Using External Dynamic List for Live Threat Updates

Zachary Fowler
Bryson Livingston
Advisor: Jorge Crichigno, Ali Alsabeh

Department of Integrated Information Technology
University of South Carolina

April 2021
Agenda

• Introduction
• Problem Description
• Background Information
• Proposed Solution and Implementation
• Conclusion
Introduction

- Next Generation Firewalls (NGFWs) use security policies to block/allow traffic from specified sources and destinations

- Security policies on NGFWs need to frequently updated to protect against new threats

- External Dynamic Lists (EDL) are used to keep security policies up to date
Problem Description

• Using a non-dynamic list of objects in a security policy has multiple issues
  • Does not automatically update to include new threats
  • Policy creator will constantly have to manually update the list to include new threats

• Ultimately leads to a less secure network

• External Dynamic Lists solve both issues
Background Information

- External Dynamic Lists (EDL) are text files stored on an external server
  - The text files are updated frequently to protect from new threats

- Text files contain lists of one of 4 types of EDL
  - IP Address
  - URL
  - Domain
  - Predefined IP Address

- These lists consist of dangerous source and destination objects
  - Used in security policies on NGFW
Proposed Solution and Implementation

- A text file (i.e. list of malicious IP addresses) is hosted on the external server
- NGFW1 uses the text file in a new security policy to block traffic to and from any IP address on the file
- NGFW1 dynamically imports the list at the configured interval and enforces policy without the need to make a configuration change or a commit on the firewall
Proposed Solution and Implementation

<table>
<thead>
<tr>
<th>Name</th>
<th>Tags</th>
<th>Type</th>
<th>Zone</th>
<th>Address</th>
<th>User</th>
<th>IP Profile</th>
<th>Zone</th>
<th>Address</th>
<th>Application</th>
<th>Service</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 IP Block</td>
<td>none</td>
<td>universal</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>IP ECL</td>
<td>application-d....</td>
<td>Deny</td>
</tr>
<tr>
<td>2 any-zone-to-any-zone</td>
<td>none</td>
<td>universal</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>application-d....</td>
<td>Allow</td>
</tr>
<tr>
<td>3 intrzone-default</td>
<td>none</td>
<td>intrzone</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>(intrzone)</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Allow</td>
</tr>
<tr>
<td>4 interzone-default</td>
<td>none</td>
<td>interzone</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>any</td>
<td>Deny</td>
</tr>
</tbody>
</table>

- Security Policy #1 uses the IP EDL in the address column to deny traffic to any IP address on the EDL.
Conclusion

• With the use of External Dynamic Lists in security policies, users can more easily protect their networks from dangerous sources by using frequently updated object lists
• The possibility of an attack from a dangerous source significantly decreases with the use of EDLs