7 - Blocking Threats from Known-Bad Sources

7.2 Test Access to Known Malicious IP Addresses
You can use security policy rules to block access to known malicious IP addresses. Because the list of malicious IP addresses can quickly change, you will treat two legitimate IP addresses as though they are malicious and block access to them.

1. On the client desktop, open a terminal window by double-clicking Terminal Emulator.
2. Enter the command below to obtain the IP Address of 2600.org. Write down the IP address or copy and paste it into a text document on the desktop.
    1. `nslookup 2600.org`
3. In the same CMD window, enter the command below. Write down the IP address or copy and paste it into a text document on the desktop.
    1. `nslookup www.breakthesecurity.com`
4. In the same CMD window, verify connectivity to the websites by entering the commands below.
    1. `ping 2600.org
    2. `ping www.breakthesecurity.com
5. Minimize the Terminal window by clicking the minimize icon in the upper-right.
    - Here, pinging 2600.org and breakthesecurity.com will be successful. Access will be blocked in the next tasks.
6. `Objects > Addresses> Add.`
7. In the Address window, configure the following. Click OK.
    - Parameter Value

        - Name: `malicious-ip-address-1`
        - Description: `2600.org IP address`
        - Type IP: `Netmask`
        - (address text box) `<IP_address_of_2600.org>`
8. In the Addresses window, click Add.
9. In the Address window, configure the following. Click Resolve.
    - Parameter Value
        - Name `malicious-fqdn-1`
        - Description: `www.breakthesecurity.com`
        - Type: `FQDN`
        - (FQDN text box) `www.breakthesecurity.com`
10. Once you click Resolve, you will be prompted to select Use this Address.
11. In the Address window, click OK.
12. Confirm the address objects appear in the Addresses window.
13. `Select Policies > Security > Add` to create a new security policy rule.
14. In the Security Policy Rule window, on the General tab, type Block-Known-Bad-IPs as the Name. For Description, enter Blocks traffic to malicious address objects.
15. Click the Source tab and configure the following.
    `Source Zone Add Users_Net and Extranet` Source Address Any`
16. Click the Destination tab and configure the following.
    - Parameter Value
        - Destination Zone Add Internet
        - Destination Address Add malicious-fqdn-1 and malicious-ip-address-1
17. Click the Application tab and verify that Any is selected.
18. Click the Service/URL Category tab and verify that application-default and Any are selected.

19. Click the Actions tab and configure the following. Click OK.
    - Parameter Value
        - Action Deny
        - Log Setting Log at Session End
20. Select, but do not open, the Block-Known-Bad-IPs rule in the security policy.
21. At the bottom of the window, select Move > Move Top to move the rule to the top of the security policy.
22. Verify that the Block-Known-Bad-IPs rule is rule number 1.
23. Click the Commit button at the upper-right of the web interface.
24. In the Commit window, click Commit.
25. Wait until the Commit process is complete. Click Close.
26. Minimize the Chromium browser by clicking the minimize icon and continue to the next task.
27. Return to the terminal window by clicking on the Terminal icon in the taskbar of your client desktop.
28. From the terminal window on the desktop, enter the following commands. Use Ctrl+C to stop the ping for the two commands after a few seconds.

    ```
    ping 2600.org <Enter>
    ```

    ```
    ping www.breakthesecurity.com <Enter>
    ```
29. Minimize the Terminal window by clicking the minimize icon in the upper-right.
30. If you minimized the firewall, reopen the firewall interface by clicking on the Chromium tab in the taskbar. Leave the firewall interface open and continue to the next task.
31. Pinging 2600.org will fail.
32. Pinging www.breakthesecurity will fail because access to the IP addresses was blocked by the Address objects in the Security policy.

33. Navigate to Monitor > Logs > Traffic. Enter the filter (action eq deny) in the Filter builder to look for traffic that has been denied. You should see entries indicating that your Block-Known-Bad-IPs security policy rule has denied traffic to each host.
34. Leave the Palo Alto Networks Firewall open and continue to the next task.

7.4 Block Access to Malicious IP Addresses Using Address Groups

You can use Address Groups in security policy rules to control access to IP addresses.

1. In the firewall interface, select Objects > Address Groups. Click Add.
2. In the Address Group window, configure the following. Click OK.
   Parameter Value
   Name Malicious-IP-Group
   Description Contains malicious IP address objects
   Type Static
   Addresses Add malicious-fqdn-1 and malicious-ip-address-1
3. Select Policies > Security. Click Block-Known-Bad-IPs to edit the rule.
4. In the Security Policy Rule window, Destination tab, select the `malicious-fqdn-1` and `malicious-ip-address-1` checkboxes. Click Delete.
5. In the Destination Address window, click Add. Select Malicious-IP-Group. Click OK.
6. Click the Commit button at the upper-right of the web interface.
7. In the Commit window, click Commit.
8. Wait until the Commit process is complete. Click Close.
9. Minimize the Chromium browser by clicking the minimize icon and continue to the next task.
10. Return to the terminal window by clicking on the terminal icon in the taskbar of your client desktop.

11. From the terminal window on the desktop, enter the commands below. Use Ctrl+C to stop the ping for the two commands after a few seconds.
    - `ping 2600.org` Pinging 2600.org will fail.
12. Minimize the Terminal window by clicking the minimize icon in the upper-right.
13. If you minimized the firewall, reopen the firewall interface by clicking on the Chromium tab in the taskbar. Leave the firewall interface open and continue to the next task.
14. Navigate to Monitor > Logs > Traffic. Enter the filter (action eq deny) in the filter builder to look for traffic that has been denied. You should see additional entries indicating that your Block□Known-Bad-IPs security policy rule has denied traffic to each host.
15. Leave the Palo Alto Networks Firewall open and continue to the next task. Pinging www.breakthesecurity will fail because access to the IP addresses was blocked by the address objects in the security policy.

7.6 Block Access to Malicious IP Addresses Using EDLs

You can add a list of malicious IP addresses to a file on an external web server and configure the firewall to access the list as an EDL. The advantage of this approach is that the malicious IP address list an be regularly updated without the need to recommit the firewall configuration, as you would have
to do if you updated an Address object or Address Group. EDLs simplify the maintenance of a current list of IP addresses.

1. In the firewall interface, select Objects > External Dynamic Lists. Note the three predefined EDLs contain known malicious and high-risk IP address lists. Click Palo Alto Networks – High risk IP addresses.
2. Read the description of the list.
3. Click the List Entries And Exceptions tab. Write down three IP addresses on the current list of IP addresses. You will try to ping these addresses later in this lab exercise. Click Cancel.

4. At the bottom of the External Dynamic Lists window, click Add.

For this step, we chose the first three IP Addresses on the list. You may choose any IP Addresses you would like however, it is important to write down the IP Address to complete this task.
Note that you can also copy and paste these addresses into a text file on the client desktop.

5. In the External Dynamic Lists window, create another EDL and configure the following. Click Test Source URL.
   Parameter Value
   Name custom-malicious-ips-edl
   Type IP List
   Description Contains manually entered IP address list on web server.
   Source http://192.168.50.80/malicious-ips.txt
   (The EDL contains only the IP address 192.168.50.11.)
   Check for updates Five Minute
6. The firewall should present a Test Source URL window indicating that it can access the URL. Click Close.
7. Click OK in the External Dynamic Lists window.
8. Update the security policy to include External Dynamic Lists. Navigate to Policies > Security. Click Block-Known-Bad-IPs to edit the rule.
9. Click the Destination tab and configure the following. Click OK.
   Parameter Value
   Destination Zone Internet
   Destination Address Add the following to the list:
   Palo Alto Networks – Bulletproof IP addresses
   Palo Alto Networks – High risk IP addresses
   Palo Alto Networks – Known malicious IP addresses
10. Click Users_to_Extranet to edit the rule.
    The “Block-Known-Bad-IPs” rule now is configured to block access to

the three IP addresses you wrote down in lab Step 3.

11. In the Security Policy Rule window, click the Destination tab and configure the following. Click OK.
    Parameter Value
    Destination Zone Extranet
    Destination Address custom-malicious-ips-edl
    Negate Select check box
12. Notice in the Users_to_Extranet rule that custom-malicious-ips-edl has a line through it. This line indicates that the Negate option has been employed for addresses in the list.
13. Click the Commit button at the upper-right of the web interface.

The malicious-ips-edl EDL contains the IP address of a host in the Extranet zone (192.168.50.11). When the destination address is used in conjunction with the Negate option, the rule matches and allows any address in the Extranet zone except the address listed in the EDL.

14. In the Commit window, click Commit.
15. Wait until the Commit process is complete. Click Close.
16. Return to the terminal window by clicking on the Terminal icon in the taskbar of your client desktop.
17. From the terminal window on the desktop, ping an address on the internet by issuing the following command.
    - `ping 192.168.50.11`
18. After a few seconds, use Ctrl+C to stop the connection because it will not succeed.
19. From the terminal window, use ping again, but this time try one of the three IP addresses that you wrote down earlier in lab step 3.
    The ping should fail because the IP address is listed in the custom EDL.
    These IP addresses were in one of the EDLs predefined by Palo Alto Networks.

20. Minimize the Terminal window open on the client because you will perform this same task in a later step.
21. Examine the traffic log again and use a simple filter to see if there are any entries for this session that failed. Navigate to Monitor > Logs > Traffic. In the filter field, enter (action neq allow) and (app eq ping). Click the Apply Filter button in the upper-right corner of the window. You will notice the firewall is now logging entries matching your filter.

Note that ping to 192.168.50.11 hit the interzone-default rule and not the Users_to_Extranet rule. The Users_to_Extranet rule is set to allow traffic (with the exception of the IP address 192.168.50.11). Traffic to the 192.168.50.11 address does not match the rule because of the negate setting you applied in the Destination Address section. However, that traffic does match the interzone-default rule which denies traffic.

24. In the firewall web interface, select Policies > Security. Click Users_to_Extranet to edit the rule.
25. In the Security Policy Rule window, click the Destination tab and configure the following. Click OK.
    Parameter Value
    Destination Zone Extranet
    Destination Address Delete custom-malicious-ips-edl
    Negate check box Deselect it
26. Click the Commit button at the upper-right of the web interface.
27. In the Commit window, click Commit.
28. Wait until the Commit process is complete. Click Close.
29. Leave the web interface open and continue to the next task.

7.7 Block Access to Malicious Domains Using an EDL

You can add a list of malicious domains to a file on an external web server and then configure the firewall to access the list as an EDL. The advantage of this approach is that the malicious domain list can be updated regularly

without the need to recommit the firewall configuration. In this section, you will block access to malicious domains using an External Dynamic List.

1. In the PA-VM firewall web interface, navigate to Objects > External Dynamic Lists. Click Add at the bottom of the window.
2. In the External Dynamic Lists window, configure the following. Click OK.
   Parameter Value
   Name malicious-domains-edl
   Type Domain List
   Source http://192.168.50.80/malicious-domains.txt
   (The EDL contains the domains quora.com and producthunt.com.)
   Automatically expand to include subdomains
   Check for updates Five Minute
3. Click to reopen the malicious-domains-edl.
   - This EDL will be used to block access to the quora.com and producthunt.com domains.
4. In the External Dynamic Lists window, click Test Source URL.
5. The firewall should present a Test Source URL window indicating that it can access the URL. Click Close.
6. Click OK in the External Dynamic Lists window.
7. Leave the firewall open and continue to the next task.

7.8 Add the Domain List EDL to an Anti-Spyware Profile
You can add an EDL containing a domain list to an Anti-Spyware Profile to block access to malicious domains. You must attach the Anti-Spyware Profile to a security policy rule that allows network access. Although the security policy rule might allow the traffic, the attached Anti-Spyware Profile will block
access to any domains listed in the EDL. In this section, you will add a domain list EDL to an anti-spyware profile.

1. In the web interface, select Objects > Security Profiles > Anti-Spyware. Select the checkbox next to the strict Anti-Spyware Profile. Click Clone.
2. In the Clone window, click OK.
3. A new strict-1 Anti-Spyware Profile should have been created. Click strict-1 to edit the profile.
4. Rename the profile outbound-as. Click the DNS Policies tab. Under the External Dynamic Lists section, change the Policy Action dropdown list to block. Click OK.
5. Leave the firewall open and continue to the next task.

7.9 Add the Anti-Spyware Profile to a Security Policy Rule

In this section, you will add the outbound-as Anti-Spyware Profile to the security policy. The configuration of the profile will enable the firewall to use malicious domain signatures to block access to malicious domains.

1. In the web interface, navigate to Policies > Security. Click Users_to_Internet to edit the rule.

Palo Alto Networks typically recommends the “sinkhole” action, which will be discussed and used in another lab exercise.

2. In the Security Policy Rule window, configure the following on the Actions tab. Click OK.
   Parameter Value
   Profile Type Profiles
   Anti-Spyware outbound-as
3. Click the Commit button at the upper-right of the web interface.
4. In the Commit window, click Commit.
5. Wait until the Commit process is complete. Click Close.
6. Minimize the Chromium browser by clicking the minimize icon.
7. Return to the terminal window by clicking on the terminal icon in the taskbar of your client desktop.

8. From the terminal window on the desktop, ping two addresses on the internet by issuing the
   following commands. Use Ctrl+C to stop the ping for the two commands after a few seconds.
   `ping quora.com` ping producthunt.com `
9. Minimize the Terminal window.
10. If you minimized the firewall, reopen the firewall interface by clicking on the Chromium tab in the taskbar.
11. Examine the firewall traffic log by ensuring you are at Monitor > Logs > Threat. Clear any filters in filter builder. You should see several entries indicating that the firewall has blocked DNS queries for the hosts listed in the malicious-domains-edl.

The ping commands should fail because the domains are listed in the custom EDL and the custom EDL was added to the outbound-as Anti□Spyware Profile and configured with the “block” action.

12. Minimize the Chromium browser by clicking the minimize icon and continue to the next task.

7.10 Block Access to Malicious URLs Using the Security Policy

In this section, you will block access to known-malicious URLs by configuring the firewall’s URL Filtering feature. You will add URL categories to a security policy rule configured to block traffic.

1. On the client desktop, double-click the folder for Class-Scripts.
2. Open the EDU-210 folder.

Although you can configure the security policy to control access to URLs, the URL Filtering Profile more commonly is used to configure the action that a firewall should take when it detects a URL.

3. Double-click the icon for Clear Firewall Logs.
4. Press Enter to start the Clear Firewall Logs script. Allow the script to complete. Once the Clear Firewall Logs script completes, press Enter.
5. If you minimized the firewall, reopen the firewall interface by clicking on the Chromium tab in the taskbar.

This script uses the XML API to clear the Threat, Traffic and URL Filtering log files. We are clearing the log files to make it easier to identify traffic and threats blocked by DoS Protection.

6. Open a new tab in Chromium.
7. Type hacker9.com which belongs to the URL category hacking in the address bar, and press Enter.
8. Close the hacker9.com tab by clicking the X icon.
9. In the web interface, select Policies > Security. If the URL Category column is not displayed, click the down-arrow menu that appears next to any column header (hover your pointer over a header to see the down-arrow) and select Columns > URL Category.
10. In the Security Policies window, click Add to create a new security policy rule.
11. In the Security Policy Rule window, on the General tab, type block-known-bad-urls as the Name. For Description, enter Blocks bad URL categories.
12. Click the Source tab and for the Source Zone, select Users_Net.
13. Click the Destination tab, and for the Destination Zone, select Internet.
14. Click the Application tab and verify that Any is selected.
15. Click the Service/URL Category tab and configure the following.
    Parameter Value
    Service application-default
    URL Category Add the following:
    adult

command-and-control
extremism
hacking
high-risk
malware
nudity
parked
peer-to-peer
phishing
proxy-avoidance-and-anonymizers
questionable

16. Click the Actions tab and for the action, select Deny. Verify Log at Session End is checked. Click OK.
17. Select, but do not open, the block-known-bad-urls rule in the security policy. Select Move > Move Top to move the block-known-bad-urls rule to the top of the security policy.
18. Click the Commit button at the upper-right of the web interface.
19. In the Commit window, click Commit.
20. Wait until the Commit process is complete. Click Close.
21. Open a new tab in Chromium.
22. Type hacker9.com which belongs to the URL category hacking in the address bar, and press Enter.
23. Close the hacker9.com tab by clicking the X icon.

The browser should display an error message similar to the following example because the URL category hacking is blocked in the security policy. If you get a browser window, it was likely a version cached locally by the browser. Refresh the browser window and access should be blocked.

24. In the web interface, select Monitor > Logs > URL Filtering. If the URL Category List column is not displayed, click the down-arrow menu that

appears next to any column header (hover your pointer over a header to see the down-arrow) and select Columns > URL Category List.

25. Leave the firewall open and continue to the next task.

7.11 Create a Custom URL Category

In this section, you will add your Custom URL Category to a security policy rule that has a “deny” action.

1. Open a new tab in Chromium.
2. Type www.nbcnews.com and press Enter. The browser should display a valid webpage.

You should see multiple entries that have been blocked. Several default columns have been hidden in the example URL Filtering log file shown here.

3. Close the nbcnews.com tab by clicking the X icon.
4. In the web interface, select Objects > Custom Objects > URL Category. Click Add.
5. In the Custom URL Category window, configure the following. Click OK.
   Parameter Value
   Name block-per-company-policy
   Description URLs that are blocked by company policy.
   Sites Add the following:
   .nbcnews.com
   .theguardian.com
6. Confirm the block-per-company-policy Custom URL is showing in the URL Category window.
7. Add your Custom URL Category to a security policy rule that has a deny action. Select Policies > Security. Click block-known-bad-urls to edit the rule.
8. Select the Service/URL Category tab and click Add. Add block-per-company-policy to the list. Click OK.

9. Click the Commit button at the upper-right of the web interface.
10. In the Commit window, click Commit.
11. Wait until the Commit process is complete. Click Close.
12. Test access to URLs that belong to the Custom URL Category that you added to a security policy deny rule. Open two new tabs in Chromium.
13. Type www.nbcnews.com on the first tab and press Enter. Type www.theguardian.com on the second tab and press Enter.
14. Close the nbcnews and theguardian tabs by clicking the X icon.

The browser should display an error message because the Custom URL Category in the security policy blocks access to the webpage.

15. In the web interface, select Monitor > Logs > URL Filtering. If the URL Category column is not displayed, click the down-arrow menu that appears next to any column header (hover your pointer over a header to see the down-arrow) and select Columns > URL Category.
16. Leave the firewall open and continue to the next task.

7.12 Create an EDL to Block Malicious URL Access

You can add a list of malicious URLs to a file on an external web server and then configure the firewall to access the list as an EDL. The advantage of this approach is that you can regularly update the malicious URL list without the need to recommit the firewall configuration each time, as you would have to do if you updated a security policy rule with a new URL.

In this section, you will create an EDL to block malicious URL access.

1. In the web interface, select Objects > External Dynamic Lists. Click Add.
2. In the External Dynamic Lists window, configure the following. Click OK.

   Parameter Value

   Name malicious-urls-edl

   Type URL List

Source http://192.168.50.80/malicious-urls.txt
(The EDL contains only the URL www.popurls.com)
Check for updates Five Minute

3. In the External Dynamic Lists window, click malicious-urls-edl.
The malicious-urls.txt file contains an entry for popurls.com.
4. Click Test Source URL and verify the firewall can access the EDL URL.
5. In the Test Source URL window, verify the Source URL is accessible. Click Close.
6. In the External Dynamic List window, click OK.
7. Add the EDL containing the malicious URL list to a security policy rule with a deny action. In the web interface, select Policies > Security. Click block-known-bad-urls to edit the rule.
8. In the Security Policy Rule window, click the Service/URL Category tab. Add malicious-urls-edl to the list. Click OK.
9. Click the Commit button at the upper-right of the web interface.
10. In the Commit window, click Commit.
11. Wait until the Commit process is complete. Click Close.
12. Test access to a URL contained in the EDL that you added to the block-known-bad-urls security policy. Open a new tab in Chromium.
13. Type http://www.popurls.com in the address bar.
14. The browser displays a block page because the EDL in the security policy blocks access to the popurls.com webpage.
15. Close the popurls.com tab by clicking the X icon.
16. In the web interface, select Monitor > Logs > URL Filtering. Type (action eq block-url) in the filter builder. You should see multiple entries for sessions to www.popurls.com that the firewall has blocked.
17. Leave the firewall open and continue to the next task.

7.13 Block Access to a Malicious URL Using a URL Filtering Profile

Now you will configure a URL Filtering Profile to control access to URLs. You must add the URL Filtering Profile to a security policy rule with an “allow”

action. The use of a URL Filtering Profile to block access to URLs typically is easier to maintain over time compared to the addition of URLs to a security policy block rule.

1. In the web interface, select Device > Response Pages. Locate the entry for Application Block Page and click the link for Disabled under the Action column.
2. In the Application Block Page window, place a check in the box for Enable Application Block Page. Click OK.
3. Click the Commit button at the upper-right of the web interface.
4. In the Commit window, click Commit.
5. Wait until the Commit process is complete. Click Close.
6. Test the Application Block Page response. Open a new tab in Chromium.
7. Type www.evilzone.org in the address bar, press Enter.
8. The browser displays a block page because the EDL in the security policy blocks access to the evilzone.org webpage.
9. Close the evilzone.org tab by clicking the X icon.

The browser should display a block page because the URL belongs to the URL category hacking, which is blocked by a security policy rule. You will continue to block access to this website but will use another method.

10. In the web interface, select Objects > Security Profiles > URL Filtering. Click Add to create a new profile.
11. In the URL Filtering Profile, type Corp-URL-Profile as the Name of the profile. For Description, enter Company URL Filtering profile.
12. On the Categories tab, configure the following. You will need to scroll through each Category for the value to set it to block the site access.

Parameter Value
Site Access Configure the block action for the following URL categories:

block-per-company-policy* (your Custom URL Category) malicious-urls-edl+ (your custom URL list)
adult
command-and-control
extremism
hacking
high-risk
malware
nudity
parked
peer-to-peer
phishing
proxy-avoidance-and-anonymizers
questionable

13. Select the tab for Inline ML. For Phishing Detection and Javascript Exploit Detection, set the Policy Action to block. Click OK.
14. In the web interface, select Policies > Security. Click Users_to_Internet to edit the rule.
15. In the Security Policy Rule window, click the Actions tab and configure the following. Click OK.
Parameter Value
Action Allow
Log Setting Log at Session End
Profile Type Profiles
URL Filtering Corp-URL-Profile
16. Select, but do not open the block-known-bad-urls security policy rule. Click Delete to remove the block-known-bad-urls rule.

This rule no longer will be used to block access to the URLs. Instead, the “Users_to_Internet” rule with its attached URL Filtering Profile will control URL access.

17. In the Security Rule window, click Yes to confirm the deletion.
18. Click the Commit button at the upper-right of the web interface.
19. In the Commit window, click Commit.
20. Wait until the Commit process is complete. Click Close.
21. Test the Application Block Page response. Open a new tab in Chromium.
22. Type www.evilzone.org and press Enter.
23. The browser displays a block page because the EDL in the security policy blocks access to the evilzone.org webpage. If the Web Page Blocked message does not appear, allow 1 to 3 minutes for the firewall to process the changes, then refresh the evilzone.org tab.

The browser should display a block page because the URL belongs to the URL category hacking, which is blocked by a security policy rule. You will continue to block access to this website but will use another method.

24. Close the evilzone.com tab by clicking the X icon.
25. Examine the URL Filtering Log under Monitor > Logs > URL Filtering.
26. The lab is now complete; you may end your reservation.