

The logo for Digital Scepter, with "digital" in white and "scepter" in blue. The background is a modern office interior with a white ceiling, black beams, and several long, rectangular pendant lights hanging from the ceiling. The lighting is dim, with the pendant lights providing the primary illumination.

digital**scepter**

# PAN-OS Best Practices Workshop

**ZACHRY SUM - DIRECTOR OF TECHNICAL SERVICES, DIGITAL SCEPTER**

**SEAN DAVIS - SYSTEMS ENGINEER**

**COLEMAN NUGENT - SYSTEMS ENGINEER**

**JON ROBINSON - PRESIDENT, DIGITAL SCEPTER**

**May 1st, 2024**



# Service Catalog

---

- Firewall migrations
- Firewall operations - mass upgrades, backups, change/remove/add
- Firewall Healthchecks
- Panorama design
- Zero Trust Network Access
- Network Segmentation
- MFA
- SSL Decryption
- Inbound SSL Inspection
- Remote Access (“Always on”)
- Securing Cloud infrastructure
- Dual ISP redundancy
- Network engineering
- Endpoint Security/EDR/MDR



# Contracts

---

- CMAS
- NASPO
- SPURR
- OMNIA Partners





# Vendors

- 
- Palo Alto Networks
  - CrowdStrike
  - SentinelOne
  - Okta
  - Arista
  - Juniper
  - HPe/Aruba
  - AWS
  - Microsoft/Azure
  - Proofpoint
  - Zscaler
  - Gigamon
  - Rapid7
  - Knowbe4
  - Netskope

# Agenda

---

- **Advanced Subscriptions** - difference compared to original subscriptions
- **Best Practices** - recommendations for different features across the platform
- **Zero Trust** - defined and how to configure
- **SSL Decryption** - breakdown of SSL outbound and inbound inspection
- **Network Segmentation** - brief overview of benefits to network segmentation and methods of implementation
- **GUI Walkthrough/Demos** - Review location of configuration items discussed and feature demonstrations

# Advanced Subscriptions

---

# Advanced Subscriptions and Machine Learning

---

- Palo Alto has a cloud-native system of machine learning models that they can train and retrain using the massive amounts of data they collect from all of the 85,000+ customer around the globe and 42,000+ Wildfire users
- These models are focused on certain threats, e.g. command and control, SQLi, social engineering, etc.
- The architecture takes advantage of Intel 3rd gen Xeon CPUs and ML software development frameworks
- This ML powered analysis is incorporated in the cloud threat analysis and inline on the firewall in aspects of Advanced Wildfire, Advanced URL, Advanced Threat and DNS Security

# Advanced URL Filtering

---

- Adds inline analysis for javascript exploits and phishing attacks
- Adds inline analysis of the SSL handshake to block traffic sooner based on SNI
- Delivered in real-time, without impacting the user
- These will be expanded in the future

Advanced URL Filtering will uncover attackers that were cloaking their attacks from web-crawlers and attacks that use new and unknown domains and URLs for phishing attacks.



# Advanced URL Filtering

### URL Filtering Profile ?

Name

Description

Shared

Disable override

Categories | URL Filtering Settings | User Credential Detection | HTTP Header Insertion | **Inline Categorization**

Enable local inline categorization

Enable cloud inline categorization

#### Exceptions

| <input type="checkbox"/> | CUSTOM URL CATEGORY/EDL <span>^</span> |
|--------------------------|--|
|--------------------------|--|

+ Add - Delete

OK Cancel

# Advanced URL Filtering

---

- This will obviously be enhanced by SSL decryption.
- Palo Alto has risk-categories now that can be used to selectively apply SSL decryption short of a complete roll-out. For example, perform SSL Decryption on high and medium risk URL categories only.



- Previously malicious and is now benign; 30-days
- Bulletproof ISP hosted & IPs from "bad" ASNs
- Suspect by association



- Previously confirmed high risk; 60-days
- Online-storage-and-backup by default



- Everything else!
- Benign activity for at least 90-days (or no events of malicious activity ever)

# Advanced Threat Prevention

---

- Advanced Threat Prevention is integrated with Palo Alto's cloud-based threat analysis infrastructure, like Advanced URL filtering
- The ML-Models now run deep-learning on live traffic
- First ML-models focus on command-and-control (C2) tactics like those used by Cobalt Strike. Stops 96% of these new tactics. 48% improvement over regular TP tactics
- PAN-OS Nova (11.0) adds ML models to focus on injection attacks. 90% of attacks stopped on unpatched systems and 60% improvement on 0-day injection attacks.
- ML models have to be trained. Palo Alto has the largest pile of threat analysis thanks to Wildfire and a huge customer base. The cloud security infrastructure will be improved with more threat models in the future.

# Advanced Threat Prevention

---

- Unknown C2 detection is focused on http, ssl, unknown-tcp, and unknown-udp apps

# Advanced Threat Prevention

---

<https://www.bleepingcomputer.com/news/security/alleged-source-code-of-cobalt-strike-toolkit-shared-online/>

- Cobalt Strike source code leaked in 2020. This allowed anyone to more easily fire up attack networks, command-and-control servers, and distribute ransomware
- Cobalt Strike was used in multiple attacks including Solarwinds, Colonial Pipeline, Microsoft Exchange and Kaseya.
- Cobalt Strike is evasive and makes it easy to perform zero-day exploits
- Attackers use Cobalt Strike and other tools to automate attacks that look like normal traffic to old methods of Threat Prevention

# Advanced Threat Prevention

---

## Action plan:

- License Advanced Threat Prevention
- Enable inline ML models on anti-spyware and vulnerability protection security profiles
- Enable outbound/inbound SSL Decrypt to ensure threat prevention is applied to encrypted traffic



# Advanced Threat Prevention

### Anti-Spyware Profile

Name:

Description:

Shared  
 Disable override

Signature Policies | Signature Exceptions | DNS Policies | DNS Exceptions | **Inline Cloud Analysis**

Enable cloud inline analysis

Available Analysis Engines

| MODEL                                    | DESCRIPTION   | ACTION     |
|--|---|------------|
| HTTP Command and Control detector        | Machine Learning engine to detect HTTP based command and control traffic        | reset-both |
| HTTP2 Command and Control detector       | Machine Learning engine to detect HTTP2 based command and control traffic       | reset-both |
| SSL Command and Control detector         | Machine Learning engine to detect SSL based command and control traffic         | reset-both |
| Unknown-TCP Command and Control detector | Machine Learning engine to detect Unknown-TCP based command and control traffic | reset-both |
| Unknown-UDP Command and Control detector | Machine Learning engine to detect Unknown-UDP based command and control traffic | reset-both |

Exclude from Inline Cloud Analysis

EDL URL ^

IP ADDRESS ^

# Advanced Threat Prevention

### Vulnerability Protection Profile

Name:

Description:

Shared  
 Disable override

Rules | Exceptions | **Inline Cloud Analysis**

Enable cloud inline analysis

Available Analysis Engines

| MODEL             | DESCRIPTION  | ACTION     |
|-------------------|--|------------|
|                   | attacker inserts SQL queries into an applications request  |            |
| Command Injection | Detects a common hacking technique that allows an attacker to execute arbitrary operating system (OS) commands on the server | reset-both |

Exclude from Inline Cloud Analysis

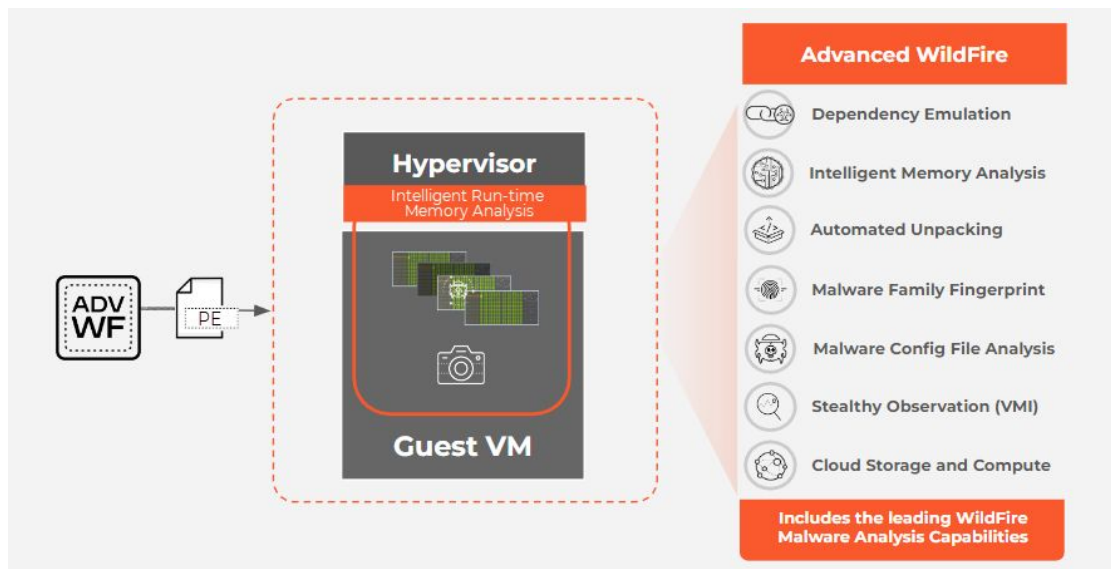
| <input type="checkbox"/> EDL URL ^ | <input type="checkbox"/> EDL IP ^ |
|------------------------------------|-----------------------------------|
|                                    |                                   |

OK Cancel

# Advanced Wildfire

---

- Adds Intelligent Run-time Memory Analysis to Wildfire submissions



# Best Practices

---

# Security Profiles

---

- Create security profile groups based on direction of traffic flow, e.g. inbound, outbound, or internal traffic
- Likewise, create security profile groups based on direction and attach these to appropriate policies
- Exceptions on security profiles should be made as specific as possible to avoid broadly disabling protections

# Antivirus

- Reset-both should be default for http, http2, ftp, and smb
- Reset-both can and should be set for imap, pop3, and smtp if it won't interfere with corporate mail flow–this should be handled by spam filter so you don't lose quarantine capability
- Signature Action column requires TP or advanced TP subscription, Wildfire Action columns require WF subscription

Antivirus Profile ⓘ

Name

Description

Shared

Disable override

**Action** | Signature Exceptions | WildFire Inline ML

Enable Packet Capture

Decoders

| PROTOCOL ^ | SIGNATURE ACTION | WILDFIRE SIGNATURE ACTION | WILDFIRE INLINE ML ACTION |
|------------|------------------|---------------------------|---------------------------|
| ftp        | reset-both       | reset-both                | reset-both                |
| http       | reset-both       | reset-both                | reset-both                |
| http2      | reset-both       | reset-both                | reset-both                |
| imap       | alert            | alert                     | alert                     |
| pop3       | alert            | alert                     | alert                     |
| smb        | reset-both       | reset-both                | reset-both                |
| smtp       | alert            | alert                     | alert                     |



# Anti-Spyware

- Reset-both should be used for critical, high, and medium
- Default (not alert) should be set for low and informational
- This requires Threat Prevention or Advanced Threat Prevention subscription

Anti-Spyware Profile ? ☰

Name

Description

Shared

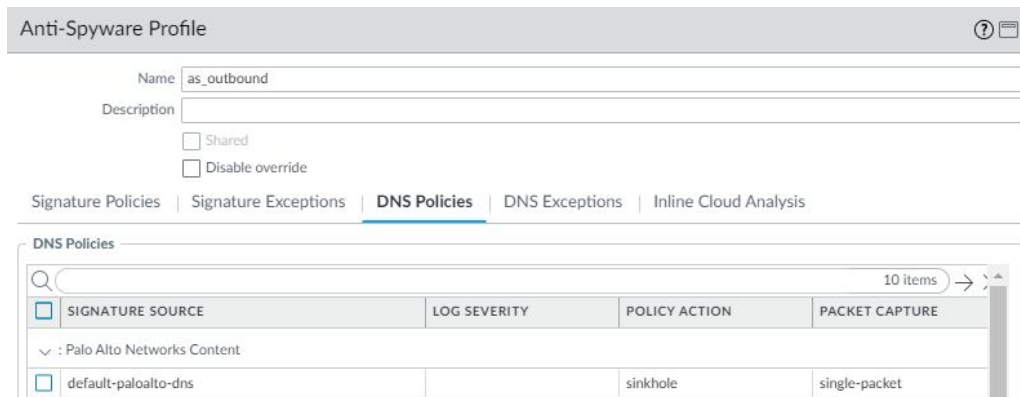
Disable override

**Signature Policies** | [Signature Exceptions](#) | [DNS Policies](#) | [DNS Exceptions](#) | [Inline Cloud Analysis](#)

| <input type="checkbox"/> | POLICY NAME                | SEVERITY                   | ACTION     | PACKET CAPTURE |
|--------------------------|----------------------------|----------------------------|------------|----------------|
| <input type="checkbox"/> | Block-Critical-High-Medium | high<br>critical<br>medium | reset-both | single-packet  |
| <input type="checkbox"/> | Default-Low-Info           | low<br>informational       | default    | disable        |

# Anti-Spyware

- Default-paloalto-dns signature source should be set to sinkhole. Block is also okay here, but sinkhole can offer additional visibility into infected endpoints on your network
- This requires Threat Prevention or Advanced Threat Prevention subscription



The screenshot shows the configuration page for an Anti-Spyware Profile. The profile name is 'as\_outbound'. Below the name and description fields, there are two checkboxes: 'Shared' and 'Disable override', both of which are unchecked. The 'DNS Policies' tab is selected, showing a table of 10 items. The table has four columns: 'SIGNATURE SOURCE', 'LOG SEVERITY', 'POLICY ACTION', and 'PACKET CAPTURE'. The first row is expanded to show 'Palo Alto Networks Content'. The second row shows 'default-paloalto-dns' with a policy action of 'sinkhole' and a packet capture of 'single-packet'.

| SIGNATURE SOURCE           | LOG SEVERITY | POLICY ACTION | PACKET CAPTURE |
|----------------------------|--------------|---------------|----------------|
| Palo Alto Networks Content |              |               |                |
| default-paloalto-dns       |              | sinkhole      | single-packet  |

# URL Filtering

---

At a minimum, it is recommended to block the following URL categories:

- Adult
- Command-and-control
- Copyright-infringement
- Dynamic-dns
- Encrypted-dns
- Extremism
- Grayware
- Hacking
- Malware
- Parked
- Phishing
- Proxy-avoidance-and-anonymizers
- Ransomware
- Unknown (should review unknown URL logs prior to blocking this category)

# URL Filtering

---

A note on blocking unknown URLs:

This is a great way to block new URLs that phishing attacks are using, but any of your apps using IP addresses instead of domain names may be categorized as unknown. Public sites that utilize source-based whitelisting will also show as unknown. Run a report ahead of time to see what this will block and make adjustments to security profiles to except them. Using separate profiles for internet traffic from datacenter traffic is recommended.

# URL Filtering

---

It is recommended to consider blocking these URL categories:

- Newly-registered-domain
- Questionable

# URL Filtering

---

It is recommended to alert on the remaining URL categories:

**Important Note:** Real-time-detection (requires Advanced URL sub) should be set to alert



# URL Filtering

- Log container page only should be turned off if you want to maximize visibility
- HTTP Header Logging should be used if there are proxies on the network

### URL Filtering Profile ?

Name

Description

Shared

Disable override

Categories | **URL Filtering Settings** | User Credential Detection | HTTP Header Insertion | Inline Categorization

Log container page only

Safe Search Enforcement

**HTTP Header Logging**

User-Agent

Referer

X-Forwarded-For

# URL Filtering

- Credential Theft Prevention should be enabled utilizing domain credential filter
- This requires a Server 2019 RODC on your network and works best in tandem with SSL Decryption

### URL Filtering Profile ?

Name

Description

Shared

Disable override

Categories | [URL Filtering Settings](#) | **[User Credential Detection](#)** | [HTTP Header Insertion](#) | [Inline Categorization](#)

**User Credential Detection**

Use Domain Credential Filter

**Log Severity**

Valid Username Detected Log Severity

# URL Filtering

---

## Action plan:

- Make sure categories are not set to 'allow' (use 'alert' instead)
- Make sure any rules that permit traffic to leave your network have your outbound security profile group applied
- Leverage User-ID groups for permitting varying levels of internet access
- Enable Credential Theft Prevention to further reduce risk of phishing attacks and password reuse

# File Blocking

---

At a minimum, it is recommended to block the following file types:

- Chm - Microsoft Compiled HTML Help file
- Hlp - Windows Help file
- Multi-level-encoding - File that's been compressed 4+ times
- Ocx - Windows ActiveX Control file
- Scr - Windows screensaver file
- Torrent

Everything else should be set to alert

# Wildfire

- Forward all supported file types to Wildfire for analysis
- Wildfire submission isn't necessarily required for internal traffic, although there are benefits

WildFire Analysis Profile ?

Name: wf\_standard

Description:

Shared

Disable override

| NAME        | APPLICATIONS | FILE TYPES | DIRECTION | ANALYSIS     |
|-------------|--------------|------------|-----------|--------------|
| Forward-All | any          | any        | both      | public-cloud |

+ Add - Delete

OK Cancel

# Wildfire

- Wildfire Signature action and inline ML action should be set identically to your antivirus signature action
- Wildfire Inline ML models should all be enabled

Antivirus Profile ?

Name

Description

Shared

Disable override

**Action** | Signature Exceptions | WildFire Inline ML

Enable Packet Capture

Decoders

| PROTOCOL ^ | SIGNATURE ACTION | WILDFIRE SIGNATURE ACTION | WILDFIRE INLINE ML ACTION |
|------------|------------------|---------------------------|---------------------------|
| ftp        | reset-both       | reset-both                | reset-both                |
| http       | reset-both       | reset-both                | reset-both                |
| http2      | reset-both       | reset-both                | reset-both                |
| imap       | alert            | alert                     | alert                     |
| pop3       | alert            | alert                     | alert                     |
| smb        | reset-both       | reset-both                | reset-both                |
| smtp       | alert            | alert                     | alert                     |

Antivirus Profile ?

Name

Description

Shared

Disable override

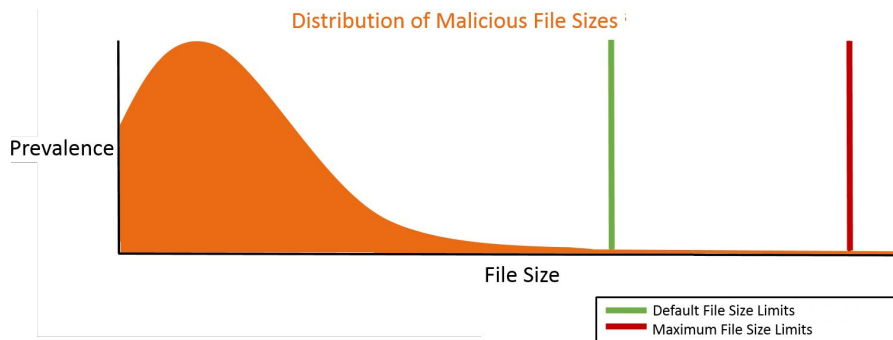
**Action** | Signature Exceptions | **WildFire Inline ML**

Available Models 6 items → ×

| MODEL               | DESCRIPTION  | ACTION SETTING                        |
|---------------------|--|---------------------------------------|
| Windows Executables | Machine Learning engine to dynamically identify malicious PE files                           | enable (inherit per-protocol actions) |
| PowerShell Script 1 | Machine Learning engine to dynamically detect malicious PowerShell scripts with known length | enable (inherit per-protocol actions) |
| PowerShell Script 2 | Machine Learning engine to dynamically detect malicious PowerShell scripts without known     | enable (inherit per-protocol actions) |

# Wildfire

- PAN recommends setting file size limits to default values based on observed distribution of malware



| FILE TYPE | PAN-OS 9.0 AND LATER FILE-FORWARDING MAXIMUM SIZE RECOMMENDATIONS | PAN-OS 8.1 FILE-FORWARDING MAXIMUM SIZE RECOMMENDATIONS |
|-----------|---|---|
| pe        | 16MB  | 10MB  |
| apk       | 10MB  | 10MB  |
| pdf       | 3,072KB   | 1,000KB   |
| ms-office | 16,384KB  | 2,000KB   |
| jar       | 5MB   | 5MB   |
| flash     | 5MB   | 5MB   |
| MacOSX    | 10MB  | 1MB   |
| archive   | 50MB  | 10MB  |
| linux     | 50MB  | 10MB  |
| script    | 20KB  | 20KB  |

# Wildfire

---

- Allow forwarding of decrypted content
  - Device > Setup > Content-ID

Content-ID Settings ?

Allow forwarding of decrypted content

Extended Packet Capture Length (packets)

Forward segments exceeding TCP App-ID inspection queue

Forward segments exceeding TCP content inspection queue

Forward datagrams exceeding UDP content inspection queue

Allow HTTP partial response



# DNS Security

---

- DNS is fundamental to using any network
- Controlling DNS you can stop attacks at the beginning of the attack lifecycle but also in the middle and the end
- Palo Alto had a list of bad domains on the firewall based on intel from Wildfire, etc. but DNS Security now moves it to the cloud-based security architecture, which means the list size is basically infinite and takes advantage of the ML model architecture like the other subscriptions

# DNS Security

---

- More than just blocking bad domains
- Looks at malicious usage of the protocol, e.g. tunneling
- Can see all DNS traffic through the box, not just from systems configured to use your approved DNS servers

# DNS Security

## Callback Domains

DNS-based indirection for reliable phone-home

Malware & C2 Domains

Botnet Domains

Fast-flux Domains



Random DGA

Dictionary DGA

## High Risk Domains

Proactive protection from likely malicious domains

Grayware

Newly Registered Domains

Parked Domains

Proxy Avoidance

Dynamic DNS

Predictive Detection

NEW

Strategically Aged Domains

## DNS Record Attacks

Domain takeovers through DNS zone hacks and abuse

Domain Squatting

Dangling DNS

NEW

Compromised DNS Zone

NEW

Wildcard DNS

NEW

CNAME Cloaking

## DNS Protocol Attacks

DDoS, exploitation, and lateral movement

DNS Rebinding

NXNSAttack

## Covert Channels

Abuse of DNS protocol for stealthy data theft and C2

DNS Tunneling

Ultra-slow DNS Tunneling

NEW

DNS Infiltration

★ Industry First

digitalscepter

# DNS Security

---

- Since malicious DNS requests are indicators of compromise, it's a good input for automating response, e.g. adding the IP address to a block list for limited network access, send to endpoint tools, etc.

# DNS Security

### Anti-Spyware Profile

Name: Sinkhole

Description:

Signature Policies | Signature Exceptions | **DNS Policies** | DNS Exceptions | Inline Cloud Analysis

#### DNS Policies

10 items

| <input type="checkbox"/> | SIGNATURE SOURCE            | LOG SEVERITY            | POLICY ACTION   | PACKET CAPTURE   |
|--------------------------|-----------------------------|-------------------------|-----------------|------------------|
| ∨                        | Palo Alto Networks Content  |                         |                 |                  |
| <input type="checkbox"/> | default-paloalto-dns        |                         | sinkhole        | extended-capture |
| ∨                        | DNS Security                |                         |                 |                  |
| <input type="checkbox"/> | Ad Tracking Domains         | default (informational) | default (allow) | disable          |
| <input type="checkbox"/> | Command and Control Domains | default (high)          | default (block) | disable          |
| <input type="checkbox"/> | Dynamic DNS Hosted Domains  | default (informational) | default (allow) | disable          |
| <input type="checkbox"/> | Grayware Domains            | default (low)           | default (block) | disable          |
| <input type="checkbox"/> | Malware Domains             | default (medium)        | default (block) | disable          |
| <input type="checkbox"/> | Parked Domains              | default (informational) | default (allow) | disable          |
| <input type="checkbox"/> | Phishing Domains            | default (low)           | default (block) | disable          |

#### DNS Sinkhole Settings

Sinkhole IPv4: Palo Alto Networks Sinkhole IP (sinkhole.paloaltonetworks.com)

Sinkhole IPv6: IPv6 Loopback IP (::1)

#### Block DNS Record Types

SVCB  HTTPS  ANY

OK Cancel

# External Dynamic Lists

- Make sure you have rules blocking the predefined EDL's inbound and outbound

| <input type="checkbox"/> | NAME  | LOCATION   | DESCRIPTION  | SOURCE  |
|--------------------------|---|------------|--|---|
| ▼ Dynamic IP Lists       |   |            |  |   |
| <input type="checkbox"/> | <a href="#">Palo Alto Networks - Tor exit IP addresses</a>        | Predefined | IP addresses supplied by multiple providers and validated with Palo Alto Networks threat intelligence data as active Tor exit nodes. Traffic from Tor exit nodes can serve a legitimate purpose, however, is disproportionately associated with malicious activity, especially in enterprise environments. | Palo Alto Networks - Tor exit IP addresses        |
| <input type="checkbox"/> | <a href="#">Palo Alto Networks - Bulletproof IP addresses</a>     | Predefined | IP addresses that are provided by bulletproof hosting providers. Because bulletproof hosting providers place few, if any, restrictions on content, attackers can use these services to host and distribute malicious, illegal, and unethical material.   | Palo Alto Networks - Bulletproof IP addresses     |
| <input type="checkbox"/> | <a href="#">Palo Alto Networks - High risk IP addresses</a>       | Predefined | IP addresses that have recently been featured in threat activity advisories distributed by high-trust organizations. However, Palo Alto Networks does not have direct evidence of maliciousness for these IP addresses.  | Palo Alto Networks - High risk IP addresses       |
| <input type="checkbox"/> | <a href="#">Palo Alto Networks - Known malicious IP addresses</a> | Predefined | IP addresses that are currently used almost exclusively by malicious actors for malware distribution, command-and-control, and for launching various attacks.  | Palo Alto Networks - Known malicious IP addresses |

# Device Settings

---

| Check  | Location   | Recommended Setting                    | Default?               |
|--|--|--|------------------------|
| Rematch Sessions                                     | Device > Setup > Session > Session Settings                                    | Enabled                                | Yes (as of PAN-OS 5.0) |
| Management TLS Mode set to TLS 1.3 only              | Device > Setup > Management > General Settings                                 | TLS 1.3 only<br>(1.2 if pre-PAN-OS 11) | No                     |
| Enable log on high DP load                           | Device > Setup > Management > Logging and Reporting > Log Export and Reporting | Enabled                                | No                     |
| Log Admin Activity (sends to a syslog server)        | Device > Setup > Management > Logging and Reporting > Log Export and Reporting | Enabled                                | No                     |
| Forward segments exceeding content inspection queues | Device > Setup > Content-ID > Content-ID Settings                              | Disabled                               | No                     |
| Forward segments exceeding TCP out of order queue    | Device > Setup > Session > TCP Settings  | Enabled                                | No                     |

# Device Settings

---

| Check                        | Location   | Recommended Setting | Default? |
|------------------------------|--|---------------------|----------|
| Log traffic not scanned      | Device > Setup > Content-ID > URL Inline Cloud Categorization<br>Device > Setup > Content-ID > Threat Prevention Inline Cloud Analysis | Enabled             | No       |
| Strip-X-Forwarded-For header | Device > Setup > Content-ID > X-Forwarded-For-Headers  | Enabled             | No       |



# Zero Trust

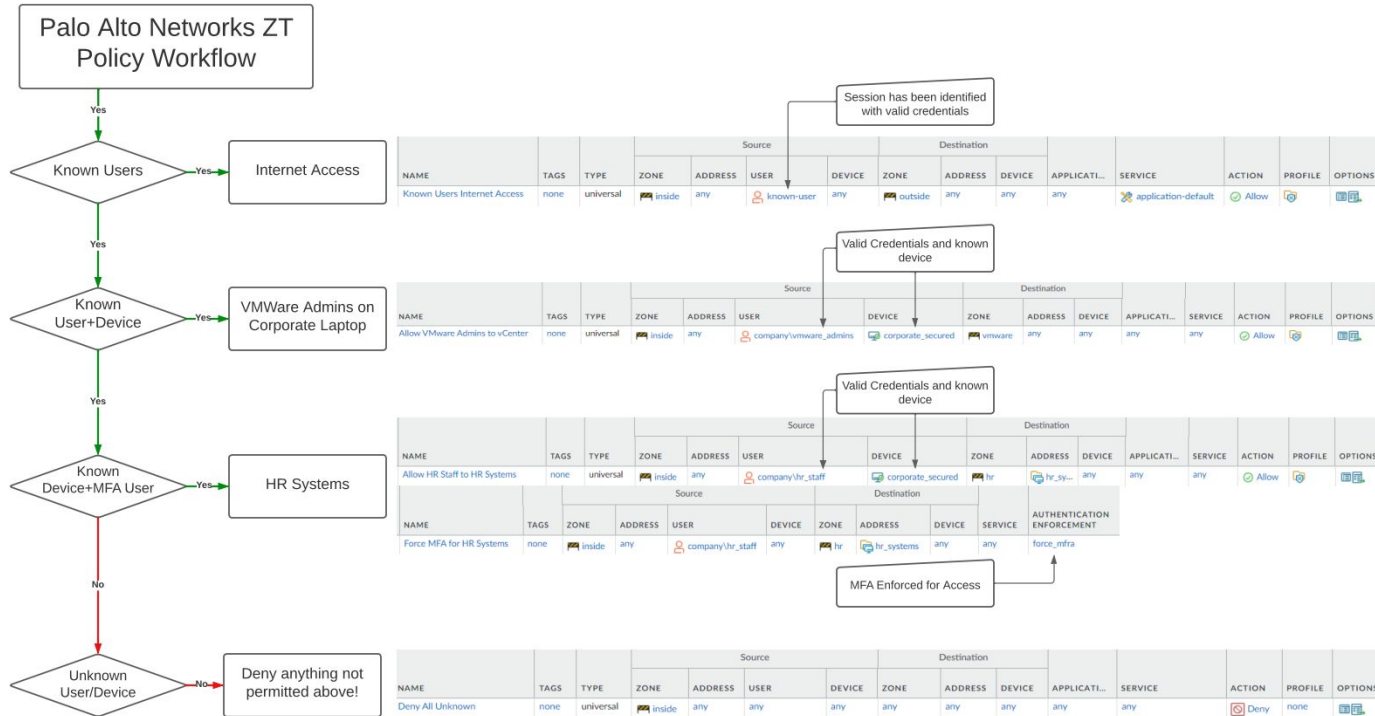
---

# What is Zero Trust?

---

- Zero trust is a concept that no user or device should be inherently trusted, whether inside or outside of a corporate network. Instead **all** traffic should be, by default, dropped. Required traffic flows should then be explicitly permitted based on principles of least privilege. Traffic should be validated against the following:
  - **Known User** - authenticated frequently with multiple factors
  - **Known Device** - corporate managed and secured with next-gen antivirus
  - **Source/Destination** - specific source and destination address
  - **Service** - nailed down for static ports, or application-default for dynamic ports
  - **Application** - static list of applications as required for inbound/internal traffic, application filters for outbound access
  - **URL Category** - an optional match condition that can be used in place of or in conjunction with a destination address

# Zero Trust Policy Flow



# Zero Trust Journey

---

The idea of getting to a zero trust model can be overwhelming. Try to break it into manageable chunks of work. For example:

- Enable inbound inspection and convert inbound rules to use App-id
- Create internet access rules based on application filters
- Add User-ID to policies that enable access to critical systems
- Add MFA to GlobalProtect
- Analyze the rulebase and try to find 3 things that you can change to improve security

# Zero Trust Prioritization

---

1. MFA for remote access
  - Email or SMS alerts for successful logins from outside of the US  
( status eq 'success' ) and ( srcregion neq 'US' ) and (( eventid eq 'portal-auth' ) or ( eventid eq 'gateway-auth' ))
2. Security Profiles
3. User-ID
4. SSL Decryption
5. App-ID
6. Device-ID

# SSL Decryption

---

# SSL Decryption Benefits

---

- App-ID visibility
- Granular app control
- Threat Prevention
- Full URL visibility
- File download/upload visibility

# Types of Decryption

---

- SSL Forward Proxy (Outbound Decryption)
  - Provides the firewall with visibility into encrypted traffic originating from users within your network
- SSL Inbound Inspection (Inbound Decryption)
  - Provides the firewall with visibility into encrypted traffic originating from the internet destined to servers on your network

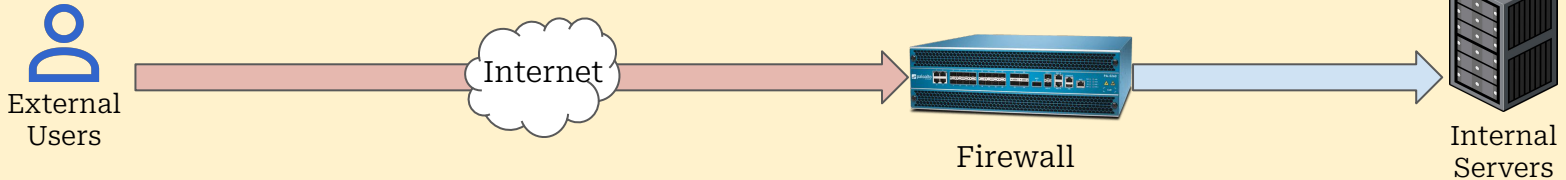


# Inbound vs Outbound

## SSL Forward Proxy (Outbound Decryption)



## SSL Inbound Inspection (Inbound Decryption)



# What the firewall sees *without* decryption

```
.....uJ..l.>k.;;g.....1.....k.}>l.h.>.o0...|.....~  
..".....+./.....,0.  
...../5.....example.com.....  
.....#.....h2.http/1.1.....".  
.....3.k.i...  
X.-DS..!c..>...d.....fG.9.}>...A...Q... }.[G.....Nr}r...6S!y.....5.!,.'...o..E.S.Zte\../...+.....  
.....-.....@.....x.{.t....!.{.....*.bs  
j.S ...k.}>l.h.>.o0...|.....~  
.....O.+.....3.E...A.r...0{.(.....!@.L.....0:.....-.....~....Loep.\.".....<k.T.7v...u....Mm.H|.  
tal.IXB.....a _M[K...!.*...9.....5.U.....^/W.b :r...s.]n.@.....d...5.w....  
.....5..dx..0..O.Lm.....w.yo.....Ep.....c1EL...2.q.f.3.O.t.=C.Y.k.n...fw.r.?9.=T..>.....O~...d,QB.m.kl.a.Q.  
..YUM.y.n...4=.[.g..h...}>.....<.6.&7...".B.T.;L.i.E.<r.""../.Snx.K..  
.rj.zBX.sE.u.....{~.A.Z@L.Y.  
..{....`Ynh..*;;!.....&2.T.V2e.,B....J...^!"v.teC..W'.k....  
..X.L.~NUw....S.Hc"|....7....9._...7A.@.+...F...u.d...6.Q...z.R.5.C.....z_..*D..F....*Ct9J....by.....jh.|.&/E.GfOY]...;-...(kE.a.....  
..s...?....&d.).....C.....e.#3f.a...:D.....U...1...Ut.)?....P.V\ ".....  
.....<...`r3[...._,R.
```

# What the firewall sees *without* decryption

## Detailed Log View

| General  | Source                          | Destination                     |
|--|---------------------------------|---------------------------------|
| Session ID 1487                                | Source User                     | Destination User                |
| Action allow                                   | Source 10.9.20.50               | Destination 10.1.64.50          |
| Action Source from-policy                      | Source DAG                      | Destination DAG                 |
| Host ID  | Country 10.0.0.0-10.255.255.255 | Country 10.0.0.0-10.255.255.255 |
| Application ssl                                | Port 61208                      | Port 443                        |
| Rule Allow Nugent and Sum In Through SDWAAAAAN | Zone sdwan                      | Zone demolition                 |
| Rule UUID 3ba1a9c5-12ce-4945-af72-a1c7e889d9be | Interface ae1.912               | Interface ae1.1646              |

| CAP | RECEIVE TIME ^      | TYPE | APPLICATION | ACTION | RULE                                      | RULE UUID           | BYTES  | SEVERITY      | CATEGORY                   | URL CATEGORY LIST                   | VERDICT | URL                      |
|-----|---------------------|------|-------------|--------|---|---------------------|--------|---------------|----------------------------|-------------------------------------|---------|--------------------------|
|     | 2023/10/10 19:46:57 | end  | ssl         | allow  | Allow Nugent and Sum In Through SDWAAAAAN | 3ba1a9c5-12ce-49... | 230373 |               | computer-and-internet-info |                                     |         |                          |
|     | 2023/10/10 19:46:48 | url  | ssl         | alert  | Allow Nugent and Sum In Through SDWAAAAAN | 3ba1a9c5-12ce-49... |        | informational | computer-and-internet-info | computer-and-internet-info,low-risk |         | demolition.int.digitl... |
|     | 2023/10/10 19:46:48 | url  | ssl         | alert  | Allow Nugent and Sum In Through SDWAAAAAN | 3ba1a9c5-12ce-49... |        | informational | computer-and-internet-info | computer-and-internet-info,low-risk |         | demolition.int.digitl... |
|     | 2023/10/10 19:46:48 | url  | ssl         | alert  | Allow Nugent and Sum In Through SDWAAAAAN | 3ba1a9c5-12ce-49... |        | informational | computer-and-internet-info | computer-and-internet-info,low-risk |         | demolition.int.digitl... |

# What the firewall sees *with* decryption

---

GET /classes/details?id=CS101 DROP TABLE STUDENTS; HTTP/1.1  
Host: example.com  
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:98.0) Gecko/20100101 Firefox/98.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Connection: keep-alive  
Upgrade-Insecure-Requests: 1  
Pragma: no-cache  
Cache-Control: no-cache

HTTP/1.1 200 OK  
Content-Encoding: gzip  
Accept-Ranges: bytes

Age: 460608  
Cache-Control: max-age=604800  
Content-Type: text/html; charset=UTF-8  
Date: Mon, 21 Mar 2022 23:54:11 GMT

# What the firewall sees *with* decryption

## Detailed Log View

| General   | Source  | Destination   |
|---|---|---|
| Session ID 11533<br>Action allow<br>Action Source from-policy<br>Host ID<br>Application web-browsing<br>Rule Allow Nugent and Sum In Through SDWAAAAAN<br>Rule UUID 3ba1a9c5-12ce-4945-af72-a1c7e889d9be<br>Session End Reason threat | Source User<br>Source 10.6.0.100<br>Source DAG<br>Country 10.0.0.0-10.255.255.255<br>Port 53776<br>Zone nugent<br>Interface tunnel3<br>X-Forwarded-For IP 0.0.0.0 | Destination User<br>Destination 10.1.64.50<br>Destination DAG<br>Country 10.0.0.0-10.255.255.255<br>Port 443<br>Zone demolition<br>Interface ae1.1646 |

| PCAP | RECEIVE TIME ^      | TYPE          | APPLICATION  | ACTION     | RULE                                      | RULE UUID          | BYTES | SEVERITY      | CATEGORY                   | URL CATEGORY LIST                   | VERDICT | URL                     |
|------|---------------------|---------------|--------------|------------|---|--------------------|-------|---------------|----------------------------|-------------------------------------|---------|-------------------------|
|      | 2023/10/10 20:03:12 | end           | web-browsing | allow      | Allow Nugent and Sum In Through SDWAAAAAN | 3ba1a9c5-12ce-4... | 83820 |               | computer-and-internet-info |                                     |         |                         |
|      | 2023/10/10 20:01:51 | vulnerability | web-browsing | reset-both | Allow Nugent and Sum In Through SDWAAAAAN | 3ba1a9c5-12ce-4... |       | high          | computer-and-internet-info |                                     |         | demolition.int.digit... |
|      | 2023/10/10 20:01:51 | url           | incomplete   | alert      | Allow Nugent and Sum In Through SDWAAAAAN | 3ba1a9c5-12ce-4... |       | informational | computer-and-internet-info | computer-and-internet-info,low-risk |         | demolition.int.digit... |
|      | 2023/10/10 20:01:51 | url           | web-browsing | alert      | Allow Nugent and Sum In Through SDWAAAAAN | 3ba1a9c5-12ce-4... |       | informational | computer-and-internet-info | computer-and-internet-info,low-risk |         | demolition.int.digit... |

# SSL Forward Proxy - What's Required

---

- Private CA Certificate trusted by all endpoints/browsers
- Periodic exclusions for sites that don't support decryption
  - Certificate pinning
  - Client-cert authentication

# SSL Forward Proxy - Certificate Authority Options

---

- PAN firewall Self-Signed Certificate
  - Less secure, but doesn't require in-house certificate infrastructure
  - Requires distribution of PAN certificate to machines
- Subordinate CA template to PAN firewall from enterprise CA
  - Simple revocation if PAN private key is compromised
  - Does not need to be distributed to domain-joined machines since enterprise CA should already be trusted

# SSL Forward Proxy - What to Decrypt

- Decrypt all URL categories except those that contain sensitive, private data, such as:
  - Financial-services
  - Health-and-medicine
  - Shopping
- Start with a test group as shown below. Only three users are being decrypted. As testing progresses, expand test group

|   | Name                 | Tags | Source  |         |  | Destination   |         | URL Category  | Service | Action     | Type              |
|---|----------------------|------|---|---------|--|---|---------|---|---------|------------|-------------------|
|   |                      |      | Zone  | Address | User   | Zone  | Address |   |         |            |                   |
| 1 | Protect Confidential | none |  inside<br> vpn | any     | any  |  outside | any     | financial-services<br>health-and-medic...<br>shopping | any     | no-decrypt | ssl-forward-proxy |
| 2 | Decrypt Users        | none |  inside<br> vpn | any     |  ds\jrobinson<br> ds\maverick<br> ds\zsum |  outside | any     | any   | any     | decrypt    | ssl-forward-proxy |



# SSL Forward Proxy - Important Settings

---

- Decrypted files should be sent to WildFire
  - Device > Setup > Content-ID > Content-ID Settings

## Content-ID Settings



  Allow forwarding of decrypted content

Extended Packet Capture Length (packets) 

  Forward segments exceeding TCP App-ID inspection queue

  Forward segments exceeding TCP content inspection queue

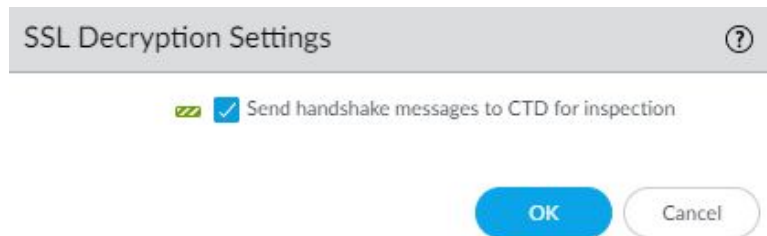
  Forward datagrams exceeding UDP content inspection queue

  Allow HTTP partial response

# SSL Forward Proxy - Important Settings

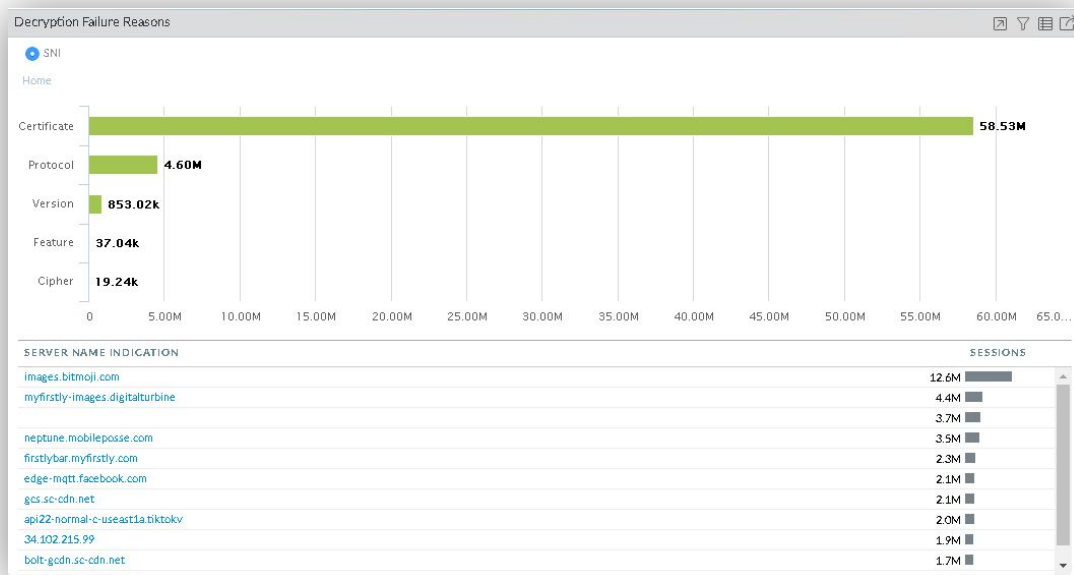
---

- (PAN-OS 11 only) Enable inspection of SSL handshake messages
  - Device > Setup > Session > SSL Decryption Settings



# SSL Forward Proxy - Decryption Failures

- Find unsupported sites
- Decide if exclusions should be made
- Create exclusion globally or on a per-user/per-IP basis



# SSL Inbound Inspection - What's Required

---

- Certificates for servers you want to inspect, e.g. company wildcard, www, etc.
- Endpoint, PAN firewall, and server all need to support common cipher suite

# SSL Decryption - Time to Configure

---

- It is recommended to be running PAN-OS  $\geq 10.1.0$  for better cipher support with inbound inspection
- Get a list of all the services you want to decrypt
- Identify any need for specific TLS versions or ciphers
- Gather certificates for all services
- Import all certificates into the firewall
- Create a decryption profile
- Create decryption rules to decrypt inbound/outbound connections
- Validate that applications work as expected

# SSL Decryption - Time to Configure

| NAME           | LOCATION | TAGS | Source        |         |      |        | Destination |                |        | URL CATEGORY | SERVICE | ACTION  | TYPE                   |
|----------------|----------|------|---------------|---------|------|--------|-------------|----------------|--------|--------------|---------|---------|------------------------|
|                |          |      | ZONE          | ADDRESS | USER | DEVICE | ZONE        | ADDRESS        | DEVICE |              |         |         |                        |
| inspect github | labfw01  | none | globalprotect | any     | any  | any    | inside      | 10.1.131.35/32 | any    | any          | any     | decrypt | ssl-inbound-inspection |

### Decryption Policy Rule ?

General | Source | Destination | Service/URL Category | **Options** | Target

Action: Decrypt

Type: SSL Inbound Inspection

Certificates:

- CERTIFICATES ^
- github

[Add](#) [Delete](#)

Decryption Profile: dp\_standard

Log Settings:

- Log Successful SSL Handshake
- Log Unsuccessful SSL Handshake

Log Forwarding: If\_standard

Packet Broker Profile: None

To decrypt and forward TLS traffic on PAN-OS (Seattle version or later), use Network packet Broker Policy. Decryption Broker configurations work only on PAN-OS 10.0 and earlier.

OK
Cancel

| GENERATE TIME  | TYPE | FROM ZONE | TO ZONE | SOURCE     | SOURCE USER | DESTINATION | DECRYPTED | TO PORT | APPLICATION | ACTION | RULE                   | SESSION END REASON |
|----------------|------|-----------|---------|------------|-------------|-------------|-----------|---------|-------------|--------|------------------------|--------------------|
| 03/31 17:13:57 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | websocket   | allow  | Allow Admins to Inside | tcp-fin            |
| 03/31 16:51:45 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | git-base    | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:51:34 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:51:33 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:46:28 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:41:54 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | websocket   | allow  | Allow Admins to Inside | tcp-fin            |
| 03/31 16:41:23 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:36:20 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:31:17 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:26:45 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 8443    | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:26:45 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 8443    | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:26:13 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:21:19 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | git-base    | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:21:08 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:21:07 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:16:03 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | github-base | allow  | Allow Admins to Inside | aged-out           |
| 03/31 16:10:59 | end  | vpn       | inside  | 172.21.2.7 | ds\zsum     | 10.1.131.35 | yes       | 443     | github-base | allow  | Allow Admins to Inside | aged-out           |

# Network Segmentation

---

# Overview

---

- Network segmentation is the process of classifying assets into unique subnets on your network with the intent of firewalling between these subnets.
- Firewalling these subnets is generally achieved by making the firewall the default gateway for the subnets assets are on, but another common option is using VRFs to force inter-VRF traffic through a firewall.



# Benefits

---

- Content inspection between subnets
- Prevent lateral spread of threats
- App-ID and User-ID between subnets
- Visibility into traffic flows between subnets
- Ability to easily isolate assets that may be compromised
- Foundation of a Zero Trust Architecture

# Methods of Implementation

---

Depending on your network topology, we would suggest taking one of the following design options:

1. Firewall on a stick model, with SVIs migrated to firewalls
2. VRF-Lite using different transit VLANs
3. L2 VNIs over VXLAN\*
4. L3VPN Technologies (L3VPN / EVPN)\*

\* - Requires >1500 MTU or TCP MSS Clamping

# Note on MTU

---

The default Internet MTU is 1500 bytes.

- Clients will use this MTU to negotiate their TCP Maximum Segment Size.
  - 1460 bytes is typical: MTU(1500) - IP Header(20) - TCP Header(20)

If you use an overlay technique, there's additional per packet overhead.

To accommodate this, either jumbo frames or TCP Clamping may be used.

If MTU isn't increased - or client's aren't aware - fragmentation will occur (Bad).

Most switches support Jumbo frames up to 9000 bytes, some further (9200+).

Most ISPs also support Jumbo frames on their Ethernet service connections.

# MTU/TCP-MSS Examples

---

- Switch MTU defines the maximum frame size a switch will carry before it is dropped. (Default is 1500 bytes).
  - This can typically be increased without impact, although the switch may require a reload.
  - Care should also be taken if the switch functions as a router.
- 
- TCP MSS Clamping is typically automatic on tunnel interfaces. Though it may need to be manually defined.
  - This configures the router to alter the TCP Maximum Segment Size negotiated during the TCP 3-way handshake between a client and host.

```
interface Ethernet1/3
no switchport
mtu 9216
```

```
SW1(config)#system mtu jumbo 9198
```

```
SW(config-if)#ip tcp adjust-mss 1380
```

# Choosing a Solution

| Supported Condition   | FW on a Stick | VRF Lite | L2 VNIs | L3VPN |
|-----------------------|---------------|----------|---------|-------|
| Layer 2 between sites | Yes           | Yes      | Yes     | Yes   |
| Layer 3 between sites | No            | Yes      | Yes     | Yes   |
| Standard MTU          | Yes           | Yes      | No      | No    |
| Jumbo frames          | Yes           | Yes      | Yes     | Yes   |
| Low latency Intrasite | No            | Yes      | No      | Yes   |
| Scalability           | Yes           | No       | No      | Yes   |

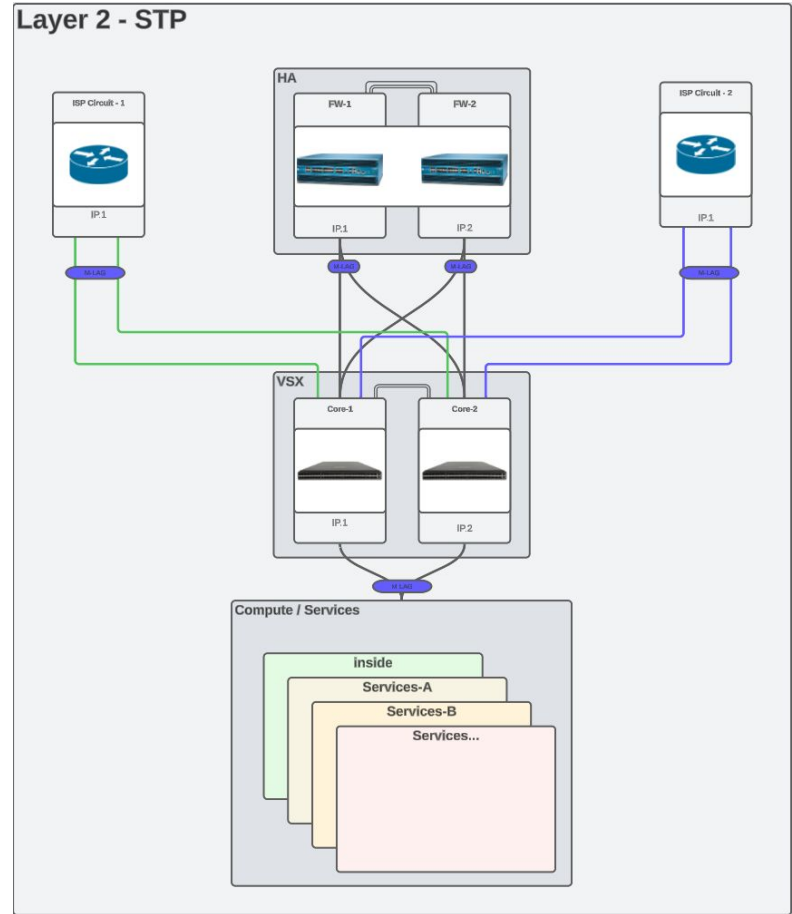
# Methods of Implementation

## Firewall on a stick

- +Simple design
- +Quick migration
- Dependency on L2 links to remote sites for firewalling remote site networks
- VLANs can't overlap\*
- MAC Limitations on Leased Circuits

\*-802.1ad Q-in-Q may be a work-around.

## Layer 2 - STP



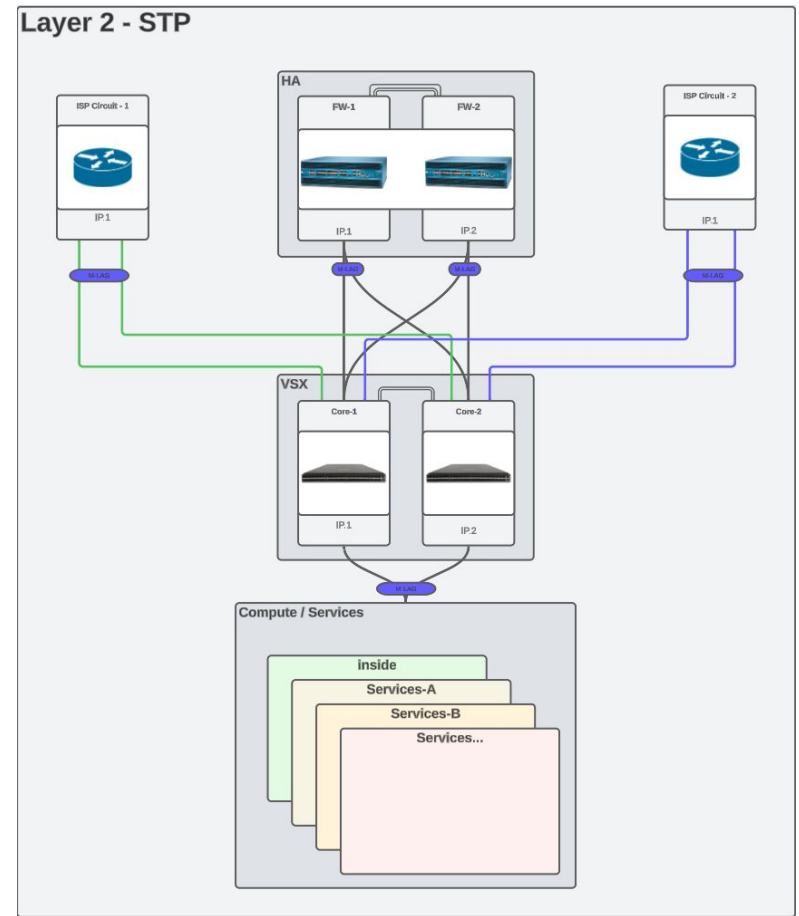
# Methods of Implementation

---

## Firewall on a stick







### Sample Scope

1. Configure aggregate group between firewalls and core
2. Migrate ACL's from core subnets to firewalls
3. Migrate SVI's from core to firewalls
4. Commit and push changes
5. Clear ARP tables and validate functionality



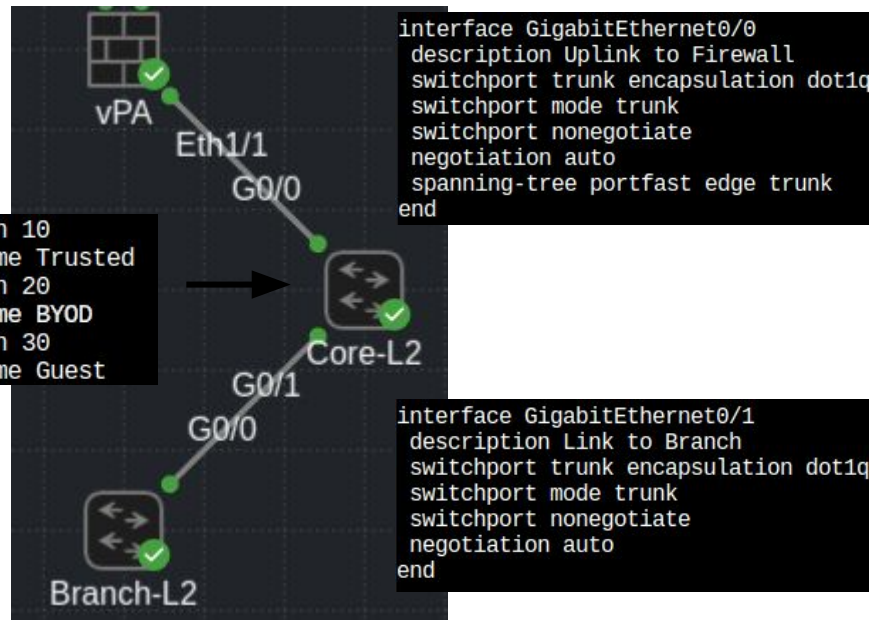
# Methods of Implementation

## Firewall on a stick

| INTERFACE  | INTERF...<br>TYPE | LINK<br>STATE   | IP ADDRESS     | SECURI...<br>ZONE |
|--|-------------------|---|----------------|-------------------|
|  ethernet1/1     | Layer3            |  | none           | none              |
|  ethernet1/1.10 | Layer3            |  | 10.1.10.254/24 | Trusted           |
|  ethernet1/1.20 | Layer3            |  | 10.1.20.254/24 | BYOD              |
|  ethernet1/1.30 | Layer3            |  | 10.1.30.254/24 | Guest             |

### Firewall on a Stick/VLAN Extension:

You only need Layer 2 VLANs and Trunks configured.

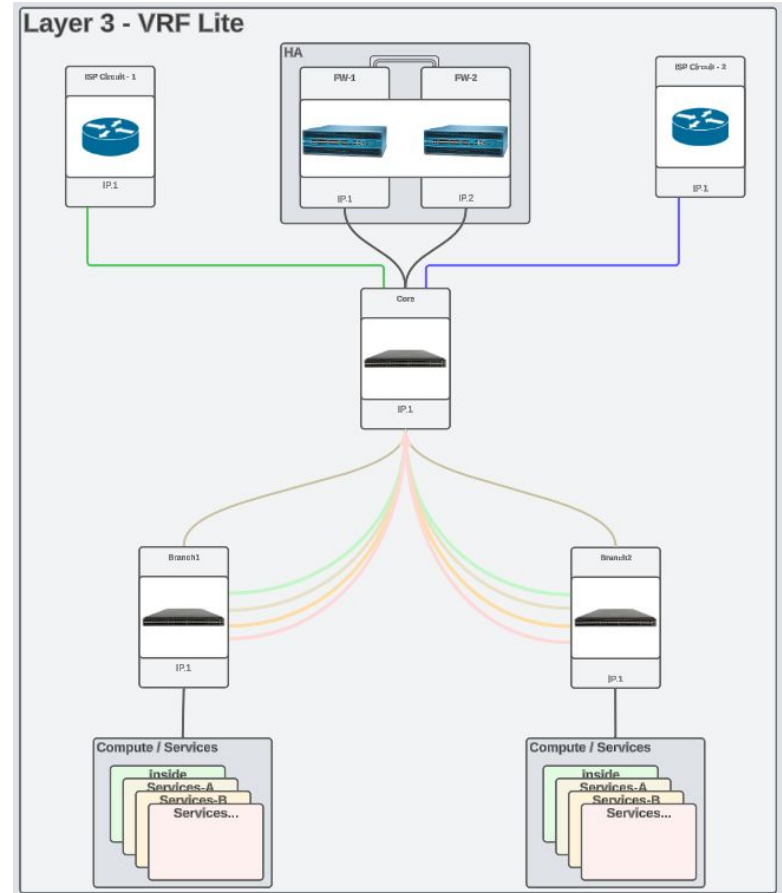




# Methods of Implementation

## VRF-Lite

- +VLANs can overlap
- +Smaller broadcast domains
- +Widely supported
- +VRF-Lite + Tunnel can act as a basic overlay.
- +/- VRF-Lite using 802.1q has no overlay overhead.
- Tunnel based overlay has high overhead.
- Possible Dependency on 802.1q L2 links to remote site
- Not-scalable - Dedicated routing protocol per VRF/Zone.



# Methods of Implementation

## VRF-Lite

| INTERF... | COMMENT         | IP ADDRESS       | SECURI...<br>ZONE |
|-----------|-----------------|------------------|-------------------|
| vlan      |                 | none             | none              |
| vlan.10   | Trust - L3 Peer | 172.20.10.254/24 | Trusted           |
| vlan.20   | BYOD - L3 Peer  | 172.20.20.254/24 | BYOD              |
| vlan.30   | Guest - L3 Peer | 172.20.30.254/24 | Guest             |

### VRF Lite:

- Each VRF needs its own router process and path.
- Each router in the path needs to have VRF configuration.

```

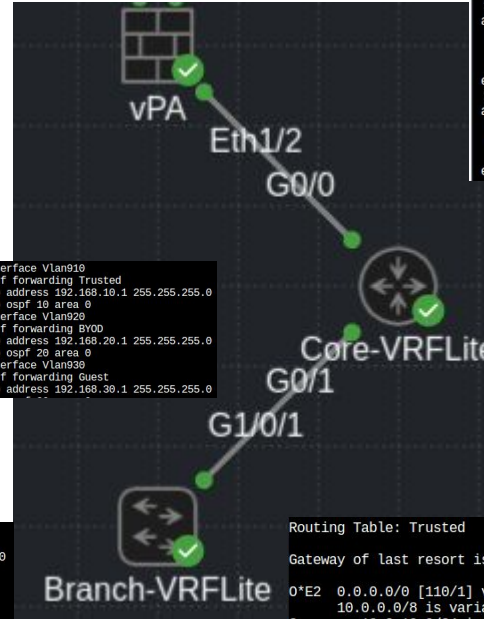
interface Tunnel10
 vrf forwarding Trusted
 ip address 192.168.210.1 255.255.255.254
 ip ospf network point-to-point
 ip ospf 10 area 0
 tunnel source Loopback0
 tunnel destination 10.255.2.1
 tunnel key 10
!
interface Tunnel20
 vrf forwarding BYOD
 ip address 192.168.220.1 255.255.255.254
 ip ospf network point-to-point
 ip ospf 20 area 0
 tunnel source Loopback0
 tunnel destination 10.255.2.1
 tunnel key 20
!
interface Tunnel30
 vrf forwarding Guest
 ip address 192.168.230.1 255.255.255.254
 ip ospf network point-to-point
 ip ospf 30 area 0
 tunnel source Loopback0
 tunnel destination 10.255.2.1
 tunnel key 30
!
    
```

```

interface Vlan10
 vrf forwarding Trusted
 ip address 10.2.10.254 255.255.255.0
 ip ospf 10 area 0
 no autostate
!
interface Vlan20
 vrf forwarding BYOD
 ip address 10.2.20.254 255.255.255.0
 ip ospf 20 area 0
 no autostate
!
interface Vlan30
 vrf forwarding Guest
 ip address 10.2.30.254 255.255.255.0
 ip ospf 30 area 0
 no autostate
!
    
```

```

interface Vlan910
 vrf forwarding Trusted
 ip address 192.168.10.1 255.255.255.0
 ip ospf 10 area 0
!
interface Vlan920
 vrf forwarding BYOD
 ip address 192.168.20.1 255.255.255.0
 ip ospf 20 area 0
!
interface Vlan930
 vrf forwarding Guest
 ip address 192.168.30.1 255.255.255.0
    
```



```

router bgp 65002
 bgp router-id interface Loopback0
 no bgp transport path-mtu-discovery
 bgp log-neighbor-changes
 no bgp default ipv4-unicast
!
 address-family ipv4 vrf BYOD
 redistribute ospf 20
 neighbor 172.20.20.254 remote-as 65535
 neighbor 172.20.20.254 activate
 exit-address-family
!
 address-family ipv4 vrf Guest
 redistribute ospf 30
 neighbor 172.20.30.254 remote-as 65535
 neighbor 172.20.30.254 activate
 exit-address-family
!
 address-family ipv4 vrf Trusted
 redistribute ospf 10
 neighbor 172.20.10.254 remote-as 65535
 neighbor 172.20.10.254 activate
 exit-address-family
    
```

```

router ospf 10 vrf Trusted
 redistribute bgp 65002 subnets
 default-information originate
router ospf 20 vrf BYOD
 redistribute bgp 65002 subnets
 default-information originate
router ospf 30 vrf Guest
 redistribute bgp 65002 subnets
 default-information originate
    
```

Routing Table: Trusted

Gateway of last resort is 192.168.210.0 to network 0.0.0.0

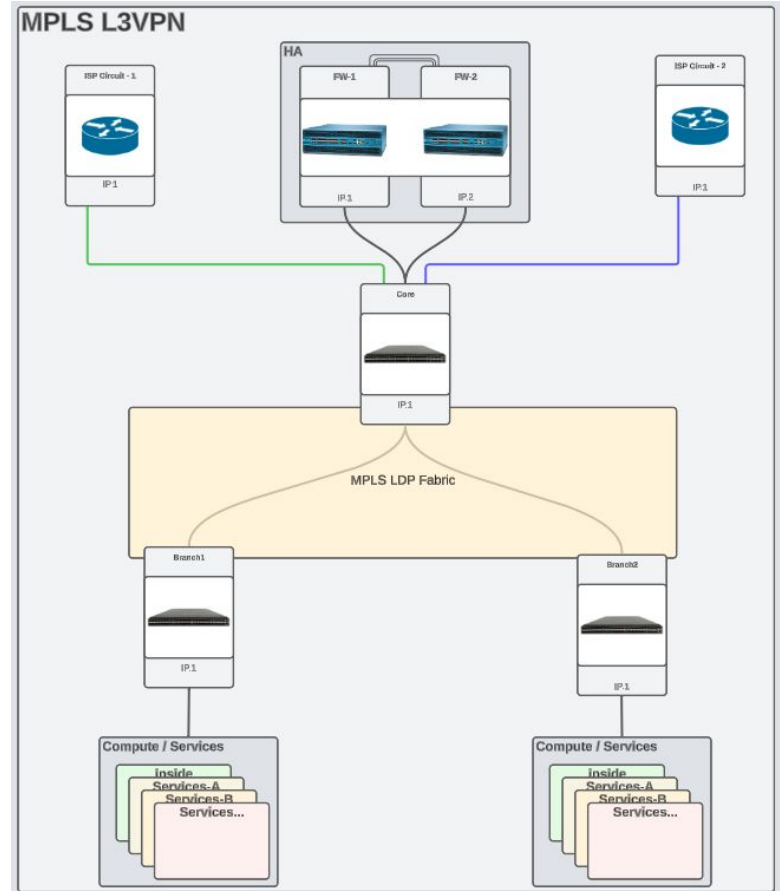
```

O*E2 0.0.0.0/0 [110/1] via 192.168.210.0, 1d11h, Tunnel10
 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C   10.2.10.0/24 is directly connected, Vlan10
L   10.2.10.254/32 is directly connected, Vlan10
O   192.168.10.0/24 [110/1001] via 192.168.210.0, 1d11h, Tunnel10
 192.168.210.0/24 is variably subnetted, 2 subnets, 2 masks
C   192.168.210.0/31 is directly connected, Tunnel10
L   192.168.210.1/32 is directly connected, Tunnel10
    
```

# Methods of Implementation

## MPLS L3VPN

- +VLANs can overlap
- +Smaller broadcast domains
- +Highly Scalable (ISPs use it Globally)
- +Low Overlay Overhead (8 bytes)
- All devices in labeled path need to support MPLS.
- Not a common skillset.
- TCP Clamping Not Easily Implemented (Use Jumbo MTU)



# Methods of Implementation

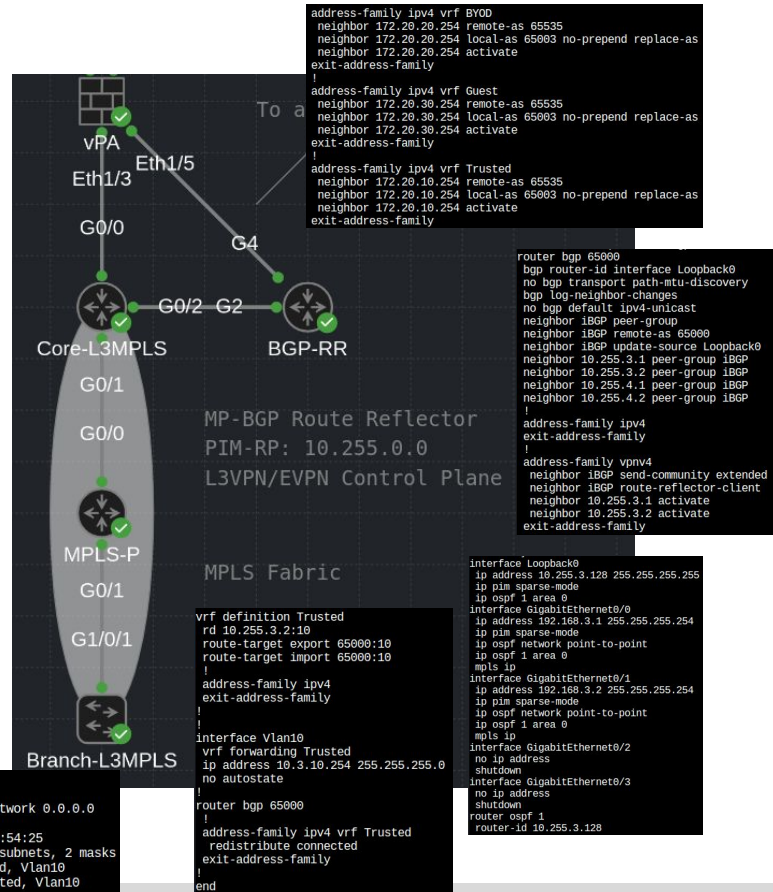
## MPLS L3VPN

| INTERF... | COMMENT         | IP ADDRESS       | SECURI... |
|-----------|-----------------|------------------|-----------|
| vlan      |                 | none             | none      |
| vlan.10   | Trust - L3 Peer | 172.20.10.254/24 | Trusted   |
| vlan.20   | BYOD - L3 Peer  | 172.20.20.254/24 | BYOD      |
| vlan.30   | Guest - L3 Peer | 172.20.30.254/24 | Guest     |

### MPLS L3VPN:

iBGP Extended Communities are used to Import/Export Routes per VRF. MPLS LDP will dynamically build a path to carry the data.

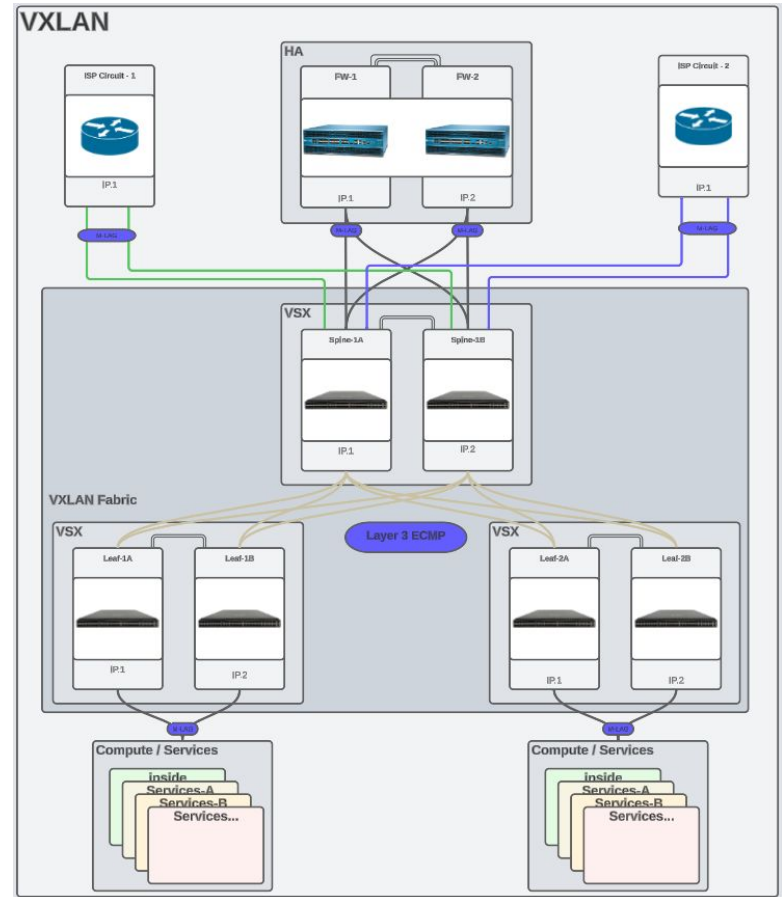
- OSPF is used in the underlay to provide reachability between loopbacks
- BGP-Route Reflector is used for easy scalability.



# Methods of Implementation

## BGP EVPN

- +VLANs can overlap
- +Smaller broadcast domains
- +Highly Scalable (DC/Colos use it Globally)
- +Data carried by UDP datagram - No special transport requirements.
- +Can function as both L2 and L3 extension.
- High Overlay Overhead (## bytes)
- Not a common skillset.
- TCP Clamping Not Easily Implemented (Use Jumbo MTU)



# Methods of Implementation

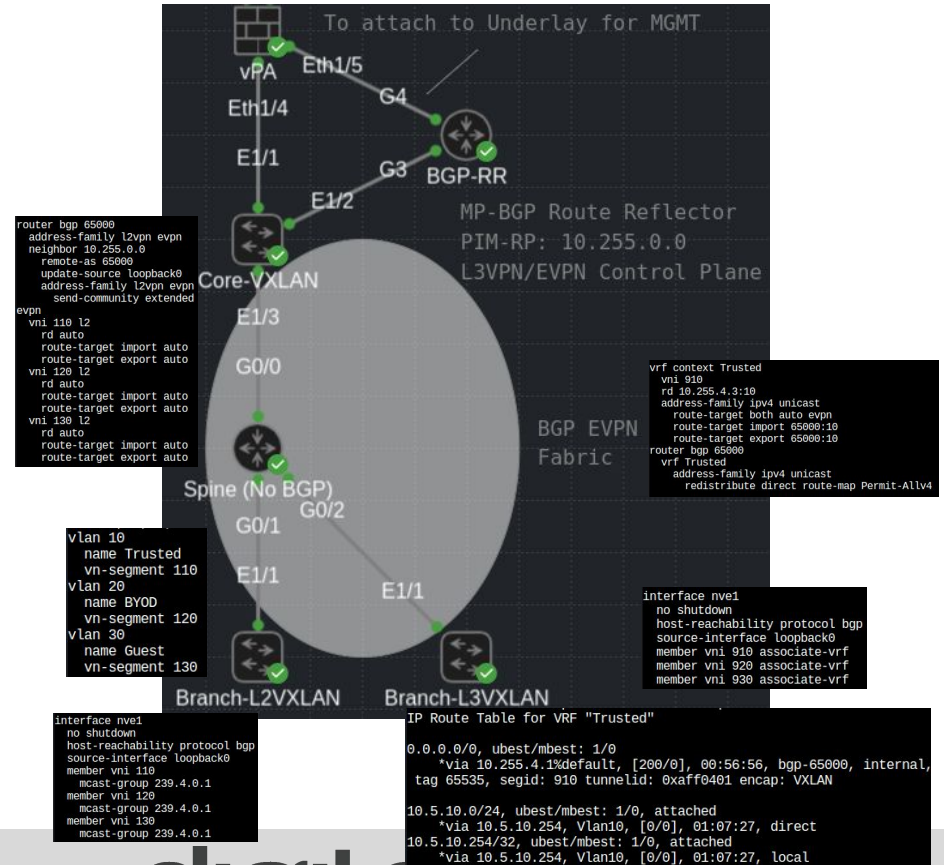
## BGP EVPN

| INTERF... | COMMENT         | IP ADDRESS       | SECURI...<br>ZONE |
|-----------|-----------------|------------------|-------------------|
| vlan      |                 | none             | none              |
| vlan.10   | Trust - L3 Peer | 172.20.10.254/24 | Trusted           |
| vlan.20   | BYOD - L3 Peer  | 172.20.20.254/24 | BYOD              |
| vlan.30   | Guest - L3 Peer | 172.20.30.254/24 | Guest             |

### BGP EVPN:

iBGP Extended Communities are used to Import/Export Routes per VRF/VNI. VXLAN NVEs will dynamically forward traffic to peer switches.

- OSPF is used in the underlay to provide reachability between loopbacks.
- PIM is used to create multicast underlay for flood BUM traffic. (Broadcast, Unknown-unicast, and Multicast)
- \*Non-Multicast options are also available (Ingress-Replication)
- BGP-Route Reflector is used for easy scalability.





# Note on MTU (Examples)

- 802.1q

```
▶ Frame 8: 118 bytes on wire (944 bits), 118 bytes captured (944 bits)
▶ Ethernet II, Src: RealtekU_00:12:27 (52:54:00:00:12:27), Dst: RealtekU_0f:d8:65 (52:54:00:0f:d8:65)
▶ 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 910
▶ Internet Protocol Version 4, Src: 10.2.10.254, Dst: 8.8.8.8
▶ Internet Control Message Protocol
```

- MPLS

```
▶ Frame 7: 122 bytes on wire (976 bits), 122 bytes captured (976 bits)
▶ Ethernet II, Src: RealtekU_01:5c:0b (52:54:00:01:5c:0b), Dst: RealtekU_15:6d:ef (52:54:00:15:6d:ef)
▶ MultiProtocol Label Switching Header, Label: 17, Exp: 0, S: 0, TTL: 255
▶ MultiProtocol Label Switching Header, Label: 56, Exp: 0, S: 1, TTL: 255
▶ Internet Protocol Version 4, Src: 10.3.10.254, Dst: 8.8.8.8
▶ Internet Control Message Protocol
```

- GRE

```
▶ Frame 10: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits)
▶ Ethernet II, Src: RealtekU_00:12:0d (52:54:00:00:12:0d), Dst: RealtekU_0f:d8:65 (52:54:00:0f:d8:65)
▶ Internet Protocol Version 4, Src: 10.255.2.2, Dst: 10.255.2.1
▶ Generic Routing Encapsulation (IP)
▶ Internet Protocol Version 4, Src: 10.2.10.254, Dst: 8.8.8.8
▶ Internet Control Message Protocol
```

- VXLAN

```
▶ Frame 6: 148 bytes on wire (1184 bits), 148 bytes captured (1184 bits)
▶ Ethernet II, Src: RealtekU_18:f4:60 (52:54:00:18:f4:60), Dst: 52:10:d7:d6:1b:08 (52:10:d7:d6:1b:08)
▶ Internet Protocol Version 4, Src: 10.255.4.3, Dst: 10.255.4.1
▶ User Datagram Protocol, Src Port: 52215, Dst Port: 4789
▶ Virtual eXtensible Local Area Network
▶ Ethernet II, Src: 52:1d:4b:d9:1b:08 (52:1d:4b:d9:1b:08), Dst: 52:10:d7:d6:1b:08 (52:10:d7:d6:1b:08)
▶ Internet Protocol Version 4, Src: 10.5.10.254, Dst: 8.8.8.8
▶ Internet Control Message Protocol
```

- IPSEC

```
▶ Frame 6: 194 bytes on wire (1552 bits), 194 bytes captured (1552 bits)
▶ Ethernet II, Src: RealtekU_08:a5:9a (52:54:00:08:a5:9a), Dst: RealtekU_1e:8a:ad (52:54:00:1e:8a:ad)
▶ Internet Protocol Version 4, Src: 10.255.2.3, Dst: 10.255.2.1
▶ Encapsulating Security Payload
```

Different frame sizes using different overlay techniques.

Base ICMP ping frame size is 114 bytes.

802.1q and MPLS are the smallest as they sit in front of the original IP header.

The other techniques encapsulate the original IP packet inside of a new IP packet.

# Methods of Implementation

---

- Option 1 - Migrate server vlan interfaces from core switch and place them on firewall
  - Quicker to implement
  - May need to migrate ACLs from switch
  - May need to further segment existing subnets
- Option 2 - Create new server subnets on firewall and migrate applications to new subnets
  - Migrating applications to new subnets is a large effort that carries risk (services using IP address versus hostname will break)
  - Will require rulebase updates for IP changes, but will lead to cleaner rulebase
  - Applications can be moved one at a time allowing slow, methodical approach



# Recommendations

---

- If there are just a few server subnets
  - Option 1, followed by option 2
  - This will allow instant improvement of security posture by getting subnets on the firewall
  - Option 2 can then be implemented over time to continue improving posture
- If there are significant server subnets
  - Option 1
  - If assets are already properly categorized into subnets, migrating the subnets straight to the firewall should be all that is needed
  - Make sure ACLs are properly migrated prior to migrating

# Considerations

---

- Security and NAT policies will need to be updated to reflect changes to zones
- Load balancers can lead to asymmetric routes and will need to be considered before migrating subnets

# What is Falco?

---

- A tool to detect configuration issues
- A managed service to assist with fixing them



**FALCO**



80% passed  
1 Devices Audited



1/1 devices  
Recommended Releases

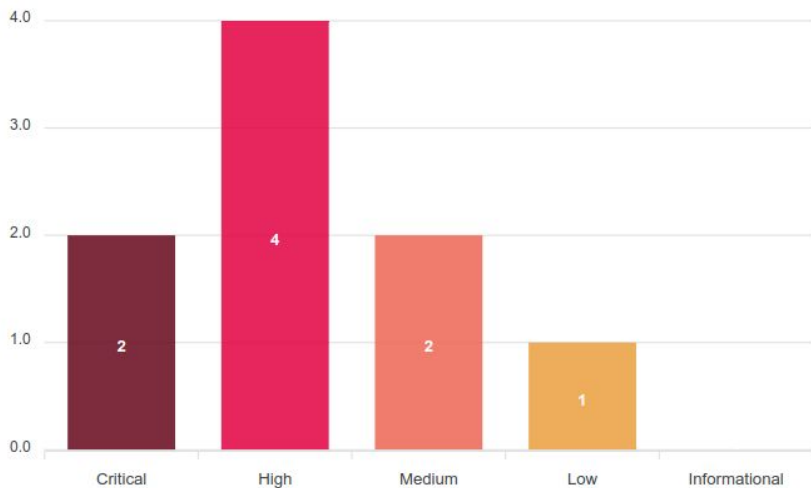


No Vulnerabilities  
No Known Vulnerabilities Found

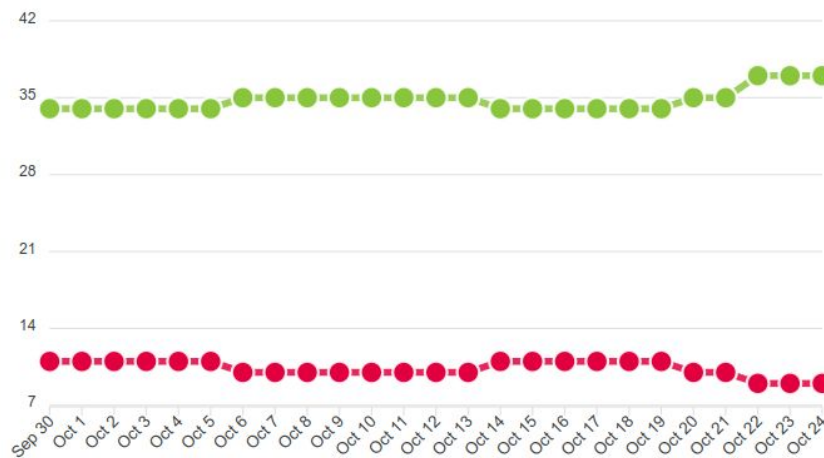


Support Licenses  
All Devices Have Valid Support Licenses

### Failed Check Severity



### Report History



A photograph of a modern office interior, heavily tinted with a teal color. The scene shows a ceiling with several long, rectangular, recessed light fixtures and some track lighting. The perspective is looking upwards, creating a sense of height and architectural detail.

# digitalscepter

---

[sales@digitalscepter.com](mailto:sales@digitalscepter.com)  
(888) 299-3718

[digitalscepter.com](http://digitalscepter.com)