Using External Dynamic List for Live Threat Updates

David Williams
Tucker Baron
Advisors: Jorge Crichigno, Ali Alsabeh

Department of Integrated Information Technology
University of South Carolina

April 2022

Agenda

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

Introduction

- Next Generation Palo Alto Firewalls use security policies to monitor and block traffic from specific sources and destinations
- New threats are discovered every day so the firewall needs to be updated regularly
- External Dynamic Lists 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 and harder to manage network
- External Dynamic Lists make it easy to update the policy

Background Information

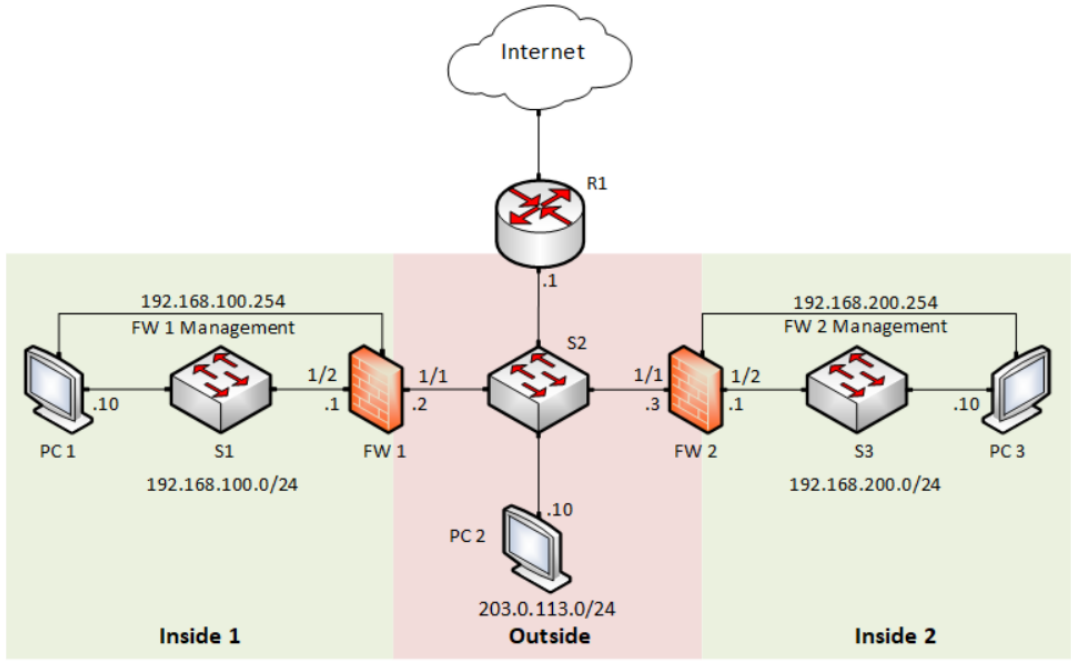
- External Dynamic Lists (EDL) are text files stored on an external server

- There are 3 types of External Dynamic Lists (EDL)
  - IP Address
  - URL
  - Domain

- These lists consist of entries for items that need to blocked
  - Used in security policies on the Firewall

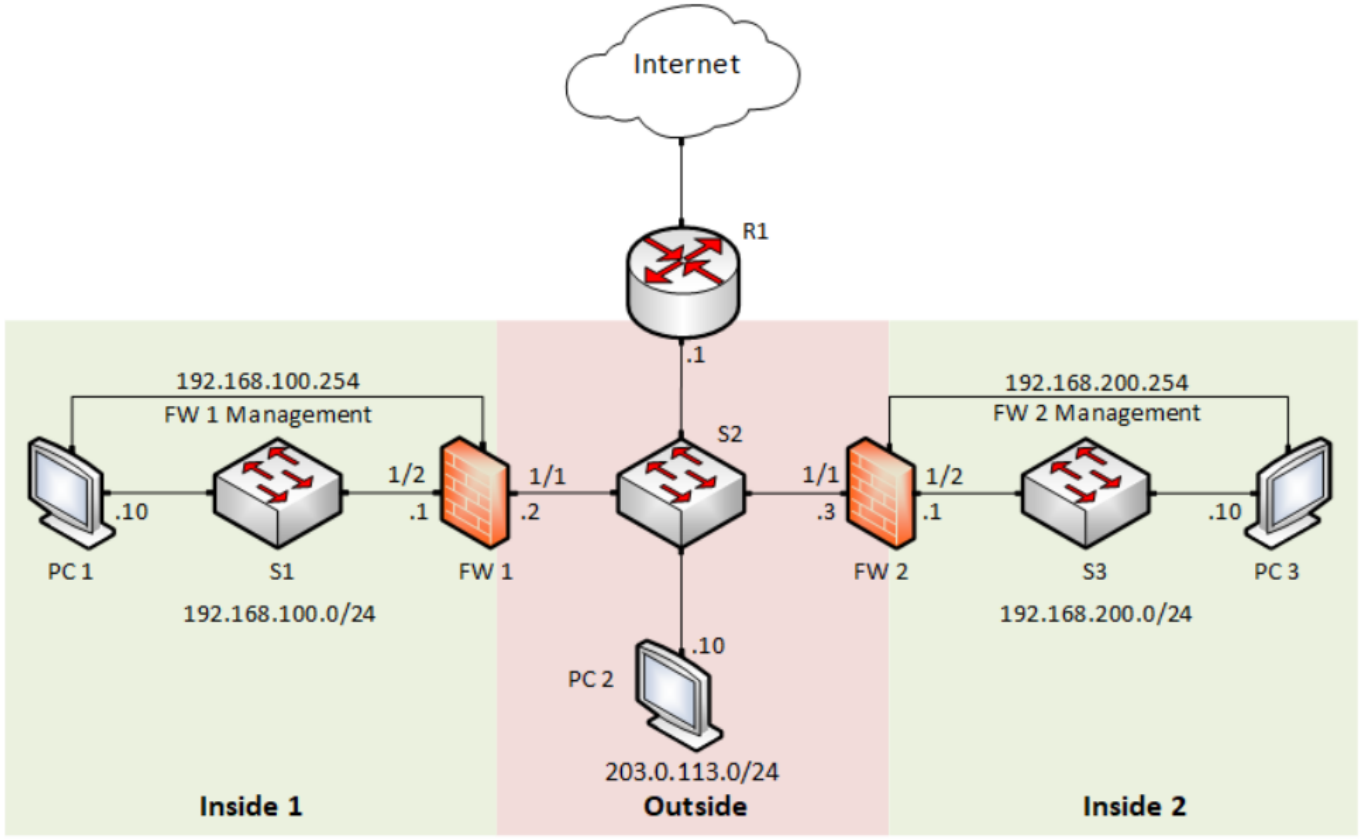
Proposed Solution and Implementation

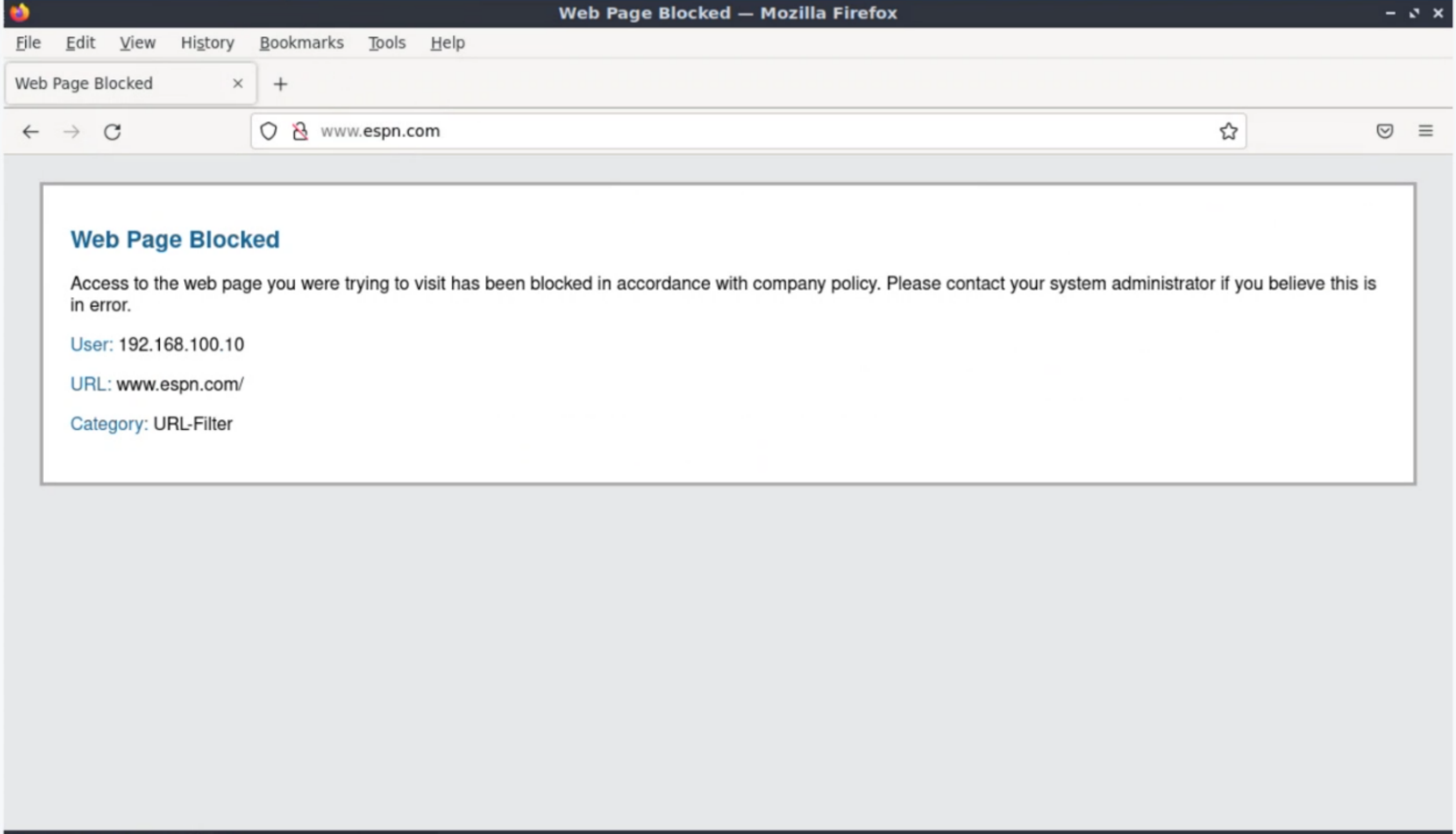
- A text file (i.e. list of IP addresses, Domains or URLs we want to block) is hosted on the external server
- FW1 uses the text file in a new security policy to block traffic to and from any IP address, Domain or URL on the file
- FW 1 will regularly update without having to commit any changes



Proposed Solution and Implementation

- Configure a security policy that targets the items on the External dynamic list
- Set it to block or monitor based on you needs




Web Page Blocked — Mozilla Firefox
File Edit View History Bookmarks Tools Help
Web Page Blocked
www.espn.com
Web Page Blocked
Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.
User: 192.168.100.10
URL: www.espn.com/
Category: URL-Filter

Conclusion

- Using External Dynamic Lists in security policies, users can easily block and monitor certain IP address, Domain or URL
- External Dynamic Lists are an easy way to keep an updated security policy
- These lists can be used used to both block and monitor both harmful sources as well as sources that might be time wasters, such as social media