Rethinking Cybersecurity in the digital transformation era

Alex Philips, CIO, National Oilwell Varco
Bill Lapp, VP, Customer Success, Zscaler

CSO50, Scottsdale, AZ
In the World of Cloud, Network security is becoming irrelevant

### Old World

**Application Location**
- On-premises data center

**Network Architecture**
- “Hub-and-spoke”: backhaul traffic to the on-premises data center

**Security Approach**
- “Castle and Moat” to secure the corporate network

### New World

**Application Location**
- Public cloud, SaaS, on-premises data center

**Network Architecture**
- Direct-to-cloud: traffic routed locally to the internet

**Security Approach**
- Securely connect users and devices regardless of network
Cloud and mobility: opportunities and challenges

“GE will run 70% of our workloads in the cloud by 2020.”
Jim Fowler, CIO, GE

127x growth in Global IP traffic from 2005-2021 (1)

Over 60% of browser-based traffic is SSL (2)

“Network security is becoming less relevant. A new approach is needed.”

Do we control the Internet? How do you secure the network?

Note: (1) Cisco Visual Networking Index: Forecast and Methodology, 2016-2021
Note: (2) Mozilla Firefox report

“The Internet will become our new corporate network”
Frederik Janssen, Head of Infrastructure, Siemens
Zscaler enables secure IT transformation to the cloud

Fast and secure policy-based access to applications and services over the Internet

**Zscaler Internet Access**
- Securely connects users to externally managed SaaS applications and internet destinations

**Zscaler Private Access**
- Securely connects authorized users to internally managed applications

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

• Legalese
• Introduction
• Old NOV IT
• Pain
• Solution
This presentation was developed by National Oilwell Varco as an internal guide and while every effort was made to insure its accuracy, this presentation is only intended to be used as a training aid. Improvements in equipment including, but not limited to, design, engineering, materials, production methods or customer specifications may necessitate changes in the equipment that may result in inconsistencies between the contents of this publication and the end product. National Oilwell Varco reserves the right to make these changes without incurring any liabilities or obligations beyond those stipulated in a signed purchase contract with its customer. The images, photographs, charts, diagrams, drawings, verbal contents and specifications contained herein are not to be construed as giving rise to any warranty, and are not to be regarded as approval or disapproval of any specific product or practice on the part of National Oilwell Varco.

copyright National Oilwell Varco, L.P. – 2018
INTRODUCTION
Introduction – Who is NOV?

National Oilwell Varco is a leading provider of technology, equipment, and services to the global oil and gas industry that supports customers’ full-field drilling, completion, and production needs. Since 1862, NOV has pioneered innovations that improve the cost-effectiveness, efficiency, safety, and environmental impact of oil and gas operations.

NOV powers the industry that powers the world.

36,000 Employees

635 locations

66 Countries

$7.3 Billion Revenue 2017

$13.7 Billion Market Cap – NOV (NYSE)

300+ Acquisitions in last 20 years
Introduction – Who am I?

Alex Philips

CIO/CISO
NOV – 20 years
MBA – Rice Univ.

CIO Responsibilities
- Global IT
- Product IT
- Corporate Engineering Technology
- Corporate Financial Systems
- Corporate Data Warehouse

CISO Responsibilities
- IT Security
- eDiscovery
- Incident Response
- Vulnerability Management
- M&A Security
- Product IT Security
Old NOV IT – Massive Growth

- 2002 – 4,200
- 2003 – 4,800
- 2004 – 6,520
- 2005 – 8,300 (Varco)
- 2006 – 9,500
- 2007 – 13,500
- 2008 – 19,200 (Grant)
- 2009 – 21,000
- 2010 – 23,700
- 2011 – 25,500
- 2012 – 27,835 (Ameron)
- 2013 – 36,620 (Wilson & R&M)
- 2014 – 36,620 (DNOW Spin)
PAIN!
Revenue: $24B to $7B
Employees: 65,000 to 35,000

Pain!

Historic Oil Price

OIL AT $100 A BARREL
Solution
Solution - Zscaler

**Phase 1:** URL Filtering, A/V, IPS, Phishing, Sandbox, etc.

**Phase 2:** SSL Decrypt (in Progress)

**Phase 3:** Road Warrior – Endpoint Agent

**Phase 4:** Zscaler Private Access (ZPA)
New Capabilities

- Reliable
- Highly Scalable
- Available
THE BAD GUYS KNOW IT!

**Source: Gartner**

>50% of all malware will use SSL by 2017*

**Advanced Threats use SSL to hide C&C almost as default**

- *sslbl.abuse.ch* (the “Zeus Tracker” site)
- 423 blacklisted SSL certificates (May `14 – Jan `15):
  - Most (recently) are “Dyre C&C”
  - Many are “KINS C&C”, “Vawtrak MITM”, “Shylock C&C”
  - Several are generic “Malware C&C”
- …that’s a dozen recent malware families using SSL

---

*Source: Gartner*
Results
Results – Cost Savings

• Operational Savings
  – No more upgrades / patching
  – Team can focus on other projects
  – Administration Consolidation
    • Rules set follows user
    • Single Pane of Glass
    • Consolidated logging

• Hardware Savings
  – No EOL (End of Life)
  – No Max Capacity, new appliance
  – No new acquisition costs
Results – Office 365

- No need for ExpressRoute
- Zscaler Direct Peering
- 1 Click Configure
- TCP/IP Window Scaling
- Optimal GTM DNS
Results – SSL Visibility

Past 60 Days NOV SSL Traffic

• 70% of NOV traffic
• Of 5% total HTTPS inspected, 40% was blocked due to threats
  – Currently send uncategorized
• 96 0-day malware items were detected as malicious in Sandbox via SSL/HTTPS traffic
Security Advisory – February 13, 2018
Zscaler protects against 11 new vulnerabilities for Internet Explorer, Microsoft Edge, Microsoft Windows, ChakraCore and Microsoft Word.

Zscaler, working with Microsoft through their MAPP program, has proactively deployed protection for the following 11 vulnerabilities included in the February 2018 Microsoft security bulletins. Zscaler will continue to monitor exploits associated with all vulnerabilities in the February release and deploy additional protections as necessary.

CVE-2018-0742 – Windows Kernel Elevation of Privilege Vulnerability

Severity: Important
Subscriptions Required
  • Advanced Cloud Sandbox

Affected Software
  • Windows 7 for 32-bit Systems Service Pack 1
  • Windows 7 for x64-based Systems Service Pack 1
  • Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
  • Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
  • Windows Server 2008 R2 for x64-based Systems Service Pack 1
  • Windows Server 2008 for 32-bit Systems Service Pack 2 (Server Core installation)
  • Windows Server 2012
  • Windows Server 2012 (Server Core Installation)
  • Windows 8.1 for 32-bit systems
  • Windows 8.1 for x64-based systems

Security Advisory – February 13, 2018
Zscaler protects against 22 new vulnerabilities for Adobe Flash Player and Acrobat Reader.

Zscaler, working with Microsoft through their MAPP program, has proactively deployed protections for the following 22 vulnerabilities included in the February 2018 Adobe security bulletins. Zscaler will continue to monitor exploits associated with all vulnerabilities in the February release and deploy additional protections as necessary.

APSB18-03 – Security updates available for Adobe Flash Player.

Adobe has released security updates for Adobe Flash Player for Windows, Macintosh, Linux and Chrome OS. These updates address critical vulnerabilities that could potentially allow an attacker to take control of the affected system.

Severity: Critical
Affected Software
  • Adobe Flash Player Desktop Runtime 28.0.0.137 and earlier for Windows, Macintosh and Linux
  • Adobe Flash Player for Google Chrome 28.0.0.137 and earlier for Windows, Macintosh, Linux and Chrome OS
  • Adobe Flash Player for Microsoft Edge and Internet Explorer 11 28.0.0.137 and earlier for Windows 10 and 8.1

Subscriptions Required
  • Advanced Cloud Sandbox
The overall traffic for National Oilwell Varco (US), processed by Zscaler, has increased by 15.64% in the last 6 months.

Transactions Blocked Average Comparison

Last month 0.89% of transactions processed by Zscaler for National Oilwell Varco (US) were blocked due to threats found and policies violated.
Appliance Hell
Partner – ZSR

- Quarterly Meeting
- Proactive Analysis
- Malware Deep Dive
- Recommendations
- Actionable
<table>
<thead>
<tr>
<th>CLIENT OUTCOME</th>
<th>WHAT</th>
<th>MEASURE</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>TRANSFORMATION</strong></td>
<td><strong>Coverage – Everywhere &amp; Everything</strong></td>
<td>SSL Inspection ON</td>
</tr>
<tr>
<td></td>
<td></td>
<td>~70% ssl (5% inspected)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Offnet Users Protected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Over 20k Zapp</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All Ports/Protocols</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No DLP</td>
</tr>
<tr>
<td></td>
<td><strong>Network Transformation</strong></td>
<td>28 Local Breakouts Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>52 GRE Tunnels</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 IPSec Tunnels</td>
</tr>
<tr>
<td></td>
<td></td>
<td>On-premise Appliances</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Retired</td>
</tr>
<tr>
<td></td>
<td><strong>O365 Transition</strong></td>
<td>OneClick Enabled</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(21% of Traffic)</td>
</tr>
<tr>
<td></td>
<td><strong>Cloud/App Transformation</strong></td>
<td>Legacy VPN for App</td>
</tr>
<tr>
<td></td>
<td></td>
<td>remote access</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adoption of Cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(AWS/Azure)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Cloud Application Policies Defined; 1/10</td>
</tr>
<tr>
<td><strong>EXPERIENCE</strong></td>
<td><strong>User Experience</strong></td>
<td>Best Practices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>GRE Tunnel Fail over test</td>
</tr>
<tr>
<td></td>
<td></td>
<td>100% Deployed</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Latency ~95% of traffic</td>
</tr>
<tr>
<td></td>
<td></td>
<td>has less than 10ms☺</td>
</tr>
<tr>
<td></td>
<td><strong>Quality</strong></td>
<td>Cases &amp; CSAT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>No Cloud Incidents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Project Ticket Progress</td>
</tr>
<tr>
<td></td>
<td><strong>Results</strong></td>
<td>Security Threats</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trending down</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td></td>
<td>80M Daily transactions</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ROI (VMO)</td>
</tr>
<tr>
<td><strong>ENGAGEMENT</strong></td>
<td><strong>Client &amp; Zscaler</strong></td>
<td>Zscaler Service Reviews</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Qtrly</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network, Security</td>
</tr>
<tr>
<td></td>
<td></td>
<td>team involvement</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Groups, Brand Ambassadors, Reference</td>
</tr>
</tbody>
</table>
New Mindset – ZPA (Zscaler Private Access)

- VPN Replacement
- Keeps users off network
- Full access logs per app
- Carrot to offnet filtering stick
New Mindset – SDWAN

- Cheap Boxes
- Zscaler for Security

I ❤️ SDWAN

- 4X less MPLS $$$$
- 10x – 20x Speed Increase
Key insights

- Cloud & mobile world is disruptive to traditional IT & security
- Zscaler opens the world to digital transformation
- Zscaler gives the 3 C’s: Consolidate, Reduce Complexity, Reduce Cost
- Zscaler is a partner not a vendor
- It requires progressive leadership to move away from on-prem software and security appliances

Security Health Check at [www.zscaler.com](http://www.zscaler.com)
Come Visit the Zscaler Booth in Vendor Area
Network security is becoming irrelevant

Estimated $17.7 billion spent annually on legacy security appliances

Network– Centric

Secure the corporate network to protect users and data
Build a security moat appliances to protect the network

User – Centric

Securely connect users to apps or services
Decouple network access from application access

Policy Enforcement Checkpost

SaaS
Open internet
Public cloud
Private cloud / On-premise data center

HQ
MOBILE
IOT
MOBILE
HQ
BRANCH
Move to backup depending on what Alex has
Add NOV Slides here
A three-step journey to secure IT transformation: Land & Expand

**SECURE**
Up-level security
- Replace proxy or VPN in days
- Little infrastructure change
- Enhance Security

**SIMPLIFY**
Remove multiple point products
- Phase out gateway appliances
- Outbound or inbound gateway
- Reduce cost and complexity

**TRANSFORM**
Cloud-enable network, app access
- Enable local Internet breakouts (SD-WAN)
- Enable direct access to internal apps
- Security + User Experience + ROI

Reduces sale cycles and accelerates deployments
Building a cloud with single-tenant appliances

Zscaler built from scratch a highly scalable and ultra-fast multi-tenant cloud security architecture.

- Disparate redundant control, logging, and enforcement policies
- Multiple appliances, multiple hops — slow user experience
- Expensive and complex to scale and manage

- Integrated control, logging, and enforcement
- Single pass architecture — performance SLA and security efficacy
- Infinitely scalable — cost effective

Legacy technology cannot be repurposed for the cloud

Move to backup depending on what Alex has
Zscaler: A critical Integration Partner Positioned in the Data Path

Extensible Zscaler platform is leveraging cloud eco-system

1. Cloud providers
   - Secure access without security appliances
   - In-Line
   - Faster user experience (Direct-to-Internet)

2. Identity and authentication
   - Conditional access / SAML integration

3. Reporting and analytics
   - Real-time log feed

4. Device management and protection
   - Provisioning and remediation

5. Branch (SD-WAN)
   - Automated traffic forwarding

---

1. SaaS / Workday
2. Public Cloud
3. Microsoft
4. Okta
5. VMware
6. AWS
7. Google Cloud
8. Azure
9. Splunk
10. ArcSight
11. Riverbed
12. Cisco
Zscaler = Zenith of Scalability

Unparalleled Cloud Scale

- Conglomerates: 3 of the top 3
- Oil/Gas: 3 of the top 4
- Beverage: 5 of the top 7
- Apparel: 2 of the top 4
- Chemicals: 2 of the top 3
- Food Retail: 6 of the top 12
New Leaders are Born when Megashifts take Place

Data center and hardware

Applications in the data center

On-Premise security
Example of an enterprise network and security topology

Cost, complexity, and poor user experience

- 9 Data Centers
- 8 internet egress points managed by 6 different teams
- 8 email systems managed by 6 different teams

- 900 locations across 22 countries
- 10,000 Users
- 3,000 Remote Users on 5 VPN solutions

17 MPLS providers with various configurations
ZIA – Fast, secure access to the Internet and SaaS

Differentiated Capabilities

SSL Interception at Scale
Purpose-built proxy architecture – required for SSL interception.

Identical Protection with PolicyNow™
Users connect to the closest data centers (100 around the world) and policy follows them.

Unprecedented Visibility with Nanolog™
Continuously updated dashboards with interactive mining of billions of transaction logs.

Siemens
“Siemens gains much higher resiliency with Zscaler by using their state-of-the-art cloud security gateways”

Kelly Services
“Reduced expenses for MPLS services by roughly 60 percent to enable direct connections to the internet from regional offices”
ZPA – Fast, secure access to internally managed apps

A New Approach to Remote Access (Not VPN 2.0)

Remote users are never brought on the corporate networks
(App access is decoupled from corporate network access)

Apps are invisible to unauthorized users
(No inbound user connections to the corporate network)

Native app segmentation
(Outbound microtunnels connect a named user to a named app)

Four Primary Use Cases

Simplifies access to apps on AWS and Azure
(No need for site-to-site VPNs)

VPN replacement
(Eliminates the cost and complexity of inbound gateways)

Secure partner access
(App access without corporate network access)

Accelerates M&A integrations
(No need to converge IT infrastructure)
Leading industry analysts agree...

Zscaler is a very strong choice for any organization interested in a cloud gateway.

...on-premises web content security can’t protect digital business...