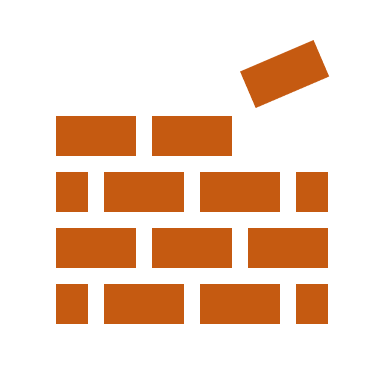
# External Dynamic Lists

# 

# harsha Bhat

# CybersecUrity P5

# Mr. Mason

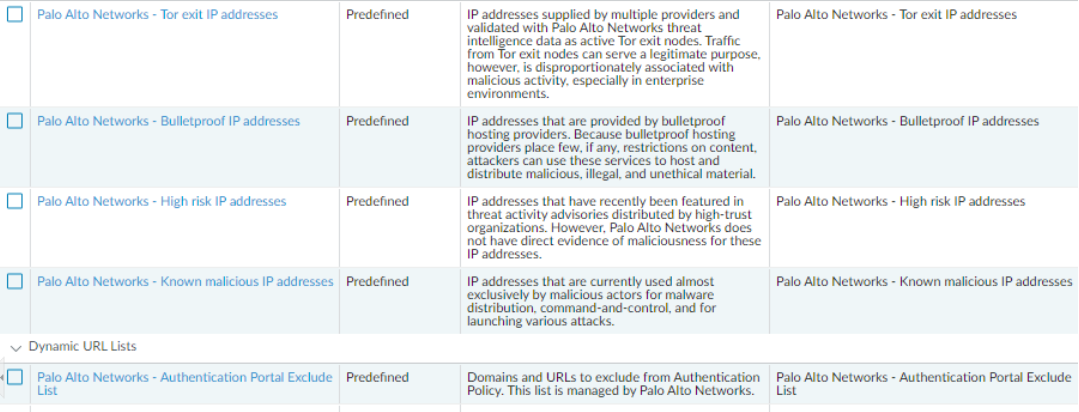


The purpose of this lab is to configure a Palo Alto networks firewall to block a custom list of potentially malicious IPs from online.

### Background Information

While URL Filtering prevents users from accessing malicious websites when connected to the network, threat actors can still distribute malicious information from or launch attacks on the network from IP addresses. The various users of the internet have wizened up to what IPs are malicious and compiled several text file lists containing the IPs they have encountered, readily available on external web servers. When firewalls are configured to use these External Dynamic Lists, traffic to the malicious IPs specified in the lists is blocked, a custom, simple, yet effective anti-spyware solution. Along with IPs, URLs and domains can be blocked, providing a way to block sites that bypass URL filtering.

Palo Alto provides 4 IP lists and 1 URL list built-in to their latest firewalls:



When you enable telemetry on your firewall, configurations you make and issues/threats you encounter contribute to Palto Alto’s “threat intelligence”, a community resource. While popular lists such as panwdbl appsot (SpamHaus DROP) and Abuse.ch’s Ransomware Tracker (SSL Abuse)\* might be discontinued, some of the information from those lists has wound up in the built-in lists thanks to threat intelligence. Moreover, if/when a malicious IP escaped any of those lists and attacked a Palo Alto system with telemetry enabled, your system would identify it as malicious as well. It’s their system’s loss but your system’s gain!

\* It appears only Abuse.ch C&C, Spyeye, and Palevo lists are missing, while SpamHaus is still there.

However, these lists don’t do anything unless you tell them to: you can configure policy to block them directly or create a new list that uses them as a source. The latter method also allows you unblock entries that would usually be blocked.

On the PA-220, only 50,000 of each threat (IPs, domains, URLs) can be blocked for one firewall (not one list). Some Palo Alto models can handle up to 4,000,000 (e.g., for domain names), and lists have no limit size. You can prioritize different lists and policies (done by dragging them above the others in the GUI) so that the important ones come into effect first and aren’t cut off by the policy limits.

### Lab Summary

I got the idea to do this lab from looking at guides from Eric Ooi, whose site was a big help for the GlobalProtect Lab, and now this lab.

First, I defined the list. Several of the lists Ooi recommended were no longer usable, so I chose the only one that was. After creating the list, I did not verify it immediately – this was the “unimportant” half of this lab.

Graphical user interface, text, application, email

Description automatically generated

Next, I created a policy,

Graphical user interface, application

Description automatically generated

then set source and destination zones, making sure to select the list.

Graphical user interface, text, application, email

Description automatically generated Graphical user interface, text, application

Description automatically generated

For the list to function, I had to set a deny rule:

Graphical user interface, application

Description automatically generated

I dragged the policy above the rest so it would be prioritized first (note it’s labeled “1” here, meaning it is on top of the rest). Since I was only using one list, I wasn’t worried about dragging the other lists.



To test the configuration, I tried to connect to a random IP displayed in the list and found that the policy worked.

Graphical user interface, application, Word

Description automatically generated

On a host device in the CCNP network but under another Cybersecurity student’s firewall, I visited the same IP, and although a connection was not established, the IP was not blocked.

Problems

There were no problems at all during this lab, it was rather short, less than 20 minutes from start to finish. As such, I will elaborate on issues with the current configuration, potential issues one could run into, and what I could have done differently.

The primary issue with the list is that is can be bypassed via IP spoofing. Even if using a malicious IP address, the attacker changes their source IP address in the packet header to a safe, even a private IP address. I took great care to make sure no private IP addresses were blocked by the list I chose as I occasionally remote into servers with private IPs, so my devices would be vulnerable to this flaw.

I can think of 2 solutions to IP spoofing:

* Change the list setup so that it would be a list of safe IPs, and it would be “allow” instead of deny. There might be a different setting for this, an IP access control list.
* Use GlobalProtect on the Firewall: GlobalProtect comes with IPSec, which requires mutual authentication, and the attack would have to reveal their IP address. At the time of this lab, GlobalProtect was operational but running into some connection issues.

I think I could have done more with this lab, in adding domain and URL lists (also a somewhat different option for MAC addresses) instead of just IP lists, and testing other lists, such as the Palo Alto built-in lists. After the conclusion of the Policy Based Routing Lab, I might repurpose one of our Apache Web servers to have my own custom list of IPs to be blocked, and give it another go.

### Conclusion

The EDL Lab was a nice exercise in lab brevity, continuing the trend exponentially from the GlobalProtect Lab. However, the concepts in this lab were very basic, an evolutionary step down from the complex VPN configuration of the latter, not to mention the troublesome VM attributes of RADIUS/TACACS+ and PBR.