What’s new with Zscaler Private Access (ZPA)

Dhawal Sharma, Senior Director Product Management, Zscaler

Dhwanit Shah, Principal Product Manager, Zscaler
What did we do since Zenith Live 2018

• Browser Access

• Multiple Identity Provider (MIDP)

• Significantly Enhanced Reporting and Analytics

• 100+ other releases/enhancements

• Almost doubled the capacity of ZPA ZENs, 13 new Data Centers added
ZPA Traffic Growth - Patrick

• Insert cool chart

ZPA Cloud Scaling – Traffic Past 12 Months

400% Traffic Growth (Mbps)
Zscaler App - 5 Million devices deployed
ZPA – Trusted and Accredited

• Today there are only 5 JAB-High FedRAMP Companies in all of IT

• In Jul’19 ZPA completed a FedRAMP JAB-High Readiness Audit
What we will discuss in this section

- Features currently running in production
- Features in limited availability
Introducing Network Exposure Detector (N.E.D) 🌟
How well do you know your **Attack Surface**?

Do you know which servers you have **exposed** to the internet?

How much information is your **namespace** giving away?

How **vulnerable** are these servers?

Is your **attack surface** expanding?
N.E.D can help!

Evaluate your Attack surface

- All exposed servers
- Known vulnerabilities against these
- Namespace-risk scoring (keyword based)
- Servers with weaker TLS support
- Public cloud instances

Based on information publicly accessible
- On-demand report (no archival)
- Authorized access

Consult your Zscaler account team
N.E.D can help!

Evaluate your Attack surface

- All exposed servers
- Known vulnerabilities against these
- Namespace-risk scoring (keyword based)
- Servers with weaker TLS support
- Public cloud instances

Based on information publicly accessible
- On-demand report (no archival)
- Authorized access

Consult your Zscaler account team
N.E.D can help!

Evaluate your Attack surface

- All exposed servers
- Known vulnerabilities against these
- Namespace-risk scoring (keyword based)
- Servers with weaker TLS support
- Public cloud instances

Based on information publicly accessible
- On-demand report (no archival)
- Authorized access

Consult your Zscaler account team
N.E.D can help!

Evaluate your Attack surface

- All exposed servers
- Known vulnerabilities against these
- Namespace-risk scoring (keyword based)
- Servers with weaker TLS support
- Public cloud instances

Based on information publicly accessible
- On-demand report (no archival)
- Authorized access

Consult your Zscaler account team
N.E.D can help!

Evaluate your Attack surface

- All exposed servers
- Known vulnerabilities against these
- Namespace-risk scoring (keyword based)
- Servers with weaker TLS support
- Public cloud instances

Based on information publicly accessible
- On-demand report (no archival)
- Authorized access

Consult your Zscaler account team
N.E.D Demo
Traditional network security methods that listen for inbound connections often expose IP addresses and namespaces to the Internet. This not only leaves servers vulnerable to attacks but also gives away information that needs to be kept private.

With just a simple domain search the Zscaler N.E.D tool performs an extensive analysis and offers a consolidated report of any unintended public network exposure of private apps.

1. Gain visibility into which servers are exposed
2. Receive a network exposure score and detailed assessment
3. Connect with us to learn how zero trust network access (ZTNA) services can help
Traditional network security methods that listen for inbound connections often expose IP addresses and namespaces to the Internet. This not only leaves servers vulnerable to attacks but also gives away information that needs to be kept private.

With just a simple domain search the Zscaler N.E.D tool performs an extensive analysis and offers a consolidated report of any unintended public network exposure of private apps.

1. Gain visibility into which servers are exposed
2. Receive a network exposure score and detailed assessment
3. Connect with us to learn how zero trust network access (ZTNA) services can help
Network Exposure Risk

- Your environment is highly exposed to known vulnerabilities
- There is a high number of servers with an outdated SSL/TLS posture
- Take immediate action to reduce your exposure

Network Assessment

Known Vulnerabilities

393 known vulnerabilities
Known Vulnerabilities

393 known vulnerabilities

These are the total number of known vulnerabilities existing in your servers exposed to the internet. This information is exposed and easily available to bad actors. These are well known vulnerabilities with known exploits and hence is a greater risk. As a result this contributes towards 30% of your overall network exposure risk grading.

SSL/TLS Risks

151 SSL/TSL risks

Nefarious actors will often target servers whose SSL/TLS posture is outdated, or that can be reverted back to a previous version. This information highlights the servers who are currently at risk. There are well known weaknesses in older SSL/TLS versions which can be exploited and we count all servers that support TLS version 1.0 or prior. As a result this contributes towards 20% of your overall network exposure risk grading.

Exposed Servers

520 exposed servers

This number represents the amount of servers running within your organization’s network currently exposed to the internet. These are therefore accessible to bad actors. The higher the number, the larger the potential attack surface is. While some of these might be intentional and available for public, internet use, many are often private applications that need to be made invisible to the internet. Since none of these might not be intentional, this contributes towards 50% of your overall network exposure risk grading.
Exposed Servers

This number represents the amount of servers running within your organization's network currently exposed to the Internet. These are therefore accessible to bad actors. The higher the number, the larger the potential attack surface is. While some of these might be intentional and available for public, internet use, many are often private applications that need to be made invisible to the internet. Since many of these might not be intentional, this contributes towards 20% of your overall network risk exposure grading.

Namespace Exposure

Calculated based on certain keywords matching your namespace. We believe these can potentially give away information about the application and intentions of the hosted server. This number provides a snapshot as to how at risk your environment is to unintended exposure. For example, a high score indicates high risk.

Public Cloud Instances

Public cloud is often an attack vector bad actors leverage. This number represents the amount of public cloud instances managed by your organization that are currently exposed to the Internet. This contributes towards 10% of your overall network risk exposure grading.
Network Assessment Report for

www.alvisonetworks.com

Network Exposure Risk

- Your environment is highly exposed to known vulnerabilities.
- There is a high number of servers with an outdated SSL/TLS posture.
Network Assessment Details

<table>
<thead>
<tr>
<th>Known Vulnerabilities</th>
<th>393 known vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Here's a list of known vulnerabilities existing in your servers exposed to the internet. This information is exposed and easily available to bad actors. You will also find the associated known CVEs for each of these vulnerable servers.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>IP</th>
<th>Product</th>
<th>Vulnerabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>ci.alvisonetworks.com</td>
<td>167.52.177</td>
<td>Apache httpd</td>
<td>CVE-2010-2068</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2011-4317</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2017-7679</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2011-3368</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2011-3348</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2012-3499</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2012-4558</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2013-1896</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2016-8612</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2012-4557</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2014-0098</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2017-7668</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>CVE-2013-6438</td>
</tr>
<tr>
<td>api.alvisonetworks.com</td>
<td>167.52.28</td>
<td>Microsoft IIS httpd</td>
<td>CVE-2010-1256, CVE-2010-2730, CVE-2010-3972, CVE-2010-1899, CVE-2012-2531</td>
</tr>
<tr>
<td>------------------------</td>
<td>----------</td>
<td>---------------------</td>
<td>-------------------------------------------------</td>
</tr>
</tbody>
</table>

**Recommended Mitigation**

- Apply known patches to mitigate the CVEs.
ZPA Platform Updates
Support for Multiple IDPs

Eliminates need to integrate directories during M&A

Simplifies partner life-cycle management in enterprise IDP

BUs can share identity across ZPA tenants while preserving admin independence

A partner organization can configure the same IDP in ZPA tenants of multiple customers
Support for Multiple IDPs

Support for multiple IDPs

- Eliminates need to integrate directories during M&A
- Simplifies partner life-cycle management in enterprise IDP
- BUs can share identity across ZPA tenants while preserving admin independence
- A partner organization can configure the same IDP in ZPA tenants of multiple customers
ZPA User portal

User experience + security

Boost user productivity
User portal displays all apps a users has access to.

Least privilege access
Visibility is based on the identity of the users and policies set by admins

Versatility
Option to white label portal with your own logo and publish apps as URLs

Integrated with key ZPA features
User portal support browser access, Zscaler app and public apps
ZPA User portal

Displays links to applications that a user is authorized to access

Any ZPA Application can be displayed on the user portal

Any public website can be published as a web link on the portal

Use Cases

Provide visibility to authorized applications for 3rd party users

Provide visibility to internal applications following an acquisition
User Portal Demo
### Software - IT Support

<table>
<thead>
<tr>
<th>Project</th>
<th>Key</th>
<th>Project type</th>
<th>Project lead</th>
<th>Project category</th>
<th>URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lab Support</td>
<td>LAB</td>
<td></td>
<td>William Hua</td>
<td>IT Support</td>
<td>No URL</td>
</tr>
</tbody>
</table>
# Approvals

## Invoices

<table>
<thead>
<tr>
<th>Invoice Name</th>
<th>Employee Name</th>
<th>Submit Date</th>
<th>Invoice Date</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No records found.</td>
</tr>
</tbody>
</table>

---

**SAP Concur**

[Processor Privacy Statement](#)

[Service Status (North America)](#)

Last logged in: 09/11/2018 3:28 PM
<table>
<thead>
<tr>
<th>Name</th>
<th>Status</th>
<th>URL</th>
<th>Notification Banner</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>My User Portal</td>
<td></td>
<td><a href="https://portal.tanuk.ca">https://portal.tanuk.ca</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Production User Portal</td>
<td></td>
<td><a href="https://www.portal.company.com">https://www.portal.company.com</a></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>Display on Portal</td>
<td>URL</td>
<td>Actions</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</td>
<td>--------------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>crm.lanuk.ca</td>
<td>✅</td>
<td>crm.lanuk.ca</td>
<td>✅ ✗</td>
<td></td>
</tr>
<tr>
<td>test.lanuk.ca</td>
<td>✅</td>
<td>test.lanuk.ca</td>
<td>✅ ✗</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.oneone.com">www.oneone.com</a></td>
<td>✅</td>
<td><a href="http://www.oneone.com">http://www.oneone.com</a></td>
<td>✅ ✗</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.onetwo.com">www.onetwo.com</a></td>
<td>✅</td>
<td><a href="http://www.onetwo.com">http://www.onetwo.com</a></td>
<td>✅ ✗</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.yahoo.com">www.yahoo.com</a></td>
<td>✅</td>
<td><a href="http://www.yahoo.com">www.yahoo.com</a></td>
<td>✅ ✗</td>
<td></td>
</tr>
<tr>
<td>Yahoo App</td>
<td>✅</td>
<td><a href="https://www.yahoo.com">https://www.yahoo.com</a></td>
<td>✅ ✗</td>
<td></td>
</tr>
</tbody>
</table>
Zscaler App
Enhanced Posture with Z App

**Use cases:**
Device posture as a criteria in Access Policy

- **Current**
  Certificate, File check and Registry Keys

- **Released with 1.5**
  Client Certificate, Device Firewall, Fill Disk Encryption, Domain, Jailbreak/Rooted device

- **EDR Partner ecosystem for posture**
  Crowd Strike, Carbon Black, Sentinel One
Support for Multiple Trusted Networks in ZPA

Tunnel or Bypass based on Location

Application A:
IF “Office A” Bypass
IF “Office B” Tunnel

Application B:
IF “Office A” Tunnel
IF “Office B” Bypass

Both Offices Are Trusted Networks
## Setting up MTN Policy

### Trusted Networks

<table>
<thead>
<tr>
<th>#</th>
<th>Network Name</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>HQ San Jose</td>
<td>HOSTNAME AND RESOLVED IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>jira.corp.zscaler.com:10.32.115.31</td>
</tr>
<tr>
<td>2</td>
<td>America Center</td>
<td>DNS SEARCH DOMAINS</td>
</tr>
<tr>
<td></td>
<td></td>
<td>corp.zscaler.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HOST NAME AND RESOLVED IP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ab.com:123.123.123.123</td>
</tr>
<tr>
<td>3</td>
<td>Sydney Office</td>
<td>SSID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ZscalerSydWiFi</td>
</tr>
</tbody>
</table>
Recommended Next Steps

- Experience ZPA with a 7-day “ZPA Interactive” demo
  - [https://www.zscaler.com/zpa-interactive](https://www.zscaler.com/zpa-interactive)
- Sign up for early access for Browser Isolation
- Set up a meeting with your rep on ZPA
In an open forum with Zscaler employees, partners, and customers

Your knowledge and learn from experts in cloud security

The conversation at community.zscaler.com