting real attempt)

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Can we block packets to known ECH servers (e.g. cloudflare-ech.com)?

Source	SPORT	Destination	DPORT	Protocol	Length	Info
2a01:110f::b4e0	58768	2a06:98c1:52::4	443	TLSv1.3	752	Client Hello (SNI=mozilla.cloudflare-dns.com)
2a01:110f::b4e0	58789	2606:4700:3030::6815:4001	443	TLSv1.2	553	Client Hello (SNI=cloudflare-ech.com)
2a01:110f::b4e0	58790	2606:4700:3030::6815:4001	443	TLSv1.2	553	Client Hello (SNI=cloudflare-ech.com)
2a01:110f::b4e0	58792	2606:4700:3030::6815:4001	443	TLSv1.2	553	Client Hello (SNI=cloudflare-ech.com)
2a01:110f::b4e0	58348	2606:4700:3030::6815:4001	443	TLSv1.2	680	Client Hello (SNI=cloudflare-ech.com)
2a01:110f::b4e0	58655	2606:4700:3030::6815:6001	443	TLSv1.2	680	Client Hello (SNI=cloudflare-ech.com)
2a01:110f::b4e0	58660	2606:4700:3030::6815:7001	443	TLSv1.2	680	Client Hello (SNI=cloudflare-ech.com)
2a01:110f::b4e0	58662	2606:4700:3030::6815:3001	443	TLSv1.2	680	Client Hello (SNI=cloudflare-ech.com)
2a01:110f::b4e0	58664	2606:4700:3030::6815:5001	443	TLSv1.3	746	Client Hello (SNI=pig-in-the-middle.pl)

DNS over HTTPs query

Connection attempts to the ECH client facing servers timing-out (15 seconds each)

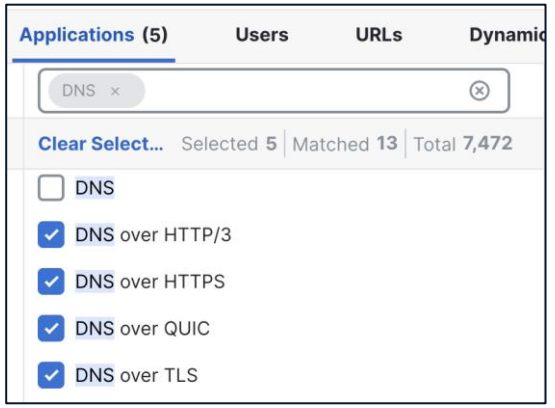
Fallback to clear-text SNI after 120 seconds...

"This technology is a way to bypass restrictions on access to information that's banned in Russia. Using it goes against Russian law." – Roskomnadzor (Russia's media censor) after it blocked thousands of websites using ECH (November 2024)

© 2025 Cisco and/or its affiliates. All rights reserved.

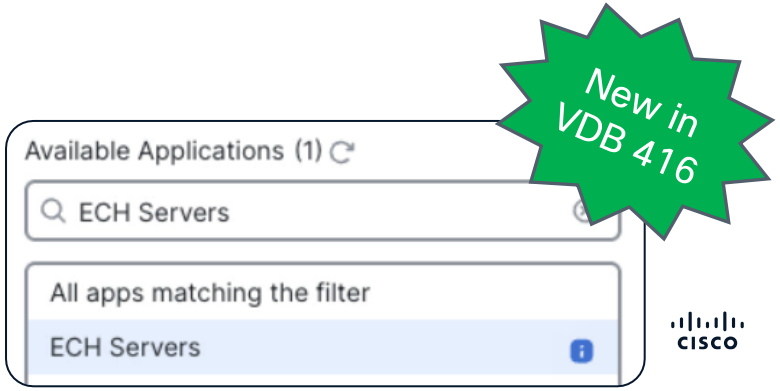
Three lines of defenses against ECH

1. **Strict control over DNS – prevent the client from learning ECH configuration**
   - Configure your DNS to scrub ECH config or block the whole HTTPS record
   - Block the ”canary domain” use-application-dns.net – to let know the browsers they can’t use DoX
   - Block encrypted DNS in the firewall policy
   - Block unauthorised DNS servers



2. **Disable ECH/encrypted DNS on managed endpoints (e.g. Firefox/Chrome policy-templates):**
   - DisableEncryptedClientHello (does not stop fake ECH)
   - DNSoverHTTPS Locked

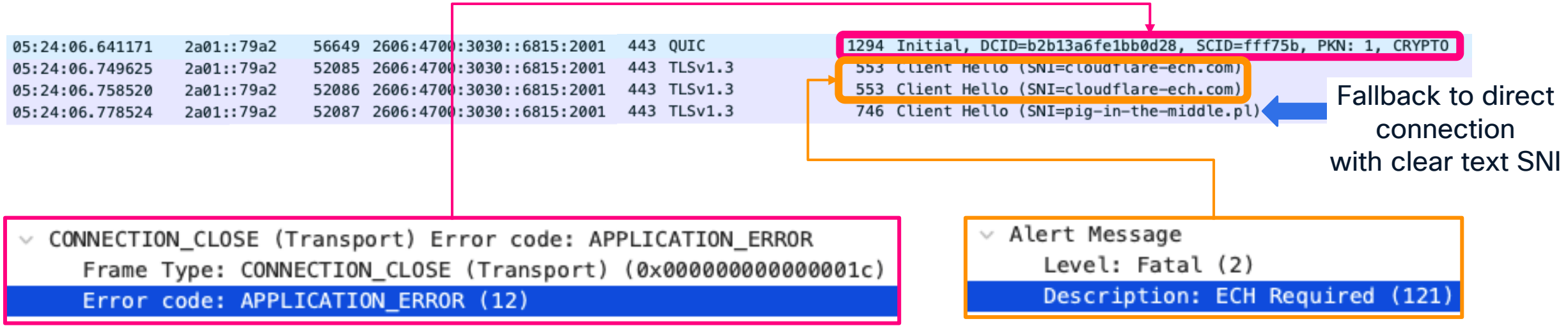
3. **Reduce ECH traffic as much as possible (with above) and consider TLS/QUIC decryption to downgrade ECH.**



© 2025 Cisco and/or its affiliates. All rights reserved.

Downgrade ECH with trusted Key-Resign Decryption

With the current backoff logic (tested on latest Firefox and Chrome), decrypting connections towards ECH Client Facing Servers gracefully downgrades the connection to clear text SNI.



As per the ECH draft 25 when a middlebox acts as TLS proxy ignoring ECH:

- *Depending on whether the **client is configured to accept the proxy's certificate as authoritative for the public name**, this may trigger the retry logic. [8.2]*
- *[...] **the client can regard ECH as securely disabled by the server**, and it SHOULD retry the handshake with a new transport connection and ECH disabled. [6.1.6]*

© 2025 Cisco and/or its affiliates. All rights reserved.

DEMO:

Downgrade ECH with decryption

© 2025 Cisco and/or its affiliates. All rights reserved.

Encrypted Visibility Engine to the rescue?

Event Type	Action	Destination IP	URL	Web Application	Encrypted Visibility Process Name	Encrypted Visibility Process Confidence Score	Encrypted Visibility Fingerprint
Connection	Allow	172.67.135.44	https://cloudflare-ech.com	ECH Servers	chromium browser	98%	quic/(00000001)(0303)(130113021303

...but the destination is hidden by ECH (https://pig-in-the-middle.pl)

EVE tells us the connection was initiated by Chrome...

The true **destination remains unknown**, but **EVE provides a strong indication** something suspicious is going on:

Time	Event Type	Action	Source IP	Web Application	Destination IP	Destination Port / ICMP Code	URL	Encrypted Visibility Process Name	Encrypted Visibility Proces...
2025-10-30 14:39:01	Connection	Allow	198.19.10.103	ECH Servers	104.18.11.118	443 (https) / tcp	https://cloudflare-ech.com	generic dmz process	65%
2025-10-30 14:36:46	Connection	Allow	198.19.10.103	ECH Servers	104.18.10.118	443 (https) / tcp	https://cloudflare-ech.com	rancher desktop	100%
2025-10-30 14:36:30	Connection	Allow	198.19.10.21	ECH Servers	172.67.135.44	443 (https) / udp	https://cloudflare-ech.com	chromium browser	98%
2025-10-30 14:36:20	Connection	Allow	198.19.10.21	ECH Servers	104.21.26.24	443 (https) / tcp	https://cloudflare-ech.com	firefox browser	100%

ECH traffic originating from a non-standard browser can be a sign of something fishy.

© 2025 Cisco and/or its affiliates. All rights reserved.

In early 2024, while analysing targeted attacks [...] we identified a noteworthy piece of malware[...] distinguishing itself by leveraging Encrypted Client Hello (ECH) for its C&C communications [...] significantly harder to detect and block using conventional security products.

Yuta Sawabe & Rintaro Koike (NTT Security Holdings)
https://www.virusbulletin.com/conference/vb2025/abstracts/stealth-over-tls-emergence-ech-based-cc-echidna-malware/

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Encrypted Client Hello – Key Takeaways

- **Implement DNS control NOW** – prevent ECH bootstrap before it happens
- **ECH hides SNI and breaks most of the NGFW stuff** – URL filtering, TLS probing, selective decryption…
- 59% of browsers and 10% of top 1M sites support **ECH – infrastructure is ready, and adoption is accelerating rapidly**
- Three-layer defense: (1) **Strict DNS Control**, (2) **Endpoint Policies**, (3) **Selective Decryption and Blocking**
- **Monitor for EVE-detected unusual processes** connecting to known ECH Servers (e.g. malware using CnC hosted behind CDNs)

© 2025 Cisco and/or its affiliates. All rights reserved.

Certificate Management

The “CA/Browser Forum Mob” says...

- “Your life ain’t gonna be too long, pal.”

© 2025 Cisco and/or its affiliates. All rights reserved.

Certificate Lifetime Shortens By Half Every 2 Years

The **CA/Browser Forum** – an alliance of browser and public CA vendors – holding the power to decide how long certificates can live on the public web.

- ✚ Frequent certificate rotation = faster adoption of stronger keys & algorithms, reduce stale ownership and security exposure
- ▬ Higher operational frequency, automation becomes essential, little tolerance to missed renewals...

From degree-length lifetime...

...to milk expiry

5 Years	3¼ Years	27 Months	13 Months	200 Days	100 Days	47 Days
2012	2015	2018	2020	15 March 2026	2027	2029

TODAY

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

When the “milk” gets sour, it brings down the Giants...

EXPIRED AUTHENTICATION CERTIFICATE

Microsoft Teams knocked offline by expired authentication certificate – a three-hour global outage of Microsoft Teams, leaving over **20 million users** unable to log in or send messages.

[3 February 2019]

EXPIRED SIP SERVER CERTIFICATE

Google Voice suffered a four-hour outage after SIP servers failed certificate validation. During the incident, **users could not initiate or receive VoIP calls**, impacting business communications across multiple regions.

[*15-16 February 2021*]

EXPIRED GROUD-STATIONS CERTIFICATE

SpaceX Starlink suffers downtime from expired ground station certificate – an expired digital certificate on SpaceX’s ground control systems triggered a **global connectivity loss** for Starlink users lasting several hours.

[8 April 2023]

EXPIRED ROOT CA CERTIFICATE

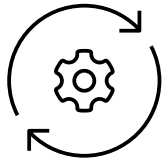
A root certificate expiration caused **Cisco SD-WAN** endpoints worldwide to lose registration with Secure Access (Umbrella DNS). The issue **disrupted network connectivity** until new trust anchors were deployed.

[30 September 2024]

© 2025 Cisco and/or its affiliates. All rights reserved.

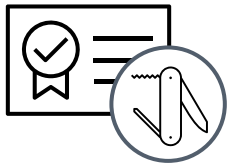
Building a process so your milk never gets that ‘extra flavour’

Server Certificate Lifecycle Management



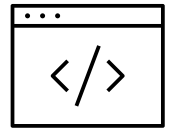
Automatically obtain, renew and deploy certificates using ACME, off-shelf CLM* or custom orchestration workflows.

Flexible Certificate Usage on the Firewall



Scale decryption configuration easily and enable seamless, zero-downtime certificate rotation.

Firewall Update API



Automate certificate provisioning and updates with an intuitive programmatic interface.

* - Certificate Lifecycle Management

© 2025 Cisco and/or its affiliates. All rights reserved.

An RFC Standard to the Rescue – Automated Certificate Management Environment (ACME)

ACME is an open RFC8555 standard protocol that automates the **issuance**, **validation**, and **renewal** of digital certificates – eliminating the need for manual, error-prone steps.

Key benefits:

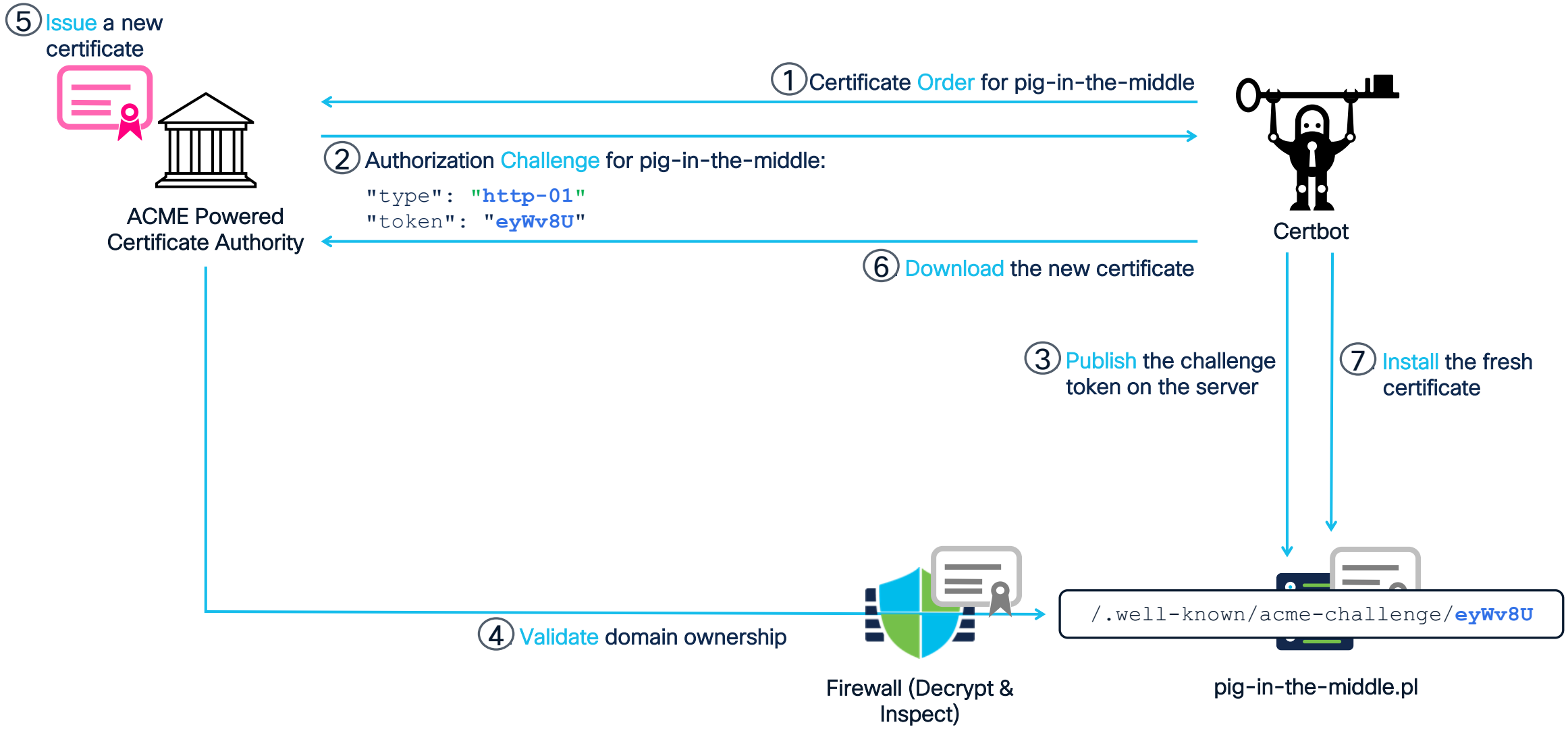
- Streamlines certificate deployment and renewal
- Ensures continuous trust without human intervention
- Integrates easily with automation tools, CLM systems, and firewalls

Domain validation methods:

- **HTTP-01 Challenge** – Proves domain control via an HTTP resource
- **DNS-01 Challenge** – Proves control by creating a specific DNS record
- **TLS-ALPN-01 Challenge** – Validates ownership through a custom TLS handshake

© 2025 Cisco and/or its affiliates. All rights reserved.

Automatic Certificate Management Environment (ACME)



© 2025 Cisco and/or its affiliates. All rights reserved.

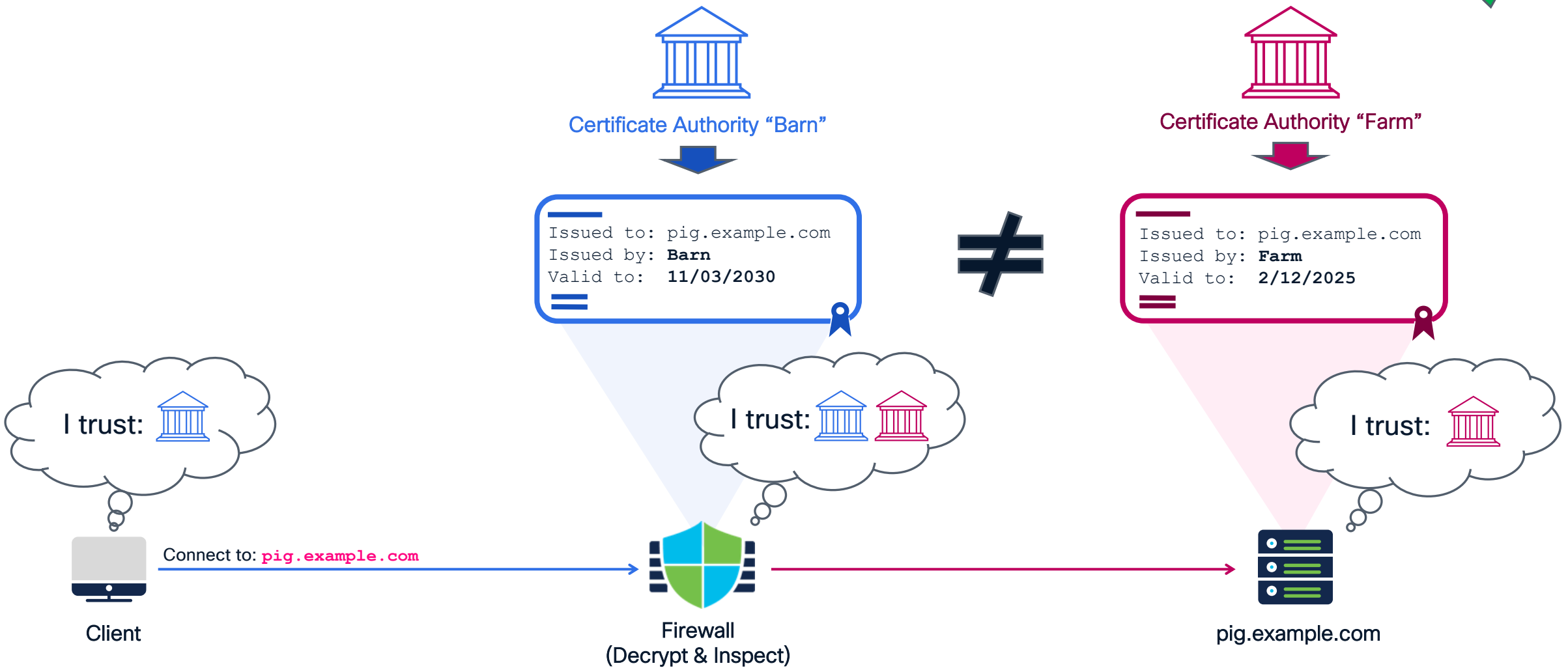
DEMO:

Automating Certificate Lifecycle with ACME and Certbot

© 2025 Cisco and/or its affiliates. All rights reserved.

Certificate Replace – Flexible Certificate Design

New in FTD 10.0

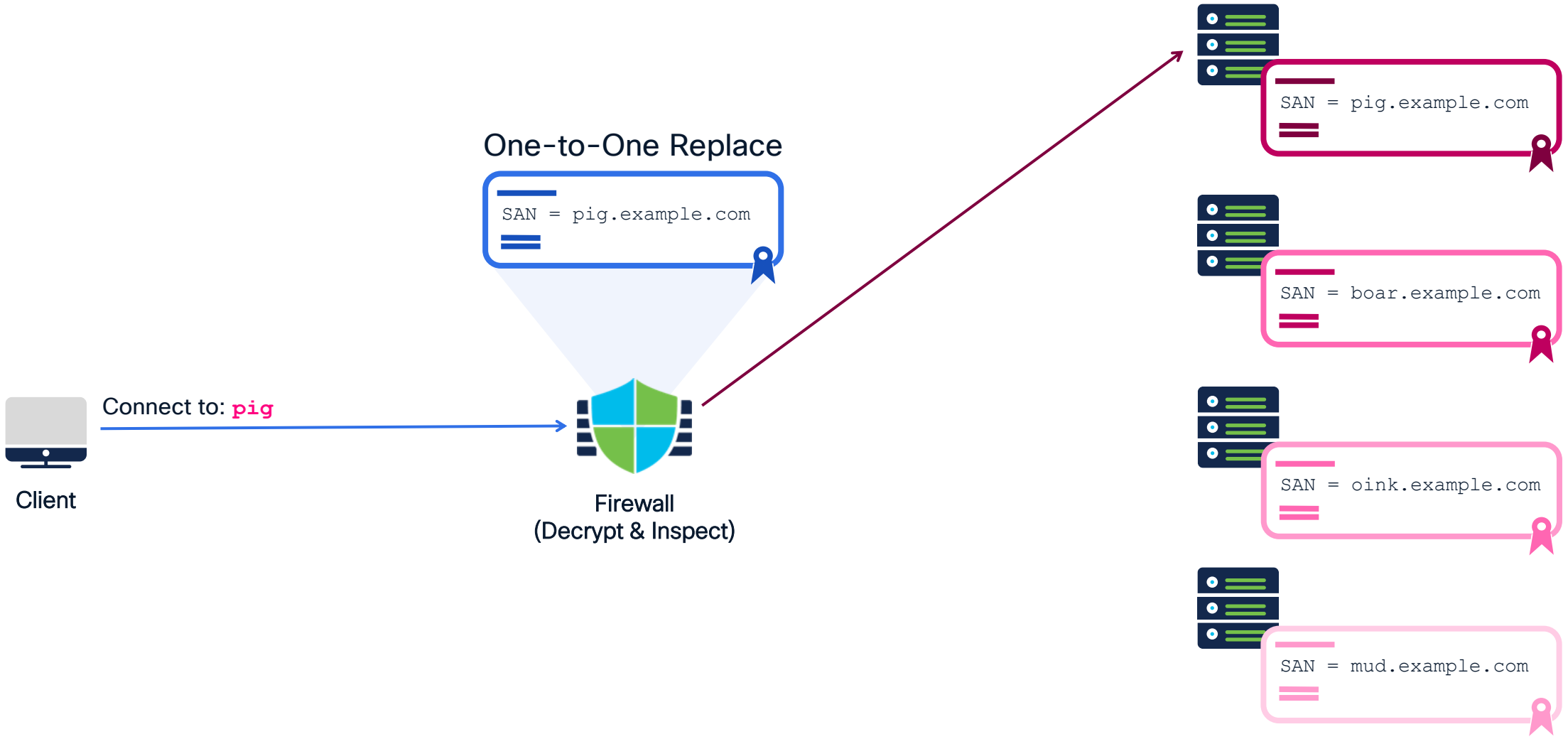


© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Certificate Replace – New Known-Key Decryption Method

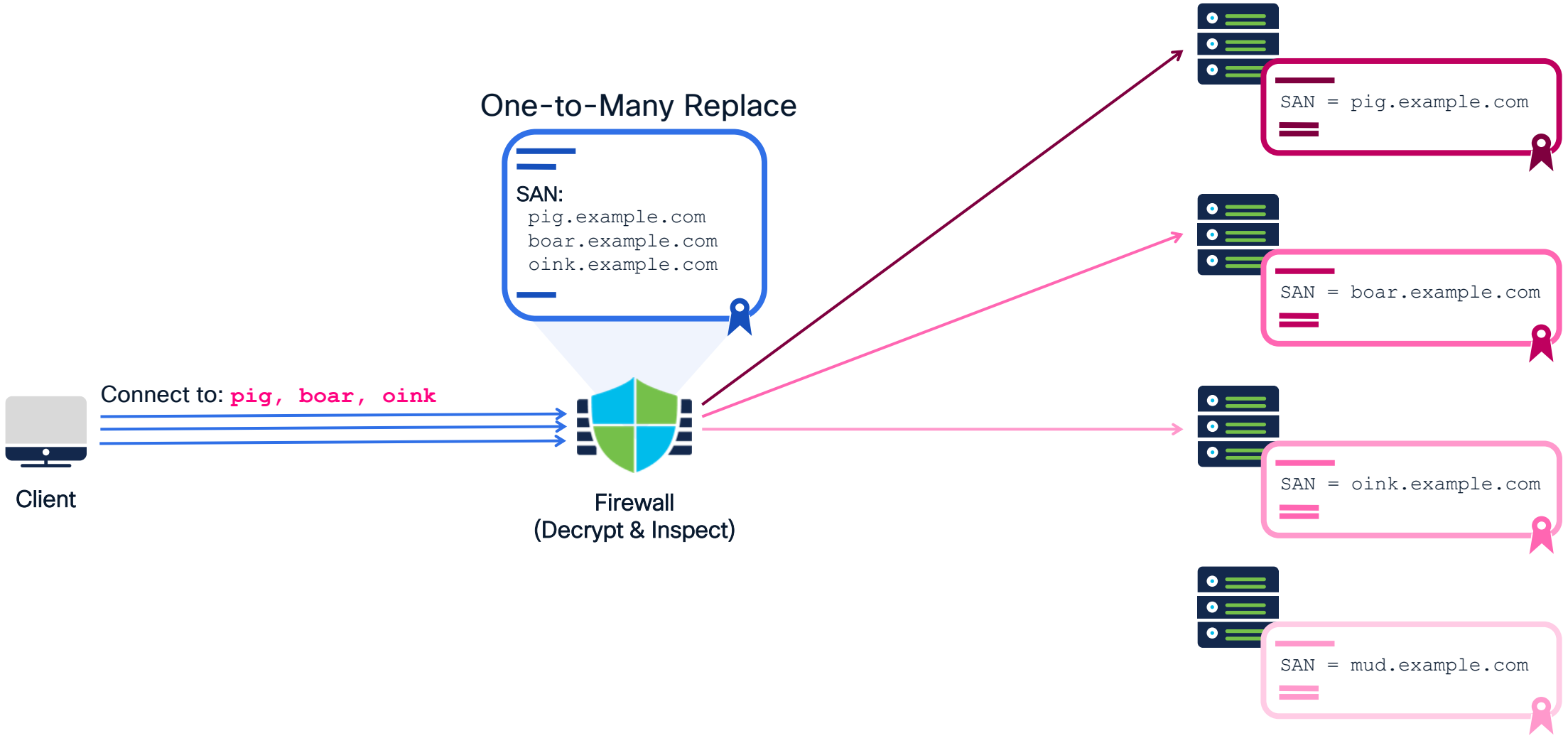
Single SAN Certificate Replace



© 2025 Cisco and/or its affiliates. All rights reserved.

Certificate Replace – New Known-Key Decryption Method

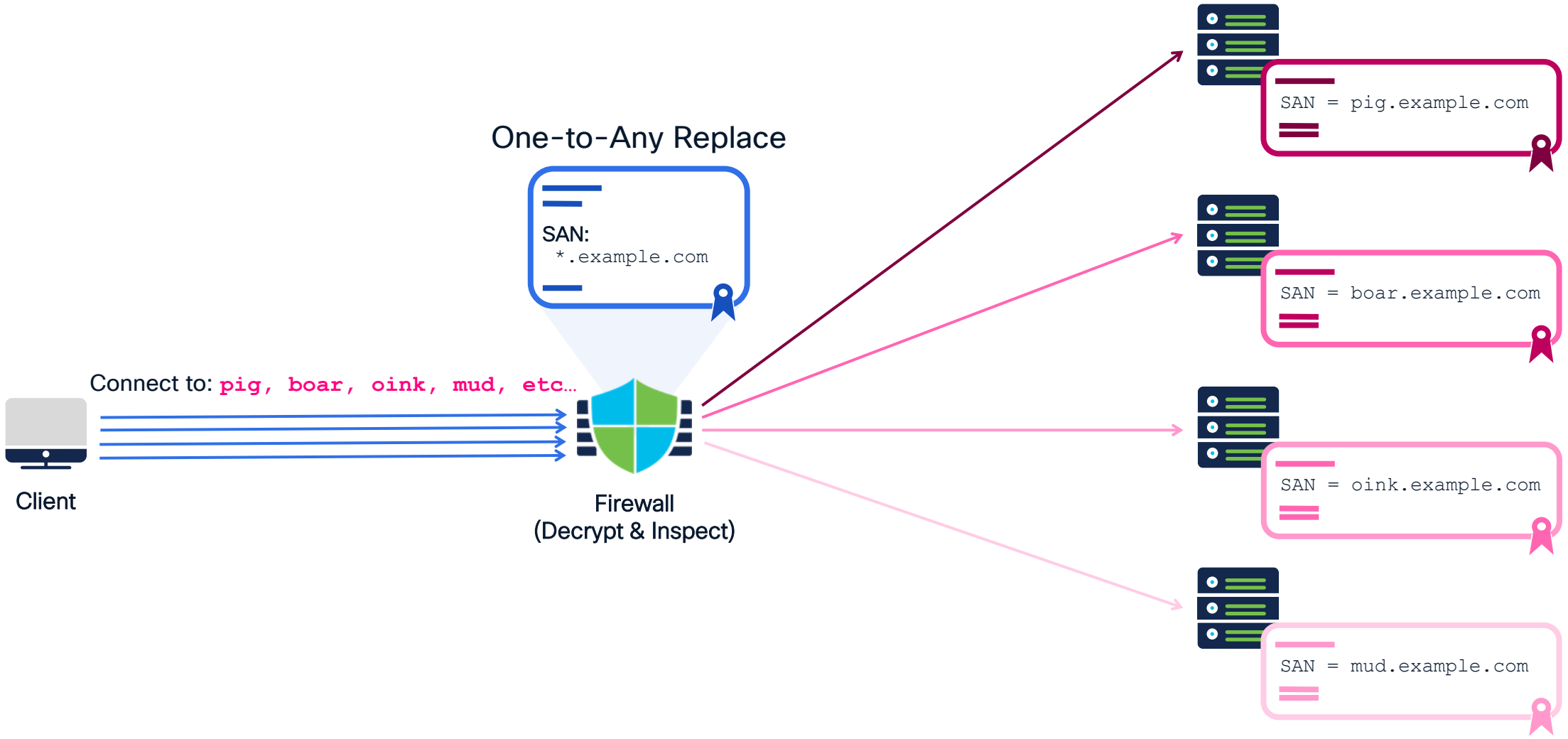
Multi-SAN Certificate Replace



© 2025 Cisco and/or its affiliates. All rights reserved.

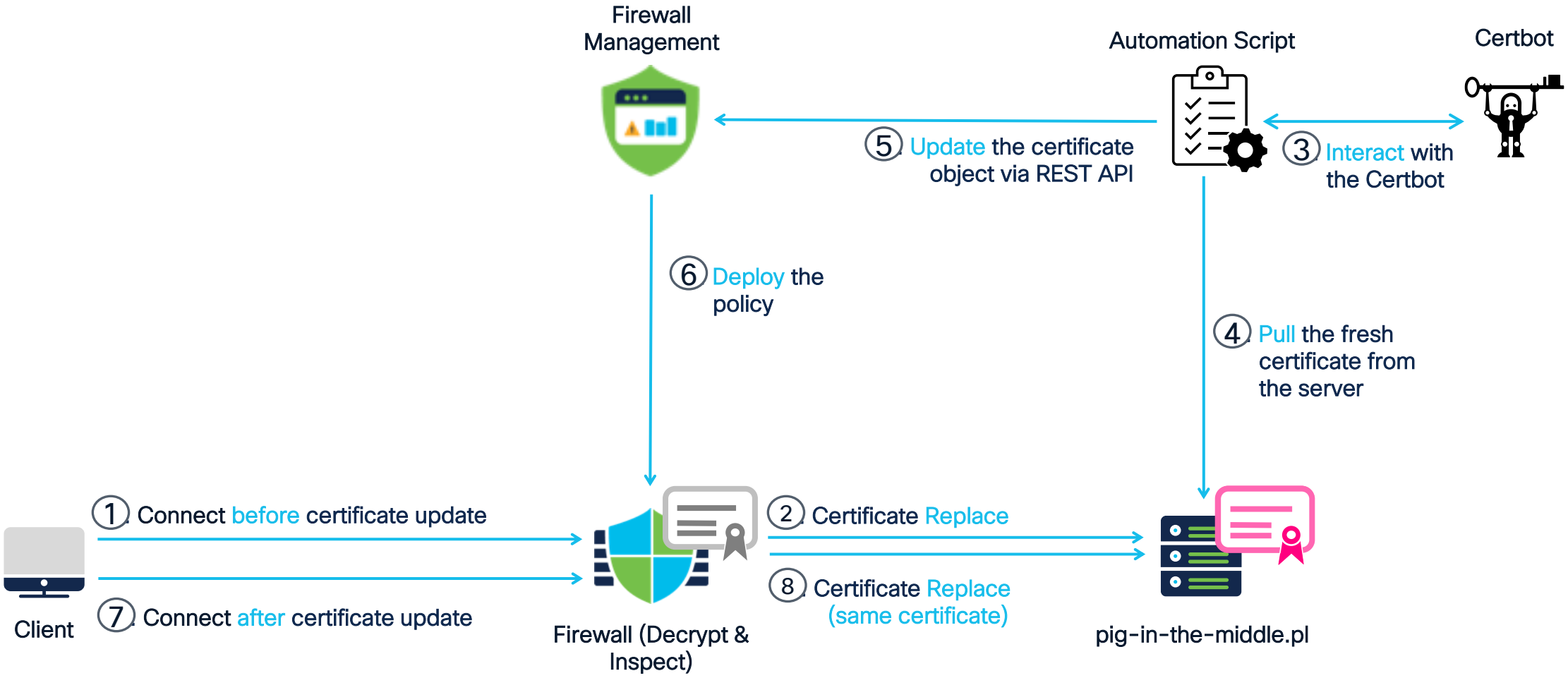
Certificate Replace – New Known-Key Decryption Method

Wildcard Certificate Replace



© 2025 Cisco and/or its affiliates. All rights reserved.

Automatic Certificate Management Environment (ACME)



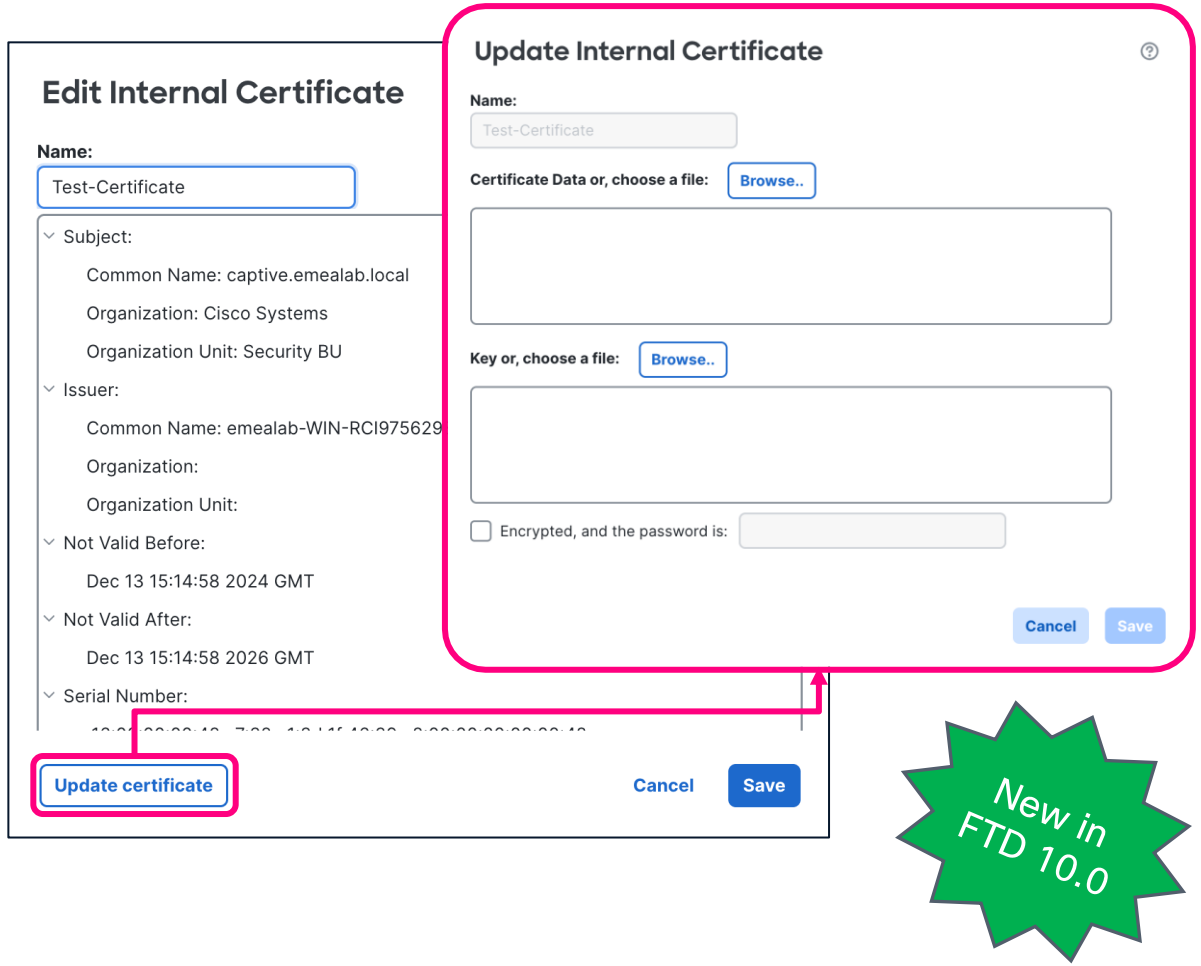
© 2025 Cisco and/or its affiliates. All rights reserved.

Streamline Certificate Updates – User Interface and REST

- Update an existing object with a new certificate
- Decryption Policy remains unchanged
- Update certificate object and re-deploy

- Available in FMC UI and via REST API:

GET	/api/fmc_config/v1/domain/{domainUUID}/object/internalcertificates
POST	/api/fmc_config/v1/domain/{domainUUID}/object/internalcertificates
DELETE	/api/fmc_config/v1/domain/{domainUUID}/object/internalcertificates/{objectId}
GET	/api/fmc_config/v1/domain/{domainUUID}/object/internalcertificates/{objectId}
PUT	/api/fmc_config/v1/domain/{domainUUID}/object/internalcertificates/{objectId}



© 2025 Cisco and/or its affiliates. All rights reserved.

DEMO:

Certificate Update with REST API

© 2025 Cisco and/or its affiliates. All rights reserved.

Certificate Management – Key Takeaways

- When certificate lifetime drops to 47 days by 2029 – **manual renewal is unsustainable**
- Simplify with certificate replace – 1 wildcard certificate = decrypt entire domain (*.example.com) – backend certificates are not exposed to the end users
- **Implement ACME or other Certificate Lifecycle Management (CLM) solutions NOW** – don't wait for the first outage
- Manual certificate renewal takes around **45 minutes vs. 30 seconds** with CLM-powered automation* – multiply by hundreds of certificates...

© 2025 Cisco and/or its affiliates. All rights reserved.

* - https://www.sectigo.com/resource-library/reducing-risk-costs-high-volume-certificate-environments

Post Quantum Cryptography

What's the big deal about Quantum Computing?

Quantum computing:

- Is a fundamentally new model of computation
- Enables an **exponential speed-up** for specific mathematical problems

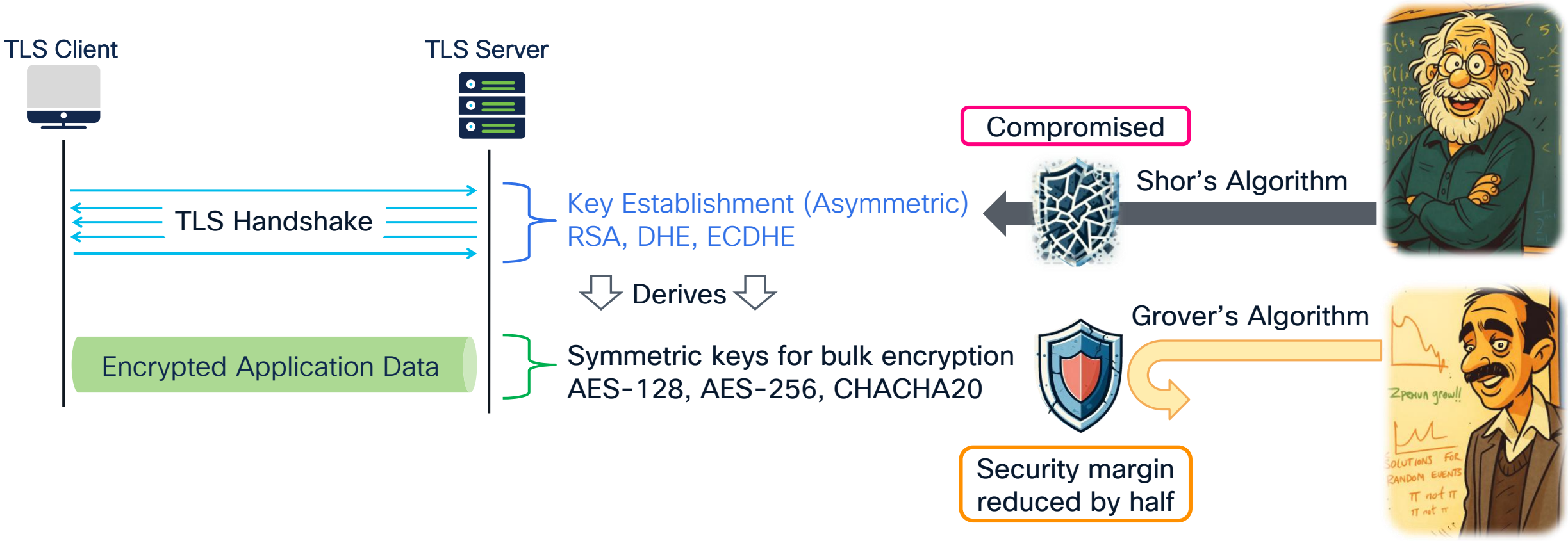
The impact:

- Poses a serious **long-term threat** to **data confidentiality**
  - "Harvest now, decrypt later" – becomes a real concern
- **Cryptographically relevant** quantum computers expected within **5-15 years**
- Breaking today's encryption will be **extremely costly – but feasible** for well-funded actors
- Anticipate **targeted attacks** on the **highest value data**:
  - state secrets, intellectual property, executive communications

That is still sometime in the future... but inevitable...

© 2025 Cisco and/or its affiliates. All rights reserved.

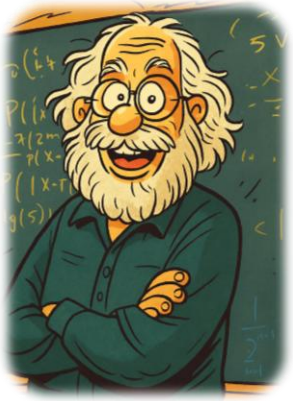
How does quantum computing affect TLS security?



© 2025 Cisco and/or its affiliates. All rights reserved.

The Impact on Asymmetric and Symmetric Cryptography

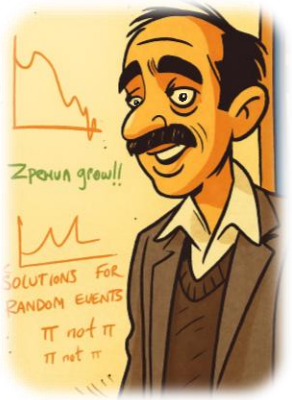
Peter Shor



Algorithm	Based On	Classical Computer Time	Shor's Algorithm Time on Quantum Computer (Future)
RSA-3072	Integer Factorization	~10^{25} years	Hours -> Weeks
ECC-256	Elliptic Curve Log	~10^{38} years	Hours -> Days

We need a new Quantum-Resistant public key algorithm.

Lov Grover



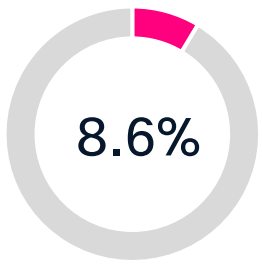
AES Key Size	Grover's Effective Attack (Brute-Force)	Effective Key Strength
AES-128	~2^{64} operations	Equivalent to 64-bit key
AES-256	~2^{128} operations	Equivalent to 128-bit key

Doubling symmetric key size provides Quantum-Safety.

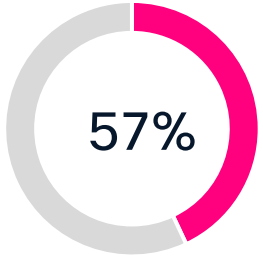
© 2025 Cisco and/or its affiliates. All rights reserved.

How Much Traffic on The Internet is Quantum Safe?

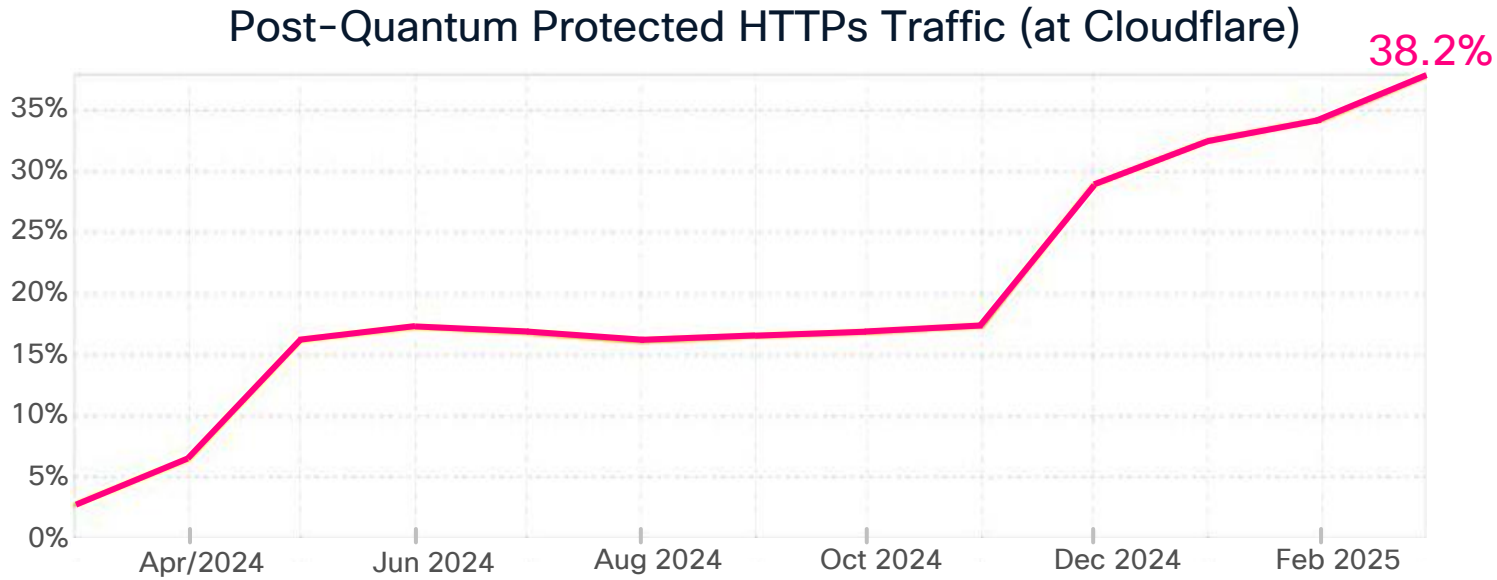
- ML-KEM requires server-side and client-side support



of top 1M sites support PQC*



of browser requests propose PQC*



Source: Cloudflare Signals Report 2025

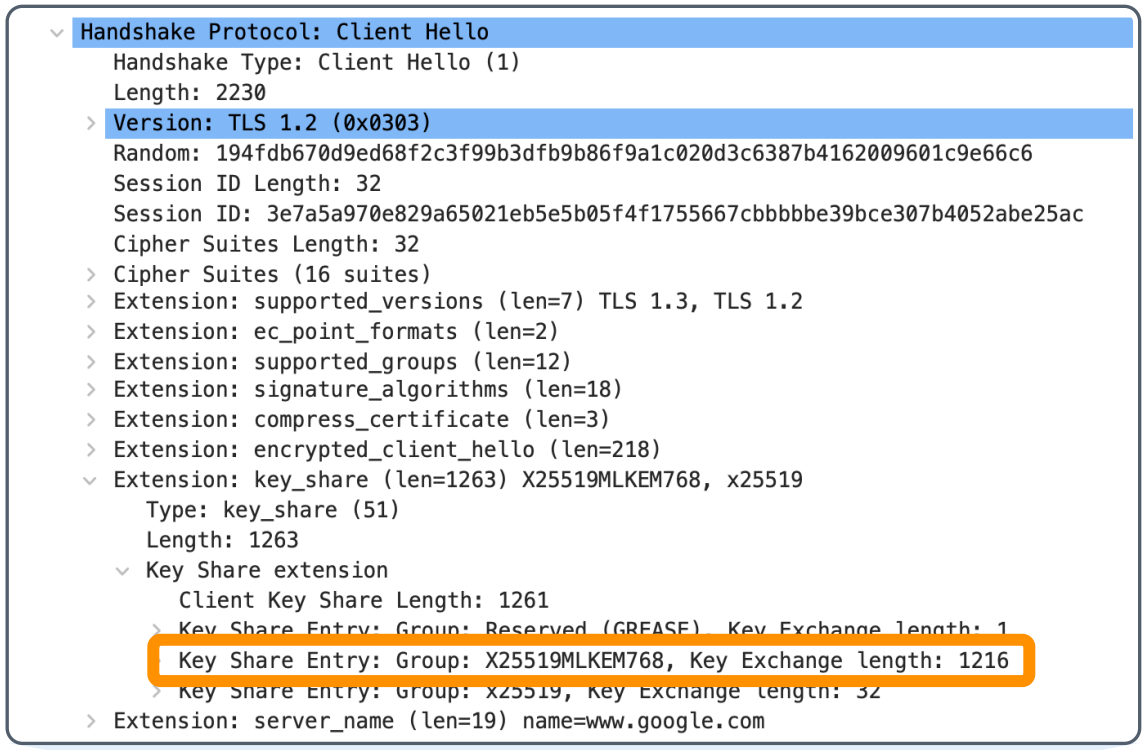
- **Client-side support:**
  - Firefox 132+(Oct/2024)
  - Chrome/Edge 131+ (Nov 2024)
  - Safari 26+ (Sep/25)

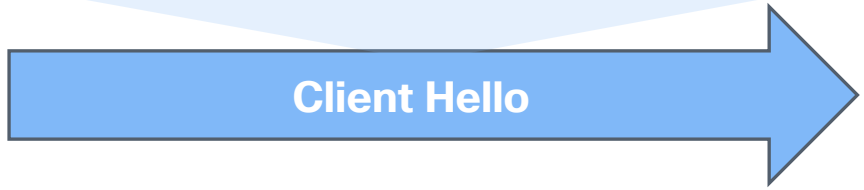
Module-Lattice Key-Encapsulation Mechanism (ML-KEM) – post-quantum key encapsulation mechanism based on **mathematical problem designed to resist quantum attacks**.

*Source: https://www.f5.com/labs/articles/the-state-of-pqc-on-the-web (data from June/25)

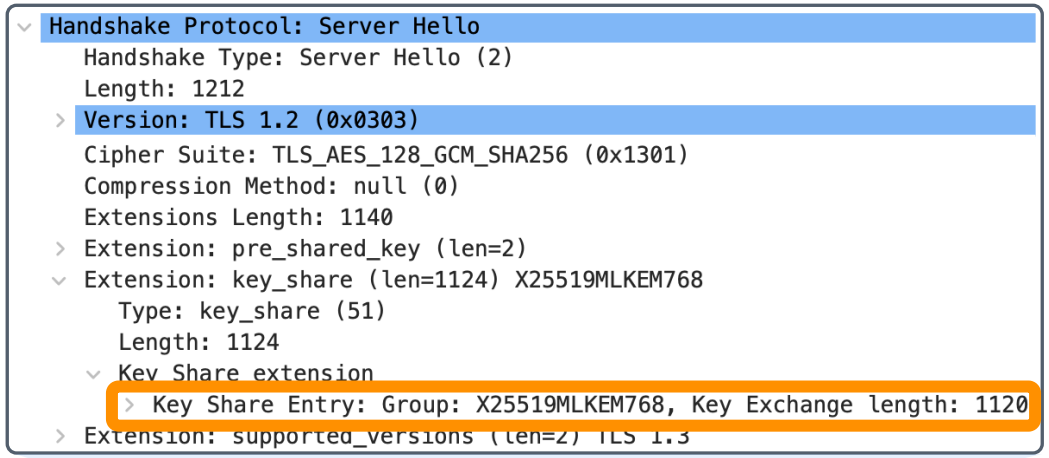
© 2025 Cisco and/or its affiliates. All rights reserved.

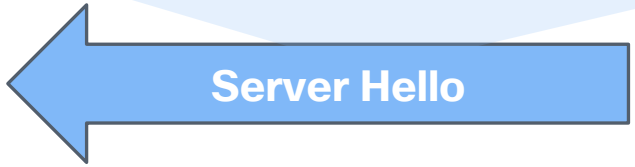
How to check if my connection is Quantum Safe?





Client

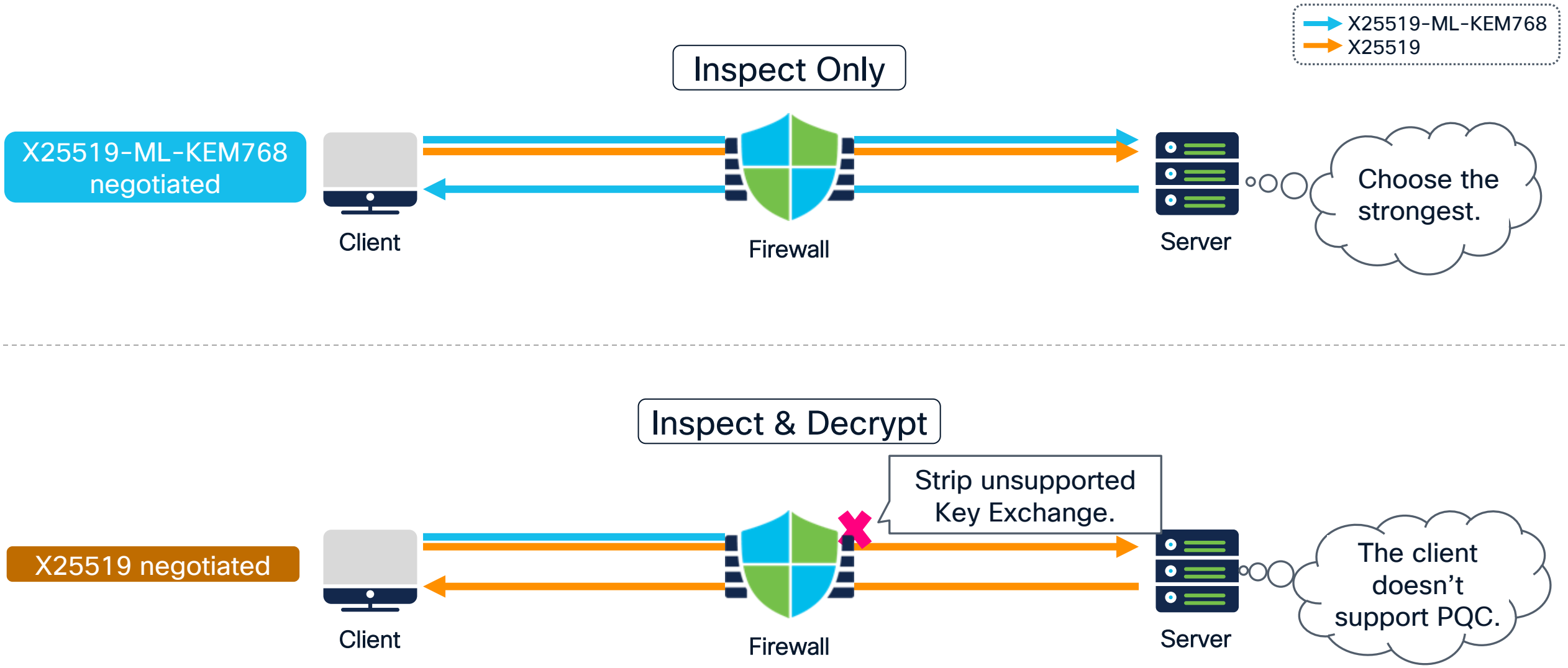




Server

© 2025 Cisco and/or its affiliates. All rights reserved.

Quantum Resistant Key Exchange Through a Firewall



© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Post-Quantum Cryptography - Key Takeaways

- Quantum computers will break RSA/ECC within 5-15 years – **"harvest now, decrypt later" is real**.
- Put yourself in the attacker's shoes: **What encrypted data in YOUR network is worth paying to store for a decade, waiting for quantum computers to crack it open?**
- **Enable TLS 1.3 everywhere to support hybrid PQC key exchange** – 57% of browsers already propose ML-KEM768
- Hardware refresh cycles: **ensure new security infrastructure purchases include PQC support** – retrofitting is expensive
- Consider PQC downgrade when firewall decrypts for inspection – **Cisco Secure Firewall will support ML-KEM768 in CY26**

© 2025 Cisco and/or its affiliates. All rights reserved.

Conclusions

The security is going dark...

Your Action Plan – Priority Matrix

IMMEDIATE (Next 30 days)

- Enable EVE and update to VDB including ECH Servers AppID
- Audit encrypted DNS settings – implement strict DNS control
- Review certificate inventory – identify manual renewal risks
- Baseline QUIC and ECH traffic in you network

SHORT-TERM (Next 90 days)

- Evaluate ACME/CLM solution for certificate automation
- Implement selective TLS/QUIC decryption for critical traffic
- Test ECH downgrade for known CDN servers
- When on 10.0 enable Shadow Traffic detection on all FTD devices
- Review PQC readiness (TLS 1.3 everywhere)

STRATEGIC (Next 6-12 Months)

- Design security stack assuming zero clear-text visibility
- Prepare for post-quantum cryptography migration – watch out for software updates
- Train security teams on encrypted visibility techniques

© 2025 Cisco and/or its affiliates. All rights reserved.

cisco

Please share your feedback and ideas

Before leaving the room, please share your feedback on this session!

- It is very important for me personally and ...
- ... your comments, feedback and ideas provide **the most valuable input** for our engineering

© 2025 Cisco and/or its affiliates. All rights reserved.

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to claim a Cisco Live T-Shirt.

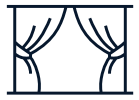
Earn up to 800 points by completing all surveys and climb the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live Events app.

© 2025 Cisco and/or its affiliates. All rights reserved.

Continue your education



Visit the Cisco Stand for related demos

Book your one-on-one Meet the Expert meeting

Attend the interactive education with Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: cgrabows@cisco.com

© 2025 Cisco and/or its affiliates. All rights reserved.

Thank you

CISCO