Architecting for a Secure Cloud-Enabled Network (HQ, Branch, Mobile Workforce)

Andreas Sartori, Team Lead Security, Porsche Informatik GmbH
Jürgen Rabba, Networking, Volkswagen AG
Nils Ullmann, Solutions Architect, Zscaler
Who we are.
Digital Workplace - Overall schedule 2.0

Legend: Green = Done | Gray = Scope

Stream 0
Q4 2018: DE
Q1 2019: ES
Q2 2019: CS
Q3 2019: UA
Q4 2019: MK, KS, AL, BA
Q1 2020: RO

Stream 1
RS, ME
SI, HR

Stream 2
SG
MY
CO, CL

Stream 3
VU
PL

Summer Holidays
Foundations
Architecture

What drives architecture?

• Goals (What we want) => Cloud, Mobile, Internet Centric
  • Improved end-user performance
  • Cost savings
  • Simplification
  • Agility/Flexibility
  • Improve security and visibility

• Current environment (What we have)

• Phased approach (The path between the two)
  • Phase 1 (Secure) Do no harm!
    • Forward the traffic at the existing egress points
  • Phase 2+ (Simplify => Transform)
    • Reduce dependency on on-premises infrastructure
    • Local internet egress leads to better performance in an internet-centric world
    • Opportunistic optimization
Architecture

Core structural details

• Service edge, tunnels, or client only?

• Routing
  • What to send where and how?

• Failover

• Security
  • ACLs?
  • VRFs?

• Client-forwarding
  • ID, intelligent client decisions (SRC-IP)?
  • Authentication and provisioning
HQ, DC, Hubs
Large Site
Where we typically start

ISP

DMZ
Internet Path

DMZ
(SMTP/Web/etc.)

Corporate Network

©2011 Zscaler, Inc. All rights reserved. ZSCALER CONFIDENTIAL INFORMATION
HQ, DC, Hubs

Decision points

• User population (bandwidth requirements)
• Requirement for continued security infrastructure (DMZ)
• Routing decisions
  • DMZ/Extranet
• Capabilities of existing hardware
  • Positives (GRE, L7 health checks, etc.)
  • Negatives (vulnerable to overload, etc.)
• Phased deployment
  1. Least disruption possible (do no harm)
  2. Optimization (realize benefit of transformation)
Option 1
Usual suspects

- Border routers terminate primary/backup GRE tunnels. IP SLA testing used to detect performance degradation; GRE keepalives for rapid failure detection
- Outbound internet requests exempted from NAT at firewall tier
- Tunnel to Zscaler at border using PBR for outbound internet requests (excludes DMZ traffic)
- Front door VRF at border router optional, ensuring the internal routing table not exposed to internet

- Tunnel termination
  - Do we need tunnels?
- Routing
  - What to send, and how?
- Failover
- Security
  - ACLs?
  - VRFs?
- Client forwarding
track 1 ip sla 1
   delay down 120 up 180.
track 2 ip sla 2
   delay down 120 up 180
ip sla 1
http raw http://172.18.56.162:9480
timeout 5000
threshold 300
http-raw-request
   GET http://gateway.<zscaler-cloud>.net/vpntest HTTP/1.0\r\n   User-Agent: Cisco IP SLA\r\n   End\r\n\r\nexit
ip sla schedule 1 life forever start-time now
ip sla 2
<SNIP>
ip sla reaction-configuration 1 react rtt threshold-value 300 1 threshold-type
consecutive 3
<SNIP>
interface Tunnel301
<SNIP>
!
interface Tunnel302
description "Primary Tunnel B"
<SNIP>
!
interface GigabitEthernet0/0
description "VM Network 10/24"

ip policy route-map zscaler
!
ip route 185.46.212.88 255.255.255.255 Tunnel301 track 1
ip route 185.46.212.88 255.255.255.255 Tunnel302 200 track 2
!

ip access-list extended zscaler
deny ip 10.96.0.0 0.0.0.255 10.0.0.0 0.255.255.255
deny ip 10.96.0.0 0.0.0.255 172.16.0.0 0.15.255.255
deny ip 10.96.0.0 0.0.0.255 192.168.0.0 0.0.0.255
permit ip 10.96.0.0 0.0.0.255 any
!
ip sla 1
<SNIP>
!
route-map zscaler permit 10
match ip address zscaler
set ip next-hop recursive 185.46.212.88
Option 2
Technically best practice

- Core switches terminate primary/backup GRE tunnels; IP SLA testing used to detect performance degradation; GRE keepalives for rapid failure detection (DON’T NAT)
- Firewall tier no longer sees anything but a GRE tunnel
- Tunnel to Zscaler at core using PBR/routing for outbound internet requests
Goal
North star

- Border routers terminate primary/backup GRE tunnels; IP SLA testing used to detect performance degradation; GRE keepalives for rapid failure detection
- NO on-premises firewall
- Tunnel to Zscaler at border using normal default route
- Front door VRF at border router optional, ensuring the internal routing table not exposed to internet
- This looks like an internet café?
• Design decision “default route”
  • No way out for devices
  • Road runners needed some “fixing” for client firewall

• Best performance for web, TCP, and UDP traffic
  • Easy setup, lots of changes 😊
  • Server and application migration is ongoing
  • Public-exposed servers still need proxy PAC

• Dedicated tunnel devices
• Localization is tricky for some countries
  • Language
Beware

Common pitfalls

• Beware the shortcut
  • Today we…so it will just be easier to…
  • We don’t have the resources to…so we will just…

• Failover
  • L7 health checks if possible
  • Testing
  • Consider all single failure scenarios (ISP, MPLS, CPE, Zscaler DC, etc.)

• Z App
  • No one likes agents
  • Everyone likes easy authentication
  • Mobile security is nice too
Zscaler Service Edge

- All the same functionality offered by Zscaler Enforcement Nodes deployed closest to the user in customer’s DC/premises
- Monitored, managed, maintained by Zscaler as an extension of the Zscaler Cloud Enforcement Plane in customer’s premises
- Consistent policy follows the user – no separate configuration required
Zscaler Service Edge
What do I use this for?

Geo localization: Zscaler Service Edge is recommended for addressing geo-localization issues when the network latency to the nearest available Zscaler data center is not within the prescribed limit.

Regulation: Zscaler Service Edge is recommended when regulatory requirements restrict the use of Zscaler public data centers.

Maintaining Source IP: For applications and services requiring a dedicated egress IP address.

Best practice: Zscaler Service Edge should be deployed for high-bandwidth networks (2Gbps and above).
Zscaler Service Edge

Where?

Corporate Network

ISP

DMZ (SMTP/Web/etc.)

Service Edge

GRE Primary
GRE Backup

Outbound Internet Path

Service Edge
Branch
Branch Example

Usual suspects

Zscaler PRIMARY/BACKUP (internet)
Zscaler Private Access (intranet)

Details
• Default route/PBR/etc.
• SD-WAN or traditional route/switch look similar
• There is still a need for a WAN at many organizations
  • Servers and IoT mixed with users
• ZPA is still typically disabled for on-net

Zscaler TERTIARY (internet)
SRC-IP anchored path
VZEN used to pull destinations with source IP restrictions back to the data center (internet)
Zscaler bypass (internet)
Next Steps

Kick the users off the intranet

Zscaler PRIMARY/BACKUP (internet)
Zscaler Private Access (intranet)

Details
- Default route/PBR/etc.
- SD-WAN or traditional route/switch look similar
- There is still a need for a WAN at many organizations
  - KICK USERS off the intranet
- ZPA now defines the end-user perimeter

Zscaler TERTIARY (internet)

SRC-IP Anchored path
VZEN used to pull destinations with source IP restrictions back to the data center (internet)
Zscaler bypass (internet)
• Design needed to be as close as HQ
  • Policy-based routing by source IP to tunnel devices
  • “Default route” for specific IP addresses

• No way out for devices
  • Road runners needed some “fixing”
  • Best performance for web, TCP, and UDP traffic
  • Server and application migration is ongoing
  • Public exposed servers still need proxy PAC

• Dedicated tunnel devices
Internet Only
Zscaler App for BOTH internet/ZIA and intranet/ZPA traffic flows

Details
• Ideally a single managed device (just dial tone)
• Perimeter defined in cloud software for both internet and intranet flows
Internet-Only Branch

Some WAN requirement remains

Zscaler PRIMARY/BACKUP (internet)
Zscaler Private Access (intranet)

Details
• Default route/PBR/etc.
• SD-WAN or traditional route/switch look similar
• There is still a need for a WAN at many organizations
  • KICK USERS off the intranet
• ZPA now defines the end-user perimeter

Zscaler TERTIARY (internet)

SRC-IP Anchored path
VZEN used to pull destinations with source IP restrictions back to the data center (internet)

Zscaler bypass (internet)
Internet Centricity
Centralized vs. Distributed

Legacy

SaaS

Open Internet

IaaS

$Loop + $Port

Data center/Hub

$Loop + $Port

MPLS

$Core network

$Loop + $Port
Centralized vs. Distributed

Colocation strategy

- SaaS
- Open Internet
- IaaS

Core?

Core network

$Loop + $Port

Better Performance?

Better Performance!

Multi-Cloud!

$Loop + $xcon

$Loop + $Port

$Loop + $Port

Core network

MPLS

$Loop + $Port

Better Performance?
Centralized vs. Distributed

Internet-centric (separate intranet from internet)

- SaaS
- Open Internet
- IaaS

- Data center
- Hub

- $Loop + $Port
- $xcon + $Port

- Better Performance!
- Multi-Cloud!

- ISP
- Core network

- $Loop + $Port
- $xcon + $Port

What Else?
What else?

• No default route
• Layered firewalls
• Firewall-based tunnels
• Service Edge and SRC-IP anchored applications
• Global ZEN IPs
• Requirements for local security policy enforcement
• Local intranet traffic flows (intra-branch)
• More detailed discussion surrounding failover and the ways to address this problem
• SD-WAN and how that impacts the above topics
What’s Next?

- Improving monitoring
  - Client calls “internet is not working!!!”
- Cloud be …
  - Firewall
  - Tunnel device
  - Tunnel
  - Zscaler
  - Route missing?
  - Customer equipment
  - …
So, what now?

- Architecture Session
- Come prepared with your network diagrams
- Identify growth pattern for your top 20% of locations
- Bring the team, including network, security, application, end-user compute, etc.
- Give some thought about why your intranet is still required
Thank You
Please share your feedback on this session!

Four easy steps:

2. Select Session Ratings
3. Choose this session from the list
4. Provide your feedback
Template appendix
All documents and communications (including emails) containing Zscaler Confidential Information must be prominently labeled with the following marking on every page: Zscaler Confidential Information.

Zscaler Confidential Information includes any information, whether technical, financial, business, strategic or operational, that when ultimately disclosed to parties unauthorized to have access to it, could be detrimental to the company’s competitive advantage or could adversely affect the company’s ability to conduct business operations.

Disclosure of Zscaler Confidential Information to any non-Zscaler person or entity requires execution of either a Non-Disclosure Agreement (NDA) or contractual agreement with suitable confidentiality provisions. To obtain the most current company NDA, please go to the Legal Department’s page on APEX or email contracts@zscaler.com.

Please note that Zscaler Confidential Information that is highly sensitive should only be distributed to a controlled group of people who have a legitimate need to know business reason and should be password protected.

The full policy can be found here.