
go
cyber
COLLECTIVE

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

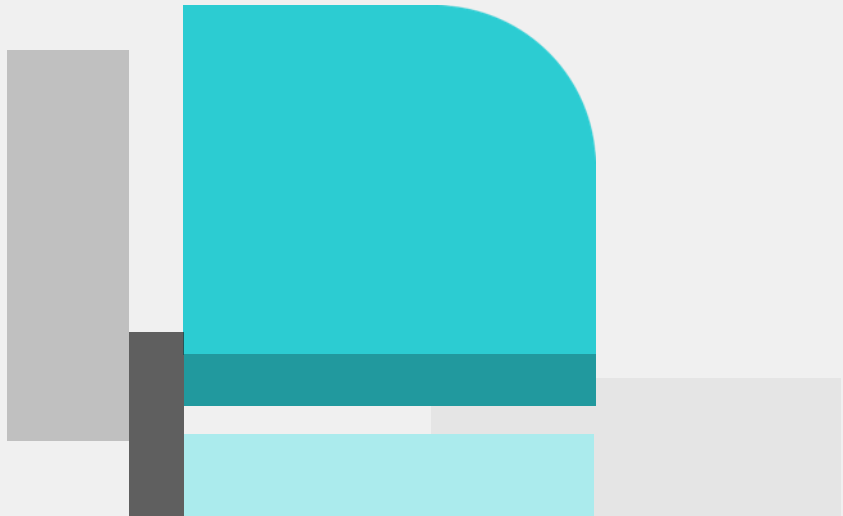
Victor Weis
Systems Engineer
Fortinet

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:

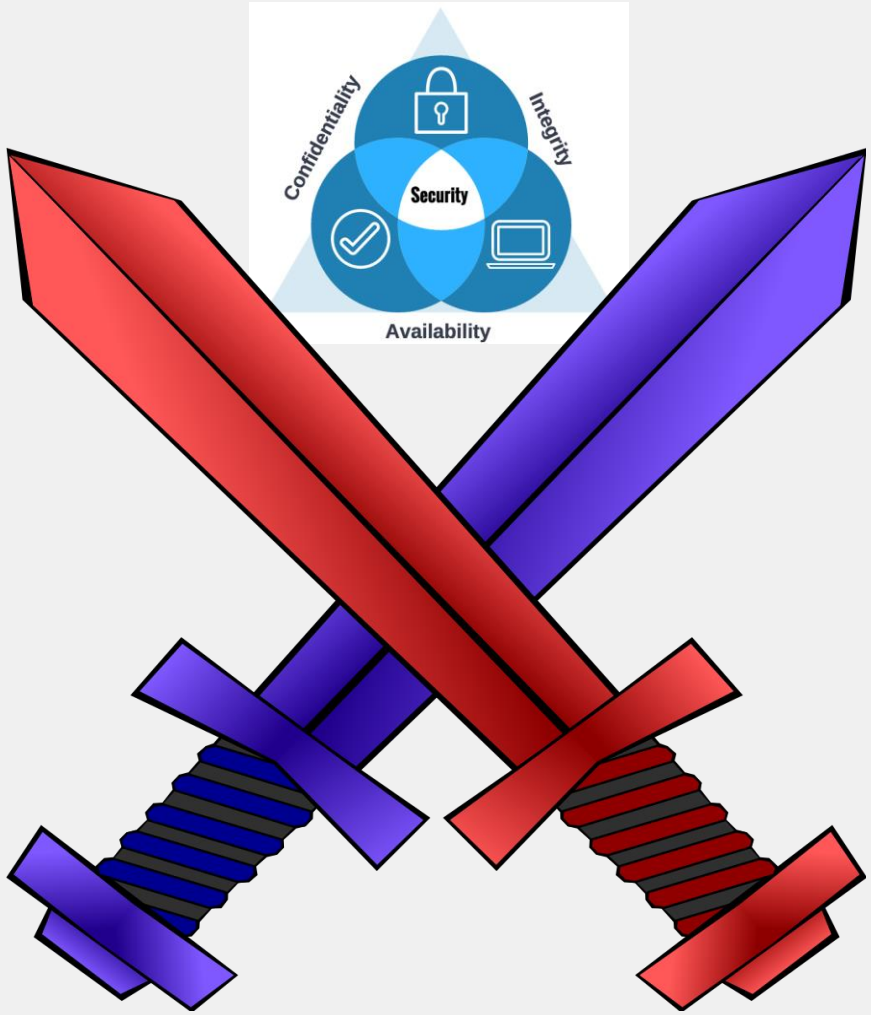
- In this presentation, I will use “SSL” and “TLS” interchangeably
- “Deep SSL Inspection” = “SSL/TLS Decryption” = “Deep Packet Inspection”
- “Firewall” / “Middlebox” will refer to any network device that transforms, inspects, and filters traffic for purposes other than packet forwarding
    - This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

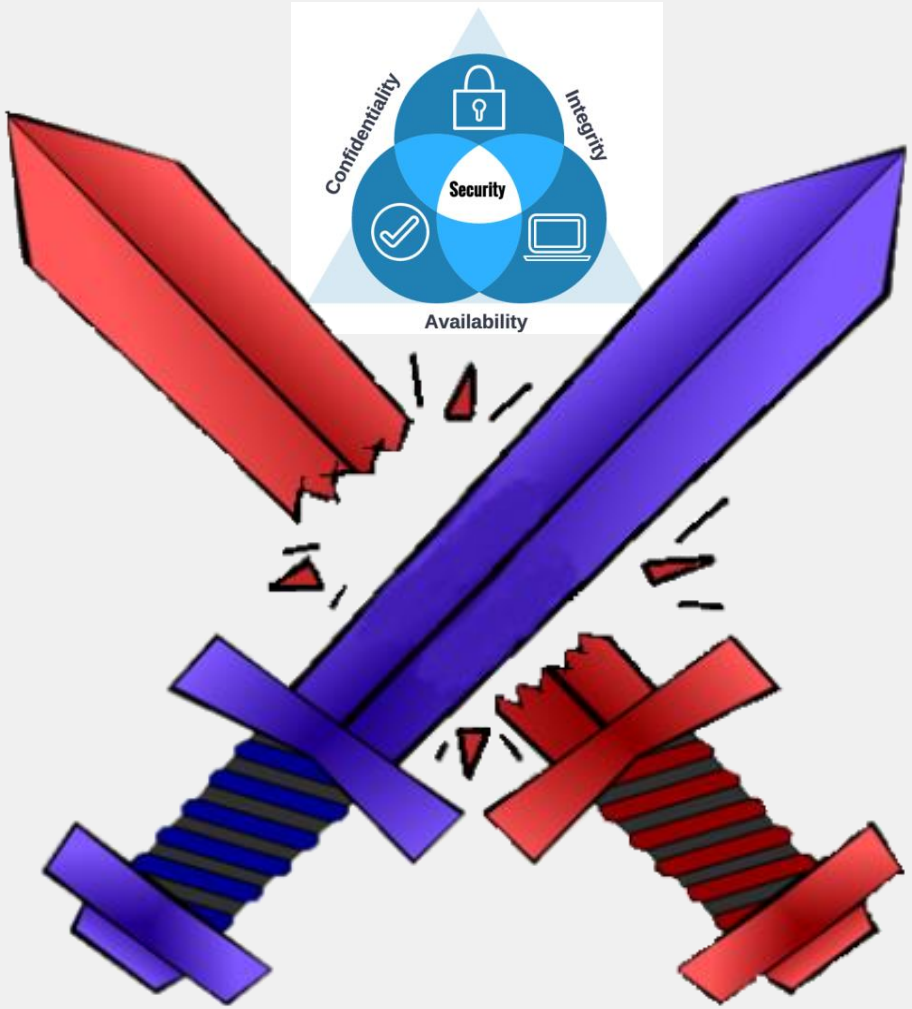
Encryption: The Double-Edged Sword

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



Gain the Upper-Hand with Deep SSL Inspection

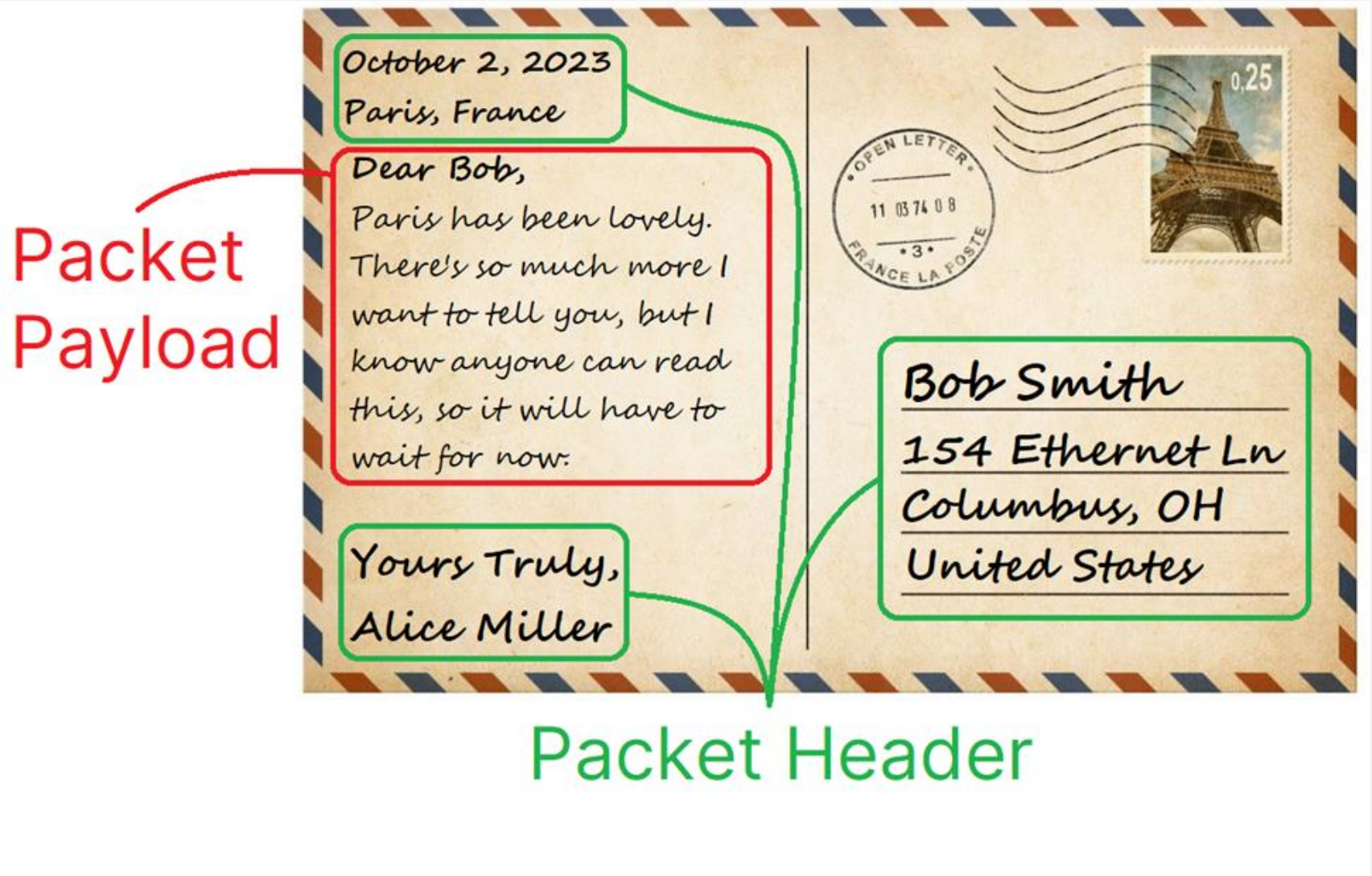
Achieve the best of both worlds



What is SSL Encryption?

Postcards vs Envelopes

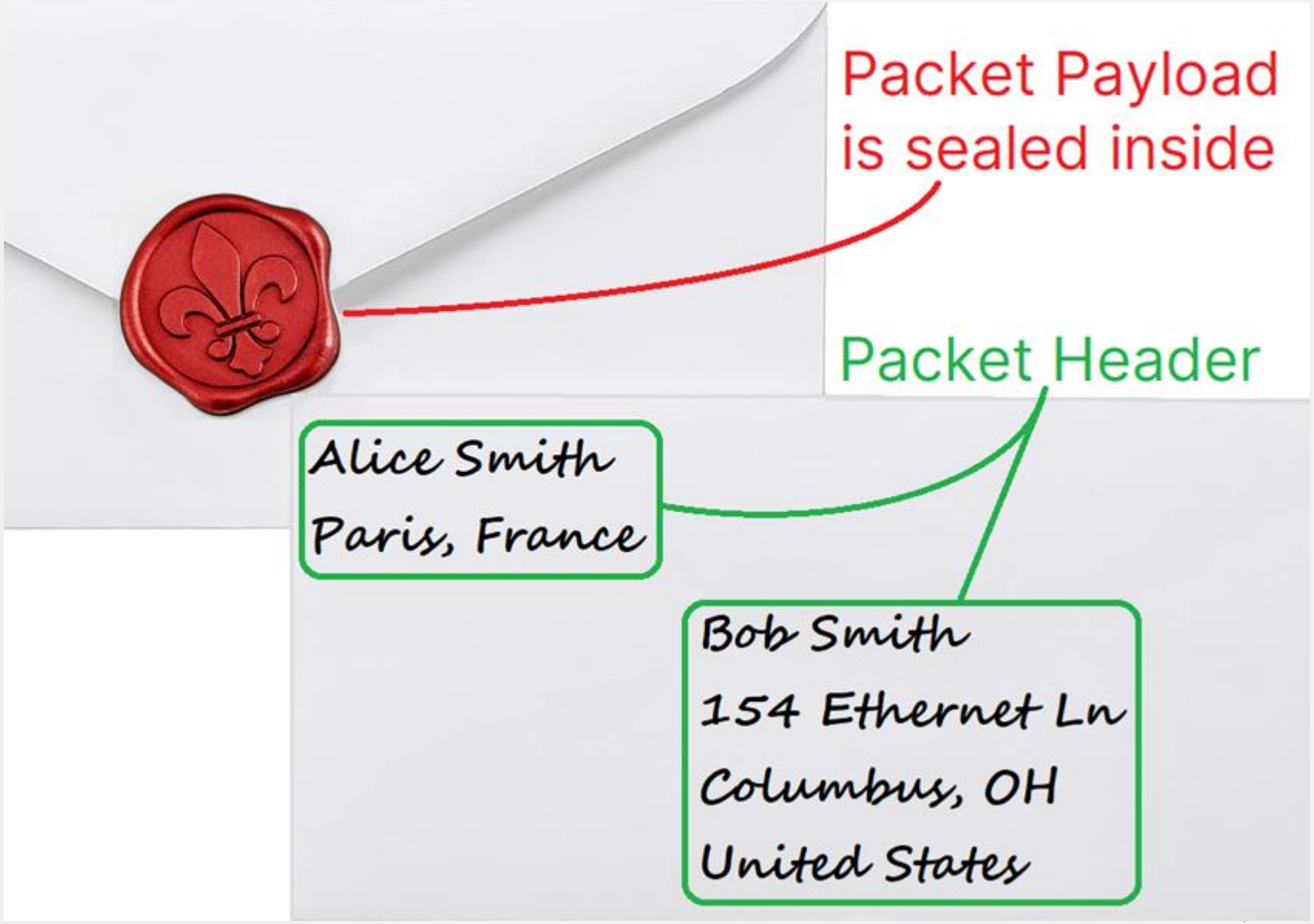
- Data is sent over the network in packets
- Packets have a header to get them to their destination
- Packets also have a payload: the contents of the message
- Unencrypted packets are like using a postcard
- Anyone can see the contents of the message (and tamper with it!)



What is SSL Encryption?

Postcards vs Envelopes

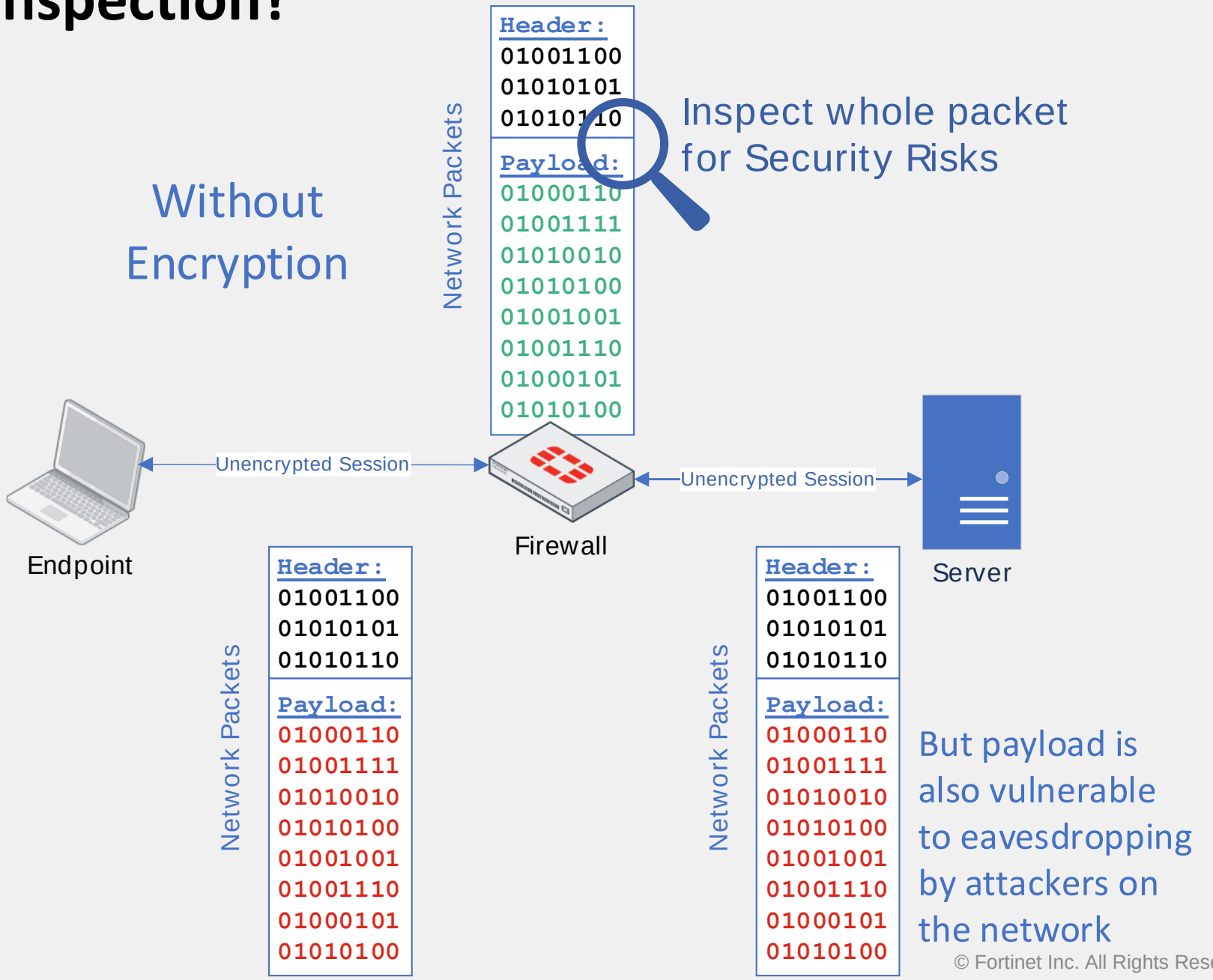
- Encrypted packets are like using an envelope
- Only the header may be seen in transit
- The message contents are sealed inside the envelope
- The seal can also reveal tampering attempts



What is Deep SSL Inspection?

A History Lesson

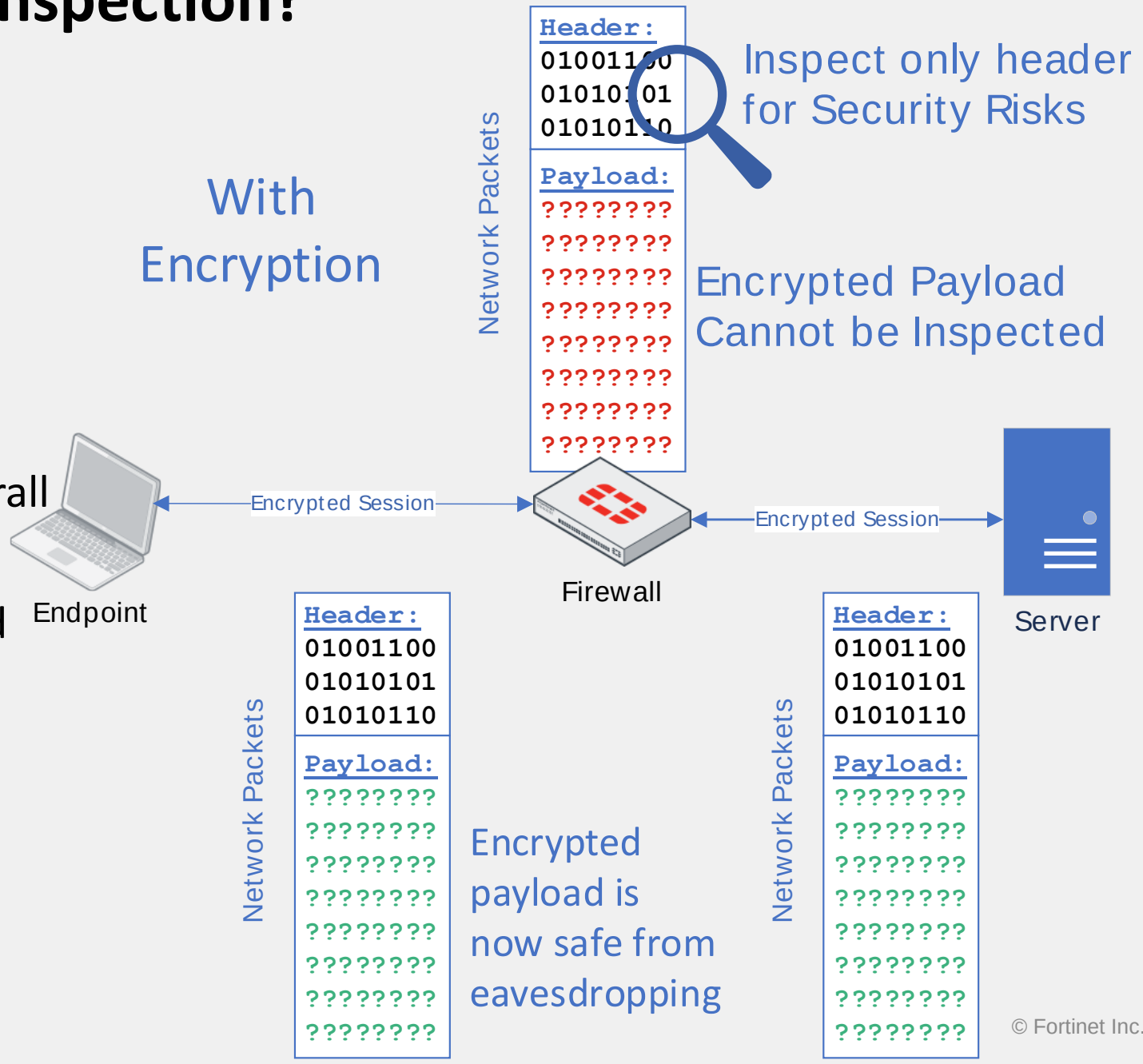
- In the early days, most packets were unencrypted
- Easy for firewalls to inspect for security risks
- But vulnerable to eavesdropping and tampering by attackers



What is Deep SSL Inspection?

A History Lesson

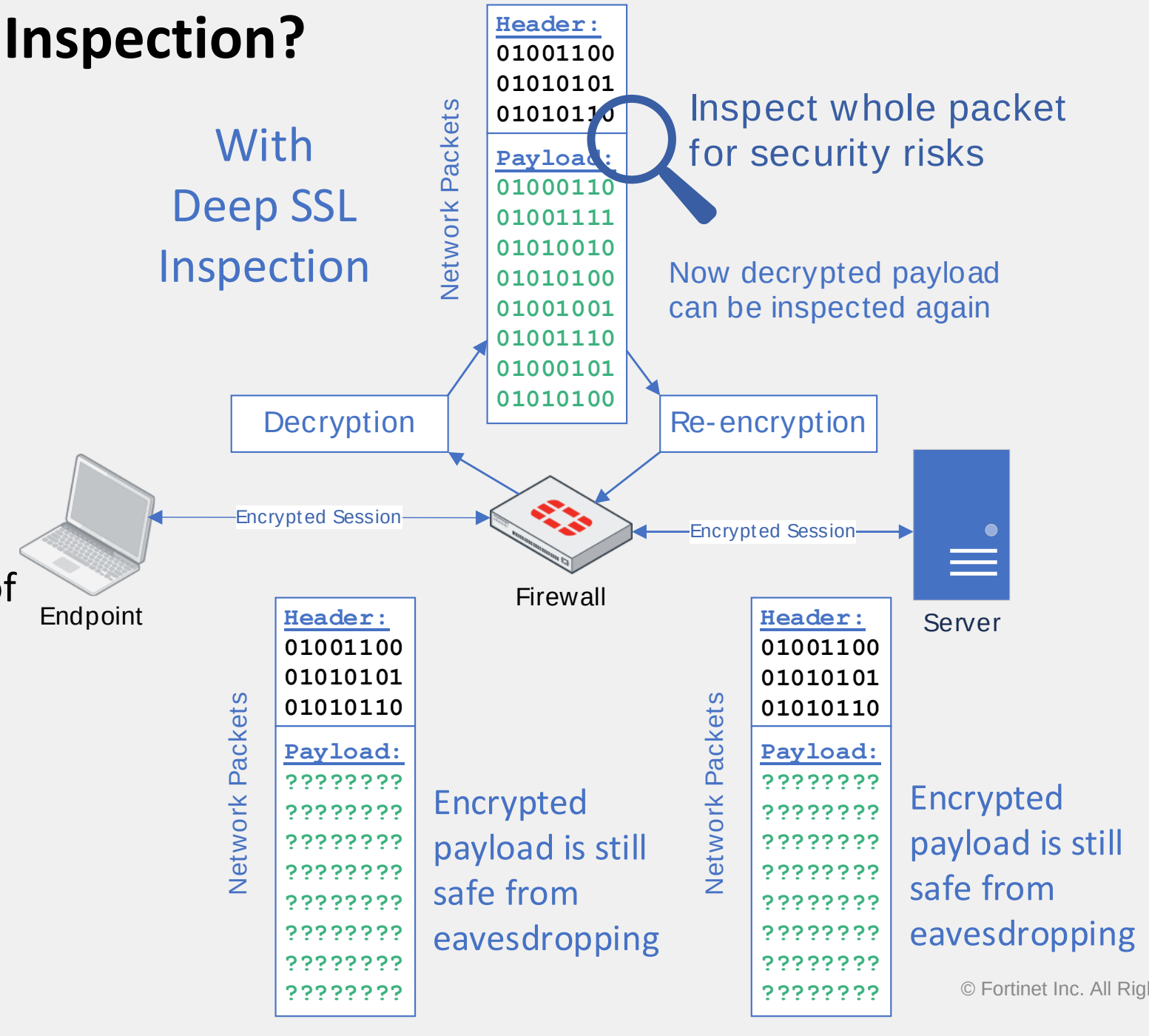
- SSL encryption prevents eavesdropping and tampering
- But now firewalls can't inspect the full packet
- This greatly reduces overall security effectiveness
- Attackers quickly learned they could hide attacks using SSL encryption of their own



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?

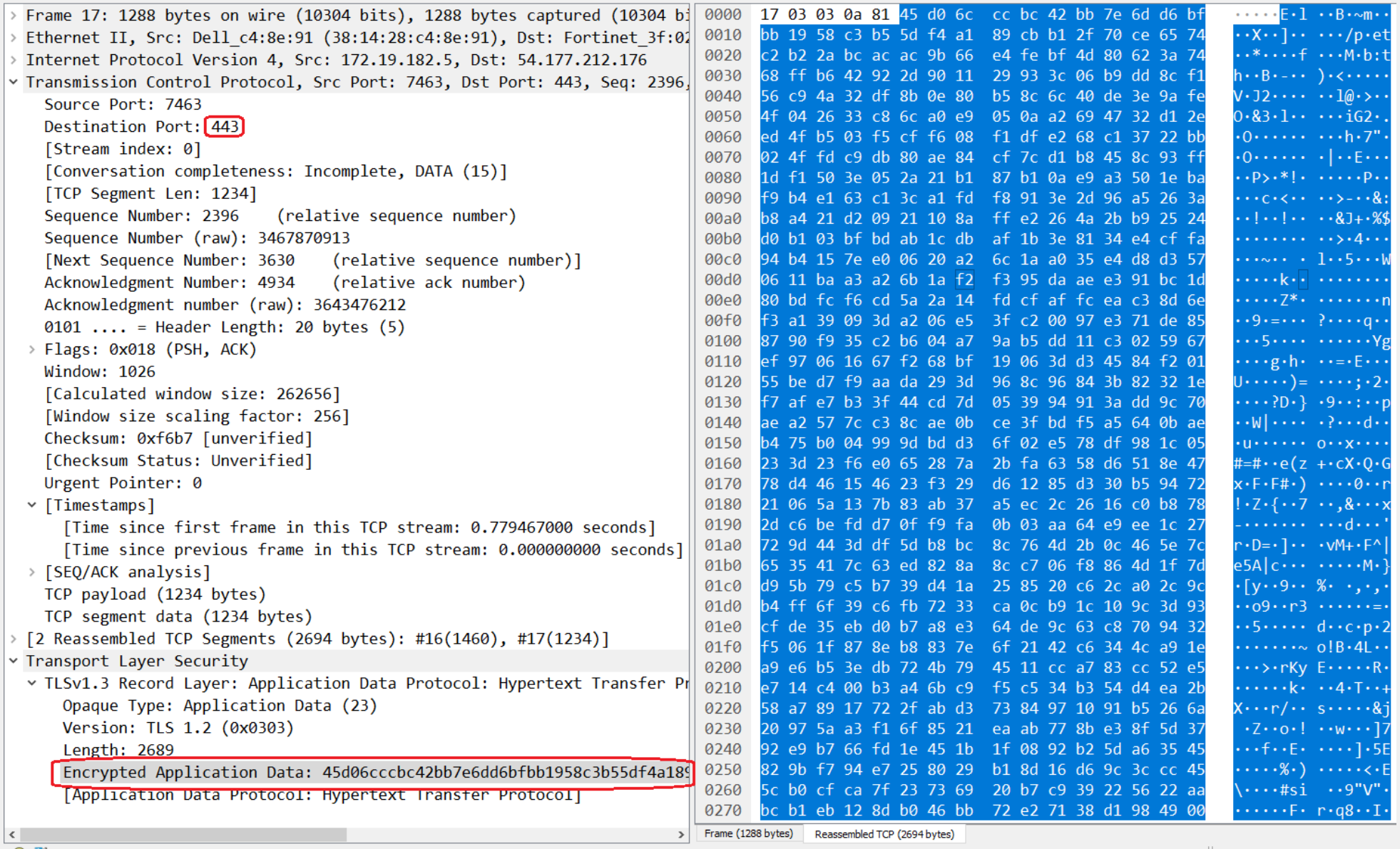
Almost all of it!

Is there malware lurking in the encrypted data?

Phishing links?

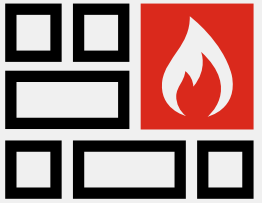
Data exfiltration?

Only way to know is Deep SSL Inspection!



Visibility when HTTP is Encrypted (HTTPS)

A tale of two Google Forms links



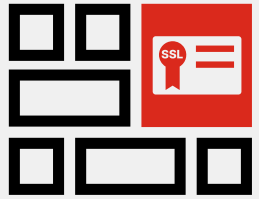
Without SSL Decryption, only the header is visible to the firewall

- 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

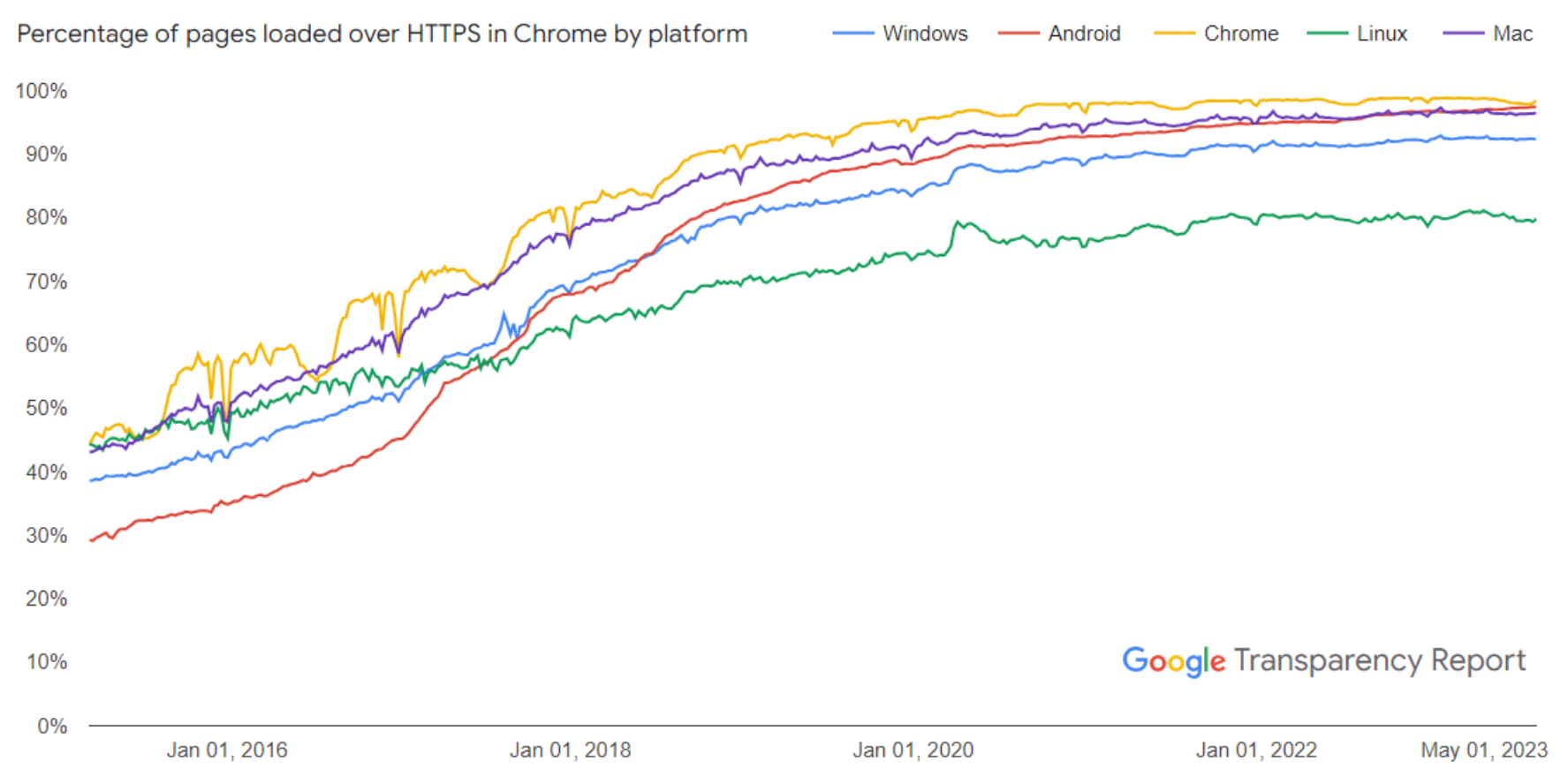
- Link 1: hxxps://forms.gle/GRFYjJwtDqVHVSf9A ✓
  - Web Filter inspects: Category = Web-Based Applications
  - This site is safe: Let it pass!
- Link 2: hxxps://forms.gle/DsW75p3St1dUMTyK6 !!!
  - Web Filter inspects: Category = Phishing!
  - This site is malicious: Block it!

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

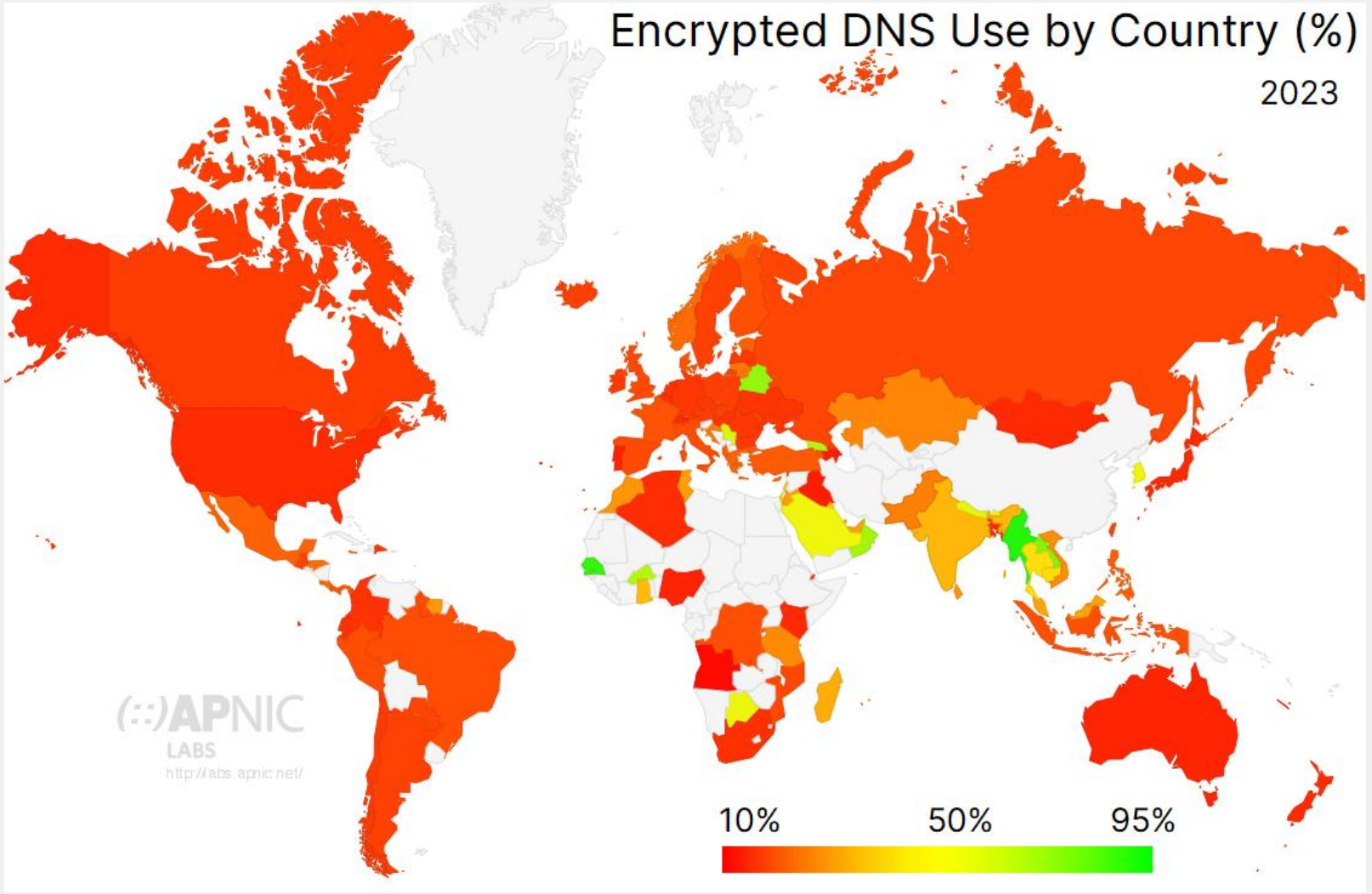


Source: https://transparencyreport.google.com/https/overview

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

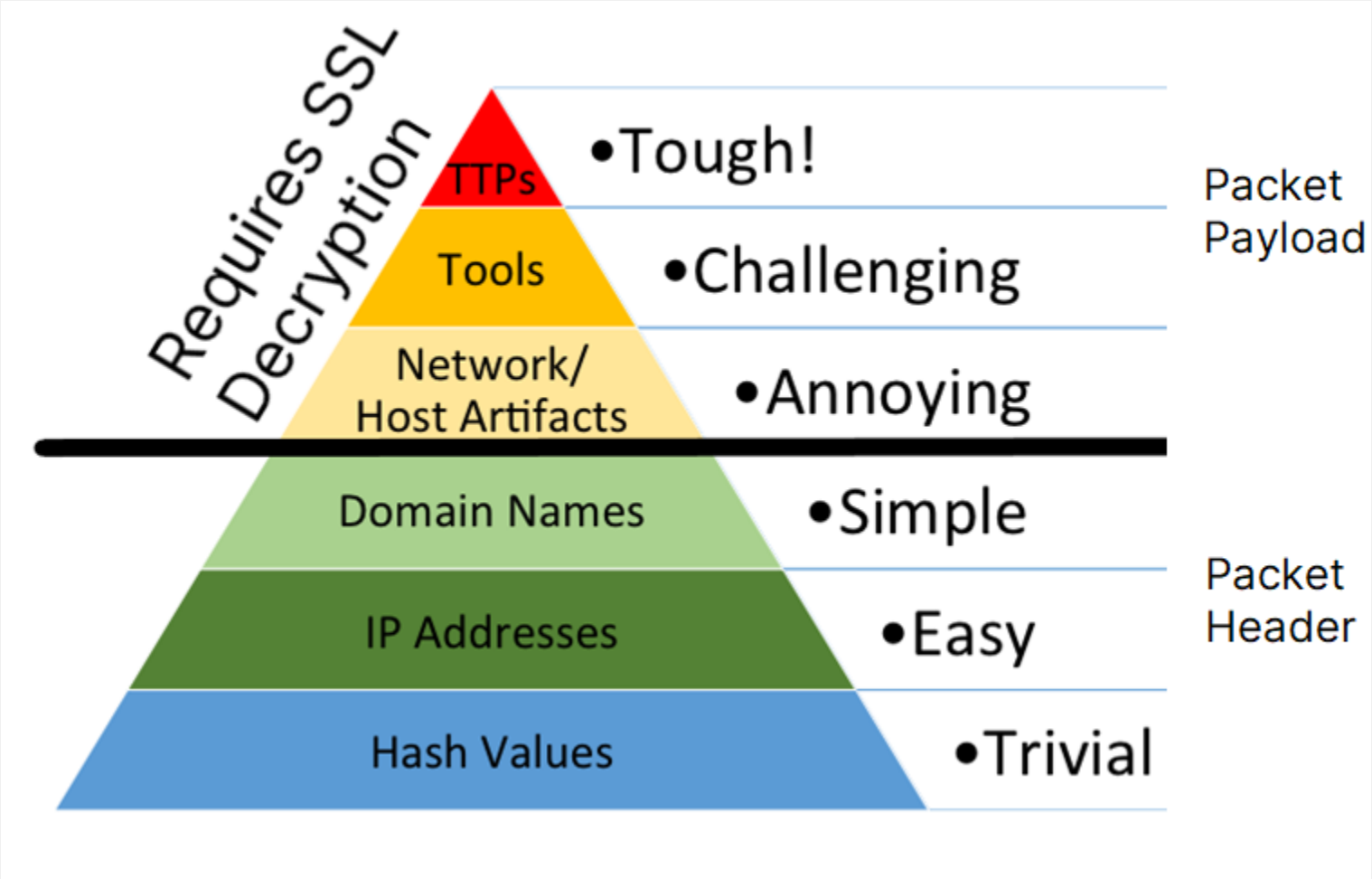


Source: https://stats.labs.apnic.net/edns

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

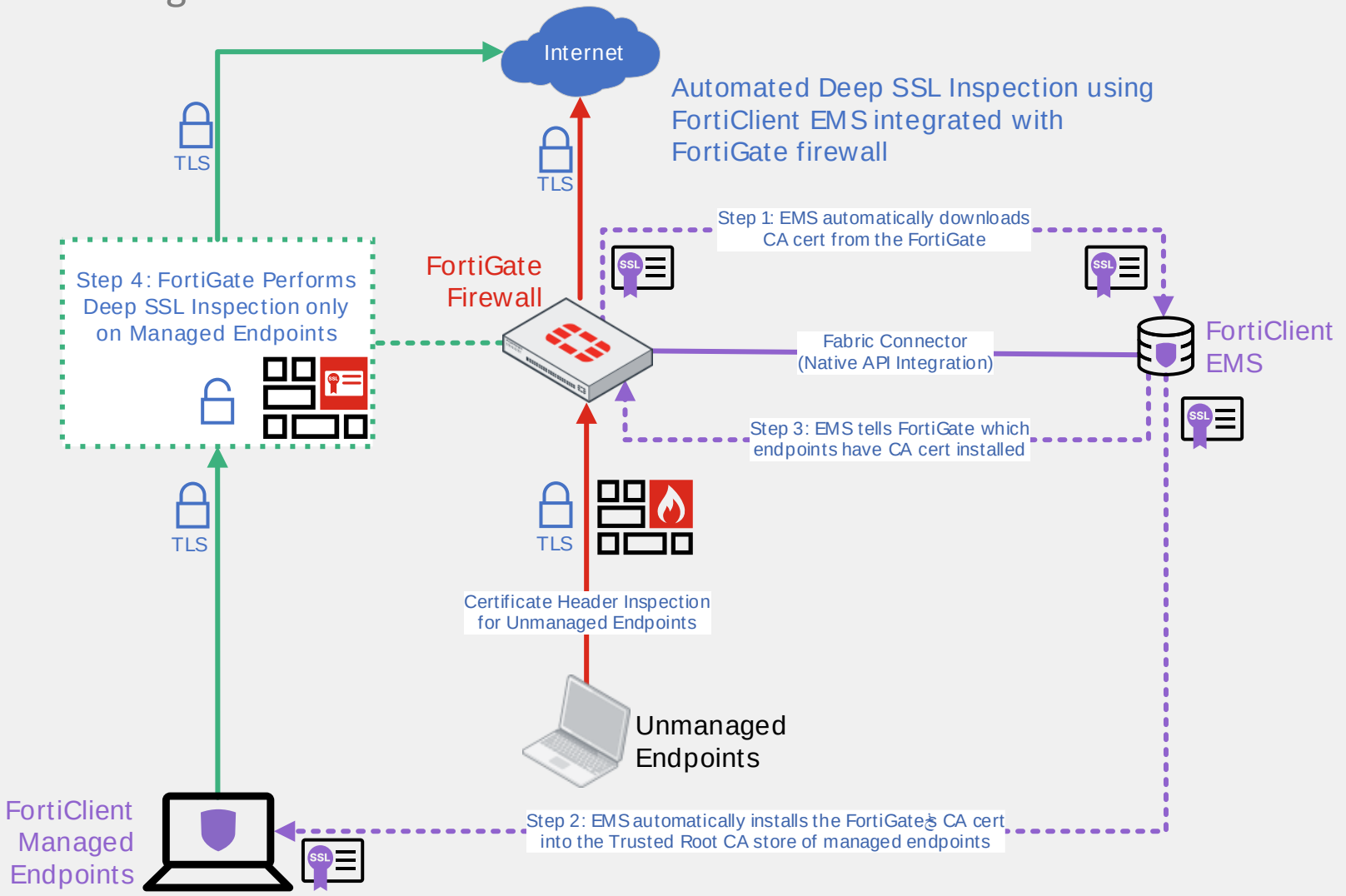


Attribution: David Bianco
Source: https://www.sans.org/tools/the-pyramid-of-pain/

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 are 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

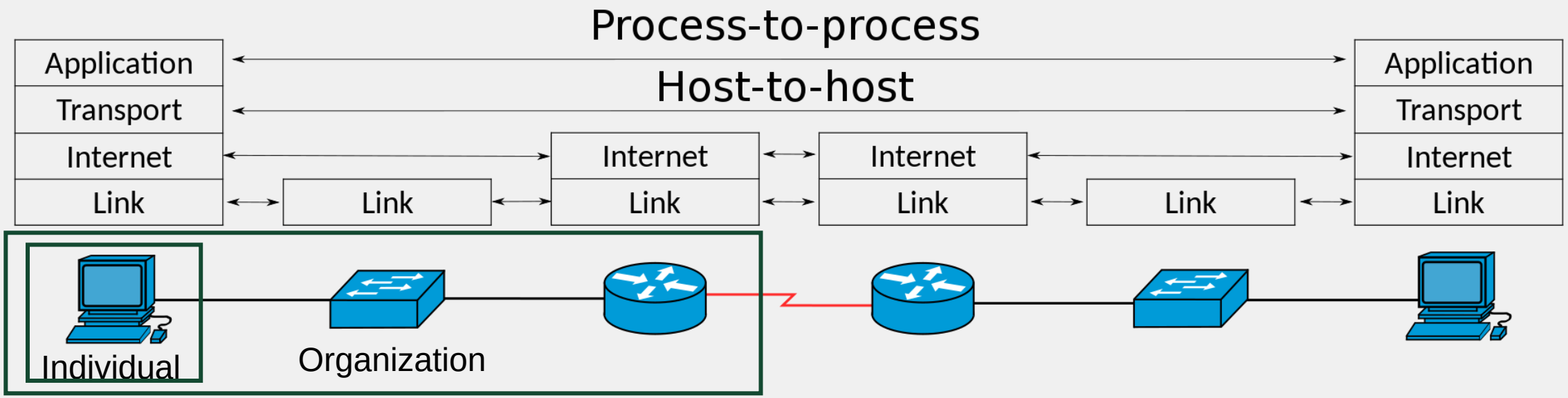


Image Source: https://en.wikipedia.org/wiki/End-to-end_principle

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

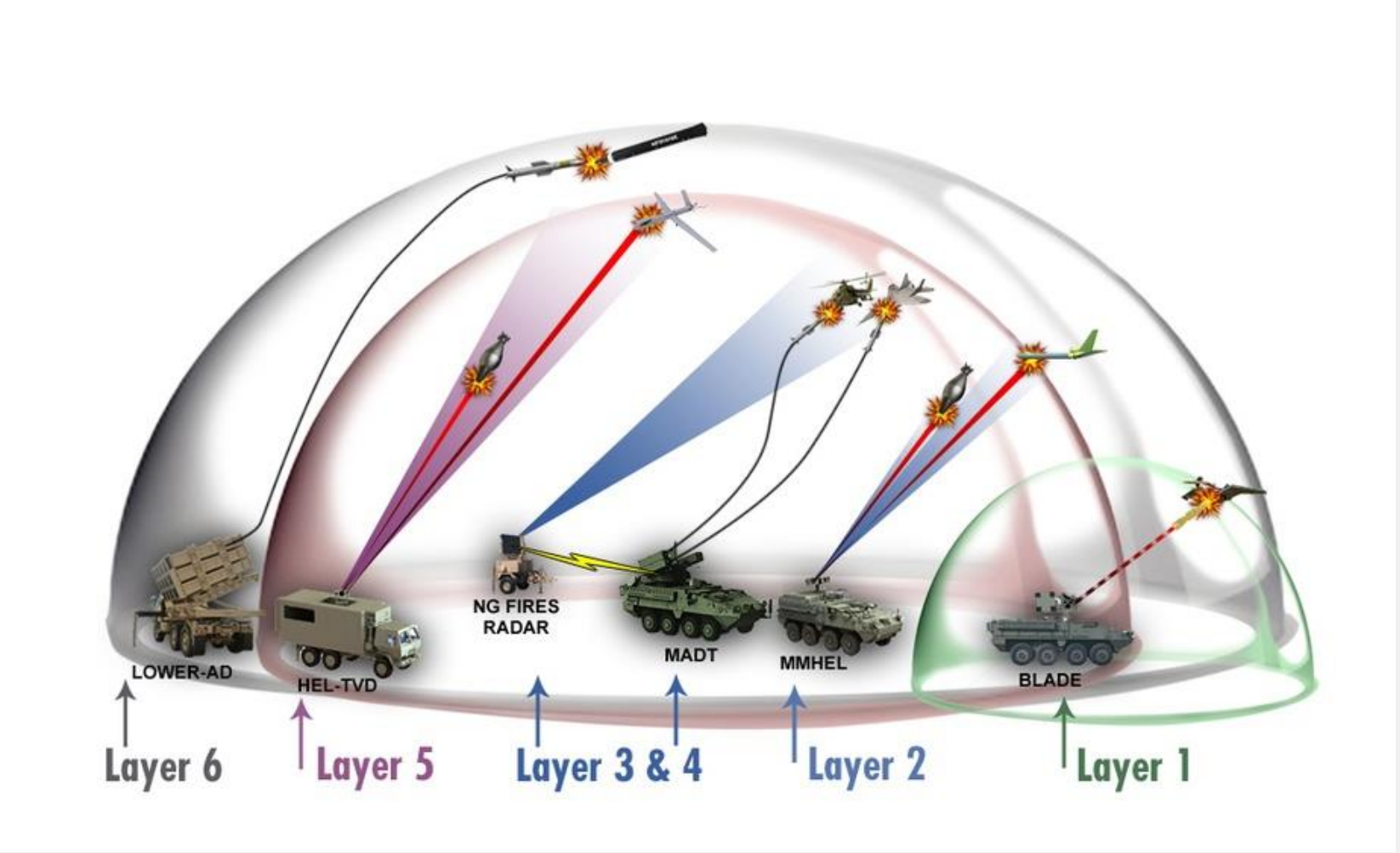
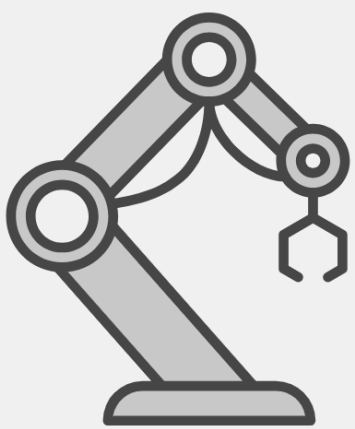


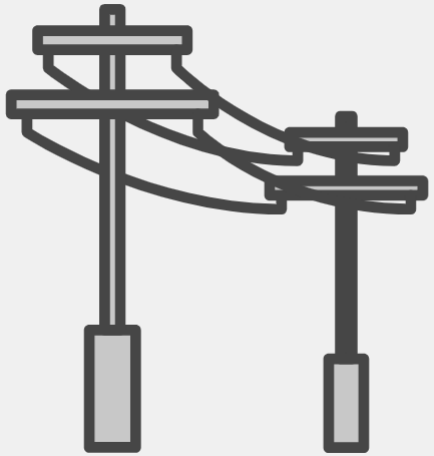
Image Source: https://www.dvidshub.net/image/5735184/tiered-defense

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!

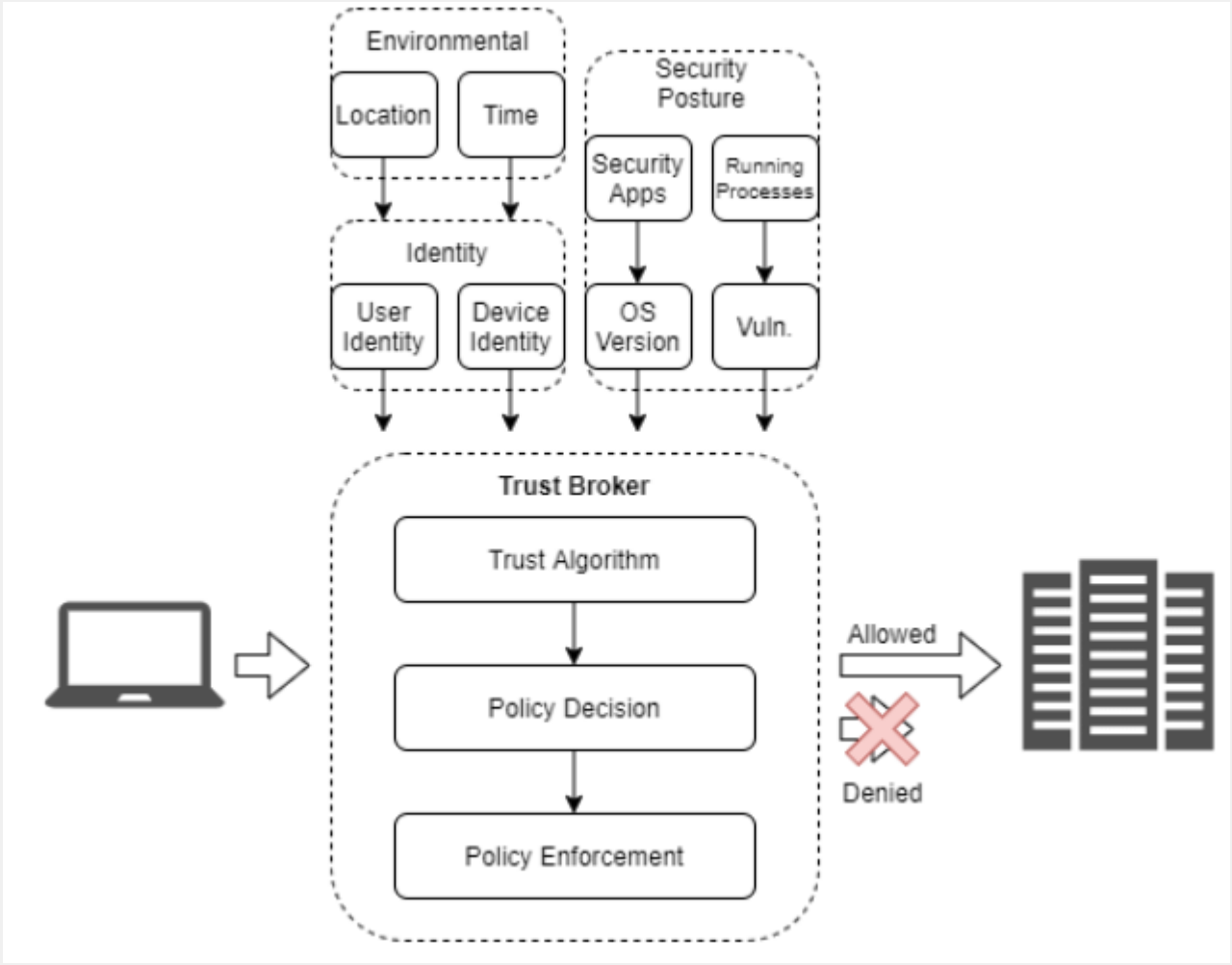
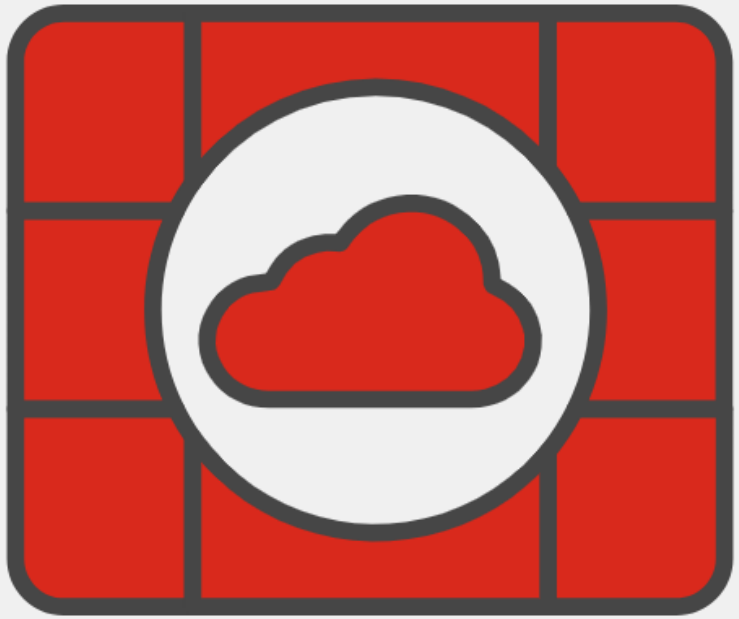


Image source: https://docs.fortinet.com/document/fortigate/7.0.0/ztna-concept-guide/324163/trusted-entities

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

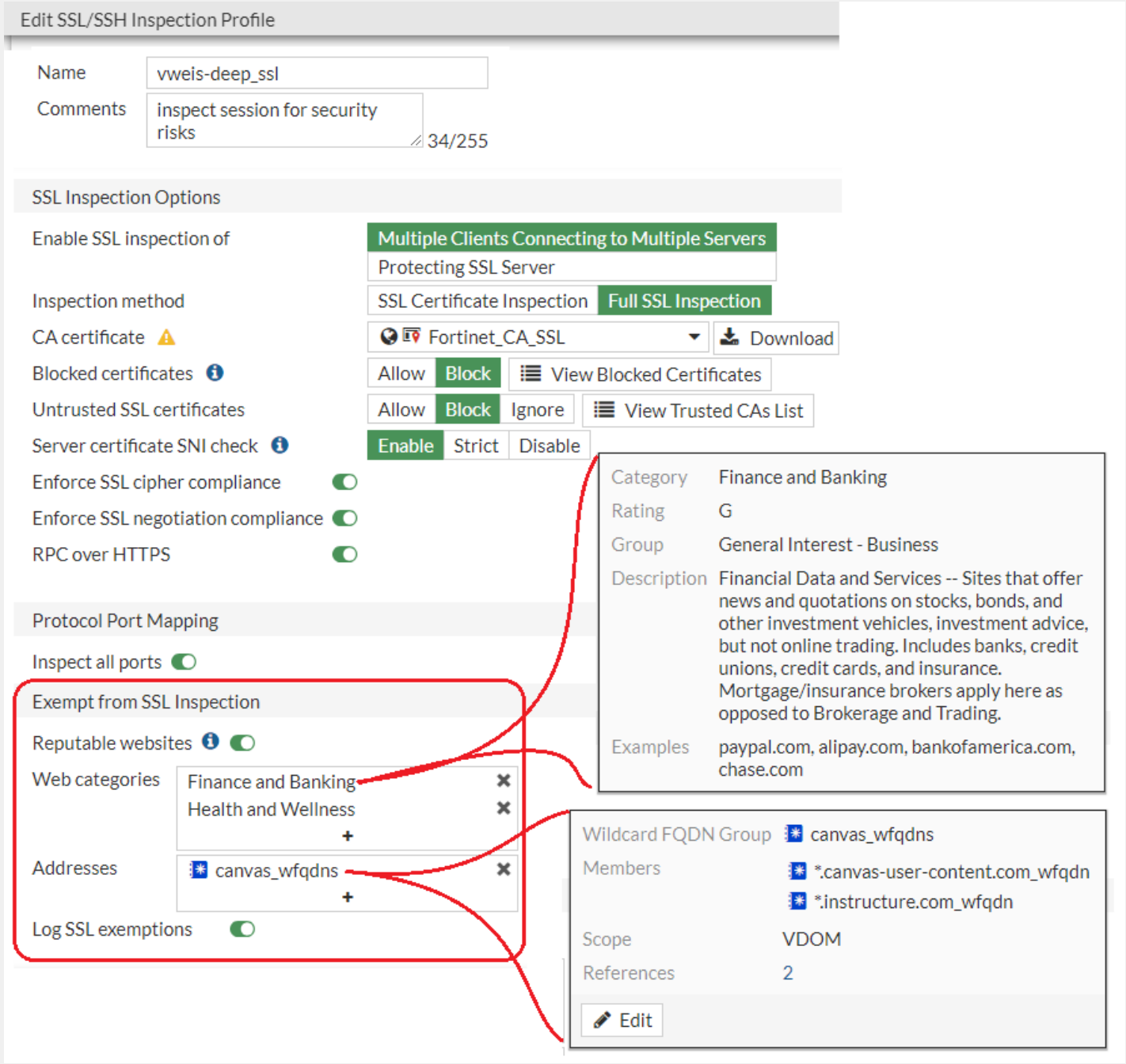
What the CISOs are concerned about

- 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



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?”

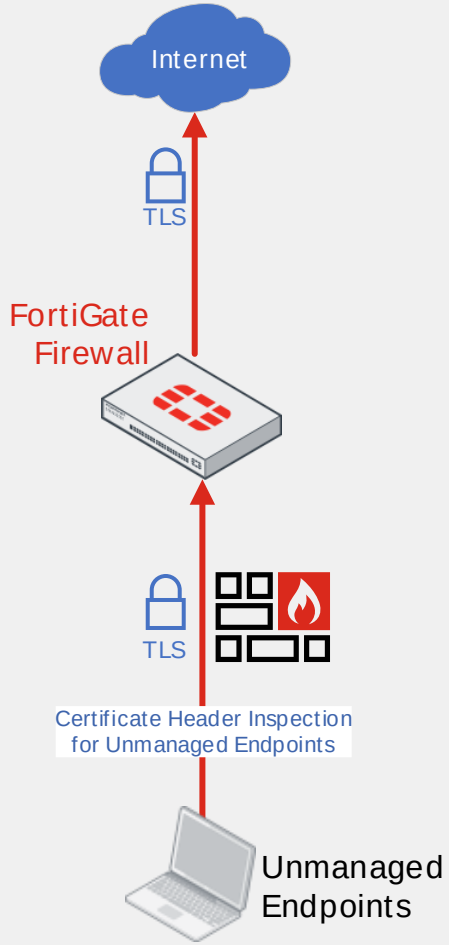
Complexity Objections

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

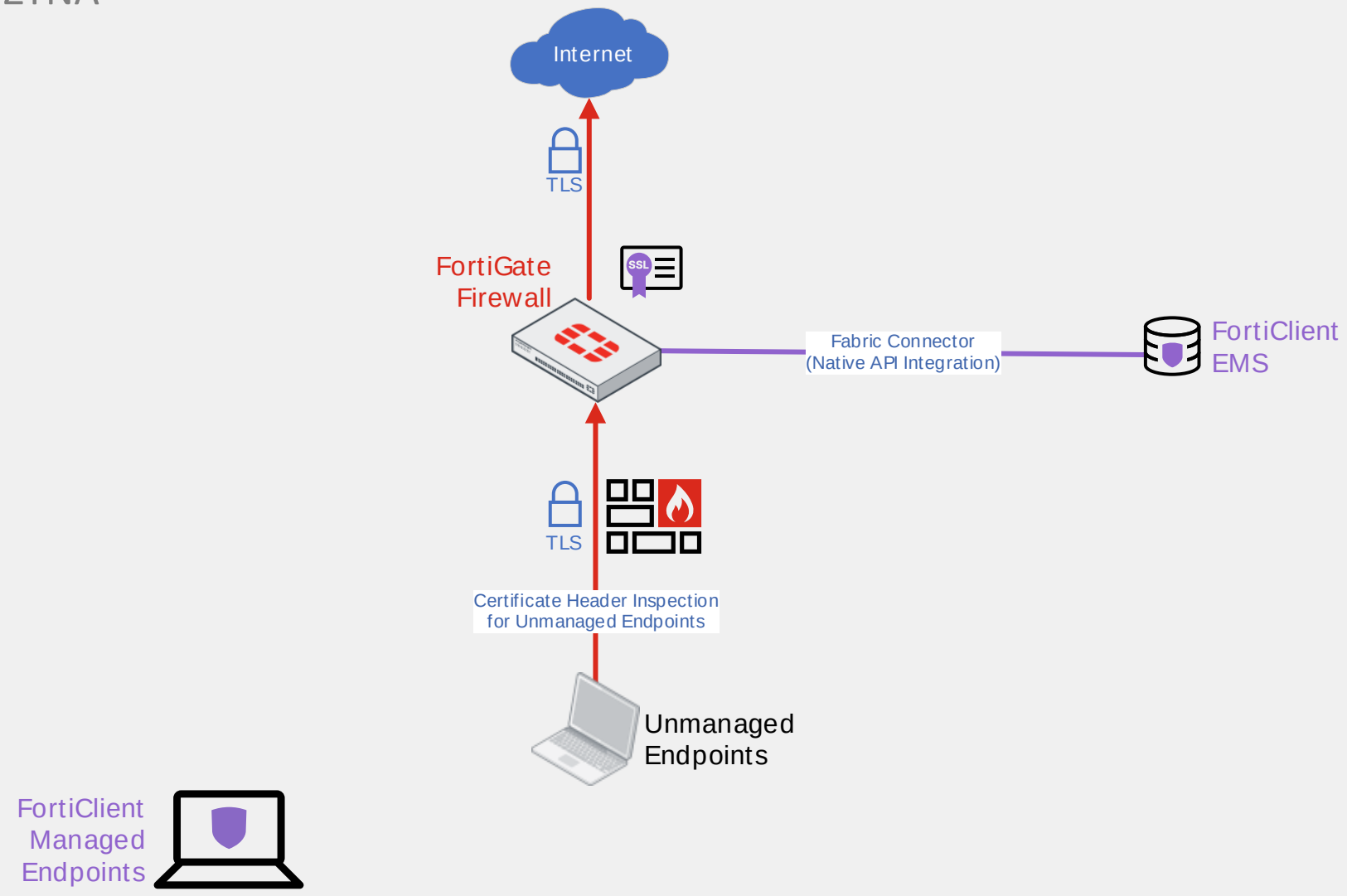
Easy Rollout of Deep SSL with FortiClient ZTNA

Before FortiClient ZTNA



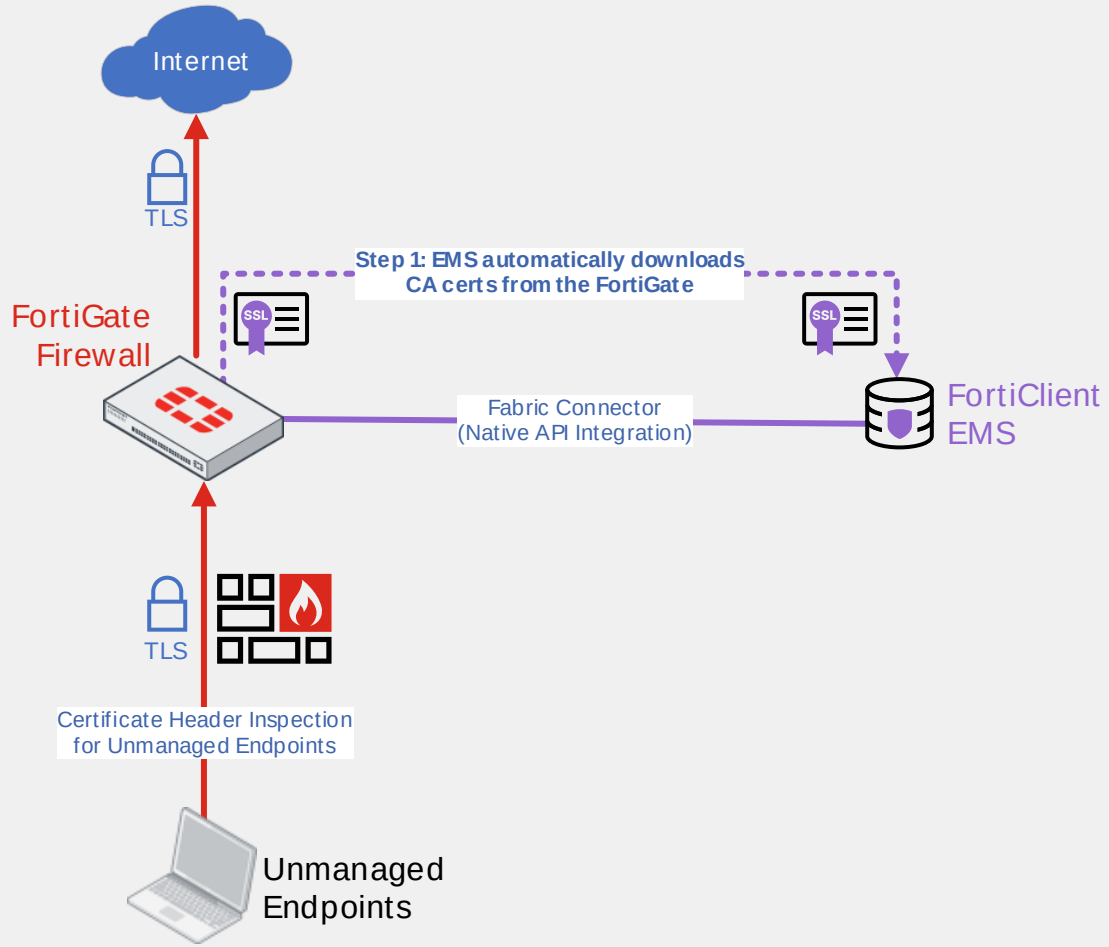
Easy Rollout of Deep SSL with FortiClient ZTNA

Add in FortiClient ZTNA



Easy Rollout of Deep SSL with FortiClient ZTNA

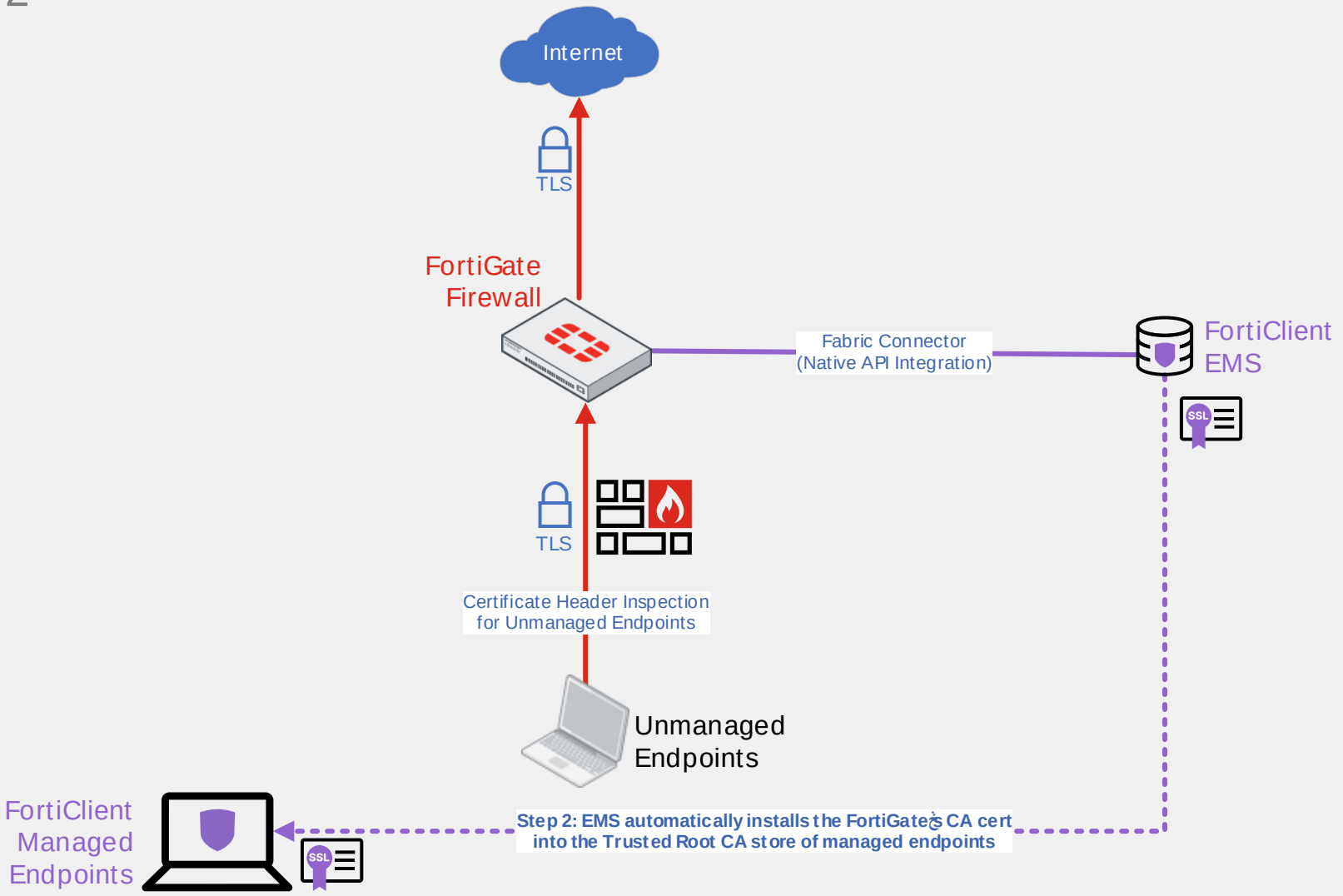
Automation Step 1



FortiClient
Managed
Endpoints

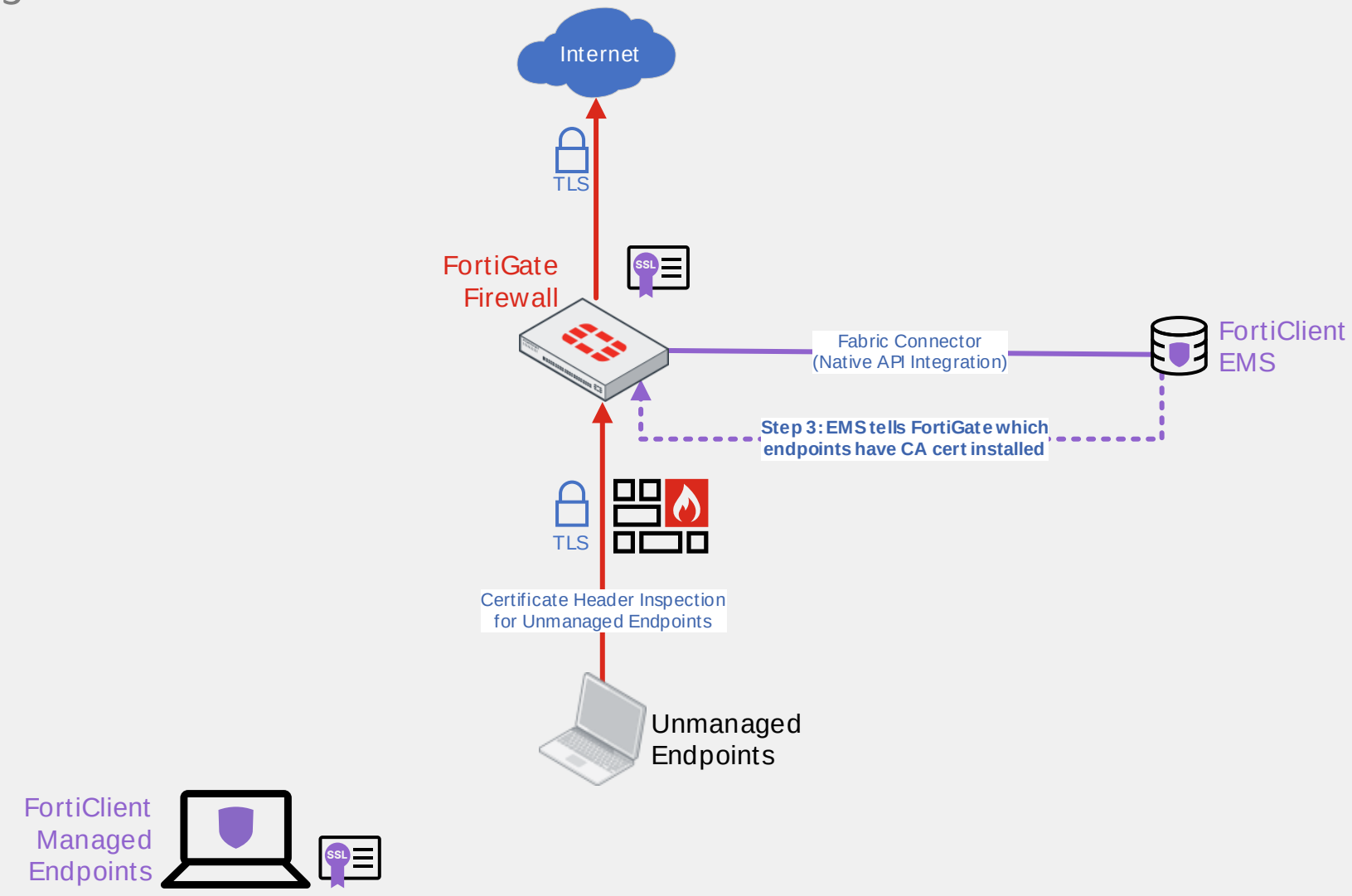
Easy Rollout of Deep SSL with FortiClient ZTNA

Automation Step 2



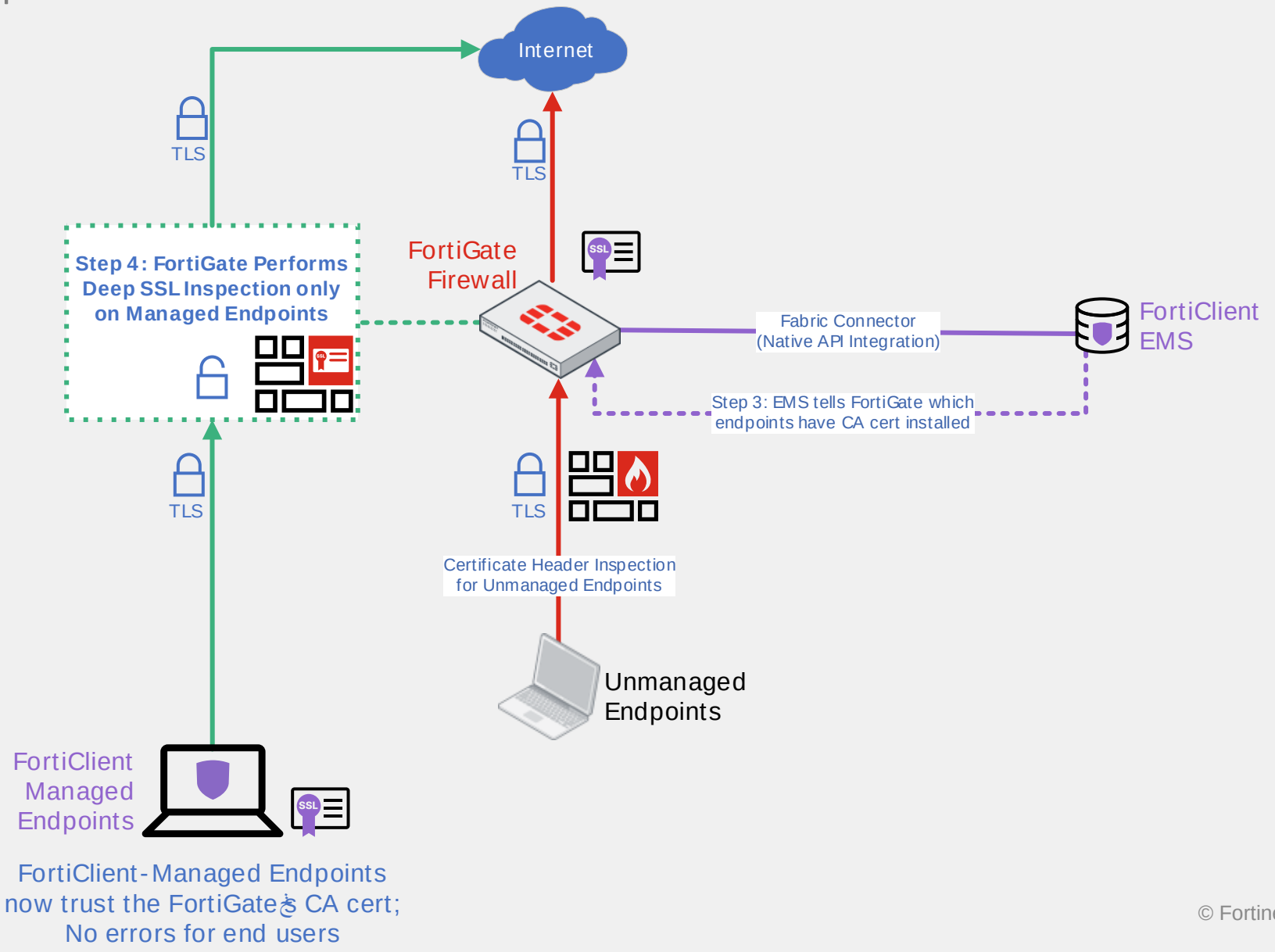
Easy Rollout of Deep SSL with FortiClient ZTNA

Automation Step 3



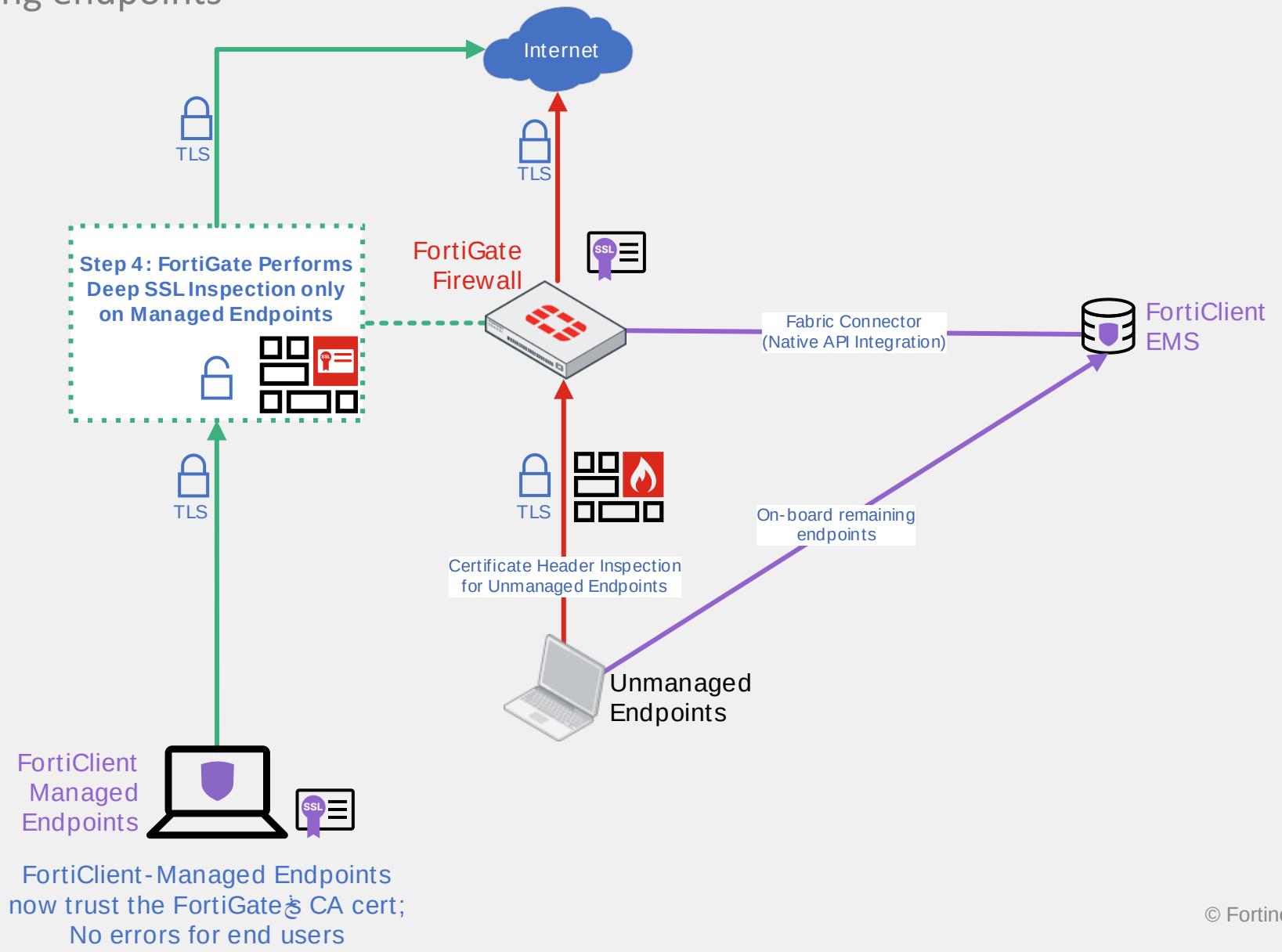
Easy Rollout of Deep SSL with FortiClient ZTNA

Automation Step 4



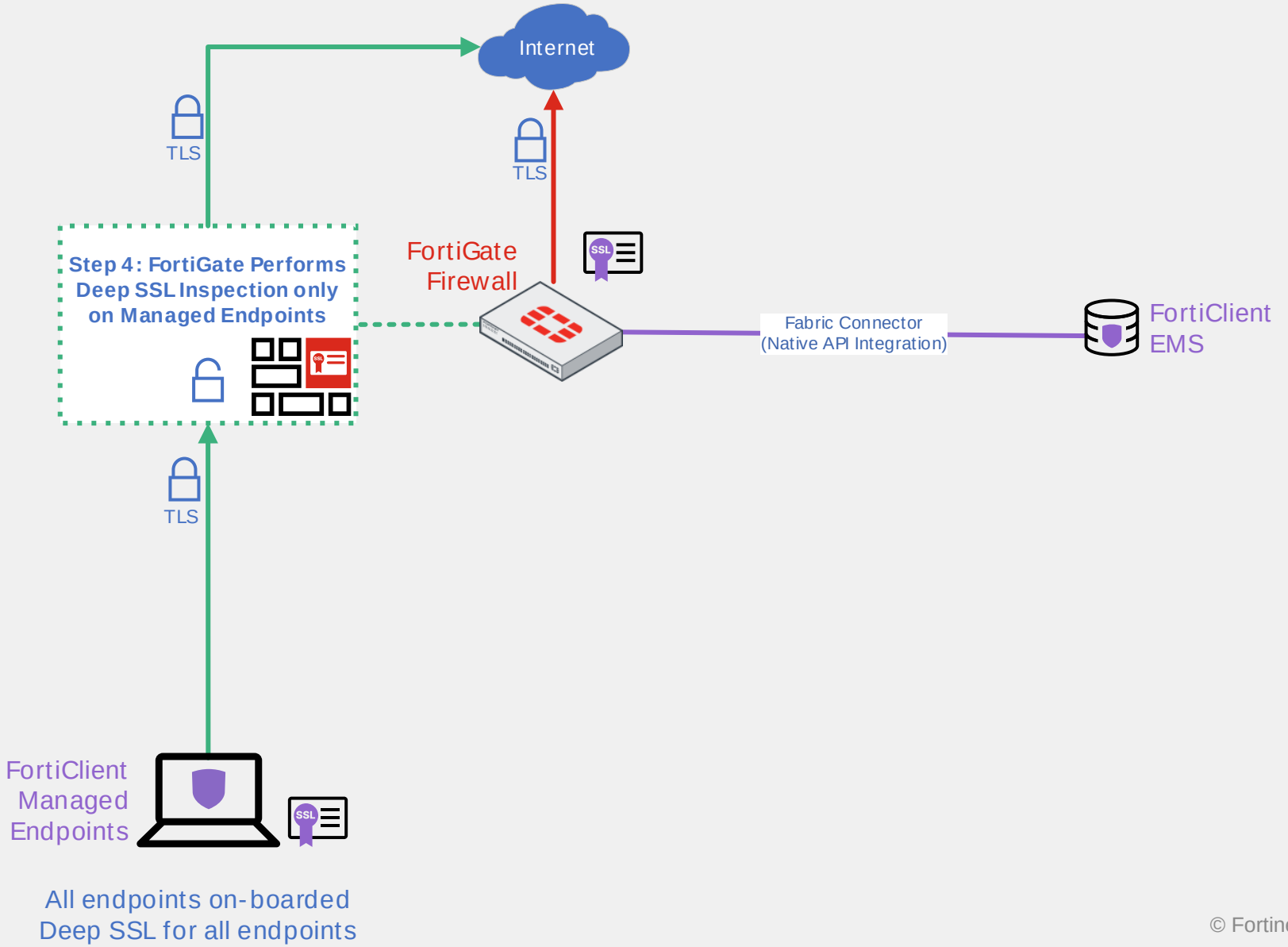
Easy Rollout of Deep SSL with FortiClient ZTNA

On-board remaining endpoints



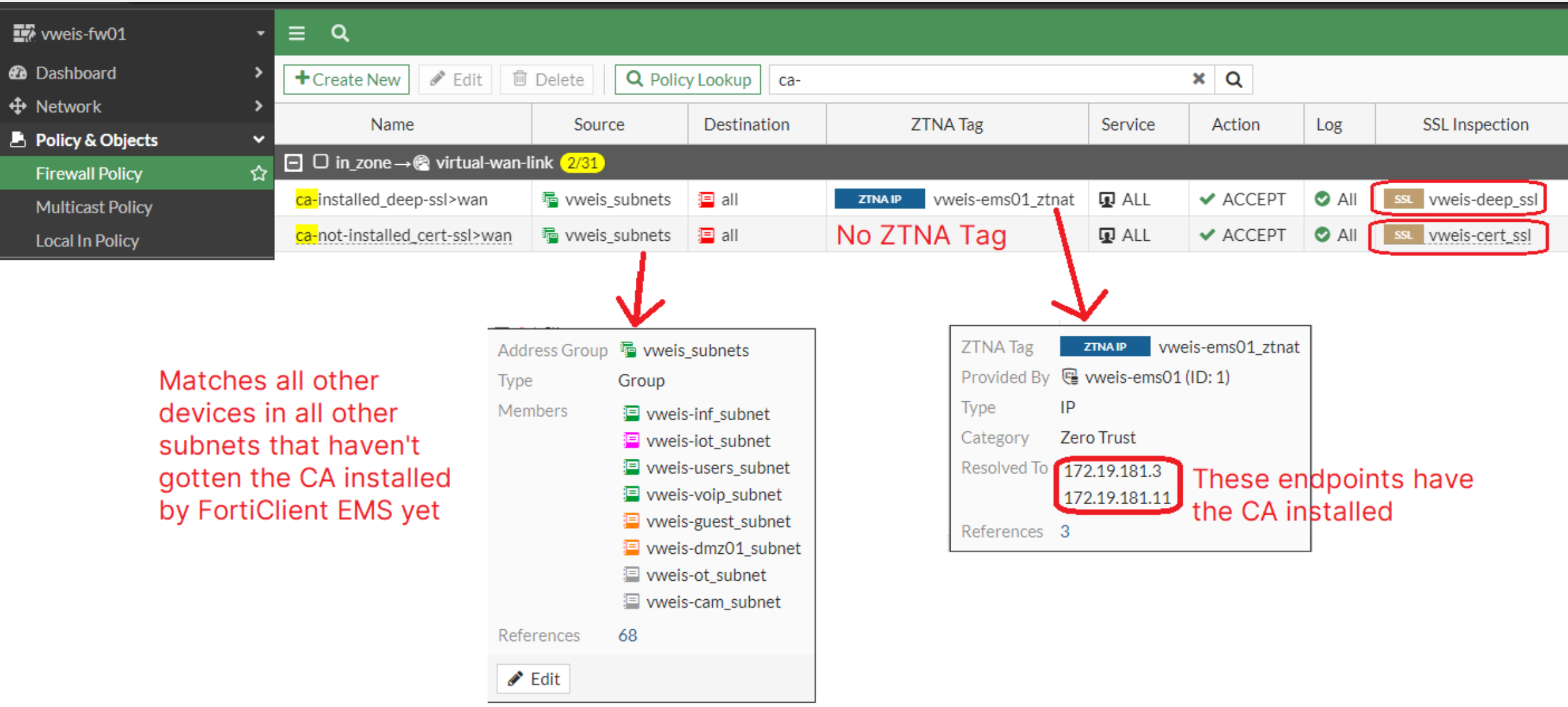
Easy Rollout of Deep SSL with FortiClient ZTNA

Endgame



Corresponding policies on FortiGate

Can be as simple as two policies



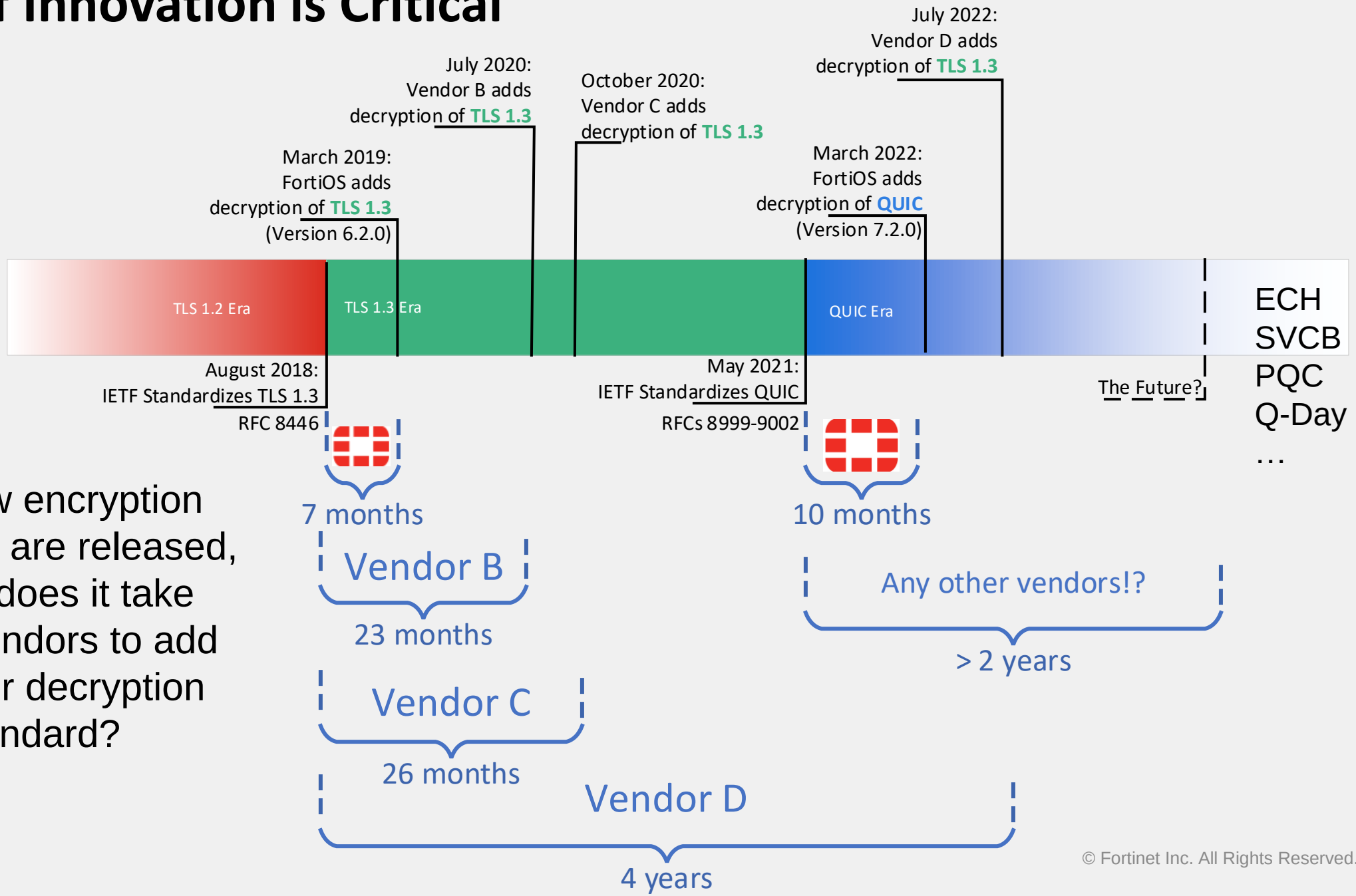
Matches all other devices in all other subnets that haven't gotten the CA installed by FortiClient EMS yet

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!

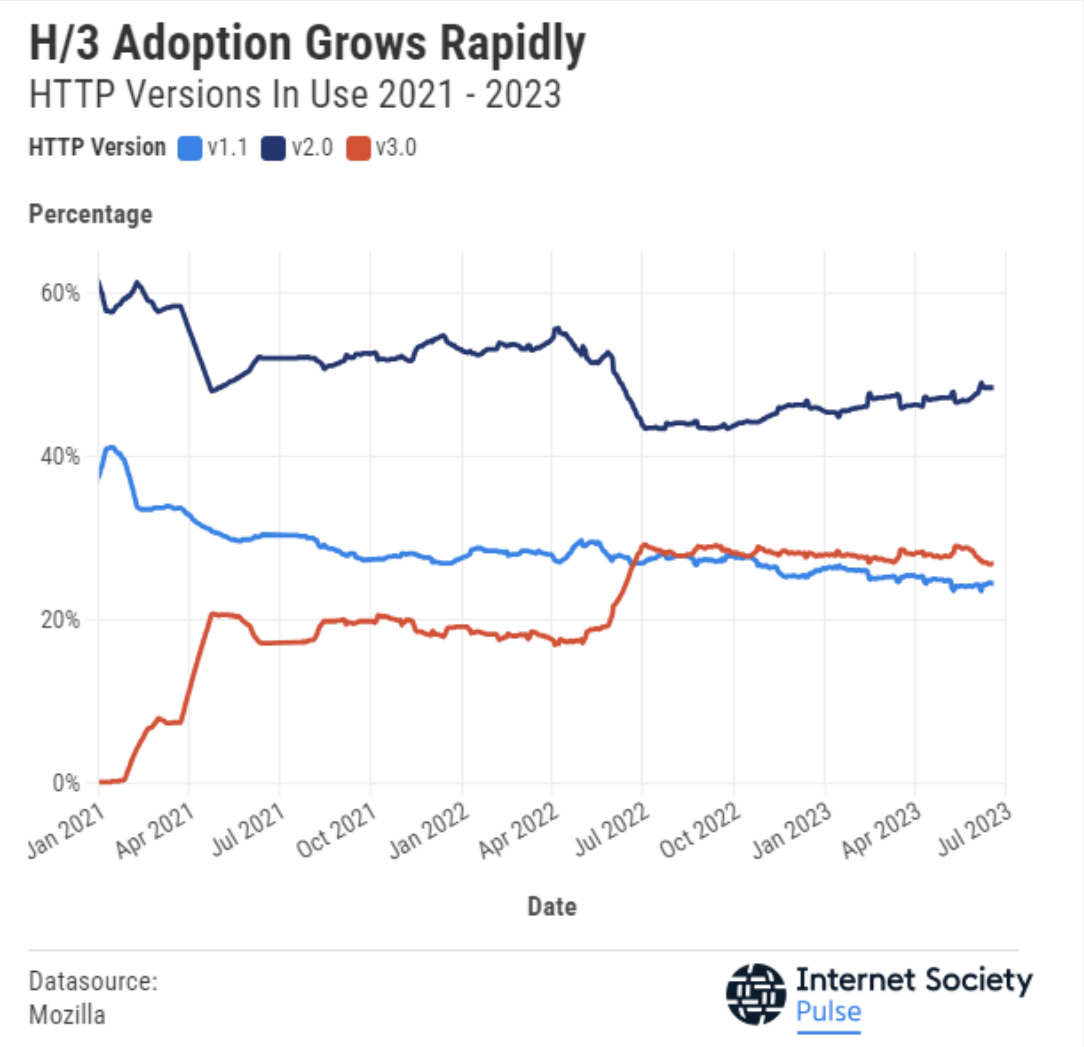
Speed of Innovation is Critical



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

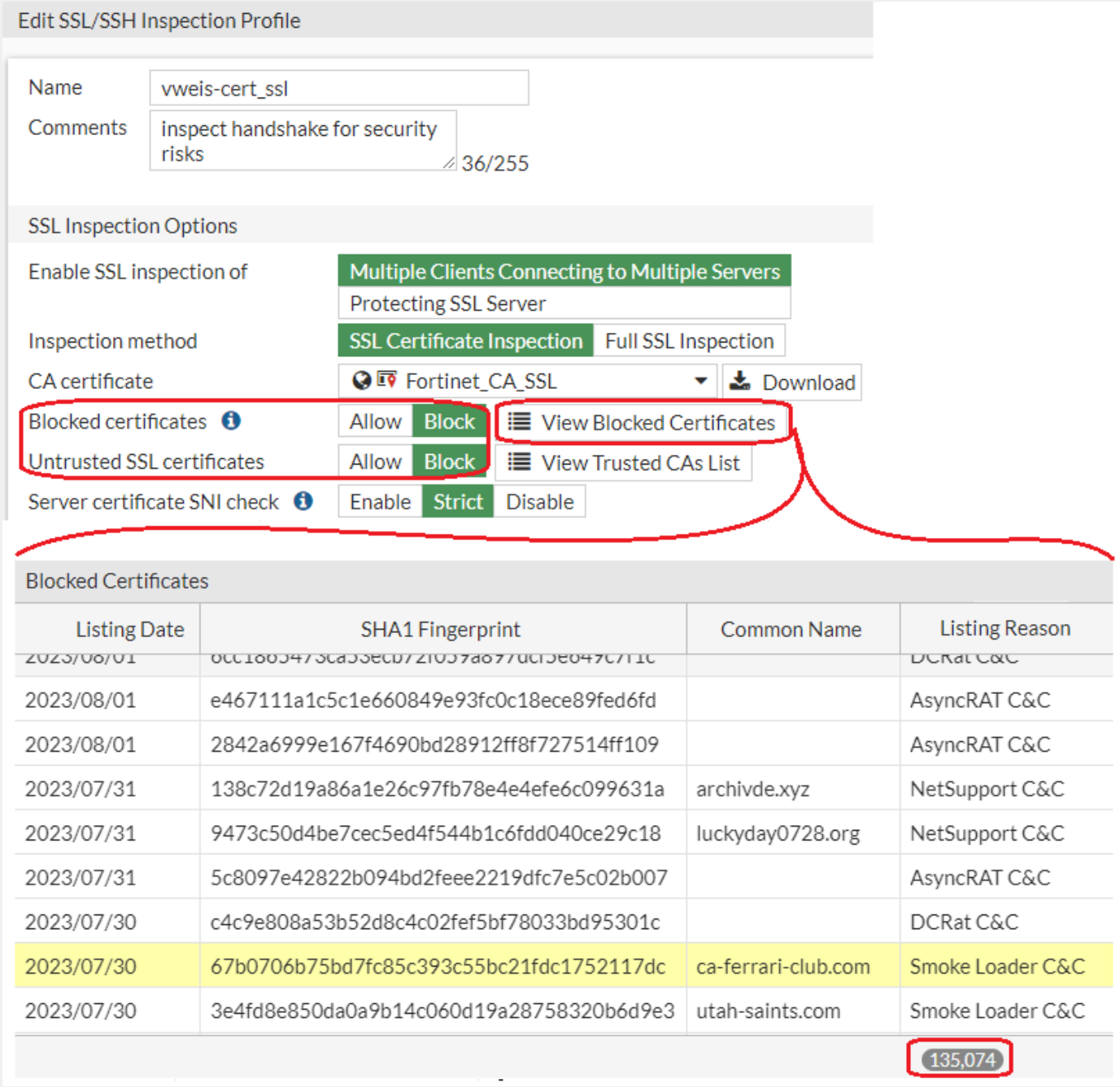
Where to Start

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

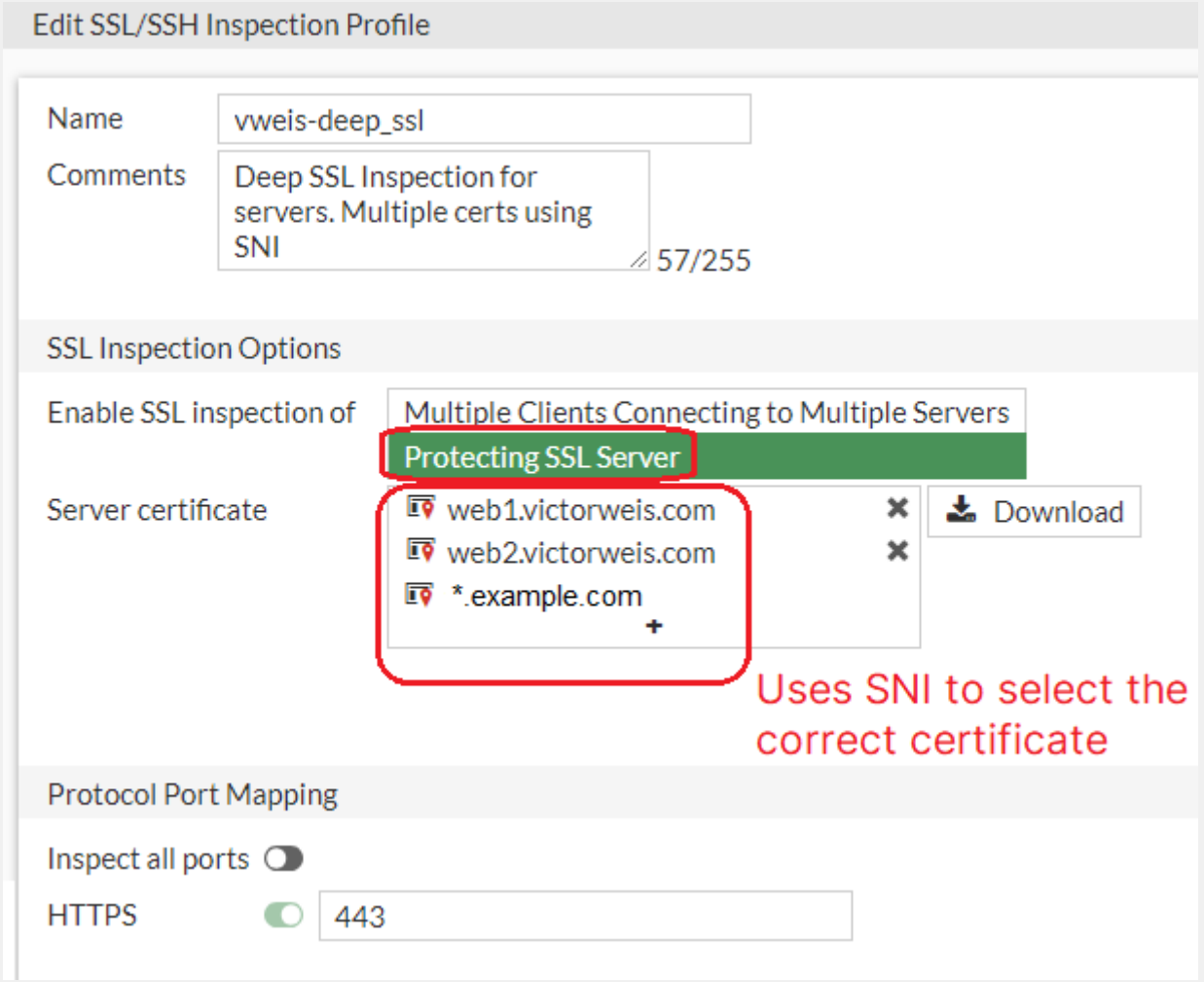
Step 1:
Certificate Fingerprinting

- 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



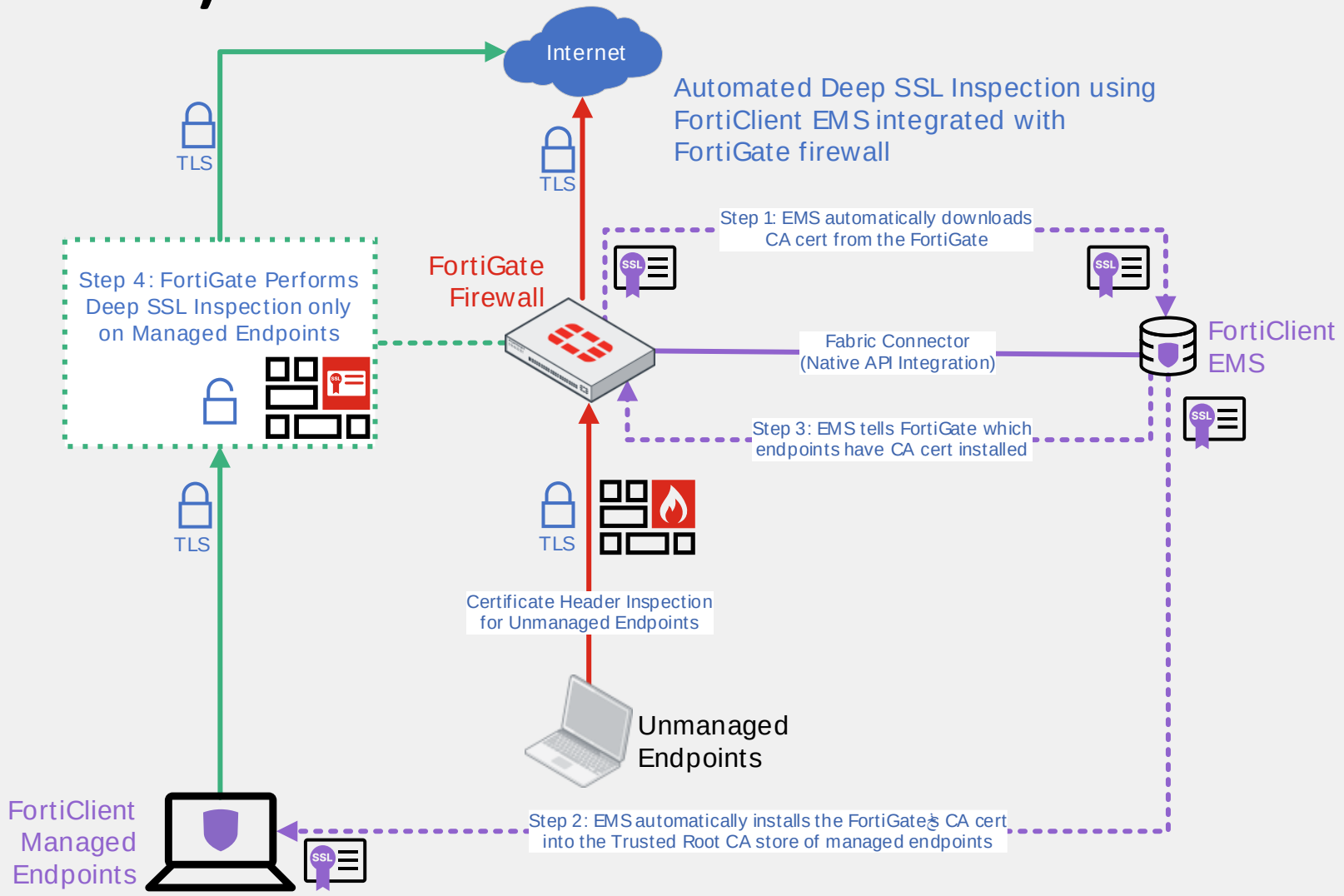
Step 2: Servers

- 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



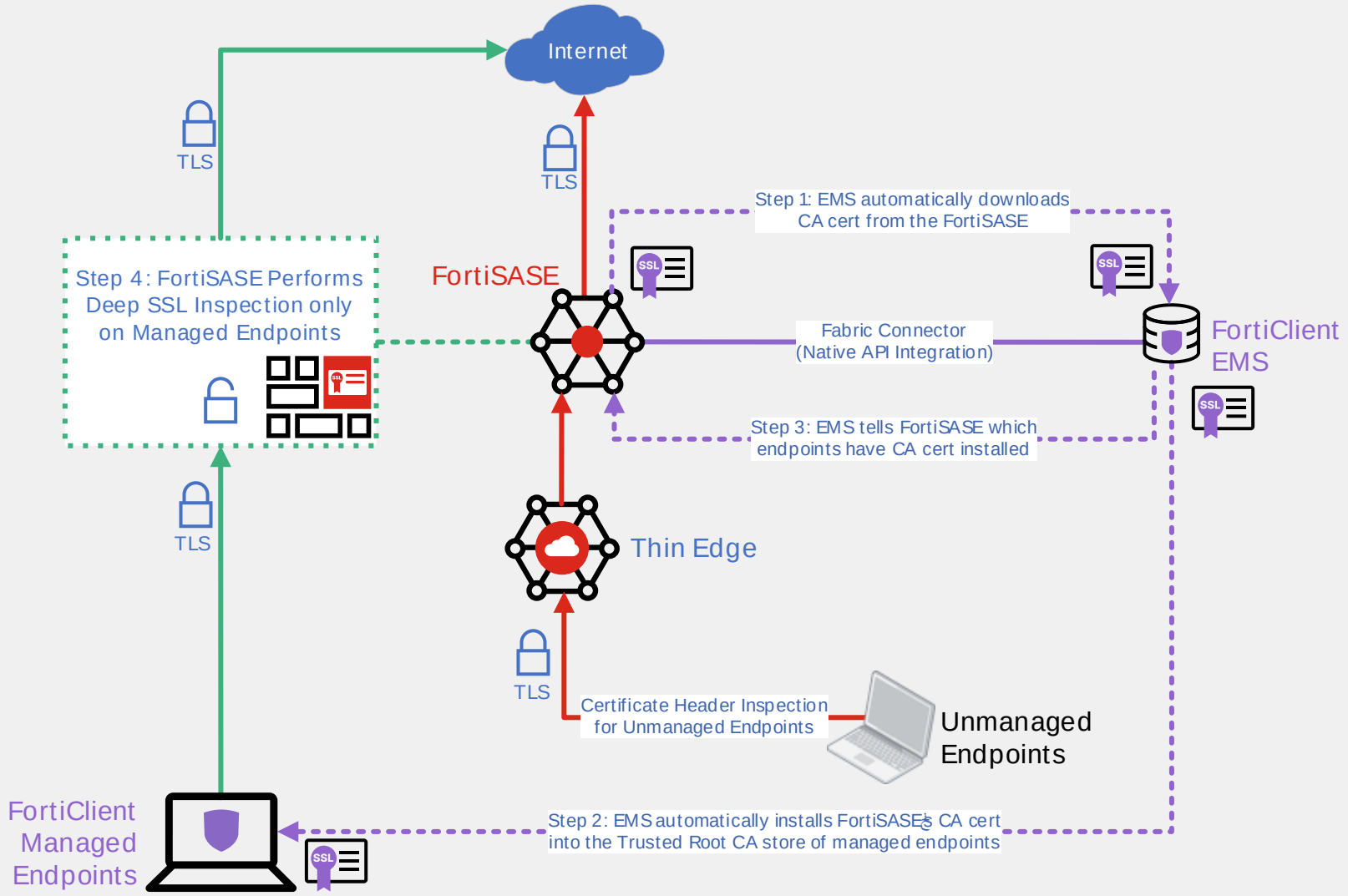
Step 3:
Endpoints (On-Prem FortiGate)

- 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

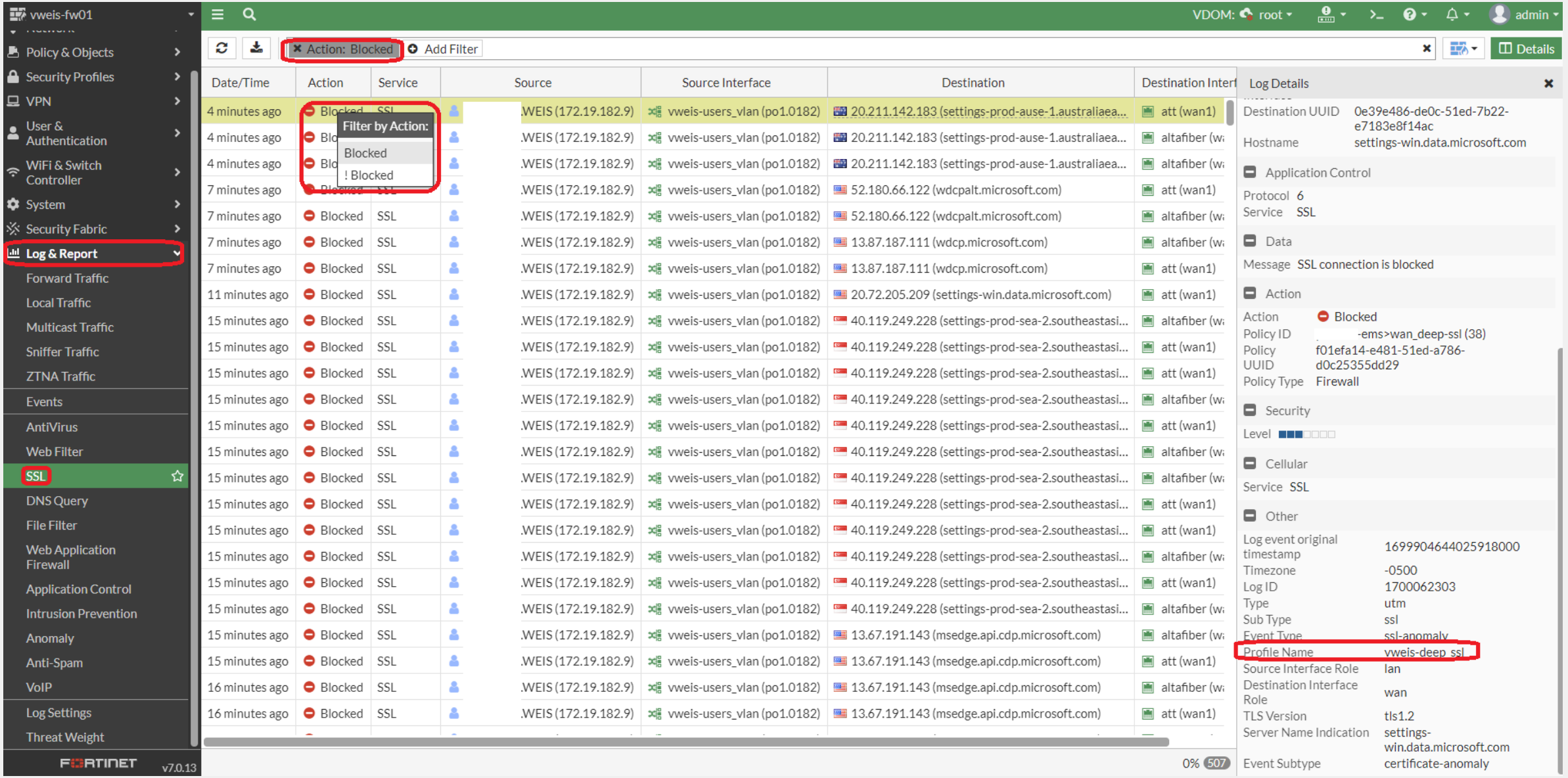
- Performance! Make sure you got it!
  - Ease in with rolling out certs to devices in batches and monitor for performance
- Firefox has a separate certificate store
  - Will either have to install CA into Firefox store, or configure Firefox to use OS store
  - This is part of the AUP definitions. Do 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

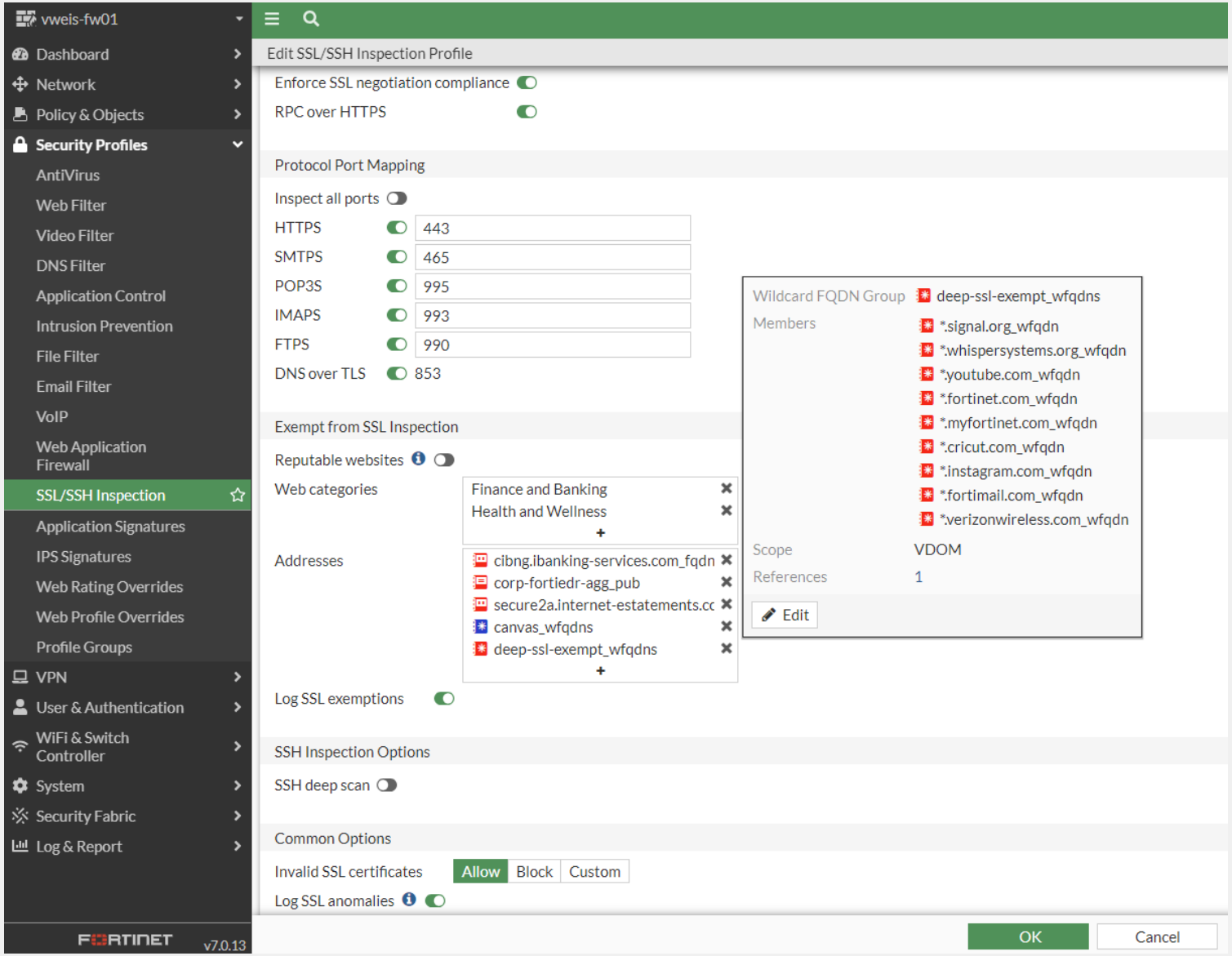
Things to watch out for

- 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



Creating Exemptions with Categories and FQDNs



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

FORTINET®