

The background features a vibrant, multi-colored abstract design. On the left, there are horizontal, wavy bands of color in shades of red, orange, yellow, and green. On the right, a bright white light source emits a series of sharp, triangular rays in various colors, including blue, green, and yellow, creating a sunburst effect.

CISCO *Live!*

Let's go

#CiscoLiveAPJC





The bridge to possible

Critical Requirements for Defending Government Networks

Andrew Benhase, Federal Architect
@CyberSecOps, @ThreatCowboy
BRKSEC-2067

CISCO *Live!*

#CiscoLiveAPJC

Cisco Webex App

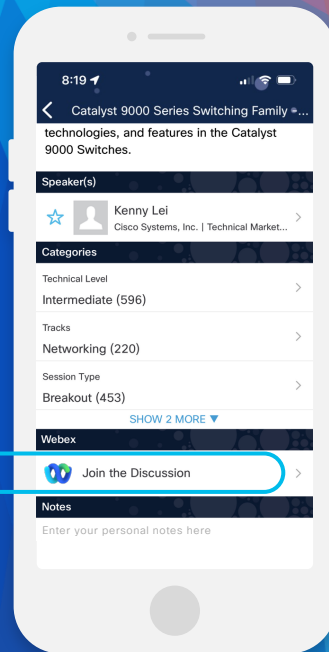
Questions?

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 December 22, 2023.



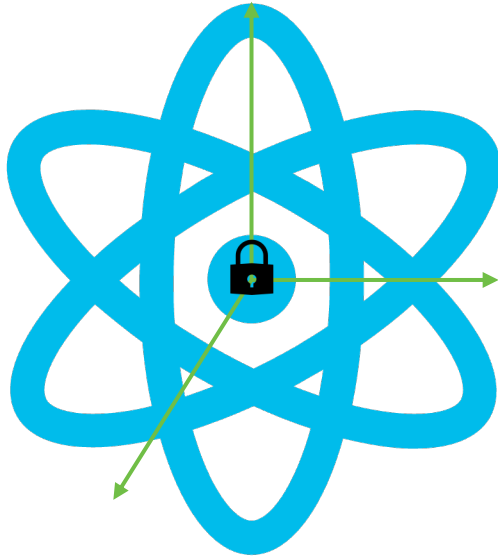
<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2067>

New Things to talk about

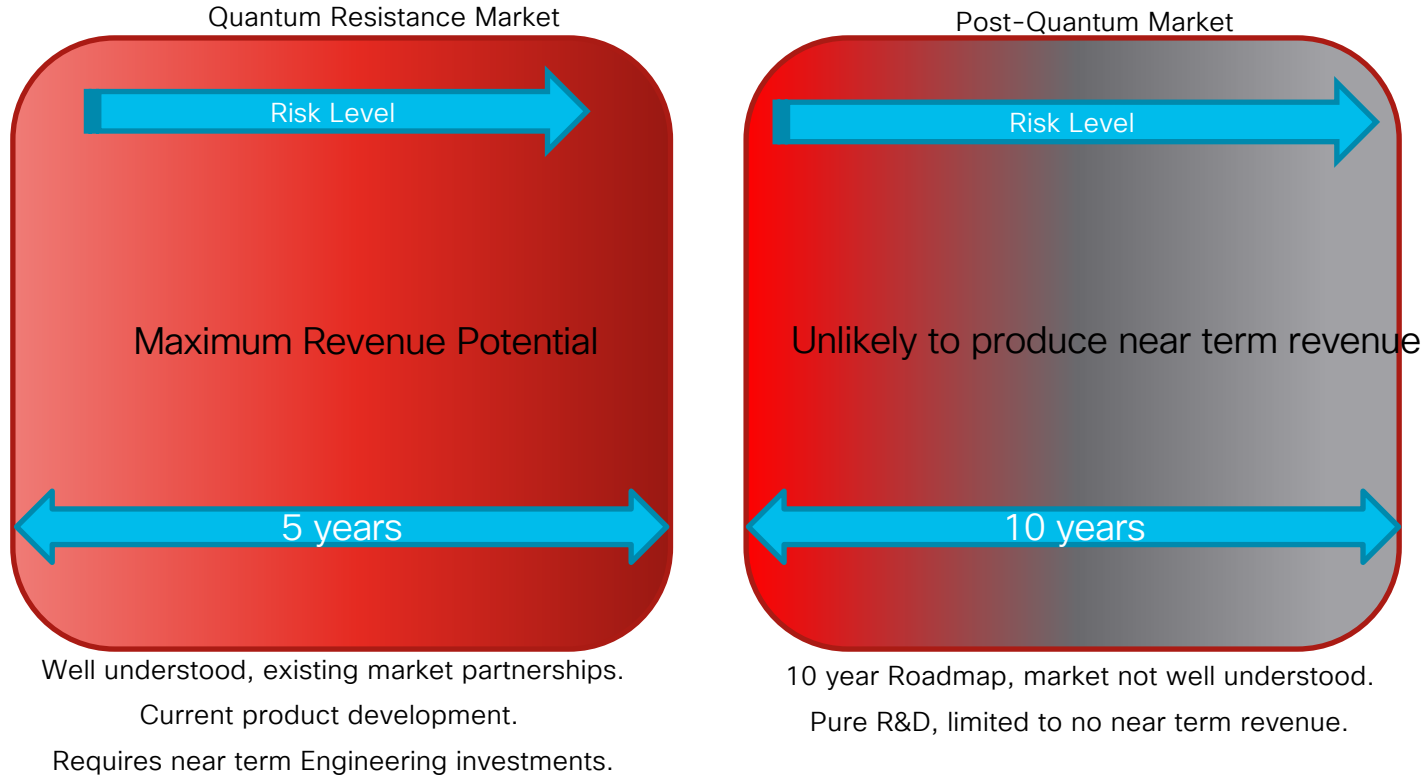
Quantum Resistance and Post Quantum

Quantum Resistance and Post-Quantum Plan

A Roadmap for Cisco Innovation



Quantum Crypto Market



Post Quantum Direction

US Government (NIST) urges maximum flexibility and caution relative to post-quantum. Changes are likely.

Danger to Cisco is the distraction of PQ – could easily hurt current solution directions for Quantum Resistance

10 years away from broad implementations, certifications and substantial customer deliveries

NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION PLAN

JULY 2023

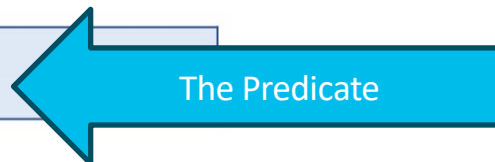




Strategic Objective 4.3: Prepare for Our Post-Quantum Future

Initiative Number: 4.3.1

Initiative Title: Implement National Security Memorandum-10



Initiative Description

The Office of Management and Budget and the National Manager for National Security Systems, in coordination with ONCD, will continue to prioritize implementation of National Security Memorandum-10 and transitioning vulnerable public networks and systems to quantum-resistant cryptography-based environments, focusing first on Federal information systems and NSS. OMB will work with NIST to develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

NCS Reference

The Federal Government will prioritize the transition of vulnerable public networks and systems to quantum-resistant cryptography-based environments and develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

Responsible Agency: OMB

Contributing Entities: NSA, ONCD

Completion Date: 1Q FY25



Initiative Number: 4.3.2

Initiative Title: Implement NSM-10 for National Security Systems (NSS)

Initiative Description

Implement the transition of NSS to quantum-resistant cryptography.

NCS Reference

The Federal Government will prioritize the transition of vulnerable public networks and systems to quantum-resistant cryptography (QRC)-based environments and develop complementary mitigation strategies to provide cryptographic agility in the face of unknown future risks.

Responsible Agency: NSA

Contributing Entities: DOD, ODNI

Completion Date: 3Q FY25

Initiative Number: 4.3.3

Initiative Title: Standardize, and support transition to, post-quantum cryptographic algorithms

Initiative Description

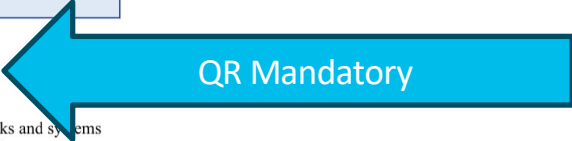
The National Institute of Standards and Technology will finalize its process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms. New public-key cryptography standards will specify one or more additional unclassified, publicly-disclosed digital signature, public-key encryption, and key-establishment algorithms that are available worldwide, and are capable of protecting sensitive government information well into the foreseeable future, including after the advent of quantum computers.

NCS Reference

To balance the promotion and advancement of quantum computing against threats posted to digital systems, National Security Memorandum (NSM) 10, "Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," establishes responsibilities and oversight to enable a timely transition of the country's cryptographic systems to interoperable quantum-resistant cryptography.

Responsible Agency: NIST

Completion Date: 1Q FY25



QR Mandatory

Detailed Recommendations

Forward Investment IOS-XE

- Enterprise Networking Investments

IOS-XE Development

- Rotational Key Management
- Robust Quantum Key Delivery with external HSM integration
- Initial option for PQ-SSH (pq-tls) cipher integration
- Uses CiscoSSH as the basis for implementation
- CiscoTLS work already underway

Forward Investment ASA

- SBG Investments

ASA Development

- SKIP Implementation
- Rotational Key Management
- Robust Quantum Key Delivery with external HSM integration
- Initial option for PQ-SSH (pq-tls) cipher integration
- Uses CiscoSSH as the basis for implementation
- CiscoTLS work already underway

Forward Investment FTD/FMC

- SBG Investments

FTD/FMC Development

- SKIP Implementation
- Rotational Key Management
- Robust Quantum Key Delivery with external HSM integration
- FMC must fully instrument all Lina QR work
- Uses CiscoSSH as the basis for implementation
- CiscoTLS work already underway

Forward Investment AnyConnect (Secure Client)

- SBG Investments

Secure Client Development

- SKIP Implementation

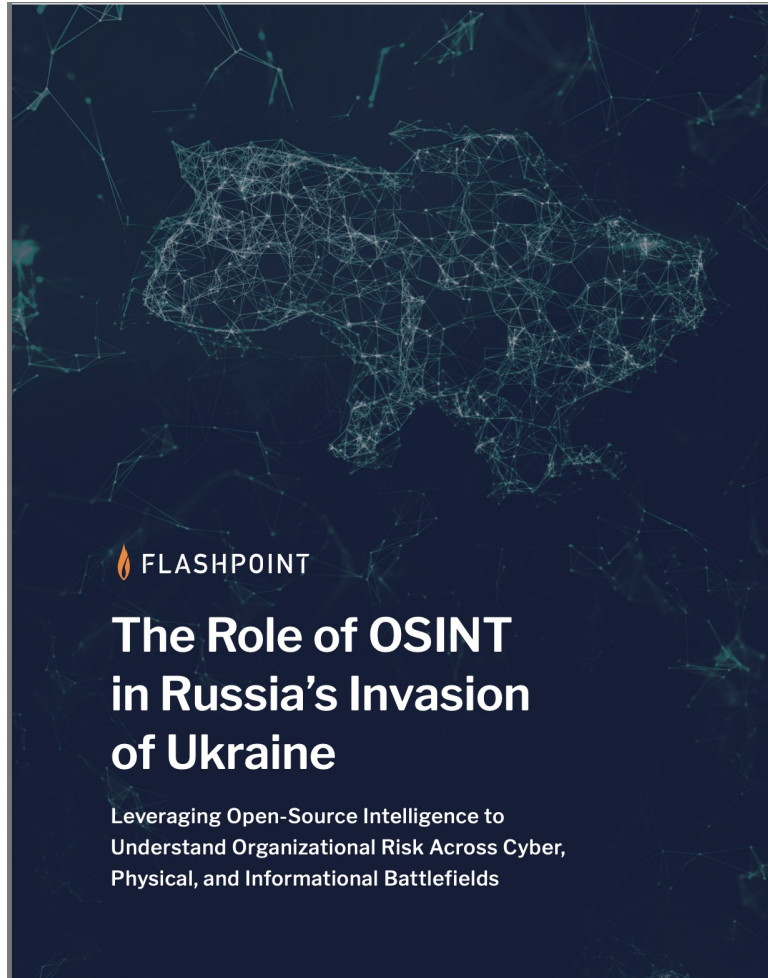
- Rotational Key Management

- Robust Quantum Key Delivery
with external HSM integration

- Must integrate with ASA and FTD
for IPSec Termination

- Should invest in PQ-TLS based
tunneling

The Rise of Open Source Intelligence



https://flashpoint.io/wp-content/uploads/Flashpoint_RUS-UK_2023-FINAL.pdf



Messages People (588) Content Meetings + Apps



1/3/23, 5:20 PM

Prigozhyn saying that every house is a new line of defense in Bakhmut and the wagnerites stating that they are lacking vehicles and ammunition to push forward

<https://twitter.com/CartesDuMonde/status/1610301906416553984?s=20&t=5sBzQhyNVpqJTpF3xr0U5Q>

1/3/23, 5:34 PM

Partisans in RU have apparently been busy over the new year holiday and have sabotaged multiple control boxes for RU railways, slowing down troop and equipment movements

<https://twitter.com/intermarium24/status/1610297992128655360?s=20&t=5sBzQhyNVpqJTpF3xr0U5Q>

1/3/23, 5:40 PM

Germany has stopped the flow of RU oil through the Druzhba pipeline as of 1 Jan, Kazakhstan is now in discussions with RU to send Kazakh oil through the pipeline instead

<https://twitter.com/ReportWar1/status/1610298919136673796?s=20&t=5sBzQhyNVpqJTpF3xr0U5Q>

1/3/23, 5:45 PM

RU troops trained for artillery for 3 months, get to the front just to be told their going to be used as infantry

<https://twitter.com/wartranslated/status/1610296498155028480?s=20&t=5sBzQhyNVpqJTpF3xr0U5Q>



1/3/23, 8:49 PM

Report that 40 IT specialists from the RU MoD were taken out, which could have long lasting effects on MoD operations

<https://twitter.com/igorsushko/status/1610332305641574401?s=20&t=5sBzQhyNVpqJTpF3xr0U5Q>



1/3/23, 9:25 PM

Retired 3-star general Ben Hodges giving good insight into where the war is going

<https://twitter.com/igorsushko/status/1610173194077630464?s=20&t=5sBzQhyNVpqJTpF3xr0U5Q>



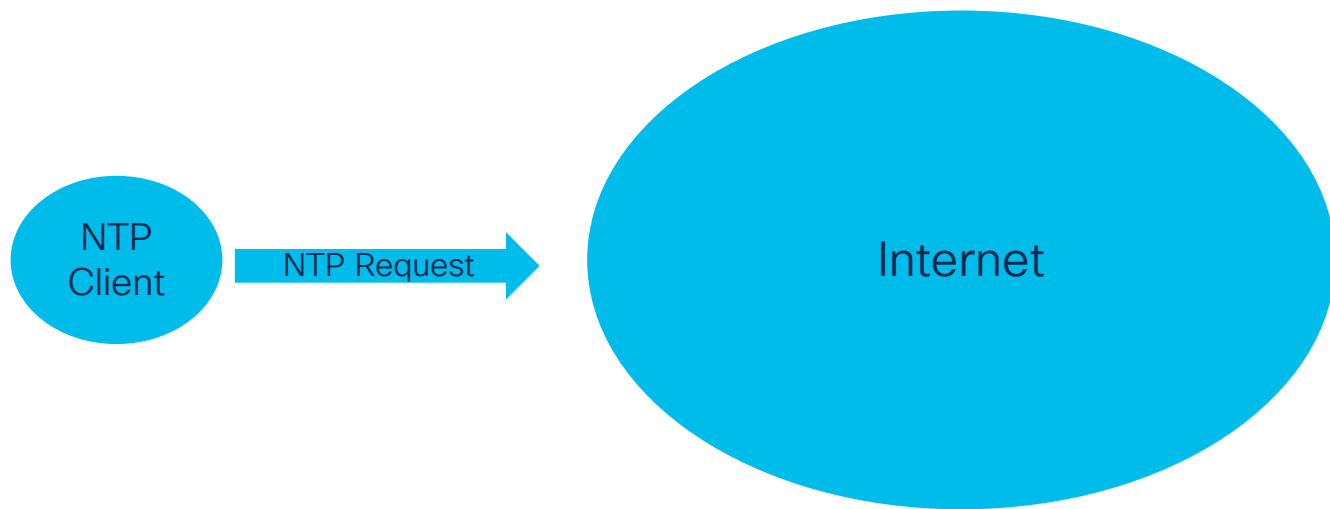
Tactics, Techniques and Procedures

Current Trends and TTPs

- New TTPs – massive increase in scanning occurring on US networks
- C2 networks running out of Russia, Belarus to Vietnam, Ukraine and to the US
- Looking at Federal Government related networks
- Reconnaissance taking place, probing
- Deny_All is of course super effective
- Event Load so high had to disable outside Interface of sensors
- Rolled our FMCs, had to move to 9XL Instances in Amazon to keep up

Some New Observed TTPs

- Service Request Networks are a real target
 - Network Time Protocol Pools are observed targets



Subject Port/Protocol	Subject Host Groups	Subject Location	Subject Bytes	Subject Byte Rate	Subject Interfaces	Application	To
123/UDP	Russian Federation	Russian Federation	768	6.45	192.133.161.242(ifIndex-3), 192.133.161.242(ifIndex-1)	NTP (unclassified)	
123/UDP	Russian Federation	Russian Federation	768	18.73	192.133.161.242(ifIndex-3), 192.133.161.242(ifIndex-1)	NTP (unclassified)	
123/UDP	Russian Federation	Russian Federation	576	4	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	NTP (unclassified)	
123/UDP	Russian Federation	Russian Federation	480	3.33	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	NTP (unclassified)	
123/UDP	Russian Federation	Russian Federation	384	2.61	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	NTP (unclassified)	
123/UDP	Russian Federation	Russian Federation	384	8.53	192.133.161.242(ifIndex-3), 192.133.161.242(ifIndex-1)	NTP (unclassified)	
123/UDP	Russian Federation	Russian Federation	384	4.99	192.133.161.242(ifIndex-3), 192.133.161.242(ifIndex-1)	NTP (unclassified)	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	280	70	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	
123/UDP	Russian Federation	Russian Federation	144	1	192.133.161.242(ifIndex-3), 192.133.161.242(ifIndex-1)	NTP (unclassified)	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	224	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	74.67	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	224	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	74.67	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	224	192.133.161.242(ifIndex-3), 192.133.161.242(ifIndex-1)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	224	192.133.161.242(ifIndex-3), 192.133.161.242(ifIndex-1)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Ukraine	224	224	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	224	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	224	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	224	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	224	192.133.161.242(ifIndex-3), 192.133.161.242(ifIndex-1)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	74.67	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	224	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	
ICMP	Russian Federation, Trusted Internet Hosts	Russian Federation	224	74.67	192.133.161.242(ifIndex-1), 192.133.161.242(ifIndex-3)	ICMP	

Interesting Denial Concept

1. If I constantly overwhelm with security events
2. And shorten the practical window of FIFO collection
3. Effectively shortening the observation windows and effective collection
4. I can real dollar cost expense out a large portion of observation outside of possibly the Federal Government
5. Make observation so expensive, people lose interest in Monitoring
6. This is the kind of behavior we're seeing, adaptive Recon with overwhelming amounts of attack traffic
7. Can I cost out the monitoring?

Overt Ops



Chat about current Ops

CHAT TIME

Critical Network Defenses

Critical Network Defenses

Detailed Egress
ACLs

Granular Ingress
ACLs

Map out Cloud
access points

Establish Cloud
Only Access with
no CSP Pivot
Points

Employ CSP tools
such as AWS
GuardDuty

Process VPC
Flow Logs, know
your CSP traffic
patterns

Critical Protocols to Block

IPv6 – if you are not prepared, deny_all

- [IP in IP](#) (Protocol 4): IP in IPv4/IPv6 (requires a smart firewall)
- SIT/IPv6 (Protocol 41): IPv6 in IPv4/IPv6
- [GRE](#) (Protocol 47): Generic Routing Encapsulation
- [OpenVPN](#) (UDP port 1194): Openvpn
- [SSTP](#) (TCP port 443): Secure Socket Tunneling Protocol (requires a proxy)
- [IPSec](#) (Protocol 50 and 51): Internet Protocol Security
- [L2TP](#) (Protocol 115): Layer 2 Tunneling Protocol
- PPTP (TCP Port 1723): RFC 2637
- [VXLAN](#) (UDP port 4789): Virtual Extensible Local Area Network
- LISP udp port 4341 encapsulated user data
- LISP udp port 4342 control plane packets
- OTV: tcp/udp 8472 (per the RFC, but practically is IP/47)

Why Block them?

Because no DPI solutions inspect them

They *may be natively dropped (maybe not)

Most likely they are explicitly forwarded

Minimally establish monitor rules for these protocols

Airgapping the Attack Surface

Do you need to be connected to
the Internet 100% of the time?

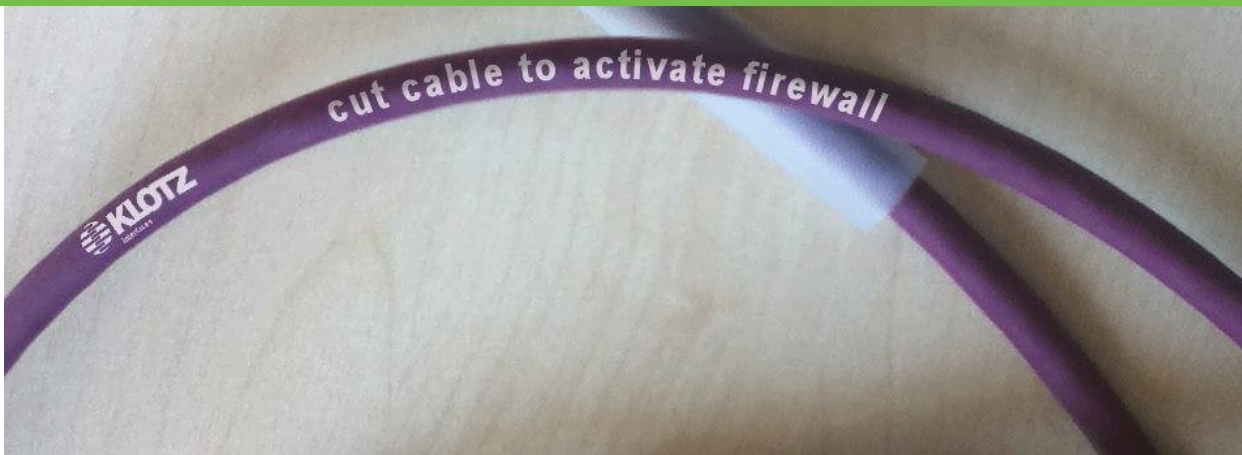
What would you do if you had to
immediately disconnect from the
Internet?

Can you disconnect all of your
networks from the Internet in less
than 5 minutes?

If it took you 60 minutes to find
“the guy” to disconnect your networks, how
much damage would have occurred?

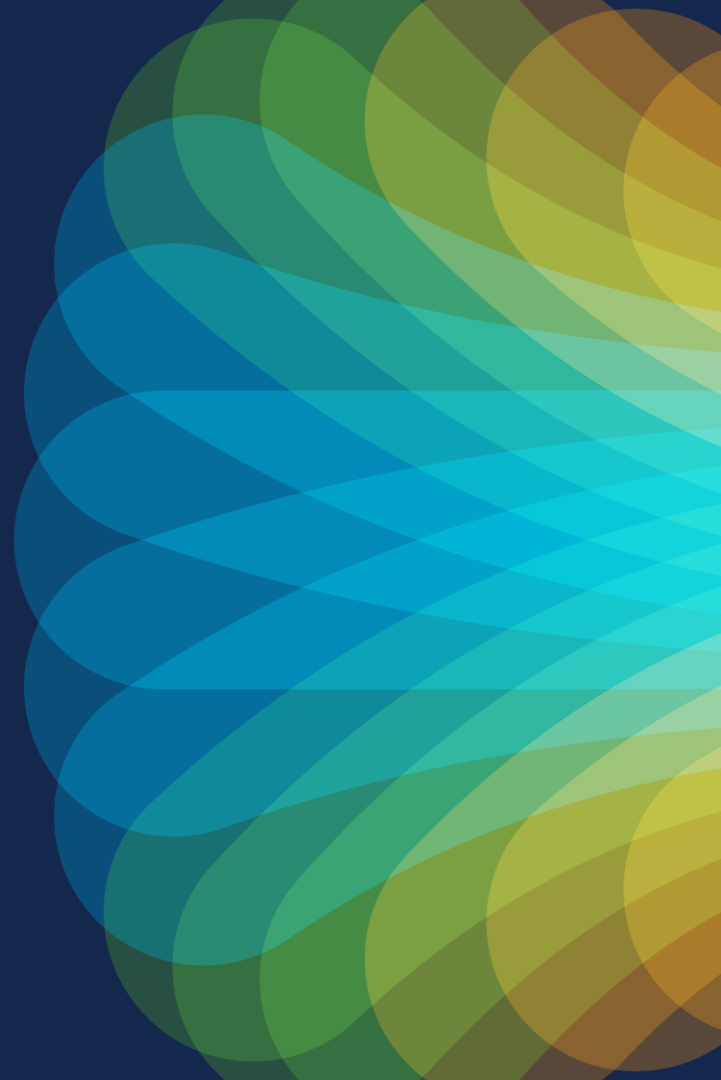


Is this really the practical option?



Scenario #1

Security Emergency

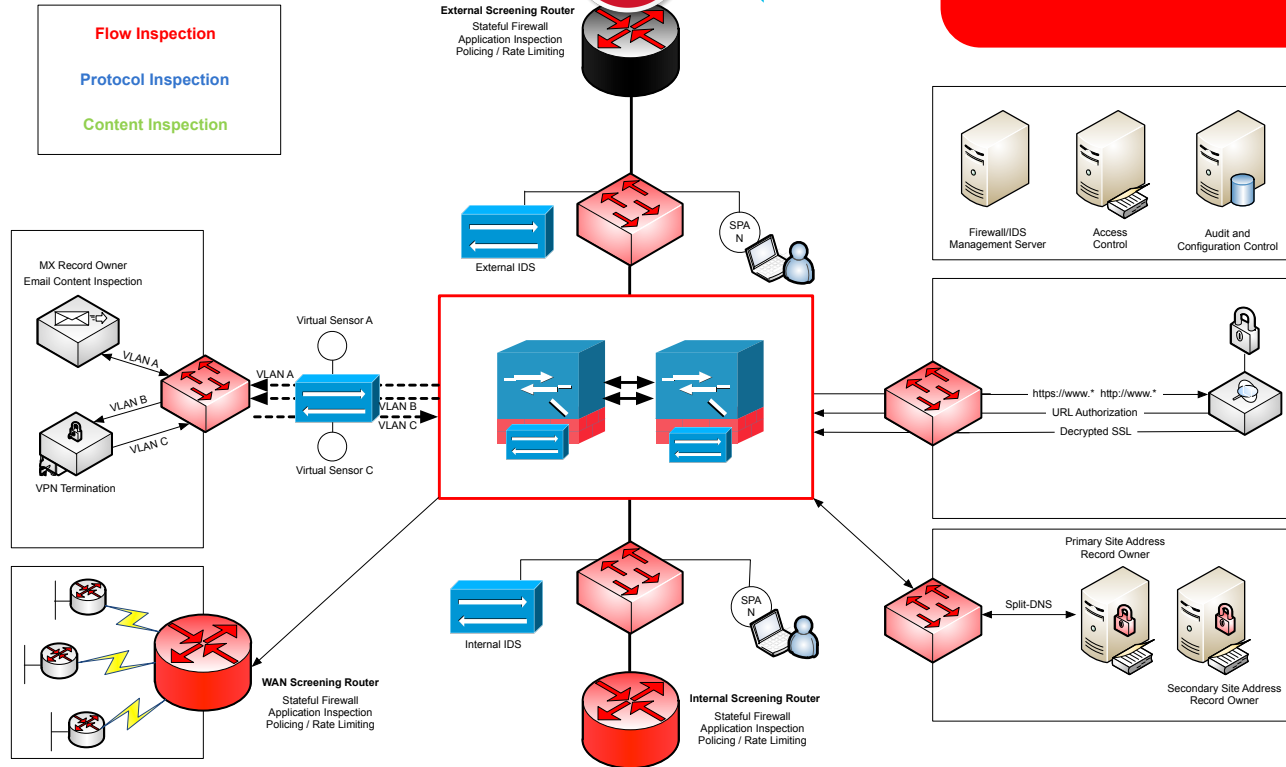


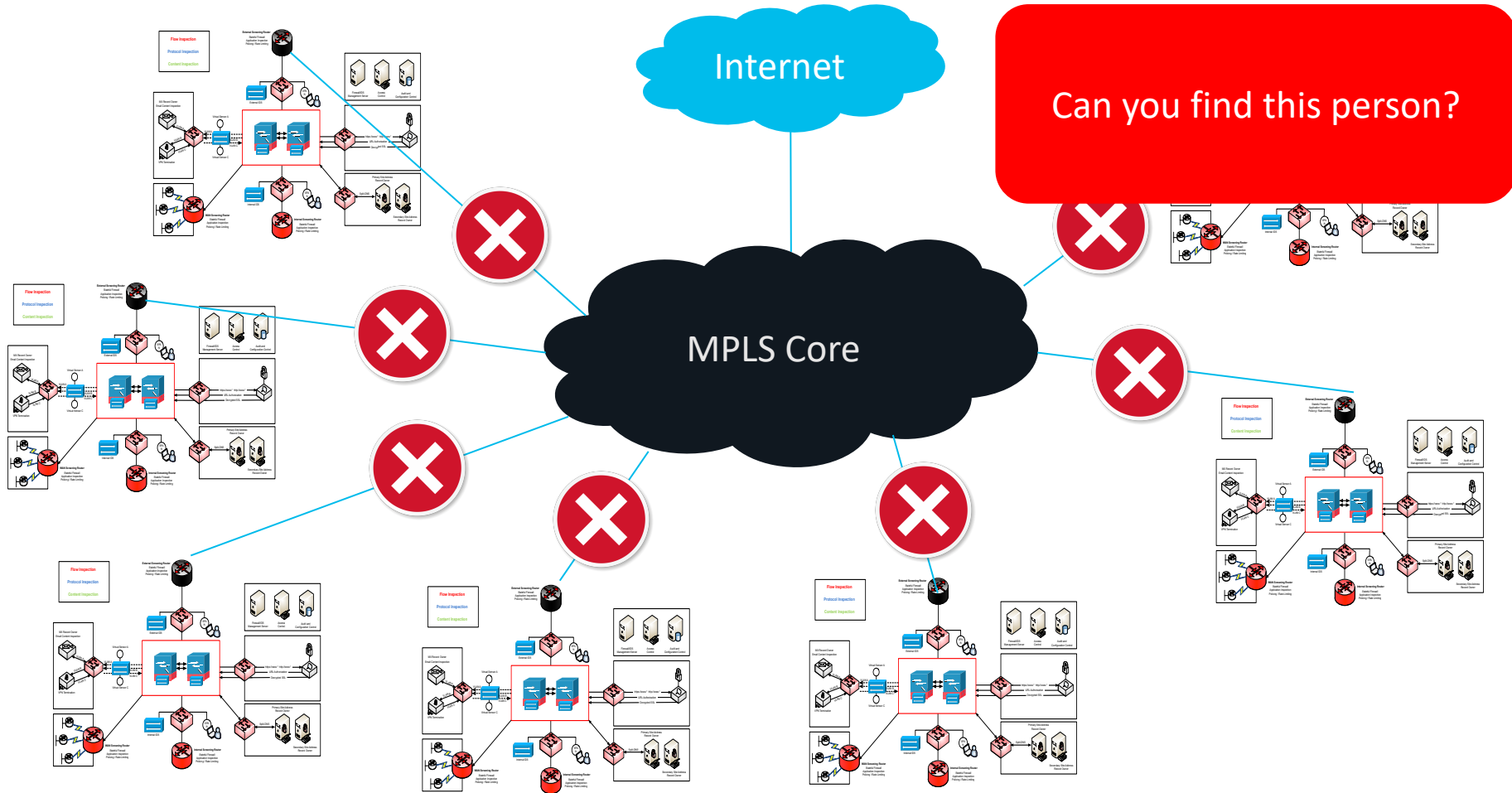
Security Emergency

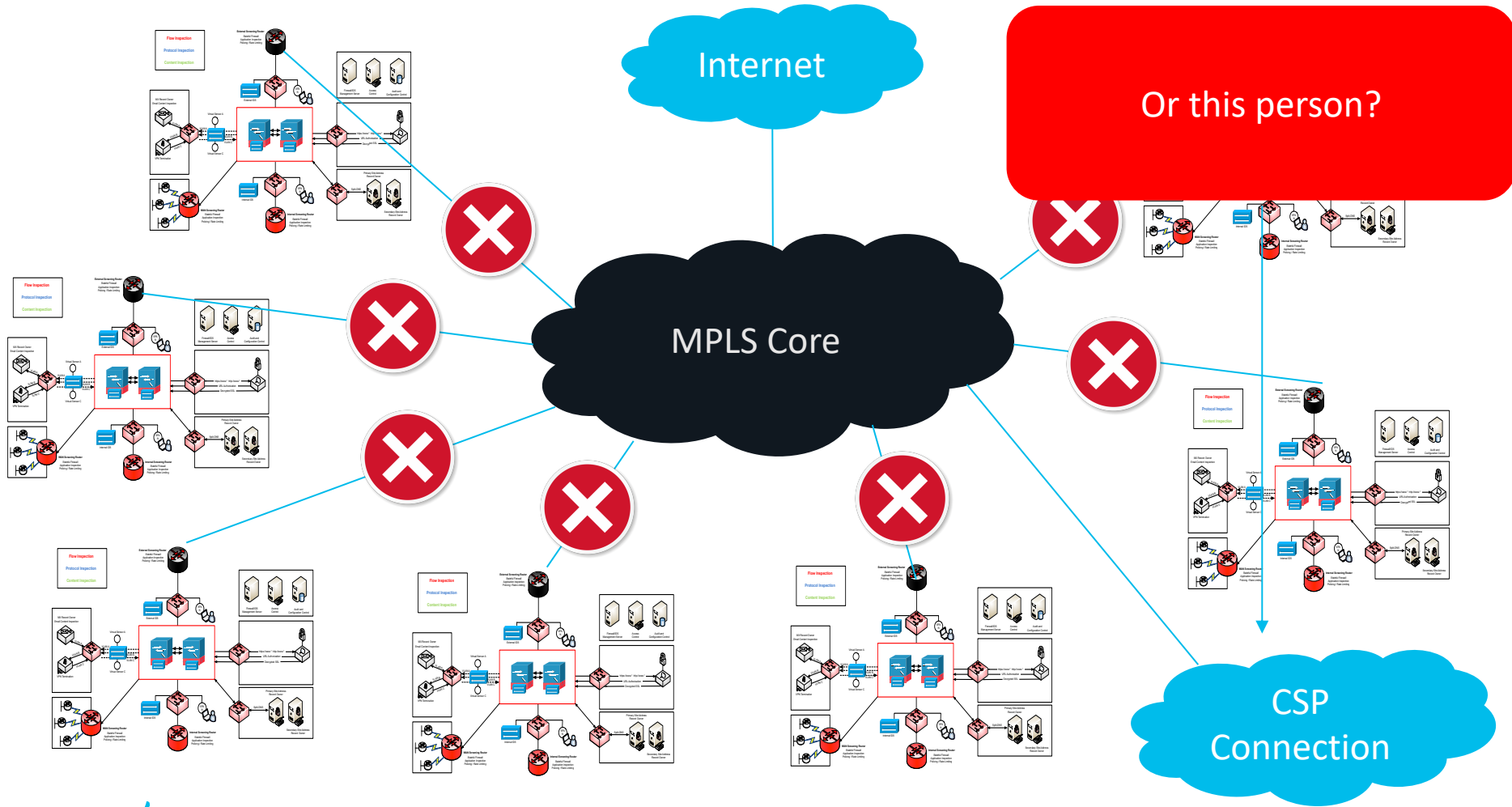
- Large volumes of data being actively exfiltrated from network
- Containment measures unsuccessful
- 70 minutes have passed since flow detection has occurred
- Must stop data exfiltration at all costs, immediately

Internet

You can probably find the person to disconnect this....

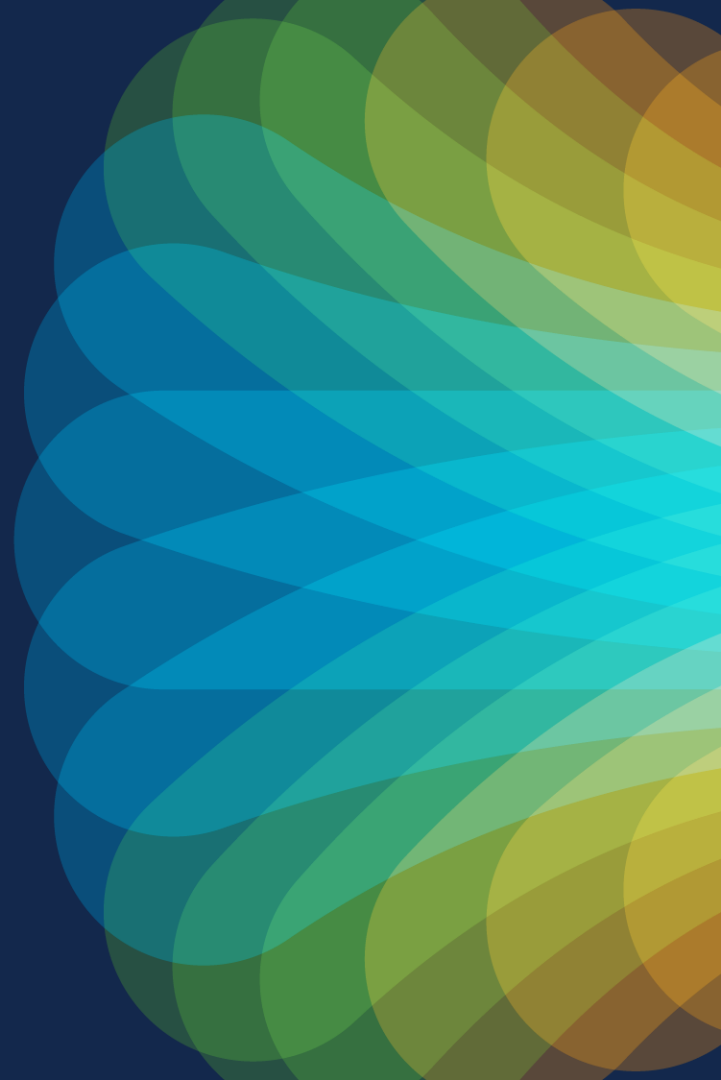






Scenario #2

Asset Based Risk Reduction



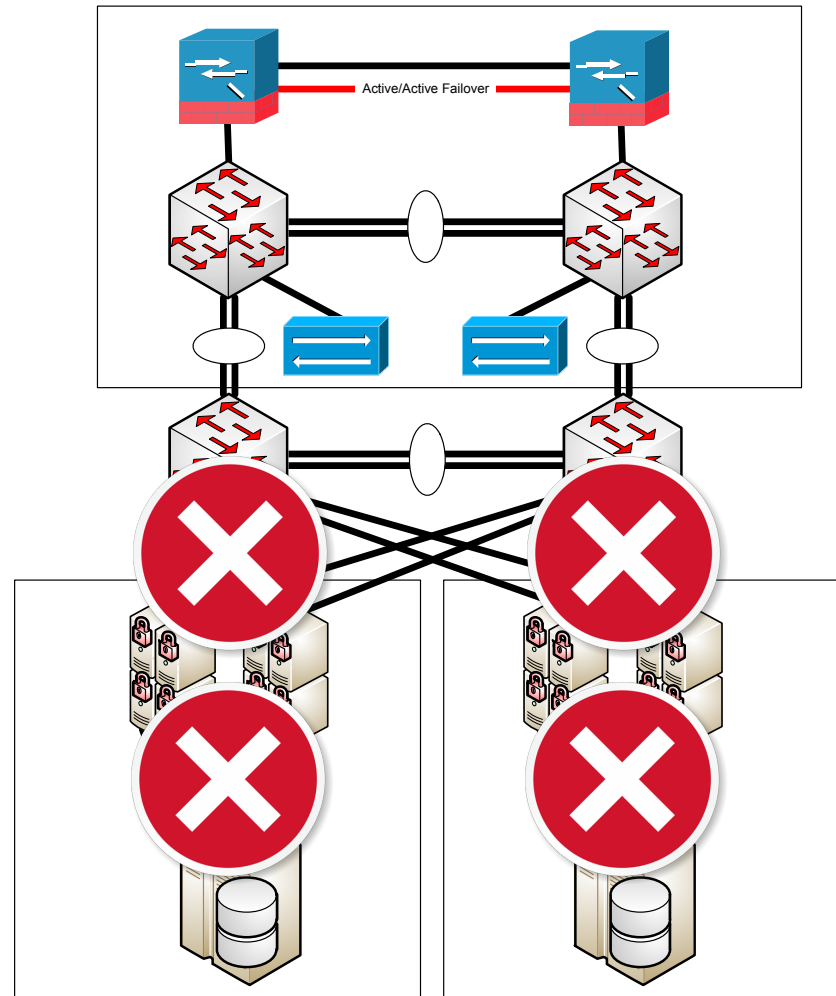
Asset Based Threat Risk Reduction

- Breach containment is failing
- Clear signs that database access is the goal
- Brute force failed login attempts from lateral assets
- Decision is made to disconnect primary databases

Critical Systems Disconnect

- Understanding that database operations are generally the target of any successful cyber heist, a planned disconnect for database operations could yield significant attack surface reduction during scheduled periods
- **This is not an INTERNET disconnect use case, it is a critical systems disconnect only**
- Strategically placed disconnect appliances could be employed within the network to offer a critical protect function, while maintaining a primary internet connection which may be needed for triage, assistance and remote access

Lateral
Server Risk
Reduction

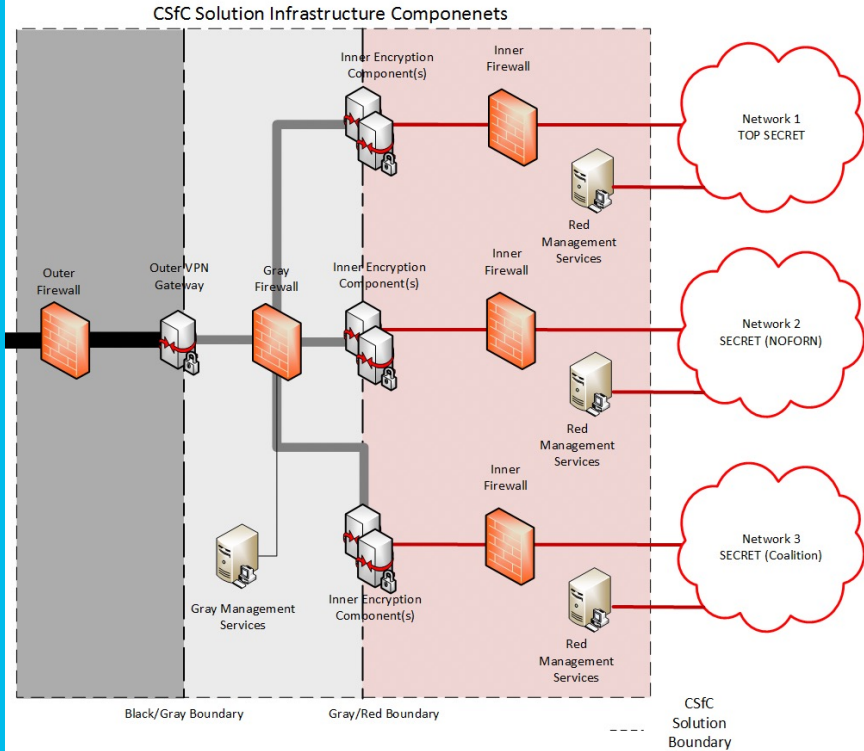


Emergency
Database
Protection

Government Cross Domain Use Case



AUTOMATED AIRGAP



Hardware based Airgap

Drawbridge –physical disconnect

- Physical Relay Ports
- Cellular or Local Admin controlled
- No IP on the physical interfaces
- Allows for Executive Disconnect Option
- Can be scheduled for relay closed operations base



Physical Relay based Disconnect



Signed in As
Admin

- Dashboard
- Ports
- Users
- Logs
- Settings
- Sign Out

Ports

Disable All

Port	Name	Availability	Status	Control
01	Port 1 CCTV	2 users have access	Disabled	
02	Port 2 Crown Jewels	2 users have access	Disabled	
03	Port 3 New York WAN Router	1 user has access	Disabled	
04	Port 4 File Server 1	1 user has access	Disabled	
05	Port 5 Building Management System	1 user has access	Disabled	
06	Port 6 Security Control Centre	1 user has access	Disabled	

Highly Secured Airgapping

Highly Secured Airgap Management



SMS

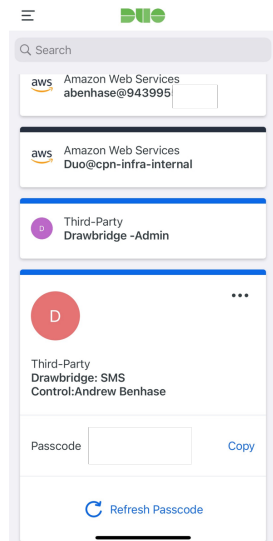
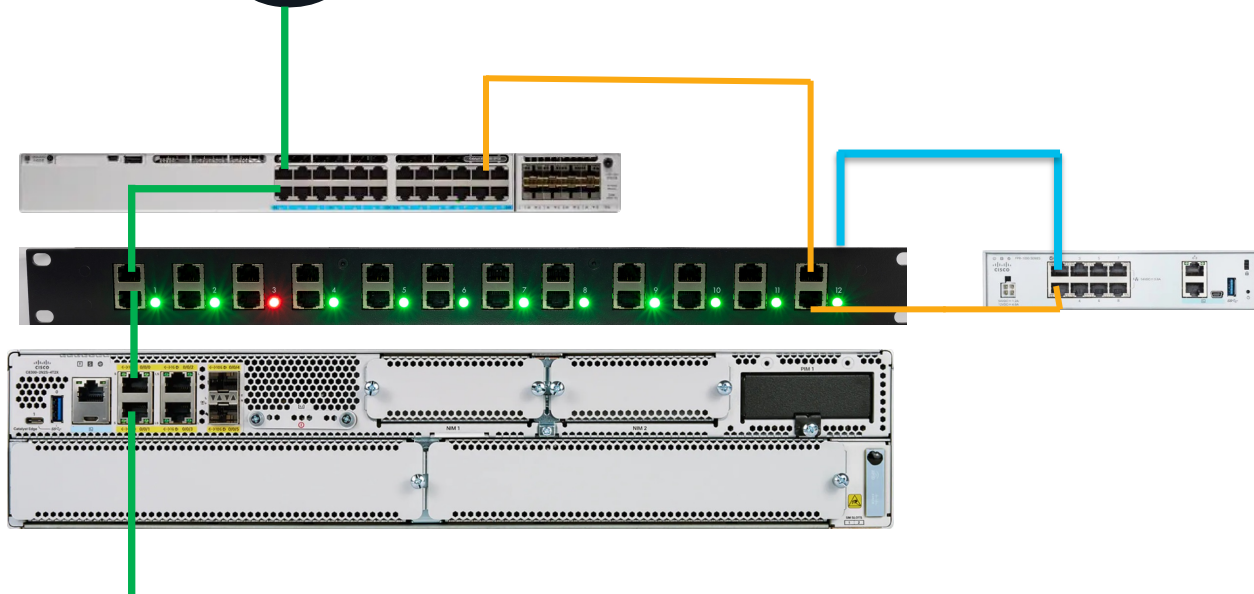
Disable Port 1

Enable Port 12

Enterprise Network



Highly Secured Airgap Management



Enterprise Network

Scenario Details

1 Cell/OTP pair is for MGMT port access enablement only

Enables MGMT port to FPR1010

Establishes AnyConnect VPN to FPR1010

Logs into WebUI with OTP

Disable Internet Access on Port 1-10

Automatic schedule resets MGMT port to closed on each hour



Signed in as
admin

- Dashboard
- Ports
- SMS Control
- Schedules
- Logs
- Settings
- Log Out

Schedules

[+ New Scheduled Event](#)

Recurring Events

One-Time Events

Name	State	Ports	Day & Time
Disable MGMT 0000	Disable	12	Every day at 12:00:00 AM
Disable MGMT 0100	Disable	12	Every day at 1:00:00 AM
Disable MGMT 0200	Disable	12	Every day at 2:00:00 AM
Disable MGMT 0300	Disable	12	Every day at 3:00:00 AM
Disable MGMT 0400	Disable	12	Every day at 4:00:00 AM
Disable MGMT 0500	Disable	12	Every day at 5:00:00 AM
Disable MGMT 0600	Disable	12	Every day at 6:00:00 AM

Security Details

- Inbound number is whitelisted
- Duo/Google/MFA Client is linked to a specific user
- All other inbound SMS messages are ignored
- Inbound number is only provided access to certain ports
- 321-555-1212 is allowed access to Port 12 only
- 321-555-2222 is allowed access to enable Port 1 only

>>Hey, I can do all of this with
software/scripts....<<

- `sudo /kill/disconnect.pl`
- `sudo /kill/db_disconnect_all.pl`

Secured DNS

Secured DNS Slides

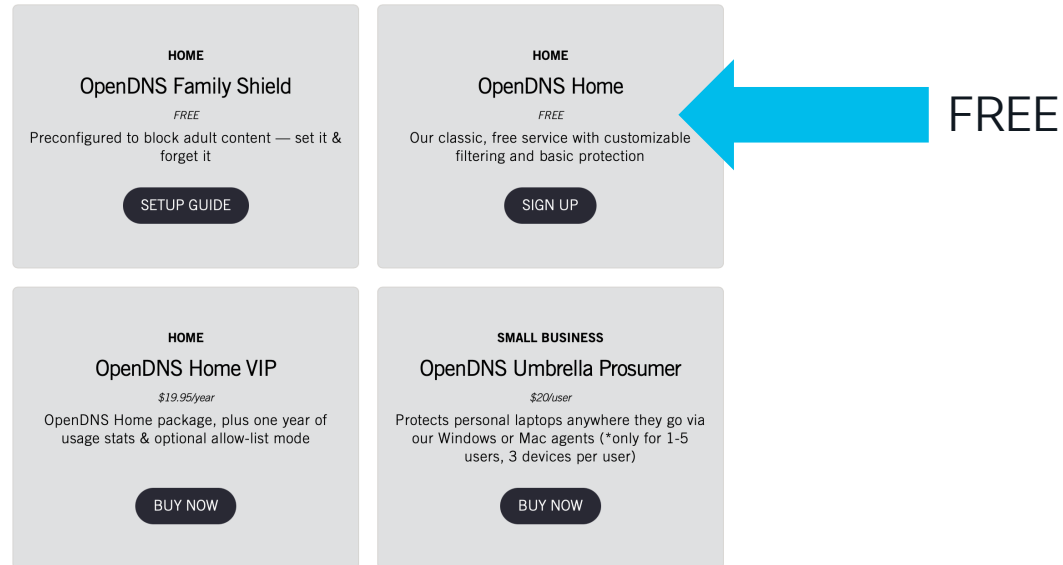
Block Outbound DNS to known DNS providers

Use Security Policy as DNS Overlay

Use Encrypted DNS Requests

Be sure to include IPv6 DNS Destinations

I'm not saying use OpenDNS, but use OpenDNS or Commercial Umbrella or some Secured DNS provider



The image shows a grid of four OpenDNS service plans. A large blue arrow points from the right towards the 'OpenDNS Home' plan, which is labeled 'FREE' in large blue text. The plans are as follows:

Category	Plan Name	Price	Description	Action
HOME	OpenDNS Family Shield	FREE	Preconfigured to block adult content — set it & forget it	SETUP GUIDE
HOME	OpenDNS Home	FREE	Our classic, free service with customizable filtering and basic protection	SIGN UP
HOME	OpenDNS Home VIP	\$19.95/year	OpenDNS Home package, plus one year of usage stats & optional allow-list mode	BUY NOW
SMALL BUSINESS	OpenDNS Umbrella Prosumer	\$20/user	Protects personal laptops anywhere they go via our Windows or Mac agents (*only for 1-5 users, 3 devices per user)	BUY NOW

HYDRACRYPT



HYD

All Your files and d
ID :

Encryption was made with
There **NO CHANCE** to d
software and your unique

To buy your software You need to contact us by EMAIL:
1) XHELPER@DR.COM
or
2) AHELPER@DR.COM
Your email text should contain your unique ID number and o

We will decrypt one of your file for FREE! It's your guarant
Remember! Your time has a limit: 72 hour.
If You will not send any email We will turn on a sanctions:
1) Your software's price will be higher
2) Your unique private key will be destroyed (After that your
3) Your private info, files, documents will be sold on the Darl

Attention: all your attempts to decrypt your PC without our s

**ONLY YOU CAN
PREVENT RANSOMWARE**



personal files are encrypted by CTB-Locker.



personal files are encrypted by CTB-Locker.

ts, photos, databases and other important files have been encrypted with strongest
d unique key, generated for this computer.

ption key is stored on a secret Internet server and nobody can decrypt your files
and obtain the private key.

96 hours to submit the payment. If you do not send money within provided time, all
be permanently crypted and no one will be able to recover them.

to view the list of files that have been encrypted.

or the next page.

**WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION
TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE
YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE
INSTRUCTION.**

View 95 59 22 Next >>

Secured Time

In any conflict, time is a critical asset

In cyber secops, trusted time is the single most
important asset

Why is Time so important?



Correlation of security events



Forensic replay - Investigations

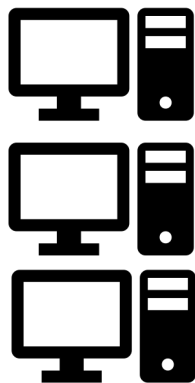


Sequence of packet times



All Simulations require synchronized time

Secured NTP Slides



Give me Time!

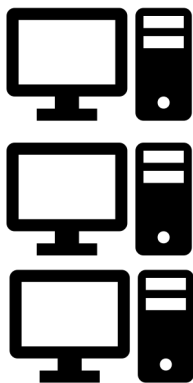


NTP
Pool
1

NTP
Pool
2

NTP
Pool
3

Secured NTP Slides



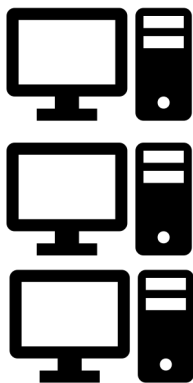
Give me Time!



List of Source IP addresses
requesting time:

```
{ "ipvAPrefix": "157.55.39.0/24" },  
{ "ipv4Prefix": "207.46.13.0/24" },  
f"ipv4Prefix": "40.77.167.0/24"3,  
{ "ipv4Prefix": "13.66.139.0/24" },  
f"ipv4Prefix": "13.66.144.0/24"3,  
{ "ipvaPrefix": "52.167.144.0/24" },  
f"ipv4Prefix": "13.67.10.16/28"3,  
{ "ipv4Prefix": "13.69.66.240/28" },  
{ "ipv4Prefix": "13.71.172.224/28"3,  
{ "ipv4Prefix": "139.217.52.0/28" },  
{ "ipv4Prefix": "191.233.204.224/28" },  
{ "ipv4Prefix": "20.36.108.32/28" },  
f"ipv4Prefix": "20.43.120.16/28"3,  
{ "ipv4Prefix": "40.79.131.208/28" },  
{ "ipv4Prefix": "40.79.186.176/28" },  
{ "ipv4Prefix": "52.231.148.0/28" },  
{ "ipv4Prefix": "51.8.235.176/28" },  
{ "ipv4Prefix": "51.105.67.0/28" }
```

Secured NTP Slides



Thanks for adding to
my list of known host
addresses

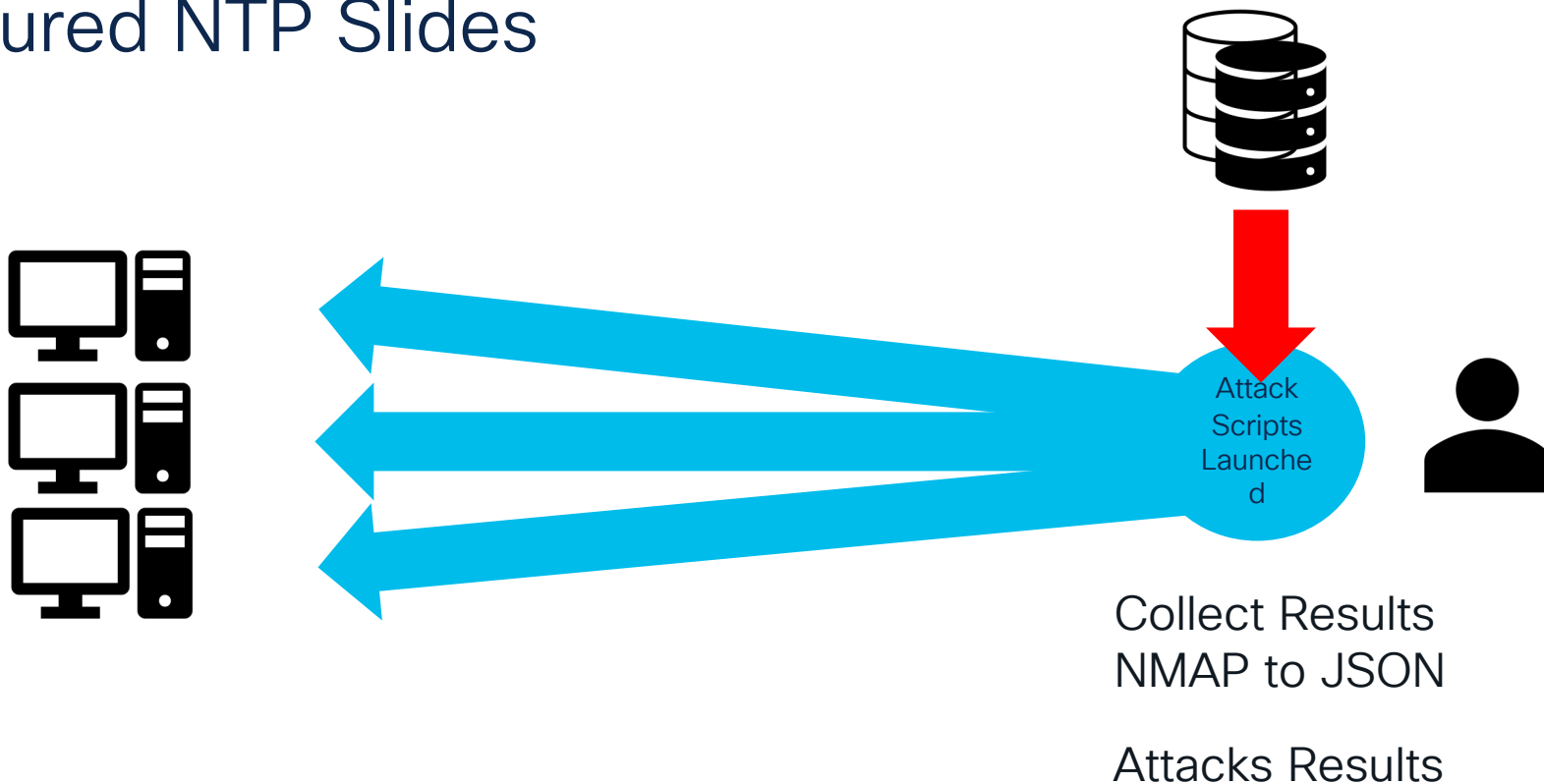
List of Source IP addresses
requesting time:

```
{ "ipvAPrefix": "157.55.39.0/24" },  
{ "ipv4Prefix": "207.46.13.0/24" },  
f"ipv4Prefix": "40.77.167.0/24"3,  
{ "ipv4Prefix": "13.66.139.0/24" },  
f"ipv4Prefix": "13.66.144.0/24"3,  
{ "ipvaPrefix": "52.167.144.0/24" },  
f"ipv4Prefix": "13.67.10.16/28"3,  
{ "ipv4Prefix": "13.69.66.240/28" },  
{ "ipv4Prefix": "13.71.172.224/28"3,  
{ "ipv4Prefix": "139.217.52.0/28" },  
{ "ipv4Prefix": "191.233.204.224/28" },  
{ "ipv4Prefix": "20.36.108.32/28" },  
f"ipv4Prefix": "20.43.120.16/28"3,  
{ "ipv4Prefix": "40.79.131.208/28" },  
{ "ipv4Prefix": "40.79.186.176/28" },  
{ "ipv4Prefix": "52.231.148.0/28" },  
{ "ipv4Prefix": "51.8.235.176/28" },  
{ "ipv4Prefix": "51.105.67.0/28" }
```

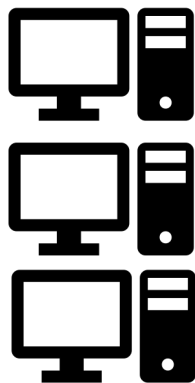
CISCO *Live!*



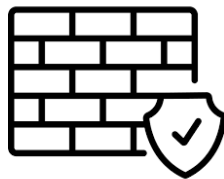
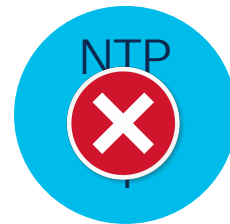
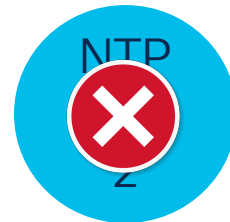
Secured NTP Slides



Secured NTP – What you should do



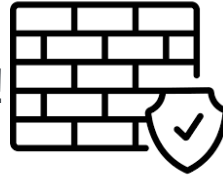
Give me Time!



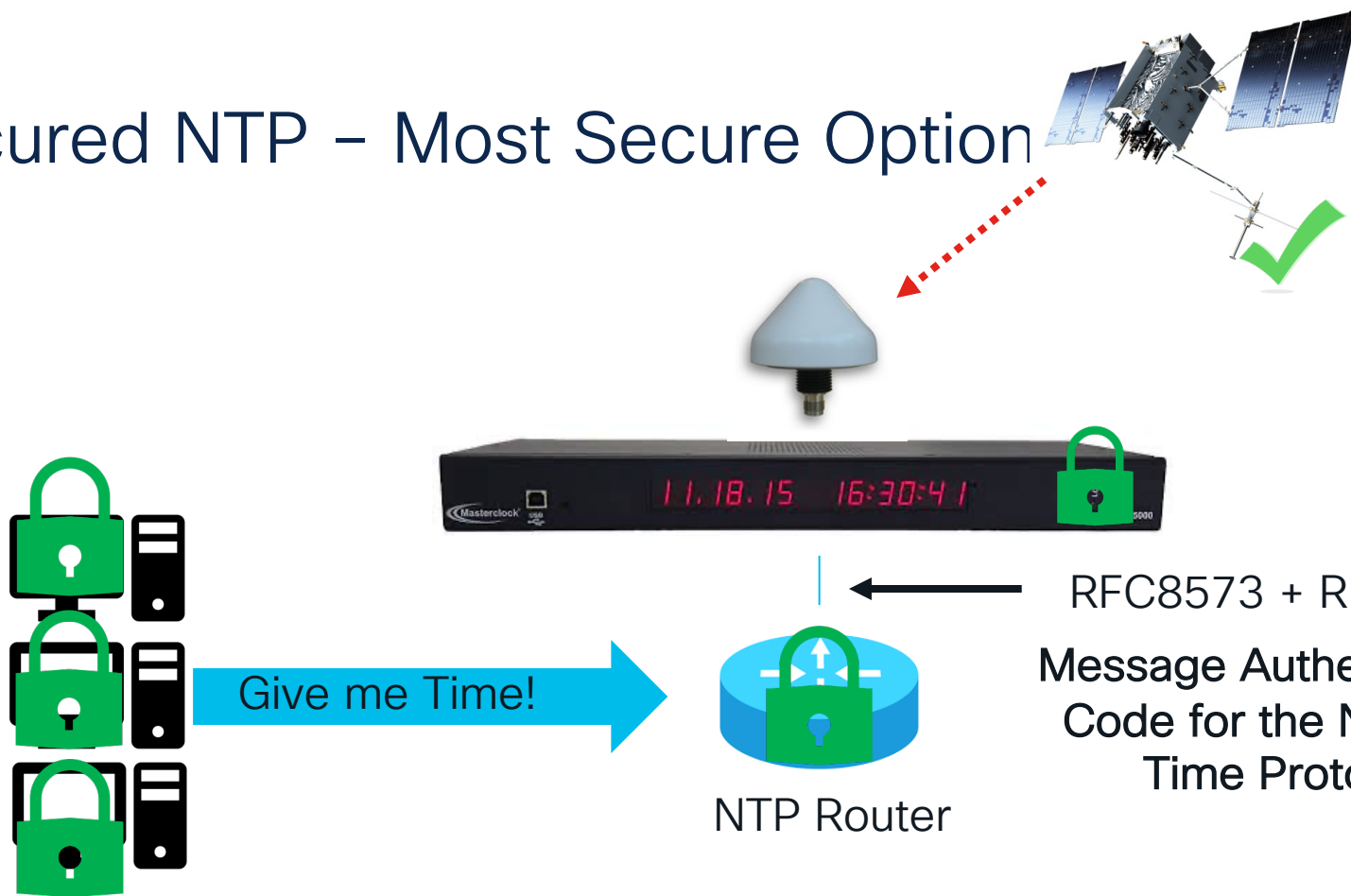
Secured NTP – What you should do



Give me Time!



Secured NTP – Most Secure Option



RFC 4493, RFC 8573, RFC 5905

- RFC 5905 – defines NTPv4

<https://www.rfc-editor.org/rfc/rfc5905>

- RFC 4493 – defines AES-CMAC (128 bit)

<https://www.rfc-editor.org/rfc/rfc4493>



- RFC 8573 – defines AES-CMAC in place of MD5 for NTPv4

<https://www.rfc-editor.org/rfc/rfc8573>



If you need to run Certified Firewalls

Cert/Project	FIPS	CC	DoDIN APL	USGv6	
ASA 9.16.x + ISA 3000	Waiting on entropy	Posted to NIAP!!!	Waiting for FIPS		
ASAv 9.16.x	In test				
ASA 9.16.x and FX-OS 2.10.x on 4k/9k	Waiting on entropy	Posted to NIAP!!!	Waiting for FIPS	N/A	
ASA 9.16.x and FX-OS 2.10.x on 2k and 1k	Entropy received	Posted to NIAP!!!		N/A	
FTD 7.0.x and FX-OS 2.10.x on 4k/9k	Waiting on Entropy	Posted to NIAP!!!	Waiting for FIPS	FX-OS	
FTD 7.0.x and FX-OS 2.10.x on 2k/1k	Entropy received	Posted to NIAP!!		1K	
				2K	
FTD 7.0.x on ASA HW+ ISA3000	Waiting on entropy	Posted to NIAP!!!	Waiting for FIPS	FTD	ISA
FTDv 7.0.x	Submitted to CMVP 4/28/23				
FMC 7.0.x	Waiting on entropy	Posted to NIAP!!!	Waiting for FIPS	USGv6 and Ready Logo	
FMCv 7.0.x	Submitted to CMVP 3/30/23				
NGIPsv 7.0.x	Submitted to CMVP 4/14/23			N/A	
Red = Not submitted; off track	Yellow = In progress; at risk	Lt. Green = On-Track Blue = Submitted	Green/Red = Gap in coverage	Blue = Complete/Posted	

Dashboard 7.0

Cert/Project	FIPS	CC	DoDIN APL	USGv6	
ASA 9.16.x	FIPS CR only	Posted to NIAP!!!	Waiting for Modified APL or FIPS CR		
	FIPS Level 2 - cancelled				
ASAv 9.16.x	Submitted to CMVP 6/30/23 Review Pending				
ASA 9.16.x and FX-OS 2.10.x on 4k/9k	FIPS CR only	Posted to NIAP!!!	Waiting for Modified APL or FIPS CR	N/A	
	FIPS Level 2 - cancelled				
ASA 9.16.x and FX-OS 2.10.x on 2k and 1k	FIPS CR only	Posted to NIAP!!!		N/A	
	FIPS Level 2 - cancelled				
FTD 7.0.x and FX-OS 2.10.x on 4k/9k	FIPS CR only	Posted to NIAP!!!	Waiting for Modified APL or FIPS CR	FX-OS	
	FIPS Level 2 - cancelled				
FTD 7.0.x and FX-OS 2.10.x on 2k/1k	FIPS CR only for 1k	Posted to NIAP!!		1K	
	FIPS Level 2 - cancelled			2K	
FTD 7.0.x on ASA HW	FIPS CR only	Posted to NIAP!!!	Waiting for Modified APL or FIPS CR	FTD	ISA
	FIPS Level 2 – cancelled				
FTDv 7.0.x	Submitted to CMVP 4/28/23 In Review as of 11/3/23				
FMC 7.0.x	FIPS CR only	Posted to NIAP!!!	Waiting for Modified APL or FIPS CR	USGv6 and Ready Logo	
	FIPS Level 2 – cancelled				
FMCv 7.0.x	Submitted to CMVP 3/30/23 In Review as of 10/20/23				
NGIPSv 7.0.x	Submitted to CMVP 4/14/23 In Review as of 10/27/23			N/A	
	Orange = CRs delayed due to waiting for FOM 7.3a to be validated and inserted in product	Blue = Complete/Posted	Red = Gap in coverage	Blue = Complete/Posted	

Dashboard 7.4

Cert/Project	FIPS	CC	DoDIN APL	USGv6
ASA 9.20.x	Level 2 and CR In Planning	In Planning	In Planning	
ASAv 9.20.x	Level 2 and CR In Planning			
ASA 9.20.x and FX-OS 2.14.x on 4k/9k	Level 2 and CR In Planning	In Planning	In Planning	N/A
ASA 9.20.x and FX-OS 2.14.x on 2k and 1k	Level 2 and CR In Planning	In Planning		N/A
ASA 9.20.x and FX-OS 2.14.x on 3k	Level 2 In Test – on IUT list CR in Planning	In Test	In Planning	
ASA 9.20.x and FX-OS 2.14.x on 4200s	Level 2 and CR In Planning	In Planning	In Planning	
FTD 7.4.x and FX-OS 2.14.x on 4k/9k	Level 2 and CR In Planning	In Planning	In Planning	FX-OS – In Planning
FTD 7.4.x and FX-OS 2.14.x on 2k/1k	Level 2 and CR In Planning	In Planning		1K – In Planning
				2K – In Planning
FTD 7.4.x and FX-OS 2.14.x on 3k	Level 2 In Test – on IUT list CR in planning	In Test	In Planning	3k - In Planning
FTD 7.4.x and FX-OS 2.14.x on 4200s	Level 2 and CR In Planning	In Planning	In Planning	4200s – In Planning
FTDv 7.4.x	Level 2 and CR In Planning	In Planning	In Planning	FTD
FMC 7.4.x	Level 2 and CR In Planning	In Planning	In Planning	USGv6 and Ready Logo
FMCv 7.4.x	Level 2 and CR In Planning			
				N/A
Red = Gap in coverage, not submitted; off track	Yellow = In progress	Green = Submitted Blue = Completed		

Firewall Certification Plan – 2021 and beyond

	Spring 2021 	Fall 2021	Spring 2022	Fall 2022	Spring 2023 	Fall 2023	Spring 2024
	Certified FIPS, CC, DoDIN APL, USGv6	Skip	Skip	Skip	Certified FIPS, CC, DoDIN APL, USGv6	Skip	Skip
ASA	9.16.x	9.17.x	9.18.x	9.19.x	9.20.x	9.21.x	9.22.x
FTD	7.0.x (was 6.8.x)	7.1.x	7.2.x	7.3.x	7.4.x	7.5.x	7.6.x
FMC	7.0.x(was 6.8.x)	7.1.x	7.2.x	7.3.x	7.4.x	7.5.x	7.6.x
FDM	7.0.x(was 6.8.x)	7.1.x	7.2.x	7.3.x	7.4.x	7.5.x	7.6.x
FX-OS	2.10.x	2.11.x	2.12.x	2.13.x	2.14.x	2.15.x	2.16.x
HW	*Certify FPR1150 and FPR4112		FPR 2k refresh available** (Tufnell Park – FPR 3k)	FPR 4k refresh available ** (Warwick Avenue – FPR 42xx) FPR3105 available	Certify Warwick Avenue (FPR 42xx) and Tufnell Park (FPR 31xx) Also FMC M6		
Key Fed Features	RFC7030, RFC8573, IPv6 RFC8200, DoD IN IPv6 only, TLS 1.3	TBD	RFC8784 available, but will be matched with AnyConnect in 7.4	TBD	RFC 6668, RFC 8268, RFC 8332, RFC 8784, RFC 8996, PLR 3.0, FLT on FDM	TBD	TBD

Cisco CSfC Product Tracking Table – Security Products

Product	VID	Check-in Package Submitted to NIAP by CC Lab	NIAP In-Evaluation List**	MOA Submitted	CSfC Listed	Common Criteria Posted
FPR 1k - 1010, 1120, 1140, 1150 - running ASA 9.16	11255	09/22/2021	02/07/2022	Requested 2/24/22		7/15/2022
FPR 1k - 1010, 1120, 1140, 1150 - running FTD 7.0	11290	03/15/2022	8/3/2022	Requested 8/9/22		1/31/2023
FPR 2k - 2110, 2120, 2130, 2140 - running ASA 9.16	11255	09/22/2021	02/07/2022	Requested 2/24/22		7/15/2022
FPR 2k - 2110, 2120, 2130, 2140 - running FTD 7.0	11290	3/15/2022	8/3/2022	Requested 8/9/22		1/31/2023
FPR 4k/ 9k - 4110, 4112, 4115, 4120, 4125, 4140, 4145, 4150 9300 w/ SM-24, 36, 44, 40, 48, 56 - running ASA 9.16	11256	09/22/2021	03/02/2022	Requested 3/17/22		8/12/2022
FPR 4k/ 9k - 4110, 4112, 4115, 4120, 4125, 4140, 4145, 4150 9300 w/ SM-24, 36, 44, 40, 48, 56 - running FTD 7.0	11292	3/30/2022	8/18/2022	Requested 2/1/23		2/13/2023
ASA - 5506, 5508, 5516, ISA 3000 - running ASA 9.16	11257	09/22/2021	01/31/2022	Requested 2/24/22		7/14/2022
ASAv - 9.16	11257	09/22/2021	01/31/2022	Requested 2/24/22		7/14/2022
ASA - 5508, 5516, ISA3000 - running FTD 7.0	11300	4/6/2022	8/18/2022	Requested 2/1/23		2/13/2023
FTDv - 7.0	11300	4/6/2022	8/18/2022	Requested 2/1/23		2/13/2023
NGIPSv - 7.0		Sep 2022				
AnyConnect 4.9 for iOS	11205	01/22/2021	06/08/2021	Requested 07/12/21	posted	9/16/2021
AnyConnect 4.10 for Android	11127	05/19/2021	09/15/2021	Requested 9/20/21	posted	12/29/2021
AnyConnect 4.10 on Windows	11126	05/19/2021	09/15/2021	Requested 9/20/21	posted	12/29/2021
AnyConnect 4.10 on Linux	11289	01/28/2022	03/08/2022	Requested 3/17/22	posted	7/18/2022
Identity Services Engine (ISE) 3.1	11271	11/16/2021	03/29/2022			

Hardening Reference Slides

Cisco Hardening

Cisco Guide to Hardening IOS Devices

<https://www.cisco.com/c/en/us/support/docs/ip/access-lists/13608-21.html>

Guide to Harden Cisco Firepower Management Center

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/hardening/fmc/FMC_Hardening_Guide_v64.html

Guide to Harden Cisco ASA Firewalls

<https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/200150-Cisco-Guide-to-Harden-Cisco-ASA-Firewall.html>

Cisco Hardening

Cisco Firepower Threat Defense Hardening Guide

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/hardening/ftd/FTD_Hardening_Guide_v64.html

Cisco FXOS Hardening Guide

https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/hardening/b_FXOS_4100_9300_Hardening/introduction.html

Cisco Guide to Hardening NX-OS

https://tools.cisco.com/security/center/resources/securing_nx_os.html

US National Security Agency Guides

<https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/>

Network Infrastructure Security Guide

https://media.defense.gov/2022/Mar/01/2002947139/-1/-1/0/CTR_NSA_NETWORK_INFRASTRUCTURE_SECURITY_GUIDANCE_20220301.PDF

Guide to Cisco Password Best Practices

https://media.defense.gov/2022/Feb/17/2002940795/-1/-1/0/CSI_CISCO_PASSWORD_TYPES_BEST_PRACTICES_20220217.PDF

Adopting Encrypted DNS in Enterprise Networks

https://media.defense.gov/2021/Jan/14/2002564889/-1/-1/0/CSI_ADOPTING_ENCRYPTED_DNS_U_OO_102904_21.PDF



Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Continue your education



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



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background is a vibrant, abstract graphic featuring a spectrum of colors from red and orange on the left to blue and green on the right. The colors are arranged in a series of overlapping, wavy bands that create a sense of movement and depth. A bright, white, starburst-like light source is positioned on the right side, from which rays of light emanate across the entire scene, enhancing the dynamic feel.

cisco *Live!*

Let's go

#CiscoLiveAPJC