The Future Zero Trust in the Cloud

Stephen Kovac
VP, Global Government
Head of Corporate Compliance
Zscaler
Cloud and mobility: enablers, but disrupt networking and security

Old World

It started with cloud app adoption...

And that drives Network Transformation...

Which disrupts network security

New World

Cloud + DC

Direct-to-Cloud

Hub-and-Spoke to DC

DC

Network Security
Legacy Datacenter

The data center was the center of gravity

Legacy Network

Internal networks were built and optimized to connect users to apps in the datacenter

- MPLS connects 100’s of offices worldwide
- 3 – 6 DCs with a few internet gateways
- VPN to connect mobile workforce (50%)
Instead: decouple app access from network access

**Network – Centric**
- Secure the corporate network to protect users and data
- Build a security moat of appliances to protect the network

**User – Centric**
- Securely connect users to apps or services
- Decouple network access from application access

Policy Enforcement Checkpost

Securely connect users to apps or services

Securing your cloud transformation
Current State of Network

How things are
Legacy Federal castle and moat network security

Network security = secure the network to protect users and apps

Perimeter (moat) of appliances to protect the network

And serve as gateways (drawbridges) to go in and out

You controlled: network, apps/data, users
Cloud breaks Federal legacy networks and security

The cloud is the new data center

Backhaul Traffic
Branch: MPLS / Mobile: VPN

Natural path
Direct-to-Cloud

But, security is still sitting in the DC

Poor user experience
MPLS backhaul costs
Security risk

NotPetya
Can you do network security in the world of cloud?

How do you secure a network you don’t control?

Can’t build a ‘moat’ around it with firewalls and proxies

How do you protect your users and apps?

A new approach to security is needed

Agnostic
Cloud
Network
Device
Current IT: Typical Federal network (static perimeter)
Castle and moat: Secure the network to secure servers, apps, and users

Outbound gateways
Secure access to Internet
More threats, more appliances

Inbound gateways
VPN to access DC apps
More users, more appliances

Challenges – ‘90s Design

- Expensive to deploy
- Castle and Moat
- Complex to manage
- Remote Users
- BYOD
- Shadow IT
- Manual cloud migration
- Security compromises
- Poor user experience
Internet: The Next Generation Network
Transform to a new approach to Network Access and Security
Fast, secure, policy-based access connecting the right user to the right service and app

INTERNET ACCESS
Secure access to the Internet and SaaS apps

Securing the network is no longer relevant
Cloud Internet Access – Fast, secure access to the Internet and SaaS

Real-time policy and analytics

- Real-time policy engine
  Polices follow the user
  Changes are immediately enforced, worldwide

- Business analytics
  Global visibility into apps and threats blocked
  Identify botnet infected machines for remediation

Your security stack as a service

<table>
<thead>
<tr>
<th>Access Control</th>
<th>Threat Prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud Firewall</td>
<td>Adv. Protection</td>
</tr>
<tr>
<td>URL Filtering</td>
<td>Cloud Sandbox</td>
</tr>
<tr>
<td>Bandwidth Control</td>
<td>Anti-Virus</td>
</tr>
<tr>
<td>DNS Filtering</td>
<td>DNS Security</td>
</tr>
</tbody>
</table>

Data Protection

- Data Loss Prevention
- Cloud Apps (CASB)
- File Type Controls

The best approach for SD-WAN and Office 365
Cutting edge security capabilities in the cloud – No service Chaining

**Full Inline Inspection & Correlation of Threat Indicators**

- **Secure All Ports & Protocols**
- **Multiple Proprietary Inspection Methods**
- **Advanced Threat Protection**
- **Control Bandwidth**

- **Internet Traffic**
  - Cloud FW (NGFW)
  - Proxy (SSL)
  - Dynamic Content Classification
  - CVE Protection
  - Sandbox
  - Bandwidth Control
  - QoS
  - DNS Filtering
  - URL Filtering
  - Anti-Malware
  - Proprietary Risk Index
  - XSS Protection
  - Behavioral Analysis
  - File Type Control
  - Block Lists
  - Native SSL scanning
  - Proprietary Risk Index
  - XSS Protection

- **SSMA™**
  - All security engines fire with each content scan – only microsecond delay

- **ByteScan™**
  - Each outbound/inbound byte scanned, native SSL scanning

- **NanoLog™**
  - 50:1 compression, real-time global log consolidation

- **PageRisk™**
  - Risk of each object computed inline, dynamically

- **PolicyNow™**
  - Policies follow the user for same on-premise, off-premise protection™

- **Behavioral Analysis**

- **120,000**
  - Unique updates per day

- **125 Million**
  - Threats blocked per Day

- **60+ threat feeds**

- **Cloud Effect**

- **Find once, block everywhere**
Internet: The Next Generation Network

Securing private applications with Zero Trust
VPN over **TIC / JRSS** causes latency
Network-centric methods are no longer effective

**TIC / JRSS** cause latency for all your users, and creates more issues than it solves

**Risk** is introduced by giving too much trust to users and networks

**Complexity** of ACLs and firewalls can make remote access difficult to manage

**Users** become frustrated with a poor experience

**Months** often spent on getting infrastructure set up
Security problems with VPN technology

Broader attack surface = Higher risk

- App access requires a user to be on the network; corporate network extends to every location of a VPN user. This broadens the attack surface, exposing apps to attacks.
- Once on your network, a user can laterally scan other resources and exploit their vulnerabilities.

Over-exposed = Vulnerable

- VPNs are exposed to the Internet – a DDoS target, potential service disruption.
- Attackers will target any exposed surface, discover vulnerabilities, and attack them.

"Attackers who discover services often find vulnerabilities in applications and in (APIs) that bypass firewalls and intrusion prevention systems (IPS). Attackers will target services, users of the services, or both." - Gartner
Fast, secure, zero trust access to internal apps

Zero trust security architecture

1. **Brokers**
   - secure user to app connection

2. **App / Browser Access**
   - request access to app

3. **App Connectors**
   - sit in front of apps – outbound-only connection

Zero trust access

- Treat all as untrusted – both outside & inside the perimeter
- Verification prior to granting access
- Access is granted on a strict “need to know” basis
- App access without requiring network access
- Segment of one is created between named users & named application
Current State of Network
How things are
Bypass the TIC/JRSS thru secure policy-based access to applications, Internet and SaaS services over encrypted connections

Open Internet

3rd Party Cloud/IAAS

Private Applications

Any device, any location, on-network or off-network

HQ

Branch

SO-WAN

Remote / Mobile

Endpoint Agent

Encrypted Connection

TIC

Encrypted Connection

Tunnel

Encrypted Connection

Z Connector

Peering

DHS/Einstein

Legend

PARTNER

EMPLOYEE

CONTRACTOR

Nanologs

Central Authority

IPSoc Tunnel

FedRAMP

Salesforce

Office 365

Box

AWS

Azure

Google Cloud Platform
The 4 tenets that set ZTM apart

1. Proven Zero Trust Model - Users are never placed on-net
2. Dark Network- “Inside-out” connectivity - apps invisible to unauthorized users
3. No inbound connections and no inside listeners allowed
4. Application segmentation, not network segmentation
5. Bypass MTIPS/TIC/JRSS - The Internet is the new secure network
ZPA vis-à-vis NIST 800-207 draft Zero Trust Architecture

• Fulfills the ZTA tenets defined in section 2.1; adheres to assumptions in section 2.2

• Section 2.3 core components (PE, PA, PEP) reside in Zscaler cloud
  • Integrates with existing data sources (direct: IdP, SIEM, PKI; indirect: CDM, compliance, threat intel)

• ZPA maps to multiple Section 3.1 deployment models
  • With Z App - Device Agent/Gateway-Based (3.1.1) & Micro-Perimeter-Based (3.1.2) models
  • With Browser access - Resource Portal-Based model (3.1.3)

• Utilizes singular, criteria-based trust algorithms (section 3.2.1); independent control plane / data plane (section 3.3)

• Applicable to all section 4 use cases - satellite, multi-cloud, contractor, collaboration

• Contributes to mitigation of threats described in section 5
  • Hardened against subversion (5.1), DoS (5.2); stored metadata & policies are protected (5.5)
  • Provides tools to help address insider thread (5.3), network visibility (5.4)
Zero Trust – discoveries & challenges

• Existing networks / access solutions were not designed with Zero Trust in mind
  • Apps, app users, network paths to apps may be undocumented or even unknown
  • Start in discovery mode / more open connectivity, then lock down as you understand more

• Organizations need visibility first into what apps they have, then into who is using what
  • No easy button – best approach is a phased deployment
  • Start with well-characterized use cases while gathering data for more complex scenarios

• Many typical network / security project challenges still apply
  • Agent deployment, IAM integration / maturity, resource classification

• Accountability can be an impediment to implementing a Zero Trust solution
  • Multiple stakeholders with different agendas, responsibilities, visions

• Need to build a comfort level with a new model of access enablement
  • Look forward, not back – build today for tomorrow, not with tools of the past
Recommended Resources

• ACT-IAC
  • Zero Trust whitepaper - https://www.actiac.org/zero-trust-cybersecurity-current-trends
  • Panel discussion - https://www.youtube.com/watch?v=LJip0JsRps0

• Zscaler for government - https://www.zscaler.com/solutions/government

• Zscaler Private Access - https://www.zscaler.com/zpa
  • VPN vs ZPA - https://www.youtube.com/watch?v=EanV0tE9goU

• Zscaler on Zero Trust:
  • Zero Trust and Beyond (webinar)
    • https://community.zscaler.com/t/zero-trust-and-beyond/4302
  • SDP, ZTNA, and CARTA (blog)
  • Zero Trust 10 Years Later (blog)
    • https://www.zscaler.com/blogs/corporate/zero-trust-ten-years-later-it-time-think-bigger
Thank You