ZTCA - Notes

Overview of zero trust

3 Key areas of zero trust architecture.

Learning objectives:

- Recognize importance of shifting from legazy to ZTA.
- Identify the 3 key areas of ZTA
  - Verify Identity and Context
  - Control Content and Access
  - Enforce Policy
- Discover how connections are made to/from Zscaler Zero Trust Exchange

---

Legacy network & security to ZTA.

Selskap gjennfører digital transformasjon for å:

- Increase effiency
- Improve agility
- Achieve competetive advantege.

Legacy architecture - Castle and moat architecture.

Hub and spoke networks.

- Apps moved to cloud
- Work from anywhere

- Traffic must go direct

Architectural advantages to ZTA vs Legacy Architecture

	Legacy Network and Security Architecture	Zero Trust Architecture
Attack Surface	Firewalls/VPNs published on the internet Can be exploited, susceptible to DDoSed	Apps not exposed to the internet You can't attack what you can't see
Connection	App access requires corporate network access, allows lateral movement of users and threats	Connects a specific authorized user to a specific, authorized resource
Proxy/Passthrough	Firewall/Passthrough Inspects a limited data buffer Unknown files pass through Alerts after infection	Proxy Full content inspection, including TLS/SSL Hold and inspect unknown files before reaching the endpoint
Tenancy	VMs of single-tenant appliances in a public cloud	Cloud-native, multitenant design like Salesforce/Workday

Connecting to ZTE

Establish Zero Trust Connections.

Connect to ZTE - Zero Trust Exchange (cloud).
Liste over Connectors:

- Zscaler Client connector - Endpoints. TLS basert.
    - Beskytter SaaS, internet-trafikk.
    - Persistent control plane
    - Dynamic micro-segmentet data-plane tunnels to ZTE.
        - For Internal App protection.
- Zscaler Browser Access
    - For Unmanaged User devices / Kan ikkje installere Client Connector/Agent.
    - DNS Redirects using CNAME.
    - Protects Private web-based apps.
- Zscaler Branch Connector
    - Site-Forwarding.
    - Branches / Offices / IaaS / On-Prem.
    - Hosted on-prem eller As a Service frå Zscaler.
    - Biderectional
- Edge Forwarding Protocols
    - Alternativ til Client Connector for Sites (branch,office etc)

    - GRE / IPSEC
    - Over SD-WAN
    - Integrerer med mange SD-WAN leverandører.
- Zscaler Cloud connector
    - For skyløysinger (Iaas)
    - sky-sky
    - sky-internet
    - Bidirectional

Connector initierer ein Inside-Out connection til ZTE. **ZTE er ein forwarding-proxy.**

Building an org-architecture

3 Key areas of ZTA.

Section 1 - Verify Identity and Access

3 main areas for verifying identiy:

- **Who** is the initiator (User / device, workload, IoT/OT)
- **What** are the attributes of the connection (user group, device type, location, time)
- **Where** is the initiator trying to go (destination app)

Section 2 - Control Content and Access

Apply **Controls to identity** based on:

- Dynamic risk assesment
- Compromise prevention
- Data Loss Prevention

Desse 3 teknikkane blir Contextually applied på all trafikk generert av **Initiator**

Tradional Architecture for control.

- NGFW - Permieter fw.
- Not designed for content inspection. Focus on L3-L4, not L7.
- Limited inspect buffer.
- Passthrough connection (terminated at server, not fw)
    - Reset connection if bad.

Zscaler Proxy Architecture:

- Designed for content inspection.
- Connection terminated at ZTE
- Establish if good.
    - Motsatt av fw, FW block if BAD, ZT establish if good.
    - Default good, action on bad. ZTE = Default bad, action on good.
- Inspect full content, terminere connection og kan difor sjå kryptert trafikk.

Elements

Risk assesment - Blocked Malware? Blocked phishig? Impossible travel? Change in BW / transaction volume? Certificates, disk encryption status.

Prevent compromise - Patterns, signature. Block known bad - quantify unknown, put in Sandbox

Prevent data loss - Control file transfer, Inspect destinations, block risky apps.

Section 3 - Enforce Policy

Input frå Section 1 og 2 tillater **"Granular defined policies to be enforced"**

- Conditional Allow
- Conditional Block
- Mulige policy action - Levels.
    - Conditional block
    - Deceive - direct identified attacker to decoy
    - Quarantine - Limit and protect access. Sandboxed for example.
    - Isolate - Stream pixels to browser, restrict download / copy-paste
    - Warn - Alert user of policy violation - potention risk
    - Prioritize - ERP / CRM priority over youtube.
    - Conditional Allow

Initating connections to apps

Access is not based on sharing a network. It is based on a policy:
who, what, where) + (risk of access, compromise prevention + loss prevention)

- Can connect internal and External apps

ZTA - Deep Dive

Verify Identiy and Context

3 Element

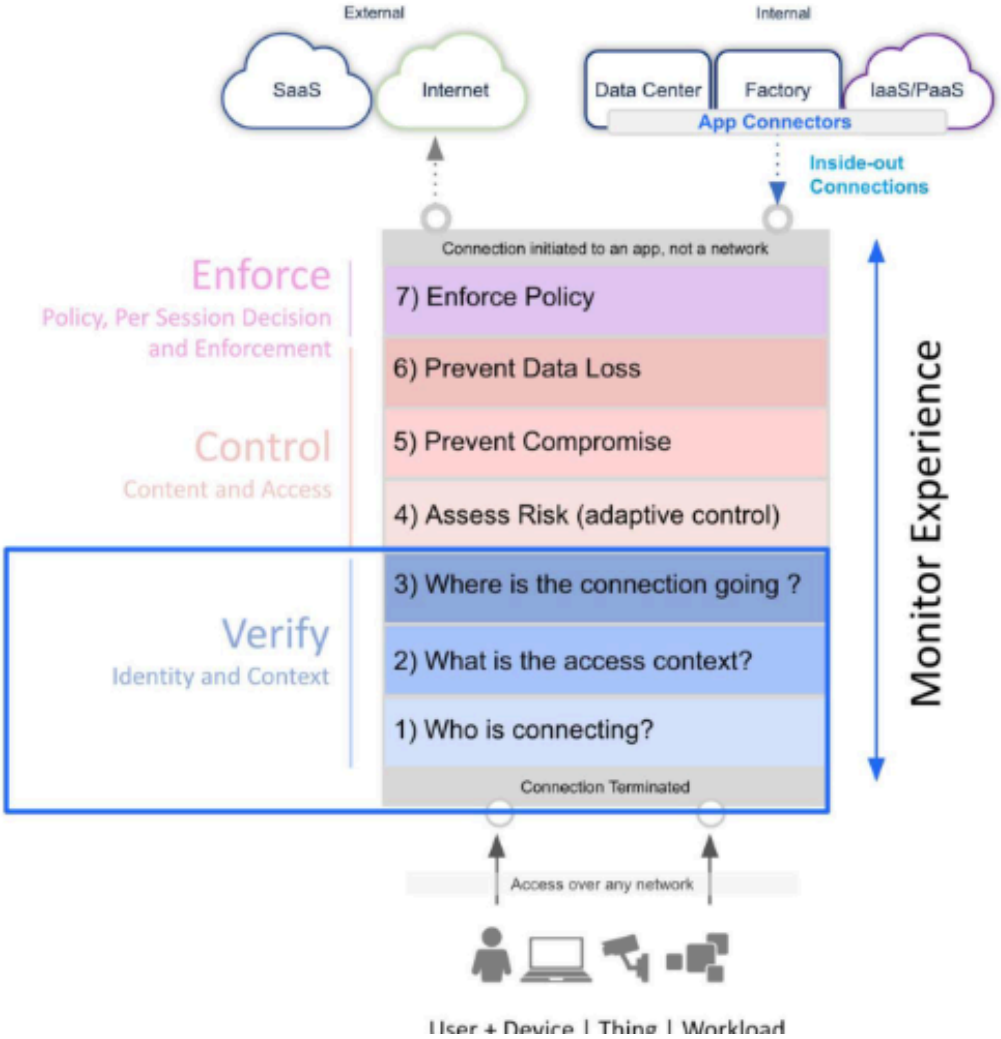
- Who is connecting
- What is the access context
- Where is the connection going.

ZTA består av 3 seksjoner, og 7 element.

- **Verify** identity and context.
    - Who is connecting
    - What is the access context
    - Where is the connectiong going.
- **Control** content and access

- Assess Risk
- Prevent compromise
- Prevent Data Loss

- **Enforce**, Policy, per session decisions and enforcement.
  - Enforce policy.



Verify Deep Dive.

Element1 - Who is connecting


Submit to Inspection
Bypass Inspection
Inspect
Bypass
Location of App
Define Critical Apps
Collect Conditions for Public App
Flag as Discovered for Shadow Report
Categorize Private App
Collect Conditions for Private App
Known
Unknown
Unknown
Unknown
Do we know the app?
Known or Unknown
?
External
Location of App
Internal
App Requested