IT Digital Chat

July 14, 2017
Agenda

- Strategic Goals & Action Plans
- Enterprise Firewall Project Overview
- Identity Management Update
- General Announcements
Strategic goals

Transforming Teaching & Learning
Expanding Research
Streamlining Service Delivery
Enhancing Security, Privacy, and Accessibility
Investing in the Workforce
Aligning through Governance & Transparency
Continuously Transforming the Technology Enterprise
Next Generation Firewall Migration

Moving from Cisco ASA to Palo Alto
July 2017
1. **Automation** – Our firewall web page has provided automation and self service functionality for over 10 years. The tool processes hundreds (750+) of self service changes each month!

2. **Scale/Segmentation** – Between 2003 and 2008, the firewall team put every network behind a unit level firewall. Today we manage over 580 virtual firewalls.

3. **Platform Capability** – Our current ASA platform is limited to packet header inspection (up to layer 4).
Why not stay with the ASAs?

- Stateful inspection, port-based firewalls are steadily becoming less effective
  - Many legitimate applications leverage common ports.
  - Malicious traffic runs on non-standard ports in order to penetrate firewalls or avoid detection.
  - Certain attacks, such as IP fragmentation attacks, can be crafted to totally bypass stateful, Layer 4 based firewalls.

The chosen solution and why

- On December 12, 2016, a Georgia Tech employee’s computer containing sensitive data was compromised with malicious software.
- We have done extensive evaluations of both Cisco FirePower and Palo Alto appliances. It became clear to the firewall team that Palo Alto was the superior platform.
- Throughout our testing, we have validated features we currently use and those we plan to use. We have also verified compatibility with our current tools.
- We have also run a production network through a Palo Alto appliance for the last few months with very few reported issues.
Benefits and Advanced Features

• Application based firewall rules
  – Rules can be based on application, regardless of the layer 4 ports being used. We will even have the capability to block/allow specific features within applications.

• User-ID based firewall rules
  – We will have the ability to create user-ID based rules. This will allow us to not only control what is accessed, but who accesses it.

• Threat Prevention
  – End users can be protected from worms, viruses, spyware, malicious files, etc. If a file is suspect, it can be uploaded to Palo Alto’s security center for analysis. Once malware has been identified by Palo Alto, a signature update can be pushed out to our firewalls within 5 minutes. Advanced URL filtering can also protect us from malicious urls embedded within e-mails!

• Advanced monitoring and Reporting
Very Advanced Features (Optional)

- We can automatically quarantine hosts within seconds of being identified as compromised, create Service Now tickets, and redirect end users to Splash pages informing them of the compromise.

- DDoS Mitigation capability

- We can create rules based on VMWare tags. This will allow VMWare administrators to dictate firewall policy by applying tags. No one will need to touch a firewall. Once the VM is destroyed, the firewall rule is automatically cleaned up!
Limited User Impact

• We have fully integrated fw.noc with our Palo Alto appliances. The migration will be seamless for users of our self service tools.

• We have the capability to easily steer traffic back to the old ASA(SM)s in the event we need to back out of the upgrade. It can be done per firewall, with two commands on the router.

• Our VPNs are not part of the scope of this migration. We plan on continuing to use our current VPN appliances.
Phased Rollout

Phase 1
- All current firewalls and rules will be migrated to Palo Alto appliances by October 26th
- This includes the replacement of our current IPS functionality at our border.

Phase 2
- Application-ID rule migration (layer 4 rules will still be supported)
- Enablement of Threat Prevention on unit firewalls
- Turn on DDoS mitigation tools

Phase 3 (tentative)
- Enable automatic quarantine of infected hosts
- Utilize VMWare tag based policies
- User-ID rule migration (based on situation)
# Phase 1 Schedule

<table>
<thead>
<tr>
<th>Appliance</th>
<th>Dates</th>
</tr>
</thead>
<tbody>
<tr>
<td>resnet-dept-pa migration</td>
<td>August 8, 2017</td>
</tr>
<tr>
<td>ni-border-pa migration (Resnet Border)</td>
<td>August 10, 2017</td>
</tr>
<tr>
<td>rich-border-pa migration (Campus Border)</td>
<td>August 15, 2017</td>
</tr>
<tr>
<td>bcdc1-dept-pa migration</td>
<td>September 5, 2017</td>
</tr>
<tr>
<td>rich-dept-pa migration</td>
<td>September 19, 2017</td>
</tr>
<tr>
<td>dc-dept-pa migration</td>
<td>September 26, 2017</td>
</tr>
<tr>
<td>ni-dept-pa migration (part 1)</td>
<td>October 3, 2017</td>
</tr>
<tr>
<td>ni-dept-pa migration (College of Computing)</td>
<td>October 5, 2017</td>
</tr>
<tr>
<td>si-dept-pa migration</td>
<td>October 10, 2017</td>
</tr>
<tr>
<td>ei-dept-pa migration</td>
<td>October 24, 2017</td>
</tr>
<tr>
<td>gtsav-dept-pa migration</td>
<td>October 26, 2017</td>
</tr>
</tbody>
</table>
What do I need to do?

• Once we migrate your networks, please check your applications and let us know if you see any issues.

• The firewall team can be contacted at:
  oit-firewall-help@lists.gatech.edu

• Questions?
IAM Admin Tools

NEW SERVICE FOR OIT
IDENTITY ACCESS TEAM
IAM & GT 360: Enablement

GT360: LOOKING FORWARD

GT360
Enterprise IT Strategy
- Integrated
- Engaging
- Intuitive
- Trusted
- Holistic
- Transformative

Five & Five
- Organizational Performance Management
- Transformation Early Wins
- Technology Business Model
- Enterprise Systems & Strategy
- Creating Innovation Capacity
- ...Not sure...

OneIT
- Shared Values
  - Common Methodologies
  - Increased Collaboration
  - Effective Governance
  - Continuous Improvement

Digital Experience Footprint
- Student Information Systems
- Financial Systems
- Human Capital Management
- Learning Management Systems
- Customer Relations Management

!! CREATING THE NEXT !!
Submit IAT Feedback

We would like your feedback to make IAT as useful as possible. Please use this form to create a Footprints ticket reporting any problems or suggestions you have. The ticket will be created in Application Support - Identity Access Management - IAM-General.

Summary

This field can't be blank

Details

Create Ticket
IAT provides a single pane of glass for GT identities

Before: 10+ different consoles!
After: One - https://iat.gatech.edu

Benefits
Holistic view of information, both Cloud & OnPrem

Intuitive/graphical pages replace obscure commands
Continually being improved and extended with more modules
Provides standard APIs for OIT & Campus Innovation
# GT Identity Systems & Tools

- MAGE
- GTED
- DUO
- Office 365
- GRS
- Splunk
- GTAD
- Kerberos
- BuzzApi
- Passport

<table>
<thead>
<tr>
<th>1 Holistic Console</th>
<th>IAM Admin Tools</th>
<th>Intuitive GUI</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MAGE</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GTED</td>
<td></td>
</tr>
<tr>
<td></td>
<td>DUO</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Office 365</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GRS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Splunk</td>
<td></td>
</tr>
<tr>
<td></td>
<td>GTAD</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Kerberos</td>
<td></td>
</tr>
<tr>
<td></td>
<td>BuzzApi</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Passport</td>
<td></td>
</tr>
</tbody>
</table>
Person has administrative permissions within Duo

- Account: /gt/central/services/iam/two-factor/duo-user
  Account is set up in Duo

- Account: /gt/central/services/iam/cas/cas-duo-req-account-prod/enabled
  Account is required to use duo in production cas

**Duo Account**

<table>
<thead>
<tr>
<th>User ID</th>
<th>Last Duo Login</th>
<th>Status</th>
<th>Backup Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>DU60F7BFQ6EK05BXYBNM</td>
<td>7/13/2017 11:36:11</td>
<td>Active</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- Create Backup Codes
- Create Rescue Code
- Delete Account

**Phones**

- JohnSmartPhone (+16789929276)
  Platform: Google Android
  Also owned by: bryson mwbrsson
  - [Activate App](#)
  - [Edit](#)
  - [Remove](#)

- John Bryson Deskphone (+14048946153)
  Platform: Landline
  - [Edit](#)
  - [Remove](#)

- [Add a phone to this account](#)

**Hardware Tokens**

- YubiKey1932155
  Type: YubiKey AES
  Also owned by: bryson mwbrsson
  - [Add a token to this account](#)

**Duo Logs**

- [20 per page](#)
- Start time: [ ]
- End time: [ ]
- [Search](#)

Press the Search button to load logs.
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Source</th>
<th>Error Type</th>
<th>Description</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/13/2017</td>
<td>06:46:41</td>
<td>Passport</td>
<td>Async load error</td>
<td>BuzzAPI error checking async load</td>
<td>143.215.19.141</td>
</tr>
<tr>
<td>7/13/2017</td>
<td>06:46:40</td>
<td>Passport</td>
<td>Async load error</td>
<td>BuzzAPI error checking async load</td>
<td>143.215.19.141</td>
</tr>
<tr>
<td>7/13/2017</td>
<td>06:46:40</td>
<td>Passport</td>
<td>Async load error</td>
<td>BuzzAPI error checking async load</td>
<td>143.215.19.141</td>
</tr>
<tr>
<td>7/13/2017</td>
<td>06:46:40</td>
<td>Passport</td>
<td>Async load error</td>
<td>BuzzAPI error checking async load</td>
<td>143.215.19.141</td>
</tr>
<tr>
<td>7/13/2017</td>
<td>06:46:40</td>
<td>Passport</td>
<td>Async load error</td>
<td>BuzzAPI error checking async load</td>
<td>143.215.19.141</td>
</tr>
<tr>
<td>7/13/2017</td>
<td>06:46:39</td>
<td>Passport</td>
<td>Async load error</td>
<td>BuzzAPI error checking async load</td>
<td>143.215.19.141</td>
</tr>
<tr>
<td>7/13/2017</td>
<td>06:46:40</td>
<td>Passport</td>
<td>Async load error</td>
<td>BuzzAPI error checking async load</td>
<td>143.215.19.141</td>
</tr>
<tr>
<td>7/13/2017</td>
<td>06:46:40</td>
<td>Passport</td>
<td>Async load error</td>
<td>BuzzAPI error checking async load</td>
<td>143.215.19.141</td>
</tr>
<tr>
<td>7/13/2017</td>
<td>06:46:40</td>
<td>Passport</td>
<td>Async load error</td>
<td>BuzzAPI error checking async load</td>
<td>143.215.19.141</td>
</tr>
</tbody>
</table>
IAM: By the Numbers

- Passport Users: 20,000 unique users/month (Self Service IDM)
- Login.gatech Users: 55,000 unique users/month
- Delegated Admin Users: 320 active *(up from 200 earlier in the year)*
- Integrated Applications: 1000-1500
- # People, # Accounts, # Guests: 2.4M / 600,000 / 4,000
- # Duo Accounts: 12,700
General Announcements
Announcements

• **Staff Appreciation Breakfasts**
  - July 19, 7:30am – 9:00am – 811 Marietta
  - July 26, 7:30am – 9:00am – Rich Building

• **OIT Summer Picnic**
  - Lake Lanier Islands
  - Includes Food, Park access
  - July 31 – 10:00am
Questions?