Zscaler Zero Trust Certified Architect (ZTCA) – Study Guide

What is Zero Trust?

Zero trust is about securely connecting the right entities - the right user, right application and right device - using business policies - over any network.

More broadly in the industry, Zero trust is a framework for ensuring organizations can deliver connectivity to and protection of their assets, in that no user, application or network should be trusted by default. Assume that all entities are untrusted to start with. Then following a key zero trust principle, least-privileged access, trust is built up based on context (e.g., user identity and location, the security posture of the endpoint, the app or service being requested) with policy checks at each step.

What is Zscaler's Zero Trust Offer?

The Zscaler Zero Trust Exchange™ (ZTE) is an integrated platform of services that acts as an intelligent switchboard to secure user-to-app, app-to-app, and machine-to-machine communications - over any network and any location. The Zero Trust Exchange helps you reduce business risk while enabling you to realize the promise of digital transformation, including increased productivity, simplified IT, reduced costs, and an increase in business agility.

The ZTE is a cloud native, secure connectivity platform built on the least privileged principle. It allows enterprises to granularly define how to connect initiating entities to connect to destination applications. All initiators must build trust through context, such as a user's location, their device's security posture, the content being exchanged, and the application being requested. Once trust is established, your employees get fast, reliable connections—wherever they are—without ever being placed directly on your network.

Historical Network functions and challenges

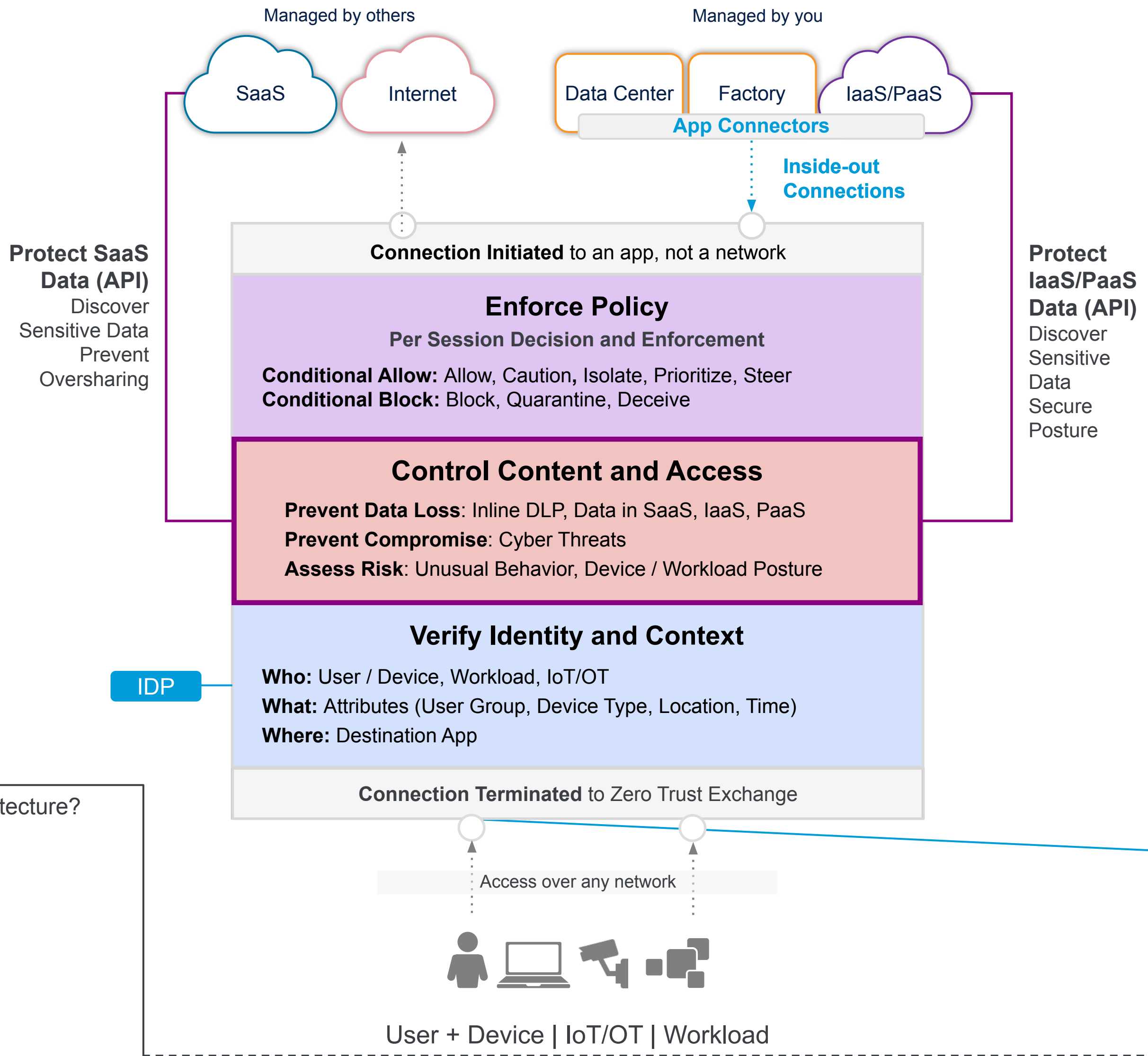
Reliance on the TCP/IP network model, where an initiator and the destination would share the same network is the crux of connectivity and security issues today. The idea is anchored in the medieval world, the world of castles and moats. Everything we trusted was inside the castle. Today's enterprise networks look similar to this, but it gets complicated when you try to layer in security and controls within the castle (e.g. a cook trying to get to the kitchen, but no one else) as well as building out the castles and roads that lead to the castle as people want to live and work outside.

What are the main elements of Zscaler's Zero Trust Architecture?

- There is an initiator and a destination (historically, these shared the same network)
- When that initiator tries to go to its destination, we must apply certain controls:

1) Verifying Identity & Context – where the following is verified:
   - ○ Who is connecting
   - ○ What is the context of the request
   - ○ Where are they going
2) Controlling Access, Control and ultimately Risk of the request by:
   - ○ Dynamically assessing behavior
   - ○ Preventing Threats
   - ○ Preventing Loss
3) Enforcing Policy – so to ensure the correct controls are implemented to:
   - ○ conditionally allow access
   - ○ conditionally block access

It's also critical to understand how enterprises connect to the Zero Trust Exchange, and how each application is accessed.



Managed by others

SaaS

Internet

Managed by you

Data Center

Factory

IaaS/PaaS

App Connectors

Inside-out Connections

Protect SaaS Data (API)
Discover Sensitive Data
Prevent Oversharing

Protect IaaS/PaaS Data (API)
Discover Sensitive Data
Secure Posture

Connection Initiated to an app, not a network

Enforce Policy

Per Session Decision and Enforcement

Conditional Allow: Allow, Caution, Isolate, Prioritize, Steer
Conditional Block: Block, Quarantine, Deceive

Control Content and Access

Prevent Data Loss: Inline DLP, Data in SaaS, IaaS, PaaS
Prevent Compromise: Cyber Threats
Assess Risk: Unusual Behavior, Device / Workload Posture

Verify Identity and Context

IDP

Who: User / Device, Workload, IoT/OT
What: Attributes (User Group, Device Type, Location, Time)
Where: Destination App

Connection Terminated to Zero Trust Exchange

Access over any network

User + Device | IoT/OT | Workload

Your notes

What you need to know

- Networks require shared access to a network
- Zero Trust access is from any initiator to any application, on any network
- It is not about the network route, but rather if the access and path is allowed or not. If access is not allowed, then the destination cannot even be seen
- Granular permissions are dependant on understanding
  - Identity
  - Control rights
  - Policy enforcement

Prevent Loss

- Data can be lost to the Internet in many ways - especially when companies consume SaaS / IaaS / PaaS services (out of their control)
- Enterprises need to set rules for what data is shared & how it is shared on these platforms to mitigate loss of intellectual property

Prevent Breach

- With over 80% of web traffic being encrypted, if you aren't looking at the contents, you cannot stop malicious content.
- True inline controls require the ability to control more than just the URL

SSL/TLS Inspection (Control Risk)

- without the ability to look at the contents of access, the correct controls cannot be applied
- Inspection allows for true understanding of behaviour, thus risk.
- Inspection allows for additional protections to be enabled

Ways to connect to the Zero Trust Exchange

- Zscaler Client Connector (ZCC) – an agent installed on an endpoint that forwards traffic

- Browser access - for unmanaged user devices, DNS redirect based
- Branch connector - Site forwarding from branches, offices, factories
- Edge forwarding protocols – GRE or IPSec tunnels from 3rd party network routers using SD-WAN
- Zscaler Cloud Connector – connection mechanisms for IaaS locations, allowing workload-to-workload or workload-to-Internet. Both branch connector and cloud connector allow bi-directional communication.