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

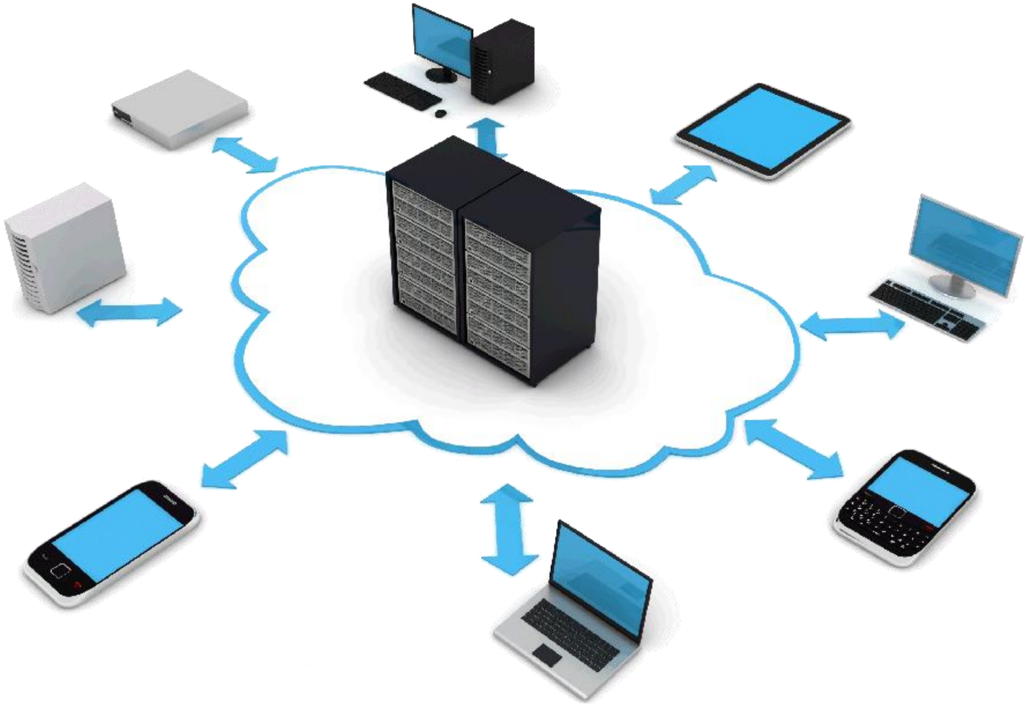
- External Dynamic Lists (EDL) are used to keep security policies up to date

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

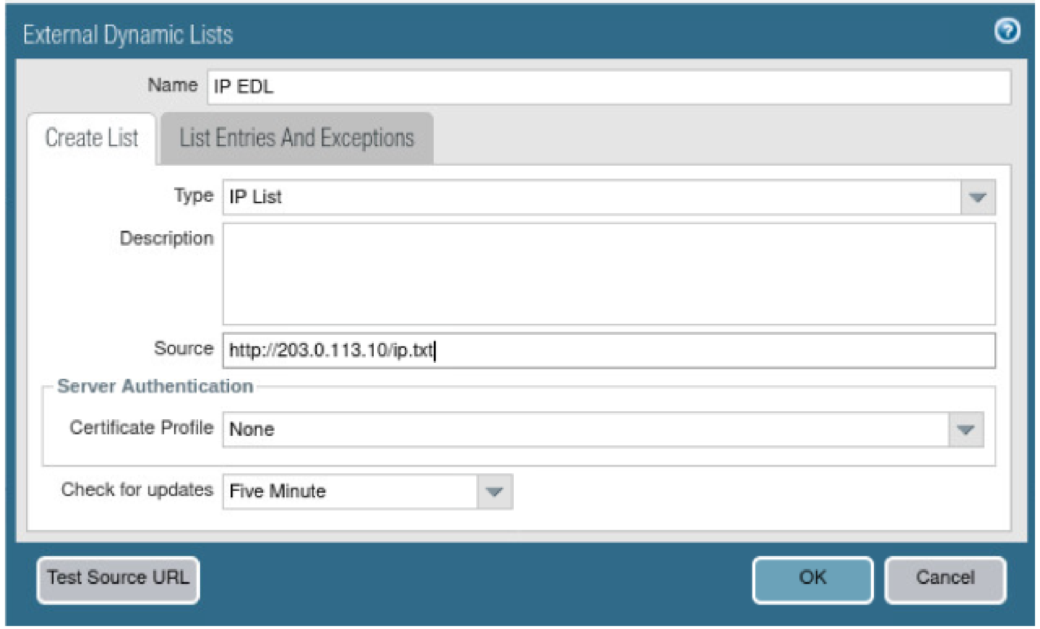


Background Information

- 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


External Dynamic Lists

Name: IP EDL

Type: IP List

Description:

Source: http://203.0.113.10/ip.txt

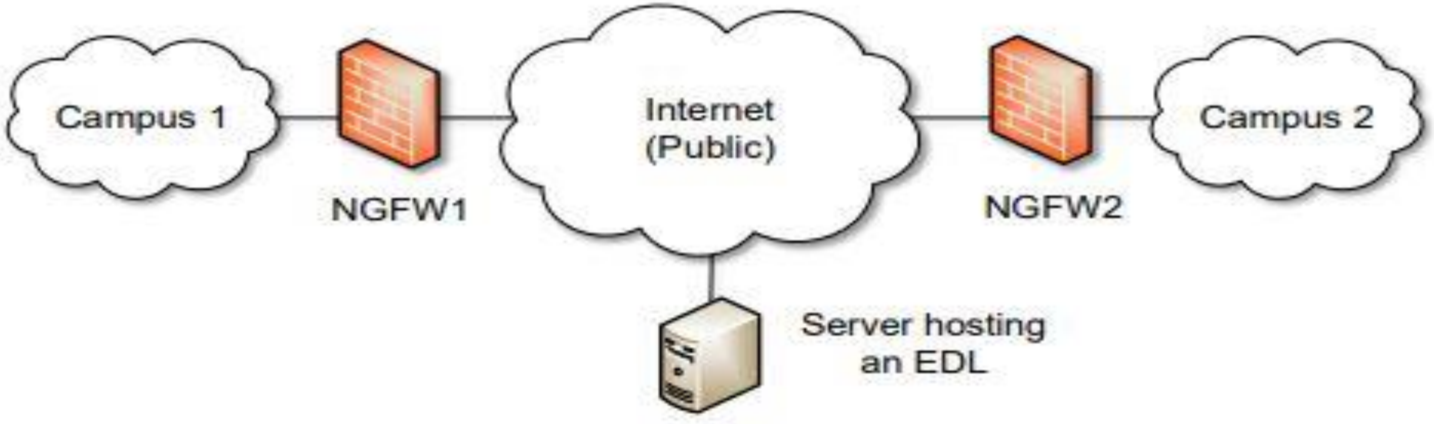
Server Authentication

Certificate Profile: None

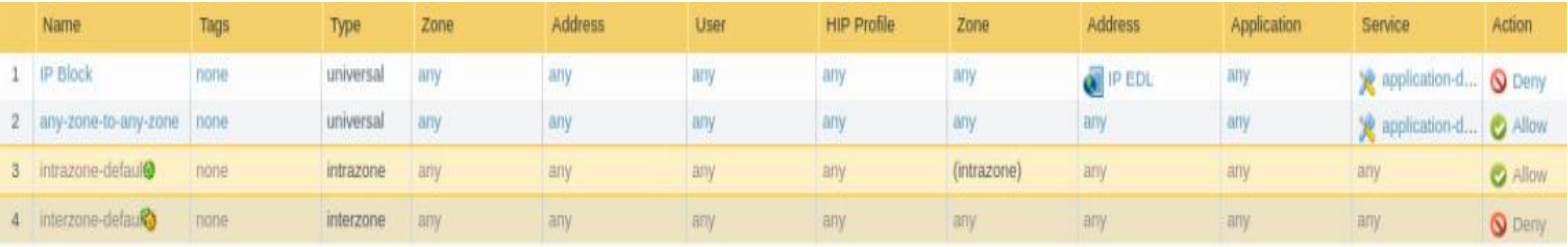
Check for updates: Five Minute

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



	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action
1	IP Block	none	universal	any	any	any	any	any	IP EDL	any	application-d...	Deny
2	any-zone-to-any-zone	none	universal	any	any	any	any	any	any	any	application-d...	Allow
3	intrazone-defaul	none	intrazone	any	any	any	any	(intrazone)	any	any	any	Allow
4	interzone-defaul	none	interzone	any	any	any	any	any	any	any	any	Deny

- 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