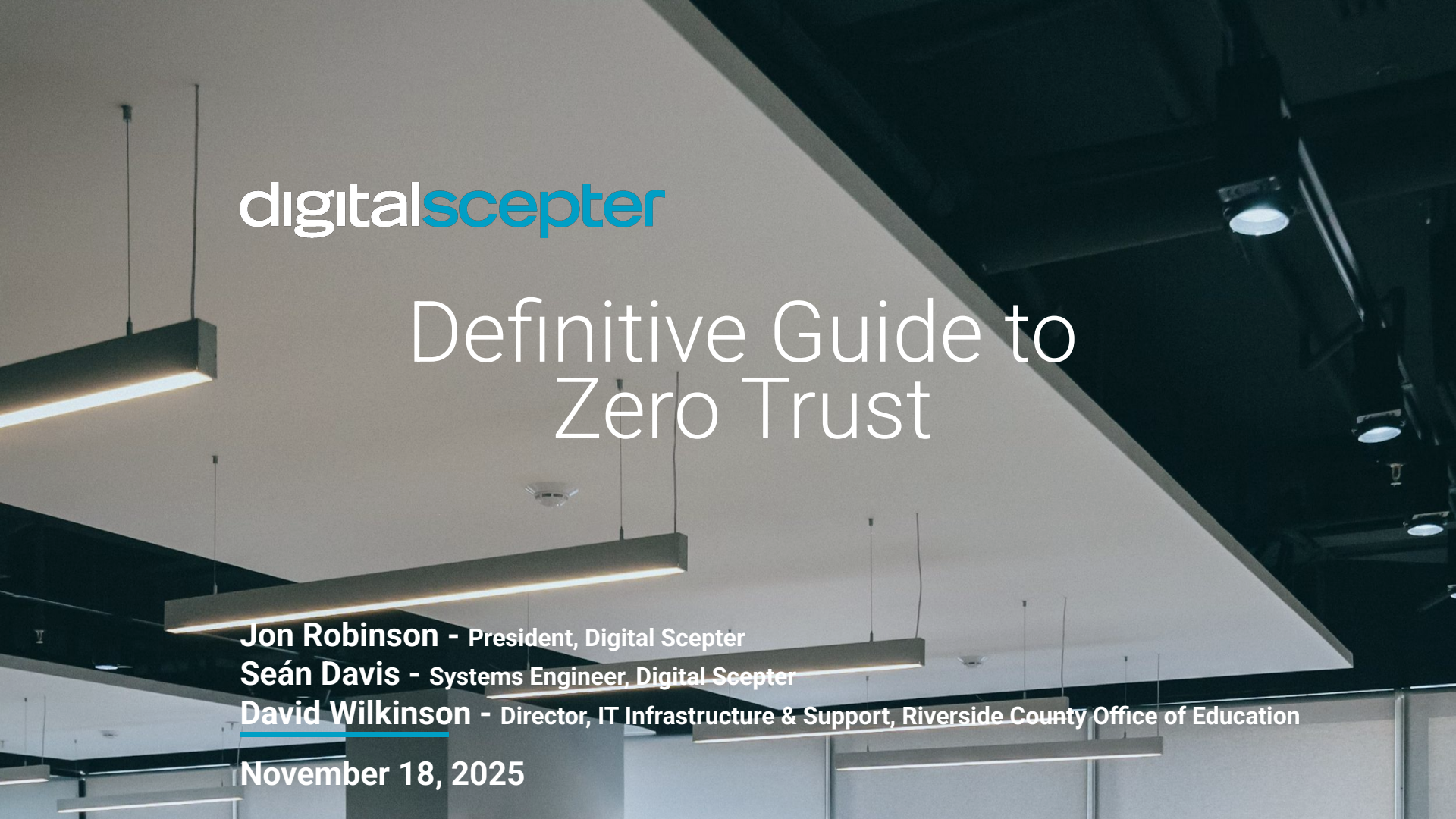


digitalscepter

Definitive Guide to Zero Trust

Jon Robinson - President, Digital Scepter
Seán Davis - Systems Engineer, Digital Scepter
David Wilkinson - Director, IT Infrastructure & Support, Riverside County Office of Education

November 18, 2025

Today's Roadmap

1. Where it started
   - Quick History
   - Overview of "Zero-Trust"

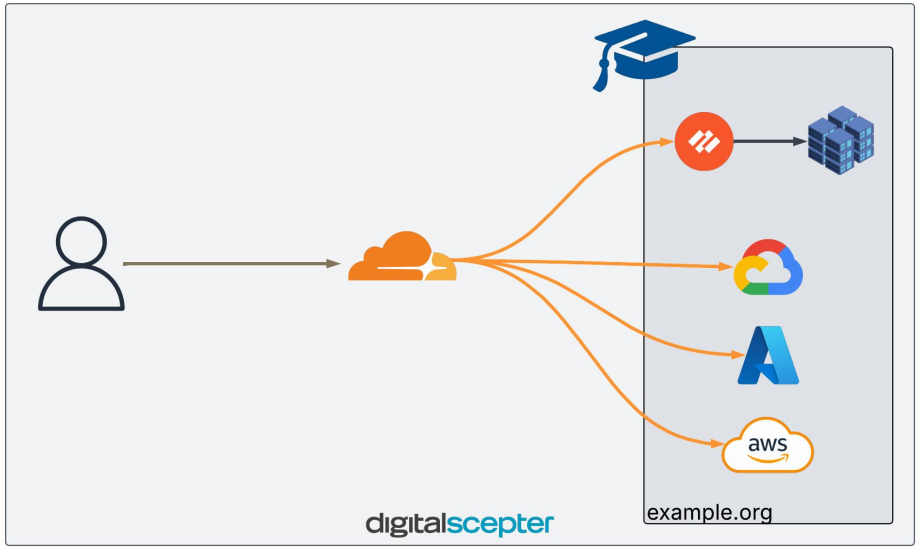
2. Logical Models
   - NIST
   - BeyondCorp (Google)

3. Network Models
   - Classic
   - Collapsed (Firewall on a Stick)
   - Fabric
   - Network Authentication
   - Policy Flow

4. Modern Campus Network Design and Alignment
   - Zone based/Segmented Networks
   - Application filtering, User / Device Identification and Tunneling of Internal Applications

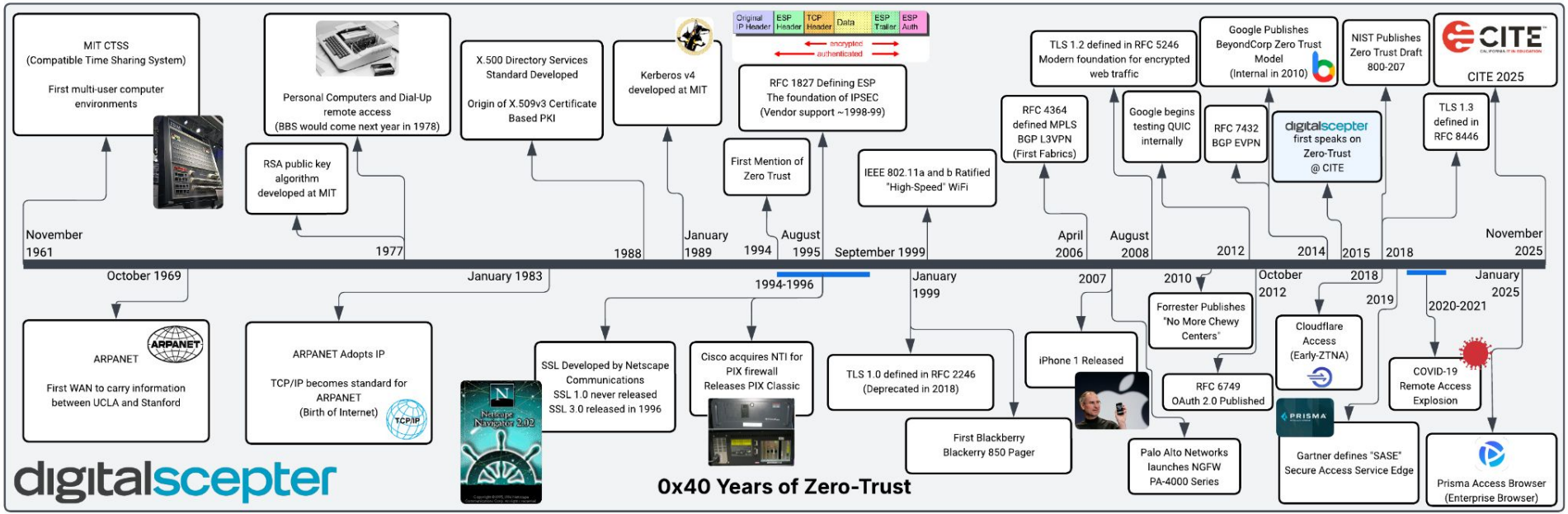
5. Putting It Together - Hybrid/Full Stack Designs
   - Blending on-premises NGFW with cloud enforcement
   - Map user roles (Staff, Student, Faculty, Parents...) to appropriate access tiers

6. RCOE Zero-Trust in Action
   - Using Cloudflare and FusionAuth to deliver critical applications anywhere



digitalscepter

Timeline



digitalscepter

Origin

“Zero Trust” didn’t begin as a cybersecurity slogan. It originated in 1994 as a mathematical construct within Stephen Marsh’s Ph.D. thesis, describing the absence of certainty within a system.

Zero Trust is the state between trust and untrust.

Akin to the Schrödinger’s Cat thought experiment, until it is observed or quantified, we don’t know what state the device is in.

The trust an agent has in another in a specific situation is a function of the amount of trust in that agent in general and the importance of the situation to the trusting agent. In addition, the trust the other agent has in the first may play a part — knowing that you trust me may help me to reciprocate that trust, as does an estimate of how much I think you may trust me:[4]

$$T_x(y, \alpha_x) = f(T_x(y), I_x(\alpha_x), \widehat{T_y(x)}^x, \widehat{\widehat{T_x(y)}}^{y^x})$$

Before trust can exist, the device must first be verified, its identity confirmed, and its posture assessed.

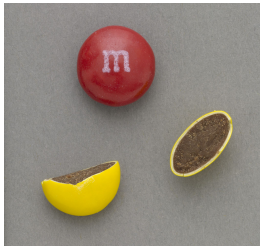
https://dspace.stir.ac.uk/bitstream/1893/2010/1/Formalising%20trust%20as%20a%20computational%20concept.pdf

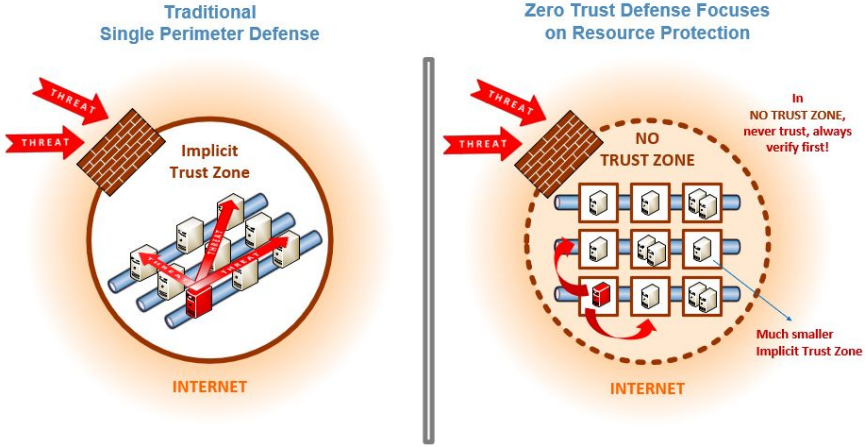
digitalscepter

Origin

The phrase “Never trust, always verify” was popularized by John Kindervag of Forrester Research in 2009.
He described legacy networks as being like M&Ms, hard and crunchy on the outside, but soft and chewy on the inside.

Zero Trust aims to remove that chewy center by authenticating and authorizing every user and connection.





https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify

digitalscepter

Zero-Trust Principles Aren't New

They are security principles repackaged.

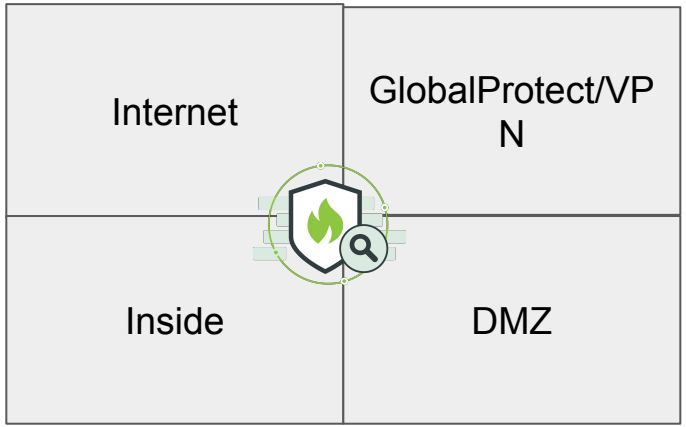
- **Principle of Least Privilege** - everything should have only the minimum level of access necessary to perform its legitimate tasks, and nothing more; AKA "default deny" or RBAC - role-based access control
- **Authentication** - verifying identity of a user or device
- **Authorization** - granting the appropriate privileges based on least privilege

But Zero-Trust Architecture strives to redefine the scope of where and when these principles are applied, e.g. from a VPN to a LAN to verifying identity everywhere all the time and having more data to consider before authorization, e.g. verify a user but also consider recent behavior and device status.

Definitions

- Zero Trust - overall philosophy
- Zero Trust Architecture - serve applications to users based on principle of least privilege wherever they are
- Zero Trust Network Access (ZTNA) - an implementation pattern that replaces legacy VPN solutions (agent+cloud gateway model)

Zones

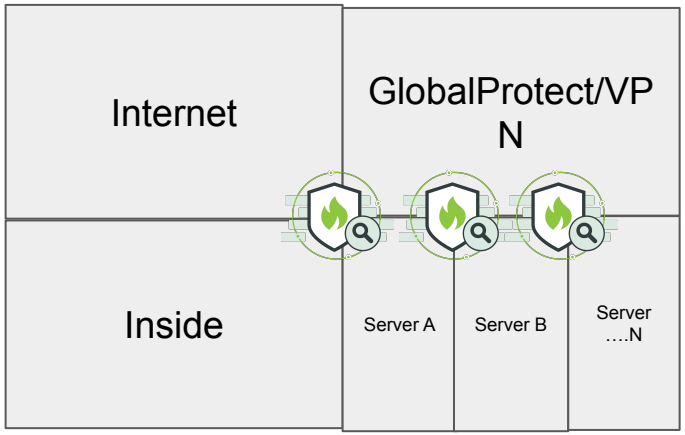


Zones or networks protected by a perimeter device. Depending on the granularity of the access rules, this could implicitly trust inside traffic to DMZ (seen frequently before 2015).

Remote users were given access to the company applications via VPN. The VPN policies could be “allow onto this network” or they could be based on least privilege.

It’s a common straw-man argument that VPN gives users too-broad of access.

Zones



This model separates apps and servers into zones based on their criticality. Could be three zones: high, medium, low or it could be based on function: web, database, etc. or it could be one zone per server.

Inside to server rules could be role-based as well.

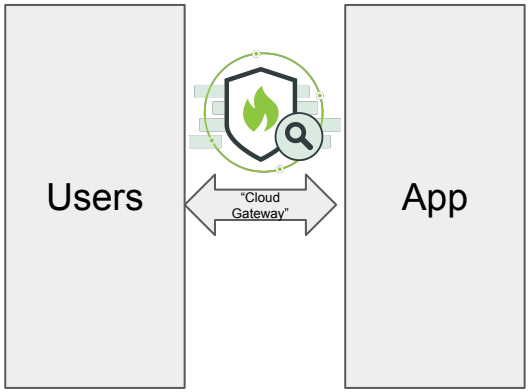
You can do zero-trust with your on-premise devices.

The reasons you might want to update to “Zero-trust Network Access” (ZTNA) include:

- Avoid backhauling traffic
- Avoid managing VPN gateway infrastructure (although you introduce other infrastructure to maintain)
- Make user-id tracking easier
- Possibly make device-health tracking easier
- Make the status of the user/device more dynamic
- Allow for the reality that your apps reside in cloud infra or Saas and are no longer solely in your datacenter

digitalscepter

Zones



The new model is user/device and app focused. The network and location is abstracted away and access policies happen through a single logical gateway. This gateway resides in the cloud and performs authentication and authorization. You can access this gateway through a clientless VPN, an agent (AKA VPN client), explicit proxy, an enterprise browser (aka a fancy agent), or remote browser isolation. In order to do this a lot of underlying infrastructure or information is required.

Pri	Name	Mode	Scope	Destinations	Web access	Data controls	Tracking
1	Allow Accounting Team to Accounting Tools	✓	DS_Accounting	QuickBooks	Allow	Block download (1)	On
2	Allow PKI Admins to PKI Servers	✓	PKI_Admins	PROD - Root CA +1	Allow		On
3	Allow VMware Admins to vCenter	✓	ESX_Admins	PROD - vCenter	Allow		Enhanced Screenshot

This screenshot is from Palo Alto Networks Prisma Access Browser.

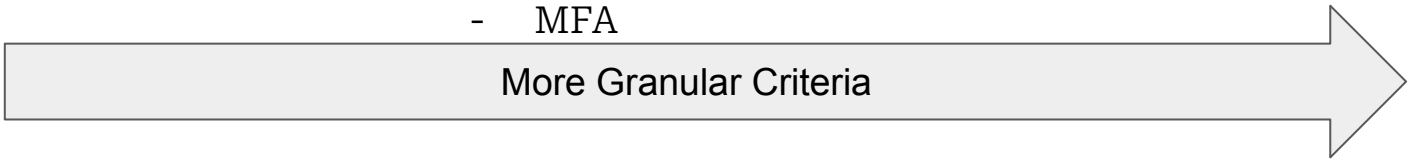
digitalscepter

Access Policy Trend

FW ACLs
- IP addresses
- Ports

NGFW Policies
- IP Addresses (Dynamic)
- Ports
- User-ID (AD sync or authentication)
- App-ID
- Device-ID
- URL Categories
- Threats
- MFA

ZTNA Policies
- User (based on authentication and risk)
- Device health (ideally dynamic)
- Application



digitalscepter

Why Zero-Trust Matters in K12

- Cloud apps replace many on-prem apps
- Students roaming on unmanaged devices
- VPN doesn’t align with Saas or cloud
    - Scaling and management issues
- Need to segment but not everything is in the datacenter and users aren’t on-campus
- Expectation: access from anywhere, safely

Benefits:

- Smaller blast radius - compromised hosts can’t move laterally in network
- Drastically reduce attack surface (no VPN on internet, fewer apps on internet)
- Onboard employees and vendors to required apps more easily

Trust Algorithm

- This determines your stopping point for authentication
- Password only
- Password and MFA
- Password, MFA and device cert
- Password, mfa, device cert and device health
- Password, mfa, device cert, device health and dynamic user risk (e.g. from SIEM, firewall or endpoint detection and response software)

NIST calls this the trust algorithm. Google calls it Trust Evaluation

Logical Models

NIST Zero Trust Diagram

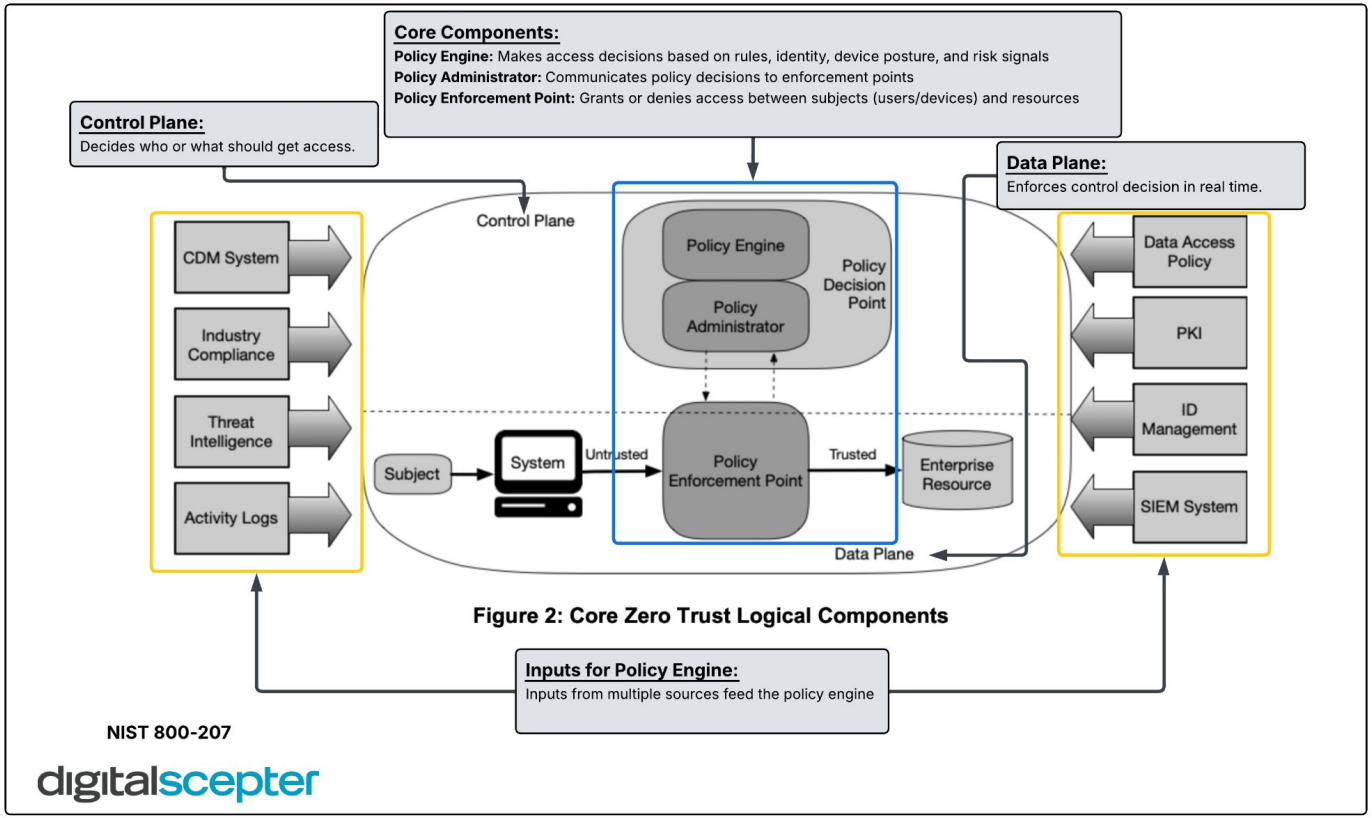


Figure 2: Core Zero Trust Logical Components

digitalscepter

NIST Zero Trust Diagram

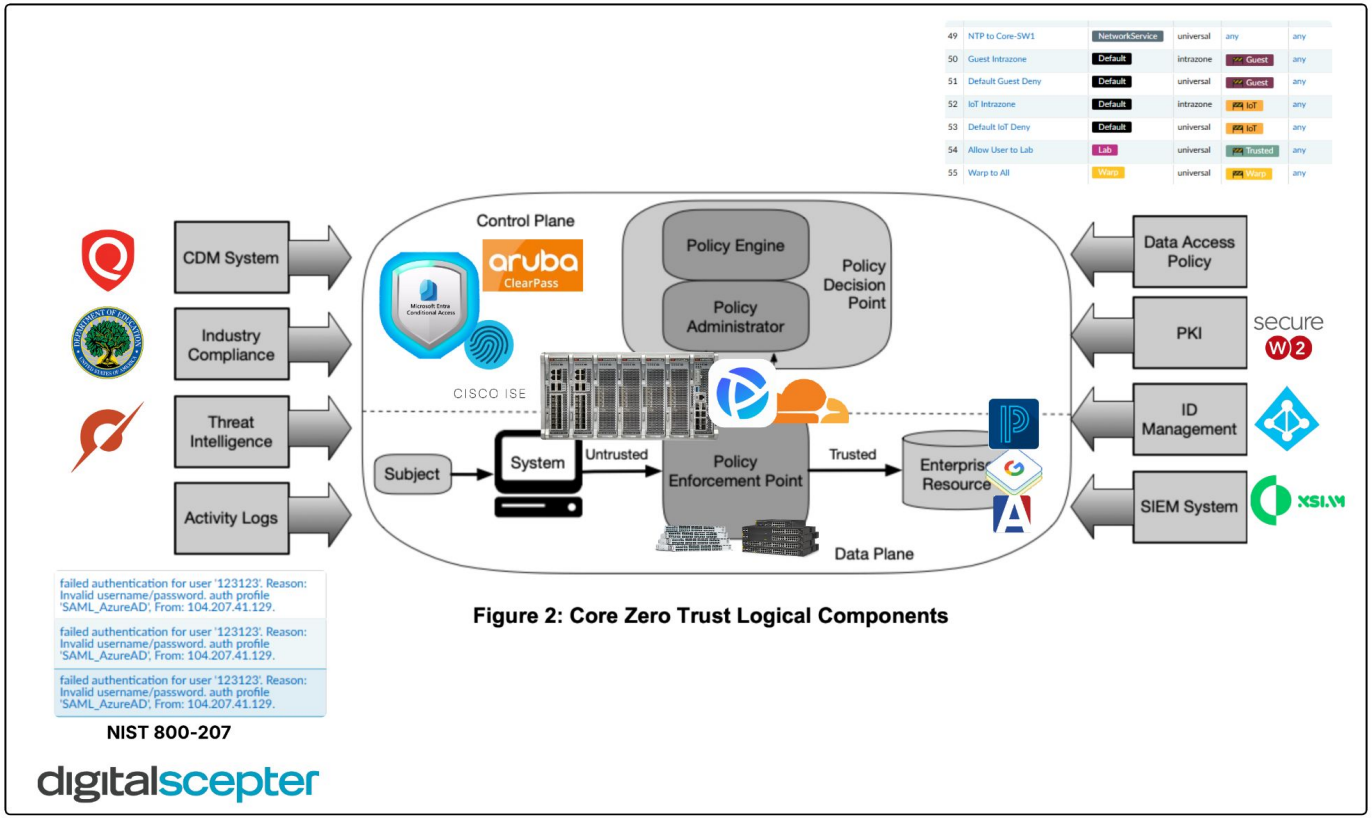


Figure 2: Core Zero Trust Logical Components

digitalscepter

Logical Components per NIST SP 800-27

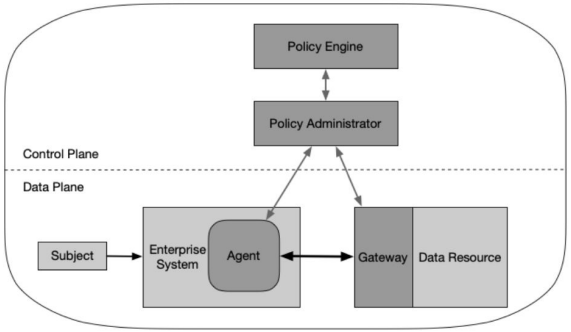


Figure 3: Device Agent/Gateway Model

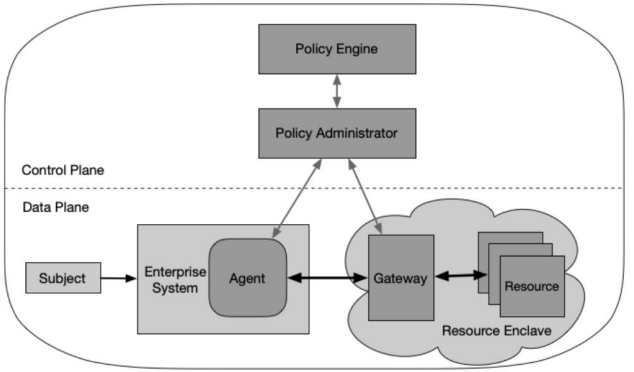


Figure 4: Enclave Gateway Model

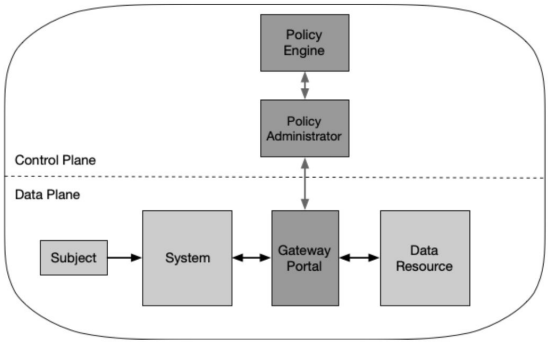


Figure 5: Resource Portal Model

The gateway needs access to the resources, typical via a VM deployed that acts as a “connector” and creates a tunnel to the cloud gateway. This can be one-to-one or one-to-many. The User/Subject can connect via agent (i.e. GlobalProtect/Prisma Access Agent), enterprise browser, URL in a browser (DNS), PAC file (explicit proxy) or remote browser isolation. Every vendor has these same models built out; they differ in management, usability, logging, integration, scalability.

digitalscepter

BeyondCorp Components

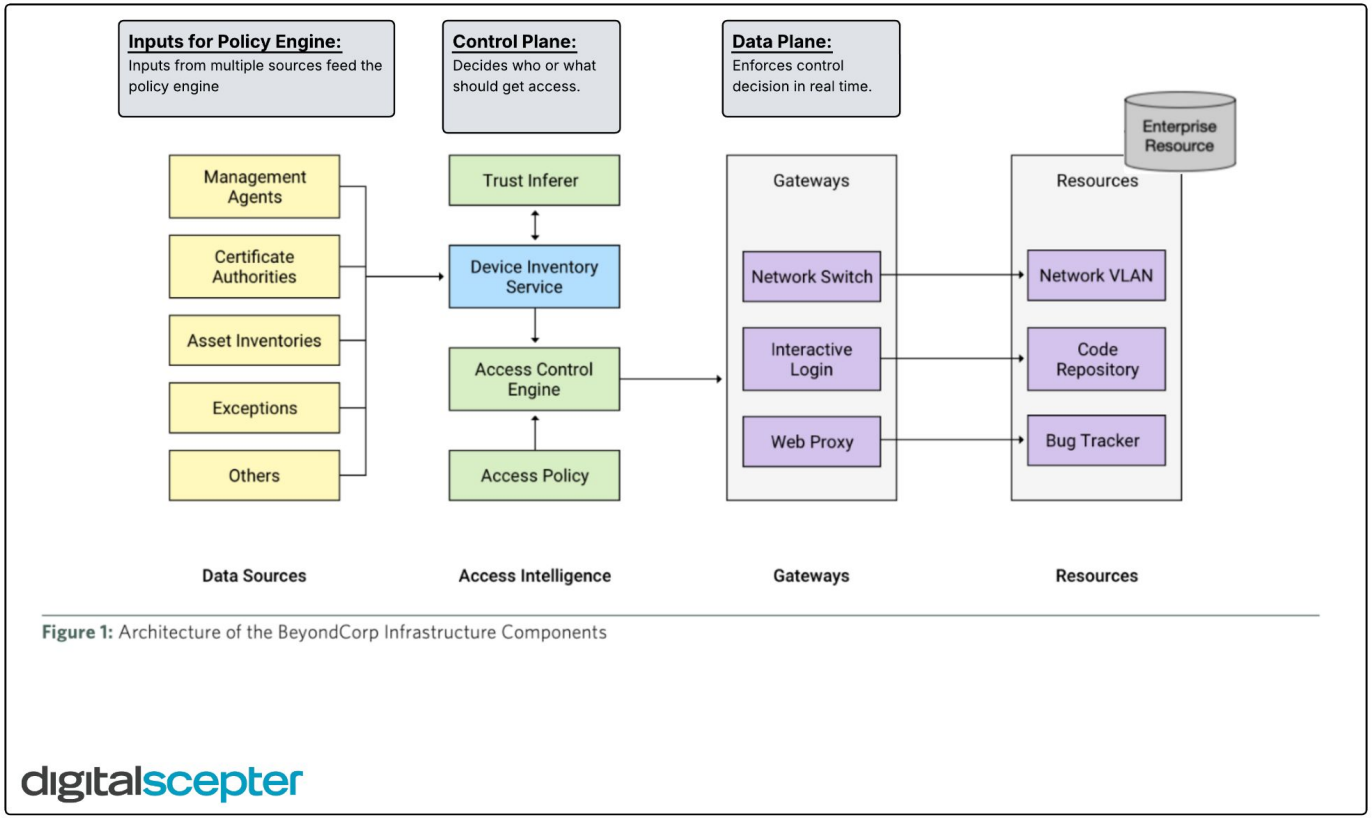
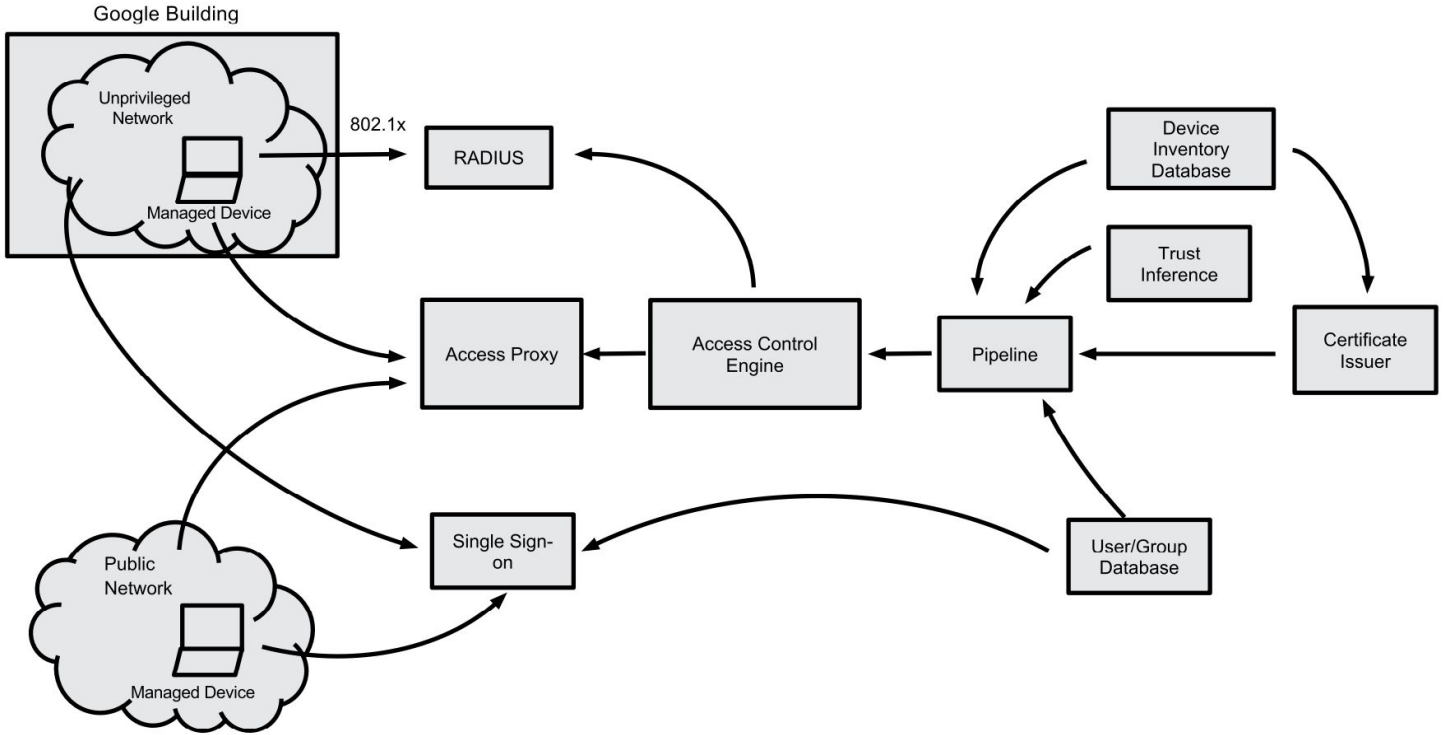


Figure 1: Architecture of the BeyondCorp Infrastructure Components

digitalscepter

digitalscepter

BeyondCorp Components



digitalscepter

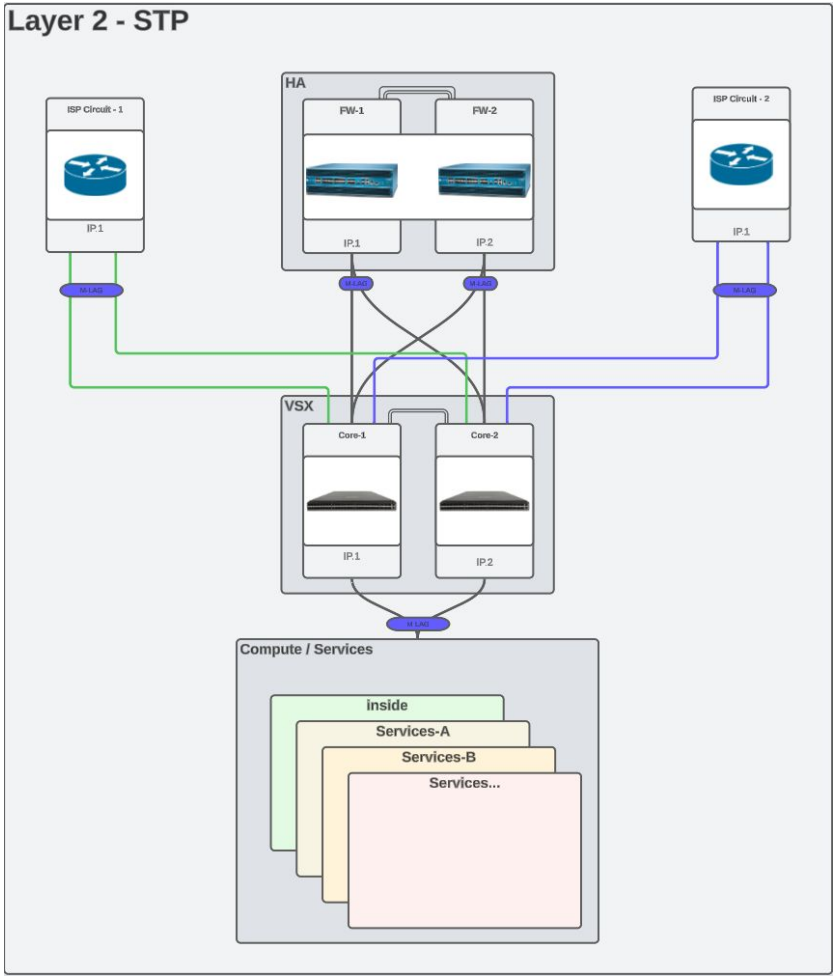
Network Examples

Network Segmentation

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.

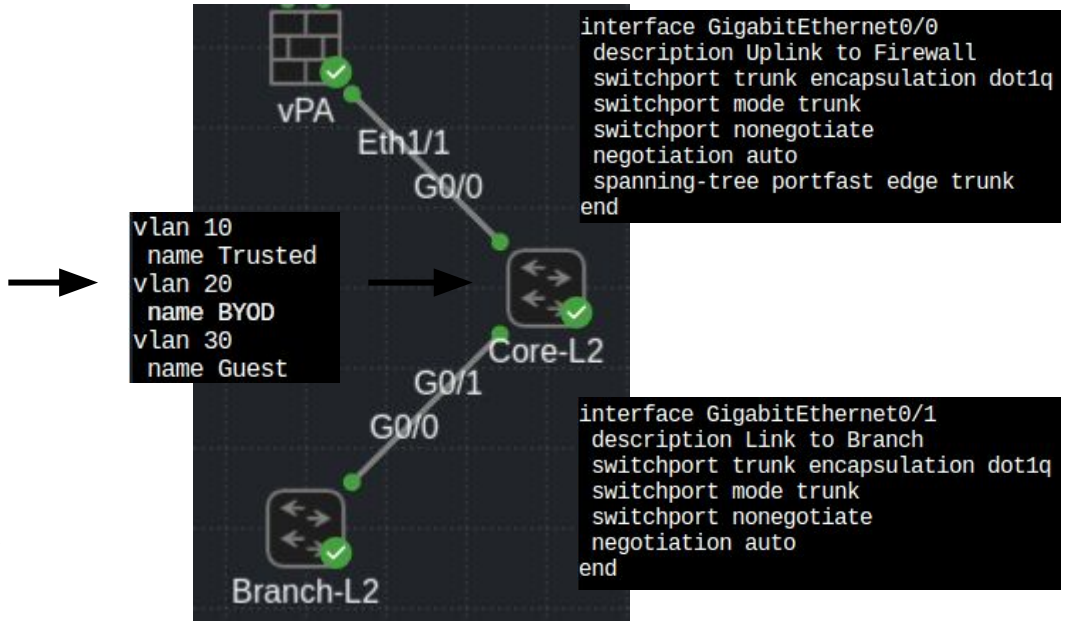


digitalscepter

Network Segmentation

Firewall on a stick

INTERFACE	INTERF... TYPE	LINK STATE	IP ADDRESS	SECURI... 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



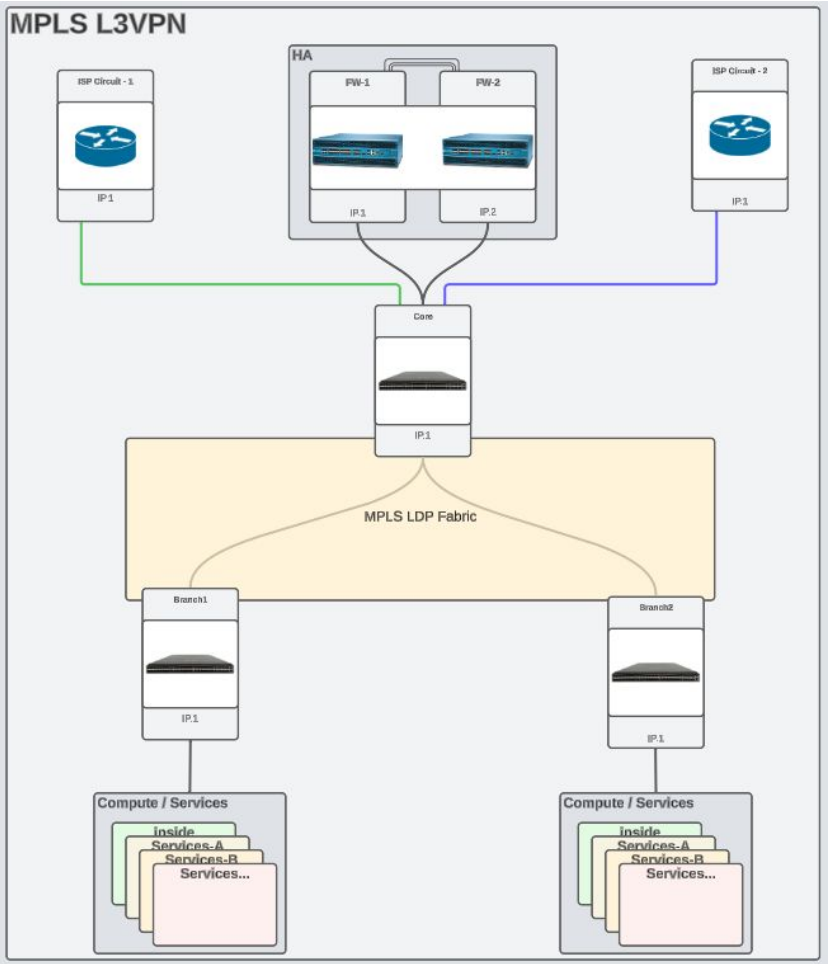
Firewall on a Stick/VLAN Extension:
You only need Layer 2 VLANs and Trunks configured.

digitalscepter

Network Segmentation

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)

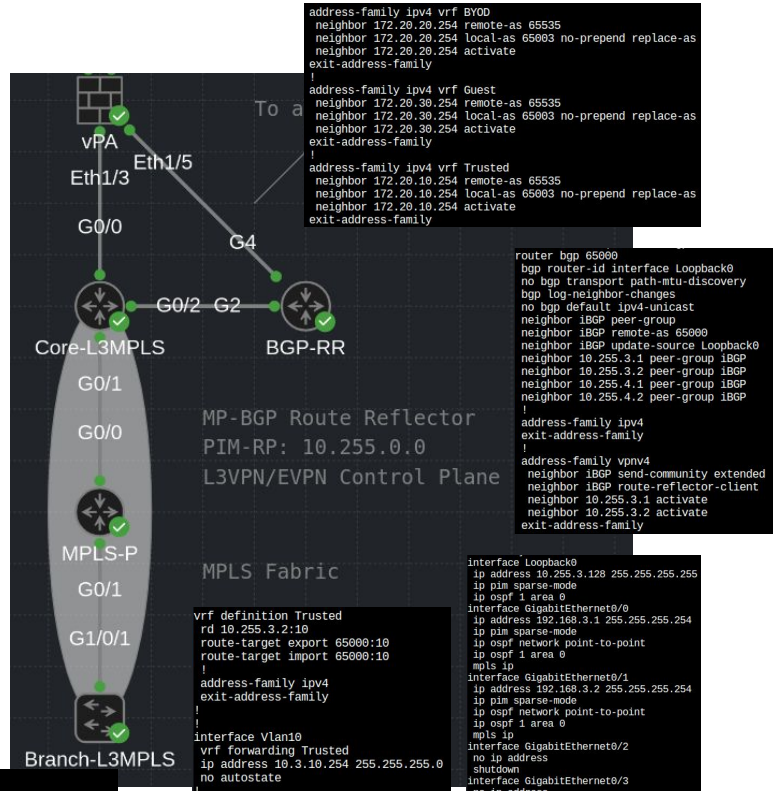


digitalscepter

Network Segmentation

MPLS L3VPN

INTERF...	COMMENT	IP ADDRESS	SECURI... 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



MPLS L3VPN:
iBGP Extended Communities are used to Import/Export Routes per VRF. MPLS LDP will dynamically build a path to carry the data.

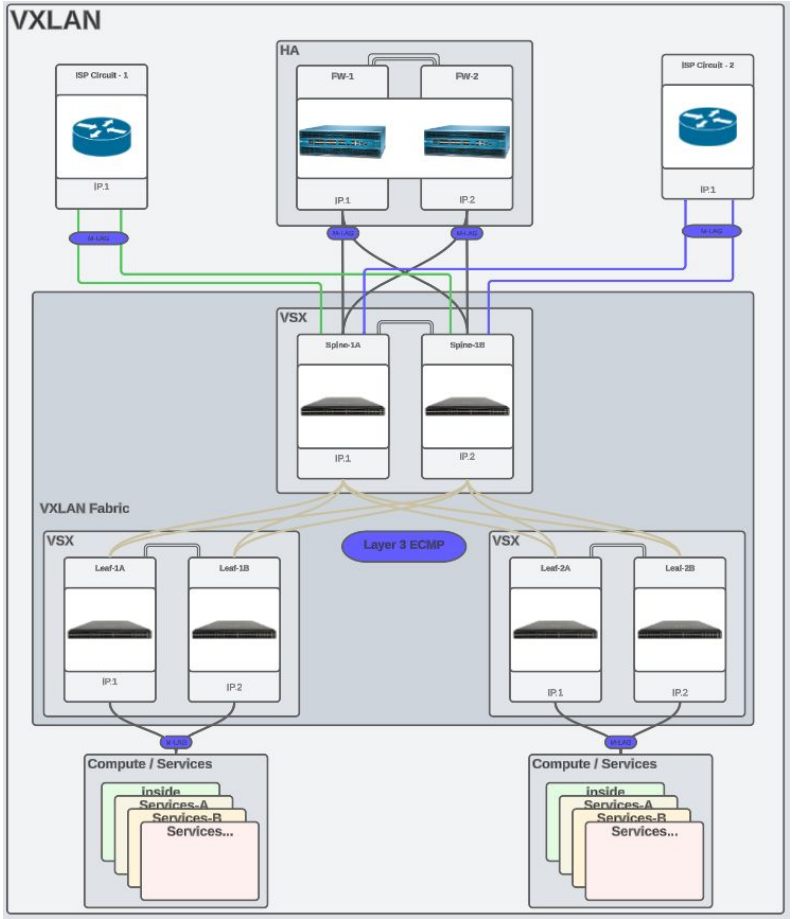
- OSPF is used in the underlay to provide reachability between loopbacks
- BGP-Route Reflector is used for easy scalability.

digitalscepter

Network Segmentation

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)



digitalscepter

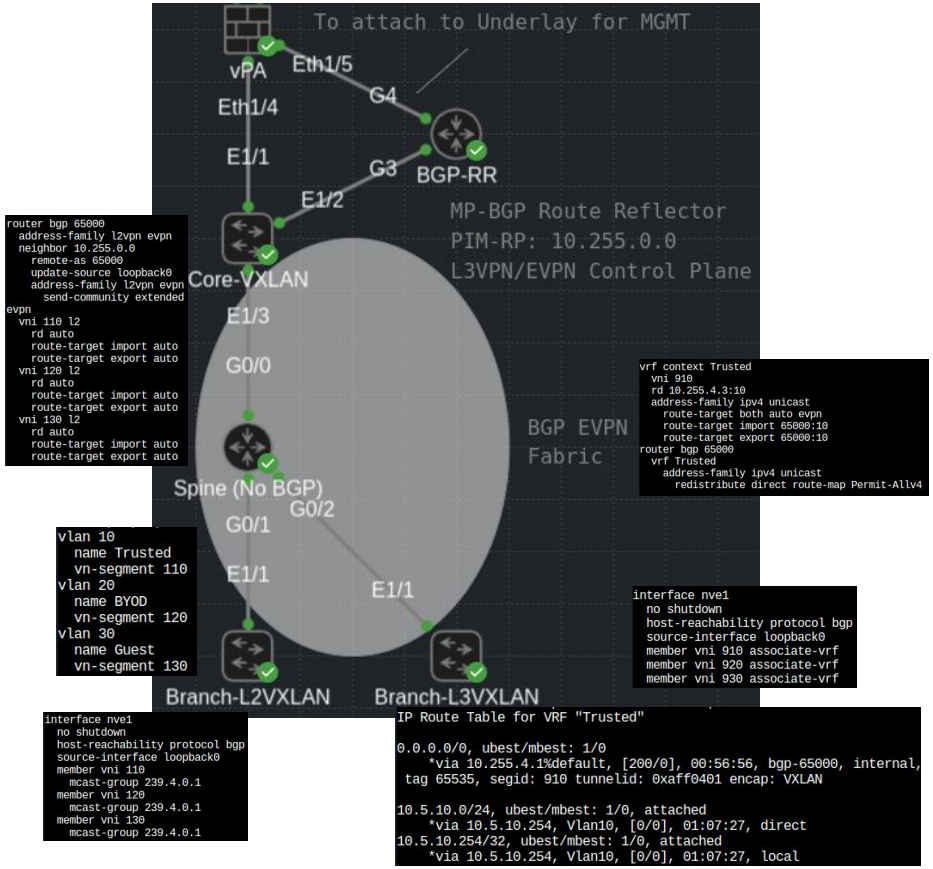
Network Segmentation

BGP EVPN

INTERF...	COMMENT	IP ADDRESS	SECURI... 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.



digitalscepter

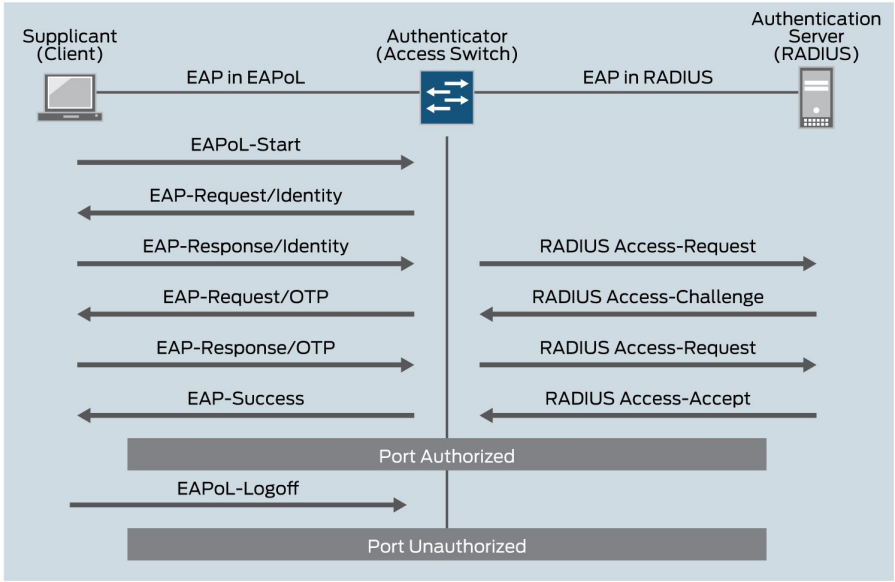
Network Authentication

802.1x Network Authentication

- Provides port-based (or wireless client) authentication at the edge
- Verifies identity before granting access
- Can steer clients to different networks based on RADIUS response
- Username/Password or PKI support
- CoA (Change of Authorization) can trigger switches to quarantine devices.

Limits:

- Limited device posture validation (client still required for full visibility)
- Hard to deploy consistently (nearly all deployments stop short):
  - Devices that lack 802.1x support require MAB (MAC Address Bypass)
  - MAB requirement and lack of inventory leads to exceptions
  - Exceptions lead back to static access VLAN configurations



digitalscepter

First Hop Security

First Hop Security Features

- DHCP Snooping
- Dynamic ARP Inspection
- IP Source Guard
- RA Guard / ND Inspection
- Private VLANs / Port Isolation / Micro-Segmentation

These features provide various protections for devices within the same broadcast domain, mostly to prevent MITM attacks from users on the same network.

Limits:

- Cumbersome to configure / Limited skill-sets
- Break how devices naturally work on the network - which may lead to unexpected results.
- May cause resource contention on some switching platforms.

```
DS-Core-SW1#show ip dhcp snooping binding
MacAddress          IpAddress       Lease(sec)  Type           VLAN  Interface
------------------  --------------  ----------  -------------  ----  --------------------
18:B4:30:EC:91:5C   10.128.0.5      1142728     dhcp-snooping   128   GigabitEthernet1/0/2
AC:BC:B5:EE:7C:B1   10.64.0.42      74380       dhcp-snooping   64    GigabitEthernet1/0/2
80:F3:DA:53:B6:BC   10.64.0.46      75905       dhcp-snooping   64    GigabitEthernet1/0/4
E0:8F:4C:F7:E6:08   10.199.0.1      75643       dhcp-snooping   199   GigabitEthernet1/0/2
64:16:66:D4:CF:DB   10.128.0.6      673093      dhcp-snooping   128   GigabitEthernet1/0/4
8C:26:AA:BA:9A:83   10.64.0.41      74805       dhcp-snooping   64    GigabitEthernet1/0/1
CC:A7:C1:5F:33:87   10.128.0.7      673128      dhcp-snooping   128   GigabitEthernet1/0/4
B8:8A:EC:37:E6:4E   10.64.0.26      85642       dhcp-snooping   64    GigabitEthernet1/0/2
D8:B3:70:52:02:1D   10.254.0.201    50057       dhcp-snooping   254   GigabitEthernet1/0/1
7C:87:CE:8B:81:6C   10.128.0.16     1202545     dhcp-snooping   128   GigabitEthernet1/0/2
7C:87:CE:8B:7D:77   10.128.0.14     1206123     dhcp-snooping   128   GigabitEthernet1/0/5
4A:5A:AE:A8:C2:A8   10.64.0.48      70178       dhcp-snooping   64    GigabitEthernet1/0/1
8C:26:AA:C4:60:52   10.64.0.43      65629       dhcp-snooping   64    GigabitEthernet1/0/2
```

```
ip dhcp snooping vlan 1-4094
ip dhcp snooping
```

```
interface GigabitEthernet1/0/10
 description Core: PVE-1
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 spanning-tree portfast edge trunk
 ip dhcp snooping trust
end
```

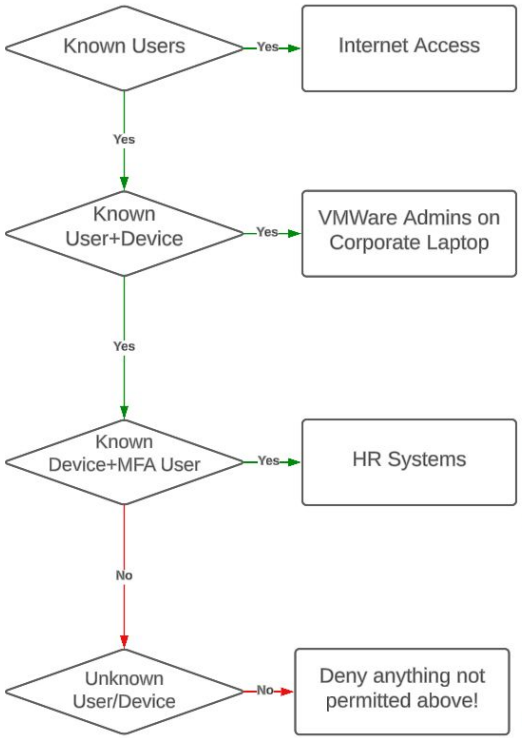
```
vrf context DISTRICT
  vni 20000
  rd auto
  address-family ipv4 unicast
    route-target both 20000:20000

vlan 20
  vn-segment 20100
evpn
  vni 20100 l2
  rd auto
  route-target export 20100:20100
  route-target import 20100:20100

vlan 21
  vn-segment 20101
evpn
  vni 20101 l2
  rd auto
  route-target export 20101:20101
  route-target import 20101:20101

interface Vlan20
  vrf member DISTRICT
  ip address 10.10.20.1/24
  fabric forwarding mode anycast-gateway
interface Vlan21
  vrf member DISTRICT
  ip address 10.10.20.1/24
  fabric forwarding mode anycast-gateway
```

```
vlan 52
  private-vlan isolated
end
```

```
interface GigabitEthernet1/0/9
 description Cust: VoIP [1000Mbit] (MDF)
 switchport access vlan 64
 switchport mode access
 switchport protected
 switchport voice vlan 252
 storm-control broadcast level 30.00
 storm-control multicast level 30.00
 spanning-tree portfast edge
 ip verify source
 ip dhcp snooping limit rate 64
end
```


digitalscepter

Sample Rulebase



Session has been identified with valid credentials

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATI...	SERVICE	ACTION	PROFILE	OPTIONS
Known Users Internet Access	none	universal	inside	any	known-user	any	outside	any	any	any	application-default	Allow		

Valid Credentials and known device

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATI...	SERVICE	ACTION	PROFILE	OPTIONS
Allow VMware Admins to vCenter	none	universal	inside	any	company\vmware_admins	corporate_secured	vmware	any	any	any	any	Allow		

Valid Credentials and known device

	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATI...	SERVICE	ACTION	PROFILE
taff to HR Systems	none	universal	inside	any	company\hr_staff	corporate_secured	hr	hr_sy...	any	any	any	Allow	

NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	SERVICE	AUTHENTICATION ENFORCEMENT
Force MFA for HR Systems	none	inside	any	company\hr_staff	any	hr	hr_systems	any	any	force_mfra

MFA Enforced for Access

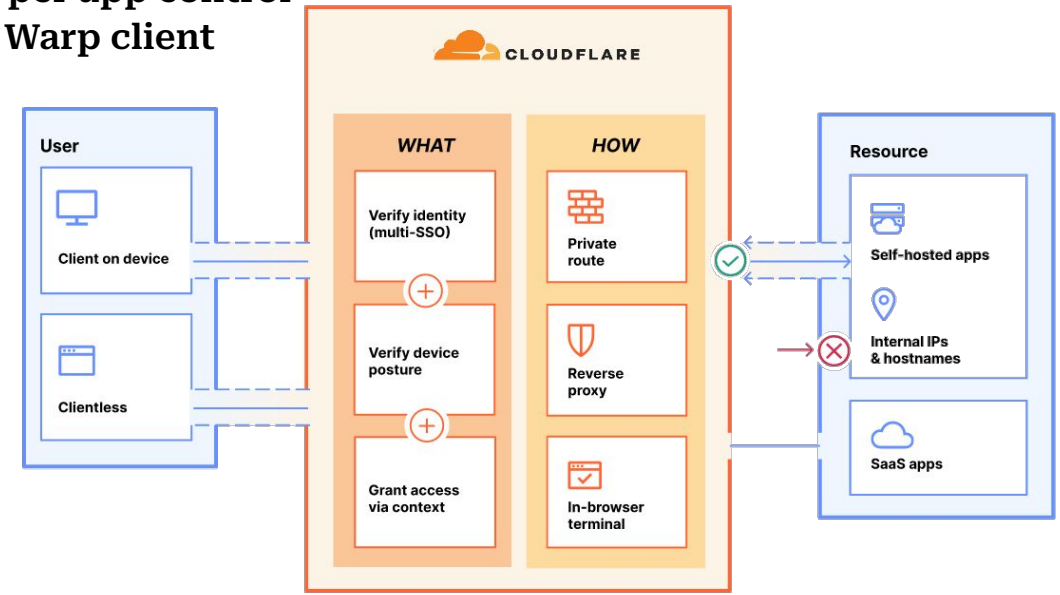
NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATI...	SERVICE	ACTION	PROFILE	OPTIONS
Deny All Unknown	none	universal	inside	any	any	any	any	any	any	any	any	Deny	none	

digitalscepter

Cloud-Delivered Models

Cloudflare Zero Trust

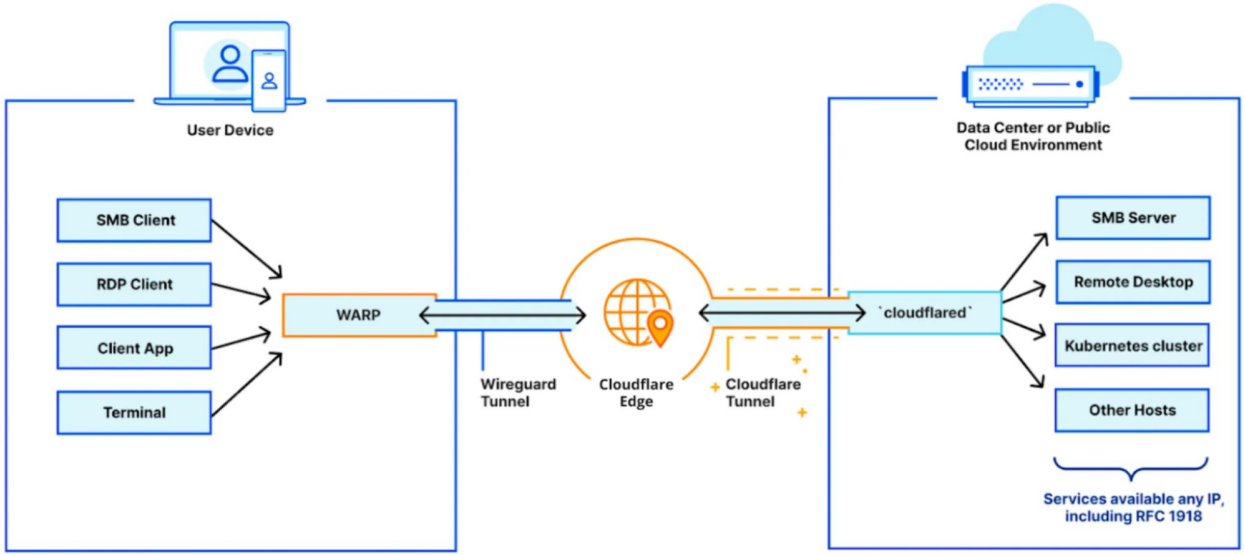
- **Snap-in user identity enforcement**
- **Enforce MFA before app access**
- **Apply policies by group (staff vs admin vs student)**
- **Replace VPN with fine-grained, per app control**
- **Device posture checks through Warp client**



digitalscepter

Extend Zero Trust with cloudflared (Access)

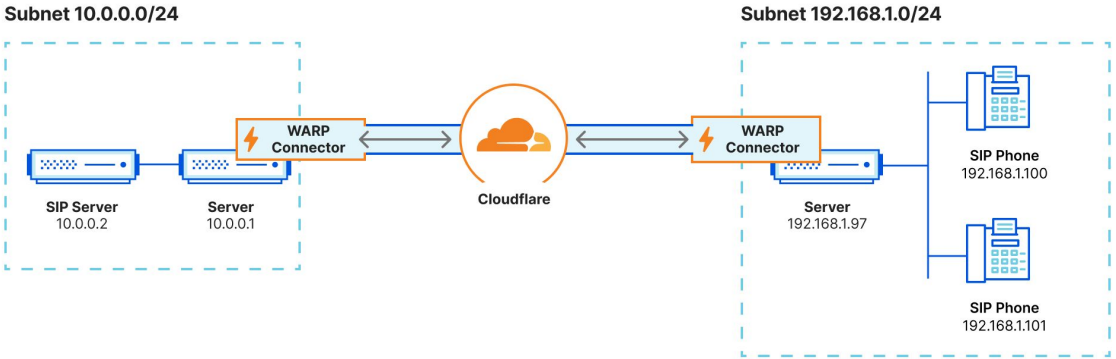
- **Publish internal apps (SIS, staff tools) without client VPN**
- **Outbound-only → no open inbound firewall ports**
- **Removes VPN complexity & risk**
- **Integrated with Cloudflare Edge**

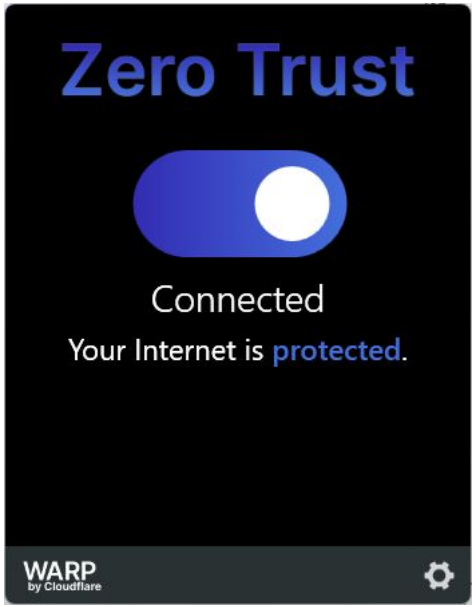


digitalscepter

Cloudflare WARP Client

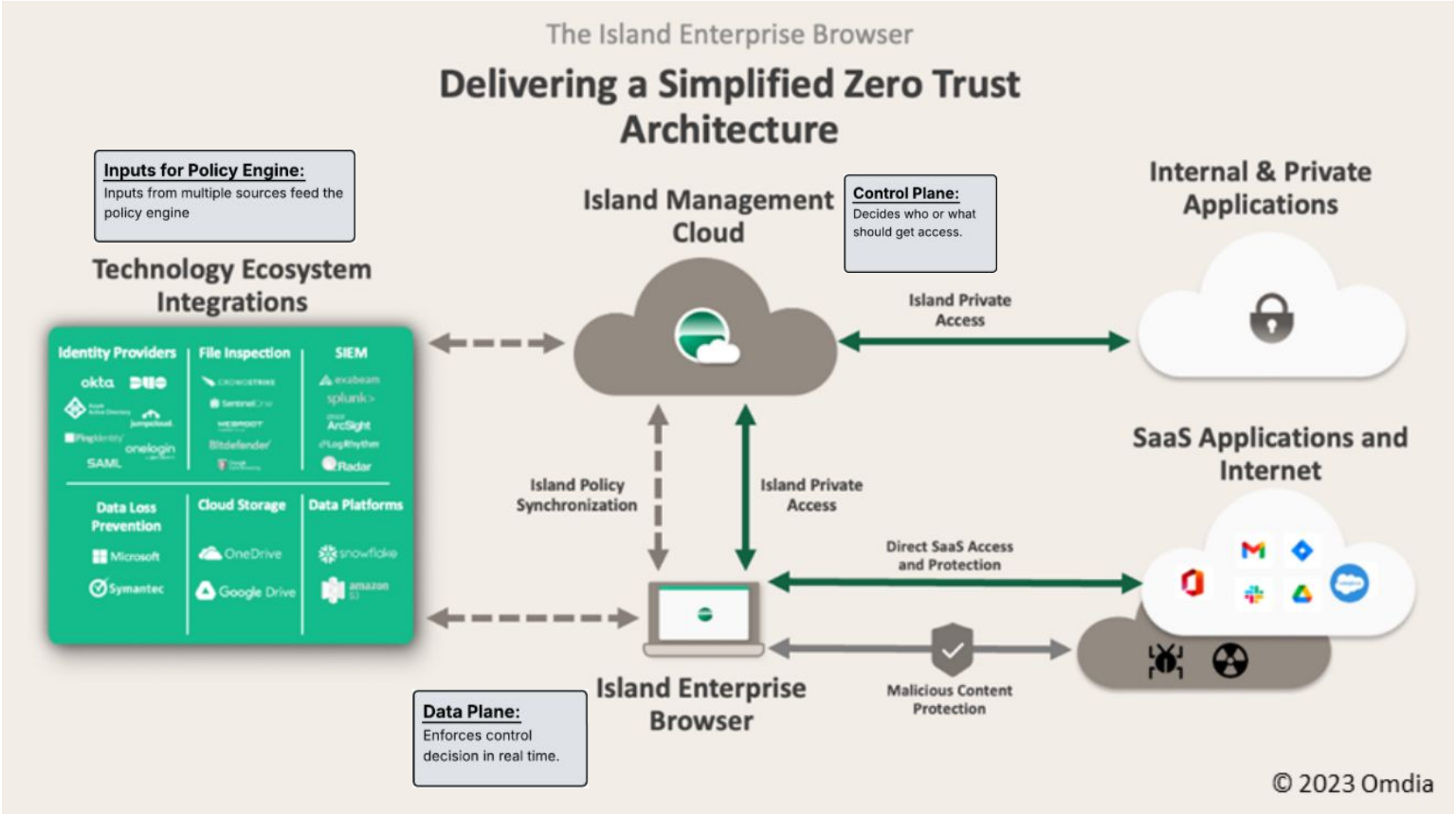
- Installs on Chromebooks, iPads, Windows, macOS, and Linux
- Forces traffic through Cloudflare Gateway
- Supports full tunnels for Zero Trust access (via cloudflared)
- Enables HTTPS inspection & Remote Browser Isolation (RBI)
- Policies follow the user - anywhere, any device
- No SSLVPN to maintain
- Link remote networks through Warp connector





digitalscepter

Enterprise Browsers



digitalscepter

RIVERSIDE COUNTY OFFICE OF EDUCATION
EDWIN GOMEZ, Ed.D. | County Superintendent of Schools

Zero Trust In Action

David Wilkinson
Director, IT Infrastructure & Support
Riverside County Office of Education

What is Galaxy?

- Business Information System
- County Financials, Personnel, Assets, Credentials…
- Previously, only accessible on district network

What Were Our Goals?

- Increase accessibility
- Increase security
- Countywide SSO
- Require multi-factor authentication
- Include districts

Where We Were

HAPROXY

Red Hat

ORACLE

Where We Are

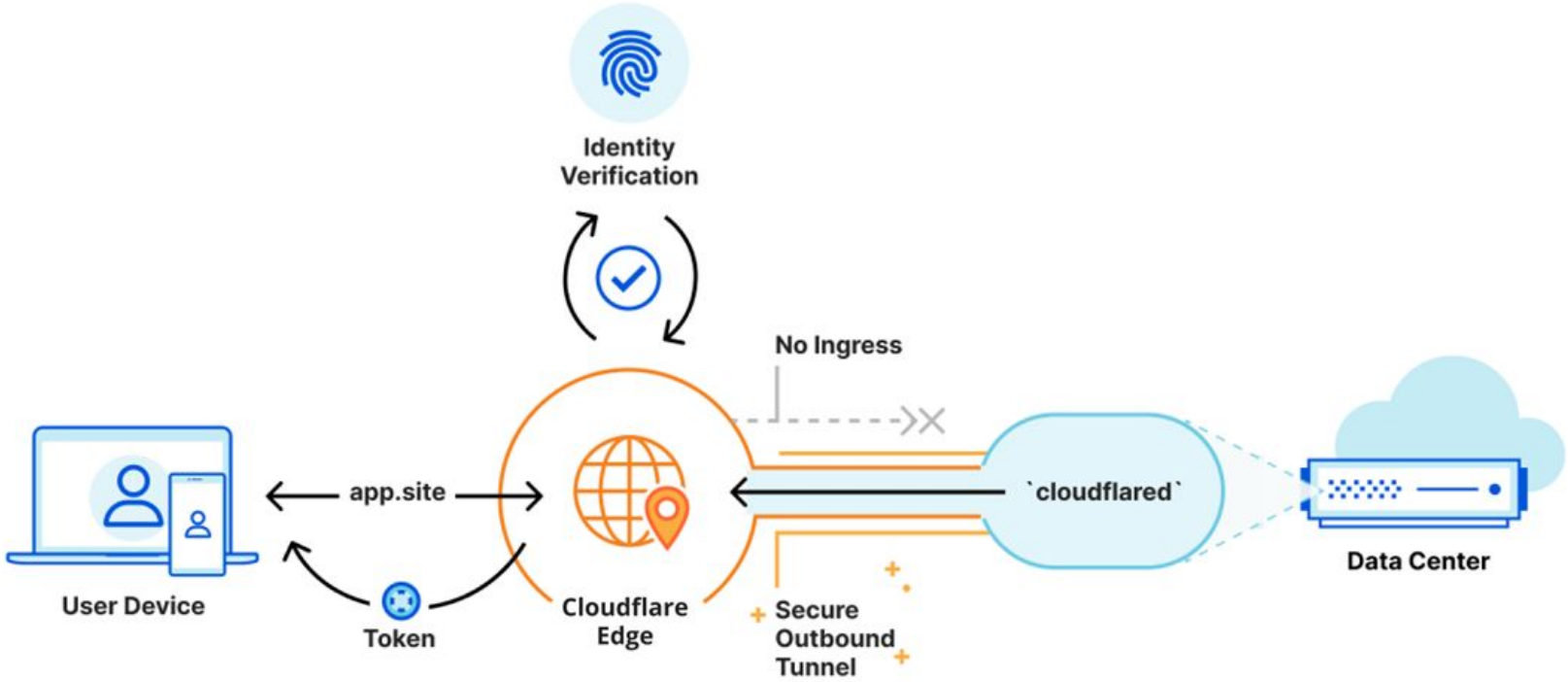
CLOUDFLARE

FusionAuth

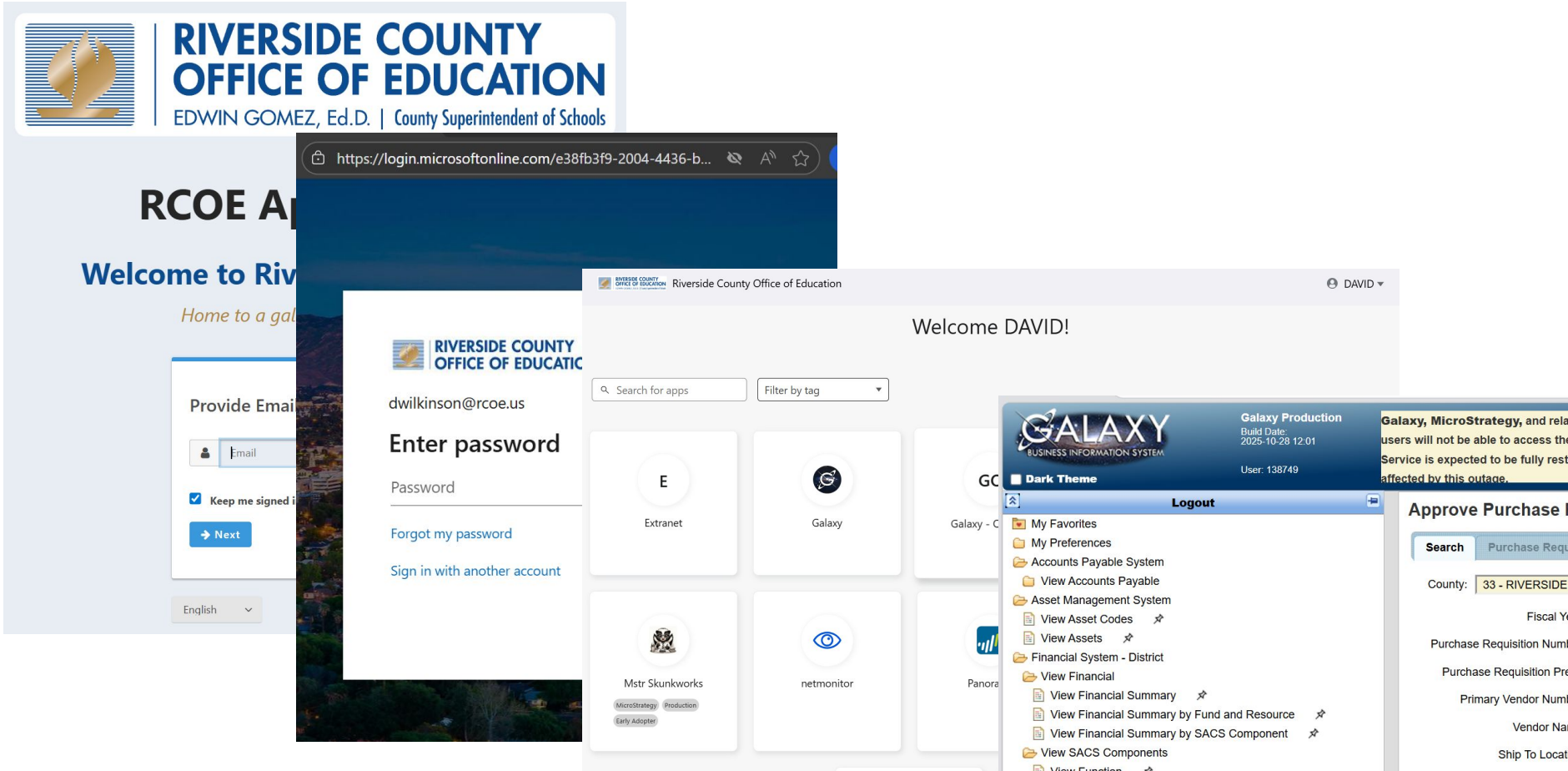
HAPROXY

Red Hat

ORACLE

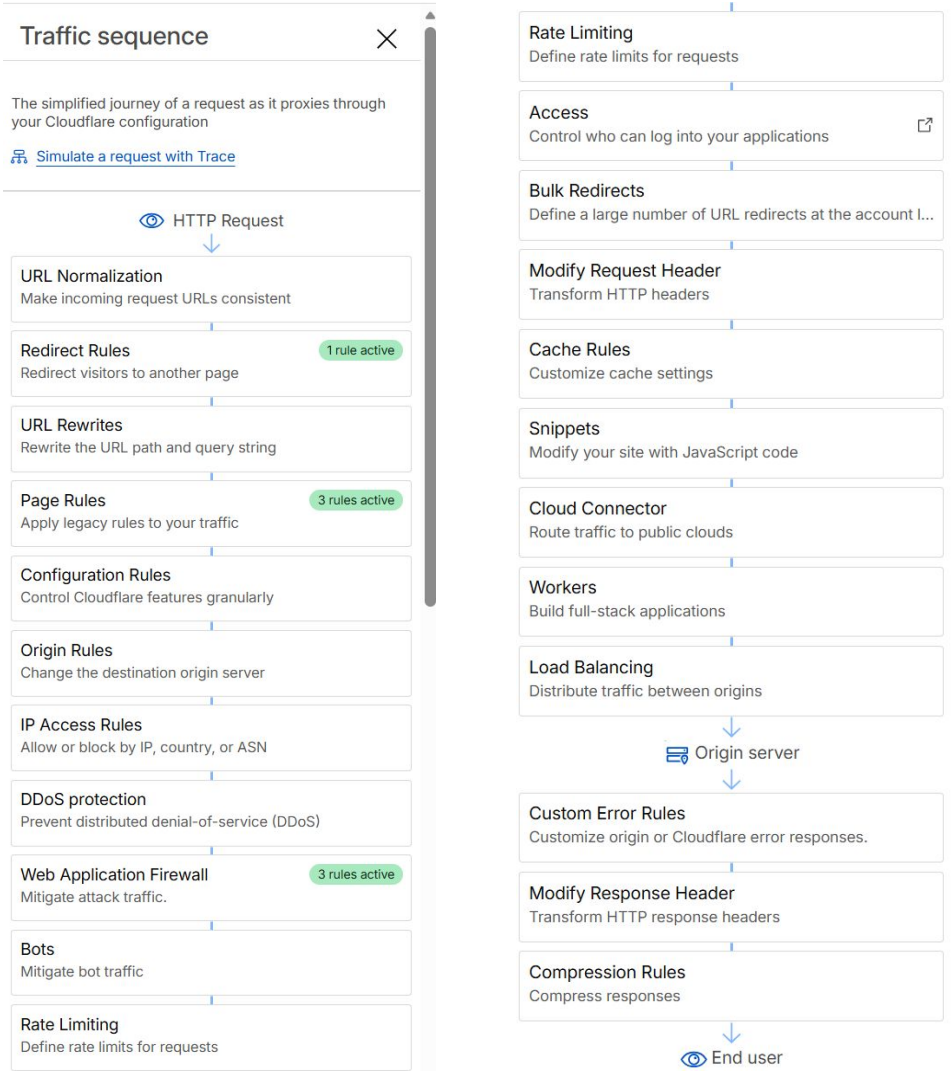

Identity
Verification
No Ingress
app.site
`cloudflared`
Data Center
User Device
Token
Cloudflare
Edge
Secure
Outbound
Tunnel

RIVERSIDE COUNTY
OFFICE OF EDUCATION
EDWIN GOMEZ, Ed.D. | County Superintendent of Schools



RIVERSIDE COUNTY OFFICE OF EDUCATION
EDWIN GOMEZ, Ed.D. | County Superintendent of Schools

Cloudflare Ruleset



Outcomes

- Cloud load balancing
- Improved security
- Improved accessibility
- Delegated district authentication
- MFA Countywide MFA for ERP
- Good support and account exec
- Account life-cycle automation

SSL/TLS encryption

Current encryption mode: Full (strict)

The encryption mode was last changed 4 years ago.

Automatic mode disabled a year ago.

Configure

Traffic Served Over TLS

Last 24 hours

Unknown	TLS v1.2	TLS v1.3
1.16k	4.23k	1.42M

Help

Challenges

- Keeping up with SAML Certificate/OATH Client Secrets
- Rapid cloud development
- Troubleshooting multi-tier application
- Email changes

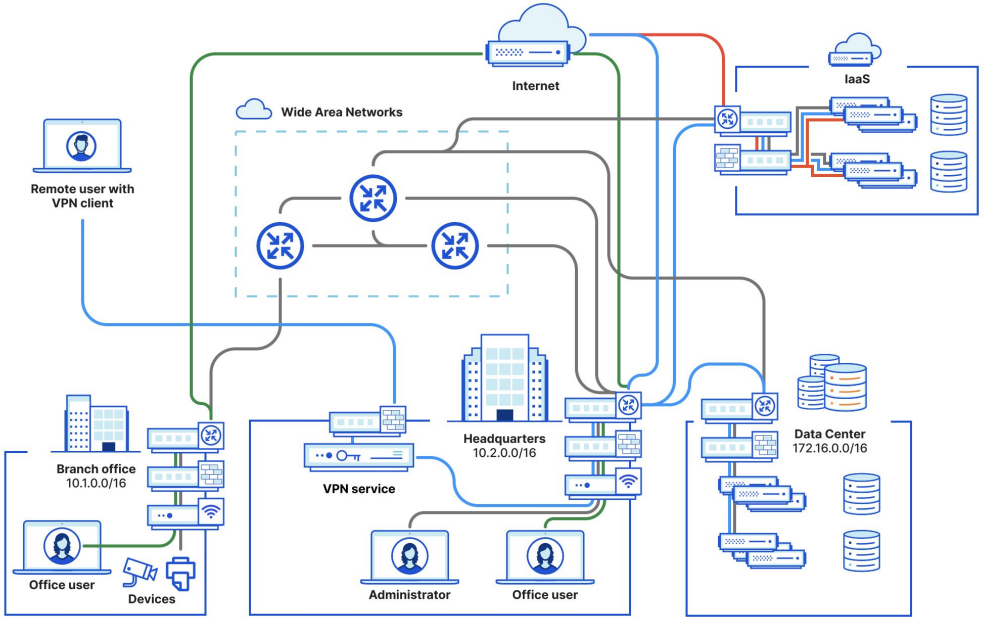
Next Steps

- Complete on-boarding Riverside County districts
  - Cloudflare DNS
  - District zero trust
- Extend zero-trust for RCOE applications

sales@digitalscepter.com
(888) 299-3718

digitalscepter.com

Perimeter Based example



Source:

-

digitalscepter