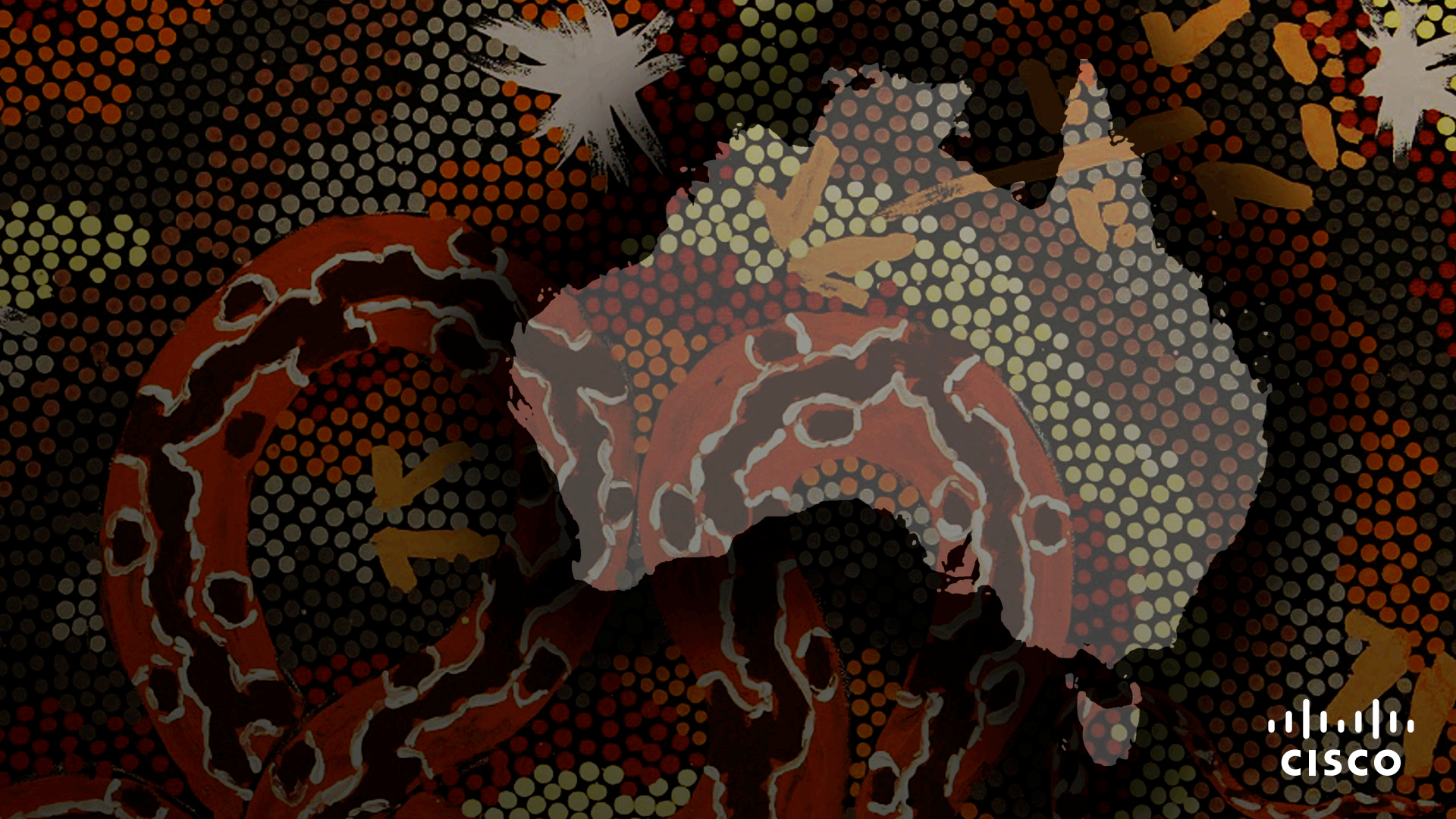
#CiscoLiveAPJC


cisco

The bridge to possible

Critical Requirements for Defending Government Networks

Andrew Benhase, Federal Architect
@CyberSecOps, @ThreatCowboy

BRKSEC-2067

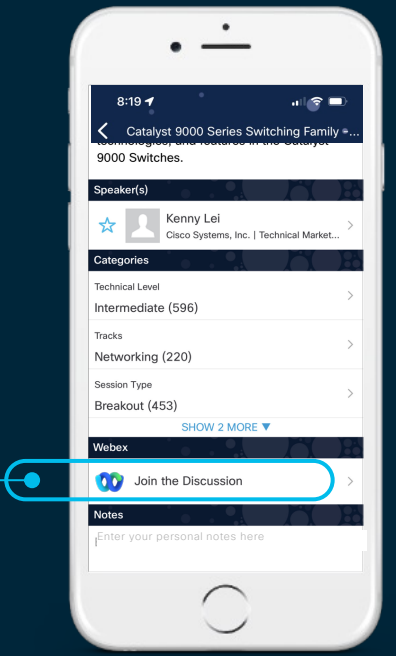
Cisco Webex App

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



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

Webex spaces will be moderated
by the speaker until Thursday 22 December, 2022.

Quick Housekeeping and Advisement

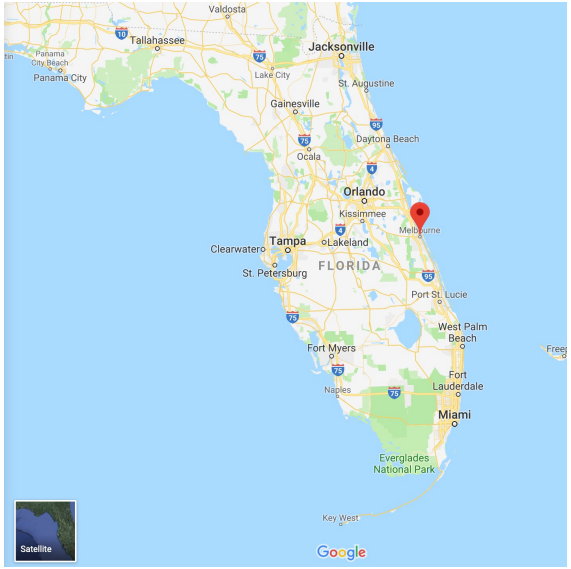
- There is nothing classified in this briefing
- There is nothing that is designated as ITAR
- There is nothing that is US Export Controlled
- There are references to US Government Intelligence Agencies
- All Information conveyed here can be discussed openly
- All information is PUBLIC in nature
- This is probably NOT the Cisco Live briefing you're expecting….

What I do here @cisco

- Federal Security Architect
- At Cisco 23 years, supporting US Federal Government
- 31 years primarily supporting US Defense, Civilian and Intelligence Communities
- Leader of the GOVSEC Technical Advisory Group
- Deep focus on defensive cyber operations, advanced encryption, making security work!
- My first Networkers was in 1997…
- https://www.linkedin.com/in/andrewbenhase/

@CyberSecOps
@ThreatCowboy
abenhase@cisco.com

From MLB to MEL



Agenda

- How the cyber world has changed *in the last 3 months
- Current Trends and TTPs
- Critical Network Defenses
- Access to the Internet is Critical
- Network Defense Architectures
- Open Q&A

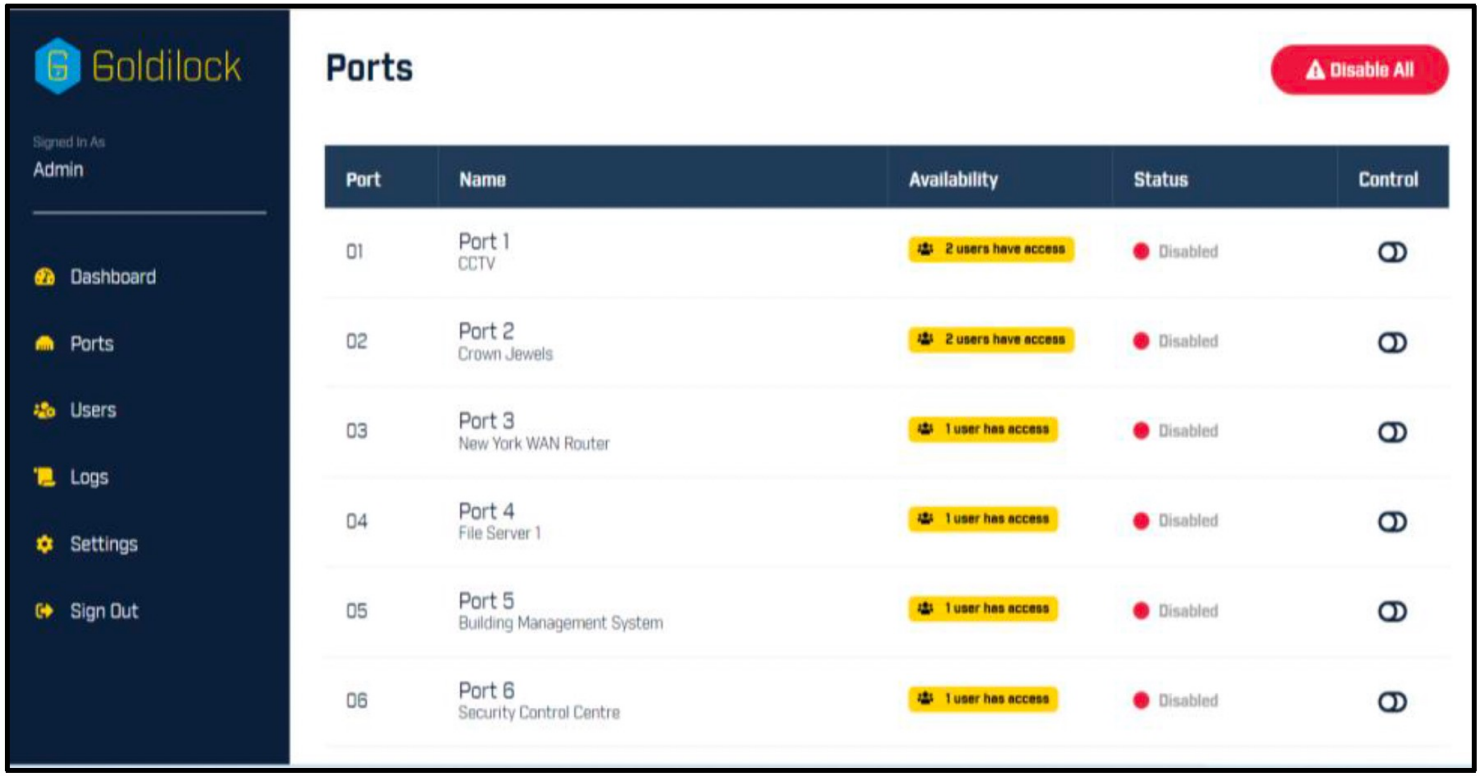
PRO TIP #1

This may not be as crazy as it seems....

But seriously…don't underestimate physical security

- 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 based on time schedule

Physical Relay based Disconnect



How the cyber world has changed

(in the last 100 days or so)

What exactly has happened?

Cyber Apocalypse models haven't emerged

Targeted increase in Industry events

- Starlink, VIASAT, Ukrainian Energy, Grid Sectors across the world

Companies have taken an overt, active role in defense of a country

Technology Embargo has happened

Removal of Services, including Licensing

What exactly has happened?

Increase in Cyber Spend focus (we'll see)

An Information Warfare campaign has been hugely successful

Internet Access has remained in place for Ukraine

- No large scale Internet blackouts
  - *when power in Ukraine was consistent

Anything else?

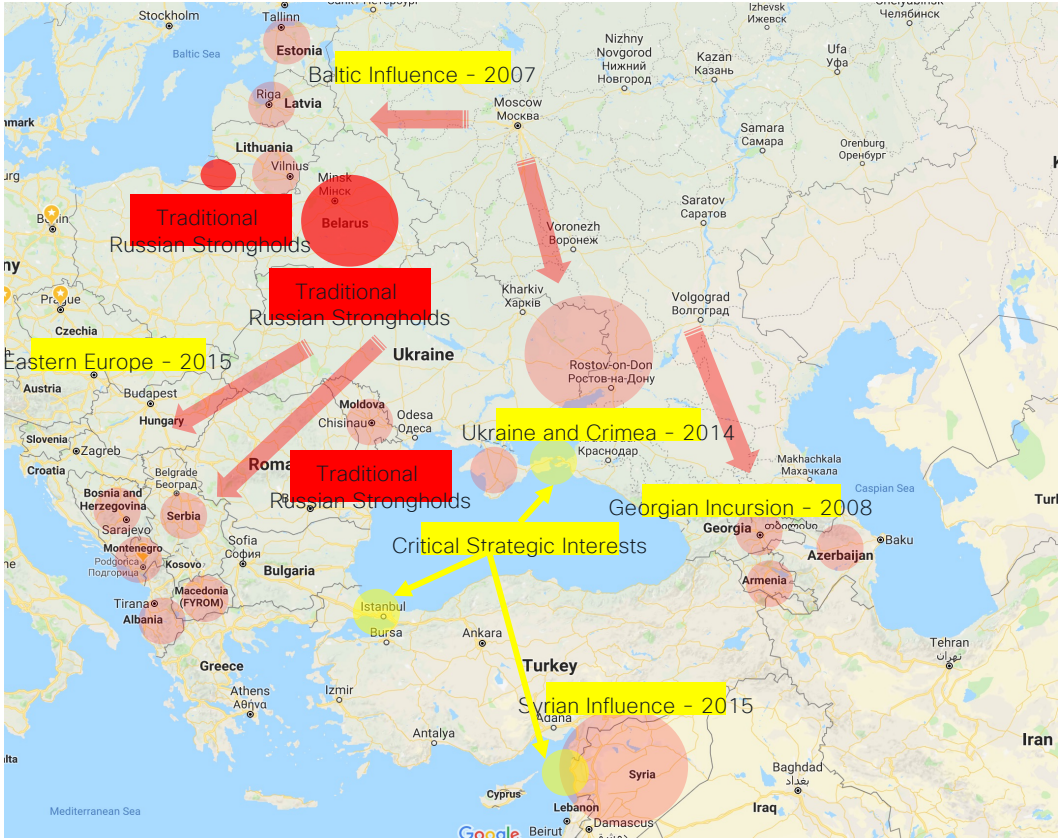
- Localized BGP Hijacks have happened
- Large Scale Country wide disruptions haven't happened yet
- BGP is more robust than we thought
- We were well prepared

Russian Campaign History and Future Influence

Originally Presented in 2019
Titled Cyber Cold War – C2W

cisco Live!

Strategic Reason for Russian Influence



Russian Cyber Dominance – Ukraine

How the world has really changed

- Countries realize how critical Internet access has become for International Support and Communications
- Countries have realized what it really means to be Internet isolated
- Conflict Countries are doing serious math on what is a sustainable network and where sovereign IT assets are located
- Sovereign Cloud is a new reality

What we can expect moving forward

- Sovereign Clouds as mandatory operations
- Huge increase in NATO Cyber spending
- Substantial focus on isolated license operations

This week in Cyber News

30 NOV 2022 NEWS

Majority of US Defense Contractors Not Meeting Basic Cybersecurity Requirements

James Coker Deputy Editor, Infosecurity Magazine
Follow @ReporterCoker

Nearly nine in 10 (87%) of US defense contractors are failing to meet basic cybersecurity regulation requirements, according to research commissioned by CyberSheath.

The survey of 300 US-based Department of Defense (DoD) contractors found that just 13% of respondents have a Supplier Risk Performance System (SPRS) score of 70 or above. Under the Defense Federal Acquisition Regulation Supplement (DFARS), a score of 110 is required for full compliance.

Anecdotally, a score of 70 is believed to be "good enough" to be considered compliant, according to the study authors.

DFARS, which was enacted into law in 2017, is designed to bolster cybersecurity in the defense industrial base. Defense contractors also must comply with the Cybersecurity Maturity Model Certification (CMMC), a certification framework they must pass to bid for contracts with the DoD.

The first version of CMMC was released in January 2020, with an updated version, 2.0, coming into effect in May 2023. It offers five certification levels spanning one through five, with five being the highest. Each level maps to a different level of process maturity.

The new study suggests the vast majority of DoD defense contractors are neither meeting current DFARS obligations or in a position to comply with the updated version of CMMC.

A Threat to National Security

This could have major consequences for defense contractors, nearly half of whom would lose up to 40% of their revenue if DoD contract loss occurs, according to the research.

Speaking to *Infosecurity*, Tom Brennan, USA Chairman at CREST, said: "CMMC is a set of commercially reasonable standards to protect data. Organizations should address it as part of doing business or they can lose the contract."

Yet, the report found that 70% have not deployed security information and event management (SIEM), 79% lack a comprehensive multi-factor authentication system, 73% do not have an endpoint detection response (EDR) solution and 80% lack a vulnerability management solution.

Related to This Story

- Is Your ISO Renewal at Risk Due to #COVID19 and Lockdown?
- Steps to Implementing Voice Authentication and Securing Biometric Data
- Interview: Deborah Golden, US Cyber Risk Services Leader, Deloitte
- 2020 Cybersecurity Predictions: Compliance, Authentication and CISO Evolution
- #Infosec19: Infosecurity's Second State of Cybersecurity Report, Available Now

What's Hot on

CYBERSECURITY

NATO prepares for cyber war

More than 1,000 cyber professionals in NATO members and its allies across the globe participated in an exercise this week to test and strengthen cyber defenses.

The war in Ukraine has injected new urgency into questions about how NATO would respond to a cyberattack on a member state large enough to invoke Article 5. | Sean Gallup/Getty Images

By MAGGIE MILLER
12/03/2022 12:07 PM EST

TALLINN, Estonia — Some 150 NATO cybersecurity experts assembled in an unimposing beige building in the heart of Estonia's snow-covered capital this week to prepare for a cyberwar.

Global Trends

Supply Chains are now Critical to Governments

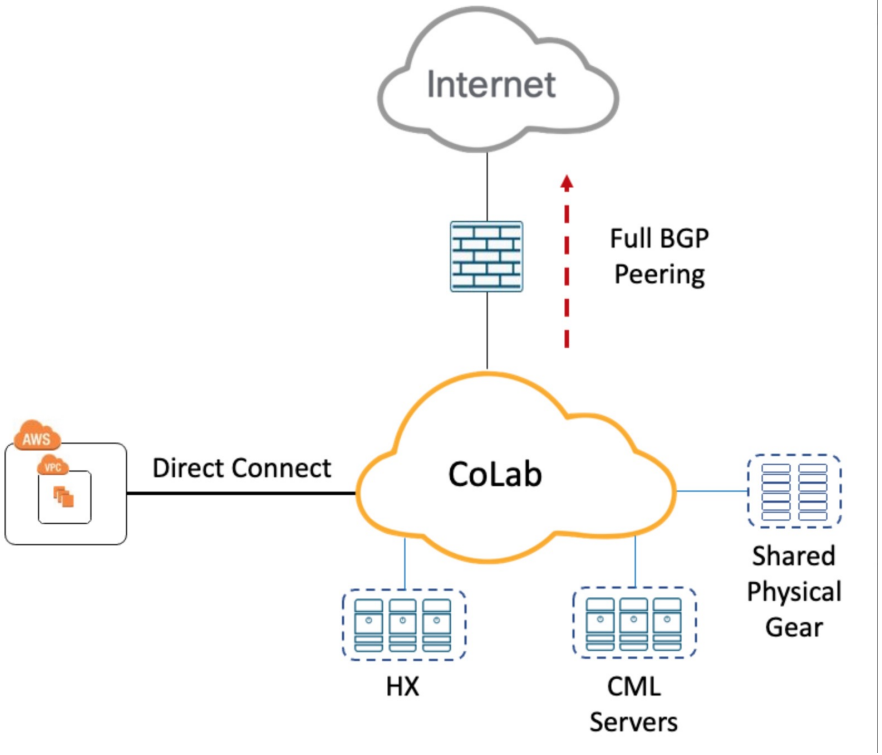
- Hardware Supply Chains have become a critical weakness
- Software Supply Chains are immediate
- Can robust, secure architecture be easily deployed with automation?

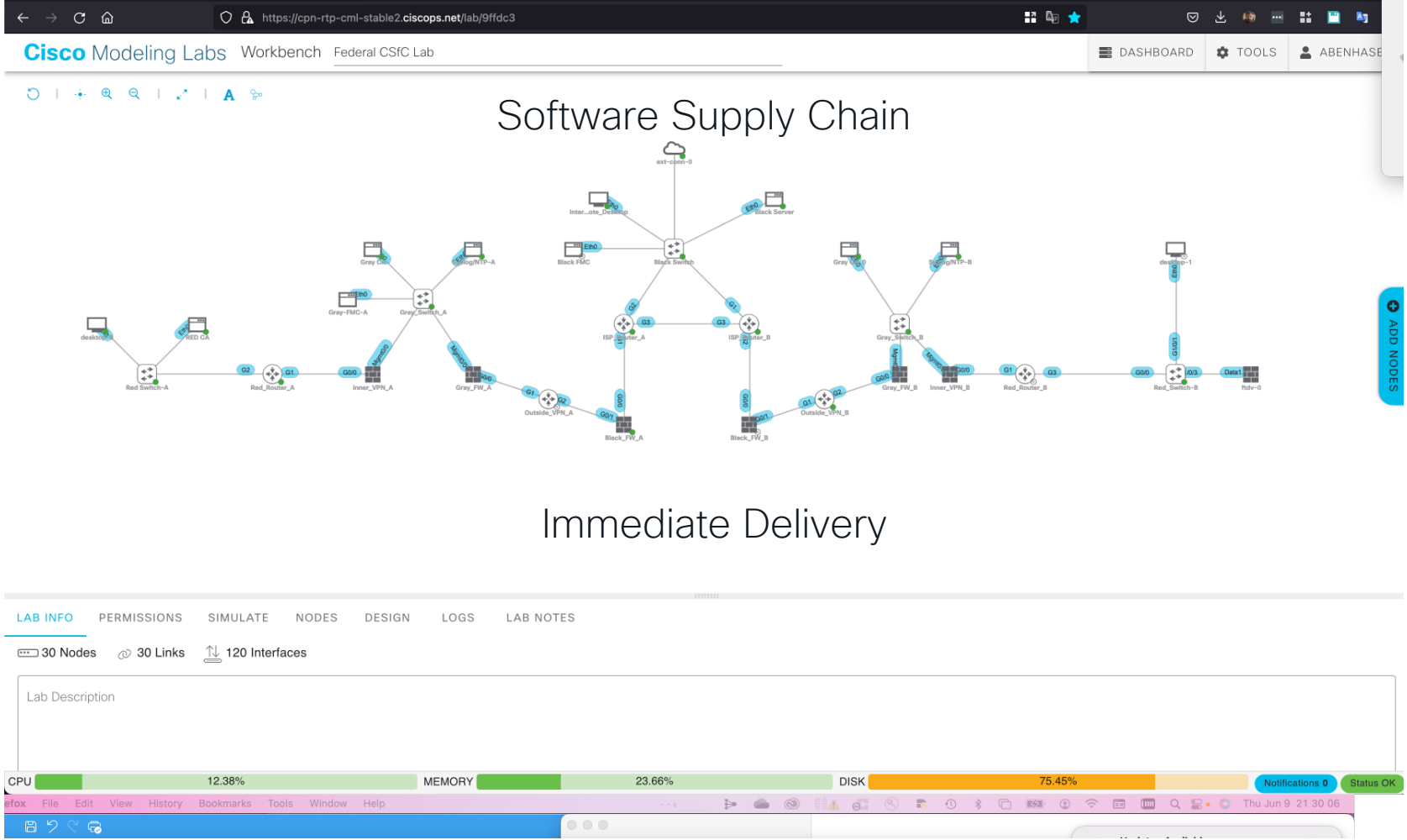
New Things to talk about

Cisco Federal CPN

- Independent Network held entirely outside of Cisco
- Full BGP Peer to the Internet
- Substantial Compute Resources
- Focused on Government Customer Modeling, Support and Assistance
- Maintains dedicated SecOps functions

Government CPN – CoLAB





Tactics, Techniques and Procedures

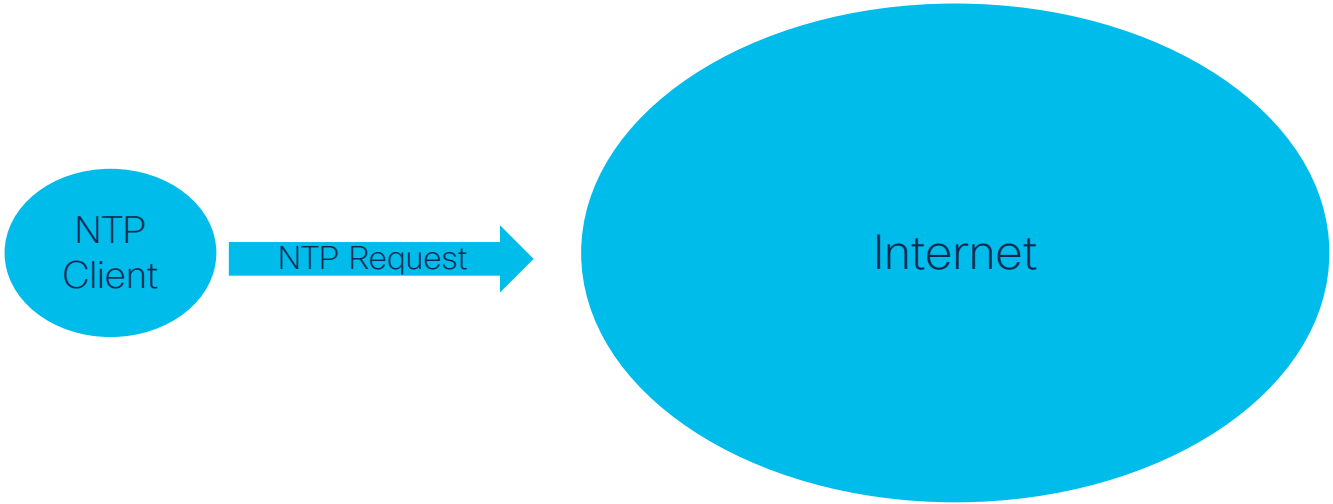
CPN gets lots of interest from friends

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



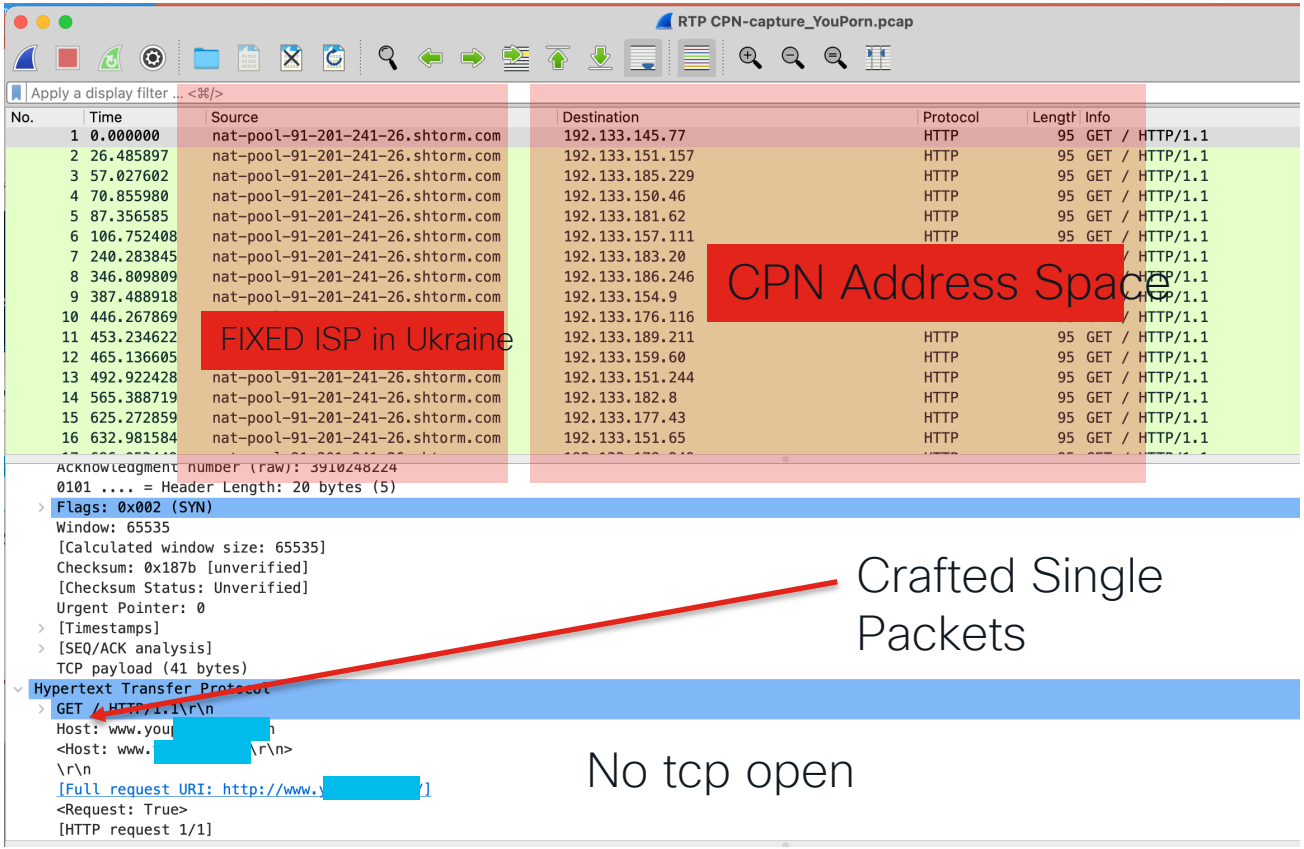
	Subject Port/Protocol	Subject Host Groups	Subject Location	Subject Bytes	Subject Byte Rate	Subject Interfaces	Application	To
	123/UDP	Russian Federation	Russian Federation	768	6.45	192.133.161.242(ifIndex-3), 192.133.161.242(ifIndex-1)	NTP (unclassified)	
	123/UDP	Russian Federation	Russian Federation	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)	
ru	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	
	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	

Interesting Denial Concept

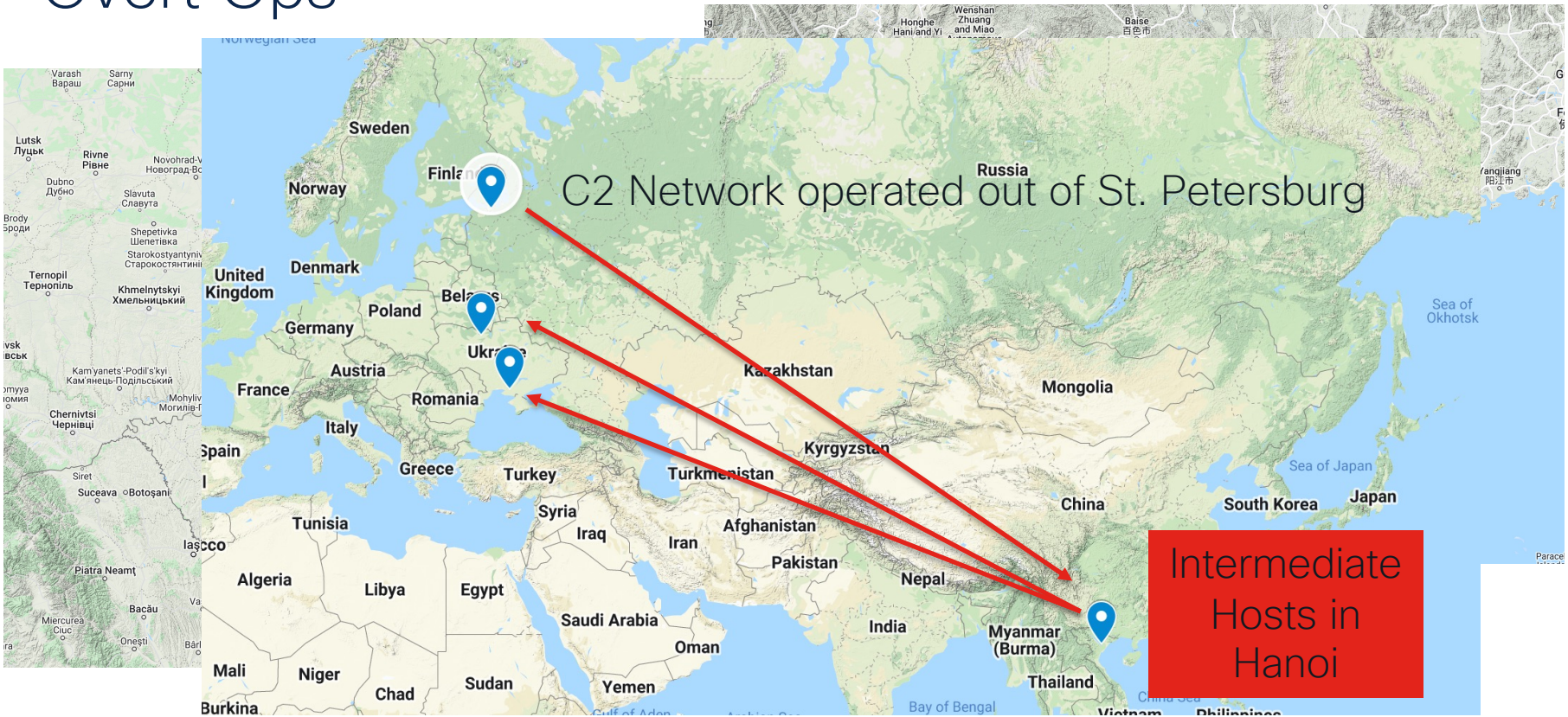
1. If I constantly overwhelm with security events
2. And shorten the practical window of FIFO collection
3. Effectively shortening the observation windows and effective collection
4. I can real dollar cost expense out a large portion of observation outside of possibly the Federal Government
5. Make observation 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

Overt Ops



Overt Ops



So why?

Waiting for a response

See who is watching

Critical Asset protection are poke and response scenarios

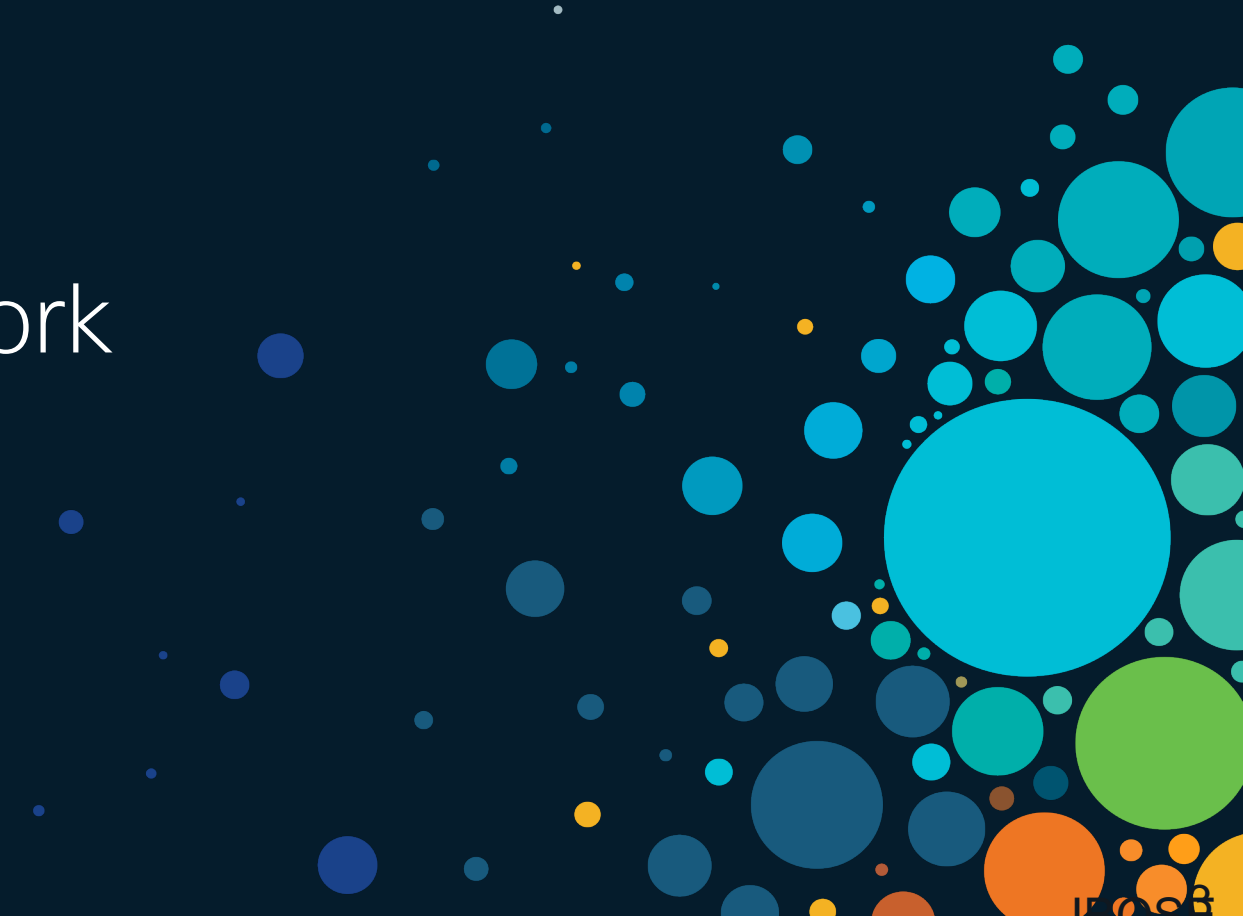
Overt defenses are an indication of something you want to protect

Cisco is now a global target of Hostile Nation States

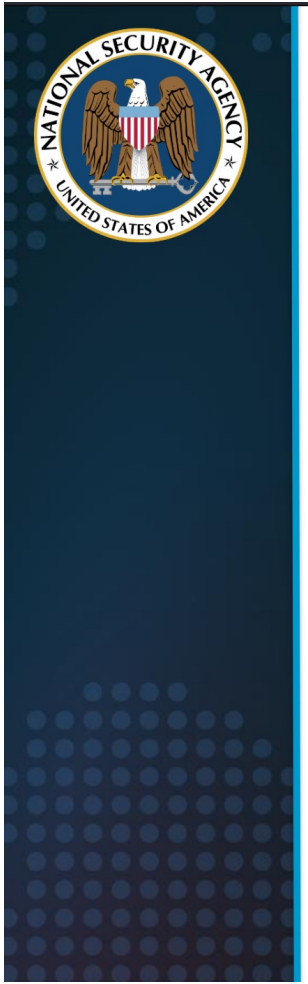
Open Topic:

What unique TTPs are you seeing today?

Critical Network Defenses



cisco Live!



National Security Agency
Cybersecurity Technical Report

Network Infrastructure Security Guidance

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

Simple Checklists still Matter – don't assume

Critical Protocols to Block

- 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

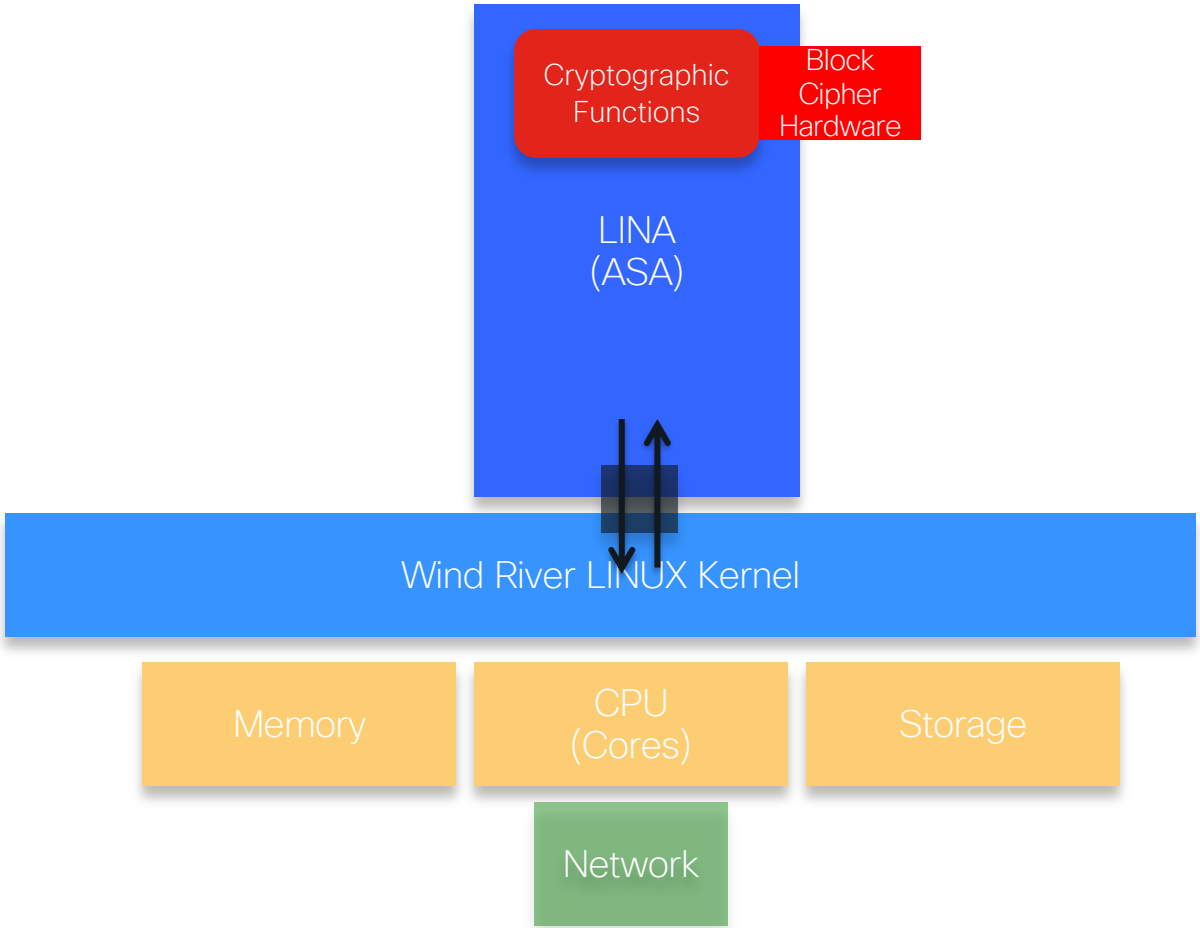
They *may be natively dropped (maybe not)

Most likely they are explicitly forwarded

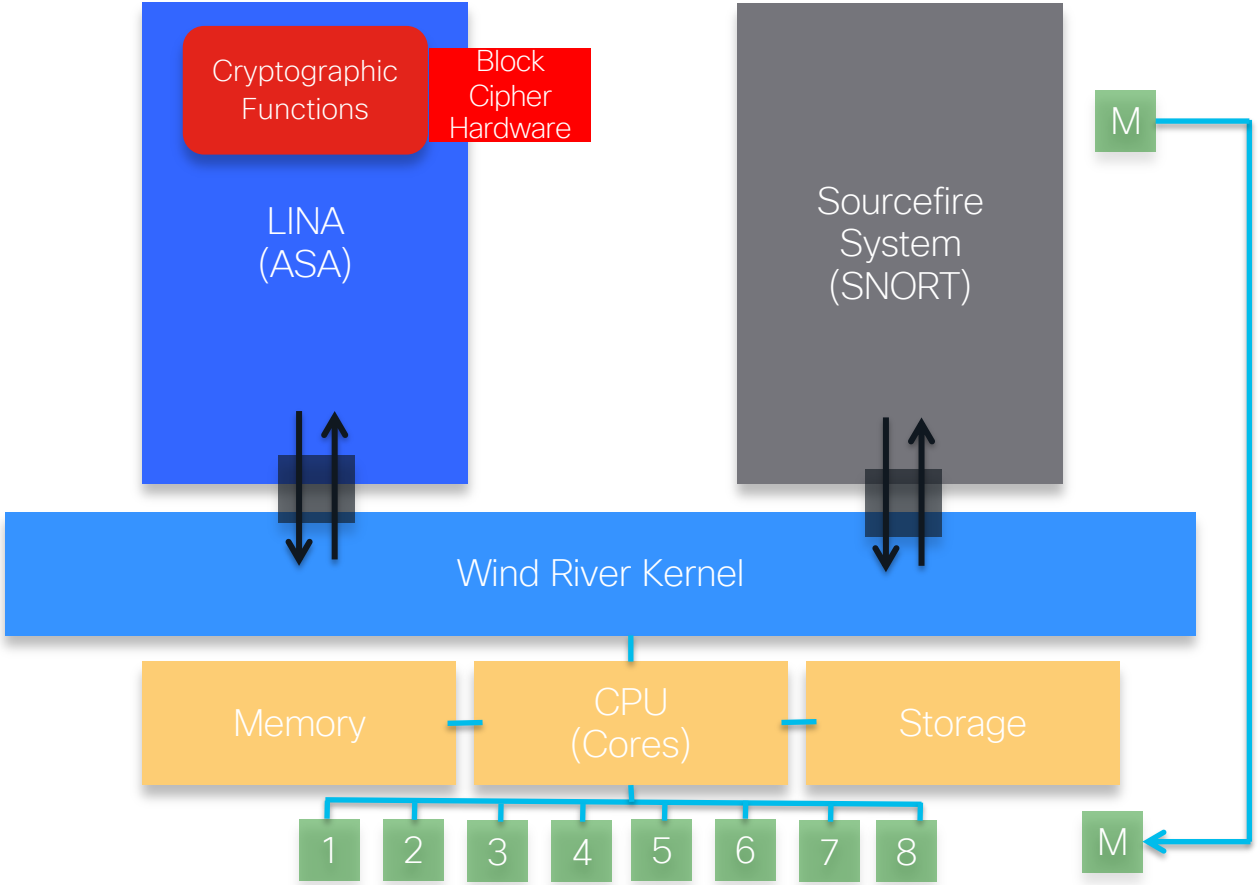
Minimally establish monitor rules for these protocols

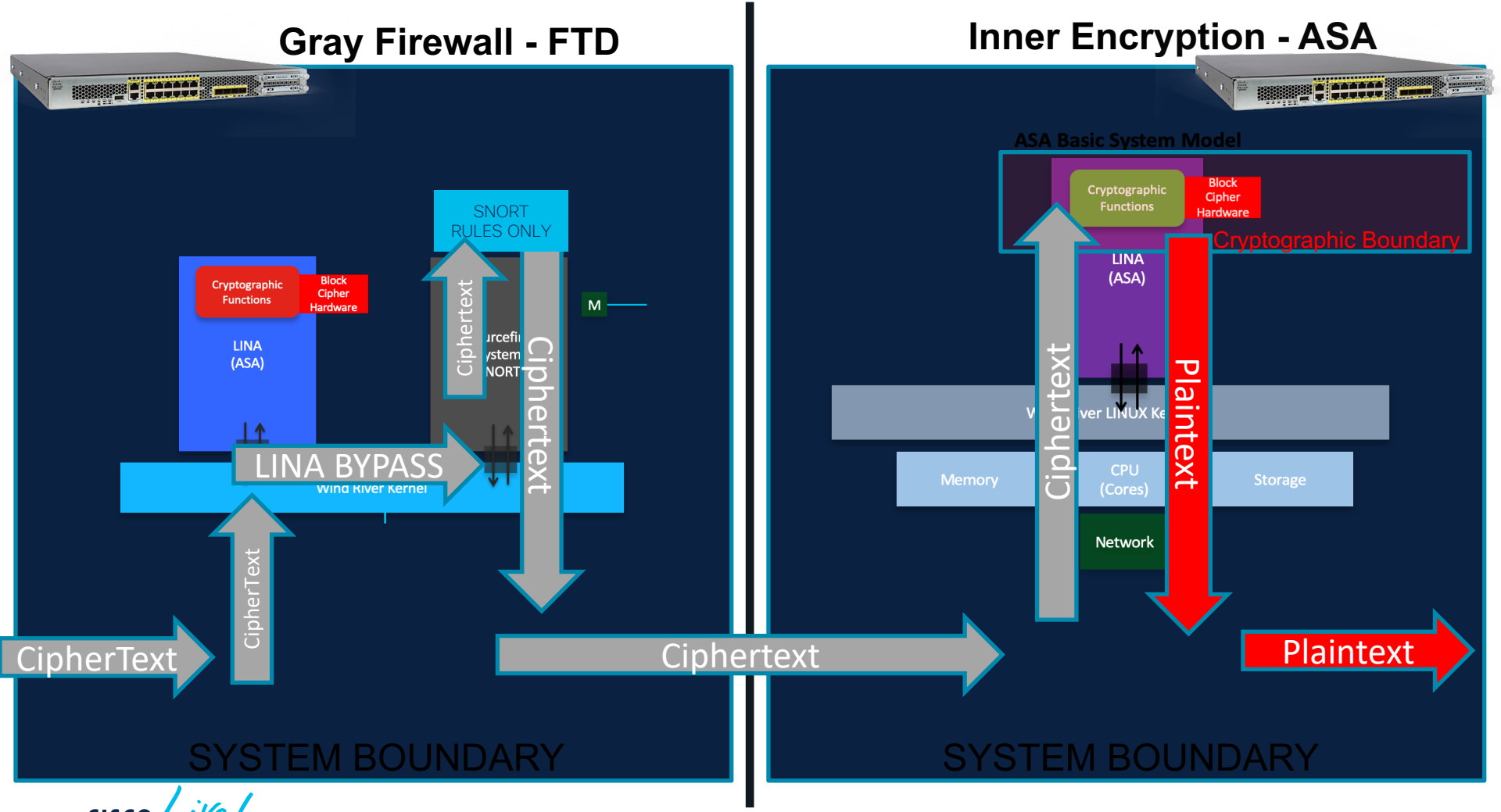
Important things to know about Cisco Firewalls

ASA Basic System Model

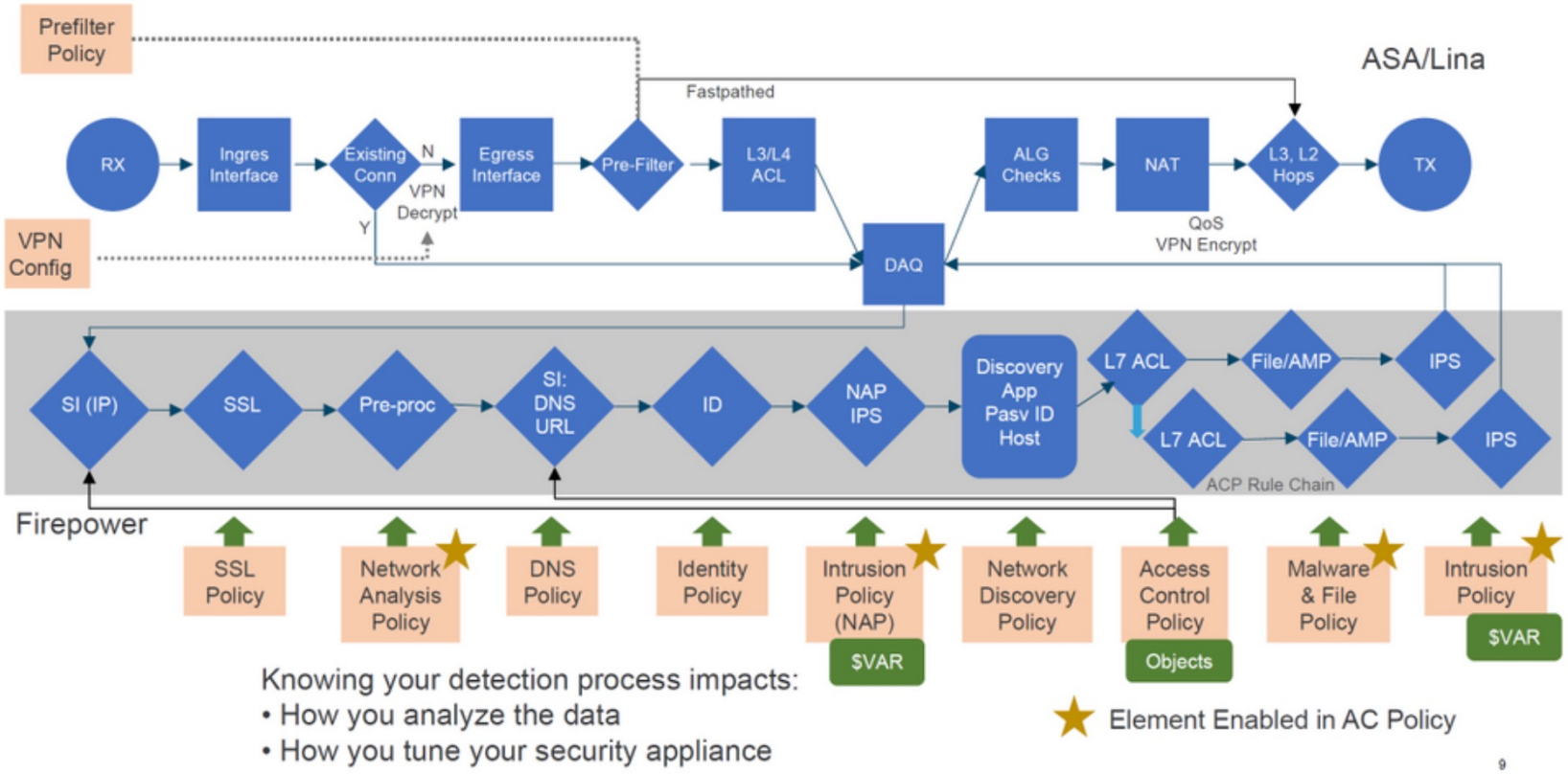


Firepower Threat Defense System Model





Packets and Policies: Know What's Happening Where



Build Robust VPN Overlays

cisco Live!

Multiple Classifications of Networks

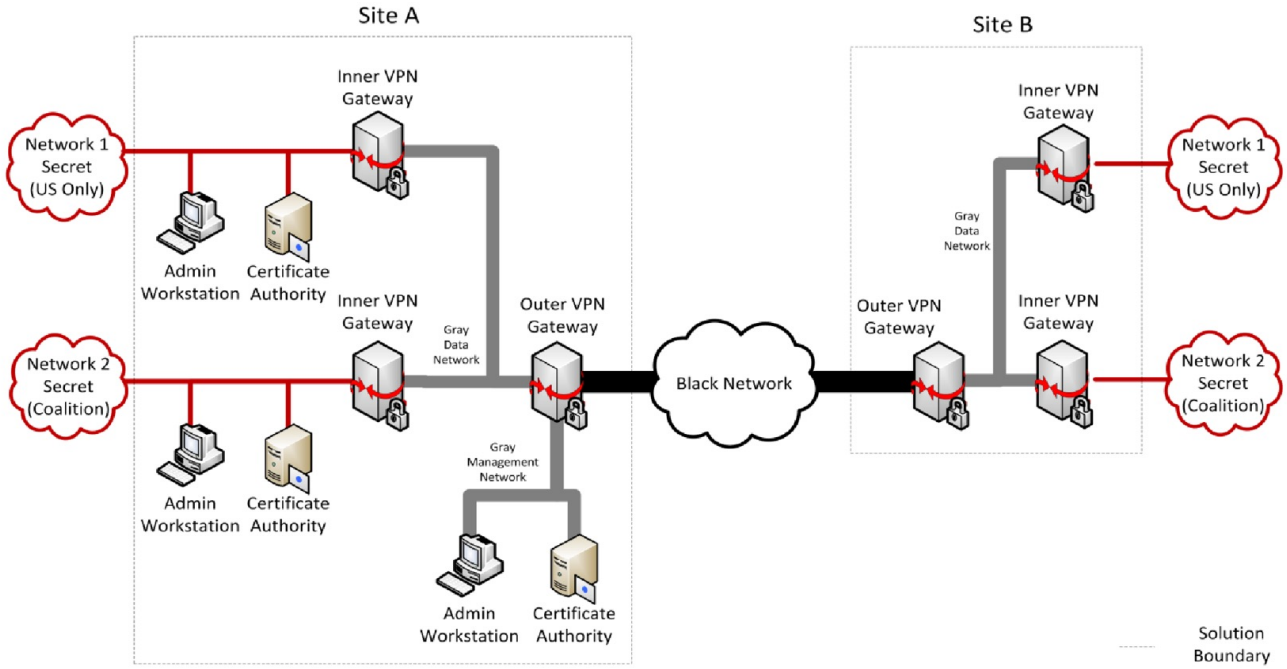
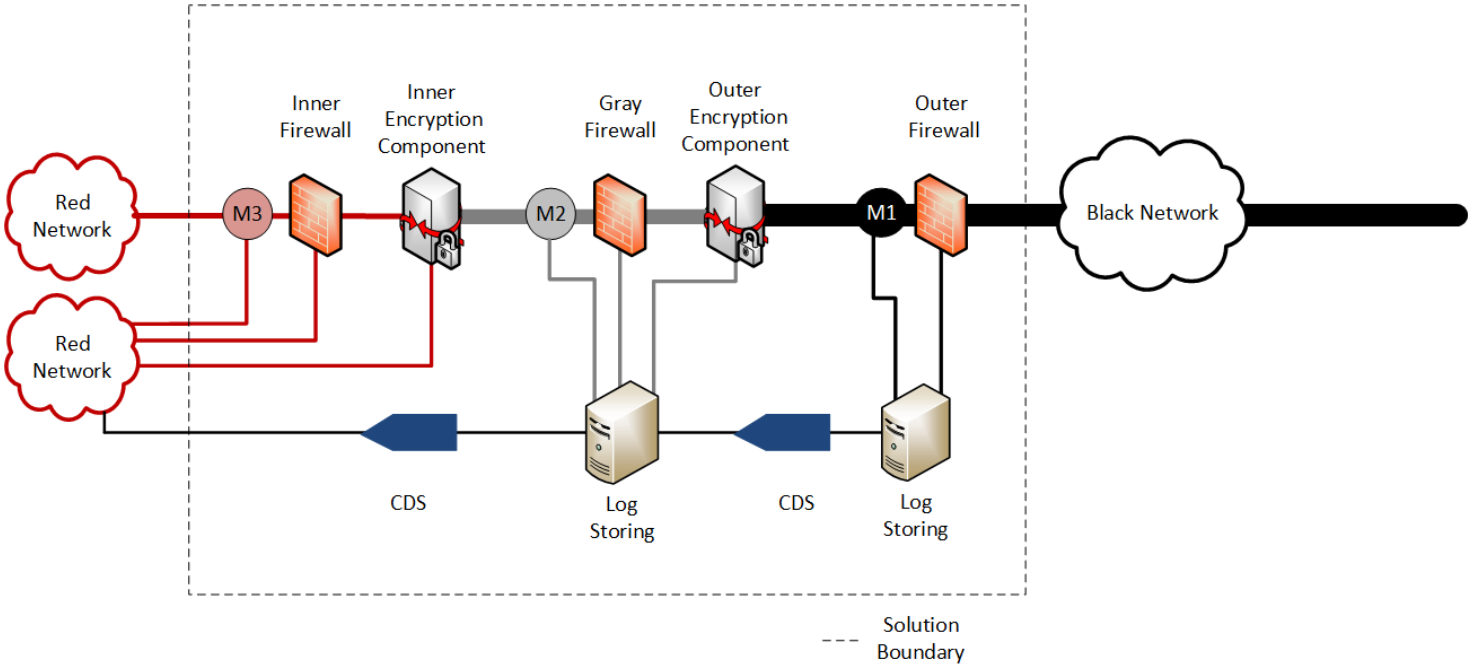


Figure 6. VPN Solution for Two Networks of the Same Classification Level

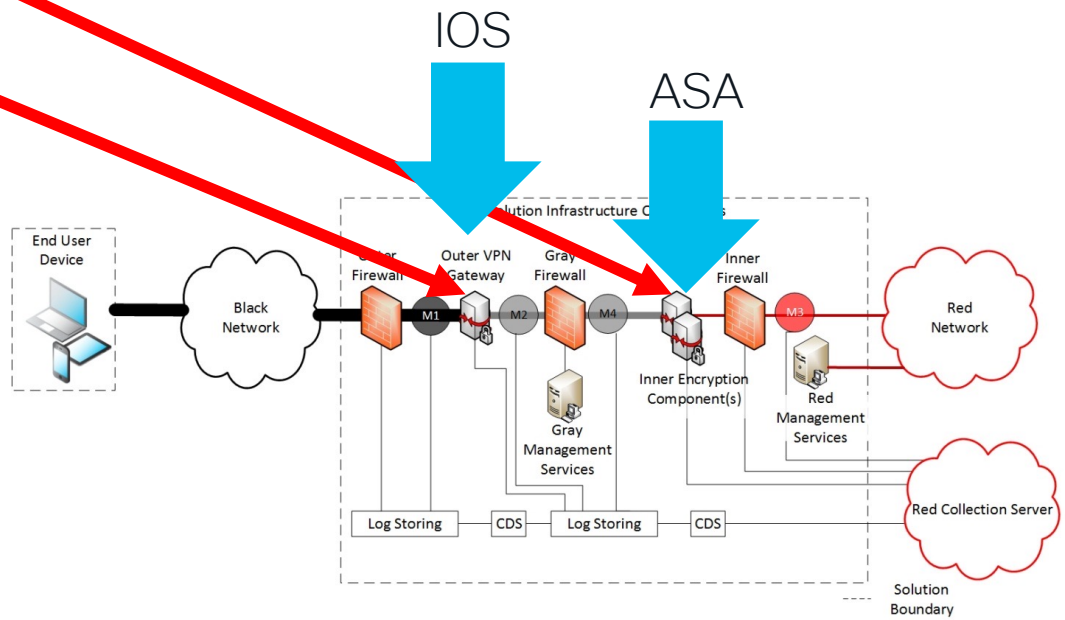
Remote Access Infrastructure



REF: https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/mobile-access-cp.pdf

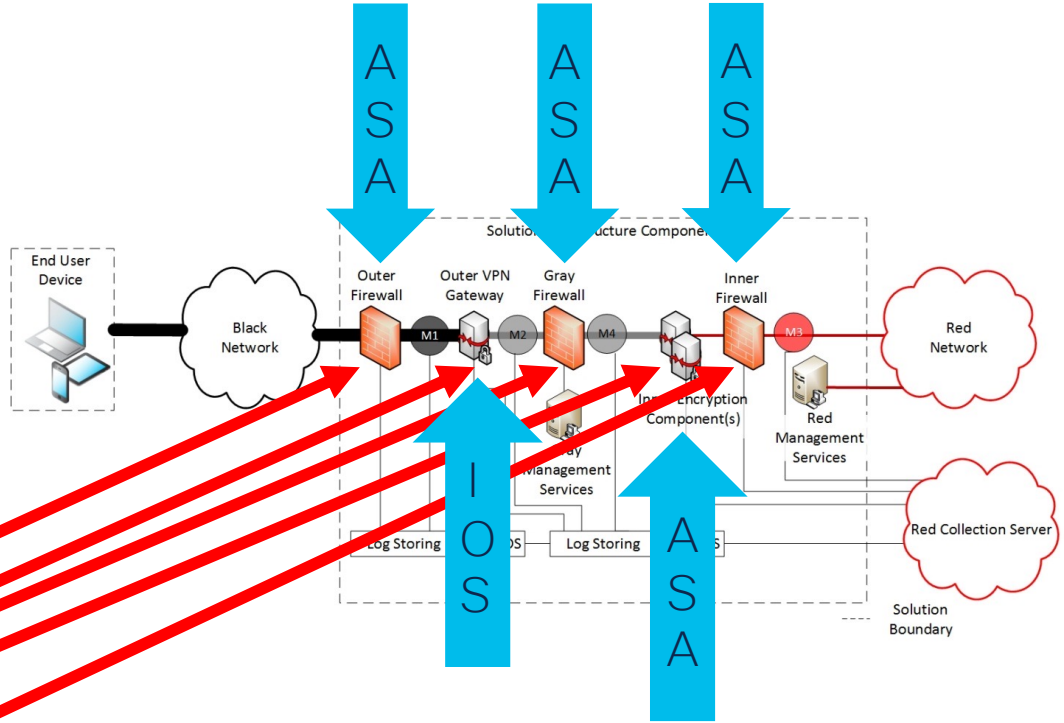
Building Trust

MA-PS-16	The Outer VPN Gateway and Inner Encryption endpoints must either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.
MA-PS-17	The Outer Firewall, Outer VPN Gateway, Gray Firewall, Inner Encryption Component, and Inner Firewall must use physically separate components, such that no component is used for more than one function (see Figure 1).



Building Trust

MA-PS-16	The Outer VPN Gateway and Inner Encryption endpoints must either come from different manufacturers, where neither manufacturer is a subsidiary of the other, or be different products from the same manufacturer, where NSA has determined that the products meet the CSfC criteria for implementation independence.
MA-PS-17	The Outer Firewall, Outer VPN Gateway, Gray Firewall, Inner Encryption Component, and Inner Firewall must use physically separate components, such that no component is used for more than one function (see Figure 1).



Defending Critical Network Access

cisco Live!

What is a critical network?

- Some asset that you care about (obviously)
- Defense Networks
- First Responder Networks
- Citizen Internet Access
- Internet access for foreign interests

Володимир Зеленський ✓
@ZelenskyyUa
Ukraine government official

Continued dialogue with 🇹🇷 President @RTErdogan. Discussed threats to food security posed by the aggressor & ways to unblock 🇺🇦 ports. Held discussions on cooperation in the security sphere. Unanimously agree on the need to restore peace. We appreciate 🇹🇷's help in this process.

3:32 PM · May 30, 2022 · Twitter Web App

Володимир Зеленський ✓ @ZelenskyyUa · Mar 22
Ukraine government official
Talked to @Pontifex. Told His Holiness about the difficult humanitarian situation and the blocking of rescue corridors by Russian troops. The mediating role of the Holy See in ending human suffering would be appreciated. Thanked for the prayers for Ukraine and peace.

Fast Forward

Chinese scientists call for plan to destroy Elon Musk's Starlink satellites

By Ben Turner published 6 days ago

Chinese military researchers say Starlink could threaten China's national security

China's Military Makes Plan to Destroy Elon Musk's Starlink

Tesla and SpaceX Chief Executive Officer Elon Musk speaks at the SATELLITE Conference and Exhibition in Washington, on March 9, 2020. (Susan Walsh/AP)

By Marisa Herman | Wednesday, 01 June 2022 06:43 AM

Comment | A A

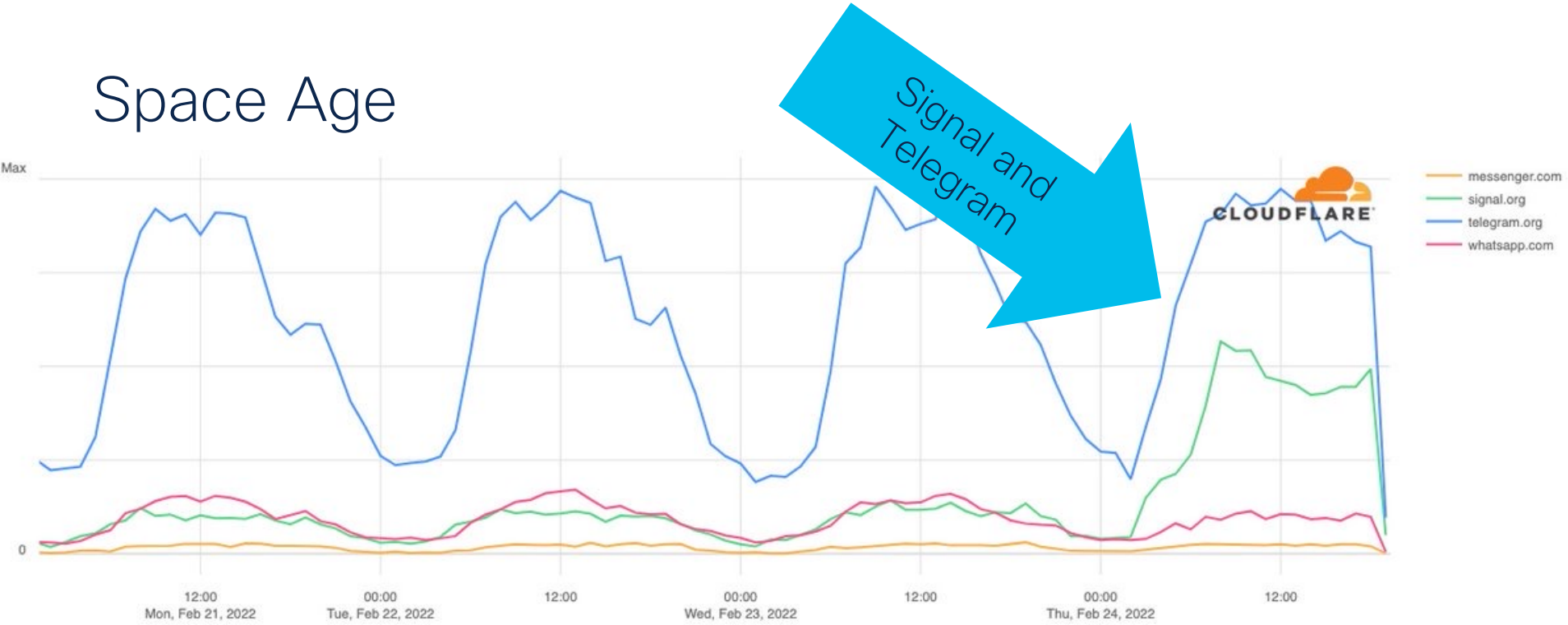
Billionaire tech entrepreneur Elon Musk's Starlink satellite constellation represents a major threat to the Chinese Communist Party's plan to knock out American satellites and render U.S. military assets ineffective if the two superpowers ever go to war – which is why China is working on ways to destroy Musk's machines, too.

published last month in the journal China's Modern Defence Technology. A translated copy of the paper is available here.

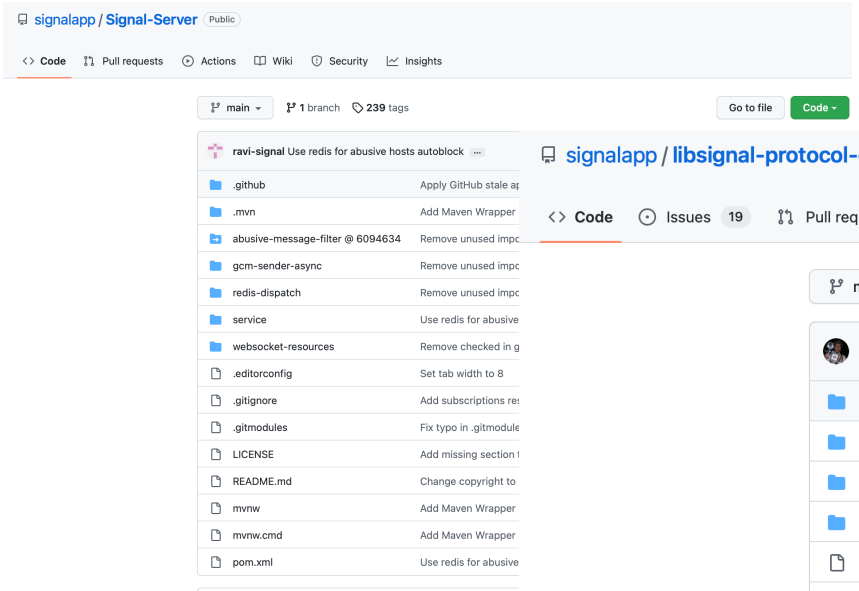
Lets be clear on some differences

Unencrypted
No frequency hopping
Manual shifts
Static Keywords
Analog Radio
Set frequency ranges

Space Age



Signal is a game changer



Peer Reviewed
Public Repository

```
/*-------------------------------------------------------------------*/

int ciphertext_message_get_type(const ciphertext_message *message)
{
    assert(message);
    return message->message_type;
}

signal_buffer *ciphertext_message_get_serialized(const ciphertext_message *message)
{
    assert(message);
    return message->serialized;
}

/*-------------------------------------------------------------------*/

int signal_message_create(signal_message **message, uint8_t message_version,
        const uint8_t *mac_key, size_t mac_key_len,
        ec_public_key *sender_ratchet_key, uint32_t counter, uint32_t previous_counter,
        const uint8_t *ciphertext, size_t ciphertext_len,
        ec_public_key *sender_identity_key, ec_public_key *receiver_identity_key,
        signal_context *global_context)
{
    int result = 0;
    signal_buffer *message_buf = 0;
    signal_buffer *mac_buf = 0;
    signal_message *result_message = 0;

    assert(global_context);

    result_message = malloc(sizeof(signal_message));
    if(!result_message) {
        return SG_ERR_NOMEM;
    }
    memset(result_message, 0, sizeof(signal_message));
    SIGNAL_INIT(result_message, signal_message_destroy);

    result_message->base_message.message_type = CIPHERTEXT_SIGNAL_TYPE;
    result_message->base_message.global_context = global_context;

    SIGNAL_REF(sender_ratchet_key);
    result_message->sender_ratchet_key = sender_ratchet_key;

    result_message->counter = counter;
    result_message->previous_counter = previous_counter;
```

Critical Tools and Differences

- Run from Dubai
- Run by former Russians
- Threats of country wide blocks
- Not open source
- Questionable server side operations
- Politically uncertain
- Useful intelligence tool

27 FEB, 13:18

Telegram decides not to block channels in countries involved in conflict around Ukraine

Earlier on Sunday, Durov said that the messenger was looking at blocking, partially of completely, its channels in the countries involved in the conflict around Ukraine for the period of the conflict, since Telegram channels are often used to spread fakes and the messenger is physically unable to verify the authenticity of publications

MOSCOW, February 27. /TASS/. Telegram has dropped the idea of blocking, partially or completely, its channels in the countries involved in the situation around Ukraine following numerous requests from users, Pavel Durov, the founder of the messaging app, said on Sunday.

"Many users have asked us not to look at blocking Telegram channels during the conflict because we are the only source of information for them. Bearing in mind these requests, we have decided not to look at such measures. However, I ask once again in this difficult period to verify information and not to take any data published in Telegram channels for granted," he wrote on his channel.

Earlier on Sunday, he said that the messenger was looking at blocking, partially of completely, its channels in the countries involved in the conflict around Ukraine for the period of the conflict, since Telegram channels are often used to spread fakes and the messenger is physically unable to verify the

Telegram: the app at the heart of Ukraine's propaganda battle

It's the most popular messaging service in Ukraine, and used by protesters of all kinds. Now it must find a way to make money

Telegram co-founder Pavel Durov has supported the app from his $17bn fortune, but there is now talk of a flotation. Photograph: Manuel Blondeau/Getty Images

In the days after Vladimir Putin's invasion of his country, Ukraine's president, Volodymyr Zelenskiy, used his Telegram channel to send a defiant video message from the centre of the capital, Kyiv, calling on the nation to unite and resist the Russian attack.

The WhatsApp-like messaging service, co-founded by exiled Russian billionaire brothers Pavel and Nikolai Durov, has become a key weapon in a digital propaganda battle that will ultimately boost its usage and investor profile ahead of a possible $50bn stock market flotation next year.

Ukraine's 44-year-old president, a former TV actor and comedian who campaigned over Telegram in the run-up to his landslide victory in the 2019 presidential election, used the service to refute claims that the army had been told to lay down arms, that an evacuation had been ordered - and to galvanise the populace by proving he would not be leaving the capital.

Russia is spying on Telegram chats in occupied Ukrainian regions. Here's how.

Thanks to a Ukrainian in occupied Kherson, we now know how Russian occupiers are using Telegram to surveil Ukrainians — and how dangerous its design flaws are.

Matt Tait
Dec 2

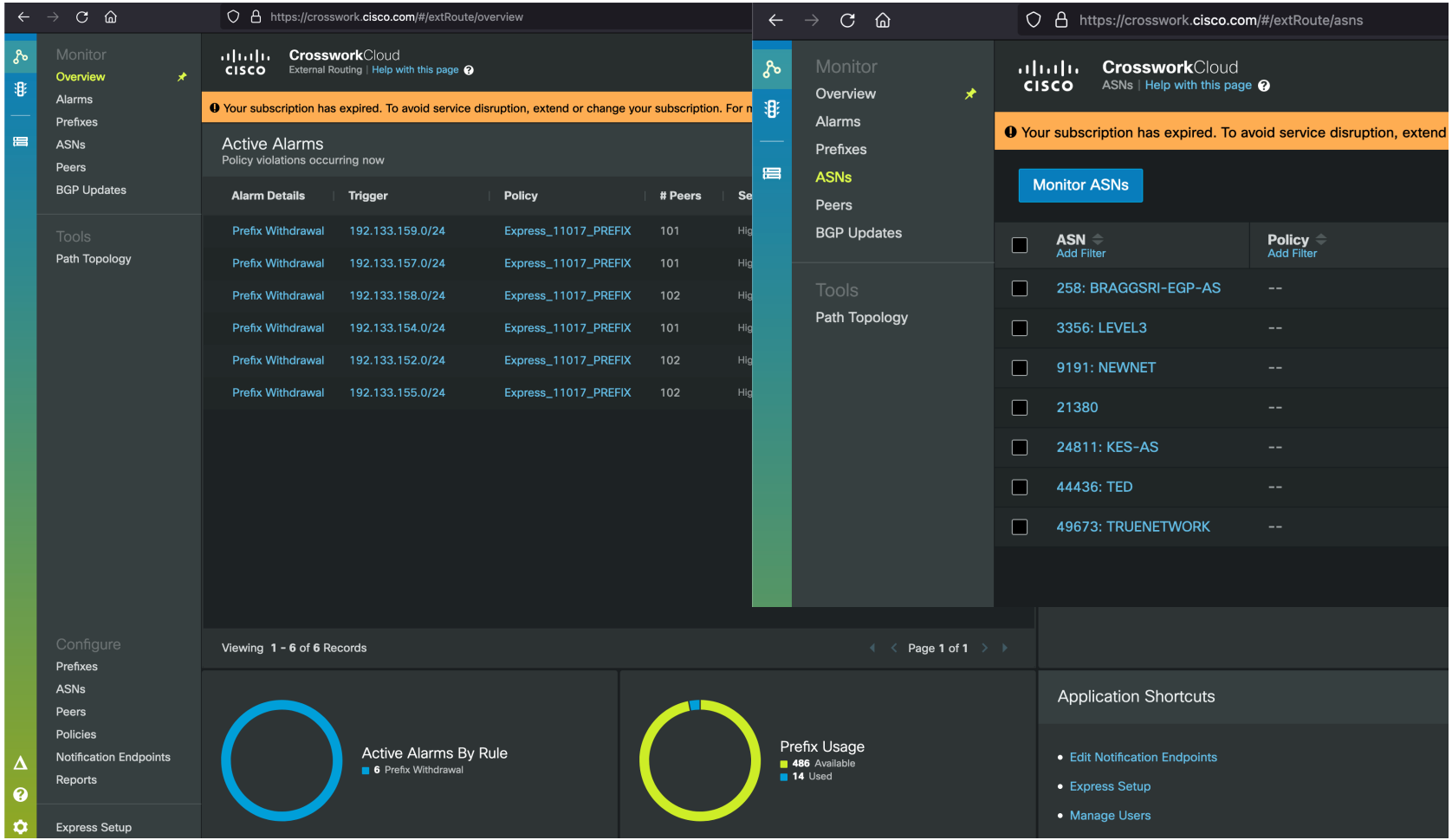
14 13

Last month, a story broke in the Washington Post about "stay behind" operations by Ukraine in then-occupied Kherson. The story discusses Ihor, a Ukrainian in Kherson, who was in communication with a Ukrainian special forces officer in Ukrainian-controlled Mykolaiv called "Smoke". Ihor, with help from Smoke, helped perform sabotage and espionage operations behind enemy lines.

At one point, Ihor was captured and tortured by Russian occupation forces for 11 days. Russia eventually released Ihor, but tried to use him to capture other partisans in the area. To do this, they instructed him to provide screenshots of all of his further interactions with Smoke, under threat of death if he didn't comply. Thanks to some ingenuity and prior planning, Ihor was able to secretly tip-off Smoke to defeat this Russian plan, and survived to tell the tale after Kherson was later liberated by Ukrainian forces.

Ihor's story—and the stories of others like him—is one of extraordinary bravery in extremely dangerous conditions. But his interview with the Washington Post reveals something more: it reveals that Russia was actively surveilling Telegram chats as part of their counterinsurgency operations in occupied Ukraine.

Telegram's security has long been called into question by the information security



Secured DNS

Secured DNS Slides

Block Outbound DNS to known DNS providers

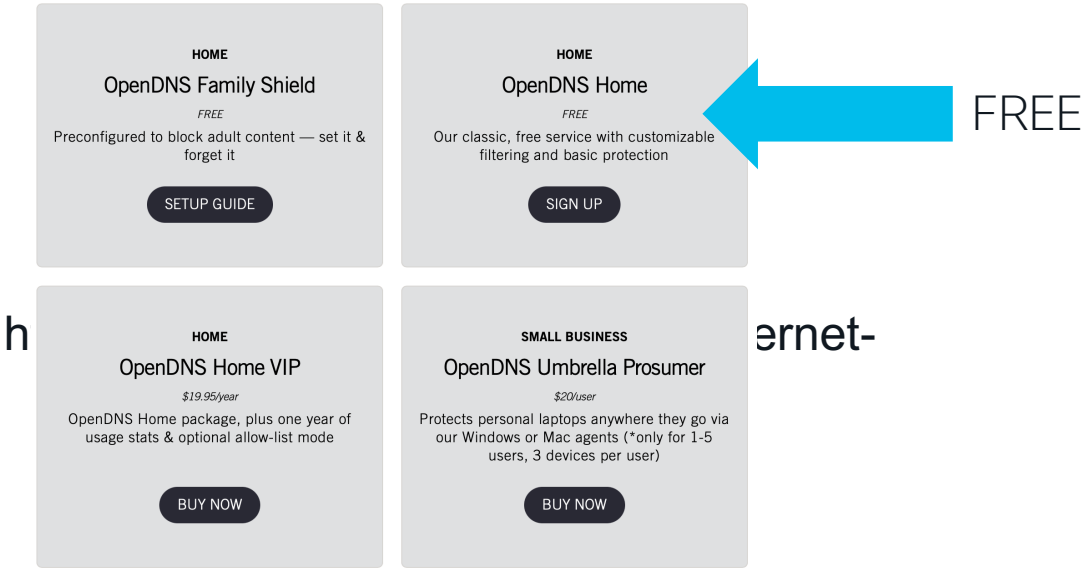
Use Security Policy as DNS Overlay

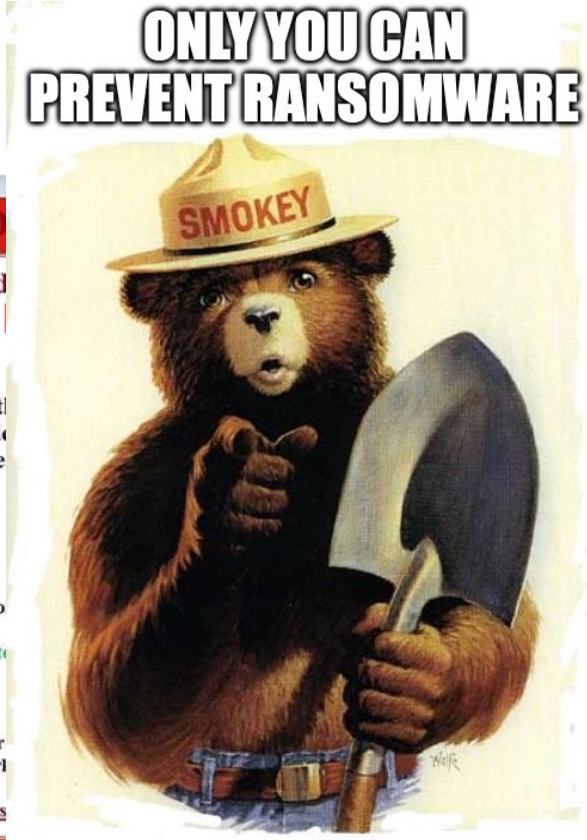
Use Encrypted DNS Requests

Be sure to include IPv6 DNS Destinations

I’m not saying use OpenDNS, but use OpenDNS

or Commercial Umbrella or some Secured DNS provider





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?

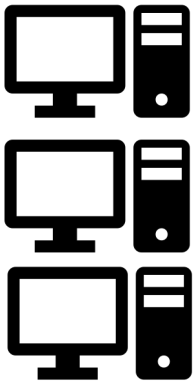
Correlation of security events

Forensic replay – Investigations

Sequence of packet times

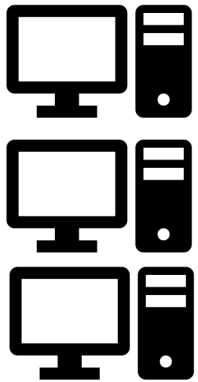
All Simulations require synchronized time

Secured NTP Slides



Give me Time!

Secured NTP Slides

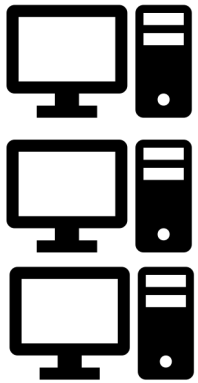


Give me Time!

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

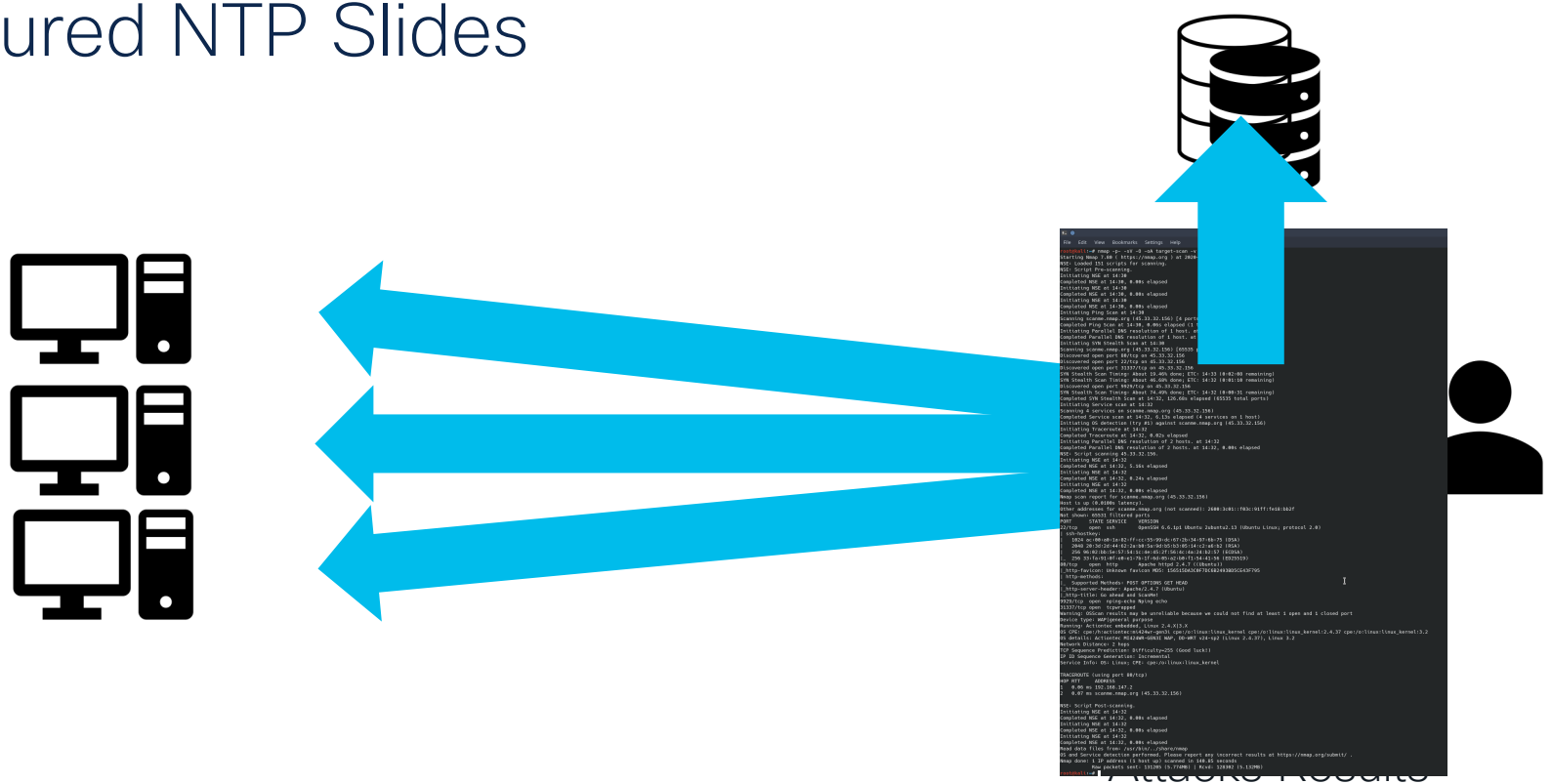


Thanks for adding to my list of known host addresses

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")

Secured NTP Slides

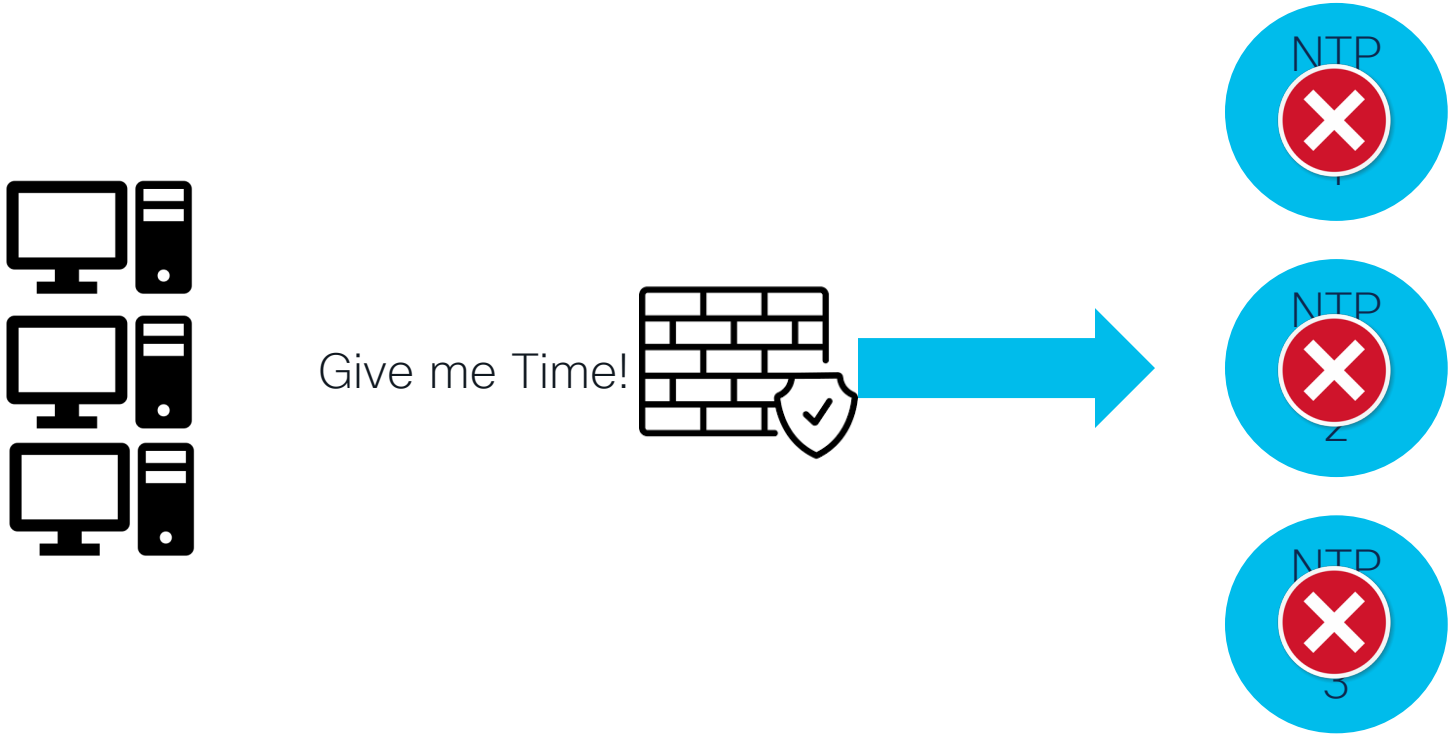


Secured NTP Slides

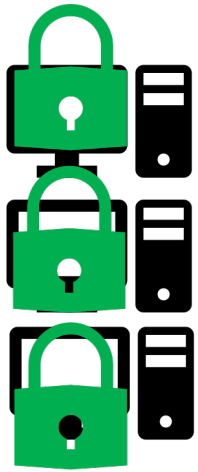
Collect Results
NMAP to JSON

Attacks Results

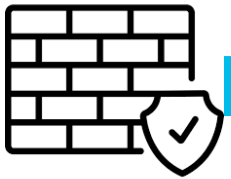
Secured NTP – What you should do



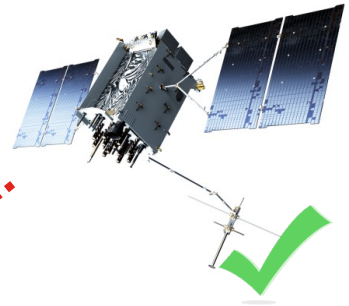
Secured NTP – What you should do

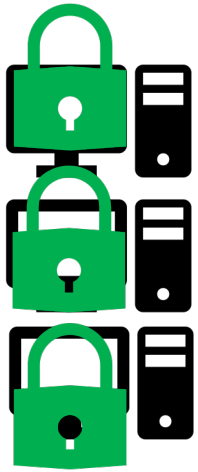


Give me Time!



Secured NTP – Most Secure Option





Give me Time!

NTP Router

RFC8573 + RFC 4493

Message Authentication Code for the Network Time Protocol

RFC 4493, RFC 8573, RFC 5905

- RFC 5905 – defines NTPv4

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

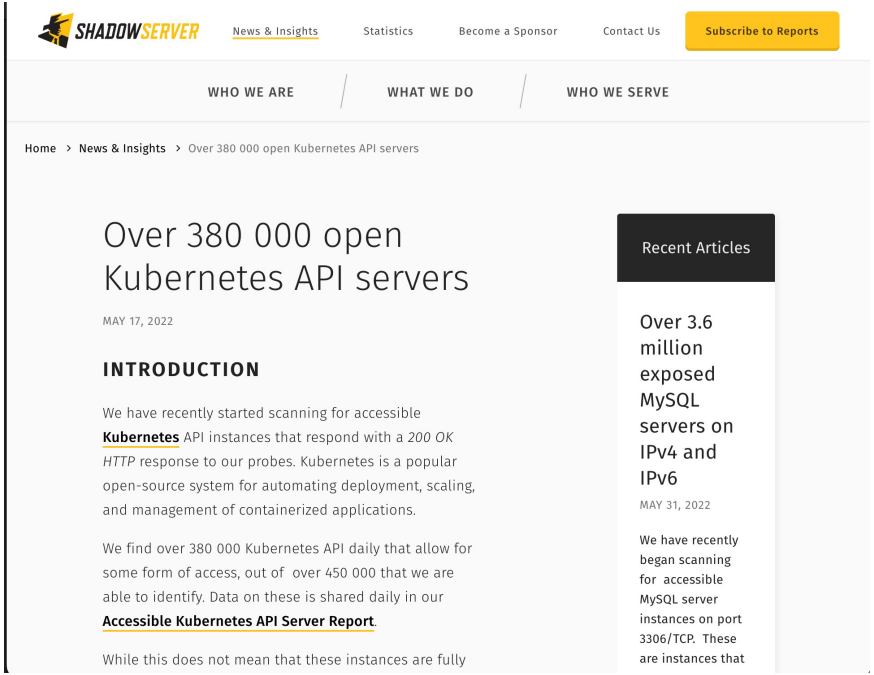
- RFC 4493 – defines AES-CMAC (128 bit)

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

Trend Lines to watch closely for Government



National Security Agency
Cybersecurity Technical Report

Deploying Secure Unified Communications/Voice and Video over IP Systems

June 2021

National Security Agency | Cybersecurity Information

Embracing a Zero Trust Security Model

Executive Summary

As cybersecurity professionals defend increasingly dispersed and complex enterprise networks from sophisticated cyber threats, embracing a Zero Trust security model and the mindset necessary to deploy and operate a system engineered according to Zero Trust principles can better position them to secure sensitive data, systems, and services.

Administration Priorities C

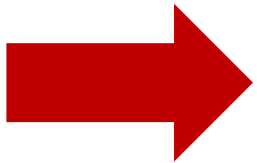
BRIEFING ROOM

Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems

JANUARY 19, 2022 • PRESIDENTIAL ACTIONS

NATIONAL SECURITY MEMORANDUM/NSM-8

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE SECRETARY OF DEFENSE
THE ATTORNEY GENERAL
THE SECRETARY OF COMMERCE
THE SECRETARY OF ENERGY
THE SECRETARY OF HOMELAND SECURITY
THE DIRECTOR OF THE OFFICE OF MANAGEMENT AND



(ii) Within 60 days of the date of this memorandum, the head of each executive department or agency (agency) that owns or operates an NSS shall, consistent with its statutory authority:

(A) update existing agency plans to prioritize resources for the adoption and use of cloud technology, including adoption of Zero Trust Architecture as practicable;

(B) develop a plan to implement Zero Trust Architecture, which shall incorporate, as appropriate:

(1) NIST Special Publication 800-207 Guidance (Zero Trust Architecture);

(2) CNSS instructions on Zero Trust Reference Architectures; and

NEWS | May 4, 2022

President Biden Signs Memo to Combat Quantum Computing Threat

FORT MEADE, Md. — The White House announced today that President Joe Biden has signed a National Security Memorandum (NSM) aimed at maintaining U.S. leadership in quantum information sciences and to mitigate the risks of quantum computing to the Nation's security.

"Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems" - also known as NSM-10 - directs U.S. Government agencies to migrate vulnerable cryptographic systems to quantum-resistant cryptography as part of multi-year effort. As the National Manager for National Security Systems, the Director of NSA will oversee this process across the 50-plus government departments and agencies using National Security Systems (NSS) - systems that contain classified information or are otherwise critical to military or intelligence operations.

A quantum computer of sufficient size and sophistication - also known as a cryptanalytically relevant quantum computer - will be capable of breaking much of the public-key cryptography used on digital systems across the United States and the world.

(A) Within 30 days of the date of this memorandum, the NSA shall review CNSS Policy 15 and provide to CNSS any updates or modifications regarding the approved list of commercial national security algorithms (CNSA).

(B) Within 60 days of the date of this memorandum, the NSA shall revise and make available to Chief Information Officers the CNSS Advisory Memorandum 01-07 (Information Assurance Cryptographic Equipment Modernization) and any associated enclosures and relevant references regarding modernizati g, use of unsupported encryption, approved mission unique protoc m resistant protocols, and planning for use of quantum resistant cr y where necessary.

(C) Within 90 d date of this memorandum, CNSS shall identify and prioritize f all cryptographic-related policies, directives, and issuanc SS shall provide to the Secretary of Defense, the Director of Nationa nce, and the National Manager a timeline, not to exceed 6 mon suance of these policies, as appropriate.

(D) Within 180 day the date of this memorandum, agencies shall identify any instances of encryption not in compliance with NSA-approved Quantum Resistant Algorithms or CNSA, where appropriate in accordance with section 1(b)(iv)(A) and (B) of this memorandum, and shall report to the National Manager, at a classification level not to exceed TOP SECRET//SI //NOFORN:

CISCO SECURE

Security Reference Architecture

TALOS — Threat Intelligence | Malware Analytics | Actionable Intelligence | Unmatched Visibility | Collective Responses

Security Operations

SECURE X (XDR)

- Managed Detection and Response Services
- Security, Orchestration, Automation and Response
- Incident Response and Remediation Services
- Threat Visibility & Hunting
- Device Insights
- Kenna Vuln Mgmt
- Secure Cloud Insights
- 3rd Party Integrations

User/Device Security

ZERO TRUST

Adaptive MFA | Passwordless | Trust

Duo Secure Access

Secure E-mail

SASE/REMOTE WORKER

Unified Client | EDR | Cloud Managed

Cisco Secure Client

- VPN
- Posture
- Telemetry
- Threat
- Query

ThousandEyes (Visibility)

Device Mgmt

Meraki SM OS, App Control

Network Security

Cloud Edge

SECURE ACCESS SERVICE EDGE (SASE) | ZERO TRUST

Threat Protection | Secure Access Control | Managed Remote Access

PRIVATE CLOUD EDGE (MSP or CUSTOMER)

Reliable | Scalable | Flexible

Umbrella/Duo

- ZTNA
- DNS-layer security
- Secure web gateway
- L7 firewall + IPS
- Cloud access security broker/ shadow IT
- RAaaS
- SSL decryption
- Remote browser Isolation
- Data loss prevention
- Cloud malware detection

SDWAN

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes
- Cloud DDoS,WAF

On-Premises

SASE/SDWAN

Scalable | Flexible | Visibility | Comprehensive Security

Network Edge

- Meraki SDWAN
- SDWAN by Viptela
- Secure Firewall
- ThousandEyes

IoT/OT SECURITY

Secure Critical Infrastructure | Unified IT and OT

- Industrial Router
- Industrial Firewall
- Industrial Switch/AP
- Cyber Vision
- ISE TrustSec

ZERO TRUST

Segmentation | Identity and Context | Profiling | Containment | Encrypted Visibility

- Security Analytics and Logging
- Secure Firewall
- DuoCloud SSO+IDP
- Network Gateway
- Secure DDoS
- Meraki Full Stack
- Secure Network Analytics
- Secure Web Appliance
- ISE TrustSec
- Cisco DNA Center

Application Security

ZERO TRUST

Policy | API Security
Application Segmentation
Run-time Application Security

Application Security Stack

- Cloud Native Security
- APIC
- Secure Workload
- Secure Application by AppDynamics

App Observability | Detection | Response

- Hybrid Private
- Public Cloud
- Secure Cloud Analytics
- Secure Firewall
- ThousandEyes
- Secure DDoS, WAF/Bot

If you need to run Certified Firewalls

Current Certification Effort: FTD 7.0 /ASA 9.16 / FX-OS 2.10

Feature / Requirement	Sales Priority	Required by CC, FIPS, DoD, IPv6 for Test	Timeframe needed	Implementation Status - FP/FTD	Implementation Status - ASA
FIPS 140-3	1	Yes - FIPS	Begins 9/2020 - mandatory 9/2021	Support additional documentation for GCT	Support additional documentation for GCT
ACVP	1	Yes - FIPS	mandatory 7/1/20	Test State - FTD has it tested	Follow the same for ASA and FX-OS
SP800-90B	1	Yes - FIPS	mandatory 11/20	FP/FX-OS handling with Intel Docs	ASA has to deal with second entropy source - Octeon, ACT2
Gapping for new IPv6/RL profiles	1	Yes - IPv6, DoD	Spring 2020	In progress	
Gapping for FIPS 140-3	1	Yes - FIPS	Spring 2020	Steve provided mini-checklist - increases work for GCT and the lab	Steve provided mini-checklist - increases work for GCT and the lab
PLR on FDM	1		Fall 2019	Backporting to FTD 6.4 from 6.6 - will be there for 7.0	N/A
Virtual Routing and Forwarding (VRF)			Fall 2019	Available in FTD 6.6	N/A
ASA Appliance Mode on 1k			Fall 2019	N/A	Available in 9.13
ASA Multi-Instance				N/A	?? - Need Business case
RFC 5246 - TLS1.2	1	Using in CC	Now	Already there	Already there
RFC 8200 - For IPv6 also RFC's 8201, 6437, 5942, 6980, 4191, 8106, 7217, 6724, 5952, 7136, 7346, 7371	1	Yes - IPv6	Spring 2021	In progress for gapping	In progress for gapping
RFC 7030 - Enrollment over Secure Transport	1			Committed - in progress	Committed - in progress
RFC 6187 - Cisco SSH – standardized across all products - x.509 certificates	1			Cisco SSH is present - not sure if this is enabled	Uses custom SSH – Need to switch to CiscoSSH
RFC 8573 - NTPv4 w/AES-CMAC*	1			Committed - in progress	Committed - in progress
RFC 8446 – TLS 1.3				Included in FOM7.2 - need clear definition of what is expected for TLS 1.3 - library planned for 7.0	Included in FOM7.2 -
RFC 6931 - FIPS 202 - SHA-3					
RFC 7366 - Encrypt-then-MAC for Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)			ASAP		Included in FOM 7.2 customization work from Marvell – Fall 2021 – pushed out for ASA – no Gov request associated
RFC 8332 - Use of RSA Keys with SHA-256 and SHA-512 in the Secure Shell (SSH) Protocol (Client and Server authent. For SSH)			ASAP		
RFC 8268 - More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH)			ASAP		
RFC 6668 - SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol			ASAP		
RFC 8784 – Mixing Preshared Keys (IKEv2) for Post-Quantum Security		Requests coming from the NSA	ASAP		

Firewall Certification Plan – 2022

	Spring 2019	Fall 2019	Spring 2020	Fall 2020	Spring 2021	Fall 2021	Spring 2022
	Certified FIPS, CC, DoDIN APL, USGv6	Skip	Skip	Skip	Certified FIPS, CC, DoDIN APL, USGv6	Skip	Skip
ASA	9.12.x	9.13.x	9.14.x	9.15.x	9.16.x	9.17.x	9.18.x
FTD	6.4.x	6.5.x	6.6.x	6.7.x	7.0.x (was 6.8.x)	7.1.x	7.2.x
FMC	6.4.x	6.5.x	6.6.x	6.7.x	7.0.x(was 6.8.x)	7.1.x	7.2.x
FDM	6.4.x	6.5.x	6.6.x	6.7.x	7.0.x(was 6.8.x)	7.1.x	7.2.x
FX-OS	2.6.x	2.7.x	2.8.x	2.9.x	2.10.x	2.11.x	2.12.x
HW	FMC1600, 2600, 4600, ,4115,4125,4145,9300 SM40, SM48, SM56, FPR1010, 1120, 1140 (FTD only)	FPR1010, 1120, 1140 (ASA) *FPR 1150 (ASA and FTD)	FPR4112*		*Certify FPR1150 and FPR4112	FPR 2k refresh available** (Tufnell Park – FPR 3k)	
Key Fed Features	U-PLR, PLR on FDM (backport), M5 HW, FTD Multi-Instance	ASA Appliance mode on 1k	VRF, PLR on FDM	ASA MI?	RFC7030, RFC8573, IPv6 RFC8200, DoD IN IPv6 only, TLS 1.3		TBD

Firewall Certification Plan – Beyond 2022

	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 to be backported to NGFW Spring 2021 Release MR	TBD	RFC 6668, RFC 8268, RFC 8332, RFC 8784	TBD	TBD

*Uncommitted

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	Complete 09/22/2021	Complete 02/07/2022	Requested 2/24/22		
FPR 1k - 1010, 1120, 1140, 1150 - running FTD 7.0	11290	March 2022	In Review			
FPR 2k - 2110, 2120, 2130, 2140 - running ASA 9.16	11255	Complete 09/22/2021	Complete 02/07/2022	Requested 2/24/22		
FPR 2k - 2110, 2120, 2130, 2140 - running FTD 7.0	11290	March 2022	In Review			
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	Complete 09/22/2021	Complete 03/02/2022	Requested 3/17/22		
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	March 2022	In Review			
ASA - 5506, 5508, 5516, ISA 3000 - running ASA 9.16	11257	Complete 09/22/2021	Complete 01/31/2022	Requested 2/24/22		
ASAv - 9.16	11257	Complete 09/22/2021	Complete 01/31/2022	Requested 2/24/22		
ASA - 5508, 5516, ISA3000 - running FTD 7.0	11300	March 2022	In Review			
FTDv - 7.0	11300	March 2022	In Review			
NGIPSv - 7.0		March 2022	In Review			
AnyConnect 4.9 for iOS	11205	Complete 01/22/2021	Complete 06/08/2021	Complete 07/12/2021		
AnyConnect 4.10 for Android	11127	Complete 05/19/2021	Complete 09/15/2021	Requested 9/20/21		
AnyConnect 4.10 on Windows	11126	Complete 05/19/2021	Complete 09/15/2021	Requested 9/20/21		
AnyConnect 4.10 on Linux	11289	Complete 01/28/2022	Complete 03/08/2022	Requested 3/17/22		
Stealthwatch (Secure Network Analytics) 7.4		May 2022				
Identity Services Engine (ISE) 3.1	11271	Complete 11/16/21	Complete 03/29/2022			

** Typically 2-3 months after Check-in Package is submitted to NIAP by the CC Lab

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

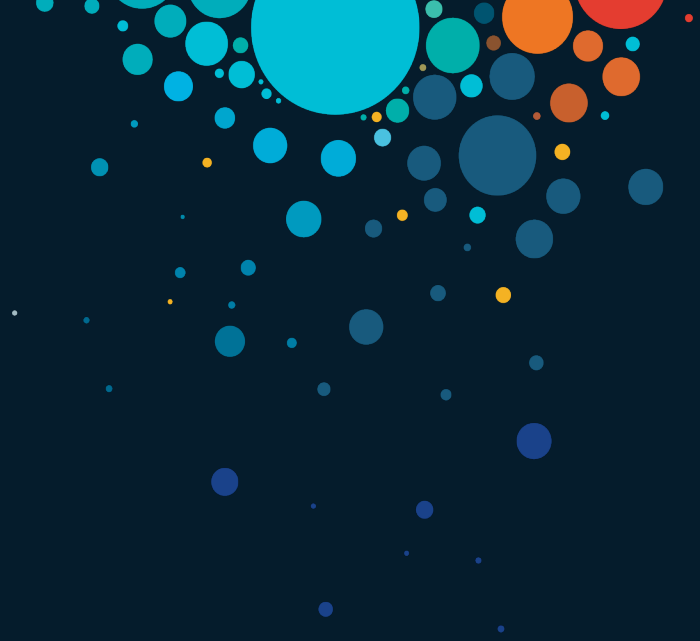
https://tools.cisco.com/security/center/resources/securing_nx_os.html

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



Questions?

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

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

#CiscoLiveAPJC

The bridge to possible

Thank you