Zscaler
Faculty Senate

Jesse Castellani - Security Architect
Dan Han - CISO
Agenda

- Goals and Challenges
- Zscaler Overview
- HTTP Overview
- FAQ / Q&A
Business Aspirations

Anywhere

Anytime

Ease

Secure
Security Challenges

74% ↑ 358% ↑

VPN 2.0

Security Features:
- Firewall as a Service
- Secure Web Gateway
- Malware detonation chamber
- Phishing site detection and prevention
- Intrusion detection and prevention
- Reverse Proxy Based always-on remote access
- Device posture management
- Application based access control

Zscaler Agent Client (ZCC)

ZScaler Internet Access and ZScaler Private Access
Zscaler Client Connector (ZCC)

**macOS**

**Windows**
**Internet Access**

- Consistent security policy for network and applications
- Warning of potentially malicious and dangerous sites
- File inspection and malware detonation
- DLP capabilities
- Risk-based classification of third party apps

**Private Access**

- Always-on access to internal university resources
- Reverse-proxy exposes access to application
- Device posture check
- Application health monitoring
- Pre-authentication connection to internal resources
- Risk-based access control
Zscaler - Warning Example

⚠️ Are you sure you want to visit this site?

You tried to visit:  http://pastebin.com/

Request method cautioned for category Anonymous Paste Sites

Proceeding to visit the site may be dangerous and/or may violate VCU’s Computer and Network Resource Use policy. Press the "Continue" button to access the site anyway or press the "Back" button on your browser to go back.

Continue  See our internet use policy.

Need help? Contact our support team at +1 (804) 828-2227, itsupport@vcu.edu
Zscaler - Block Example

We found a security threat.

The site you are trying to visit is not permitted. If you believe this site is blocked in error, then please contact the VCU IT Support Center at (804) 828-2227 or itsupport@vcu.edu

You tried to visit: http://example.com

Threat found: Virus

Click to request security review.
See our Internet use policy.

Need help? Contact our support team at +1 (804) 828-2227, itsupport@vcu.edu
How Does Zscaler Work?
HTTP Overview
HTTP (Hyper-Text Transfer Protocol)

- How our computers request and load **websites**
How It Works with Zscaler

HTTP Header
HTTP Payload

Internet

Youtube Server

Malware Sandbox
Firewall
Phishing Site Detection
IPS/IDS
DLP

Zscaler Analytics

youtube.com

WARNING
<table>
<thead>
<tr>
<th>Feature</th>
<th>Zscaler</th>
<th>Other Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access VCU Applications?</td>
<td>✔️</td>
<td>✔️</td>
</tr>
<tr>
<td>Continual Access?</td>
<td>✔️</td>
<td>❌</td>
</tr>
<tr>
<td>Detect Malware/Phishing?</td>
<td>✔️</td>
<td>❌</td>
</tr>
<tr>
<td>Protect from Harmful Traffic?</td>
<td>✔️</td>
<td>❌</td>
</tr>
</tbody>
</table>
Accomplishes
Future VCU Security Model
Roll-Out Plan

- Currently working with the vendor in designing and implementing the solution in our environment.
- Engaging all schools, colleges, and units in helping us test both the Internet protection and private access aspects.
- Need to build out access rules for private assets (e.g., SSH to a server, printing system, other unique access to assets).
Tentative Project Timeline

- **Completed Zscaler Procurement**
  - Pre-Pilot Testing
  - Oct. 2022

- **Pilot with Technology Services**
  - Jan. 2023

- **Phased Roll Out Begins**
  - March 2023

- **Phased Roll Out Ends**
  - June 2023

- **Transition to Operational Status Begins**
  - June 2023

- **Transition to Operational Status Ends**
  - July 2023

- **Pre-Pilot Beta**
  - Nov. 2022
Zscaler FAQ:

Who is it intended for?
VCU Employees, Student Workers, Graduate Assistants, and Affiliates

What devices can install the Zscaler Application (ZCC)?
VCU Managed Devices

What are the limitations of Zscaler?
Server initiated connections through ZPA (e.g. Wake-on-lan) are not possible at this time.

What will students use?
Cisco AnyConnect VPN
Zscaler FAQ Con’t

Will Zscaler replace Cisco Anyconnect?
No. Although in the future, sensitive applications would be limited to Zscaler.

Can I use Zscaler and Cisco Anyconnect at the same time?
Yes. There are some limitations when using ZPA and Cisco Anyconnect.

Do I have to reconnect to Zscaler everyday?
No.

What can VCU see when I use Zscaler?
While using Zscaler, VCU has access to logs and other metadata for network traffic while using Zscaler.