aviatrix ACE Aviatrix Certified Engineer

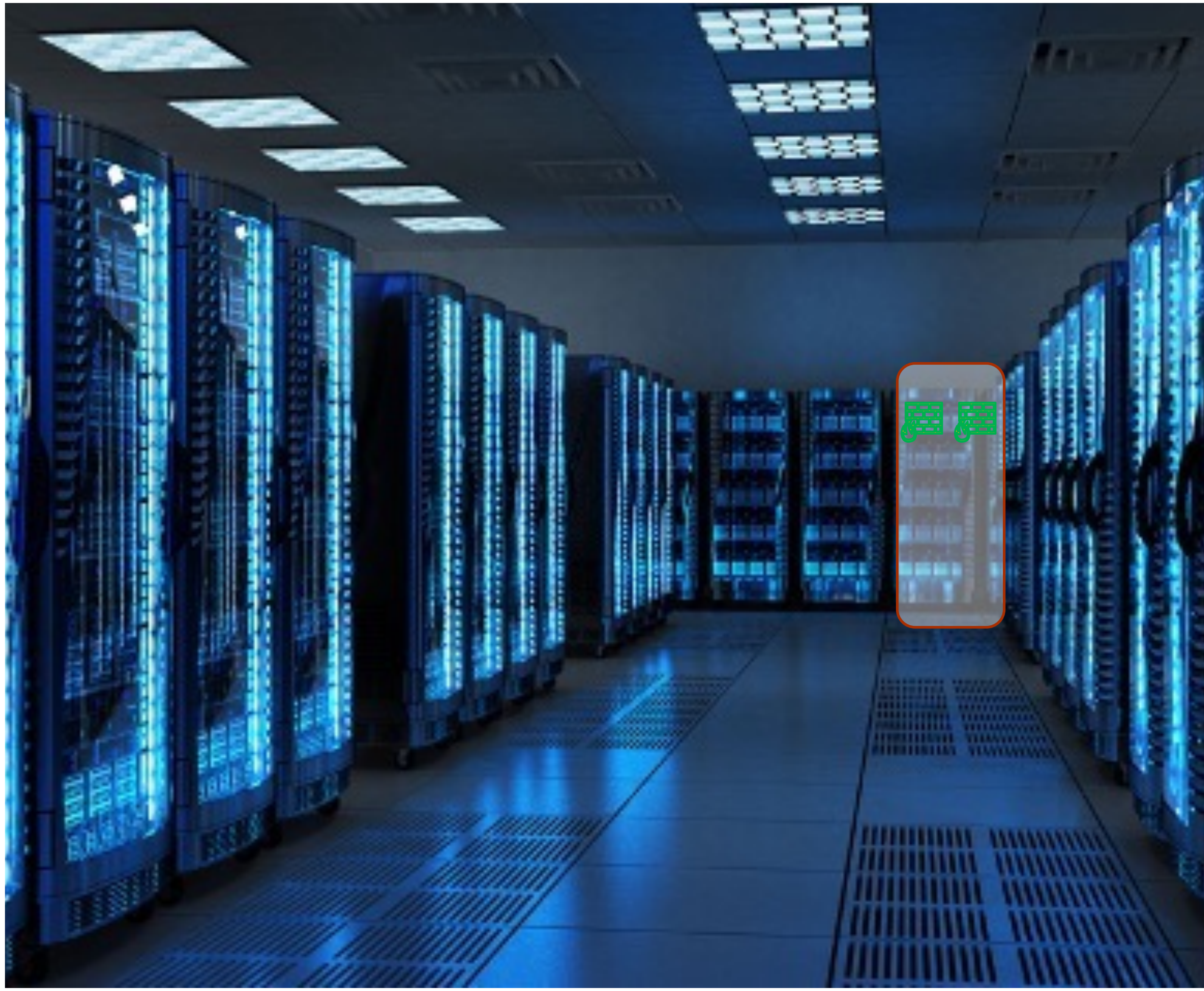
Zero Trust Network Architecture Tenets

aviatrix

How Public Cloud Security Differs from Security in a On-Prem Data Center/Colocation

On-Prem Data Center/Colocation

- Complete control over devices
- Few Internet Ingress and Egress points
- Caged and locked DMZ
- Devices have finite computing & processing capacity
- Specialized security appliances are used (Firewalls, IDS, IPS) in centralized place



Public Cloud

- Limited or no control over security devices/services
- Too many Internet Ingress/Egress points
- The public cloud has infinite computing and processing capacity
- The distributed nature of workload mandates distributed traffic patterns and distributed security
- "SHARED" responsibility model equals "YOUR" responsibility model

Google "shared responsibility model aviatrix"

aviatrix

Zero Trust Architecture (ZTA) and Customer Requirements

Aka ZTNA (Zero Trust Network Architecture)

What is Zero-Trust?

The zero-trust framework operates on the principle of ”Never Trust, Always Verify.” OR “Don’t Trust Anyone.”

- It assumes that threats can exist inside and outside the network, requiring continuous verification of trust in users, devices, and applications.

Zero Trust is a security framework. It is a mindset.

- NOT a product.
- An approach enterprises should adopt when building secure networks for mission-critical applications.

Aviatrix Zero Trust approach is based on NIST SP 800-207 Publication

- https://www.nist.gov/publications/zero-trust-architecture

Other References

- https://learn.microsoft.com/en-us/security/zero-trust/zero-trust-overview
- https://aws.amazon.com/security/zero-trust/

Zero-Trust (ZT) Evolution

- In the past, Zero Trust (ZT) discussions focused on
  - Firewall-based defense or identity-based protection.
  - Perimeter security OR centralized security model

- Cloud is distributed
- Need to re-define ZT tenets for Cloud
- Tenets are derived from NIST ZTA publication and customer requirements

Aviatrix Zero Trust Architecture (ZTA) approach complements other partner offerings, cloud-native services, and 3rd party tools to protect workloads in the cloud or hybrid cloud.

Zero-Trust Architecture Tenets

- Aviatrix has been enabling cloud and multicloud networking since 2016
- Vast experience in building secure cloud networking for enterprises
- The following are 7 tenets to implement Zero-Trust Security with Resiliency
    1. Resource Identification, Inventory and Grouping
    2. Security close to the Applications and Services
    3. Global, Dynamic, and Centralized Policy
    4. Secure Network Communication
    5. Operational and Security Visibility
    6. Audit and Reporting
    7. Least Privileged Access

1- Cloud Resource Identification, Inventory and Grouping

Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.

- The ability to leverage location/IP-independent identity
- Services, VM, EC2, etc. should properly identify to apply the security rules and policies.
- Identity for user is done with IDP solutions such as
  - Active Directory or
  - SAML based solutions like Okta
- Workloads and services don't often have a meaningful IDP.
- A workload's identity should align with components like "App Name", "Data Classification" or "Lifecycle/Environment".

2- Distributed and Embedded Security

Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

Assets and traffic moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture. Workloads should retain their security posture when moving to or from enterprise-owned infrastructure. This includes devices that move from enterprise networks to non-enterprise networks. This also includes workloads migrating from on-premises data centers to non-enterprise cloud instances.

- This can only be achieved if the security is applied close to the workloads and applications
- There is a need for a Distributed Cloud Firewall to achieve this.
- Cost savings with the distributed model
- Avoid latency issues with the centralized Firewall Designs.
- A network packet or flow must be secure when it leaves the application.
- Follow a layered security approach as per NIST guidelines

3- Global, Dynamic and Centralized Policy

Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.

- Policy should cover single cloud, multi cloud and hybrid cloud use cases
- Should be dynamic without human intervention
- Should be managed by a centralized location across all landscapes
- Smart Grouping should be consumed by the centralized policy

4- Secure Network Communication with E2E IPSec Encryption

Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

All communication is secured regardless of network location. Network location alone does not imply trust. All communication should be done in the most secure manner available.

- Not all apps are encrypted
- **Trust no one – including application (TLS)**
- All encryptions are not the same
- Encryption at rest and in motion
- Native encryption performance limitation
- MACSec encryption is NOT end-to-end encryption
  - Only layer 2 and hop-by-hop
  - IPSec is the standard protocol for end-to-end encryption
- **The data plane must be IPSec encrypted**

5- Operational and Security Visibility

Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

An enterprise should collect data about asset security posture, network traffic, and access requests, process that data, and use any insight gained to improve policy creation and enforcement.

- You cannot protect what you cannot see
- Consistent design with consistent operational visibility
- End-to-End observability
- Noise-free and single plane of glass

6- Audit, Logs, Reporting and Alerts

Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

ZTA should allow developers and administrators sufficient flexibility to satisfy their business requirements while using logs and audit actions to identify access behavior patterns. Policy Engine (PE) and Policy Admin (PA) components must be properly configured and monitored, and any configuration changes must be logged and subject to audit.

- Ability to replay topology
- Audit trail
- Alters based on performance, network behavior, etc.
- Out-of-the-box and custom reports

7- Least Privilege Access

Tenet from NIST Publication 800-207 - Zero Trust Architecture (ZTA)

Trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task.

- Trust no one, not even internal services, resources, and actors
- Parameter security solutions not sufficient (lateral movement)
- Policy-driven framework with the knowledge of applications (Tags) and users
- NGFW Service Insertion (if required)
- RBAC
- Client or User VPN

aviatrix

Aviatrix Certified Engineer (ACE)
https://aviatrix.com/ACE

COMMUNITY
https://community.aviatrix.com