DEPLOYMENT GUIDE

Implementing TIDE Feeds into Palo Alto Networks Firewalls

Table of Contents

Introduction

Infoblox Threat Intelligence Data Exchange (TIDE) leverages highly accurate machine-readable threat intelligence (MRTI) data to aggregate and selectively distribute data across a broad range of security infrastructure. The threat intelligence team curates, normalizes, and refines the high quality threat data to minimize false positives. Our threat feeds begin with information gained from native investigations and harvesting techniques. We then combine them with verified and observed data from trusted partners including government agencies, academics, several premier Internet infrastructure providers, and law enforcement. The end result is a highly refined feed with a very low historical false-positive rate.

This deployment guide shows how to incorporate the feeds into a Palo Alto Networks Firewall.

Infoblox Threat Intelligence Data Exchange Feeds

Infoblox provides the following feeds from the BloxOne Threat Defense website:

- IP list - this is a list of IP addresses that have been found to be malicious.
- Domain list – this is a list of domains that have been found to be malicious.
- URL list – this is a list of URLs that have been found to be malicious.

Requirements

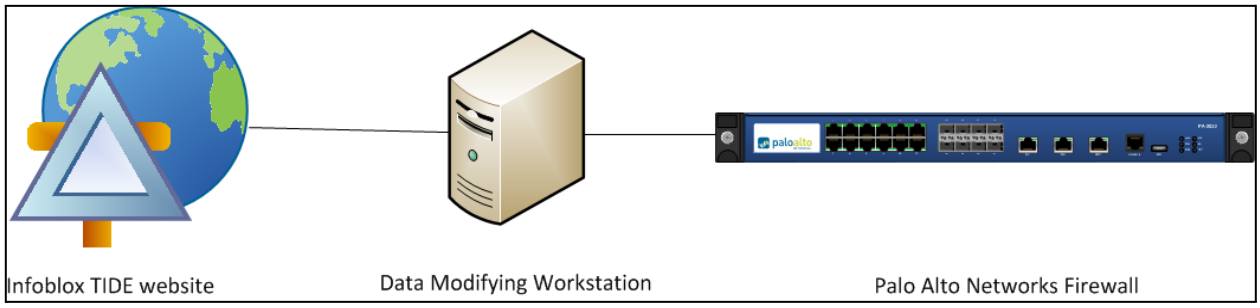
The following items are required to incorporate the Infoblox TIDE feeds into the Palo Alto Networks Firewall:

- Palo Alto Networks Firewall with Threat Protection and URL filtering licenses.
- Access to the Infoblox TIDE website to download the Threat Data feeds.
- A VM (virtual machine) or workstation to modify the feeds per the Palo Alto Networks data formats. Per the 'Formatting Guidelines for an External Dynamic List' section in the PAN OS Administrator's Guide for Formatting Information:
    - Remove the quotes.
    - Remove the field headers (i.e. IP, URL, host).
    - Remove HTTP:// and HTTPS:// from the URLs.
    - Here is a same SED command for removing the items above in the feeds:
        - sed -e 's/^ip$//' -e 's/^url$//' -e 's/^host$//' -e '/^\s*$/d' -e 's/"//g' -e 's#http://##g' -e 's#https://##g'

Tested Hardware and Software

- Palo Alto Networks Firewall model PA-VM.
- PAN OS version 11.0.1.

Sample Test Network for importing data feeds into Palo Alto firewall



Data is downloaded to the workstation to be modified per the formatting requirements. The workstation must run a webserver for the Palo Alto firewall to access the feeds. The Palo Alto firewall then downloads the newly formatted data using External Dynamic Lists.

Deployment Summary

- Obtain API key from Infoblox's Cloud Services Portal.
- View TIDE filters and generate API call.
- Use CURL to download feeds and modify the files for importing into Palo Alto firewall
- Create External Dynamic Lists for: IP address, Domains, and/or URLs.
- Create an Anti-Spyware entry for the domain list.
- Create a URL Filtering entry for the URL list.
- Create a policy for the IP list.
- Create a policy for the domain list and URL list.

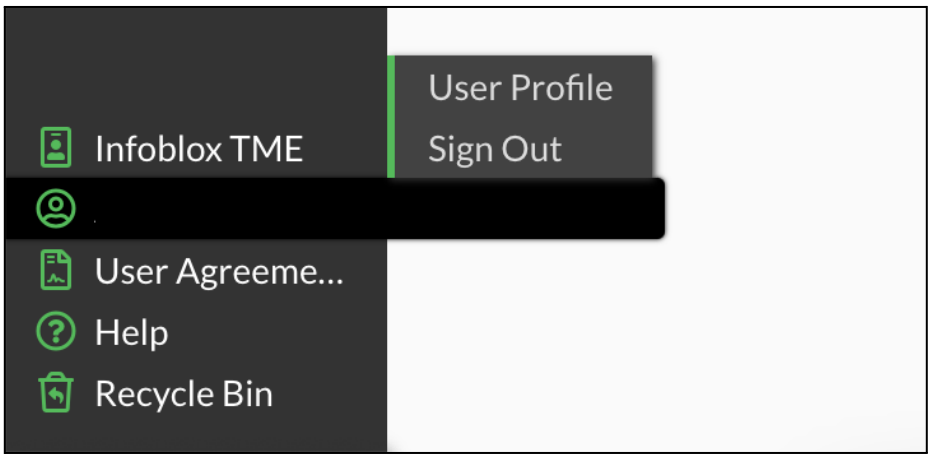
Deployment Instructions

Obtain API Key from Infoblox's Cloud Services Portal

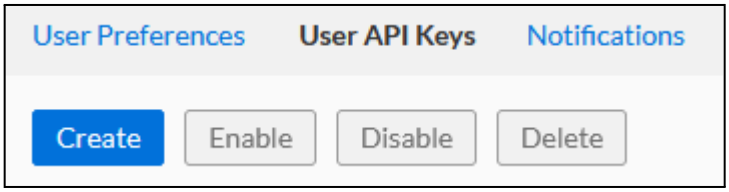
You will need a BloxOne Threat Defense Advanced API key to pull the TIDE feeds via the REST API. You can access this key through the Cloud Services Portal (CSP).

To access your API key:

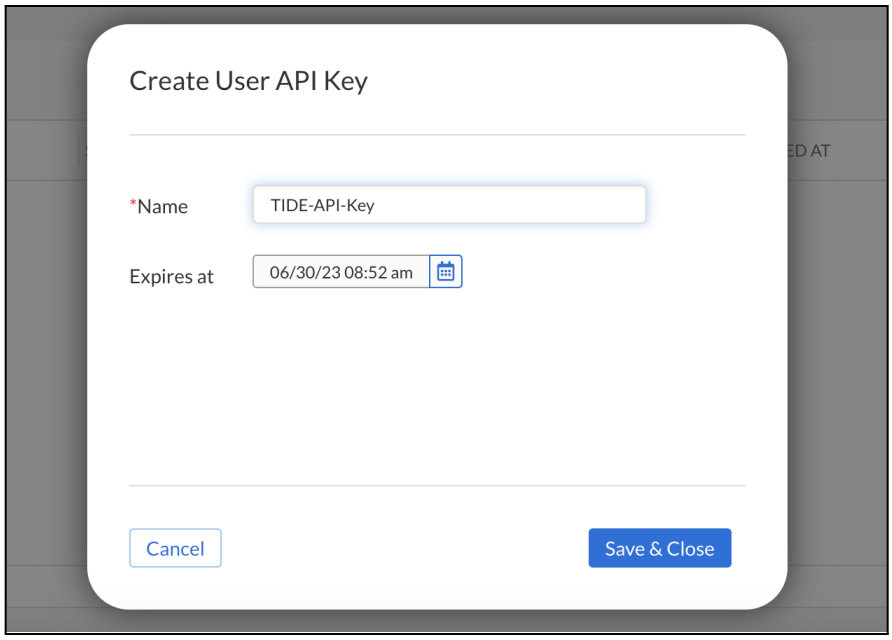
1. Log in to the CSP at https://csp.infoblox.com
2. Upon logging in, hover over your username in the bottom-left corner and select **User Profile**.



3. Navigate to the User API Keys tab

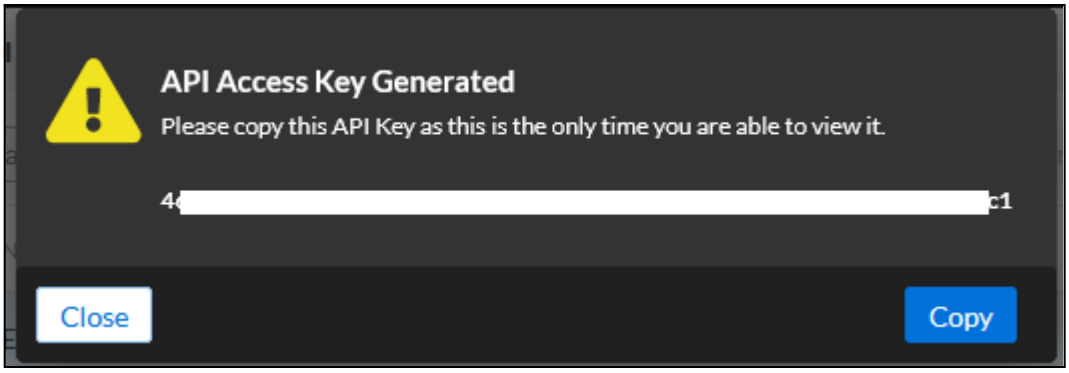


4. Click **Create** to create a new API Key.
5. In the Create User API Key dialog box. Input a **Name** and an **expiration date** for the API Key.



6. Click **Save & Close** to confirm the creation of the API Key.

7. A dialog box containing the new API Key will be shown. Click Copy to copy your API key to your clipboard. Paste it somewhere you can easily access and then copy from later, such as Notepad. This will be the key you use in CURL.

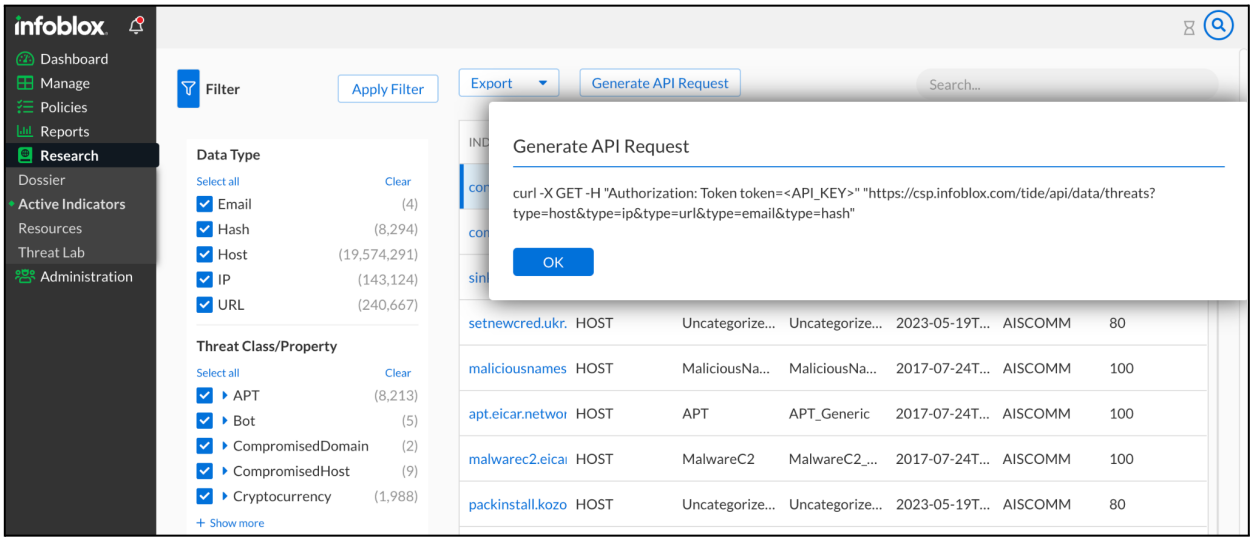


View TIDE filters and Generate API call

Infoblox TIDE provides many filters to choose from depending on your needs. This section shows you an overview of the filters and how to retrieve the appropriate API call to grab these feeds for downloads.

To View the filters, navigate to "**Research / Active Indicators**" – You can use the "**Apply Indicators**" to view the different Data types.

You can then **Generate the API Request**. As an example, for the IP List, we'll first Clear all the Categories, then select only the Data Type IP, then click on "Apply Filter", then click on Generate API Request.



Be sure to Copy the URL and save it for the next step. Repeat the process using the Data Type "**Host**" (this will provide the Domain List) and Date Type "**URL**". Be sure to '**Apply Filter**' after each step to generate the correct API request.

Use CURL to download feed(s) and modify the files for importing into Palo Alto firewall

Notes:

- Replace **[API Token]** below with Token retrieved from Step #1 above.
- In this example we're using CSV file format for downloading but JSON and XML formats are also supported.
- There is a maximum of 10k objects that can be downloaded so it is best to specify the limit (in this example we're only downloading the first 100).
- We're using the simple command line tools of 'grep', 'sed' and 'awk' to format the files to import into Palo Alto.

IP List

$curl -k -i -H "Authorization: Token [API Token]î
"https://csp.infoblox.com/tide/api/data/threats?type=ip&rlimit=100&data_format=csv" >ip_list.csv

$grep IP ip_list.csv | awk -F"," '{print $4}' > ip_list

Domain List

$curl -k -i -H "Authorization: [API Token]î
"https://csp.infoblox.com/tide/api/data/threats?type=host&rlimit=100&data_format=csv" >hosts.csv

$grep HOST hosts.csv | awk -F"," '{print $6}' > domains

URL List

$curl -k -i -H "Authorization: Token [API Token]î
"https://csp.infoblox.com/tide/api/data/threats?type=url&rlimit=100&data_format=csv" >urls.csv

$grep URL urls.csv | awk -F"," '{print $5}' | sed -e 's/^http:\/\///g' -e 's/^https:\/\///g' -e 's/^ftp:\/\///g' > urls

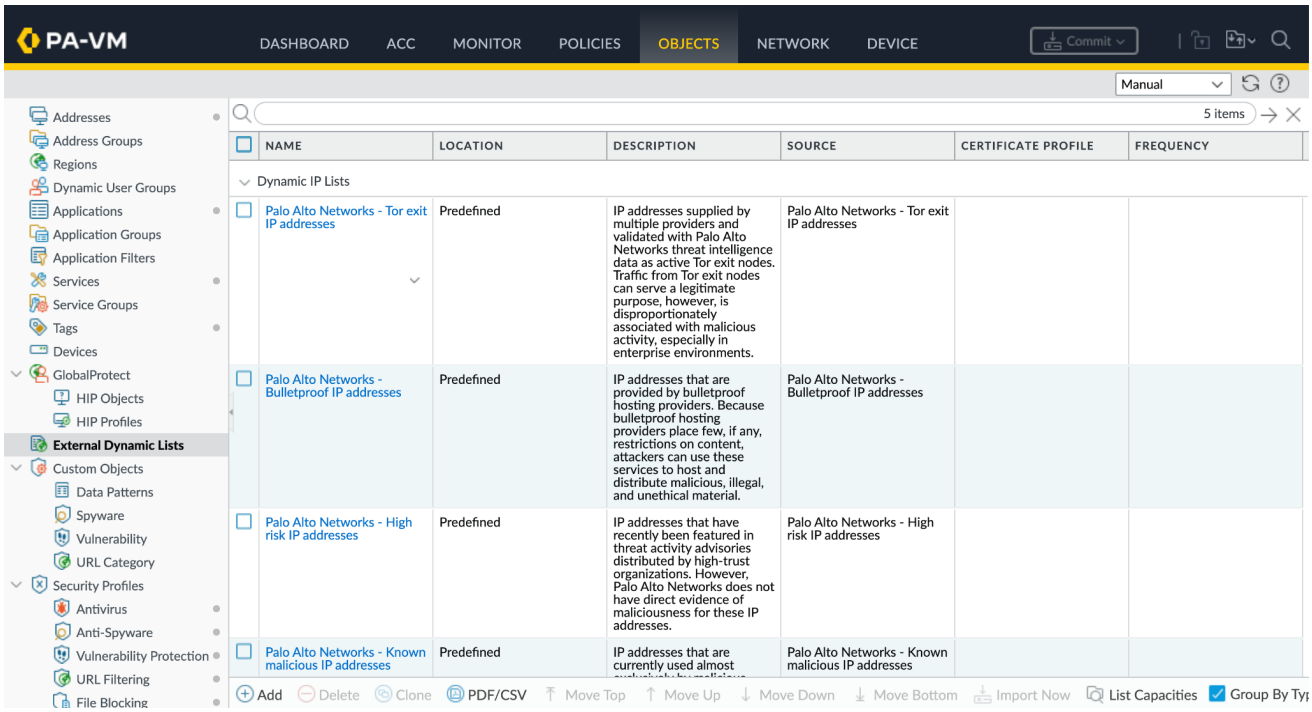
$cat urls | sed '/\$/! s|$|/|' > urls.txt

Note: Run the command above if you wish to add a trailing slash (/) to domain entries (example.com) in your URL Lists to ensure that the firewall treats them as exact matches. If you do not append a trailing slash, you may block or allow more URLs than intended. For example, xyz.com (without a trailing slash), matches any URL beginning with the xyz domain, such as xyz.com.test.site. If you enter the URL as xyz.com/ (with a trailing slash), the firewall matches exactly xyz.com and its subdirectories.

Creating External Dynamic Lists

1. Log in to the Palo Alto Networks **Firewall GUI**.

2. Navigate to **Objects → External Dynamic Lists**.



3. Click on the Add button to add an External Dynamic List entry.

a. Enter the **Name** of the External Dynamic List.

b. Select the **type** of list. Choices are: IP List, Domain List, and URL List.

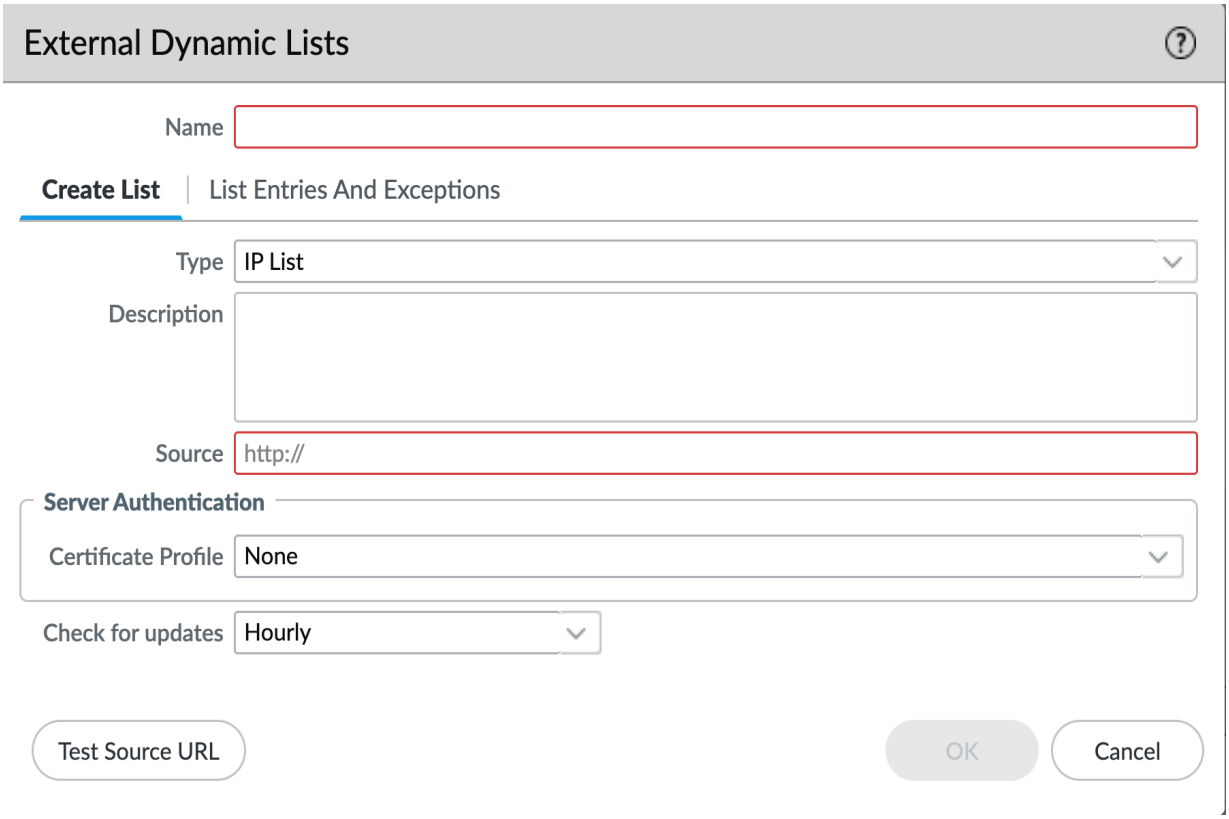
c. Enter a **Description**.

d. Enter the **URL Source**. For example, http://<IP address or FQDN>/tide_url.txt. HTTP and HTTPS are supported.

e. Select the **download interval** via the **Repeat** dropdown. Choices are: hourly, five minute, daily, weekly, or monthly.

f. Click **OK**.

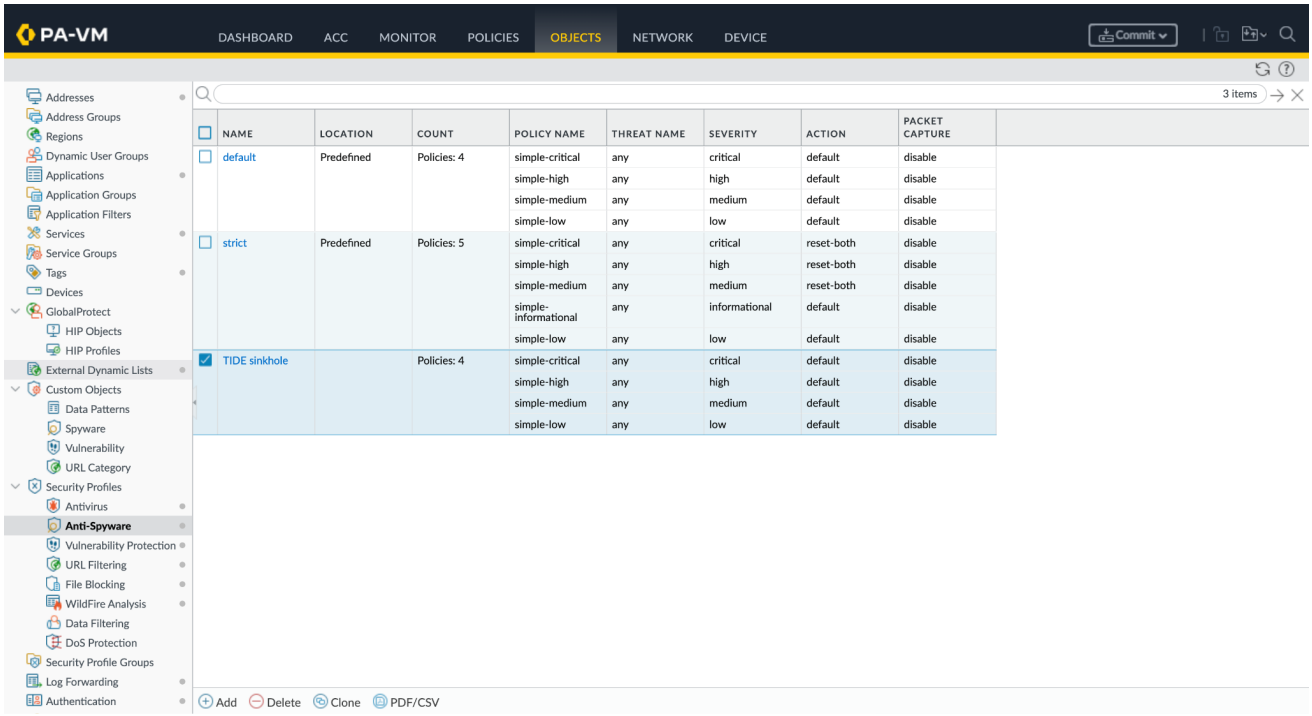
g. You can test the source **URL** to ensure connectivity. If the test fails, then there is either a network connectivity problem or there is a data format problem.



4. Click the **Commit** button.

Create DNS Sinkholing entry for the domain list

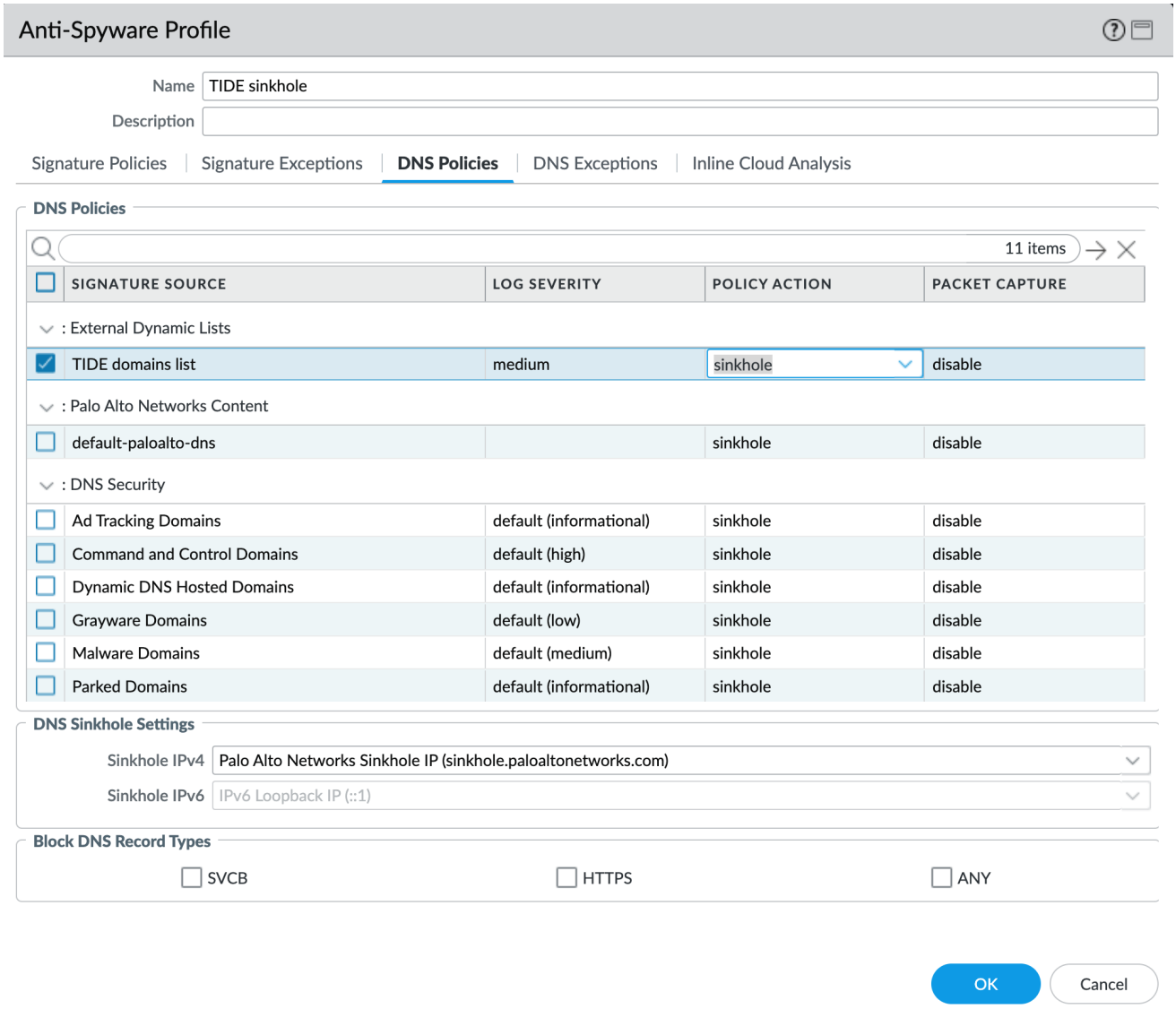
1. Navigate to **Objects** → **Security Profiles** → **Anti-Spyware**.



2. Click **Add** or **Clone** to create an entry.

    a. Enter or modify the **Name**.

    b. (Optional) Enter a **Description**.



c. Click on the **DNS Policies** tab to verify the **domain** list entered previously. In this example, it is the TIDE domains list.

d. Select the **Action** on DNS queries to sinkhole.

e. Select the **sinkhole IPv4** and **sinkhole IPv6** addresses.

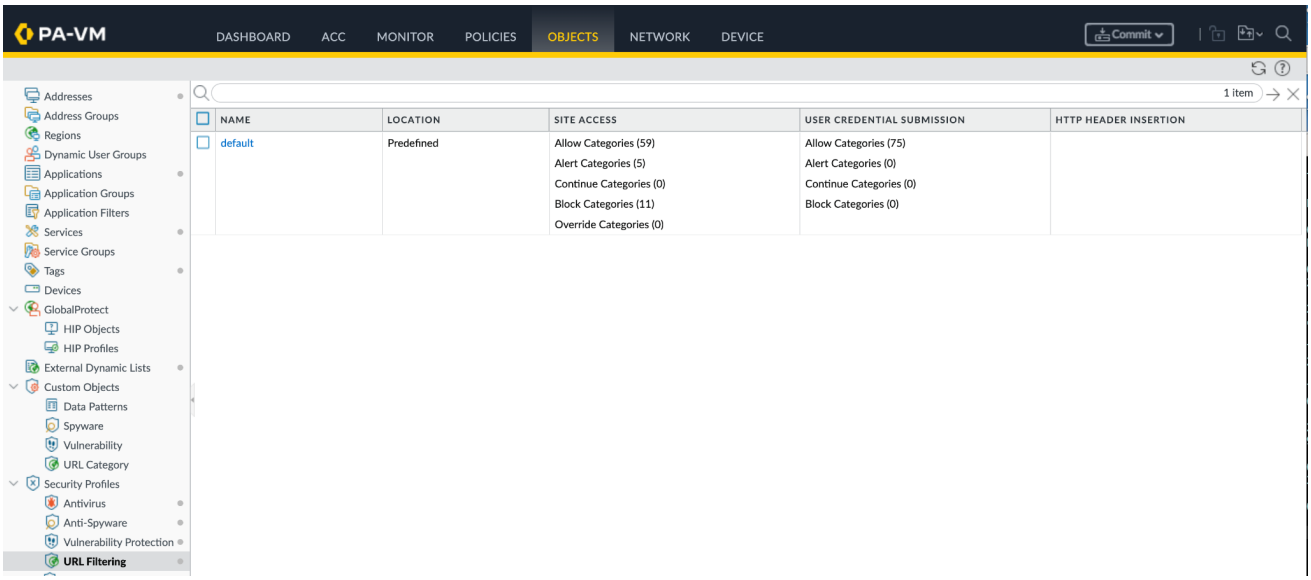
f. Select the DNS record types to block.

g. Click **OK**.

3. Click the **Commit** button.

Creating a URL Filtering entry for the URL List

1. Navigate to **Objects** → **Security Profiles** → **URL Filtering**.



2. Click Add or Clone to create an entry.

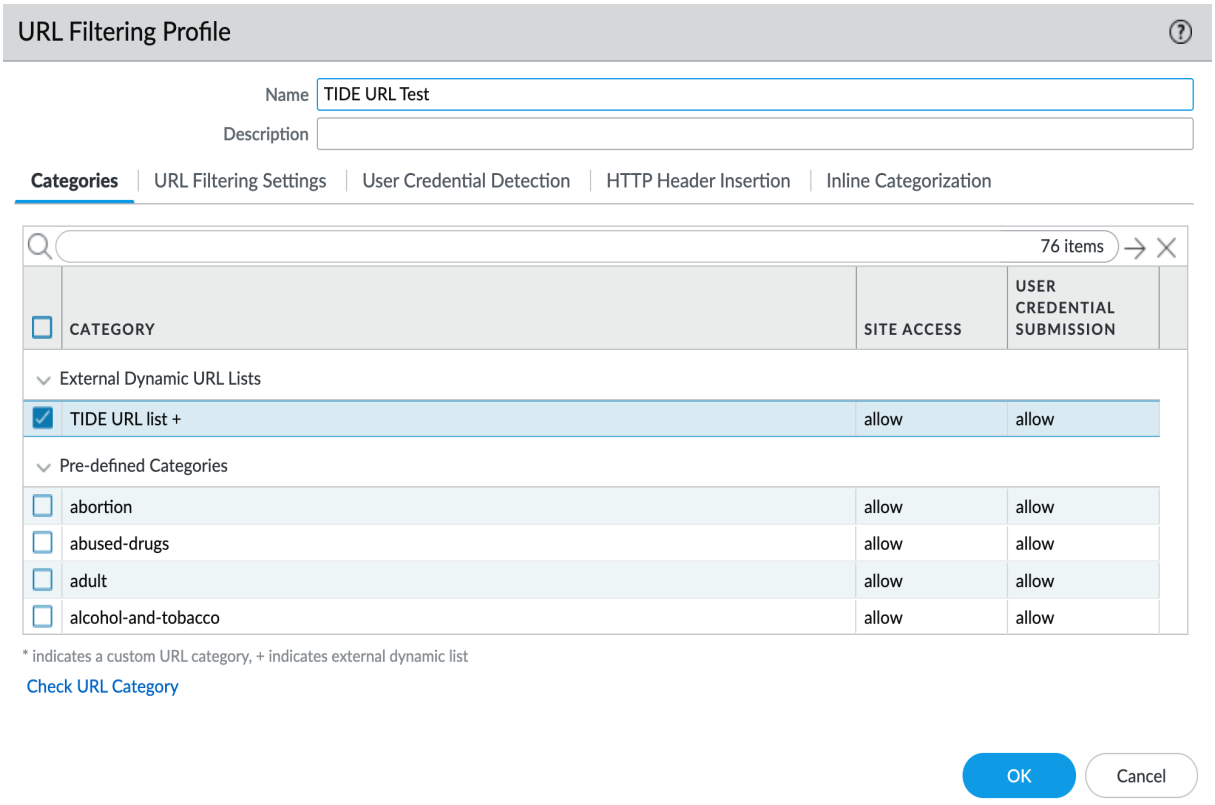
    a. Add a **Name** for the entry.

    b. (Optional) Enter a **Description**.

    c. Scroll down the list to the entry name created previously. The entry will have a + sign appended to it.

    d. Select the **Action** for this entry. Choices are block, alert, allow, continue, override, or none.

e. Click **OK**.

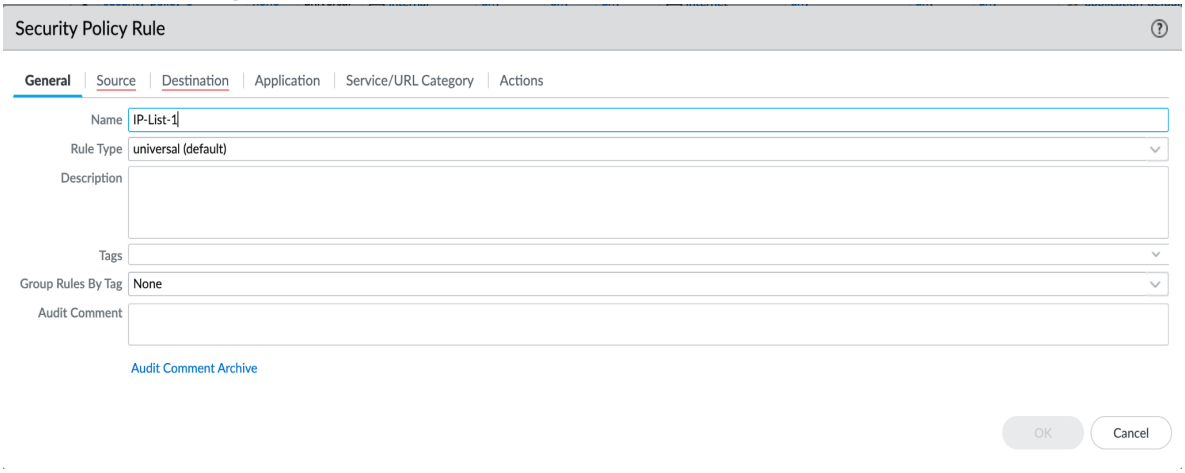


3. Click the **Commit** button.

Create the Security Policies

1. Navigate to **Policies** → **Security**.
2. Click **Add** or **Clone** to create the entry for the IP list.
    a. Enter a **Name** for the policy.
    b. Enter a **rule type** or use the default.
    c. (Optional) Enter a **Description**.

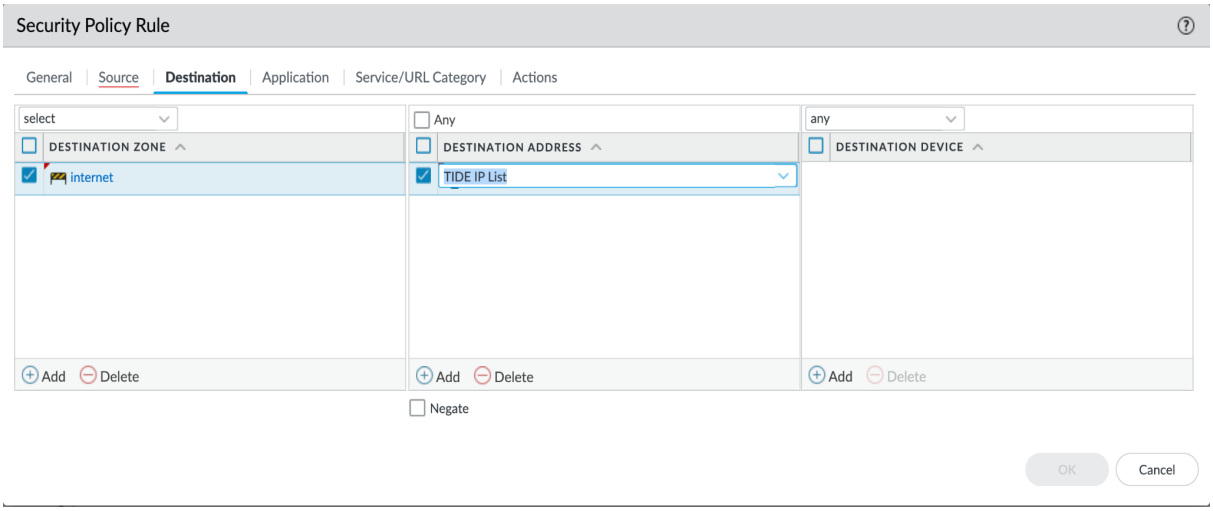
d. (Optional) enter **Tags**.



e. Click on the **Source** tab.

f. Add a **Source Zone**. In this example, the trust zone is entered.

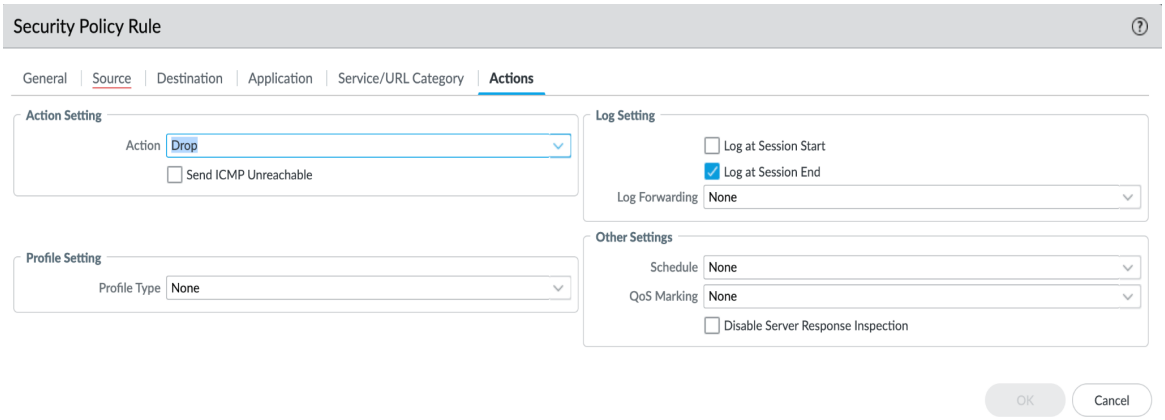
g. Click on the **Destination** tab.



h. Add a **Destination zone** and **Destination address**. In this example the zone is untrust and the destination address is the IP External Dynamic List.

i. Click on the **Actions** tab.

j. In the **Action Setting** section, select the action. In this example, drop action was selected.



k. Click **OK**.

3. Click **Add** or Clone to create an entry for the domain and URL lists.

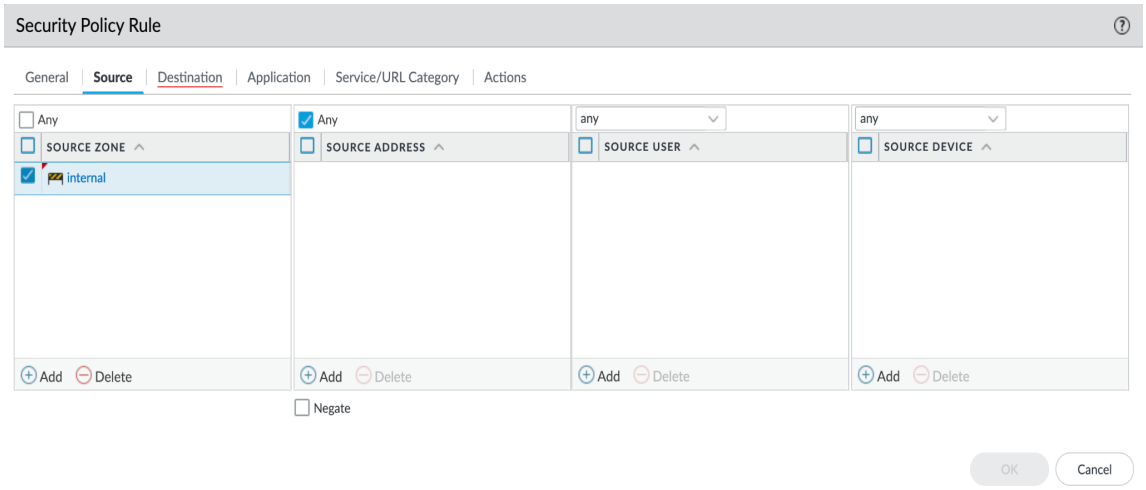
   a. Enter a **Name** for the policy.

   b. Enter a **rule type** or use the default.

   c. (Optional) Enter a **Description**.

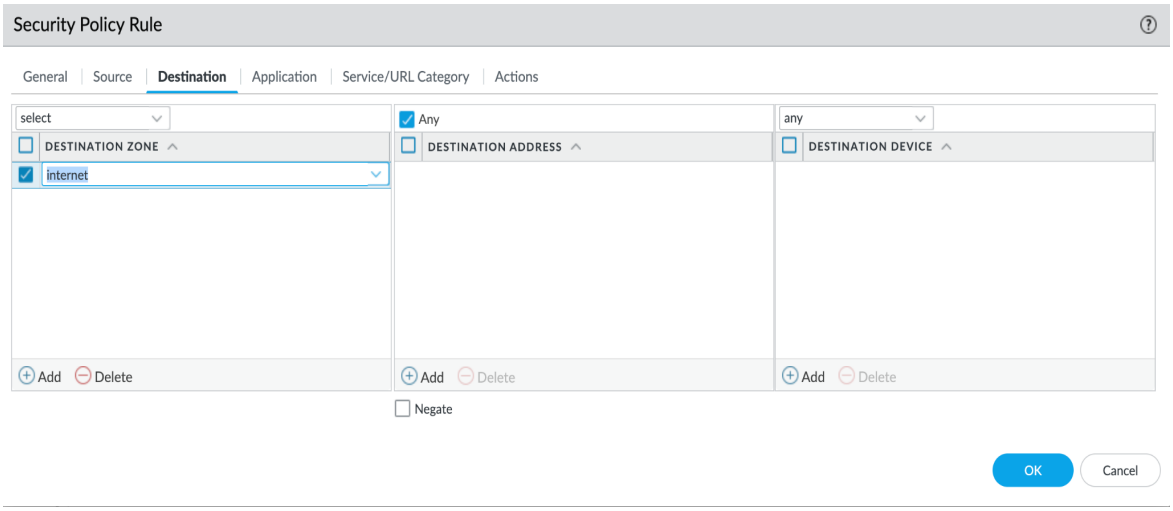
   d. (Optional) Enter **Tags**.

   e. Click on the **Source** tab. Add a **Source** Zone. In this example, the trust zone is entered.



   f. Click on the **Destination** tab.

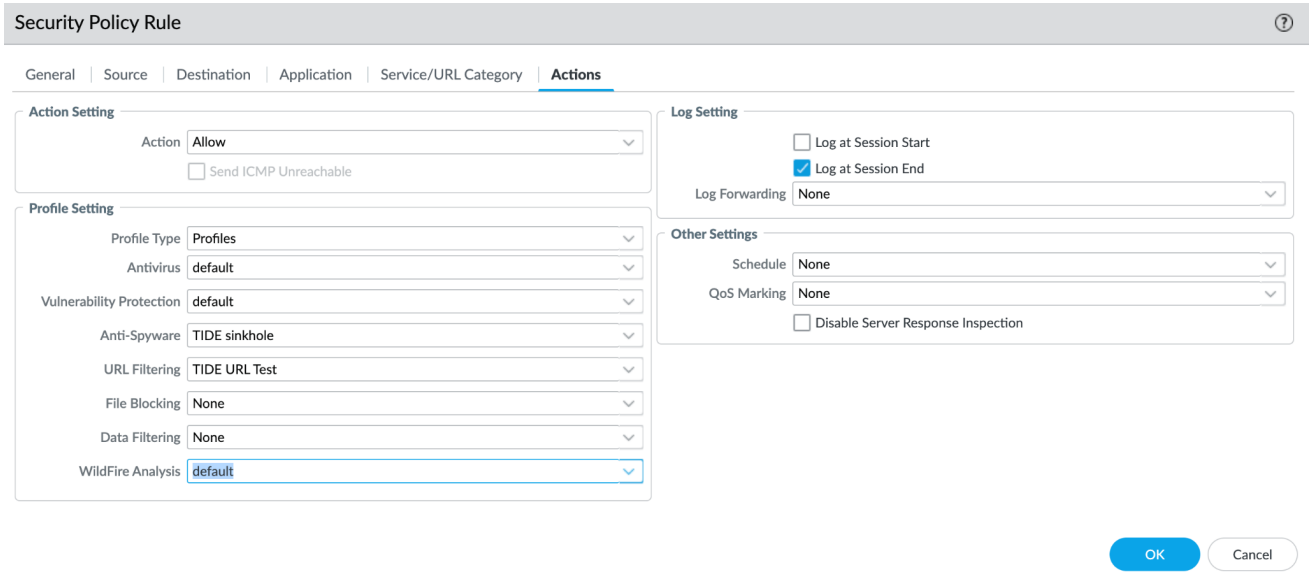
g. Add a **destination zone**. In this example the untrust zone is entered.



h. Click on the **Actions** tab.

i. Select **allow** for the action setting to allow.

j. Select the entry for the **Anti-Spyware** and **URL Filtering**.



k. Click OK.

4. Place these policies in the following order; IP policy first and Anti-spyware & URL Filtering second.

5. Click the **Commit** button.

Showing the contents of each list

1. **SSH** to the Palo Alto Networks firewall.

2. Run the following **command** to show the IP list: request system external-list show type ip name <ip list name>.

    - You should see something like this:

```
TIDE IP List
        Total valid entries     : 100
        Total ignored entries   : 0
        Total invalid entries   : 0
        Total displayed entries : 100
        Valid ips:
                104.243.249.62
                52.3.8.179
                35.227.56.199
                140.82.34.250
                194.180.48.36
                91.228.225.46
                18.142.174.21
                52.66.26.57
                81.68.214.187
                81.68.127.212
                43.198.97.153
```

3. Run the following **command** to show the contents of the domain list: request system external-list show type domain name <domain list name>.

    - The output should look like this:

```
TIDE domains list
        Total valid entries     : 100
        Total ignored entries   : 0
        Total invalid entries   : 0
        Total displayed entries : 100
        Valid domains:
                carlosdj.com.br
                leafpacknetwork.org
                amozeshmozakere.com
                evangelia.edu
                guerdofest.com
                eicar.network
                danhdeonline.top
                zoom.voyage
                itinerairesphoto.com
```

4. Run the following command to show the contents of the URL list: request system external-list show type url name <url list name>.

    - The output should look like this:

```
TIDE URL list
        Total valid entries     : 100
        Total ignored entries   : 0
        Total invalid entries   : 0
        Total displayed entries : 100
        Valid urls:
                qweastradoc.com
                connectzoomdownload.com/download/zoominstaller.exe
                guerdofest.com/gate.php
                connectzoomdownload.com/download/zoominstaller.exe
                zoom.voyage/download/zoom.exe
                jirostrogud.com
                hiperfdhaus.com
```

Test the Policies

1. To test the IP list, run either ping on traceroute. You should not get any response from either command except for a timeout.

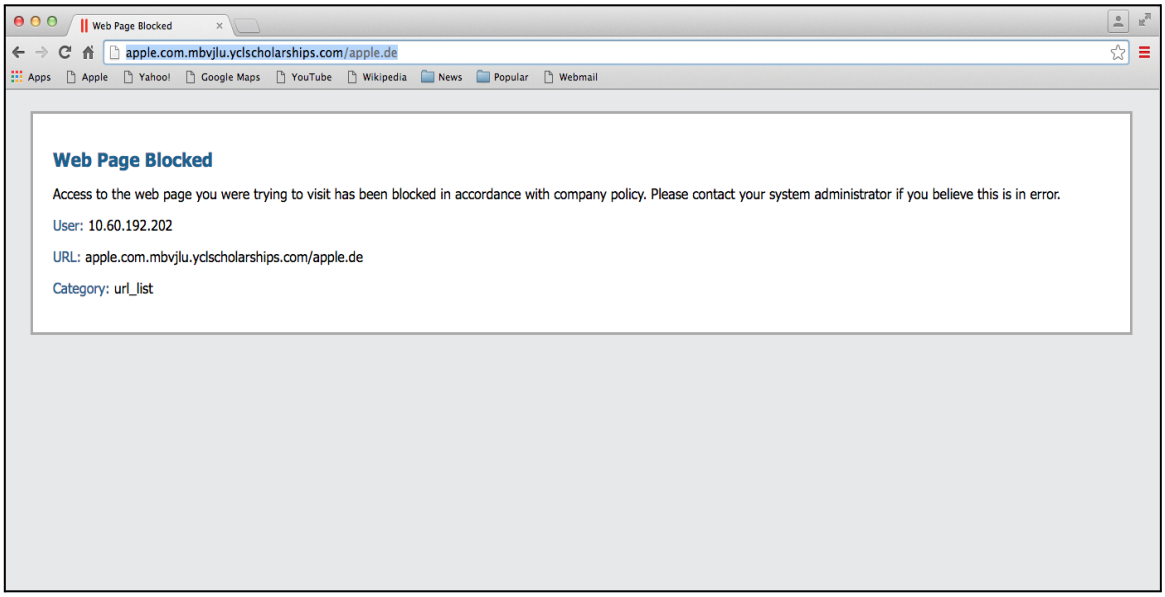
2. To test the domain list, run either nslookup or dig against an entry in the domain list.

    - You should get the following output. Notice the IP address? It is the default sinkhole address.

```
sc-m-tlee:~ administrator$ dig dpacpartbulkyf.com

; <<>> DiG 9.8.5-P1 <<>> dpacpartbulkyf.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 1618
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;dpacpartbulkyf.com.            IN      A

;; ANSWER SECTION:
dpacpartbulkyf.com.     1       IN      A       71.19.152.112

;; Query time: 1 msec
;; SERVER: 10.60.192.2#53(10.60.192.2)
;; WHEN: Wed Jan 11 09:43:54 PST 2017
;; MSG SIZE  rcvd: 52
```

3. To test the **URL list**, open a browser and browse to an entry in the URL list.

4. You should get similar output. The output below came from a Google Chrome browser.



Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier.

Corporate Headquarters
2390 Mission College Blvd, Ste. 501
Santa Clara, CA 95054
+1.408.986.4000
www.infoblox.com