



January Announcements

- ▶ GoCyber 501c3 Update
- ▶ OISC 2024 Conference Registration Open
- ▶ Seeking Additional SIG's
- ▶ February 2024 - MFA 101 - Yubikey/FIDO/FIDO2



Decrypt, Defend, Prevail

Deep SSL Inspection for the Real World

Presented at the GoCyber Collective
January 17th, 2024

Victor Weis
Systems Engineer
Fortinet



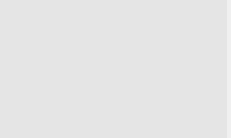




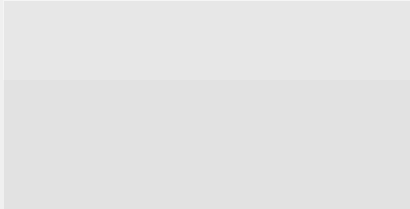


Why Deep SSL Inspection Is Essential to Network Security

You can't block what you can't see

...Or...

The exfils will continue until decryption improves



Why give a talk on Deep SSL Inspection?

My thesis

- Deep SSL Inspection is more important and more achievable than you think
- To the extent I can convince you of that, this talk will have been a success
- Moreover, I hope to arm you with the info needed for consensus-building in your org



Why give a talk on Deep SSL Inspection?

Deep SSL Inspection is as important as robust Backup and Disaster Recovery (BDR) solutions

- BDR is the last-line of defense against 1st-Order Ransomware
 - Cryptolocking compromises Integrity and Availability
- Data Leak Prevention (DLP) is the last-line of defense against 2nd-Order Ransomware
 - Exfiltration compromises Confidentiality
- DLP requires Deep SSL Inspection
- Double-Extortion Ransomware is now the norm
- Both BDR and DLP with Deep SSL Inspection are now essential, and for the same reasons
- Don't get stuck paying the ransom!



Preliminary Notes

Tomayto, Tomahto

Terminology:

- In this presentation, I will use “SSL” and “TLS” interchangeably
- “Deep SSL Inspection” = “SSL/TLS Decryption” = “Deep Packet Inspection”
- “Firewall” / “Middlebox” will refer to any network device that transforms, inspects, and filters traffic for purposes other than packet forwarding
 - This applies equally to hardware and software/virtual/cloud firewalls

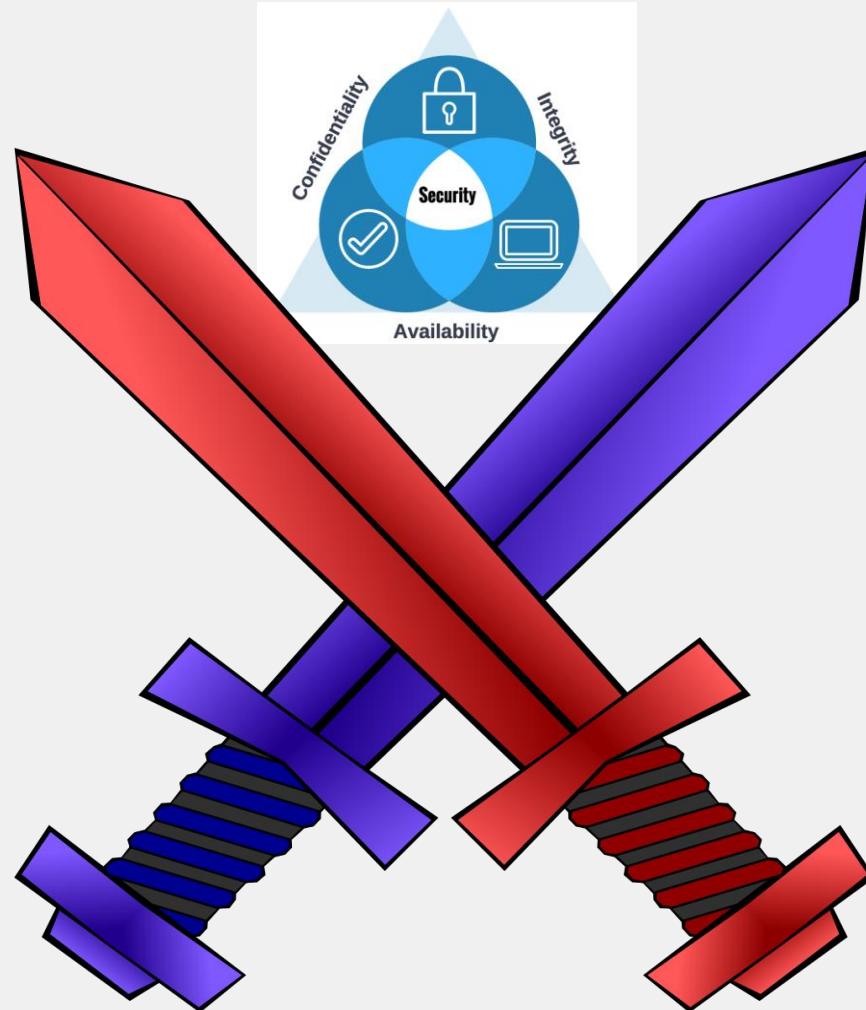
Vendor Notes:

- Fortinet solutions will be used in the examples, but the principles should apply to any environment



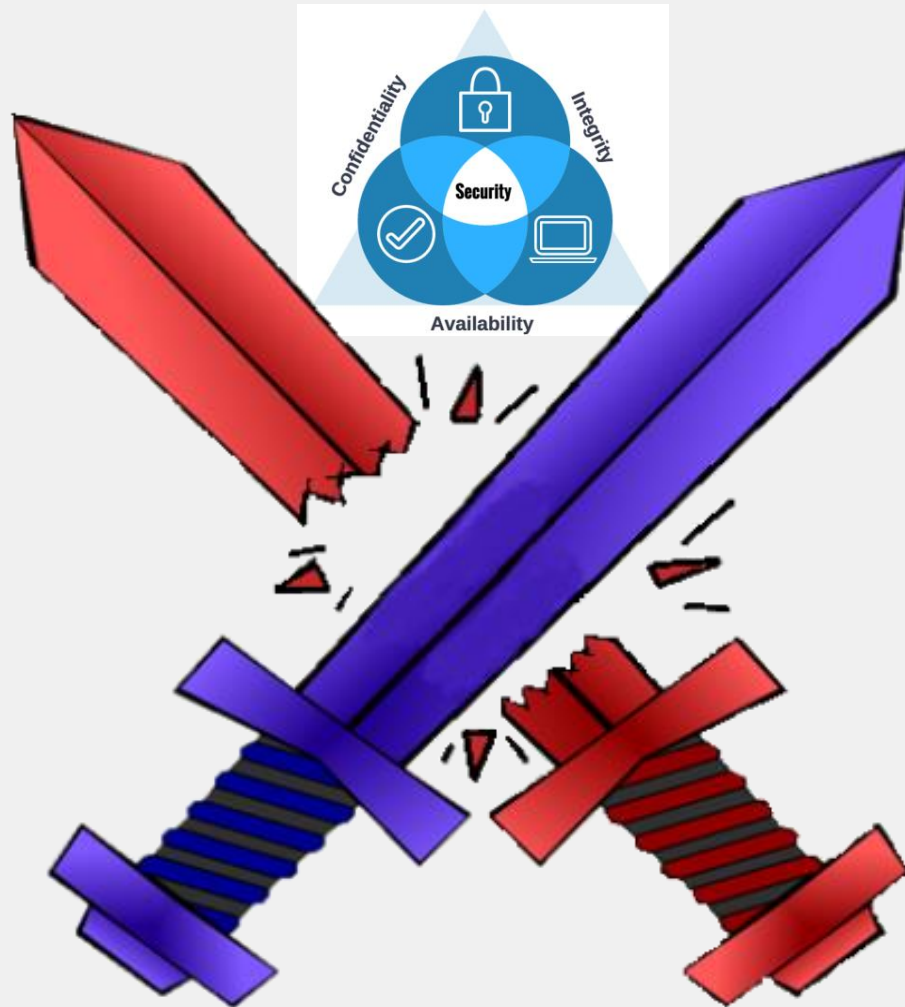
Encryption: The Double-Edged Sword

In cyber warfare, encryption is a weapon, for both the good guys and the bad guys



Gain the Upper-Hand with Deep SSL Inspection

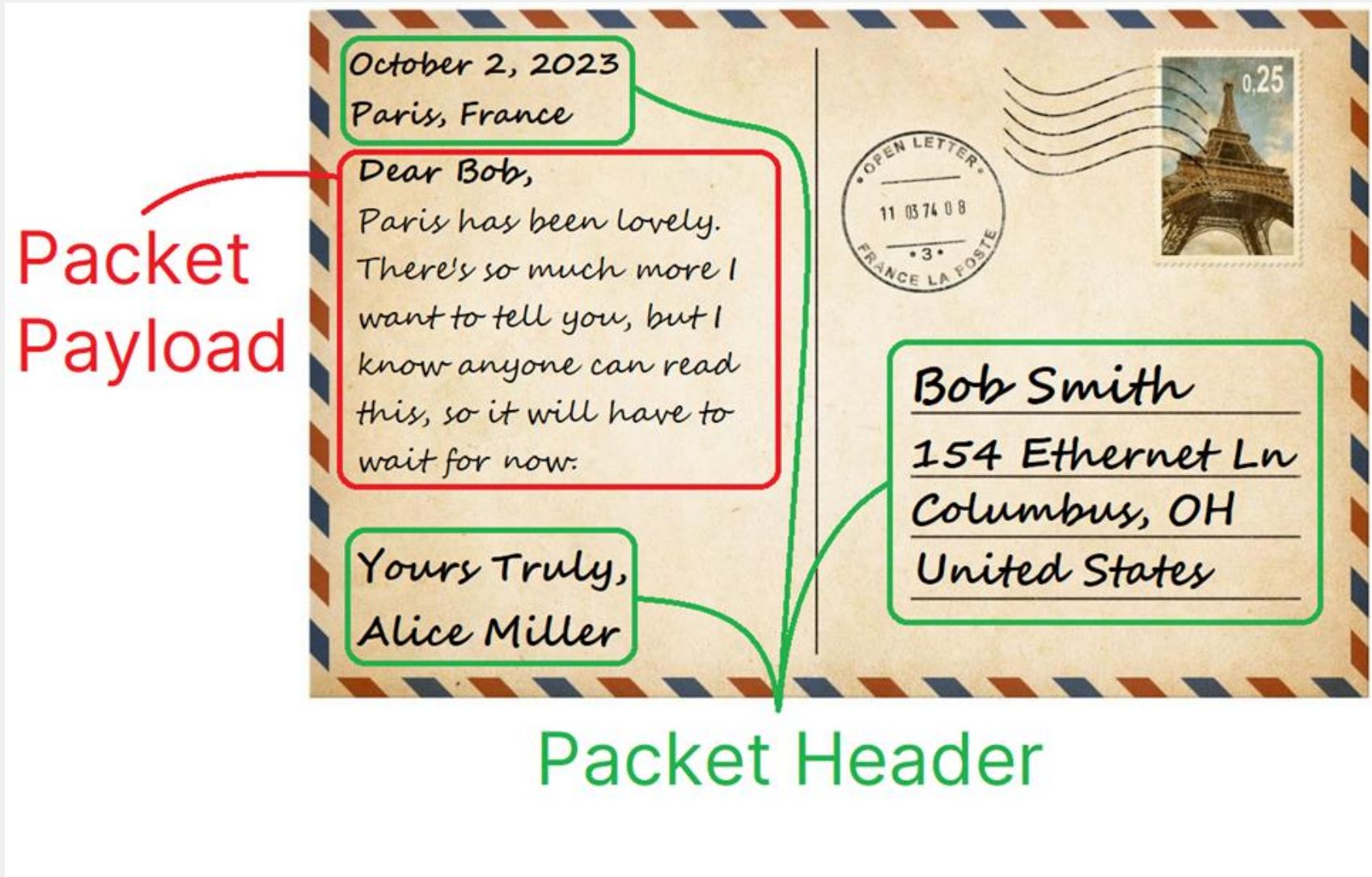
Achieve the best of both worlds



What is SSL Encryption?

Postcards vs Envelopes

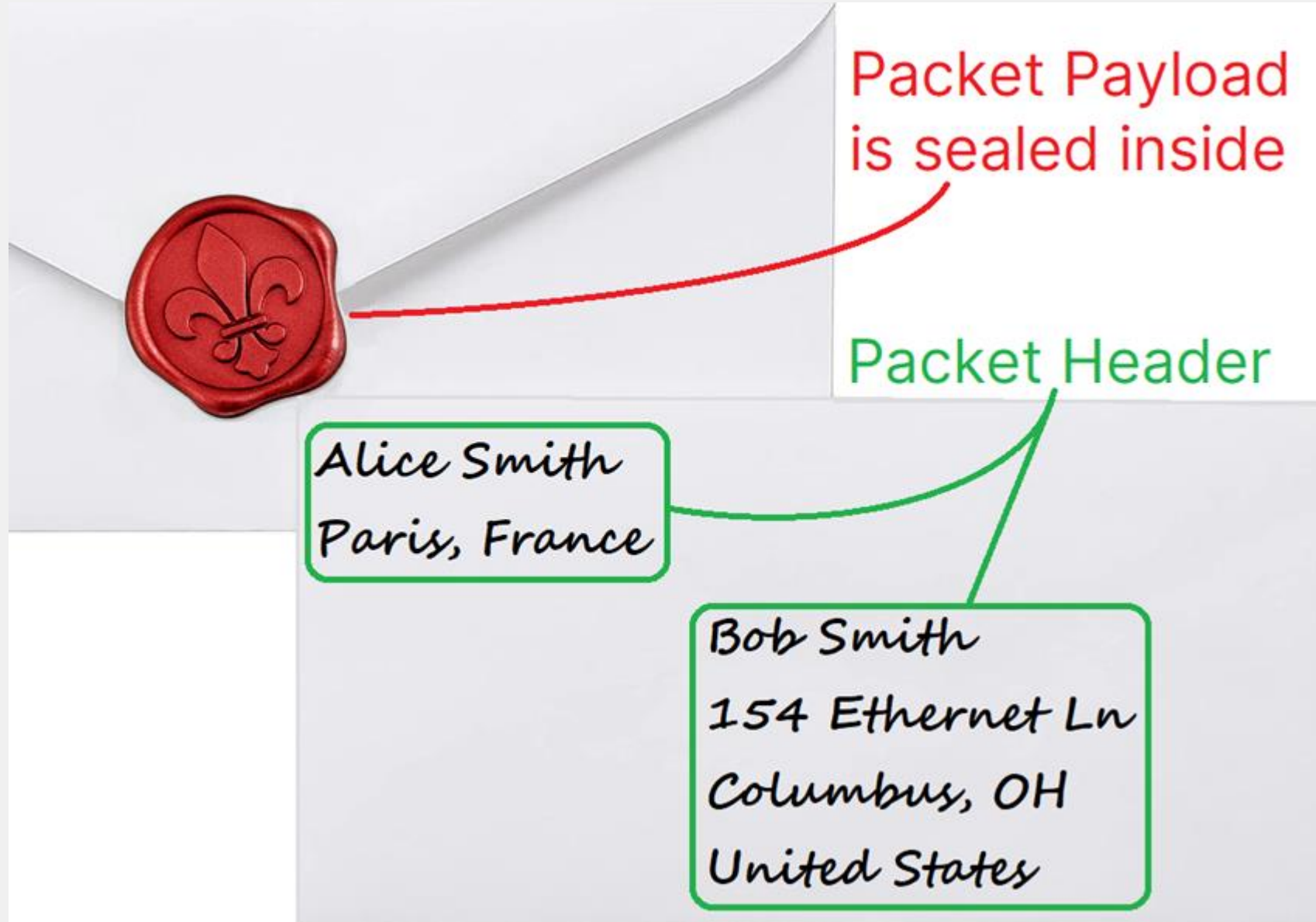
- Data is sent over the network in packets
- Packets have a header to get them to their destination
- Packets also have a payload: the contents of the message
- Unencrypted packets are like using a postcard
- Anyone can see the contents of the message (and tamper with it!)



What is SSL Encryption?

Postcards vs Envelopes

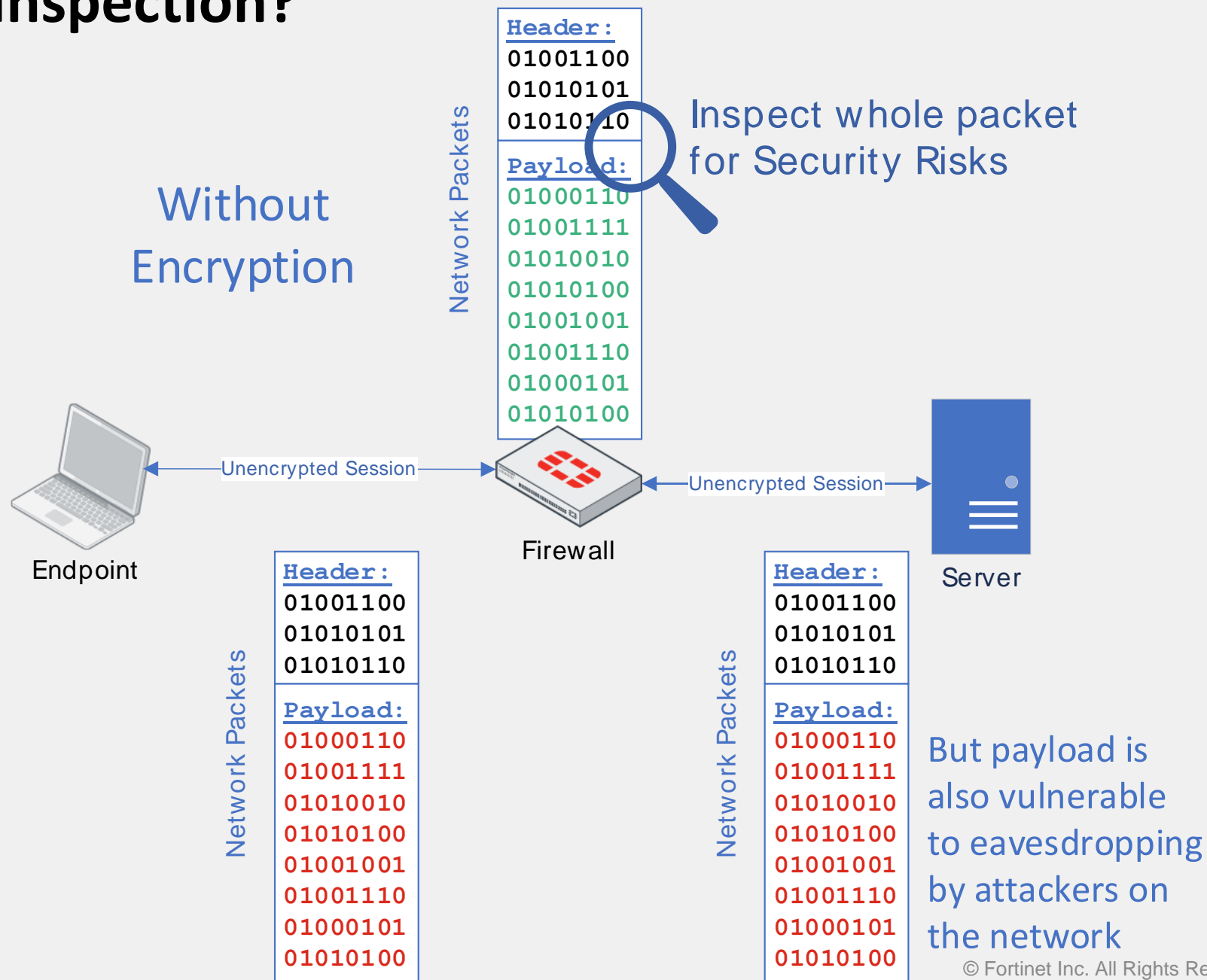
- Encrypted packets are like using an envelope
- Only the header may be seen in transit
- The message contents are sealed inside the envelope
- The seal can also reveal tampering attempts



What is Deep SSL Inspection?

A History Lesson

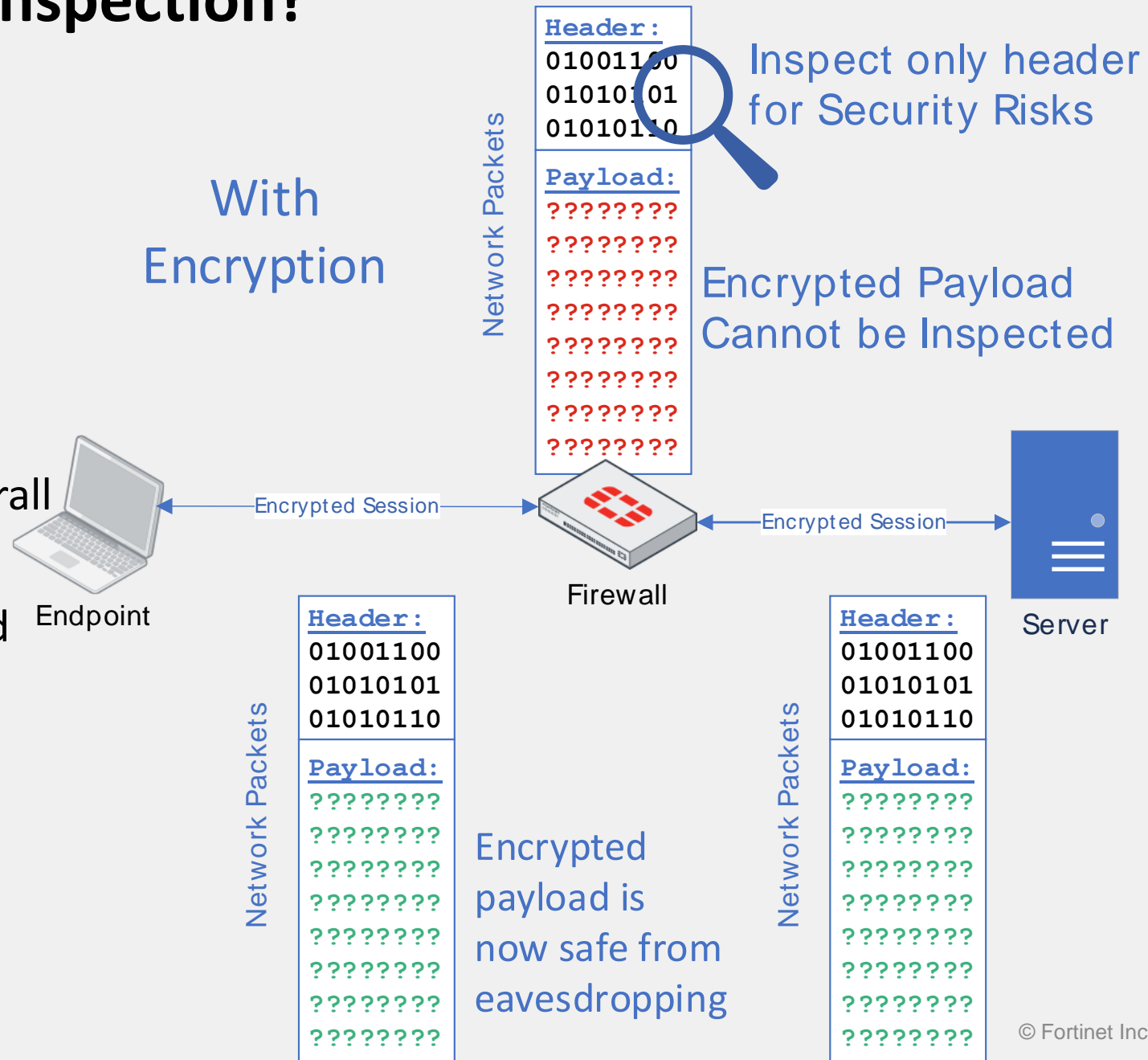
- In the early days, most packets were unencrypted
- Easy for firewalls to inspect for security risks
- But vulnerable to eavesdropping and tampering by attackers



What is Deep SSL Inspection?

A History Lesson

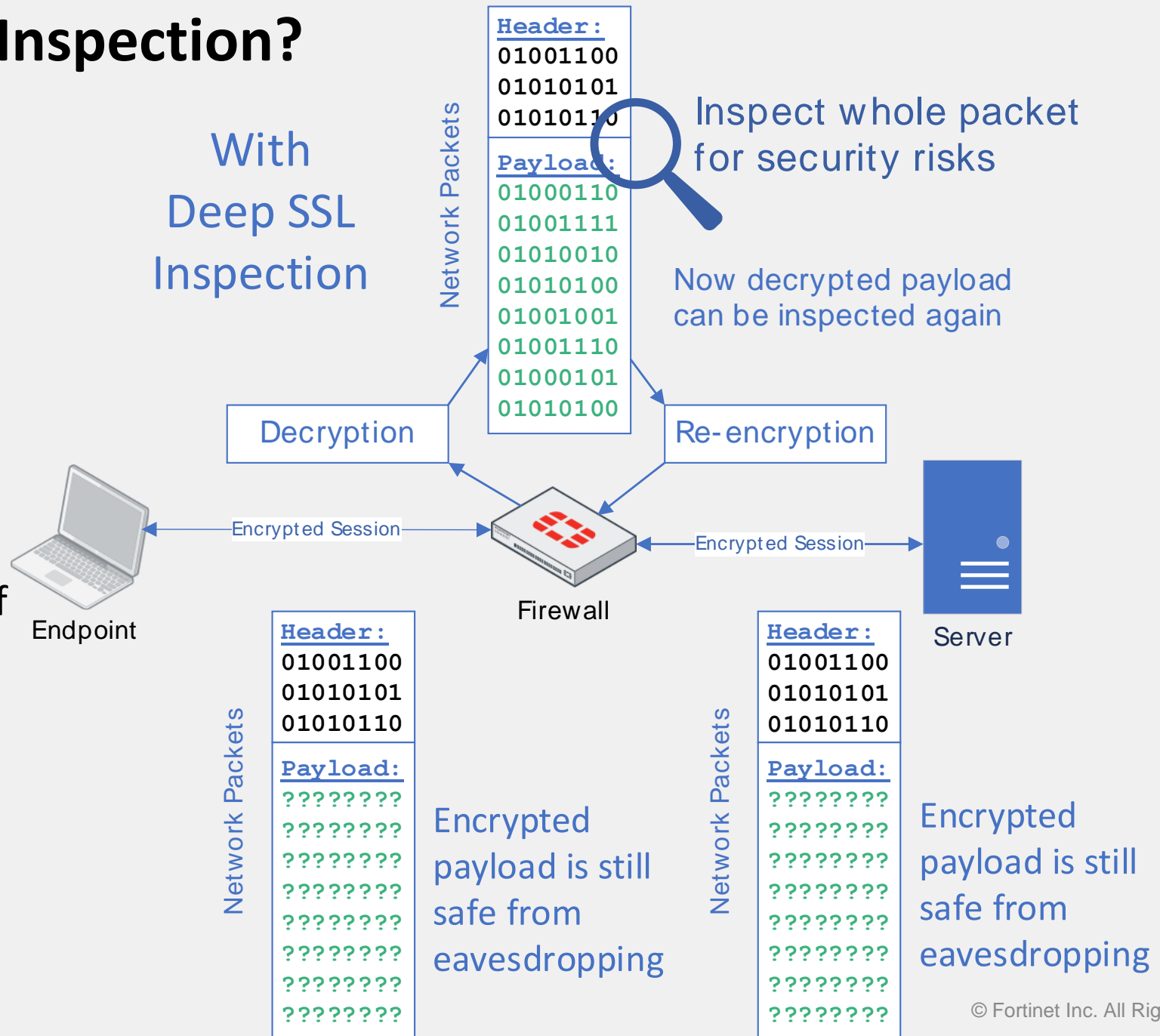
- SSL encryption prevents eavesdropping and tampering
- But now firewalls can't inspect the full packet
- This greatly reduces overall security effectiveness
- Attackers quickly learned they could hide attacks using SSL encryption of their own



What is Deep SSL Inspection?

A History Lesson

- To thwart attackers' encryption Deep SSL Inspection is needed
- Decrypt, inspect, and re-encrypt the traffic in real-time
- This restores the security effectiveness of the firewall



How much of each packet is encrypted?

Almost all of it!

Is there malware lurking in the encrypted data?

Phishing links?

Data exfiltration?

Only way to know is Deep SSL Inspection!

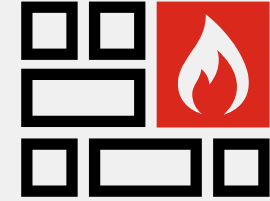
```
> Frame 17: 1288 bytes on wire (10304 bits), 1288 bytes captured (10304 b
> Ethernet II, Src: Dell_c4:8e:91 (38:14:28:c4:8e:91), Dst: Fortinet_3f:02
> Internet Protocol Version 4, Src: 172.19.182.5, Dst: 54.177.212.176
v Transmission Control Protocol, Src Port: 7463, Dst Port: 443, Seq: 2396,
  Source Port: 7463
  Destination Port: 443
  [Stream index: 0]
  [Conversation completeness: Incomplete, DATA (15)]
  [TCP Segment Len: 1234]
  Sequence Number: 2396 (relative sequence number)
  Sequence Number (raw): 3467870913
  [Next Sequence Number: 3630 (relative sequence number)]
  Acknowledgment Number: 4934 (relative ack number)
  Acknowledgment number (raw): 3643476212
  0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
  Window: 1026
  [Calculated window size: 262656]
  [Window size scaling factor: 256]
  Checksum: 0xf6b7 [unverified]
  [Checksum Status: Unverified]
  Urgent Pointer: 0
  v [Timestamps]
    [Time since first frame in this TCP stream: 0.779467000 seconds]
    [Time since previous frame in this TCP stream: 0.000000000 seconds]
  > [SEQ/ACK analysis]
    TCP payload (1234 bytes)
    TCP segment data (1234 bytes)
  > [2 Reassembled TCP Segments (2694 bytes): #16(1460), #17(1234)]
v Transport Layer Security
  v TLSv1.3 Record Layer: Application Data Protocol: Hypertext Transfer Pr
    Opaque Type: Application Data (23)
    Version: TLS 1.2 (0x0303)
    Length: 2689
    Encrypted Application Data: 45d06ccbc42bb7e6dd6bfb1958c3b55df4a189
    [Application Data Protocol: Hypertext Transfer Protocol]
```

0000	17 03 03 0a 81	45 d0 6c	cc bc 42 bb 7e 6d d6 bfE.l ..B~m..
0010	bb 19 58 c3 b5 5d f4 a1	89 cb b1 2f 70 ce 65 74	..X..].. .. /p.et	
0020	c2 b2 2a bc ac ac 9b 66	e4 fe bf 4d 80 62 3a 74	..*...f ..M:b:t	
0030	68 ff b6 42 92 2d 90 11	29 93 3c 06 b9 dd 8c f1	h..B...)<.....	
0040	56 c9 4a 32 df 8b 0e 80	b5 8c 6c 40 de 3e 9a fe	V.J2... ..l@>..	
0050	4f 04 26 33 c8 6c a0 e9	05 0a a2 69 47 37 d1 2e	0.&3.l... ..iG2..	
0060	ed 4f b5 03 f5 cf f6 08	f1 df e2 68 c1 32 22 bb	.0..... ..h.7"	
0070	02 4f fd c9 db 80 ae 84	cf 7c d1 b8 45 8c 93 ff	.0..... ..E... ..	
0080	1d f1 50 3e 05 2a 21 b1	87 b1 0a e9 a3 50 1e ba	..P>*! ..p... ..	
0090	f9 b4 e1 63 c1 3c a1 fd	f8 91 3e 2d 96 a5 26 3a	...c<... ..>..&:	
00a0	b8 a4 21 d2 09 21 10 8a	ff e2 26 4a 2b b9 25 24	..!..!.. ..&J+.%\$	
00b0	d0 b1 03 bf bd ab 1c db	af 1b 3e 81 34 e4 cf fa>.4... ..	
00c0	94 b4 15 7e e0 06 20 a2	6c 1a a0 35 e4 d8 d3 57	...~... .l.5...W	
00d0	06 11 ba a3 a2 6b 1a f2	f3 95 da ae e3 91 bc 1dk.	
00e0	80 bd fc f6 cd 5a 2a 14	fd cf af fc ea c3 8d 6eZ*	
00f0	f3 a1 39 09 3d a2 06 e5	3f c2 00 97 e3 71 de 85	..9+=... ?...q..	
0100	87 90 f9 35 c2 b6 04 a7	9a b5 dd 11 c3 02 59 67	..5.... ..Yg	
0110	ef 97 06 16 67 f2 68 bf	19 06 3d d3 45 84 f2 01	...g.h. ..=E... ..	
0120	55 be d7 f9 aa da 29 3d	96 8c 96 84 3b 82 32 1e	U.....)= ...;2..	
0130	f7 af e7 b3 3f 44 cd 7d	05 39 94 91 3a dd 9c 70	...?D.} .9...:p	
0140	ae a2 57 7c c3 8c ae 0b	ce 3f bd f5 a5 64 0b ae	..W ?...d..	
0150	b4 75 b0 04 99 9d bd d3	6f 02 e5 78 df 98 1c 05	.u..... o.x....	
0160	23 3d 23 f6 e0 65 28 7a	2b fa 63 58 d6 51 8e 47	#=#.e(z +cX.Q.G	
0170	78 d4 46 15 46 23 f3 29	d6 12 85 d3 30 b5 94 72	x.F.F#.) ...0..r	
0180	21 06 5a 13 7b 83 ab 37	a5 ec 2c 26 16 c0 8b 78	!Z.{.7 ..&...x	
0190	2d c6 be fd d7 0f f9 fa	0b 03 aa 64 e9 ee 1c 27d... ..	
01a0	72 9d 44 3d df 5d b8 bc	8c 76 4d 2b 0c 4e 5e 7c	r.D=].. ..vM+.F^	
01b0	65 35 41 7c 63 ed 82 8a	8c c7 06 f8 86 4d 1f 7d	e5A c... ..M.}	
01c0	d9 5b 79 c5 b7 39 d4 1a	25 85 20 c6 2c a0 2c 9c	.[y.9.. % . , ,	
01d0	b4 ff 6f 39 c6 fb 72 33	ca 0c b9 1c 10 9c 3d 93	..o9.r3	
01e0	cf de 35 eb d0 b7 a8 e3	64 de 9c 63 c8 70 94 32	..5..... d.c.p.2	
01f0	f5 06 1f 87 8e b8 83 7e	6f 21 42 c6 34 4c a9 1e~ o!B.4L..	
0200	a9 e6 b5 3e db 72 4b 79	45 11 cc a7 83 cc 52 e5	...>.rKy E.....R	
0210	e7 14 c4 00 b3 a4 6b c9	f5 c5 34 b3 54 d4 ea 2bk...T.+	
0220	58 a7 89 17 72 2f ab d3	73 84 97 10 91 b5 26 6a	X...r/.. s...&j	
0230	20 97 5a a3 f1 6f 85 21	ea ab 77 8b e3 8f 5d 37	.Z..o! ..w...]7	
0240	92 e9 b7 66 fd 1e 45 1b	1f 08 92 b2 5d a6 35 45	..f..E... ..]5E	
0250	82 9b f7 94 e7 25 80 29	b1 8d 16 d6 9c 3c cc 45%.)	
0260	5c b0 cf ca 7f 23 73 69	20 b7 c9 39 22 56 22 aa	\....#si ..9"V"	
0270	bc b1 eb 12 8d b0 46 bb	72 e2 71 38 d1 98 49 00F. r.q8.I.	



Visibility when HTTP is Encrypted (HTTPS)

A tale of two Google Forms links



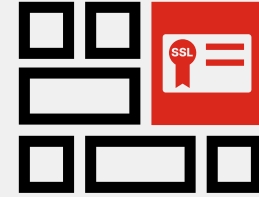
Without SSL Decryption, only the header is visible to the firewall

- Link 1: hxxps://forms.gle/[REDACTED]
 - Web Filter inspects: Category = **Web-Based Applications**
 - Looks benign... **Let it pass!**
- Link 2: hxxps://forms.gle/[REDACTED]
 - Web Filter inspects: Category = **Web-Based Applications**
 - Looks benign... **Let it pass!**

Are both of these URLs actually safe!?

Visibility when HTTPS get Decrypted

A tale of two Google Forms links



But with SSL Decryption, the firewall can see the payload too

- Link 1: [hxxps://forms.gle/GRFYjJwtDqVHVSf9A](https://forms.gle/GRFYjJwtDqVHVSf9A) ✓
 - Web Filter inspects: Category = **Web-Based Applications**
 - This site is safe: **Let it pass!**
- Link 2: [hxxps://forms.gle/DsW75p3St1dUMTyK6](https://forms.gle/DsW75p3St1dUMTyK6) !!!
 - Web Filter inspects: Category = **Phishing!**
 - This site is malicious: **Block it!**

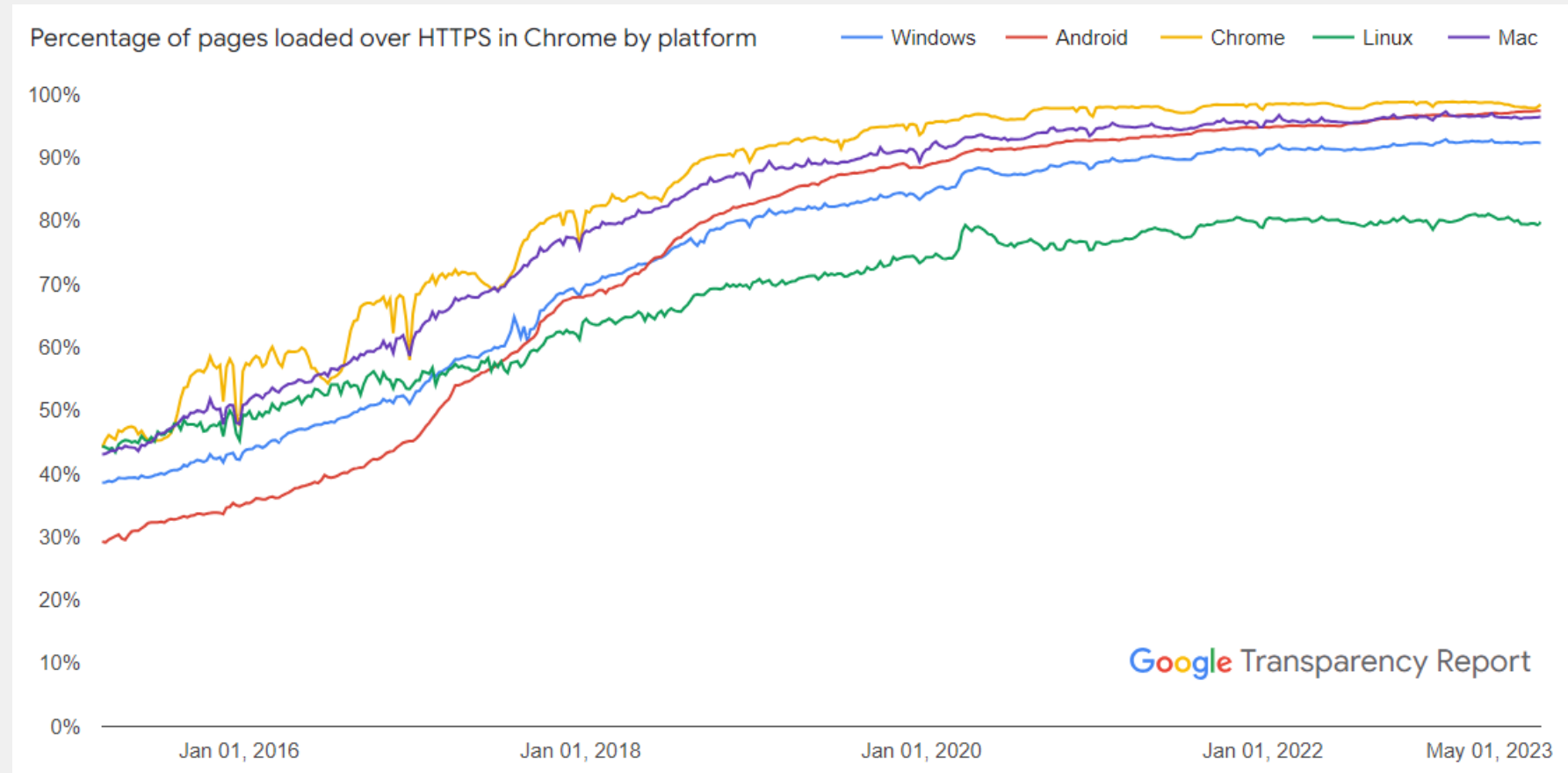
How many phishing attacks are getting through your firewall because the payload is invisible !?



How Prevalent is SSL Encryption?

Ubiquitous Encryption: Great for privacy, major challenges for security

- Strong encryption has become ubiquitous
- More than 90% of all web traffic is now encrypted
- This trend will only increase over time



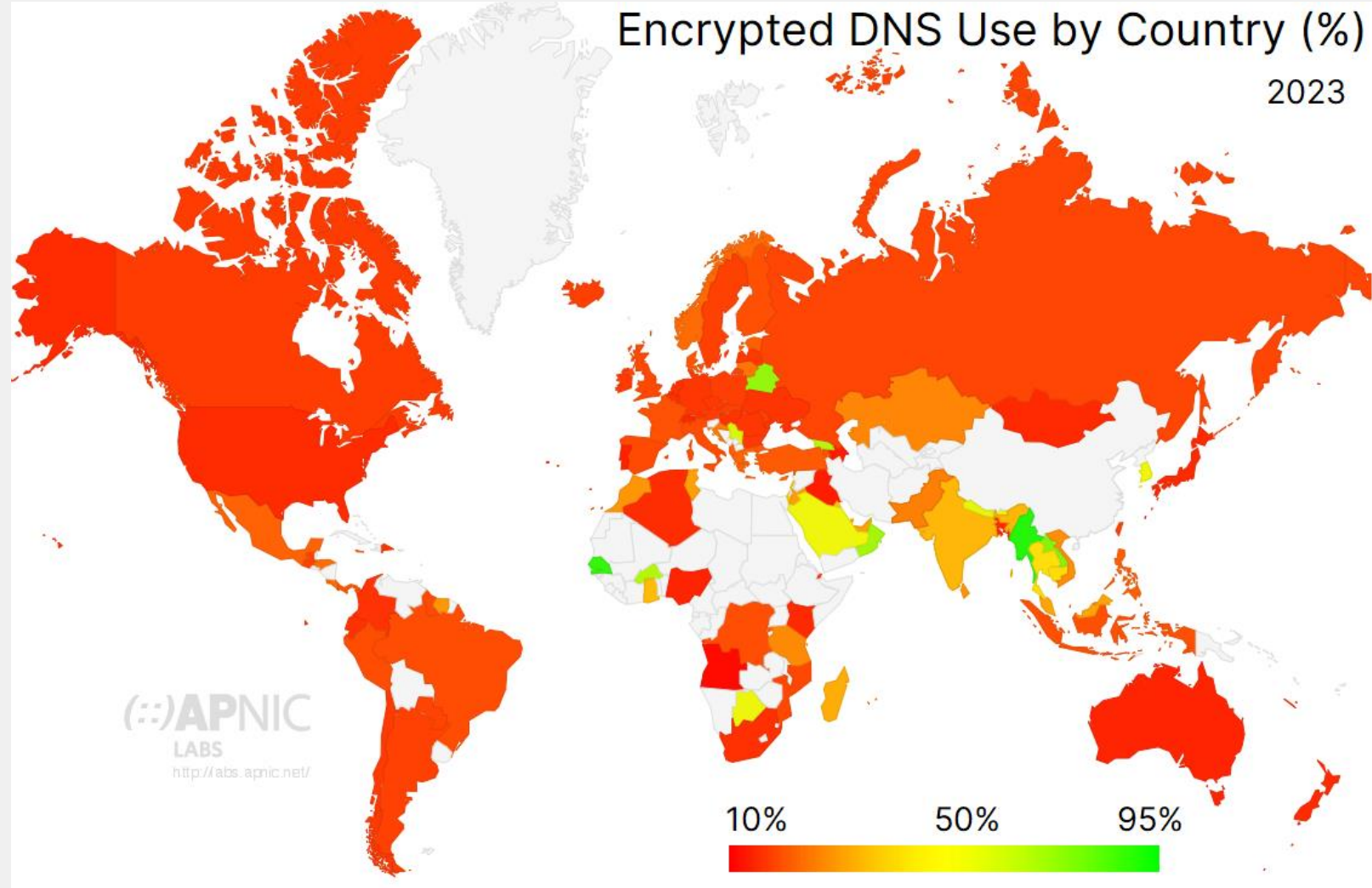
Source: <https://transparencyreport.google.com/https/overview>



DNS is Quickly Becoming SSL Encrypted Too

Your old-school DNS filters have no power here

- Many security teams rely on DNS filtering to block malicious traffic
- New encryption for DNS is rendering traditional filtering obsolete
 - DNS-over-TLS (DoT)
 - DNS-over-HTTPS (DoH)
 - DNS-over-QUIC (DoQ)
- Default in Chrome, Firefox, Android, etc.
- This trend will only increase as time goes on



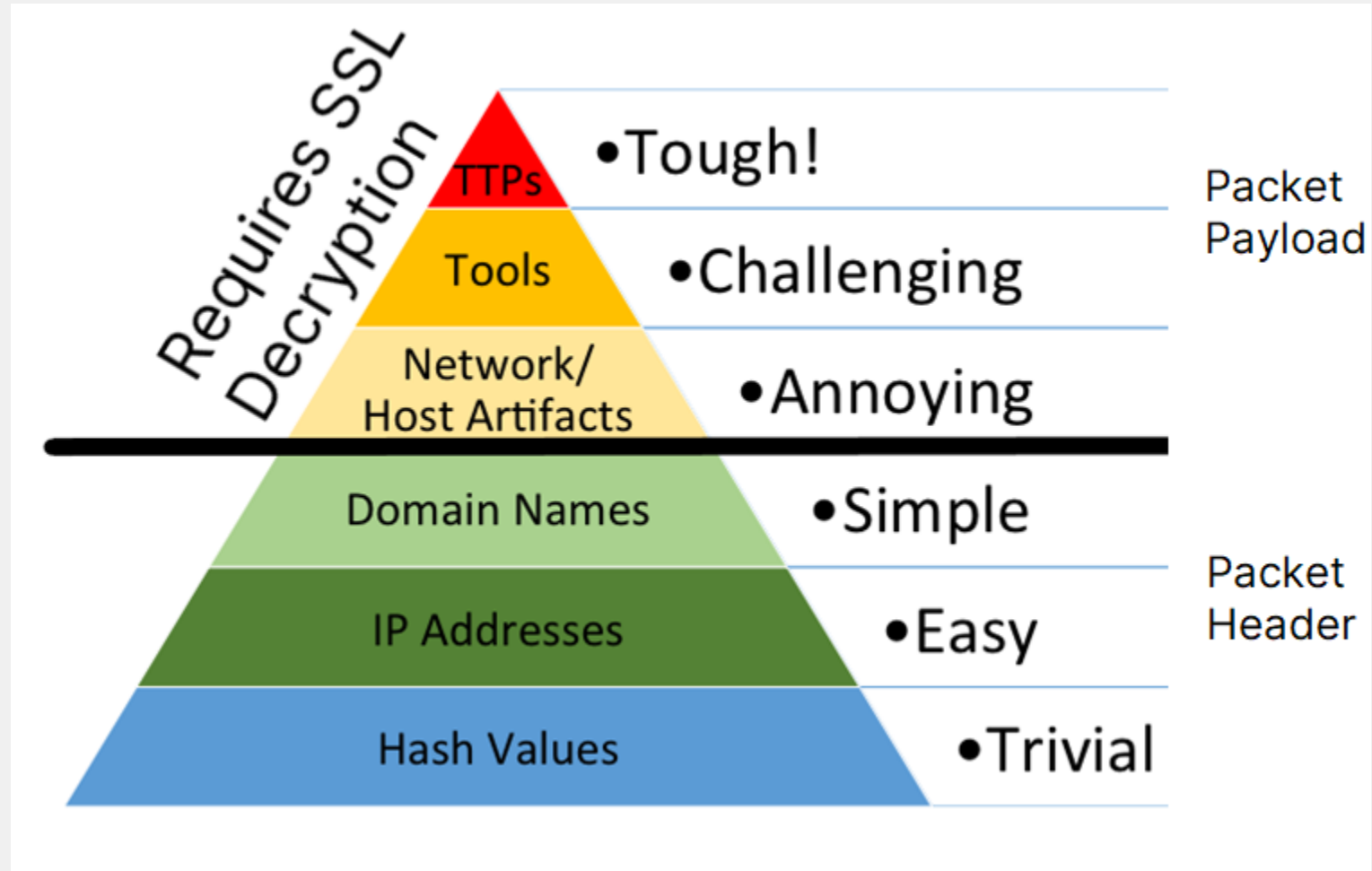
Source: <https://stats.labs.apnic.net/edns>



The Pyramid of Pain: Make Cybercrime Unprofitable Again

Which Indicators of Compromise (IOCs) provide the best value for security?

- Not all IOCs are created equal.
- Blocking Hashes, IPs, Domains provides some value
- But changing these is trivial for attackers
- Blocking Artifacts, Tools, and TTPs provides YUGE value
- These are extremely expensive for the attackers
- But this requires Deep SSL Inspection!
- It's in the encrypted payload



Attribution: David Bianco

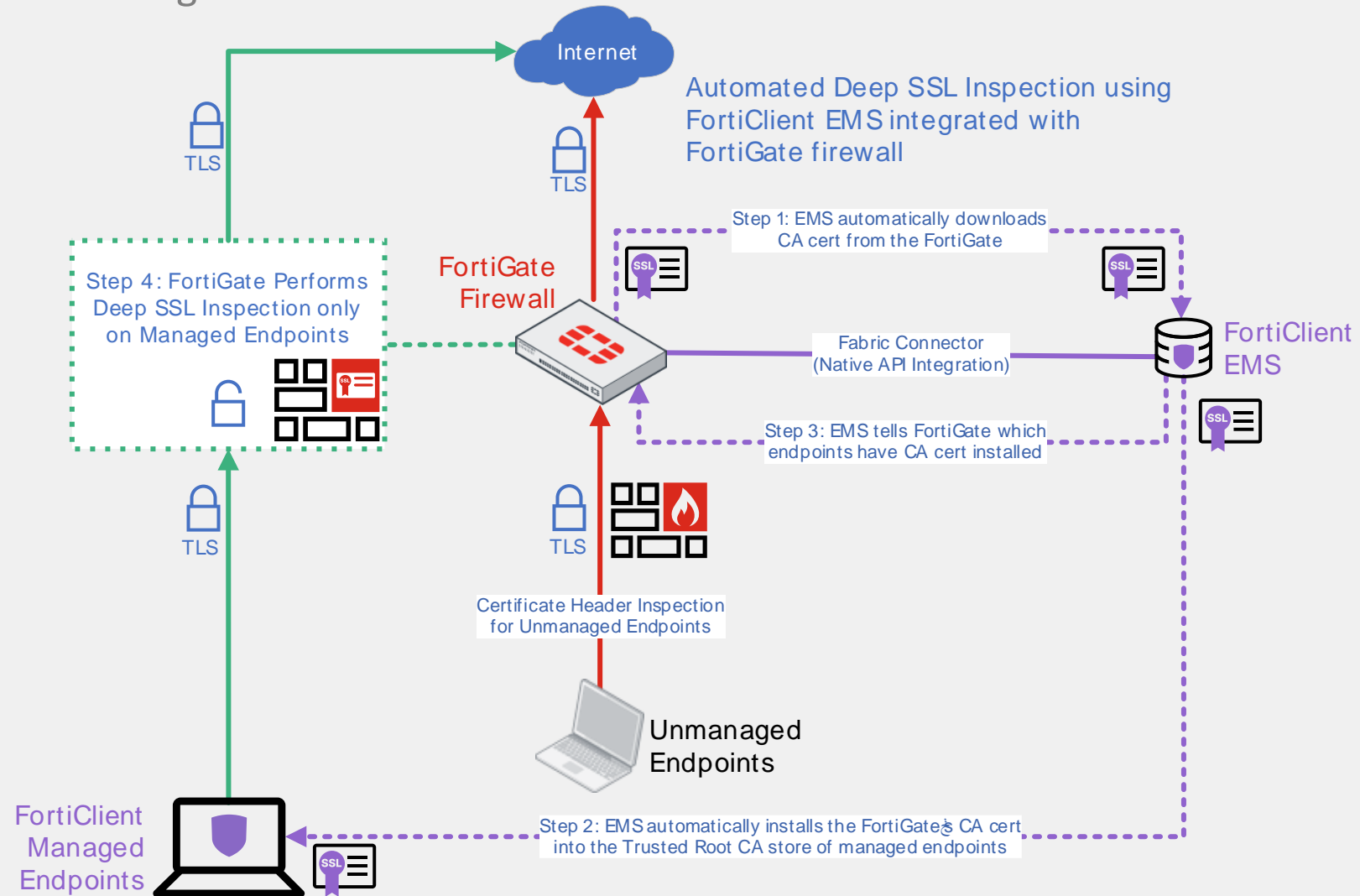
Source: <https://www.sans.org/tools/the-pyramid-of-pain/>



But doesn't this cause certificate errors!?

Yes, we're going to have to install some certs to gain trust

- Inbound: Install server's certificate on firewall
- Outbound: Install firewall's CA cert on clients
- Practical methods to automate this will be discussed in this presentation.





Addressing Objections Solving Challenges

How to Implement Deep SSL Inspection in the Real World



Objections to Deep SSL Inspection

Using Logic and Innovation to Overcome and Prevail

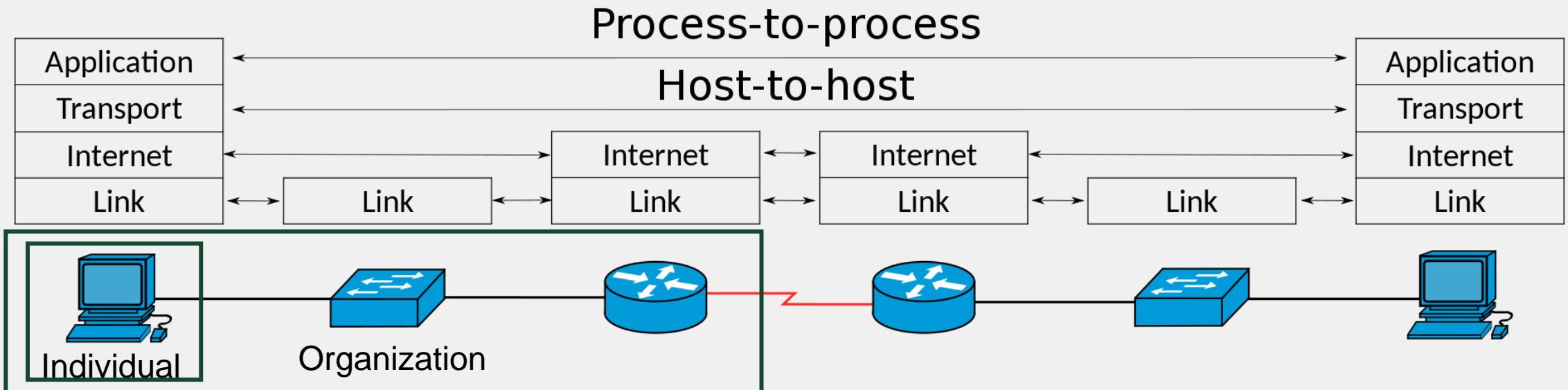
- Deep SSL Inspection is essential for a strong security posture
- So why are less than 10% of organizations implementing it?*
- Categories of Objections to implementing Deep SSL Inspection:
 - Philosophical/Strategic Objections
 - Governance Objections
 - Complexity Objections
 - Protocol Compatibility Objections
 - ~~Cost/Performance Objections~~
- Next: How to address each of these Challenges in detail

*Source: <https://malcolm.cloudflare.com/> plus personal surveys



Philosophical Objections: The End-to-End Principle

- Objection:
 - “Deep SSL Inspection violates the End-to-End Principle”
- Answer:
 - When securing an individual, their personal computer is an end node.
 - When securing an organization, the WHOLE org is a node to be secured.
 - A middlebox implementing Deep SSL Inspection is part of that org



Strategic Objections: EDR Supremacy

Forget firewalls... It's all about the endpoint! Let's just use EDR everywhere!

- EDR is crucial, but don't forget Defense-in-Depth!
 - No one solution is ever 100% in cybersecurity
 - Multiple complimenting solutions are always needed
 - Middlebox + EDR = XDR

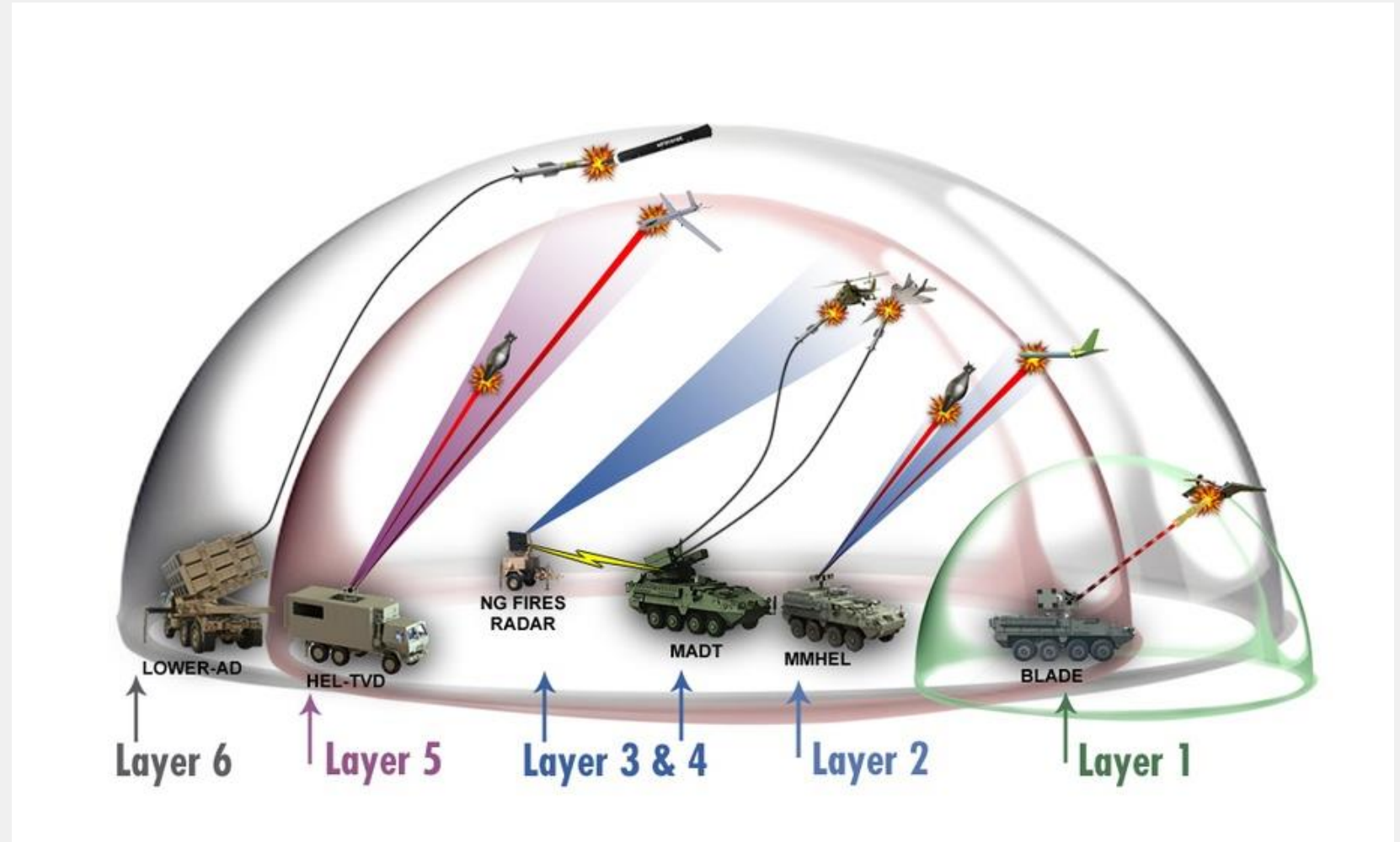
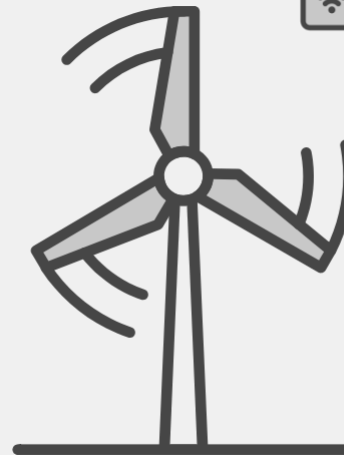
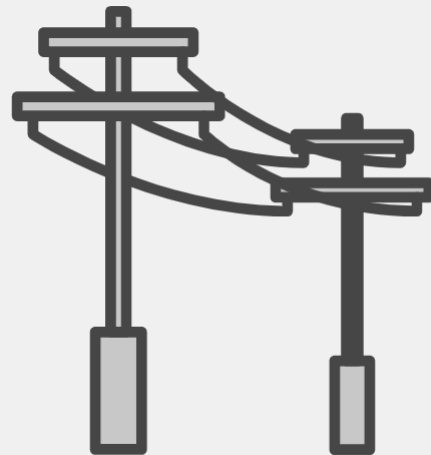
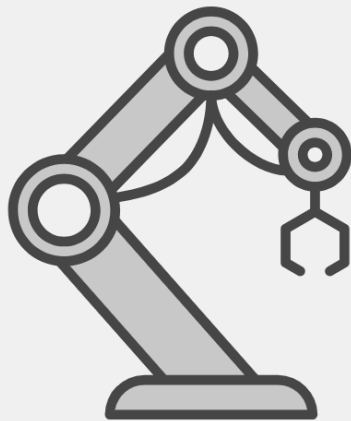


Image Source: <https://www.dvidshub.net/image/5735184/tiered-defense>

Strategic Objections: EDR Supremacy

Forget firewalls... It's all about the endpoint! Let's just use EDR everywhere!

- EDR Limitations:
 - Headless IoT / OT Devices
 - Compute & Correlation Efficiency
 - EDR Evasion Techniques are a real threat
 - Some exploit vulnerabilities and bugs
 - More often the EDR tool is misconfigured
 - See "Evading EDR" book by Matt Hand



Strategic Objections: EDR Supremacy

Forget firewalls... It's all about the endpoint! Let's just use EDR everywhere!

- EDR Limitations:

- Is the EDR agent always installed on every device?
- If not, how would you know?
- And what enforcement action would you take to correct it?
- Zero-Trust Architectures address this problem
- The Trust Broker component of Zero-Trust is... a Firewall!
- Zero-Trust components make Deep SSL easy!

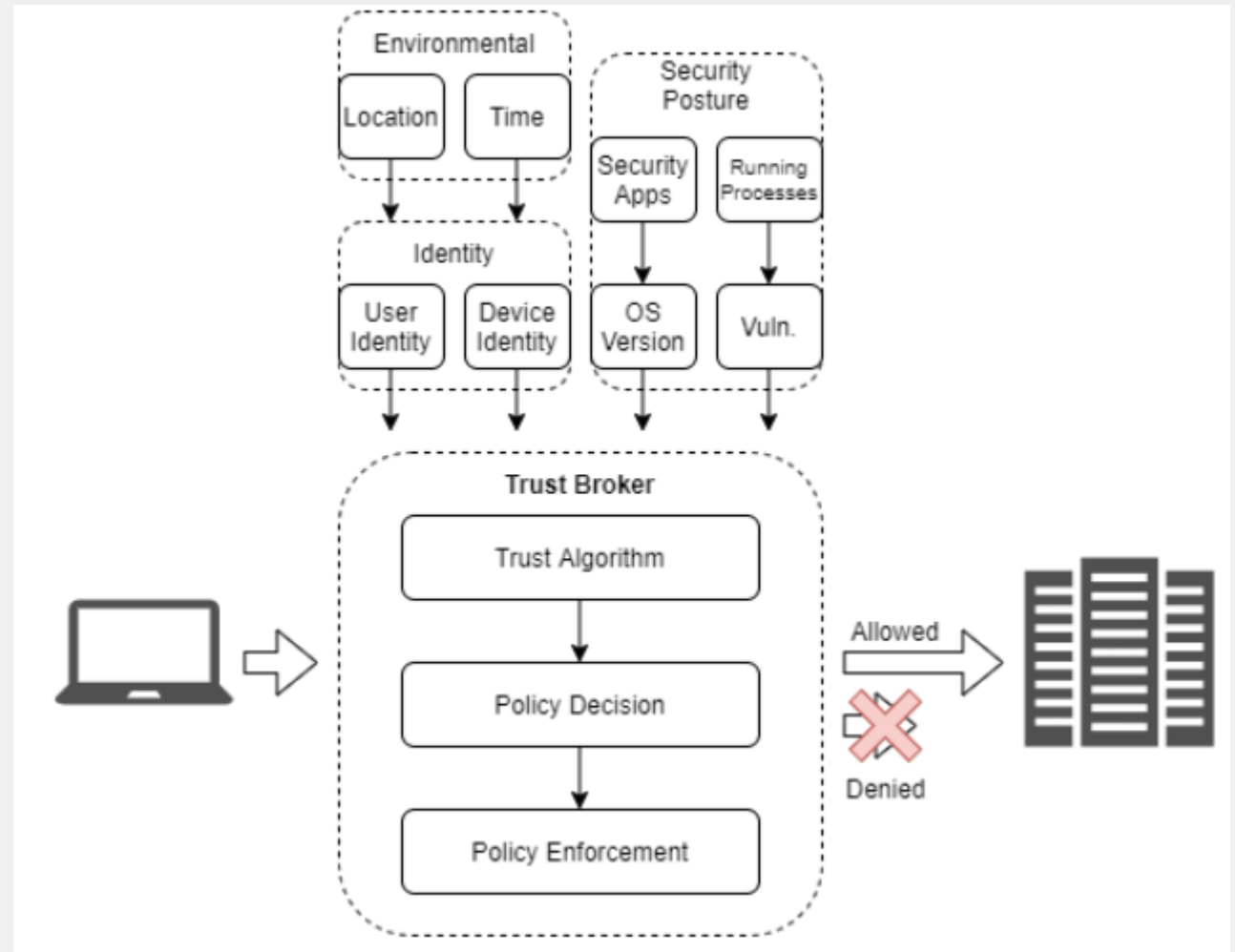
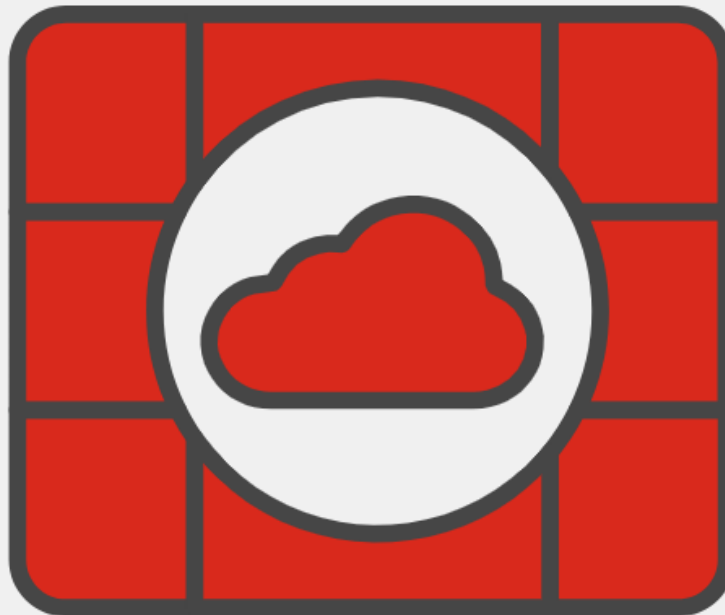


Image source: <https://docs.fortinet.com/document/fortigate/7.0.0/ztna-concept-guide/324163/trusted-entities>

Strategic Objections: Cloud Native / Remote Work

Forget firewalls... It's all about the endpoint! Let's just use EDR everywhere!

- Remote users aren't behind a firewall anymore
 - Firewalls are not just metal boxes; they exist in the cloud too
 - CNF, SASE, CASB are all forms of cloud firewalls
 - Deep SSL Inspection is still crucial for these types of firewalls



Governance Objections

What the CISOs are concerned about

- Objection: Privacy Concerns
 - Data E.g.: Medical Data, Financial Data, etc.
 - User E.g.: Guests, Dorms, Customers, etc.
- Answer: Define differentiated Acceptable Use Policies (AUPs)
 - Inspection of organization's sensitive data should be in-scope
 - Then out-of-scope data can be exempted when needed



Governance Solutions

FortiOS Example:

- Easy to specify exemptions:
 - By Category
 - By Identity/User Group
 - By Domain/IP Address
 - By Reputation
 - By IP Address
- You can still log when SSL exemptions occur

Edit SSL/SSH Inspection Profile

Name: vweis-deep_ssl
Comments: inspect session for security risks (34/255)

SSL Inspection Options

Enable SSL inspection of: Multiple Clients Connecting to Multiple Servers
Protecting SSL Server

Inspection method: SSL Certificate Inspection Full SSL Inspection

CA certificate: Fortinet_CA_SSL (Download)

Blocked certificates: Allow Block View Blocked Certificates

Untrusted SSL certificates: Allow Block Ignore View Trusted CAs List

Server certificate SNI check: Enable Strict Disable

Enforce SSL cipher compliance:

Enforce SSL negotiation compliance:

RPC over HTTPS:

Protocol Port Mapping

Inspect all ports:

Exempt from SSL Inspection

Reputable websites:

Web categories: Finance and Banking × Health and Wellness × +

Addresses: canvas_wfqdns × +

Log SSL exemptions:

Category: Finance and Banking
Rating: G
Group: General Interest - Business
Description: Financial Data and Services -- Sites that offer news and quotations on stocks, bonds, and other investment vehicles, investment advice, but not online trading. Includes banks, credit unions, credit cards, and insurance. Mortgage/insurance brokers apply here as opposed to Brokerage and Trading.
Examples: paypal.com, alipay.com, bankofamerica.com, chase.com

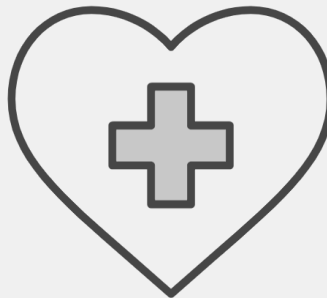
Wildcard FQDN Group: canvas_wfqdns
Members: *.canvas-user-content.com_wfqdn *.instructure.com_wfqdn
Scope: VDOM
References: 2
Edit



Governance Objections

What the CISOs are concerned about

- AUP No-Brainer: Your servers!
 - Servers usually contain the bulk of your most sensitive data
 - Deep SSL Inspection should be acceptable for nearly all out-going server traffic
 - “It’s 10pm. Do you know who your servers are talking to?”



Complexity Objections

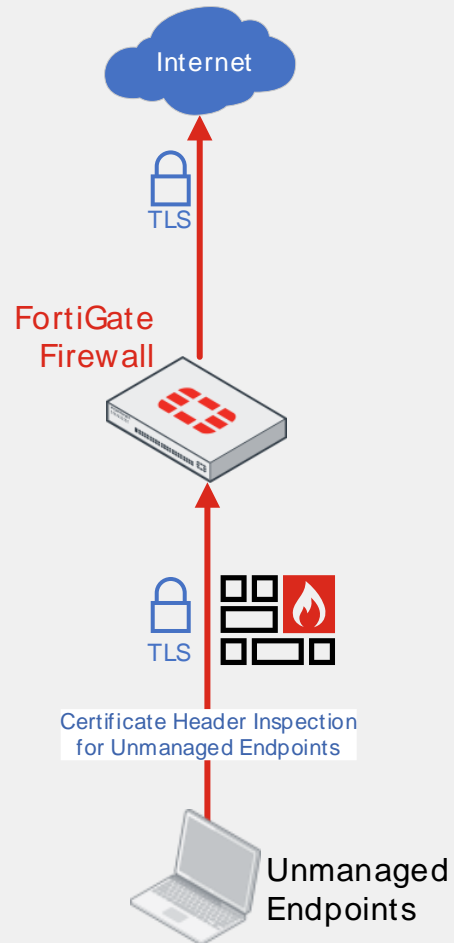
CA rollouts to endpoints are too laborious

- Objection: “It’s too difficult to deploy CA certificates to all endpoints.”
 - “If I miss some endpoints, users will complain when their internet is broken.”
 - “Little/No segmentation; can’t differentiate which endpoints have CA installed”
- Answer: Zero-Trust Architecture makes this way easier
 - Posture checking engine can know which endpoints have the CA installed
 - Policy enforcement engine applies Deep SSL Inspection only on CA-installed endpoints
 - Endpoints without CA installed yet can still function with basic header inspection
 - Ease into CA roll-outs one-by-one or group-by-group
- Let’s look at an example with the Fortinet Zero-Trust Network Access (ZTNA) system



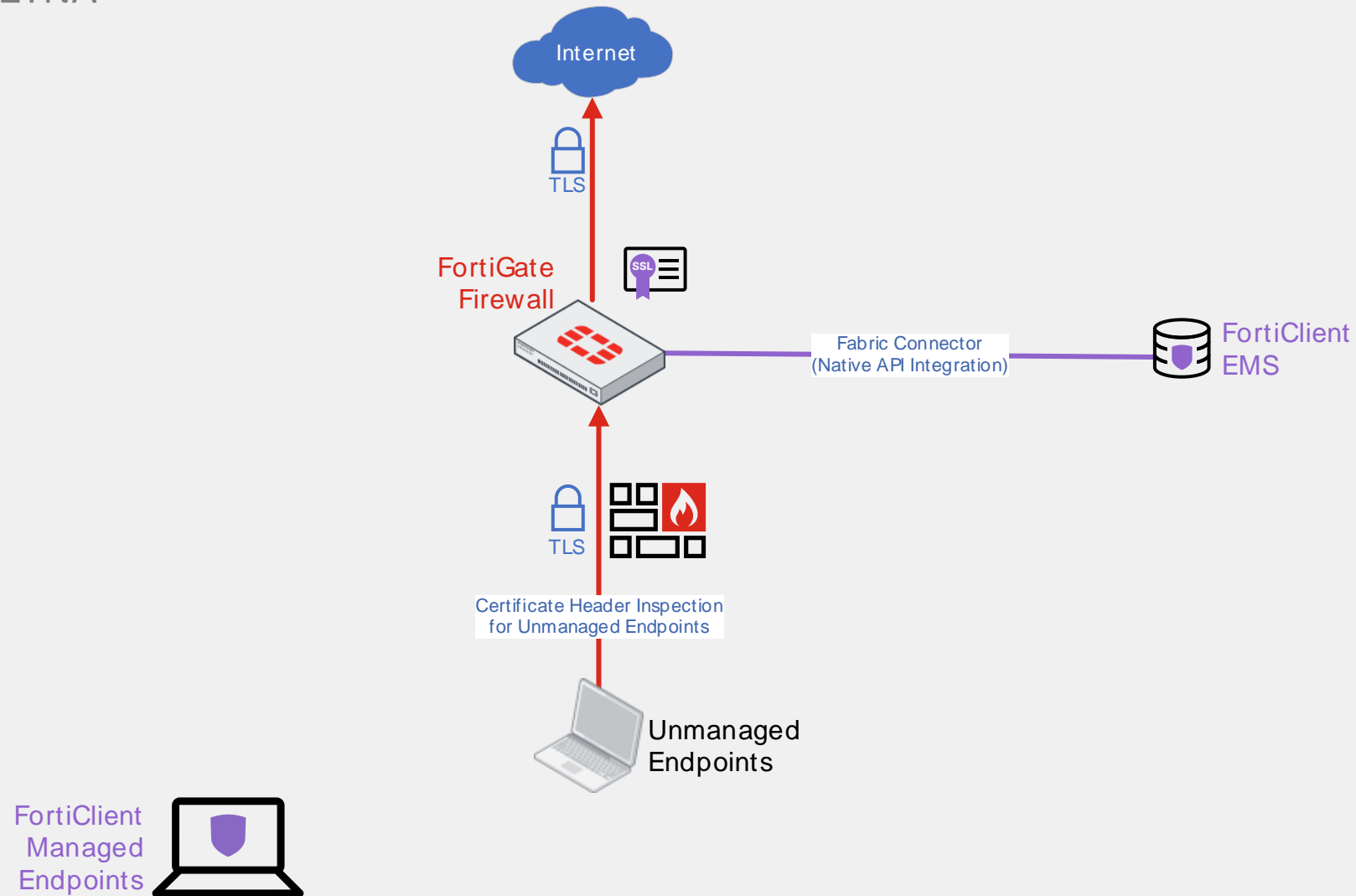
Easy Rollout of Deep SSL with FortiClient ZTNA

Before FortiClient ZTNA



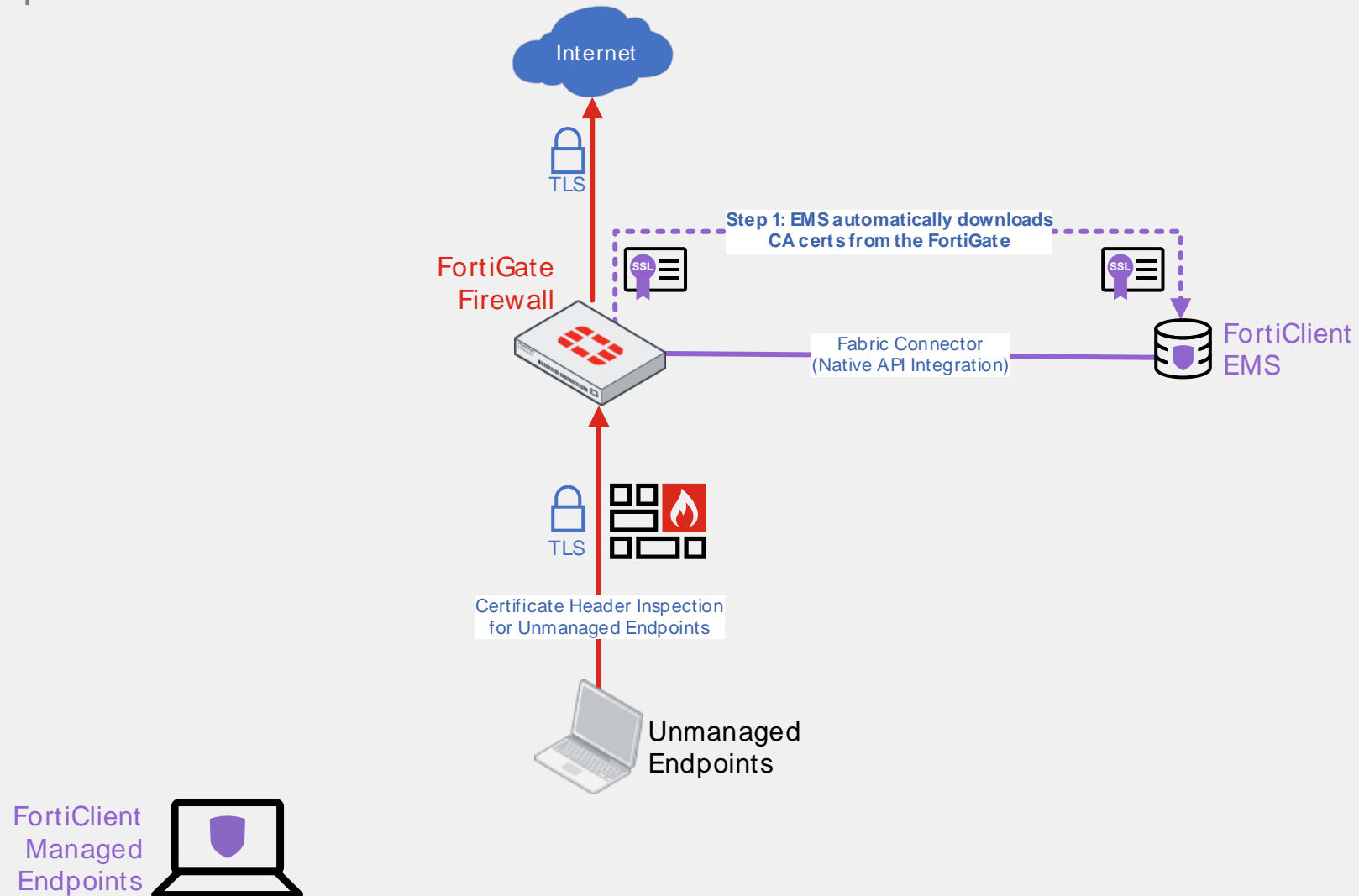
Easy Rollout of Deep SSL with FortiClient ZTNA

Add in FortiClient ZTNA



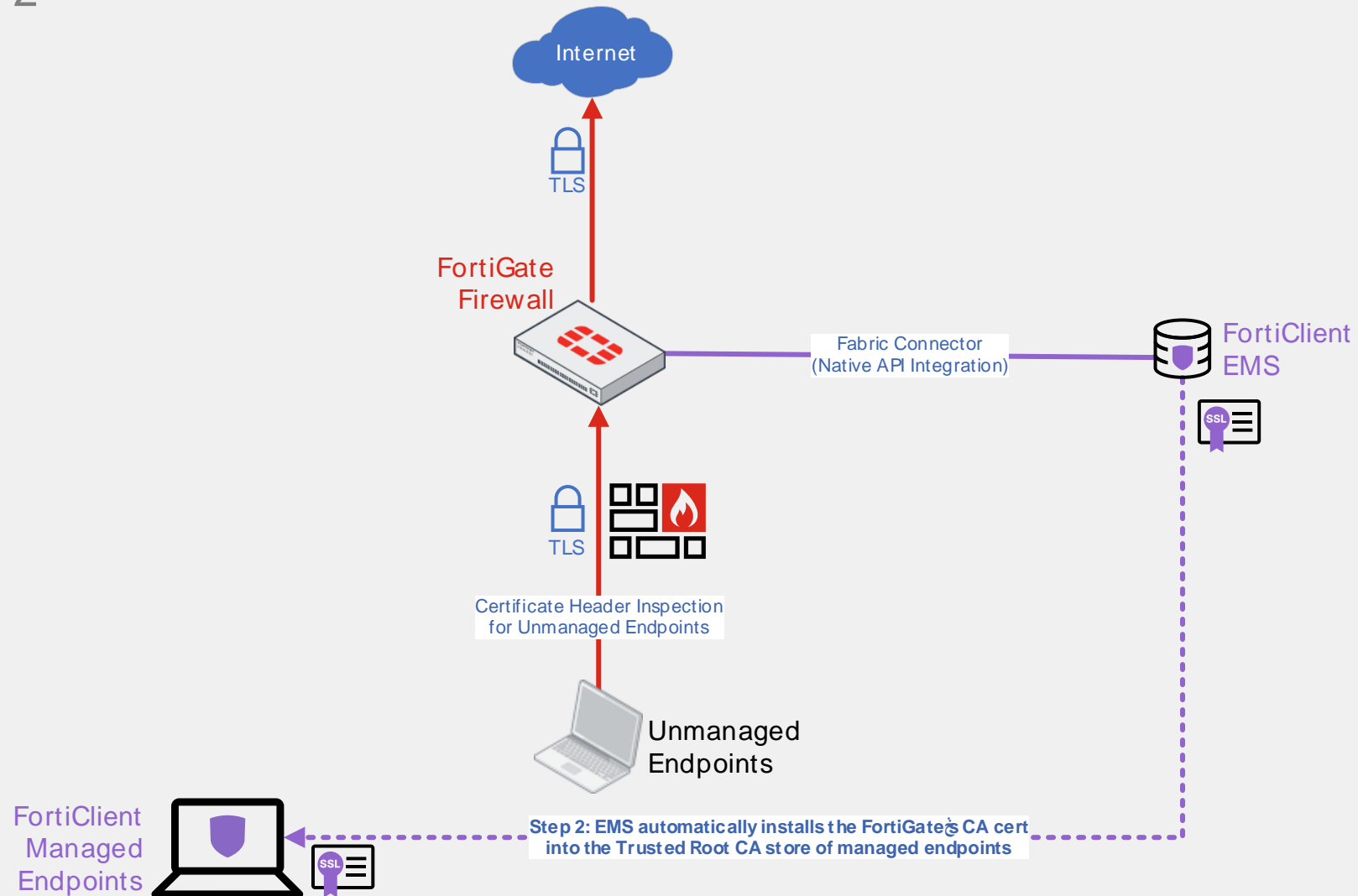
Easy Rollout of Deep SSL with FortiClient ZTNA

Automation Step 1



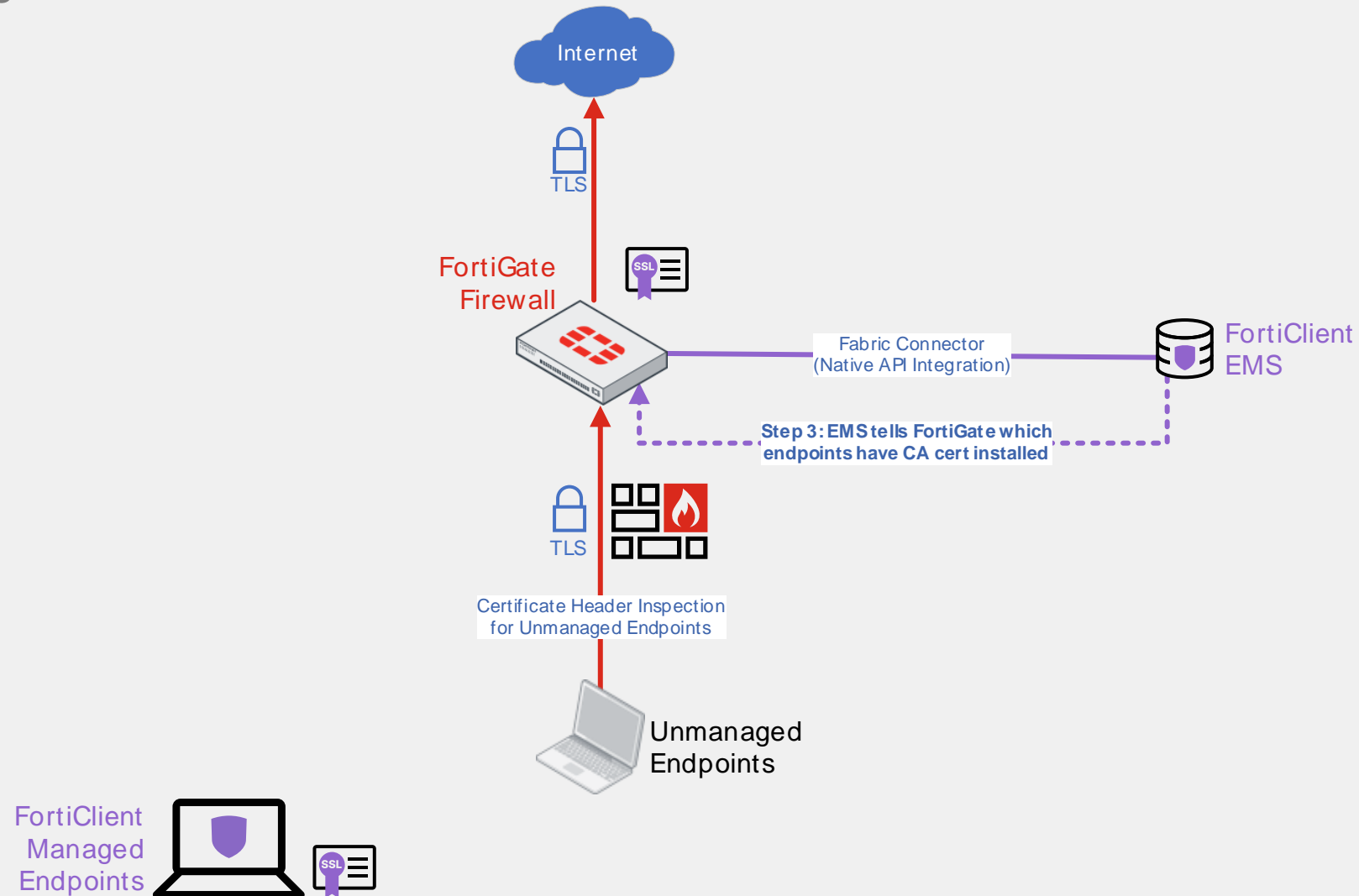
Easy Rollout of Deep SSL with FortiClient ZTNA

Automation Step 2



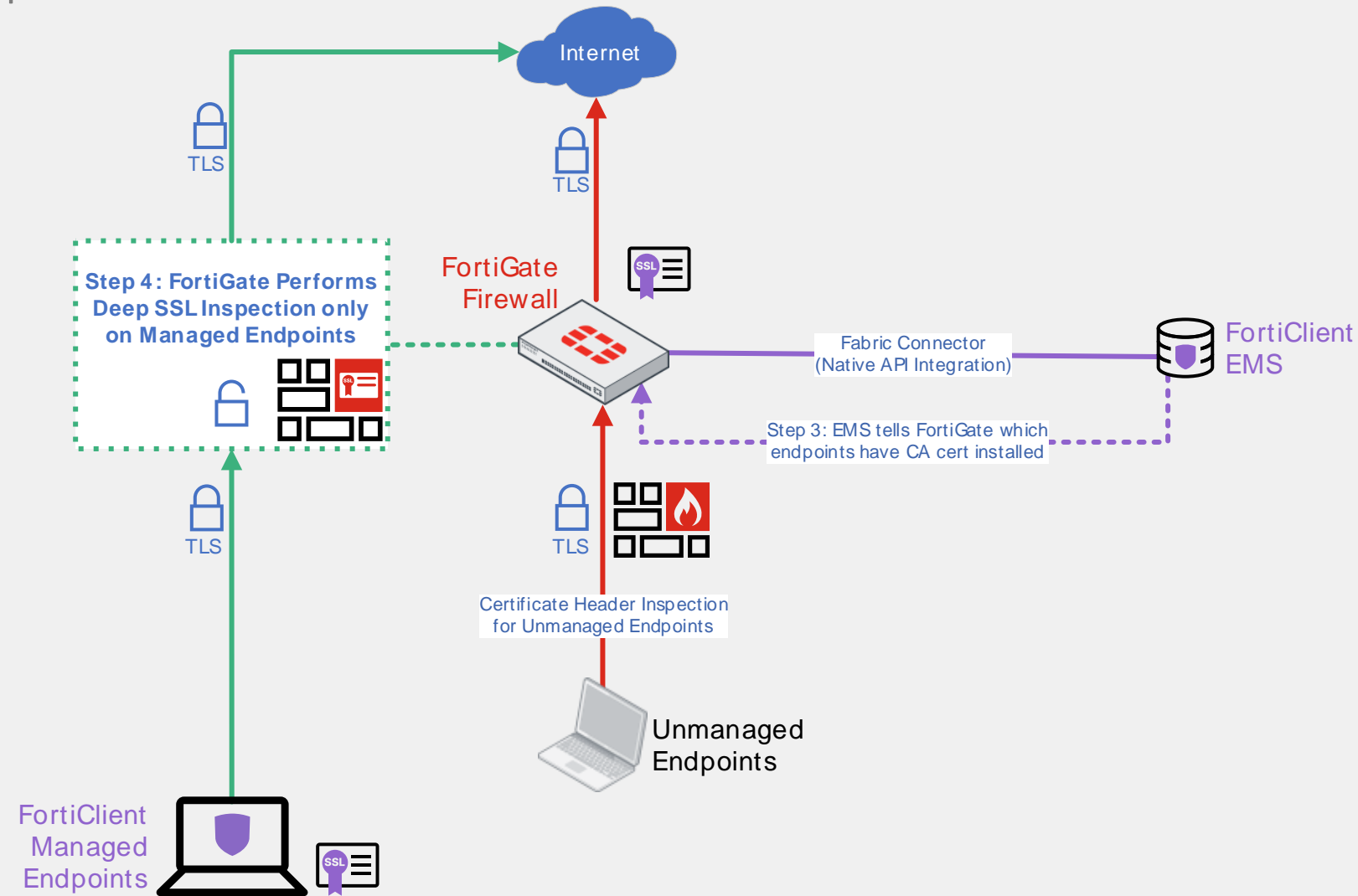
Easy Rollout of Deep SSL with FortiClient ZTNA

Automation Step 3



Easy Rollout of Deep SSL with FortiClient ZTNA

Automation Step 4

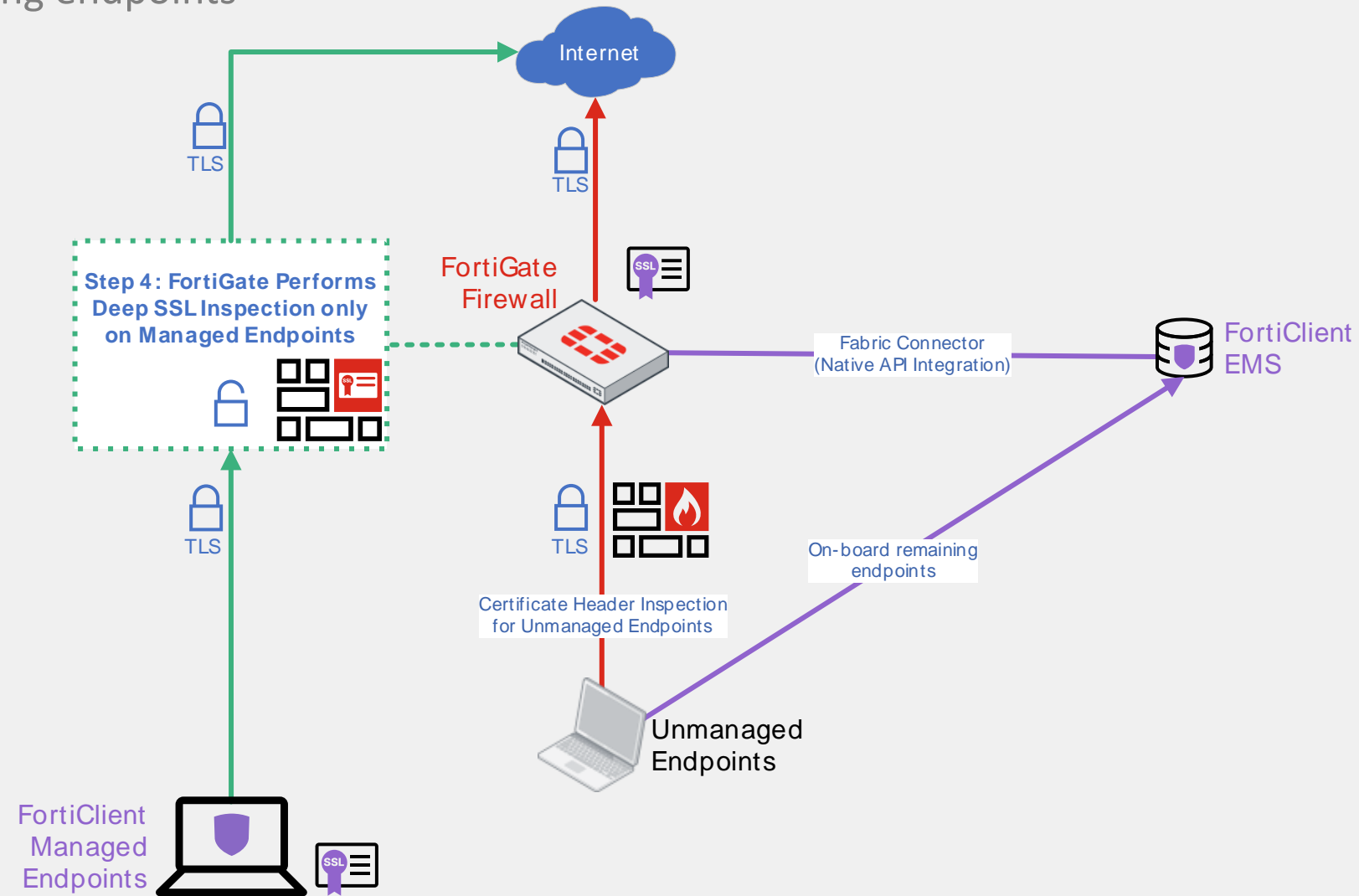


FortiClient-Managed Endpoints
now trust the FortiGate's CA cert;
No errors for end users



Easy Rollout of Deep SSL with FortiClient ZTNA

On-board remaining endpoints

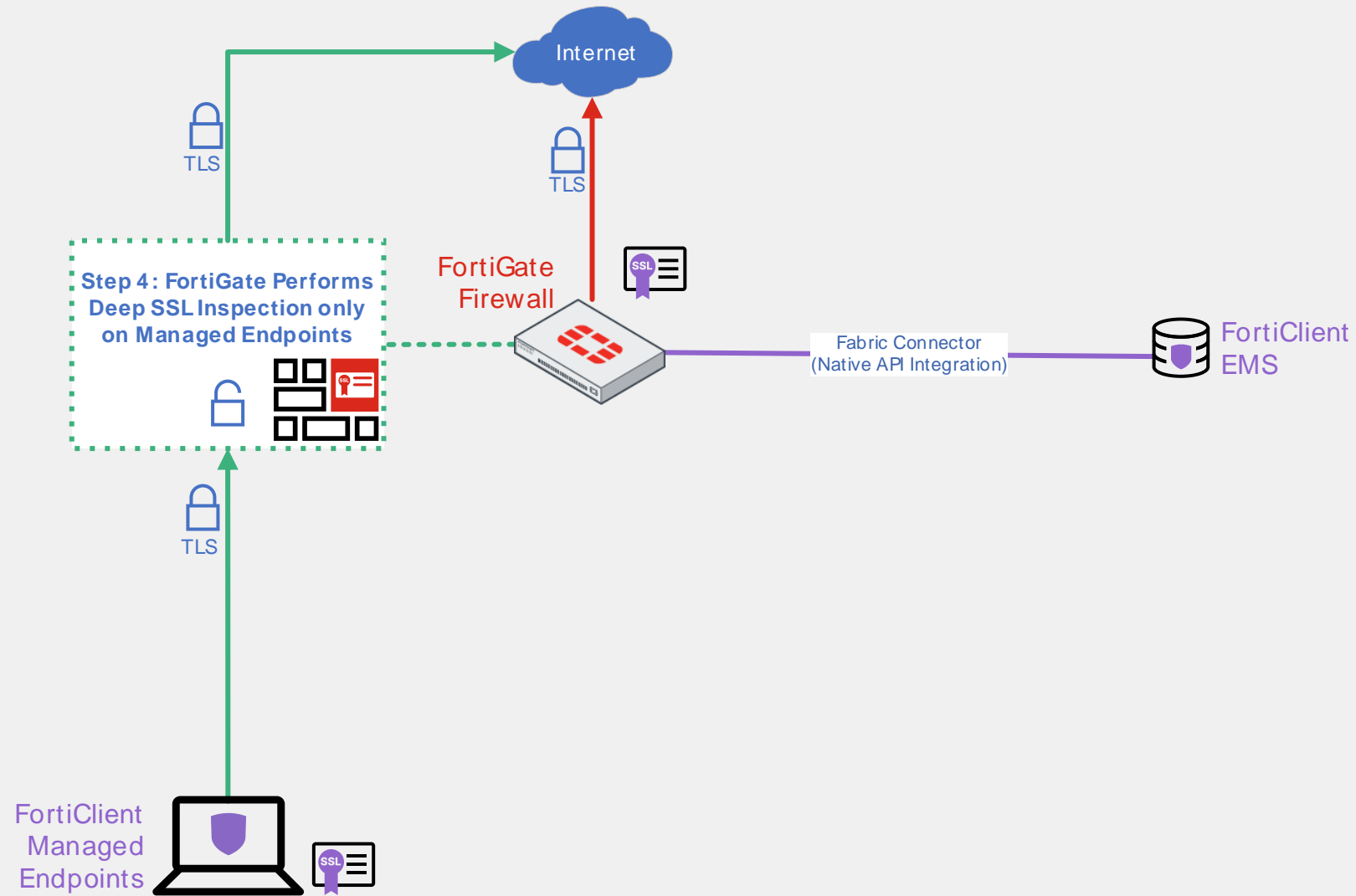


FortiClient-Managed Endpoints
now trust the FortiGate CA cert;
No errors for end users



Easy Rollout of Deep SSL with FortiClient ZTNA

Endgame



All endpoints on-boarded
Deep SSL for all endpoints



Corresponding policies on FortiGate

Can be as simple as two policies

Name	Source	Destination	ZTNA Tag	Service	Action	Log	SSL Inspection
ca:installed_deep-ssl>wan	vweis_subnets	all	ZTNA IP vweis-ems01_ztnat	ALL	ACCEPT	All	SSL vweis-deep_ssl
ca:not-installed_cert-ssl>wan	vweis_subnets	all	No ZTNA Tag	ALL	ACCEPT	All	SSL vweis-cert_ssl!

Matches all other devices in all other subnets that haven't gotten the CA installed by FortiClient EMS yet

Address Group vweis_subnets

Type Group

Members

- vweis-inf_subnet
- vweis-iot_subnet
- vweis-users_subnet
- vweis-voip_subnet
- vweis-guest_subnet
- vweis-dmz01_subnet
- vweis-ot_subnet
- vweis-cam_subnet

References 68

Edit

ZTNA Tag ZTNA IP vweis-ems01_ztnat

Provided By vweis-ems01 (ID: 1)

Type IP

Category Zero Trust

Resolved To 172.19.181.3
172.19.181.11

References 3

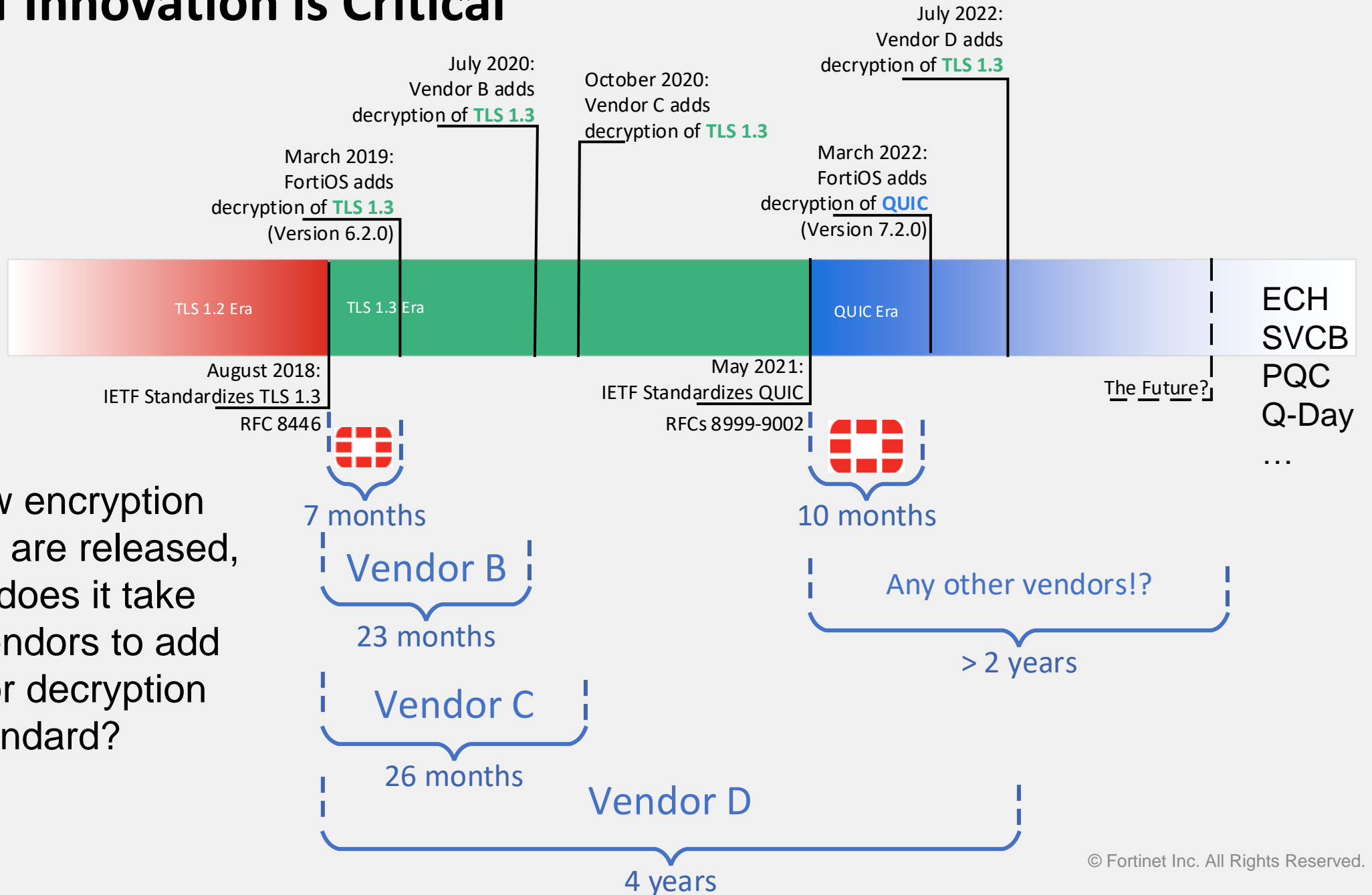
These endpoints have the CA installed

Protocol Objections

- Objection:
 - “It’s impossible to decrypt TLS 1.3, QUIC, HTTP/3... etc!”
- Answer:
 - These are all IEEE standards now
 - All network vendors should be able to implement Deep SSL Inspection for them
 - Some network vendors are faster at this than others
 - You can block newer encryption standards and force reversion to older standards
 - Pre-standardization usage
 - This works for a while, but at the cost of worse performance and weaker encryption
 - Post-standardization usage
 - The QUICer, the better!
 - 50th Birthday of TCP!



Speed of Innovation is Critical

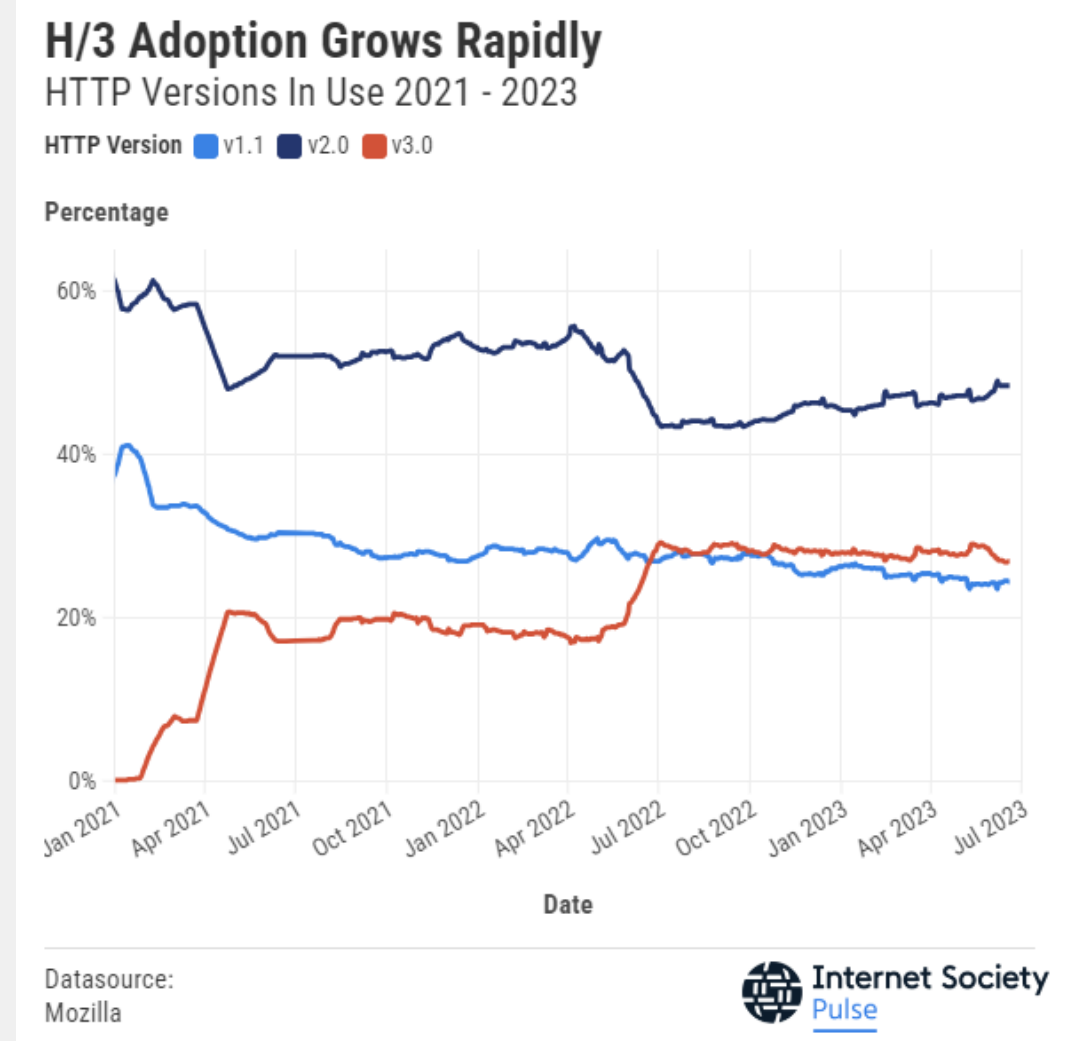


When new encryption standards are released, how long does it take firewall vendors to add support for decryption of that standard?



QUIC / HTTP3 Adoption is Growing Rapidly

- QUIC is superior to TCP in several ways:
 - Lower latency
 - Less overhead
 - Session multiplexing
- Prediction: QUIC will replace TCP sooner than IPv6 will replace IPv4.
- Future Talk: QUIC Deep Dive!



Source: <https://pulse.internetsociety.org/blog/why-http-3-is-eating-the-world>

Where to Start

80 / 20 rule

1. Certificate Fingerprinting and Blocking – EXTREMELY easy in FortiOS!
2. Servers – very easy with FortiOS
3. Endpoints – easy with FortiClient ZTNA integration to FortiOS
 - Supported for both FortiGate on-prem as well as FortiSASE FWaaS
4. IoT devices – harder!
 - Some IoT vendors provide centralized management, but many don't
 - These will require custom scripting, or manual rollouts
 - Some devices don't support custom CA certs at all
 - Segment and restrict these
 - Consider this for IoT vendor choices at next refresh cycle
5. Mobile devices
 - Harder on Android than on iOS because of certificate pinning prevalence



Step 1: Certificate Fingerprinting

- Force the bad guys to come out into the open!
- Don't allow SSL connections for certs issued by non-trusted CAs
- Even then, bad guys also use SSL certs issued by trusted CAs
- FortiGuard Labs has fingerprinted >135K of these certs
- Once blocked, the bad guys will have to revert to unencrypted communication

Edit SSL/SSH Inspection Profile

Name: vweis-cert_ssl
Comments: inspect handshake for security risks (36/255)

SSL Inspection Options

Enable SSL inspection of: Multiple Clients Connecting to Multiple Servers
Protecting SSL Server

Inspection method: SSL Certificate Inspection Full SSL Inspection

CA certificate: Fortinet_CA_SSL Download

Blocked certificates: Allow Block View Blocked Certificates
Untrusted SSL certificates: Allow Block View Trusted CAs List

Server certificate SNI check: Enable Strict Disable

Blocked Certificates

Listing Date	SHA1 Fingerprint	Common Name	Listing Reason
2023/08/01	0cc1803473ca33e0721037a077dc13e047c71c		DCRat C&C
2023/08/01	e467111a1c5c1e660849e93fc0c18ece89fed6fd		AsyncRAT C&C
2023/08/01	2842a6999e167f4690bd28912ff8f727514ff109		AsyncRAT C&C
2023/07/31	138c72d19a86a1e26c97fb78e4e4efe6c099631a	archivde.xyz	NetSupport C&C
2023/07/31	9473c50d4be7cec5ed4f544b1c6fdd040ce29c18	luckyday0728.org	NetSupport C&C
2023/07/31	5c8097e42822b094bd2feee2219dfc7e5c02b007		AsyncRAT C&C
2023/07/30	c4c9e808a53b52d8c4c02fef5bf78033bd95301c		DCRat C&C
2023/07/30	67b0706b75bd7fc85c393c55bc21fdc1752117dc	ca-ferrari-club.com	Smoke Loader C&C
2023/07/30	3e4fd8e850da0a9b14c060d19a28758320b6d9e3	utah-saints.com	Smoke Loader C&C

135,074



Step 2: Servers

- Protect your most valuable assets
- You already have the cert deployed on your servers; just import to the FortiGate
- Use Server Name Indication (SNI) to include multiple certificates at once
 - Works for wildcard and SAN certs too

Edit SSL/SSH Inspection Profile

Name: vweis-deep_ssl

Comments: Deep SSL Inspection for servers. Multiple certs using SNI 57/255

SSL Inspection Options

Enable SSL inspection of: Multiple Clients Connecting to Multiple Servers

Protecting SSL Server

Server certificate:

- web1.victorweis.com
- web2.victorweis.com
- *.example.com

Download

Protocol Port Mapping

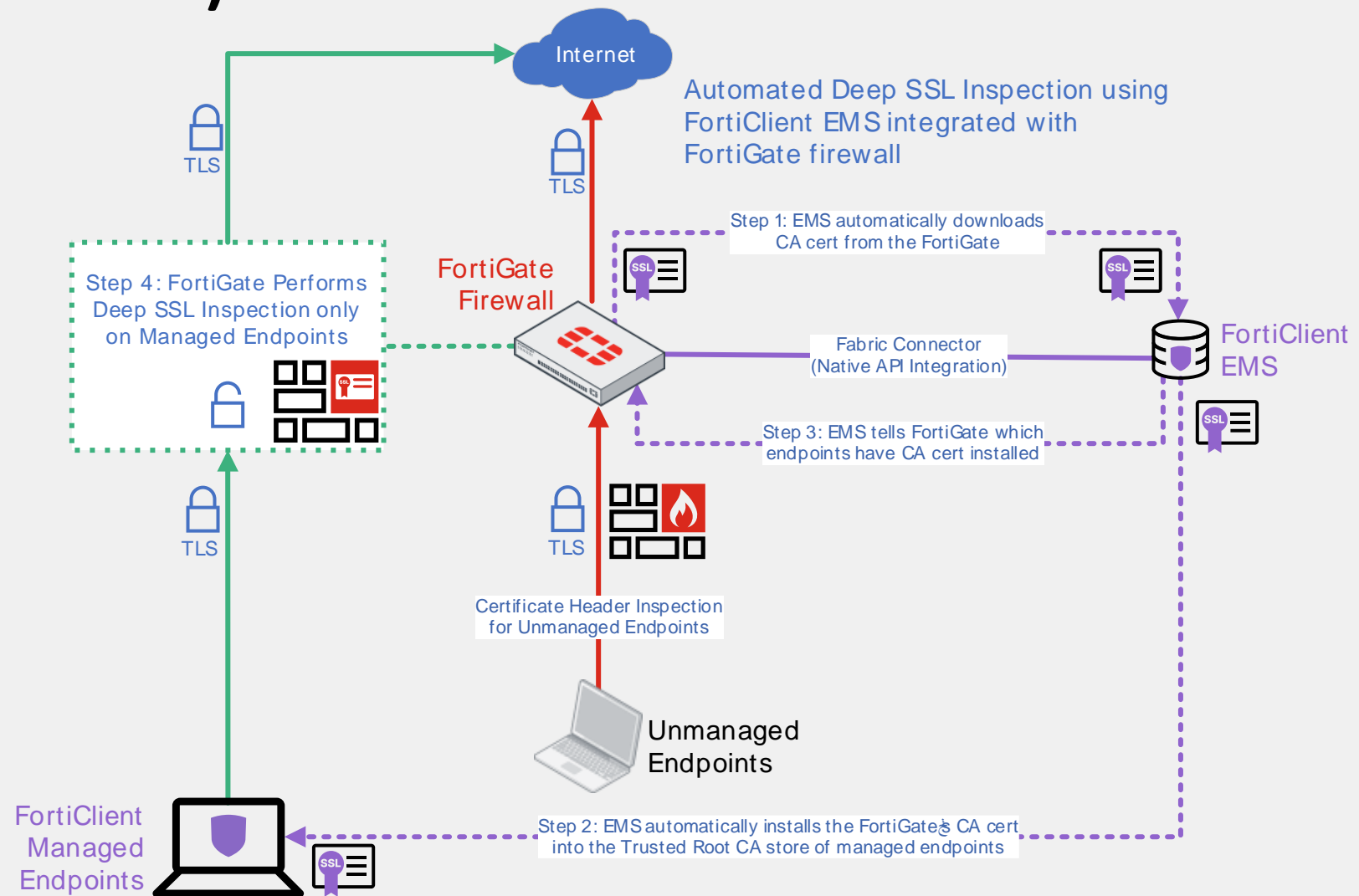
Inspect all ports:

HTTPS: 443

Uses SNI to select the correct certificate

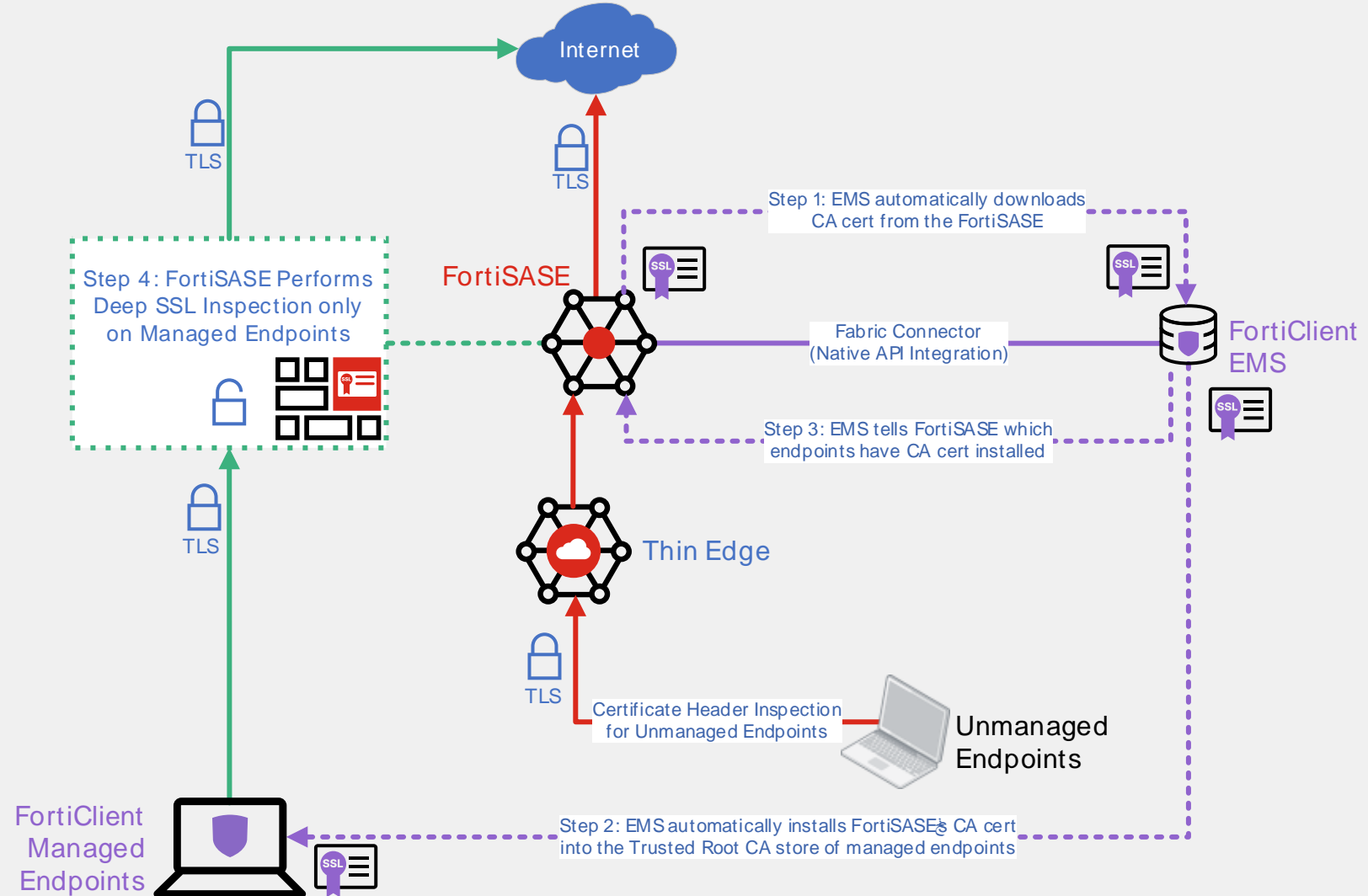
Step 3: Endpoints (On-Prem FortiGate)

- FortiClient ZTNA is the EASIEST way to not only deploy CA certificates, but also to keep track of which endpoints have the CA installed
- Can be done with 3rd party tools (Group Policy, NPS, Intune, etc.), but these are more tedious and less-feature rich.



Step 3: Endpoints (FortiSASE)

- This FortiClient ZTNA integration works the same way with FortiSASE as the firewall instead of FortiGate



Call to Action: Decrypt, Defend, Prevail!

Implement Deep SSL Inspection in the Real World

1. For CISOs and Policy Writers:

- Ask your teams: What's our Deep SSL Inspection strategy?
- Define your AUP to allow for Deep SSL Inspection appropriate to your org

2. For CFOs:

- TCO Analysis of the minimum size firewall you would need to do Deep SSL Inspection
- Compare Fortinet to your incumbent solution and prepare to be amazed!

3. For Architects/Engineers:

- Get trained!
- FREE Self-led training: <https://training.fortinet.com>
- FREE Fast Track Friday Labs: <https://events.fortinet.com/fortinetfasttrackworkshops>
 - Additional dates available upon request. Ask your account team.



Questions, Comments, Feedback

How to contact me

- Email: vweis@fortinet.com
- Github: <https://github.com/weis-victor>
- LinkedIn: <https://www.linkedin.com/in/victor-weis/>
- OISC:
 - <https://www.technologyfirst.org/Ohio-Information-Security-Conference>



FORTINET®

Possible Pitfalls when implementing Deep SSL Inspection

Things to watch out for

- Performance! Make sure you got it!
 - Ease in with rolling out certs to devices in batches and monitor for performance
- Firefox has a separate certificate store
 - Will either have to install CA into Firefox store, or configure Firefox to use OS store
 - This is part of the AUP definitions. Do you want to allow Firefox with the proper MDM/Group Policy controls in place? Or do you want to block it with either Application Control and/or ZTNA?



Possible Pitfalls when implementing Deep SSL Inspection

Things to watch out for

- Certificate pinning apps, especially for Android devices, but can also exist in iOS, MacOS, Windows, etc.
 - These will have to be identified and exempted
 - Start off by testing with a single device and test all the business-critical apps
- QUIC Support?
 - Upgrade to latest version of 7.2.x to get support to inspect QUIC!
 - If you're still running 7.0.x or older, you'll need to block QUIC under Application Control



Looking in Logs for Exemptions

Log & Report

Filter by Action: Blocked

Date/Time	Action	Service	Source	Source Interface	Destination	Destination Interface
4 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	20.211.142.183 (settings-prod-ause-1.australiaea...)	att (wan1)
4 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	20.211.142.183 (settings-prod-ause-1.australiaea...)	altafiber (w...
4 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	20.211.142.183 (settings-prod-ause-1.australiaea...)	altafiber (w...
7 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	52.180.66.122 (wdcpalt.microsoft.com)	att (wan1)
7 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	52.180.66.122 (wdcpalt.microsoft.com)	altafiber (w...
7 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	13.87.187.111 (wdcp.microsoft.com)	altafiber (w...
7 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	13.87.187.111 (wdcp.microsoft.com)	att (wan1)
7 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	13.87.187.111 (wdcp.microsoft.com)	att (wan1)
11 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	20.72.205.209 (settings-win.data.microsoft.com)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	altafiber (w...
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	altafiber (w...
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	altafiber (w...
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	altafiber (w...
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	altafiber (w...
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	altafiber (w...
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	altafiber (w...
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	altafiber (w...
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	40.119.249.228 (settings-prod-sea-2.southeastasi...)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	13.67.191.143 (msedge.api.cdp.microsoft.com)	altafiber (w...
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	13.67.191.143 (msedge.api.cdp.microsoft.com)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	13.67.191.143 (msedge.api.cdp.microsoft.com)	att (wan1)
15 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	13.67.191.143 (msedge.api.cdp.microsoft.com)	altafiber (w...
16 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	13.67.191.143 (msedge.api.cdp.microsoft.com)	att (wan1)
16 minutes ago	Blocked	SSL	.WEIS (172.19.182.9)	vweis-users_vlan (po1.0182)	13.67.191.143 (msedge.api.cdp.microsoft.com)	att (wan1)

Log Details

Destination UUID: 0e39e486-de0c-51ed-7b22-e7183e8f14ac

Hostname: settings-win.data.microsoft.com

Application Control

Protocol: 6

Service: SSL

Data

Message: SSL connection is blocked

Action

Action: Blocked

Policy ID: -ems>wan_deep-ssl (38)

Policy: f01efa14-e481-51ed-a786-d0c25355dd29

Policy Type: Firewall

Security

Level: ████

Cellular

Service: SSL

Other

Log event original timestamp: 1699904644025918000

Timezone: -0500

Log ID: 1700062303

Type: utm

Sub Type: ssl

Event Type: ssl-anomaly

Profile Name: vweis-deep-ssl

Source Interface Role: lan

Destination Interface Role: wan

TLS Version: tls1.2

Server Name Indication: settings-win.data.microsoft.com

Event Subtype: certificate-anomaly



Creating Exemptions with Categories and FQDNs

The screenshot shows the Fortinet management interface for editing an SSL/SSH Inspection Profile. The left sidebar contains a navigation menu with categories like Dashboard, Network, Policy & Objects, Security Profiles, and VPN. The main content area is titled 'Edit SSL/SSH Inspection Profile' and includes sections for 'Enforce SSL negotiation compliance', 'RPC over HTTPS', 'Protocol Port Mapping', 'Exempt from SSL Inspection', 'SSH Inspection Options', and 'Common Options'. A dialog box titled 'Wildcard FQDN Group' is open, showing a list of members and a scope of 'VDOM'.

Protocol Port Mapping

Inspect all ports	<input type="radio"/>
HTTPS	<input checked="" type="radio"/> 443
SMTPTS	<input checked="" type="radio"/> 465
POP3S	<input checked="" type="radio"/> 995
IMAPS	<input checked="" type="radio"/> 993
FTPS	<input checked="" type="radio"/> 990
DNS over TLS	<input checked="" type="radio"/> 853

Exempt from SSL Inspection

Reputable websites

Web categories

- Finance and Banking
- Health and Wellness

Addresses

- cibng.ibanking-services.com_fqdn
- corp-fortiedr-agg_pub
- secure2a.internet-estatemts.cc
- canvas_wfqdns
- deep-ssl-exempt_wfqdns

Wildcard FQDN Group deep-ssl-exempt_wfqdns

Members

- *.signal.org_wfqdn
- *.whispersystems.org_wfqdn
- *.youtube.com_wfqdn
- *.fortinet.com_wfqdn
- *.myfortinet.com_wfqdn
- *.cricut.com_wfqdn
- *.instagram.com_wfqdn
- *.fortimail.com_wfqdn
- *.verizonwireless.com_wfqdn

Scope: VDOM

References: 1

OK Cancel



January Threat Briefing

January Threat Briefing

- ▶ Google Chrome Updates
- ▶ Cisco Unity Connection
- ▶ Microsoft Patch Tuesday (Two Critical)
- ▶ Fortinet - Improper Privilege Management

January Threat Briefing

- ▶ China Claims it Cracked Apple's AirDrop
- ▶ SEC's X Account Hacked (No MFA)
- ▶ 178,000 SonicWall Firewalls Vulnerable
- ▶ Juniper Critical Vulnerability

Information

Feel free to email us at Admin@gocybercollective.org.

If you have a suggestion on meeting topics, special interest groups, breakfast menu, or anything else we want to hear from you.

You can register and download past presentations from the website.

▶ GoCyberCollective.org

Event Sponsors

