Identity & Access Management:
Getting Serious about Zero Trust Architectures

Chris Phillips | Technical Architect, Canadian Access Federation

March 10, 2022

BCNET Connect Summit

Outcomes for Today

Build a common understanding of Zero Trust Architecture (ZTA)

Show how critical IAM and federated ID toolsets are to ZTA success

Introduce access management techniques that support ZTA

Guidance on next steps

Demystifying Zero Trust Architecture Models

What is a Zero Trust Architecture Model?

A collection of concepts, ideas, and component relationships designed to eliminate uncertainty in enforcing accurate access decisions.

Some Starting Perspectives

- Existing network architectures are not far off from ZTA models.
- Security mindset of least privilege is a principle for both Identity Access Management (IAM) and ZTA.
- Identity data is key to application of dynamic policy.

Good News!

- **Using federated ID and/or participating in CAF?**
  - You are already a Zero Trust practitioner!
- Now let’s see how far along we are, and where to go next.

Definitions vary, all agree identity and attributes are key

NIST National Institute of Standards and Technology U.S. Department of Commerce

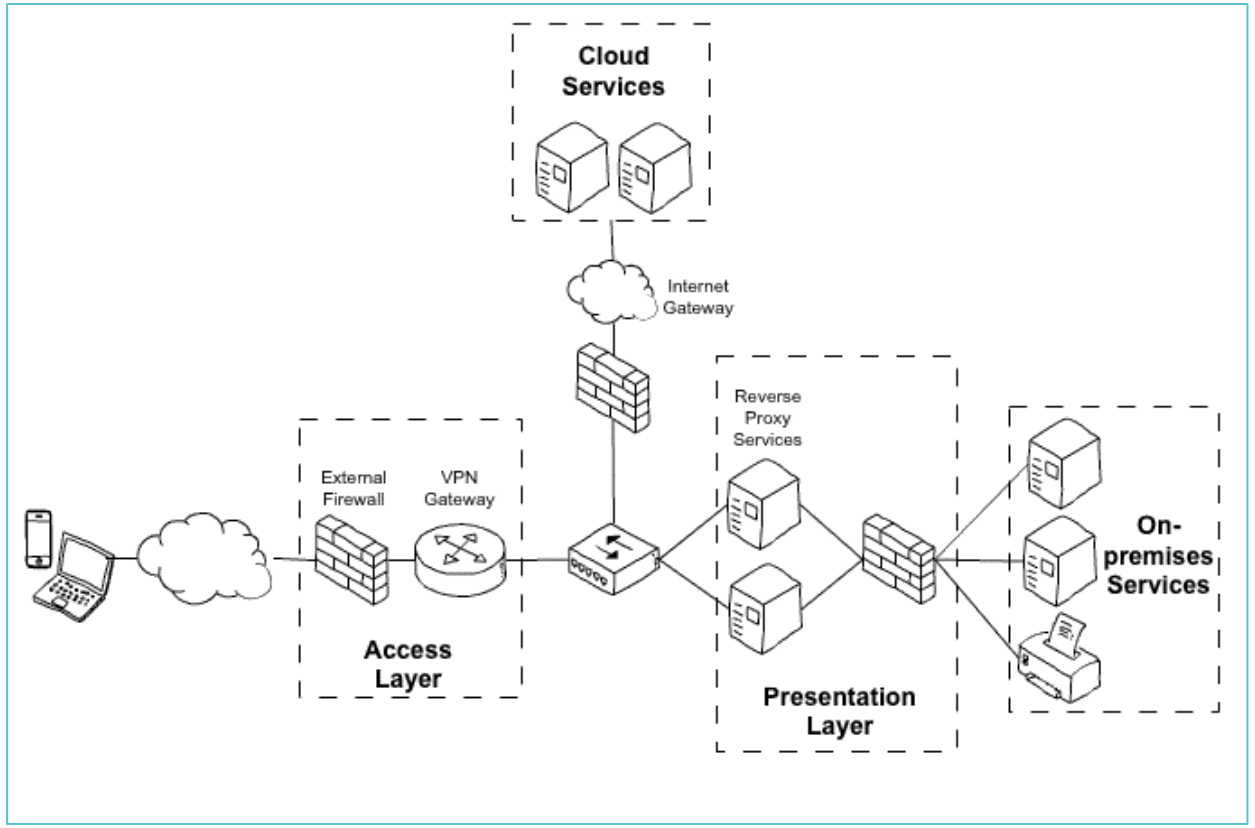
- Data sources and services are resources
- Communication secured regardless of network
- Access to resources is on a per session basis
- Access determined by dynamic policy elements
- Enhanced identity governance approach uses the identity of actors as the key component of policy creation
- Resource access policies are based on identity and assigned attributes

National Cyber Security Centre

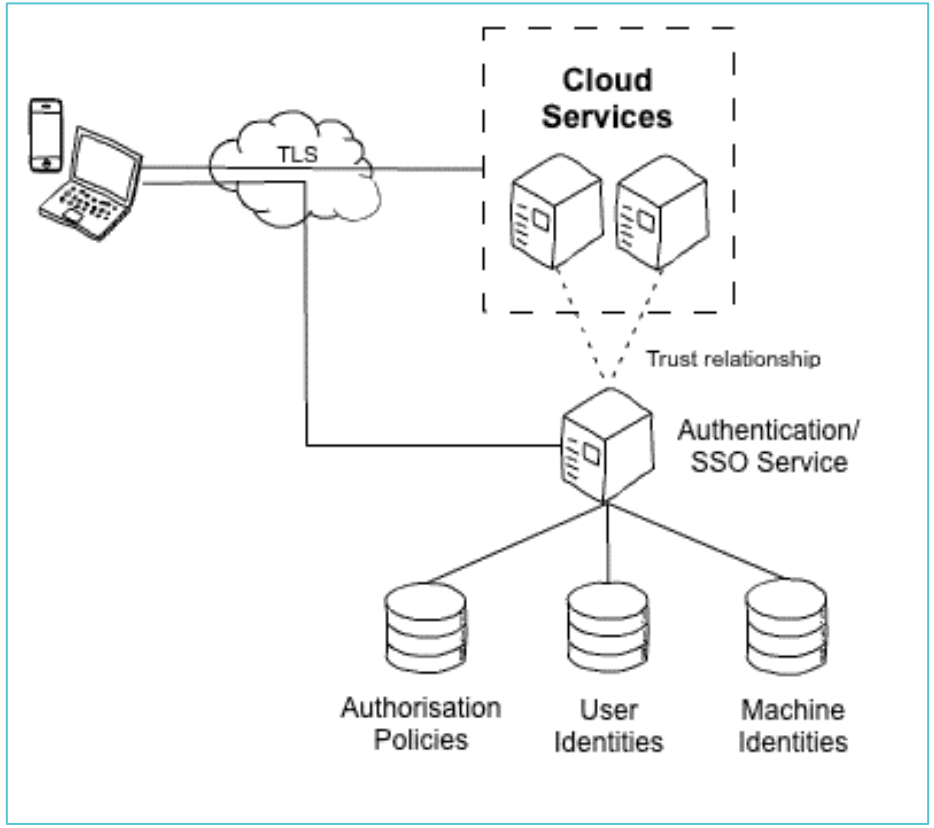
- Single strong source of user identity
- User authentication
- Machine authentication
- Additional context, e.g. policy compliance and device health
- Authorization policies to access an application
- Access control policies within an application

Comparing Traditional Trust to Zero Trust Models

Traditional Trust

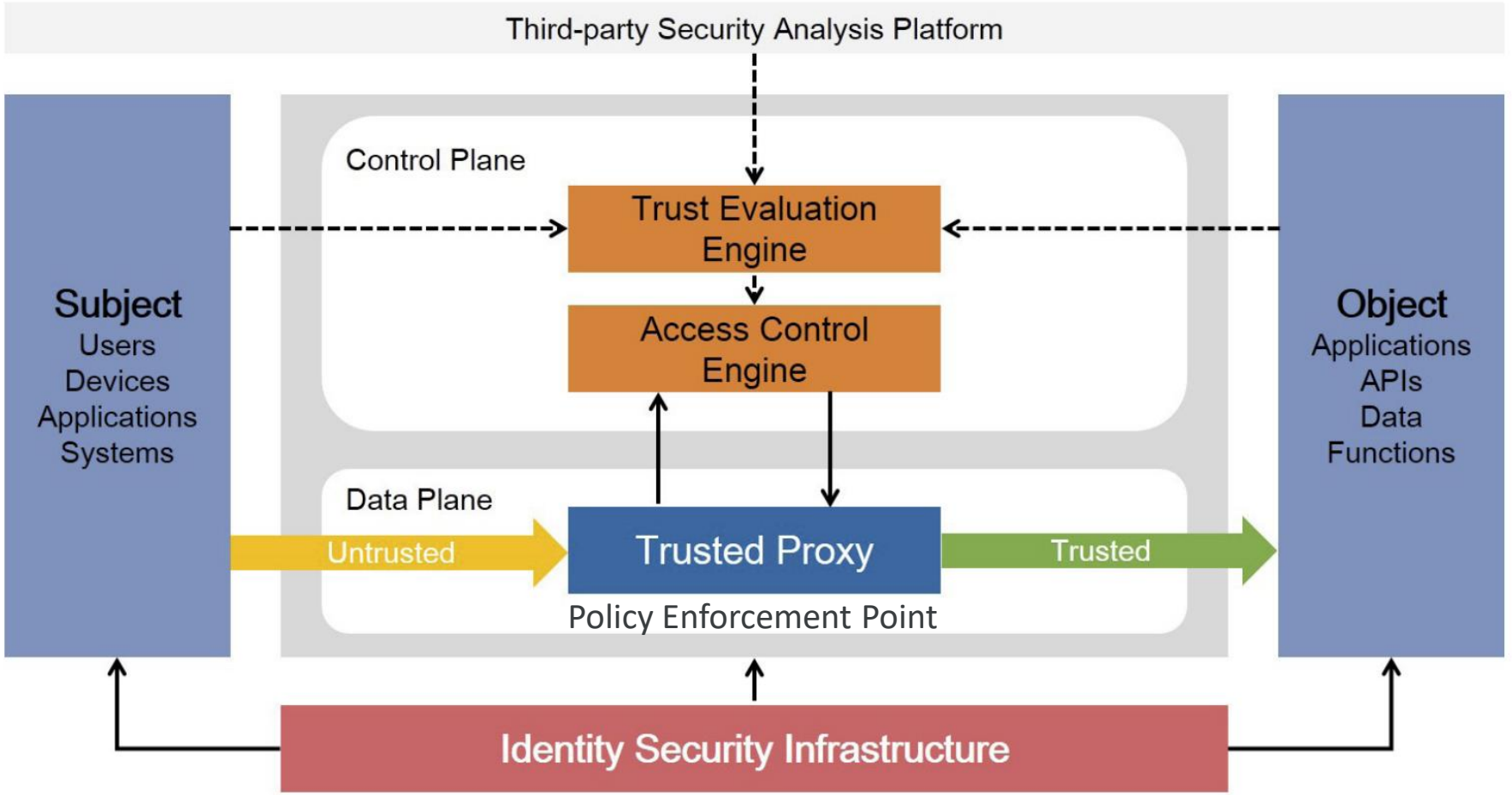


Zero Trust



- Avoid trap of one excluding the other - both can be applied in a hybrid form
- Single Sign-On (SSO), authentication, and authorization more critical than ever

Components of Zero Trust Architecture



Source Qi An Xin Group, 2019

Federated Identity Components in Zero Trust Terms: Policy Enforcement Points (PEP) and Key Actors

Id Management (IdM) System

Facilitates:

- Identity business operations
- Administrates access model, business rules
- Applies business rules to records & subsystems

Identity Store

Houses:

- Core identity and credentials
- Access management elements
- Entitlement attributes

Identity Provider

Acts as PEP, enforcing :

- Authentication levels (MFA)
- Is service trusted?
- Additional policy requirements
- Dynamic attribute release

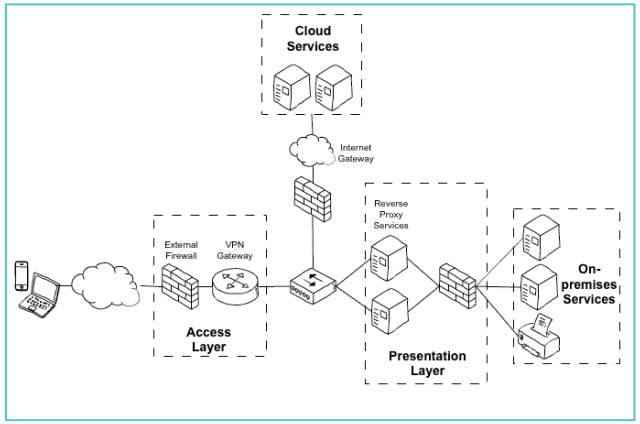
Service Provider

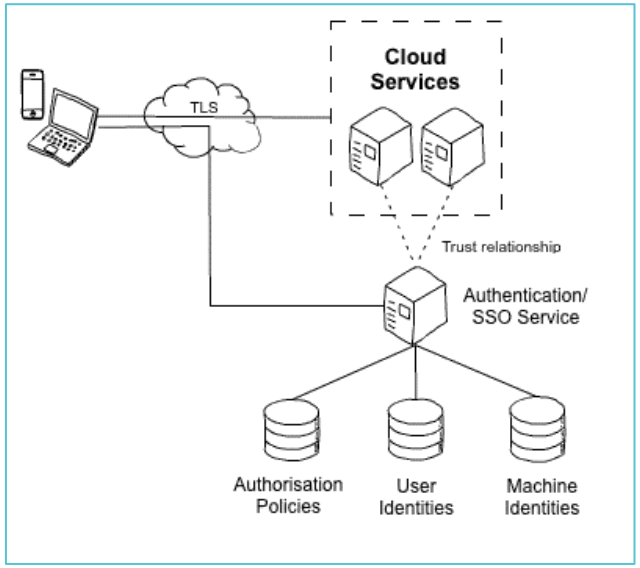
Acts as PEP by Policy Agent:

- Trustworthiness of origin
- Gatekeeps for sufficient attributes
- Applies business rules for access

Building Blocks of Dynamic Policy Evaluation

- **Capabilities available now:**
  - Ability to detect change of origin mid-session
  - Geofencing with low service touch
  - Ability to deny certain audiences
  - Ability to leverage cloud vendor ZT features by proxy

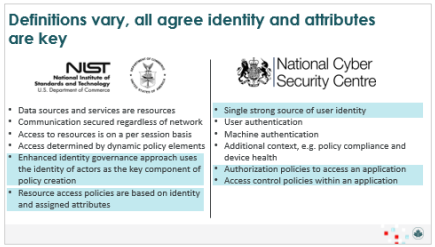


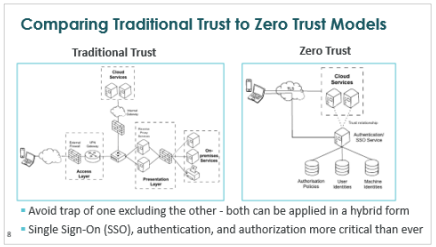


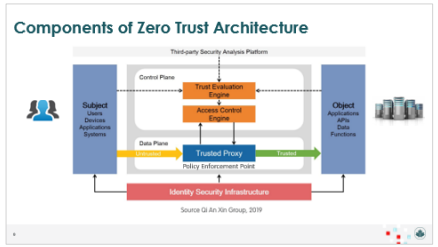
Not without challenges

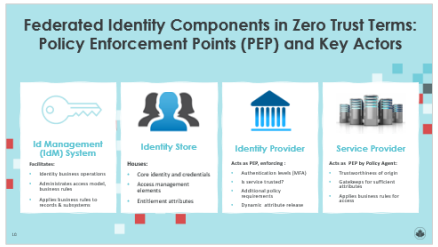
- Sophistication means customization, increasing cost, and support.
- Is return on a complex policy worth fragility and troubleshooting?
- To mature ZT deployments, significant robustness needed to operate ($$$).

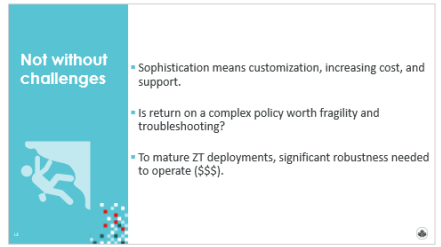
Quick Recap


Definitions vary, all agree identity and attributes are key
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
National Cyber Security Centre
Data sources and services are resources
Communication secured regardless of network
Access to resources is on a per session basis
Access determined by dynamic policy elements
Enhanced identity governance approach uses the identity of actors as the key component of policy creation
Resource access policies are based on identity and assigned attributes
Single strong source of user identity
User authentication
Machine authentication
Additional context, e.g. policy compliance and device health
Authorization policies to access an application
Access control policies within an application


Comparing Traditional Trust to Zero Trust Models
Traditional Trust
Zero Trust
Avoid trap of one excluding the other - both can be applied in a hybrid form
Single Sign-On (SSO), authentication, and authorization more critical than ever


Components of Zero Trust Architecture
Third-party Security Analysis Platform
Control Plane
Trust Evaluation Engine
Access Control Engine
Data Plane
Trusted Proxy
Policy Enforcement Point
Subject
Object
Identity Security Infrastructure
Source Gi An Xin Group, 2019


Federated Identity Components in Zero Trust Terms: Policy Enforcement Points (PEP) and Key Actors
Id Management (IdM) System
Identity Store
Identity Provider
Service Provider


Not without challenges
Sophistication means customization, increasing cost, and support.
Is return on a complex policy worth fragility and troubleshooting?
To mature ZT deployments, significant robustness needed to operate ($$$).

Three Steps to Building Your Access Management Model

Zero Trust is just an application of the model of your choosing.

Who you are is not as important as
what you are, and
what you are entitled to do.

Step 1: Assess span and type of access

Create an inventory of what is being protected

Recognize and generalize to classify by type and needs

Prioritize key assets and elements by risk and security consequence

Step 2: Craft the access management vision

Aim beyond where you are today

Set baseline for vision and values

Establish a prioritized list of preferred access models

Step 3: Apply and iterate

Designate authority for authorization

Zero Trust is a model that needs continuous refresh

No-Code Methods to Embed and Apply Zero Trust

Update procurement RFQs; include SSO, external authorization as requirements.

Include implementation time in projects for ZT access requirements.

Security assessments are fastest and least effort when a common model is used.

Access Models Used in Zero Trust

Access Models

Access Model	Common Implementation
Group based (GBAC)	Group membership in directory
Entitlements	Appears as multi-valued attribute in directory
Attribute based (ABAC)	Attribute value determines access (DOB >18 yrs old today, password reset < 1hr)
Role based (RBAC)	Role in directory
Discretionary access control (DAC)	Manually assigned permission

Which access management models fit Zero Trust?

Uses all access model data that you provide

Results in blended approach, continuously assessing access requirements

Requires new groups modeling beyond traditional origins; proliferates quickly

What's Next?

Continue refining and enriching the access management data and tools

Ensure easy access to quality access management data in the identity store

Identify dedicated tool for group management to delegate the workload

Reading References

- NIST 800-27 – Zero Trust Architecture (link)
- National Cyber Security Center – Architectures (link)
- Gartner – Zero Trust Architecture and Solutions (link)
- Government of Canada Network and Security Strategy (link)
- Paranoid IAM: Process and Architecture (link)
- IDPro.org – Introduction to Access Control (link)
- IDPro.org - Policy Based Controls (link)
- NSA – Embracing a Zero Trust Security Model (link)

Let’s continue the conversation!


A
Q

canarie

canarie.ca | @canarie_inc

CAF Support: tickets@canarie.ca

chris.phillips@canarie.ca

In Closing...

Everything's going to be wonderful.

Image source: http://theheightsanimalhospital.com