Secluded Semiconductor scenario

Bob Smith
Director Federal Systems Engineering
Bsmith@Zscaler.com

AGENDA

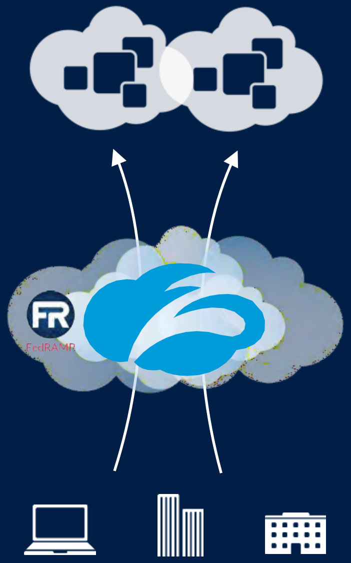
- How does Zscaler fit into M-22-09 Mandate
- Securing Secluded SemiConductor’s environment
- Disaster Strikes!
- Securing IOT /OT in a DR scenario
- Securing Smart City traffic
- Restoration of Services
- Q&A

Mapping to the M22-09 Mandate and the Zero Trust Pillars

Zscaler Federal Security Cloud

Securely transform IT for a cloud world

Governance policies connect users to apps from anywhere, over any network based on TIC 3.0 Framework



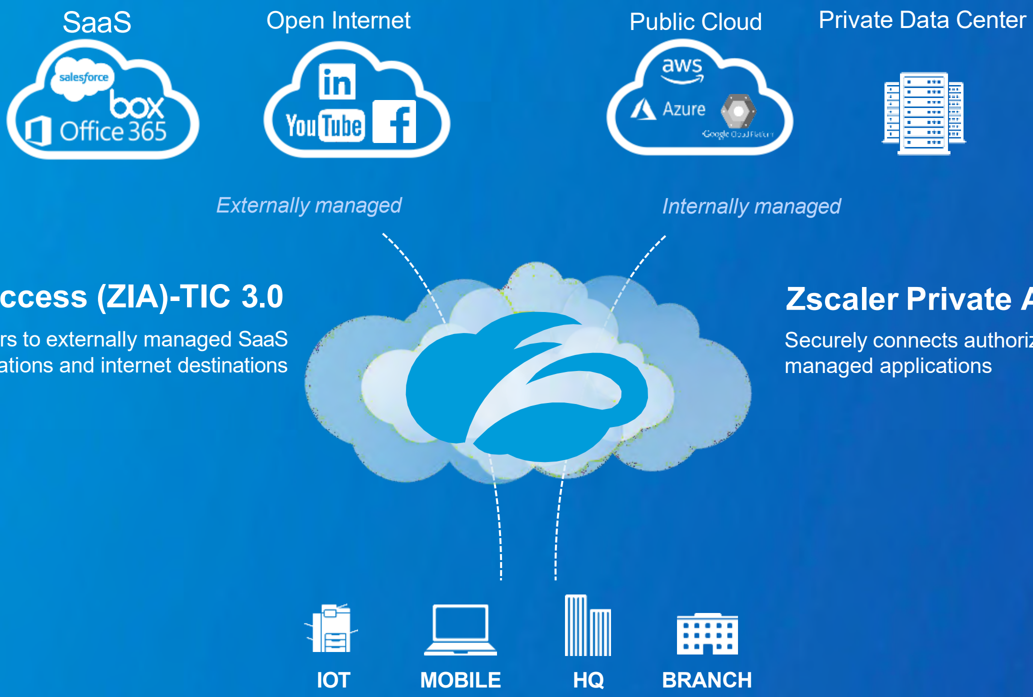
FAST. SECURE. RELIABLE.

Market Leader **50** of the **Forbes Global 2000**
Nasdaq: ZS

Proven Scale **400** **transactions** processed daily

FedRAMP High + Moderate + IL 5 **5** **data centers** across the U.S.
*For FedRamp High we leverage AWS Gov Cloud

Zscaler: Secure and fast access to any app, from anywhere



SaaS

Open Internet

Public Cloud

Private Data Center

Externally managed

Internally managed

IOT

MOBILE

HQ

BRANCH

Zscaler Internet Access (ZIA)-TIC 3.0

Securely connects users to externally managed SaaS applications and internet destinations

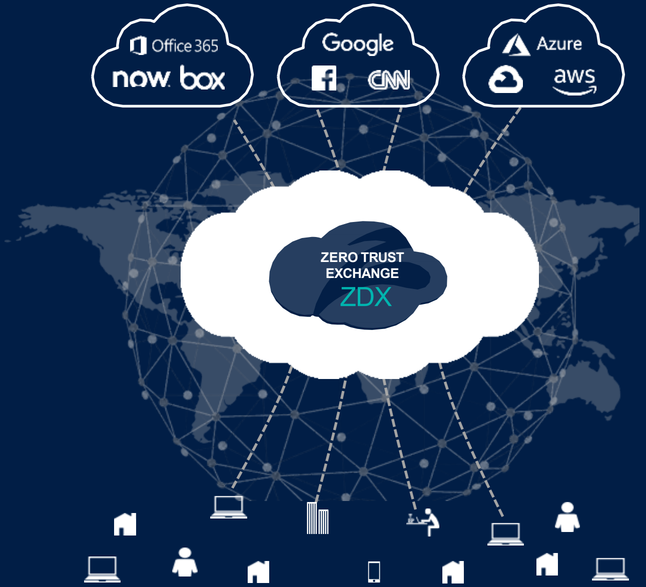
Zscaler Private Access (ZPA)- Zero Trust

Securely connects authorized users to internally managed applications

Any device, any location, on-network or off-network

Zscaler Digital Experience: Visibility From The End-user To The App

Proactive visibility and diagnostics of end-user experience issues



End-to-end visibility

from user out to SaaS/web applications

Proactive monitoring

of performance anomalies on end-user device, network (local/WAN) and apps

Simplified monitoring workflow

with real-world performance benchmarking and scoring

Isolate issues faster

eliminating IT delays and finger pointing

Zscaler Zero Trust Connectivity

Securely connect authorized users, devices and workloads over any network

Shift in Network Architectures

Early ’70s
IBM SNA
Proprietary for IBM systems

Past 30 years
IP Networking
Routable IP networks connect users, devices and apps

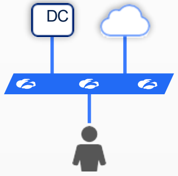
Next 30 years
Zero Trust
Non-routable networks. Connections are established through a Zero Trust Exchange

Zero Trust Connectivity

1. A ‘switchboard’ connects users, devices, apps using business policies
2. Apps are destinations, not network resources. The network is transport.
3. Users, devices, apps are never on the same network

Users

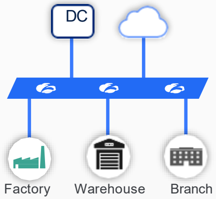
Direct app access, no VPN



Work from anywhere
Any internet connection

Sites - Branches, Factories, Warehouses

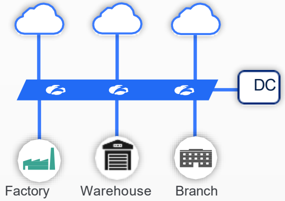
Local internet breakouts (SD-WAN), shortest path



Connects users and devices
IoT/OT - badge readers, remote printing, cameras

IaaS/PaaS -Cloud to Cloud, data center or sites

Routable Mesh to Zero Trust Network Access



Multi-cloud and hybrid environments (Cloud to DC)
No virtual FWs needed

Designed to minimize latency

150 locations - shortest path to connect. Peering in Internet Exchanges. Direct fiber connectivity with Microsoft

Reliable, better quality of service

Prioritize apps (M365 or Zoom over YouTube).
Premium China connectivity

Superior Security

Eliminate VPN (employees, Third parties), No lateral threat movement, App segmentation without network segmentation

Federal Zero Trust Strategy

> *The Federal Government can no longer depend on conventional perimeter-based defenses to protect critical systems and data.*
>
> *-President Biden*

Overview and purpose

On January 26, 2022, the Office of Management and Budget (OMB) released the Federal Zero Trust Strategy in support of Executive Order 14028, "Improving the Nation's Cybersecurity", to adapt civilian agencies' enterprise security architecture to be based on zero trust principles.

The strategy is published as *OMB Memorandum M-22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles"* . The goal of the strategy is to accelerate agencies toward a **shared baseline of early zero trust maturity.**

OMB memo M-22-09 provides guidance on how to achieve the Zero Trust mandates of the Executive Order. It further codifies the importance of moving off of legacy security structures into a Zero Trust architecture to include:

- *No longer depend on conventional perimeter-based defenses to protect critical systems and data.*
- *Provide secure access applications over the public Internet, without relying on a virtual private network (VPN).*
- *Encrypting DNS and HTTP traffic using TLS 1.3 for all internal and external connections to include APIs.*

The memo includes deadlines for implementation plans, inventories, policy changes, and more. ***Each agency's acceptable implementation plan is due by March 2022.***

Zero-Trust

Capability Model

ZERO TRUST

CORE PILLARS

CORE CAPABILITIES

DATA	DEVICE & ENDPOINT	NETWORK & ENVIRONMENT	APPLICATION & WORKLOAD	USER	VISIBILITY & ANALYTICS	AUTOMATION & ORCHESTRATION
Data Loss Prevention	Device Authorization	API Integration	DevSecOps	User Authentication	Discovery & Baselining	API Standards
Data Classification	HW & SW Inventory	Fully Encrypted Traffic	Application Delivery	User Authorization	Machine Learning	Incident Response
Metadata Mgmt.	Cloud-based Baseline Enforcement	Common Service Access	Micro Segmentation	Cybersecurity Access Policy	Advanced Threat Protection	Artificial Intelligence
Data Encryption	Compliance Enforcement	Network Segmentation	Application Segmentation	Privilege Access Mgmt.	Monitoring and Auditing	Security Orchestration, Automation & Response (SOAR)
Data Segmentation	Device Authentication	Cloud Access Security Broker (CASB)	Software Chain Supply	Single Identity Platform	Risk Evaluation & Dynamic Risk Scoring	
Dynamic Data Masking (DDM)	Cloud-based Software Deployment & Mgmt.	Software Defined Networking (SDN)	Software Defined Compute	MFA	Security and Information Event Management (SIEM)	
Fully-automated Data Tagging via ML/AI	Intelligence for Endpoint Response	Software Defined Perimeter *(Access to Apps and Data)*	Application Approved/ Prohibited List	In-session Monitoring		
Data Rights Management (DRM)		Application Proxy	Application Visibility & Access *(Anytime, Anywhere)*	ABAC		
		Management and Monitoring		Key Mgmt.		
				Transparent Authentication		

Threat Score, Risk Score, Target Valuation, Triage Priority, and Compliance Score (snapshots & trend)

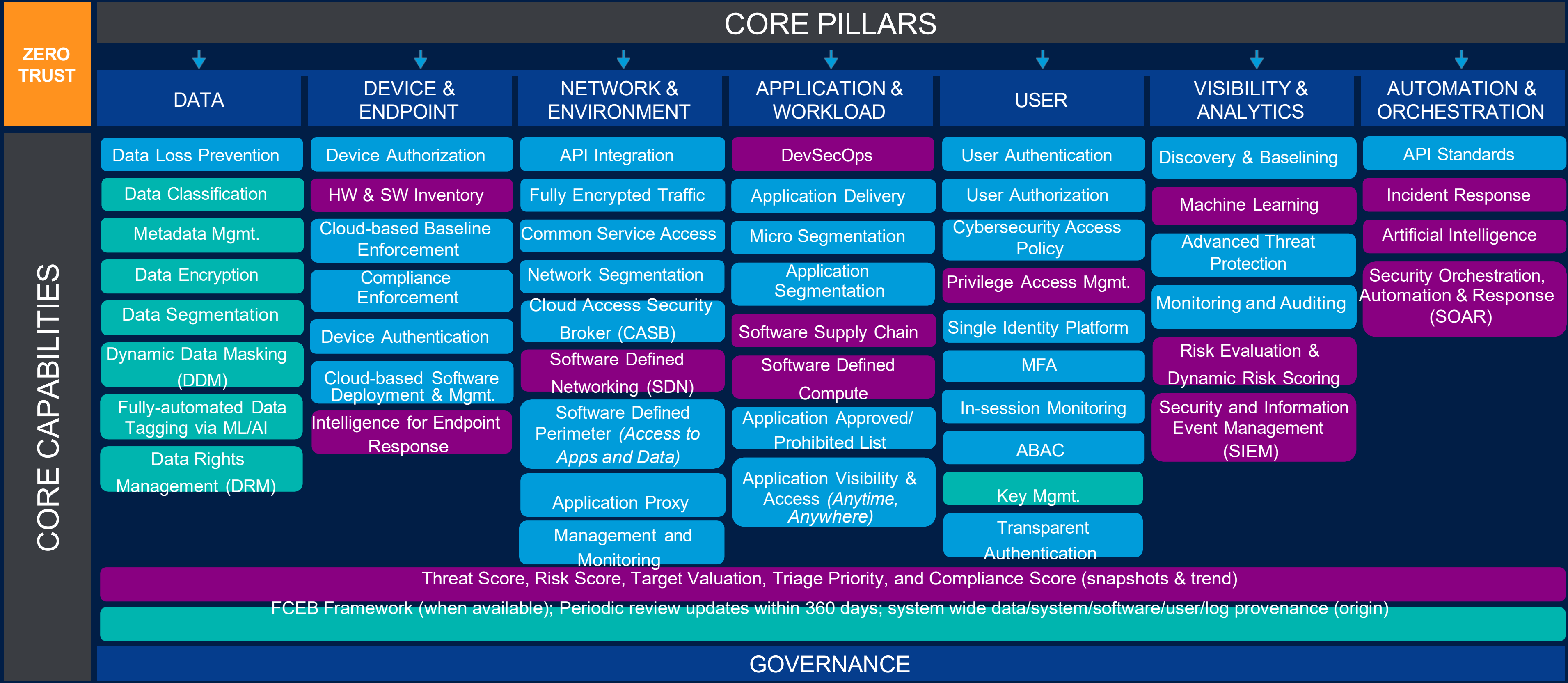
FCEB Framework (when available); Periodic review updates within 360 days; system wide data/system/software/user/log provenance (origin)

GOVERNANCE

Zero-Trust Architecture

Capability Mapping to Zscaler

🟦 zscaler Meets | 🟪 Partially Meets | 🟩 Not Applicable



ZERO TRUST

CORE PILLARS

CORE CAPABILITIES

DATA

- 🟦 Data Loss Prevention
- 🟩 Data Classification
- 🟩 Metadata Mgmt.
- 🟩 Data Encryption
- 🟩 Data Segmentation
- 🟩 Dynamic Data Masking (DDM)
- 🟩 Fully-automated Data Tagging via ML/AI
- 🟩 Data Rights Management (DRM)

DEVICE & ENDPOINT

- 🟦 Device Authorization
- 🟪 HW & SW Inventory
- 🟦 Cloud-based Baseline Enforcement
- 🟦 Compliance Enforcement
- 🟦 Device Authentication
- 🟦 Cloud-based Software Deployment & Mgmt.
- 🟪 Intelligence for Endpoint Response

NETWORK & ENVIRONMENT

- 🟦 API Integration
- 🟦 Fully Encrypted Traffic
- 🟦 Common Service Access
- 🟦 Network Segmentation
- 🟦 Cloud Access Security Broker (CASB)
- 🟪 Software Defined Networking (SDN)
- 🟦 Software Defined Perimeter *(Access to Apps and Data)*
- 🟦 Application Proxy
- 🟦 Management and Monitoring

APPLICATION & WORKLOAD

- 🟪 DevSecOps
- 🟦 Application Delivery
- 🟦 Micro Segmentation
- 🟦 Application Segmentation
- 🟪 Software Supply Chain
- 🟪 Software Defined Compute
- 🟦 Application Approved/ Prohibited List
- 🟦 Application Visibility & Access *(Anytime, Anywhere)*

USER

- 🟦 User Authentication
- 🟦 User Authorization
- 🟦 Cybersecurity Access Policy
- 🟪 Privilege Access Mgmt.
- 🟦 Single Identity Platform
- 🟦 MFA
- 🟦 In-session Monitoring
- 🟦 ABAC
- 🟩 Key Mgmt.
- 🟦 Transparent Authentication

VISIBILITY & ANALYTICS

- 🟦 Discovery & Baselining
- 🟪 Machine Learning
- 🟦 Advanced Threat Protection
- 🟦 Monitoring and Auditing
- 🟪 Risk Evaluation & Dynamic Risk Scoring
- 🟪 Security and Information Event Management (SIEM)

AUTOMATION & ORCHESTRATION

- 🟦 API Standards
- 🟪 Incident Response
- 🟪 Artificial Intelligence
- 🟪 Security Orchestration, Automation & Response (SOAR)

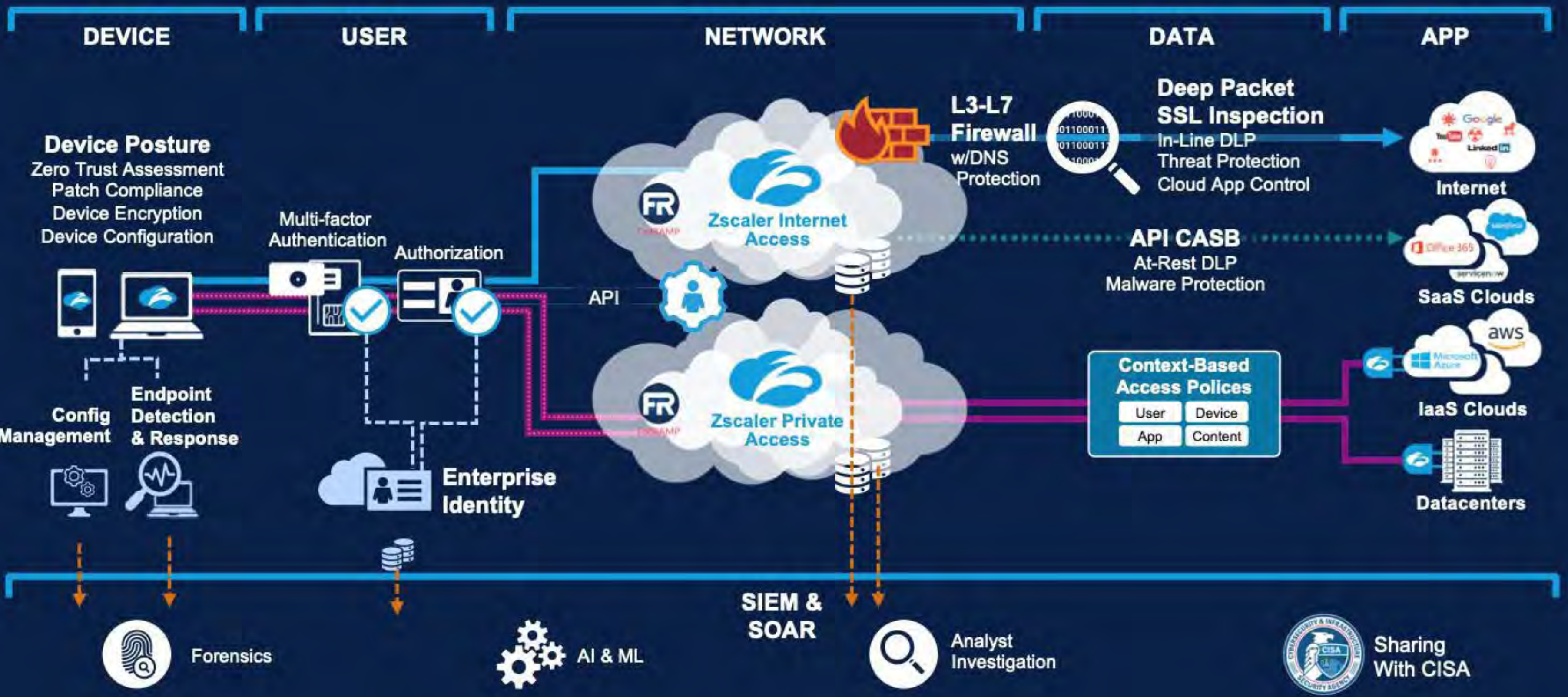
🟪 Threat Score, Risk Score, Target Valuation, Triage Priority, and Compliance Score (snapshots & trend)

🟩 FCEB Framework (when available); Periodic review updates within 360 days; system wide data/system/software/user/log provenance (origin)

GOVERNANCE

Zscaler Zero Trust Architecture

Capability Mapping Diagram



DEVICE

USER

NETWORK

DATA

APP

Device Posture
Zero Trust Assessment
Patch Compliance
Device Encryption
Device Configuration

Config Management

Endpoint Detection & Response

Multi-factor Authentication

Authorization

Enterprise Identity

API

Zscaler Internet Access

Zscaler Private Access

L3-L7 Firewall
w/DNS Protection

Deep Packet SSL Inspection
In-Line DLP
Threat Protection
Cloud App Control

API CASB
At-Rest DLP
Malware Protection

Context-Based Access Polices

User	Device
App	Content

Internet

SaaS Clouds

IaaS Clouds

Datacenters

SIEM & SOAR

Forensics

AI & ML

Analyst Investigation

Sharing With CISA

Securing your cloud transformation

Securing Secluded Semiconductor’s Users and IOT/OT

Semiconductor Island Background

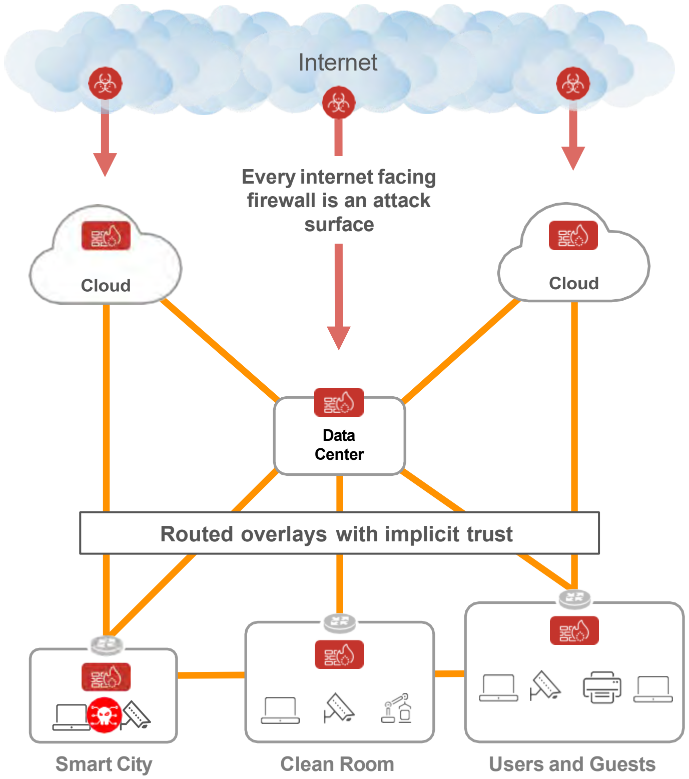
Background information

- **Secluded Semiconductors, Inc. has established a manufacturing facility on an island *1,000* miles from the continental United States (U.S.).**
- **Manufacturing runs 24x7x365**
- **1000 Employees- 20 IT, 50 Clerical, 500- Manufacturing, 400- in support functions**
- **Power is provided by green energy self sustaining – Solar , Wind with Standby deisel generators**
- **Shipping port on the island handles raw materials for chips as well as goods and services for the employees.**

Migrating Semiconductor Island’s to Zero Trust

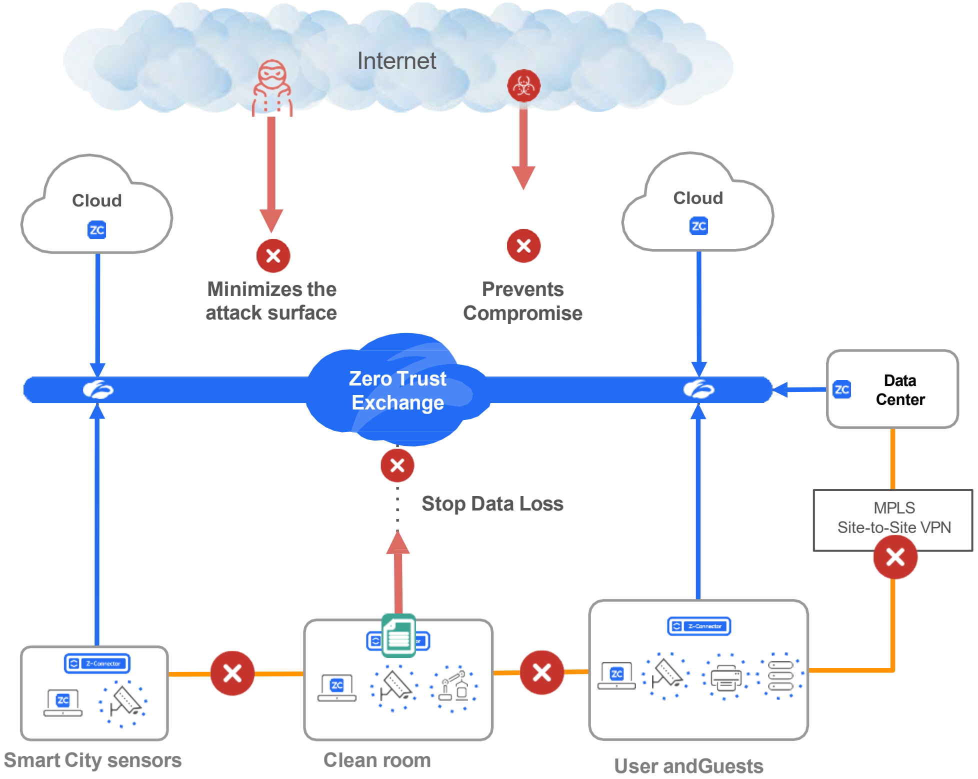
Prior architecture

Mesh of site-to-site VPNs


Internet
Every internet facing firewall is an attack surface
Cloud
Cloud
Data Center
Routed overlays with implicit trust
Smart City
Clean Room
Users and Guests

Zero Trust Architecture

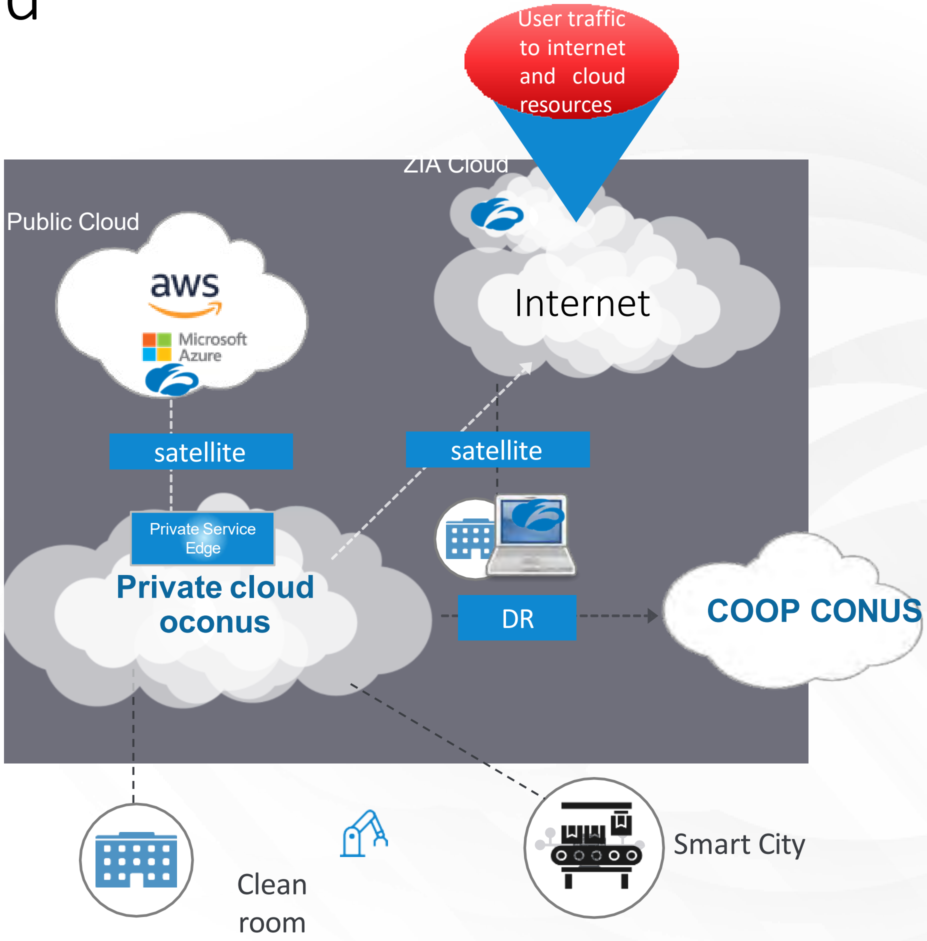
Connects any site without routed overlays or VPNs



Eliminates Lateral Threat Movement

Overall Semi Conductor Island

- 3 separate systems- Clean Room, Production, SCADA systems
- Smart sensors across infrastructure – terrabytes of information
- Smart City – measures and balances power needs across city and manufacturing needs
- Organization uses a mix of Hybrid cloud- on premises data center, COOP data center on Mainland, public cloud for other processes like order processing, social media, etc,
- Satellite and 5 G cellular coverage for island residents and manufacturing



Securing your cloud transformation

Zscaler and Airgap for Semiconductor Island Use case

Safe Harbor

Forward-Looking Statements

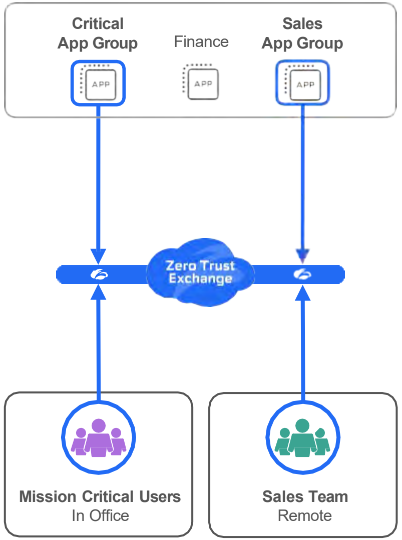
This presentation has been prepared by Zscaler, Inc. (“Zscaler”) for informational purposes only and not for any other purpose. Nothing contained in this presentation is, or should be construed as, a recommendation, promise or representation by the presenter or Zscaler or any officer, director, employee, agent or advisor of Zscaler. This presentation does not purport to be all-inclusive or to contain all of the information you may desire.

This presentation contains forward-looking statements. All statements other than statements of historical fact, including statements regarding our planned products and upgrades, business strategy and plans and objectives of management for future operations of Zscaler are forward-looking statements. These statements involve known and a significant number of unknown risks, uncertainties, assumptions and other factors that could cause results to differ materially from statements made in this message, including any performance or achievements expressed or implied by the forward-looking statements. Moreover, we operate in a very competitive and rapidly changing environment, and new risks may emerge from time to time. It is not possible for us to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results or outcomes to differ materially from those contained in any forward-looking statements we may make. Additional risks and uncertainties that could affect our financial and operating results are included in our most recent filings with the Securities and Exchange Commission. You can locate these reports though our website at http://ir.zscaler.com or on the SEC website at www.sec.gov.

In some cases, you can identify forward-looking statements by terms such as “anticipate,” “believe,” “continues,” “contemplate,” “could,” “estimate,” “expect,” “explore” “intend,” “likely,” “may,” “plan,” “potential,” “predict,” “project,” “should,” “target,” “will” or “would” or the negative of these terms or other similar words. Zscaler based these forward-looking statements largely on its current expectations and projections about future events that it believes may affect its business. Actual outcomes and results may differ materially from those contemplated by these forward-looking statements. All forward-looking statements in this message are based on information available to us as of the date hereof, and we do not assume any obligation to update the forward-looking statements provided to reflect events that occur or circumstances that exist after the date on which they were made.

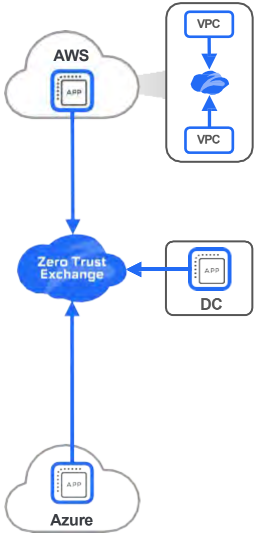
Four Areas of Zero Trust Segmentation

1 User Segmentation
Remote, In Office



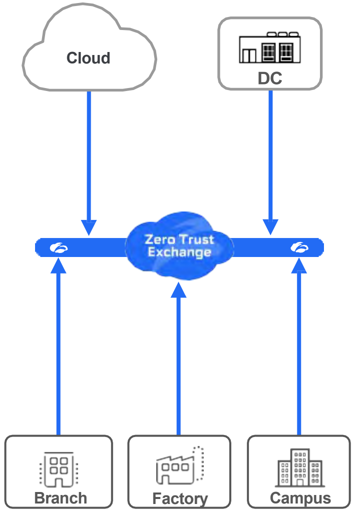
Only Mission Critical Users can access Critical Apps
Sales Team can only access Sales Group Apps

2 Workload Segmentation
Cloud, DC, Branch



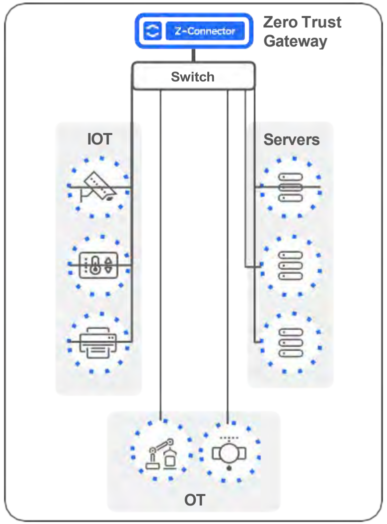
VPC to VLAN
VPC to VPC / VNET
Workload to Workload

3 Branch/Campus Segmentation
Between branches, campus, cloud, DC



Zero Trust SD-WAN (No Site-to-Site VPN / MPLS)
Each branch is a Starbucks

4 Device Segmentation
Inside branch, factory, campus

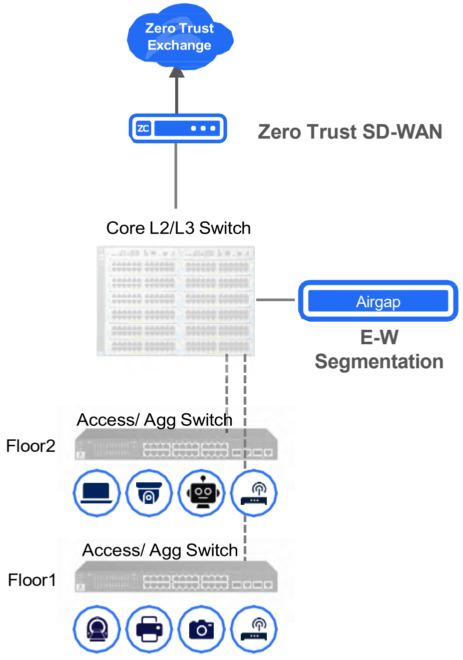


Automated IoT / OT Segmentation
Segment of 'one' for every device

Minimizes the risk of business disruption to due to ransomware propagation

Agentless Zero Trust Segmentation

How it Works



Shipping Today

1 Assumes the role of default gateway for VLANs

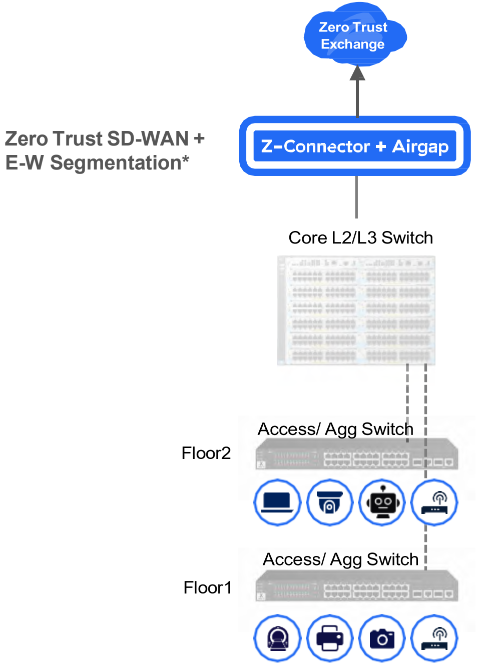
2 Auto-provisions every endpoint with a /32 subnet mask through the intelligent DHCP proxy

3 Automatically classifies device into groups (IT, IoT, OT, Servers)

4 Enforces group-based policies e.g. RDP access to cameras denied except from Admins

5 Ransomware Kill Switch™ enforces policies based on threat level for faster incident response

✓ Up to 80Gbps/Node
✓ 70 Microsecond Latency
✓ HA active/standby
✓ Hitless Upgrade

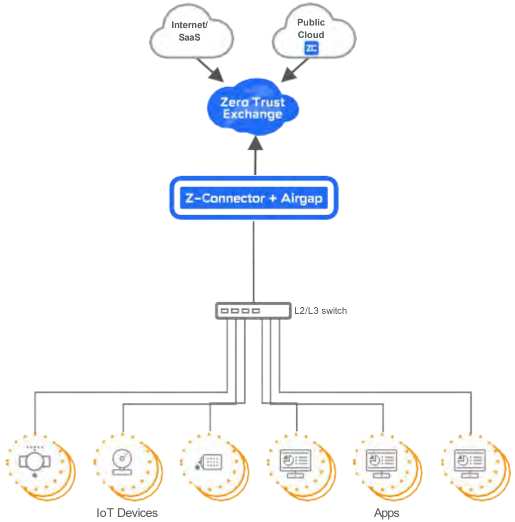


**Coming soon.*

Innovative and proven technology. Distributed scale.

Zscaler + Airgap: Key Use Cases

East-West Firewall Replacement

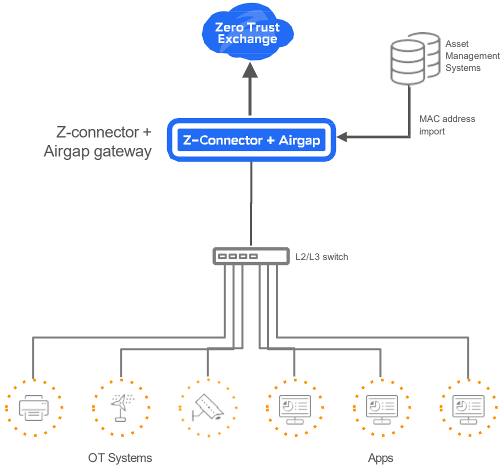


Automatic provisioning of every device into a segment of one (/32)

Autonomous grouping of devices, users and apps

Dynamic policy enforcement for east-west traffic

IT/OT Segmentation

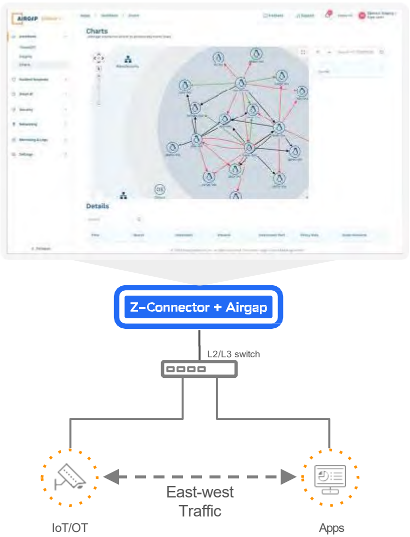


Device discovery and classification; Segregate IT devices from OT devices.

Automatic isolation of unknown MAC addresses

Integrates with asset management systems for dynamic policy updates

Automatic Device Discovery & Classification



Automatic device discovery and classification for east-west LAN traffic

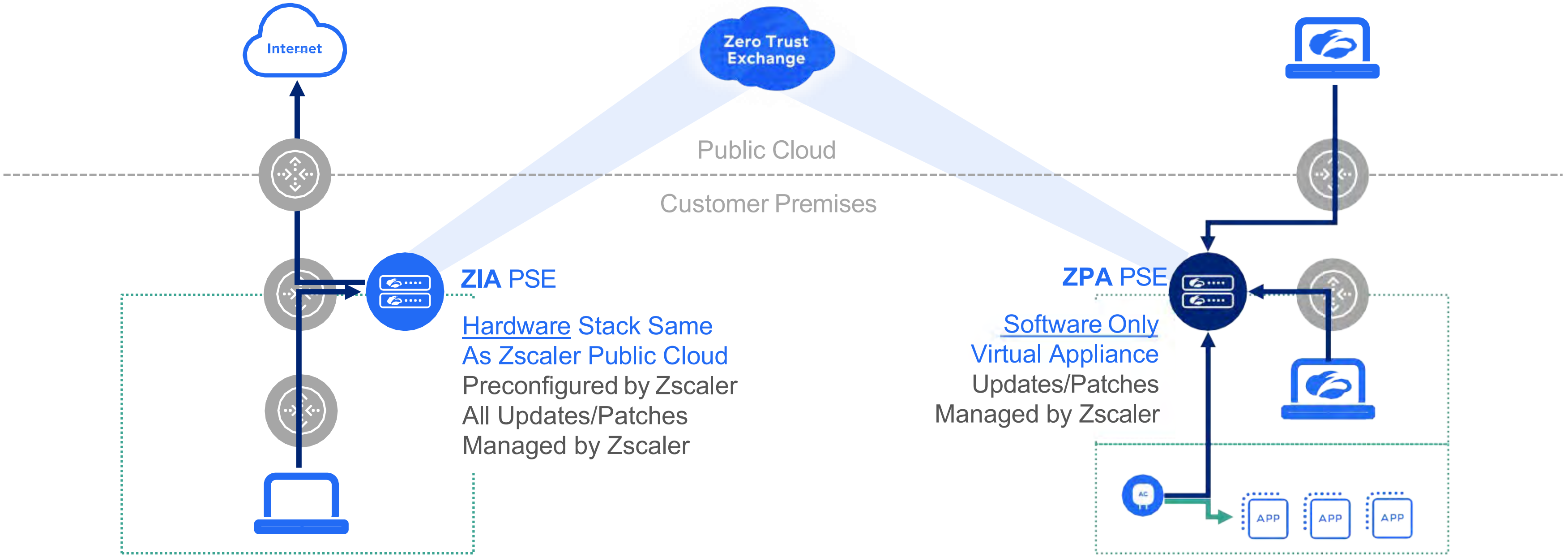
Realtime automapping and policy management

Querying, tagging and alert monitors with 3rd party integrations

Comprehensive use cases. Eliminate operational complexity and reduce cost.

What's a Private Service Edge (PSE)?

NOTE: PSEs ARE AN OPTIONAL COMPONENT



ZIA PSE

Hardware Stack Same As Zscaler Public Cloud
Preconfigured by Zscaler
All Updates/Patches Managed by Zscaler

ZPA PSE

Software Only Virtual Appliance
Updates/Patches Managed by Zscaler

Zscaler ***Internet*** Access PSE

Internet/SaaS Security & Data Protection

Zscaler ***Private*** Access PSE

Secure Optimized Remote Access to Private Apps

Use Cases (Why Would this be a good architectural fit)

Regulatory Restrictions

Rare scenarios where use of Zscaler data centers is limited in certain countries

Geographically Isolated Locations

Provide optimal secure connectivity in situations where latency to nearest Zscaler data center is suboptimal

Example: Islands or countries with poor Internet connectivity

Sites With High User Density or Traffic Loads

Large campus environments

Example: 30K+ users in a single location

Source IP Dependent Legacy Apps

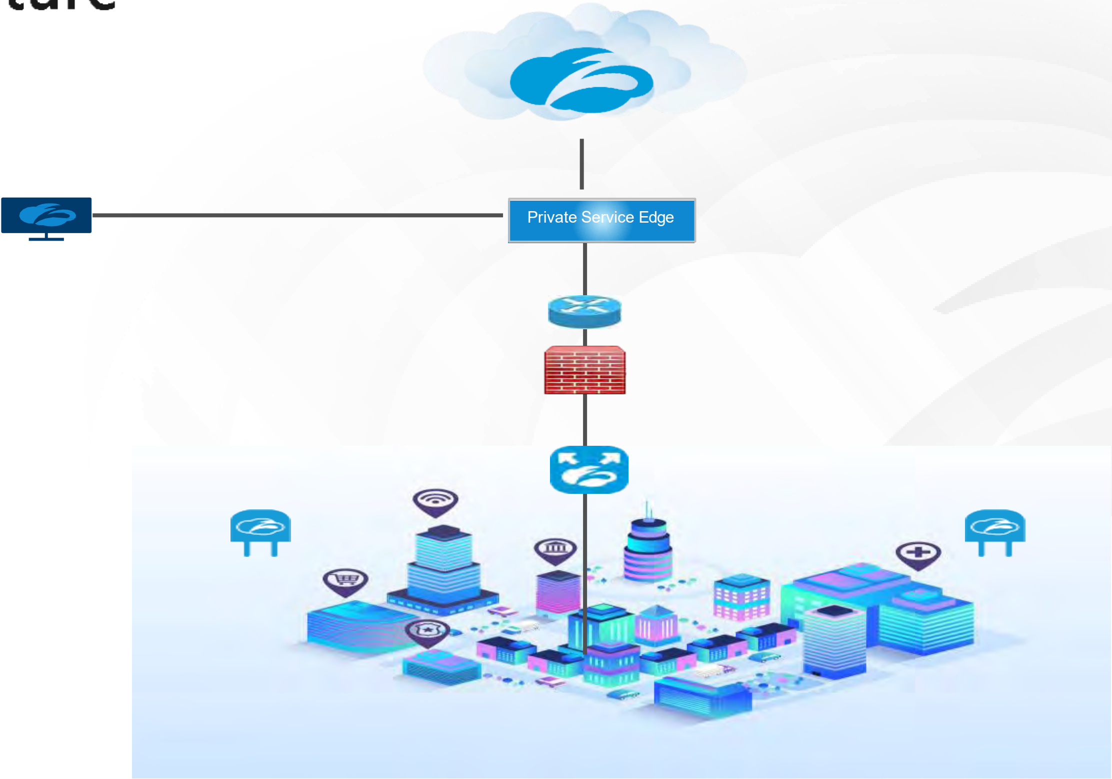
Organizations with a *large number or high volume* of Internet resources with source IP dependent access requirements.

Example: Large hospital systems accessing 1000s of online medical journals

Smart City Architecture

Managed Zscaler User Accessing Smart City Devices for Maintenance

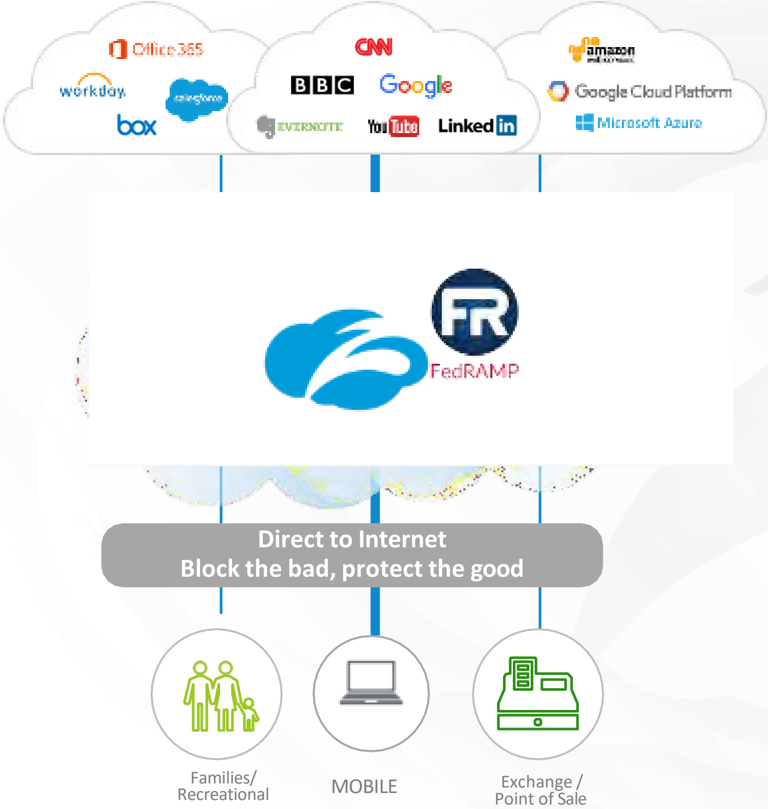
Leverage Air Gap for segmentation and discovery of the sensors



Secure Employees, Guest Wi-Fi access / Point of Sale

Employees and Contractor Use Cases

- Supports Secure Internet access for Residents of Semiconductor Island
- Supports Contractor access
- Exchange / Point of Sale systems



Direct to Internet
Block the bad, protect the good

Families/ Recreational

MOBILE

Exchange / Point of Sale

Securing your cloud transformation

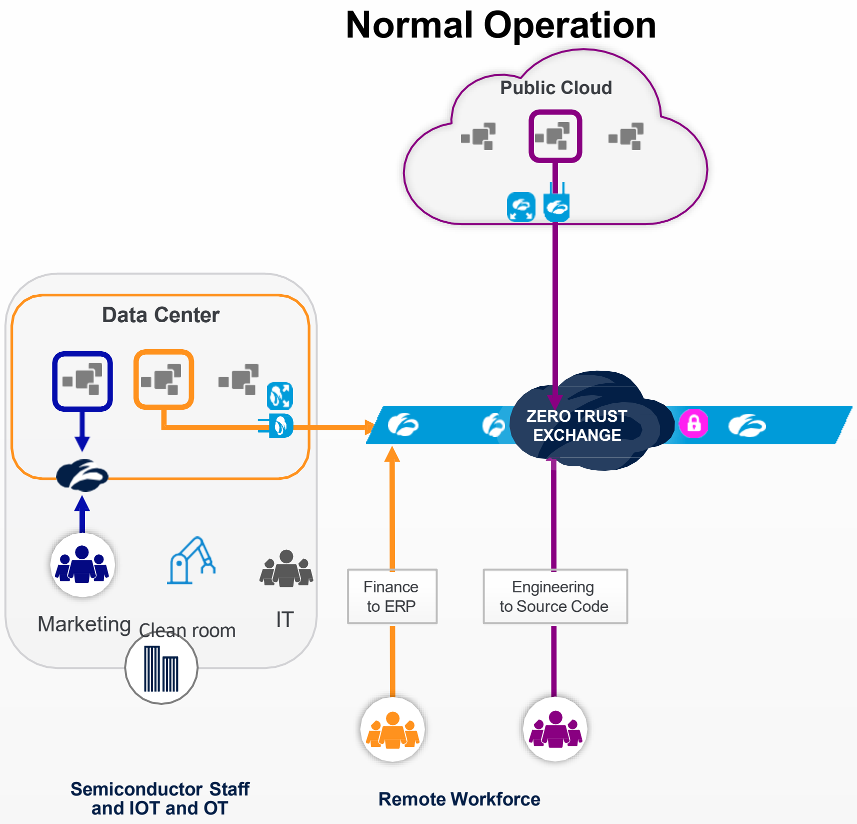
Disaster Hits !

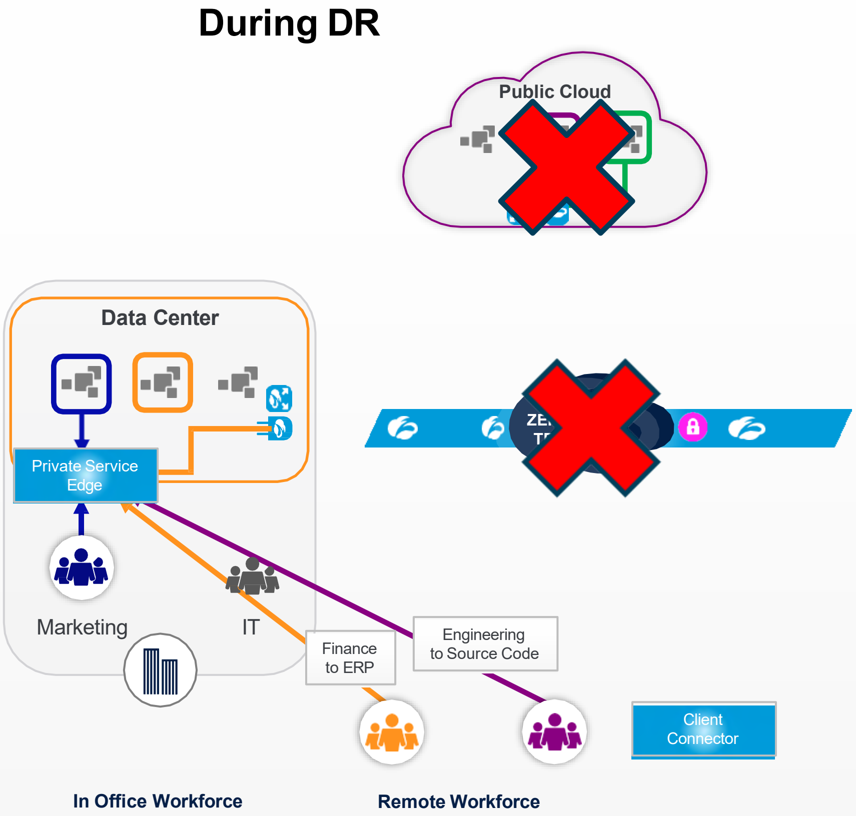
Rule #1 lets not make a bad situation worse- why Zero Trust is important

- If Jurassic Park Teaches us anything…. People will capitalize on a bad situation .

- Ransomware or other attacks during a crisis would be the worst possible scenario

Proposed Zero Trust DR Design





Customer-controlled disaster recovery – Assumptions

- Outage can last multiple hours to days
- Zscaler Cloud Infrastructure is completely unavailable
- During this period
    - Mission critical applications will be made available
    - Availability is critical, specific capabilities will be unavailable
        - Full Authentication
        - Policy configuration and updates
        - Enrollment of new clients
        - Logging and Analytics

Customer Initiated Disaster Recovery

- Supports **cloud free** functionality mode
- Customer **initiates** manual DR mode switch
- Provides access to customer identified **critical** applications
- Supports **enrolled users** in the system prior to DR switching
- Requires **deployment** and maintenance of ZPA **Private Service Edges** and **Client Connector**

Practical limitations while operating in DR mode

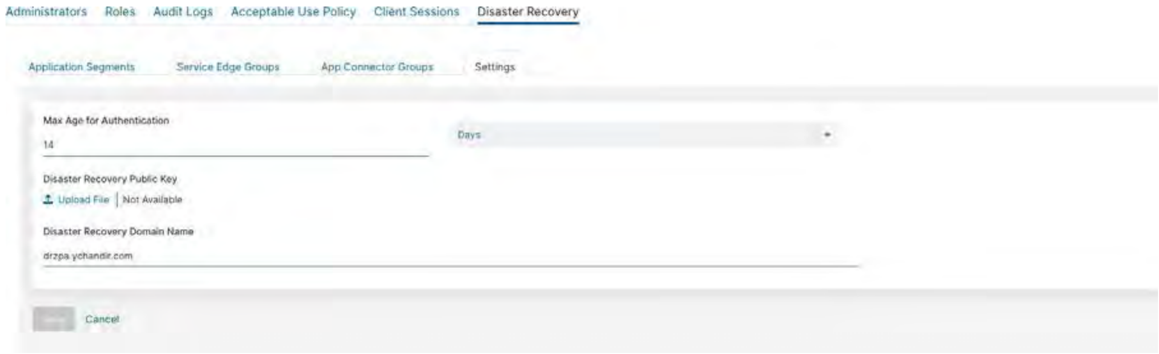
- Access through the Client Connector only
- No new users or enrollments during the DR period
- No policy or configuration updates
- No logging and analytics
- Does not support SIPA, Browser Access, Isolation, Branch/Cloud Connector, Inspection, Deception use cases

5 Steps

1. Configure DNS
2. Enable Private Service Edge for DR Mode
3. Enable App Connector for DR Mode
4. Select Business Critical App Segments for DR Mode
5. Configure App Profiles

ZPA authentication Grace Period

By default we provide a 14 days reauthentication grace period for users that need to have their credentials revalidated to the ZPA IdP



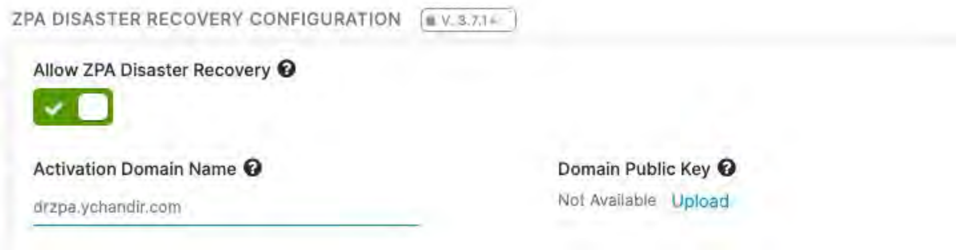
Max Age for Authentication
14
Days

Disaster Recovery Public Key
Not Available

Disaster Recovery Domain Name
drzpa.ychandir.com

Testing Disaster Recovery Mode

ZPA Disaster Recovery Test Mode can be triggered by setting the TXT Value of the Activation Domain Name to b=Test. This will allow a small set of users assigned to a test App Profile, with Test Mode Enabled, to ensure the DR activation, and behavior is as expected. An example would be to validate the needed domains are added to the custom destinations pac file to allow a needed app to function in DR mode.

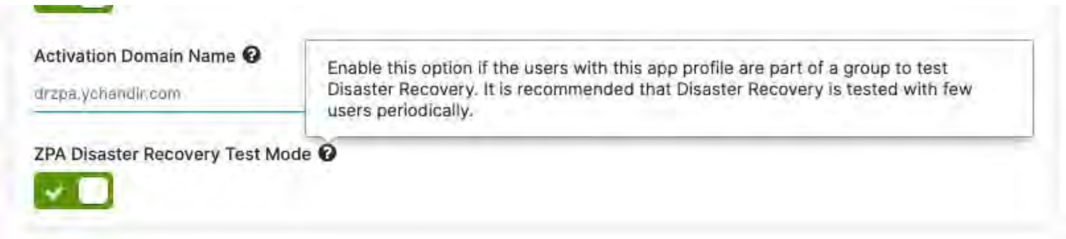


ZPA DISASTER RECOVERY CONFIGURATION V. 3.7.1

Allow ZPA Disaster Recovery ✓

Activation Domain Name: drzpa.ychandir.com

Domain Public Key: Not Available



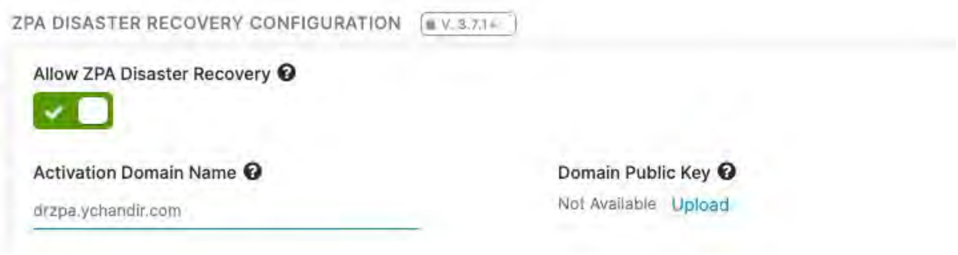
Activation Domain Name: drzpa.ychandir.com

Enable this option if the users with this app profile are part of a group to test Disaster Recovery. It is recommended that Disaster Recovery is tested with few users periodically.

ZPA Disaster Recovery Test Mode ✓

Testing Disaster Recovery Mode

ZPA Disaster Recovery Test Mode can be triggered by setting the TXT Value of the Activation Domain Name to b=Test. This will allow a small set of users assigned to a test App Profile, with Test Mode Enabled, to ensure the DR activation, and behavior is as expected. An example would be to validate the needed domains are added to the custom destinations pac file to allow a needed app to function in DR mode.

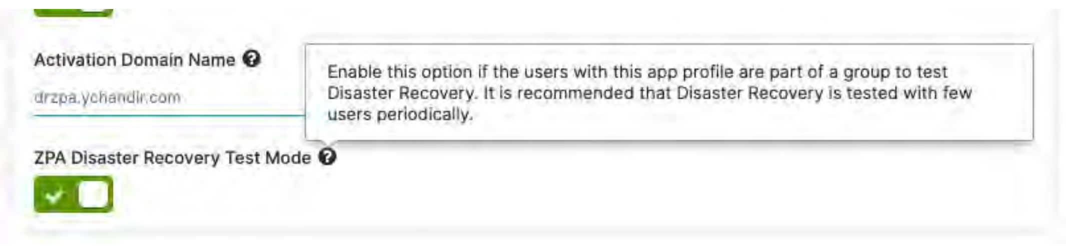


ZPA DISASTER RECOVERY CONFIGURATION V. 3.7.1

Allow ZPA Disaster Recovery ✓

Activation Domain Name: drzpa.ychandir.com

Domain Public Key: Not Available Upload



Activation Domain Name: drzpa.ychandir.com

Enable this option if the users with this app profile are part of a group to test Disaster Recovery. It is recommended that Disaster Recovery is tested with few users periodically.

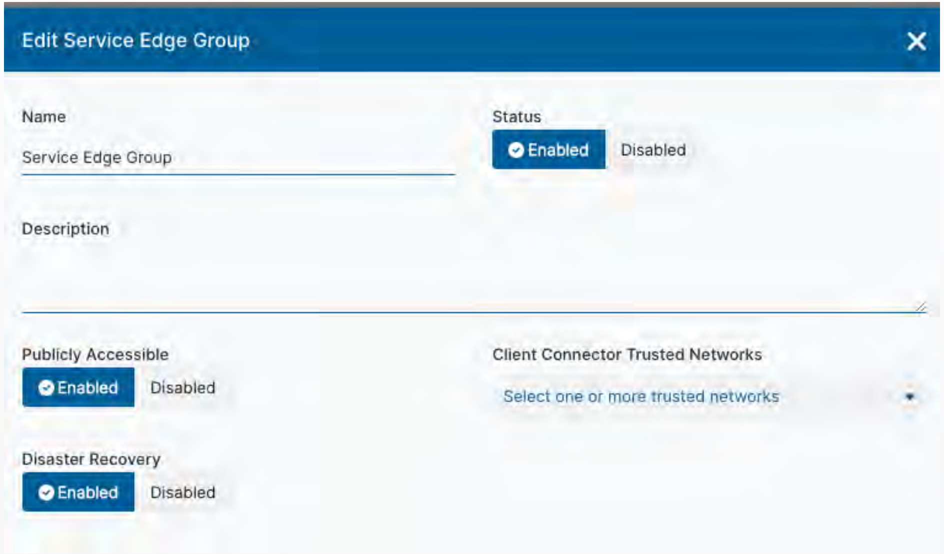
ZPA Disaster Recovery Test Mode ✓

Configuring Private Service Edge for DR

- Private Service Edge do not need to be exclusively used for DR mode
- You need to select the Private Service Edge that will participate in DR mode
- Always deploy Private Service Edge in clusters (a pair of Private Service Edge) for redundancy
- Private Service Edge mirror the policy and user database 10 times a day
- Each PSE pair supports up to 500Mbps of traffic

Configuring Private Service Edge for DR (cont)

- Enable Disaster Recovery Mode for the Private Service edge group that will participate in DR



Edit Service Edge Group

Name: Service Edge Group

Status: [✓ Enabled] Disabled

Description:

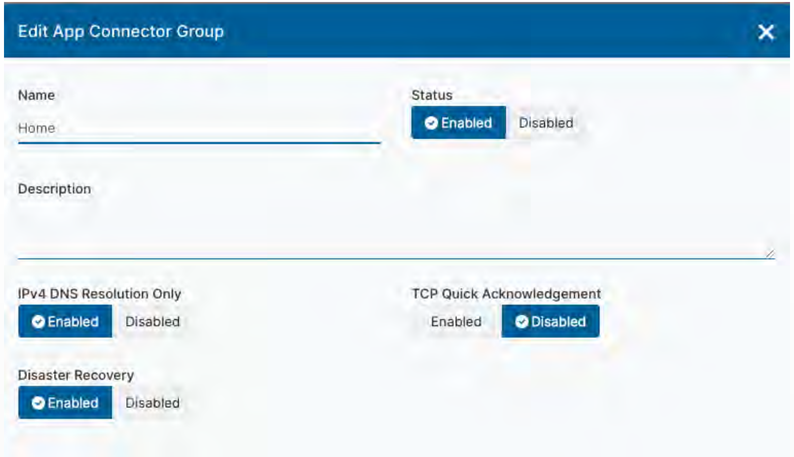
Publicly Accessible: [✓ Enabled] Disabled

Client Connector Trusted Networks: Select one or more trusted networks

Disaster Recovery: [✓ Enabled] Disabled

Configuring App Connector for DR

- App Connector Service Edge do not need to be exclusively used for DR mode
- You need to select the App Connector that will participate in DR mode
- Always deploy App Connectors in clusters (a pair of App Connectors) for redundancy



Edit App Connector Group

Name
Home

Status
[✓ Enabled] Disabled

Description

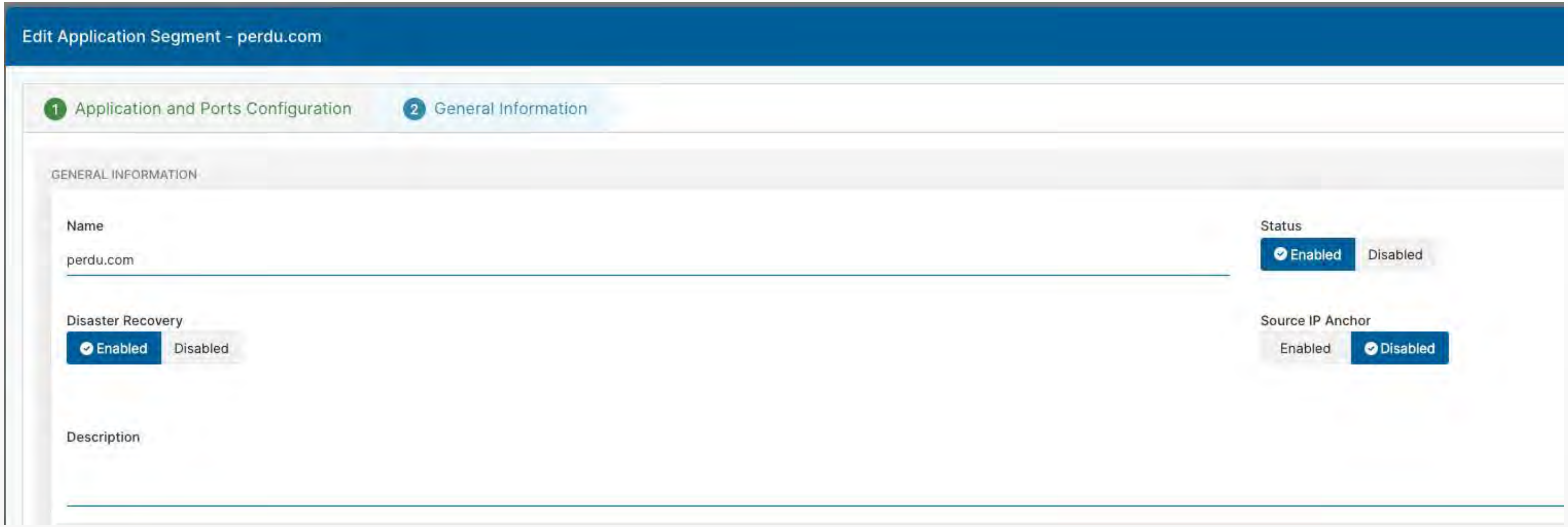
IPv4 DNS Resolution Only
[✓ Enabled] Disabled

TCP Quick Acknowledgement
Enabled [✓ Disabled]

Disaster Recovery
[✓ Enabled] Disabled

Configuring App Segments for DR

- Identify Business Critical App Segments
- Select those App Segments to be available during DR



Edit Application Segment - perdu.com

1 Application and Ports Configuration   2 General Information

GENERAL INFORMATION

Name: perdu.com

Status: [✓ Enabled] Disabled

Disaster Recovery: [✓ Enabled] Disabled

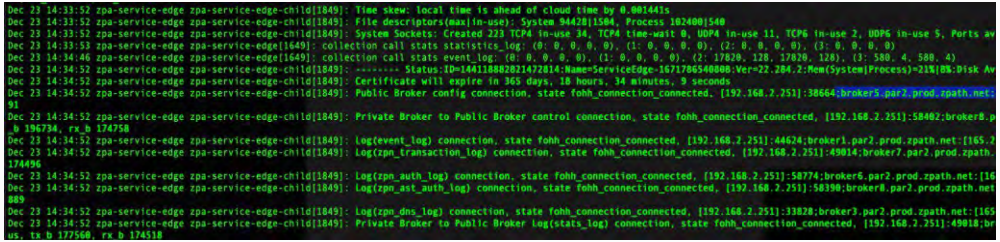
Source IP Anchor: Enabled [✓ Disabled]

Description

Verifying DR Mode

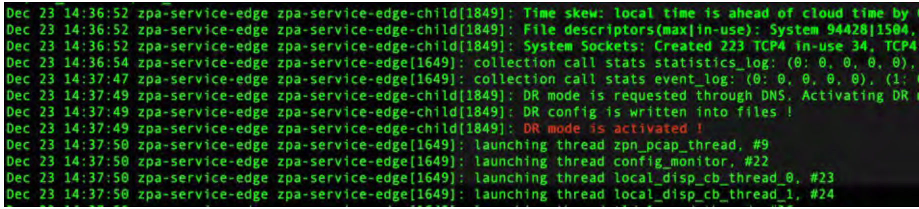
- SSh into Private Service Edge and/or App Connector
- Run the command `journaltl -f`

DR OFF (Private Service Edge)



```
Dec 23 14:33:52 zpa-service-edge zpa-service-edge-child[1849]: Time skew: local time is ahead of cloud time by 0.001441s
Dec 23 14:33:52 zpa-service-edge zpa-service-edge-child[1849]: File descriptors(max|in-use): System 94428|1504, Process 102400|540
Dec 23 14:33:52 zpa-service-edge zpa-service-edge-child[1849]: System Sockets: Created 223 TCP4 in-use 34, TCP4 time-wait 0, UDP4 in-use 11, TCP6 in-use 2, UDP6 in-use 5, Ports av
Dec 23 14:33:53 zpa-service-edge zpa-service-edge[1649]: collection call stats statistics_log: (0: 0, 0, 0, 0), (1: 0, 0, 0, 0), (2: 0, 0, 0, 0), (3: 0, 0, 0, 0)
Dec 23 14:34:46 zpa-service-edge zpa-service-edge[1649]: collection call stats event_log: (0: 0, 0, 0, 0), (1: 0, 0, 0, 0), (2: 17820, 128, 17820, 128), (3: 580, 4, 580, 4)
Dec 23 14:34:52 zpa-service-edge zpa-service-edge-child[1849]: -------- Status:ID=144118882821472814:Name=ServiceEdge-1671786540808:Ver=22.284.2:Mem(System|Process)=21%|8%:Disk Av
Dec 23 14:34:52 zpa-service-edge zpa-service-edge-child[1849]: Certificate will expire in 365 days, 18 hours, 34 minutes, 9 seconds
Dec 23 14:34:52 zpa-service-edge zpa-service-edge-child[1849]: Public Broker config connection, state fohh_connection_connected, [192.168.2.251]:38664;broker5.par2.prod.zpath.net:
91
Dec 23 14:34:52 zpa-service-edge zpa-service-edge-child[1849]: Private Broker to Public Broker control connection, state fohh_connection_connected, [192.168.2.251]:58402;broker8.p
_b 196734, rx_b 174758
Dec 23 14:34:52 zpa-service-edge zpa-service-edge-child[1849]: Log(event_log) connection, state fohh_connection_connected, [192.168.2.251]:44624;broker1.par2.prod.zpath.net:[165.2
Dec 23 14:34:52 zpa-service-edge zpa-service-edge-child[1849]: Log(zpn_transaction_log) connection, state fohh_connection_connected, [192.168.2.251]:49014;broker7.par2.prod.zpath.
174496
Dec 23 14:34:52 zpa-service-edge zpa-service-edge-child[1849]: Log(zpn_auth_log) connection, state fohh_connection_connected, [192.168.2.251]:58774;broker6.par2.prod.zpath.net:[16
Dec 23 14:34:52 zpa-service-edge zpa-service-edge-child[1849]: Log(zpn_ast_auth_log) connection, state fohh_connection_connected, [192.168.2.251]:58390;broker8.par2.prod.zpath.net
889
Dec 23 14:34:52 zpa-service-edge zpa-service-edge-child[1849]: Log(zpn_dns_log) connection, state fohh_connection_connected, [192.168.2.251]:33828;broker3.par2.prod.zpath.net:[165
Dec 23 14:34:52 zpa-service-edge zpa-service-edge-child[1849]: Private Broker to Public Broker Log(stats_log) connection, state fohh_connection_connected, [192.168.2.251]:49018;br
us, tx_b 177560, rx_b 174518
```

DR ON (Private Service Edge)



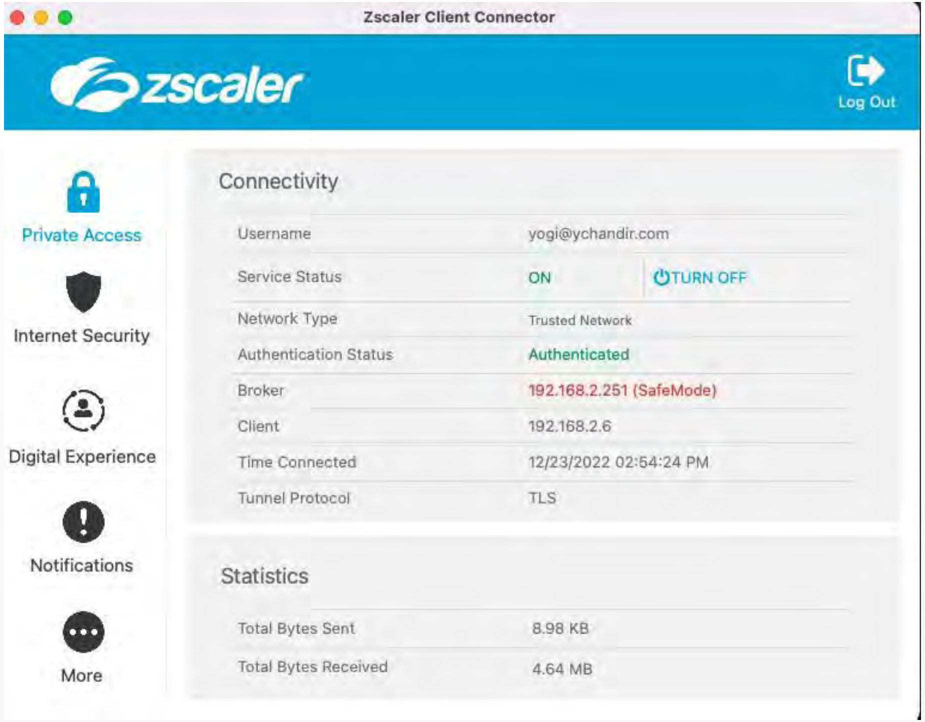
```
Dec 23 14:36:52 zpa-service-edge zpa-service-edge-child[1849]: Time skew: local time is ahead of cloud time by
Dec 23 14:36:52 zpa-service-edge zpa-service-edge-child[1849]: File descriptors(max|in-use): System 94428|1504,
Dec 23 14:36:52 zpa-service-edge zpa-service-edge-child[1849]: System Sockets: Created 223 TCP4 in-use 34, TCP4
Dec 23 14:36:54 zpa-service-edge zpa-service-edge[1649]: collection call stats statistics_log: (0: 0, 0, 0, 0),
Dec 23 14:37:47 zpa-service-edge zpa-service-edge[1649]: collection call stats event_log: (0: 0, 0, 0, 0), (1:
Dec 23 14:37:49 zpa-service-edge zpa-service-edge-child[1849]: DR mode is requested through DNS. Activating DR
Dec 23 14:37:49 zpa-service-edge zpa-service-edge-child[1849]: DR config is written into files !
Dec 23 14:37:49 zpa-service-edge zpa-service-edge-child[1849]: DR mode is activated !
Dec 23 14:37:50 zpa-service-edge zpa-service-edge[1649]: launching thread zpn_pcap_thread, #9
Dec 23 14:37:50 zpa-service-edge zpa-service-edge[1649]: launching thread config_monitor, #22
Dec 23 14:37:50 zpa-service-edge zpa-service-edge[1649]: launching thread local_disp_cb_thread_0, #23
Dec 23 14:37:50 zpa-service-edge zpa-service-edge[1649]: launching thread local_disp_cb_thread_1, #24
```

DR OFF (App Connector)

DR ON (App Connector)

Verifying DR Mode (cont)

DR ON (Client Connector)



Connectivity

Username yogi@ychandir.com

Service Status ON ⏻TURN OFF

Network Type Trusted Network

Authentication Status Authenticated

Broker 192.168.2.251 (SafeMode)

Client 192.168.2.6

Time Connected 12/23/2022 02:54:24 PM

Tunnel Protocol TLS

Statistics

Total Bytes Sent 8.98 KB

Total Bytes Received 4.64 MB

SemiConductor Island Benefits Summary

1. Identification of all IoT and OT assets
2. User traffic to critical applications are still secured during disaster following Zero Trust principals of least privileged access
3. Traffic to and from critical IOT and OT devices are still secured and segmented from the rest of the world
4. Plant can still run 24x7 for up to 2 weeks without internet.
5. Smart city sensors will also be secured during this transition.

Zscaler Resources slide

1. Zscaler Compliance Certifications- https://www.zscaler.com/compliance/overview
2. Zscaler for IoT/OT https://www.zscaler.com/secure-your-ot-and-iot
3. Zscaler IoT Discovery- https://www.zscaler.com/products-and-solutions/iot-device-visibility
4. Zscaler Air Gap Networks- https://www.zscaler.com/blogs/company-news/zscaler-acquires-airgap-networks-extends-zero-trust-sase
5. Zscaler Private Service Edges- https://help.zscaler.com/zpa/about-zpa-private-service-edges
6. Zscaler and CIMCOR - https://www.cimcor.com/partners/zscaler
7. Zscaler integrations https://www.zscaler.com/partners/technology

Questions and Follow up