DEPLOYMENT GUIDE

# Implementing Infoblox TIDE feeds into Palo Alto Networks Firewalls

# 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 ActiveTrust 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:

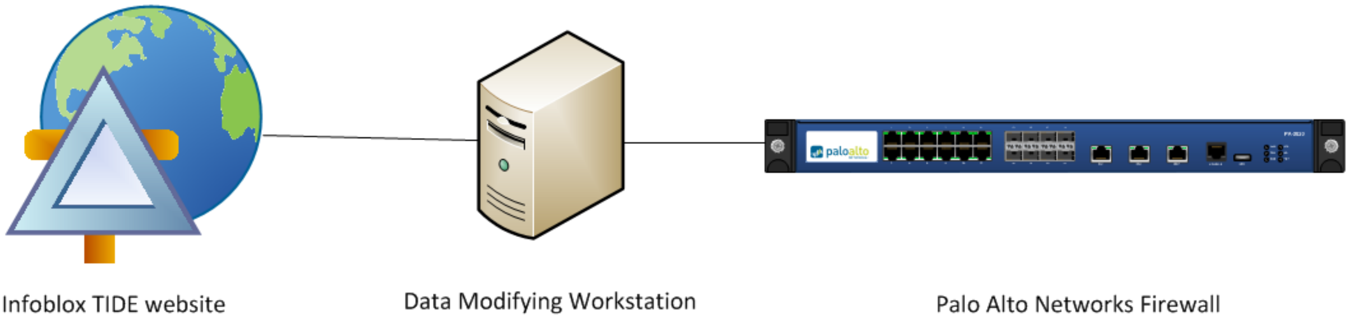
- Palo Alto Networks Firewall with Threat Protection and URL filtering licenses.
- Access to the Infoblox TIDE website to download the data feeds.
- A VM (virtual machine) or workstation to modify the feeds per the Palo Alto Networks data formats. Per the ‘Formatting Guidelines for an External Dynamic List’ section in the PAN OS administrators 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 3020.
- PAN OS version 7.1.7.

## 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.

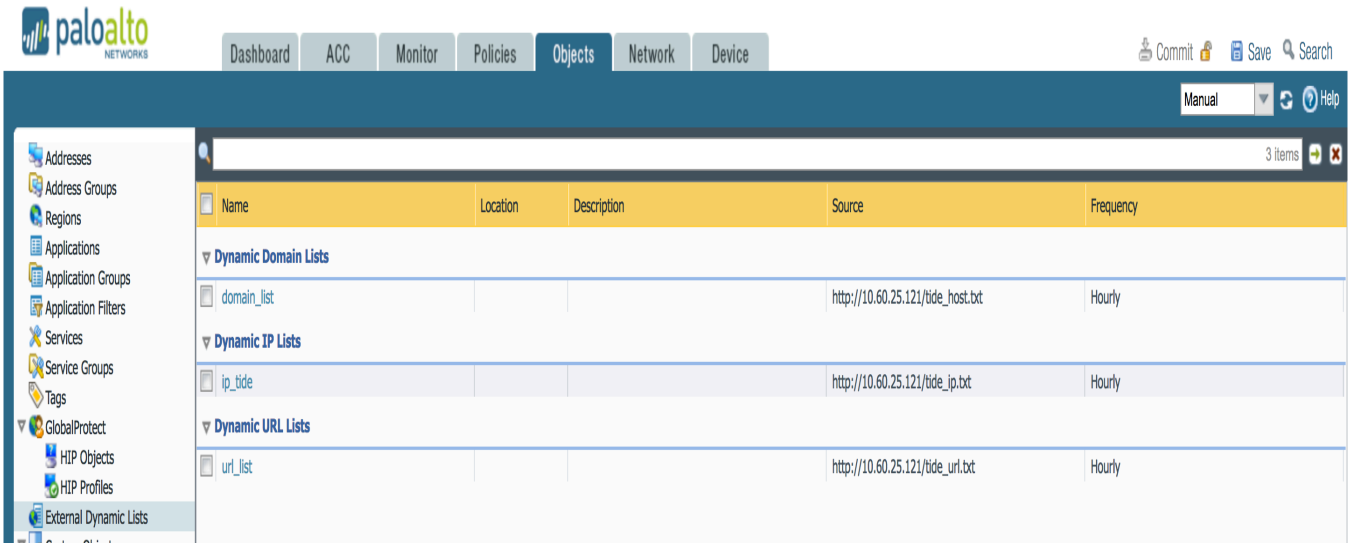
## Deployment Summary

- After downloading the feeds to the VM or workstation, 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

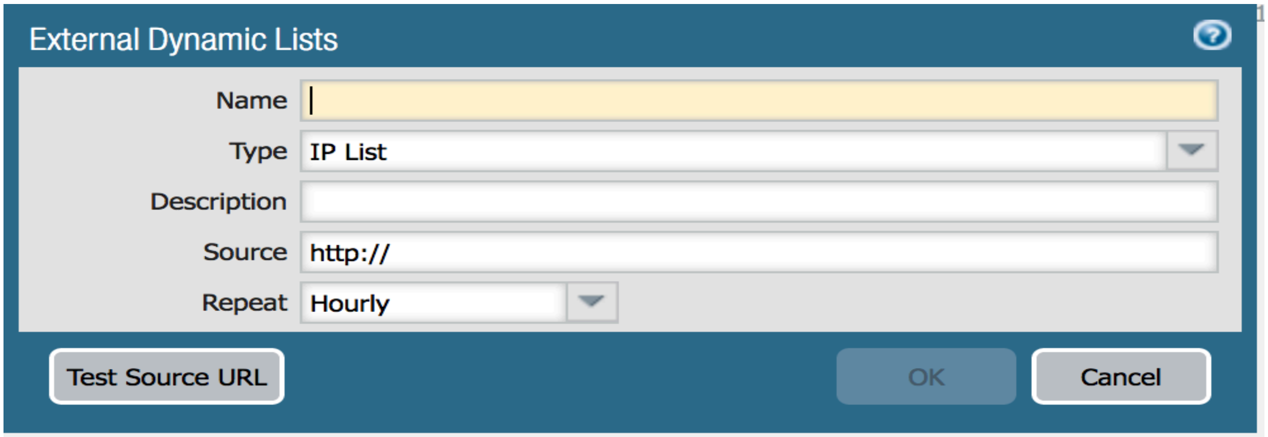
### Creating External Dynamic Lists

1. Log into the Palo Alto Networks Firewall GUI.
2. Navigate to Objects → External Dynamic Lists.



| Name | Location | Description | Source | Frequency |
|---|---|---|---|---|
| Dynamic Domain Lists | | | | |
| domain_list | | | http://10.60.25.121/tide_host.txt | Hourly |
| Dynamic IP Lists | | | | |
| ip_tide | | | http://10.60.25.121/tide_ip.txt | Hourly |
| Dynamic URL Lists | | | | |
| url_list | | | http://10.60.25.121/tide_url.txt | Hourly |

3. Click on the 'Add' button to add an External Dynamic List entry.
   I. Enter the name of the External Dynamic List.
   II. Select the type of list. Choices are:  IP List, Domain List, and URL List.
   III. Enter a description.
   IV. Enter the URL source.  For example, http://<IP address or FQDN>/tide_url.txt. HTTP and HTTPS are supported.
   V. Select the download intervals.  Choices are:  hourly, five minute, daily, weekly, or monthly.
   VI. Click OK.
   VII. 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.

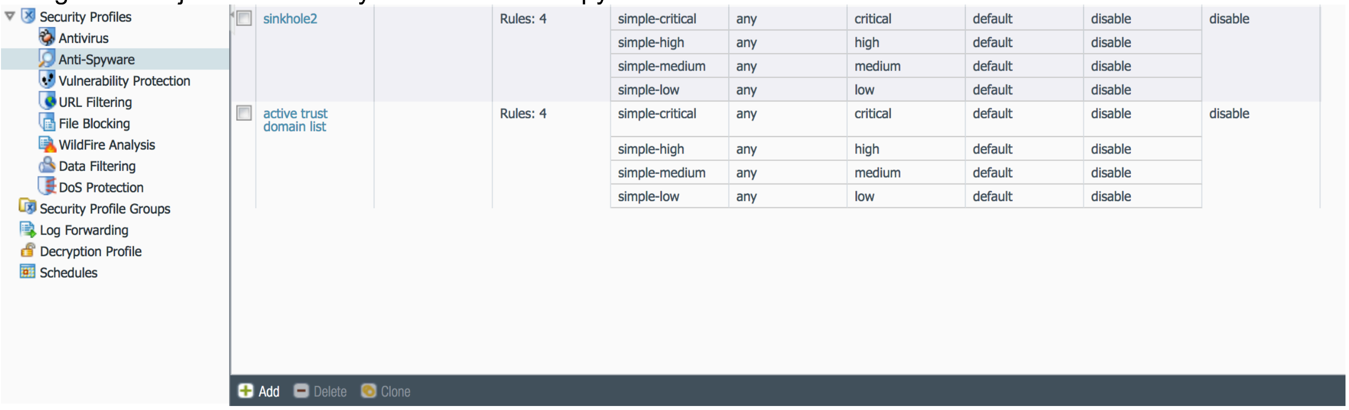


| | |
|---|---|
| Name | |
| Type | IP List |
| Description | |
| Source | http:// |
| Repeat | Hourly |

4. Click on the Commit button.

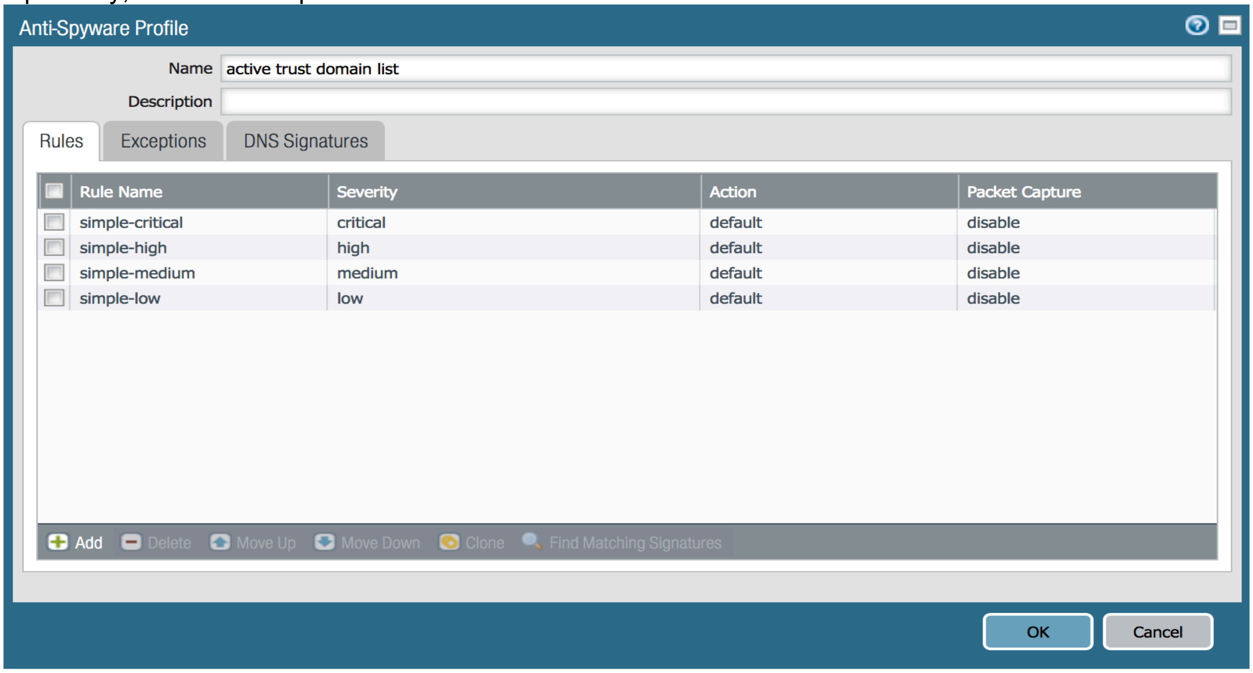
## Create DNS Sinkholing entry for the domain list

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



| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| □ | sinkhole2 | Rules: 4 | simple-critical | any | critical | default | disable | disable |
| | | | simple-high | any | high | default | disable | |
| | | | simple-medium | any | medium | default | disable | |
| | | | simple-low | any | low | default | disable | |
| □ | active trust domain list | Rules: 4 | simple-critical | any | critical | default | disable | disable |
| | | | simple-high | any | high | default | disable | |
| | | | simple-medium | any | medium | default | disable | |
| | | | simple-low | any | low | default | disable | |

2. Click Add or Clone to create an entry.
   I. Enter or modify the name.
   II. Optionally, enter a description.

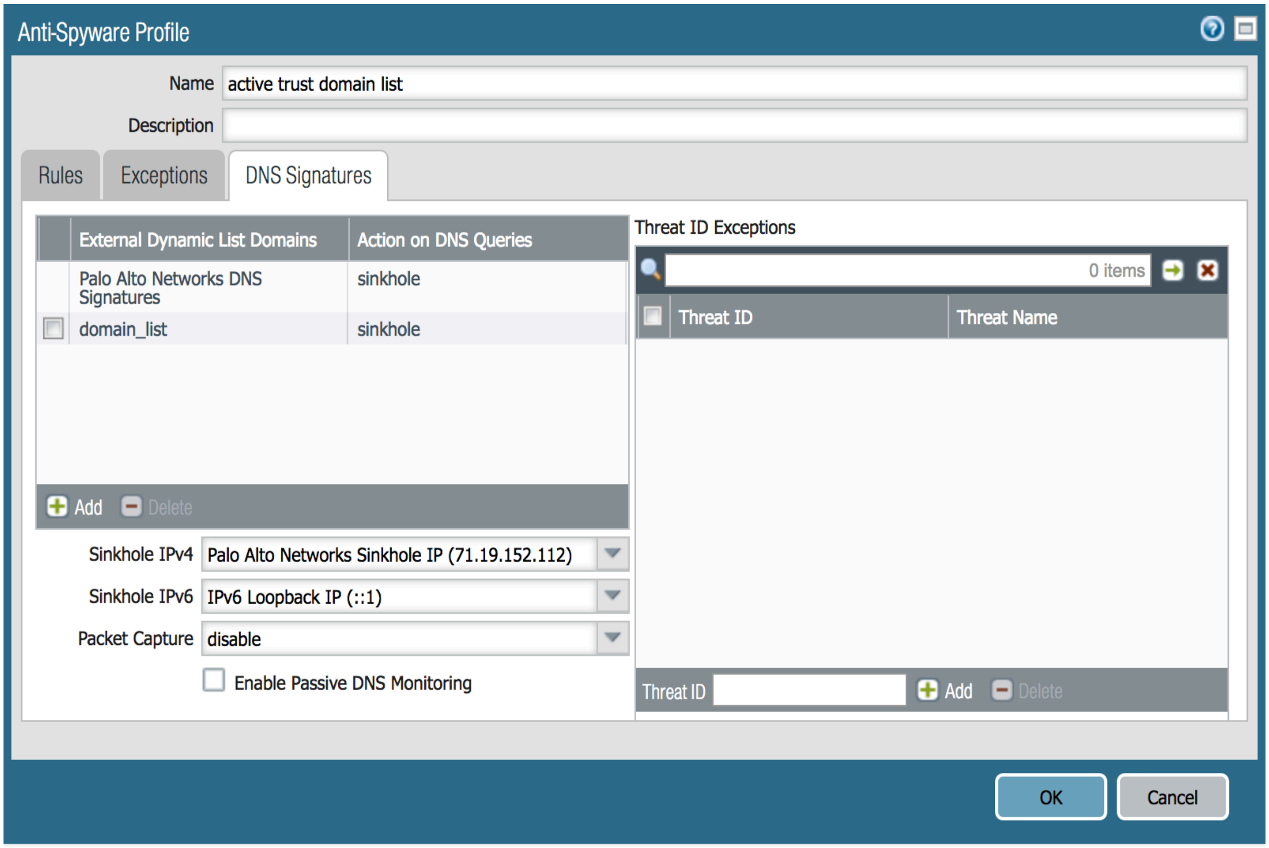


Name: active trust domain list

Description:

| □ | Rule Name | Severity | Action | Packet Capture |
|---|---|---|---|---|
| □ | simple-critical | critical | default | disable |
| □ | simple-high | high | default | disable |
| □ | simple-medium | medium | default | disable |
| □ | simple-low | low | default | disable |

III. Click on the DNS Signatures tab to enter the domain list.
IV. Click on the Add button and select the external dynamic domain list that was created previously.
V. Select the Action on DNS queries to sinkhole.
VI. Select the sinkhole IPv4 and IPv6 sinkhole addresses.
VII. Click OK.



Anti-Spyware Profile

Name: active trust domain list

Description:

| | External Dynamic List Domains | Action on DNS Queries |
|---|---|---|
| | Palo Alto Networks DNS Signatures | sinkhole |
| □ | domain_list | sinkhole |

Sinkhole IPv4: Palo Alto Networks Sinkhole IP (71.19.152.112)

Sinkhole IPv6: IPv6 Loopback IP (::1)

Packet Capture: disable

□ Enable Passive DNS Monitoring

Threat ID Exceptions

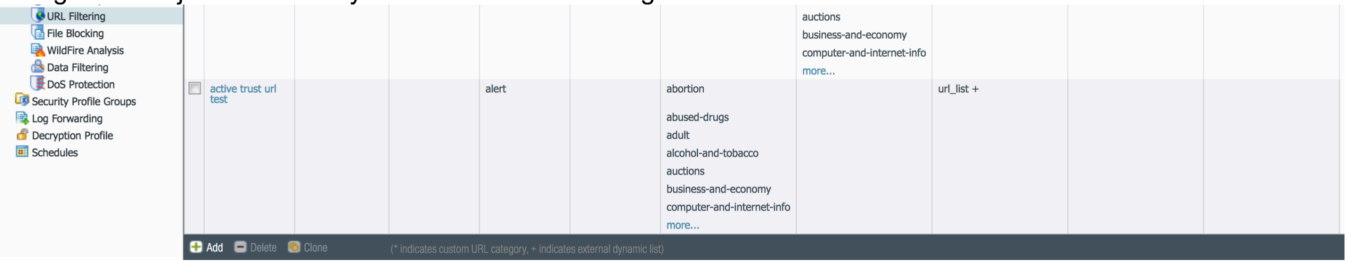
0 items

| □ | Threat ID | Threat Name |
|---|---|---|

3. Click on the Commit button.

## Creating a URL Filtering entry for the URL List

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



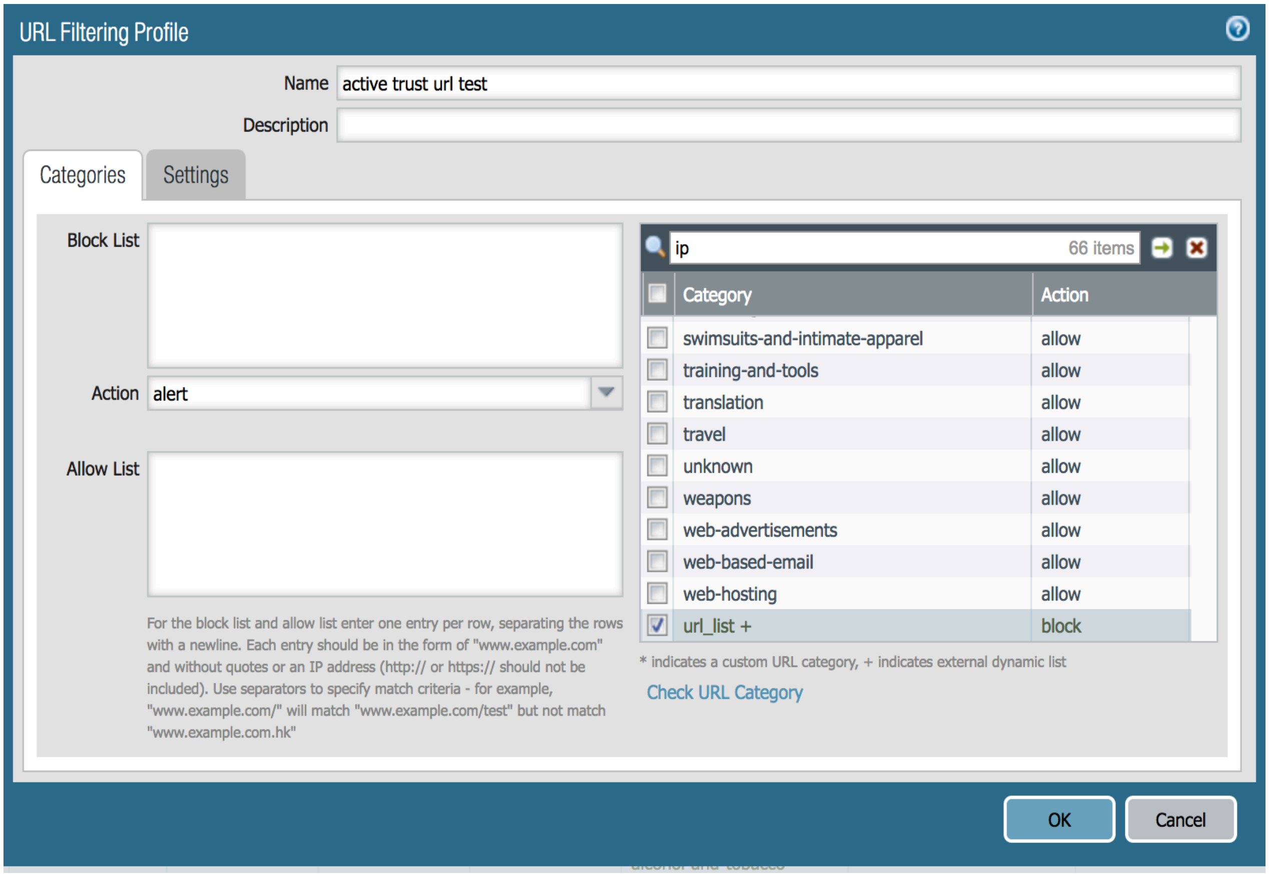
auctions
business-and-economy
computer-and-internet-info
more...

□ active trust url test | alert | abortion, abused-drugs, adult, alcohol-and-tobacco, auctions, business-and-economy, computer-and-internet-info, more... | url_list +

(* indicates custom URL category, + indicates external dynamic list)

2. Click Add or Clone to create an entry.
   I. Add a name for the entry.
   II. Optionally, add a description.
   III. Scroll down the list to the entry name created previously. The entry will have a '+' sign appended to it.
   IV. Select the action for this entry. Choices are block, alert, allow, continue, override, or none.

V. Click OK.


URL Filtering Profile

Name: active trust url test

Description:

Block List:

Action: alert

Allow List:

For the block list and allow list enter one entry per row, separating the rows with a newline. Each entry should be in the form of "www.example.com" and without quotes or an IP address (http:// or https:// should not be included). Use separators to specify match criteria - for example, "www.example.com/" will match "www.example.com/test" but not match "www.example.com.hk"

ip — 66 items

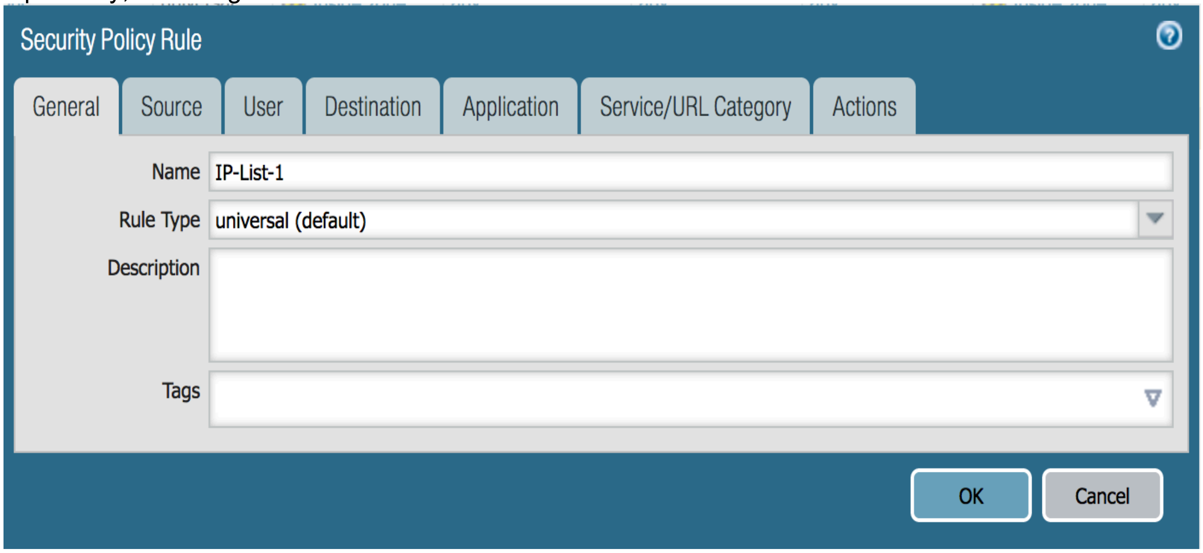
| ☐ | Category | Action |
|---|---|---|
| ☐ | swimsuits-and-intimate-apparel | allow |
| ☐ | training-and-tools | allow |
| ☐ | translation | allow |
| ☐ | travel | allow |
| ☐ | unknown | allow |
| ☐ | weapons | allow |
| ☐ | web-advertisements | allow |
| ☐ | web-based-email | allow |
| ☐ | web-hosting | allow |
| ☑ | url_list + | block |

* indicates a custom URL category, + indicates external dynamic list

3. Click on 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.
   I. Enter a name for the policy.
   II. Enter a rule type or use the default.
   III. Optionally, enter a description.
   IV. Optionally, enter tags.


Security Policy Rule

Name: IP-List-1

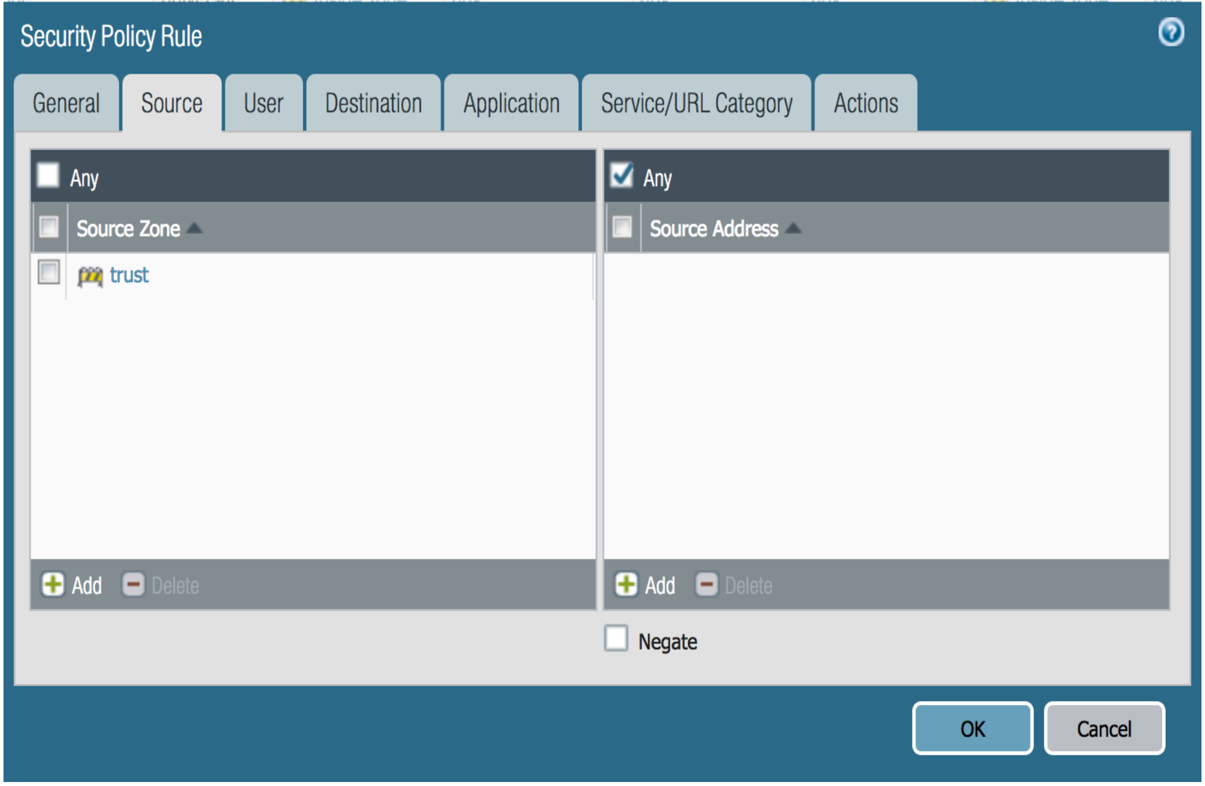
Rule Type: universal (default)

Description:

Tags:

   V. Click on the Source tab.

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



□ Any

□ Source Zone ▲

□ trust

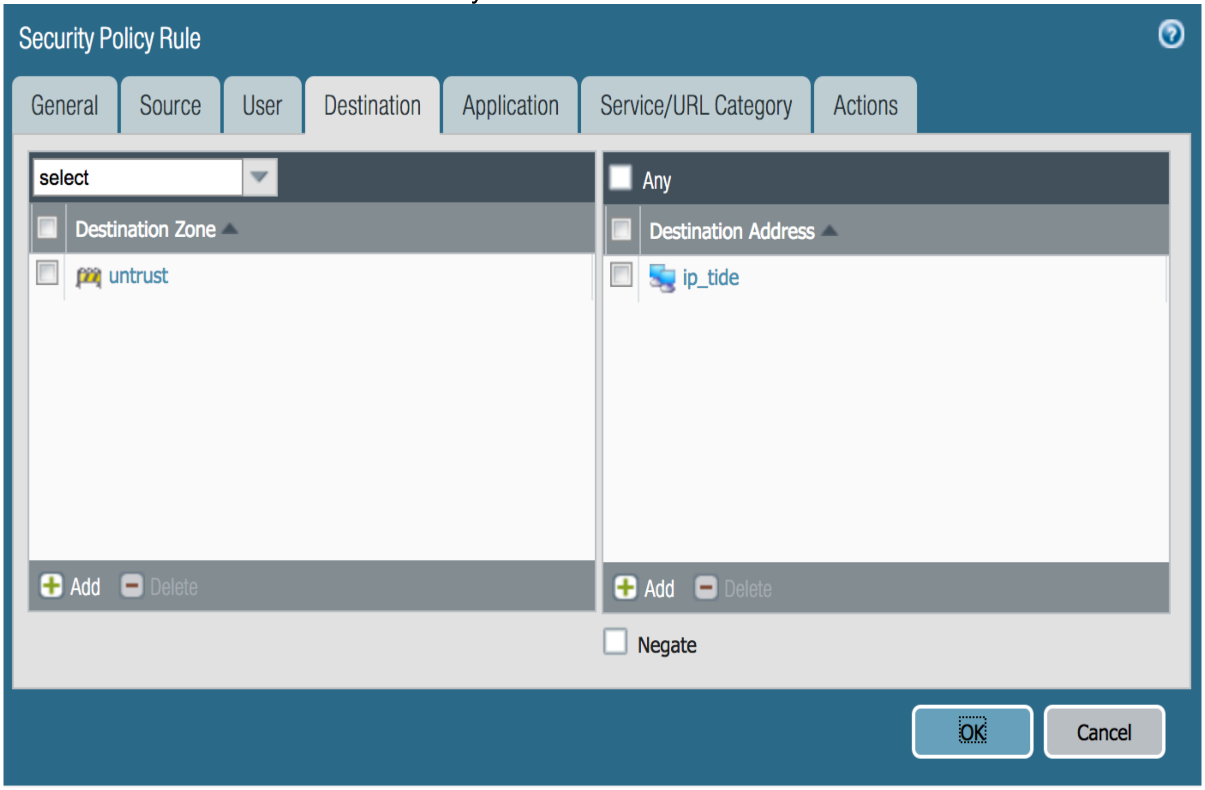
☑ Any

□ Source Address ▲

□ Negate

VII. Click on the Destination tab.

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



select

□ Destination Zone ▲

□ untrust

□ Any

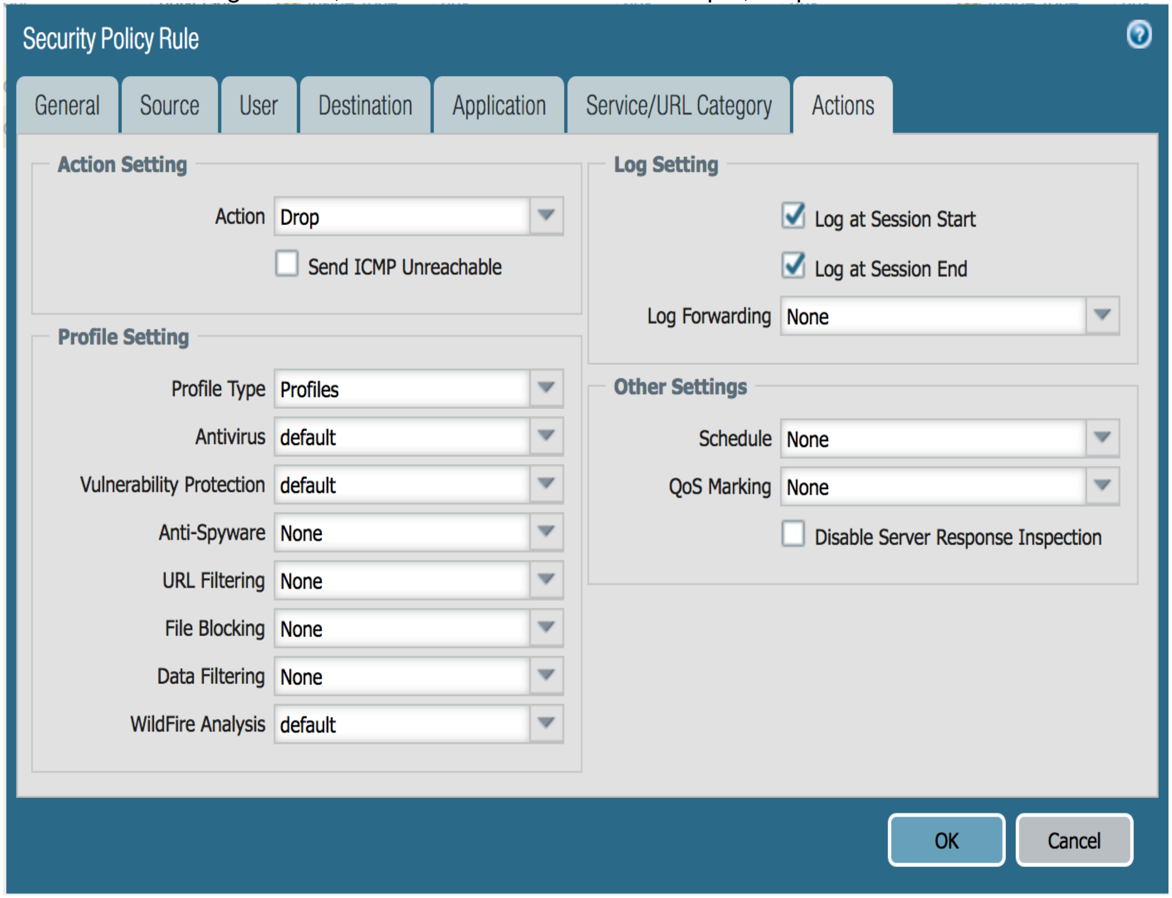
□ Destination Address ▲

□ ip_tide

□ Negate

IX. Click on the Actions tab.

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



Action Setting

Action: Drop

□ Send ICMP Unreachable

Profile Setting

Profile Type: Profiles

Antivirus: default

Vulnerability Protection: default

Anti-Spyware: None

URL Filtering: None

File Blocking: None

Data Filtering: None

WildFire Analysis: default

Log Setting

☑ Log at Session Start

☑ Log at Session End

Log Forwarding: None

Other Settings

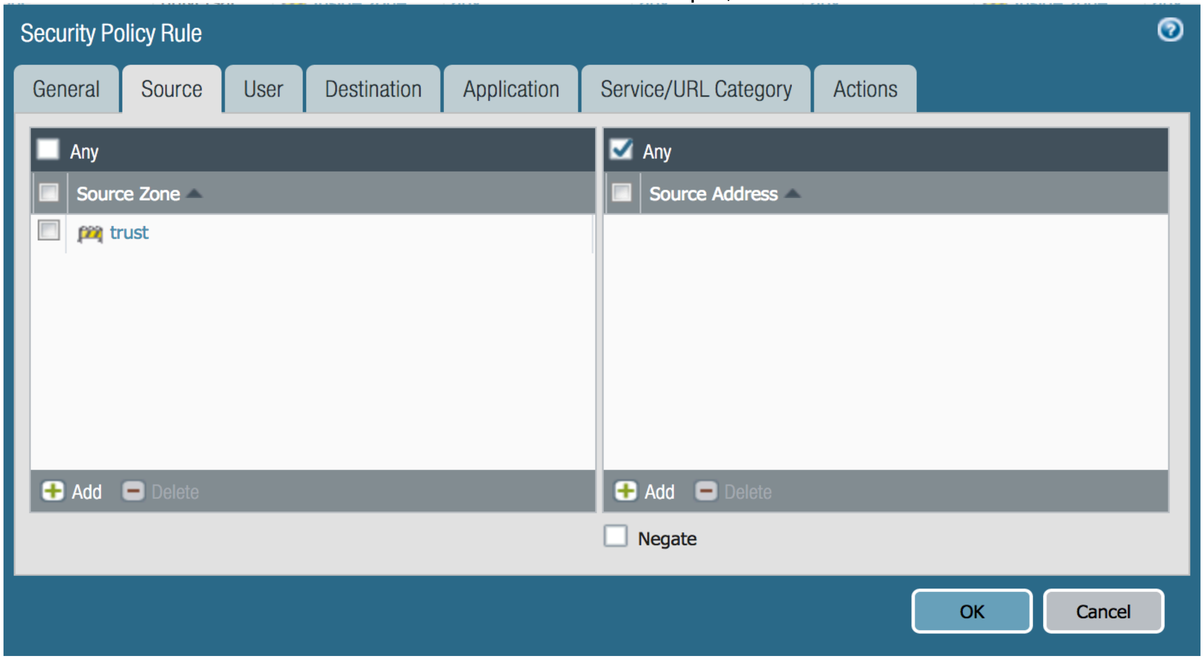
Schedule: None

QoS Marking: None

□ Disable Server Response Inspection

XI. Click OK.

3. Click Add or Clone to create an entry for the domain and URL lists.
   I. Enter a name for the policy.
   II. Enter a rule type or use the default.
   III. Optionally, enter a description.
   IV. Optionally, enter tags.
   V. Click on the Source tab. Add a Source Zone. In this example, the trust zone is entered.



□ Any

□ Source Zone

□ trust

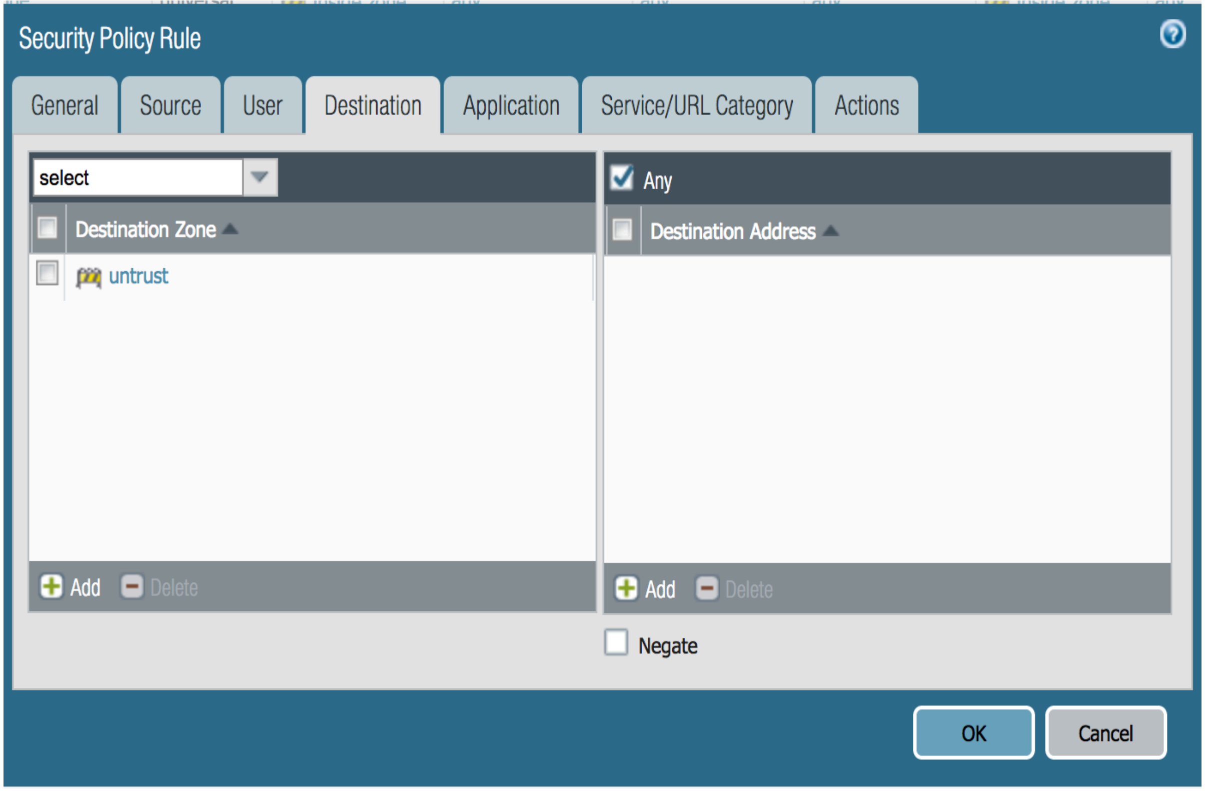
☑ Any

□ Source Address

□ Negate

VI. Click on the Destination tab.

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



| ☐ Destination Zone |
|---|
| ☐ untrust |

☑ Any

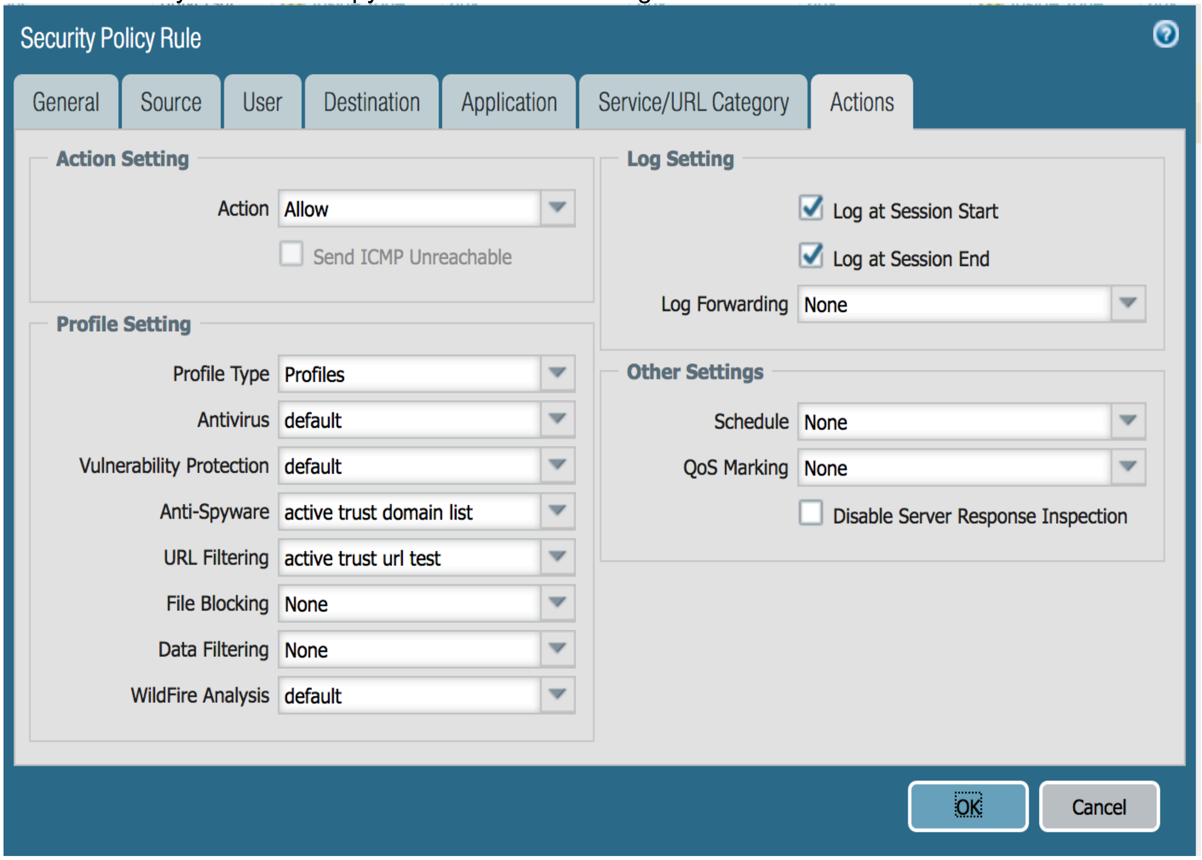
| ☐ Destination Address |
|---|

☐ Negate

VIII. Click on the Actions tab.

IX. Select allow for the action setting to allow.

X. Select the entry for the Anti-Spyware and URL Filtering.



**Action Setting**

Action: Allow

☐ Send ICMP Unreachable

**Profile Setting**

Profile Type: Profiles

Antivirus: default

Vulnerability Protection: default

Anti-Spyware: active trust domain list

URL Filtering: active trust url test

File Blocking: None

Data Filtering: None

WildFire Analysis: default

**Log Setting**

☑ Log at Session Start

☑ Log at Session End

Log Forwarding: None

**Other Settings**

Schedule: None

QoS Marking: None

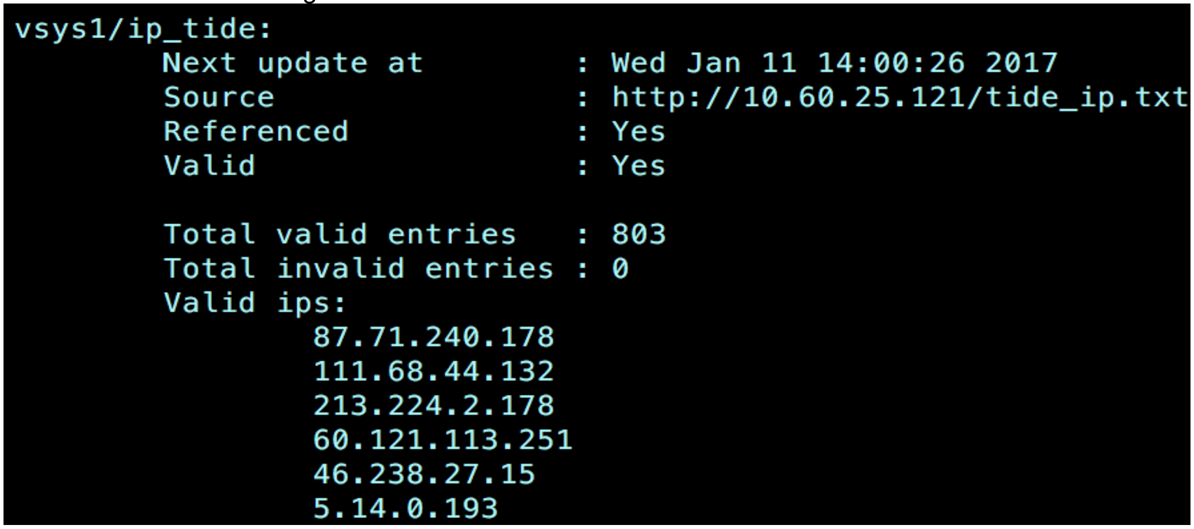
☐ Disable Server Response Inspection

XI. Click OK.

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

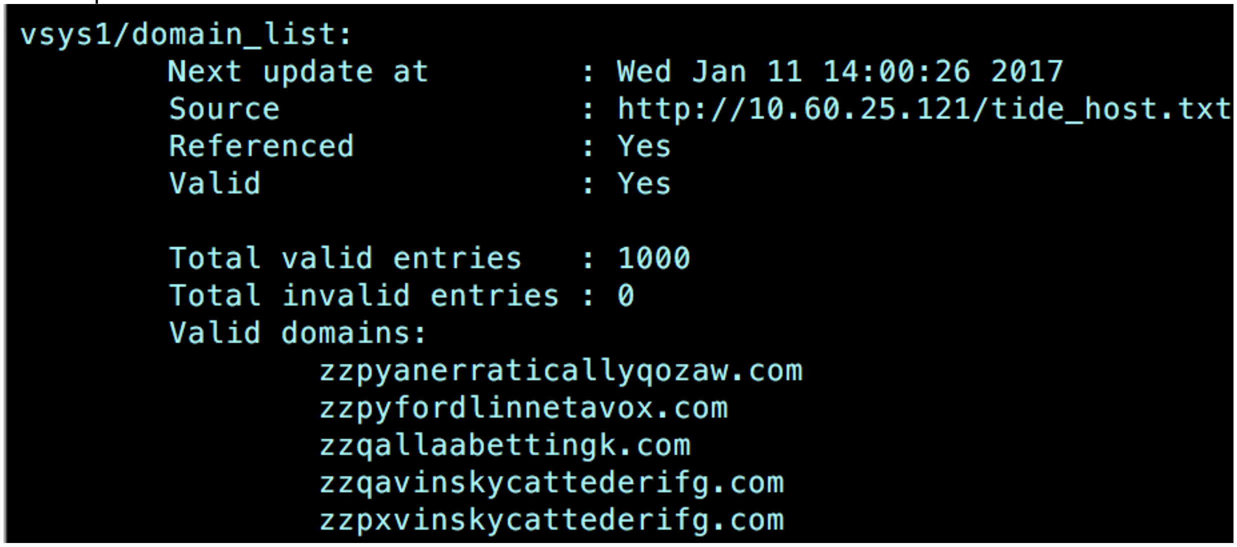
## Showing the contents of each list

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>.
3. You should see something like this:



```
vsys1/ip_tide:
        Next update at          : Wed Jan 11 14:00:26 2017
        Source                  : http://10.60.25.121/tide_ip.txt
        Referenced              : Yes
        Valid                   : Yes

        Total valid entries     : 803
        Total invalid entries   : 0
        Valid ips:
                87.71.240.178
                111.68.44.132
                213.224.2.178
                60.121.113.251
                46.238.27.15
                5.14.0.193
```

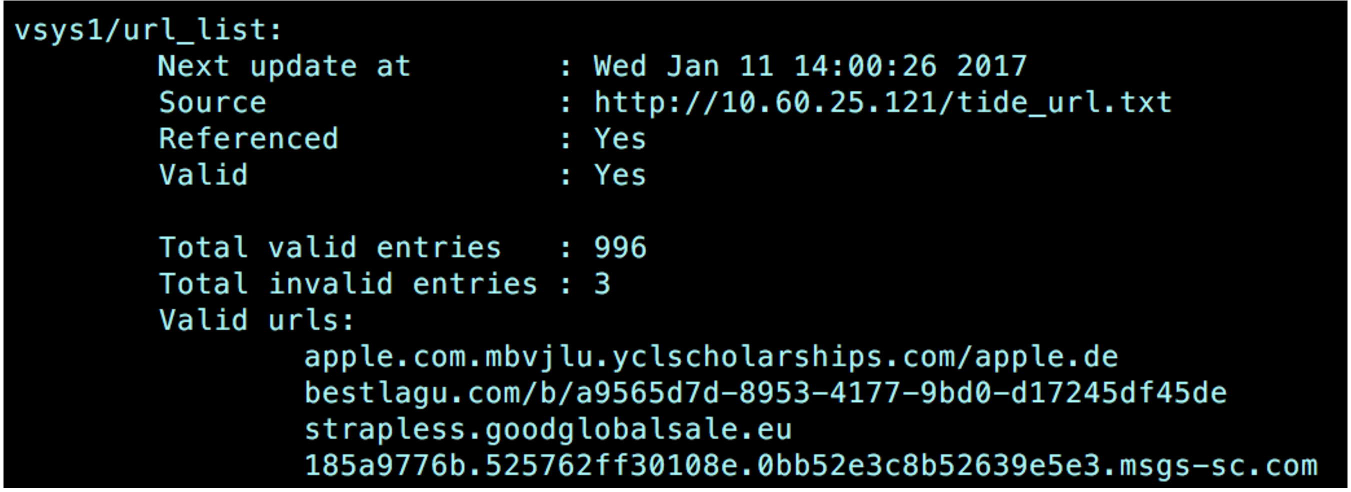
4. Run the following command to show the contents of the domain list:  request system external-list show type domain name <domain list name>.
5. The output should look like this:



```
vsys1/domain_list:
        Next update at          : Wed Jan 11 14:00:26 2017
        Source                  : http://10.60.25.121/tide_host.txt
        Referenced              : Yes
        Valid                   : Yes

        Total valid entries     : 1000
        Total invalid entries   : 0
        Valid domains:
                zzpyanerraticallyqozaw.com
                zzpyfordlinnetavox.com
                zzqallaabettingk.com
                zzqavinskycattederifg.com
                zzpxvinskycattederifg.com
```

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

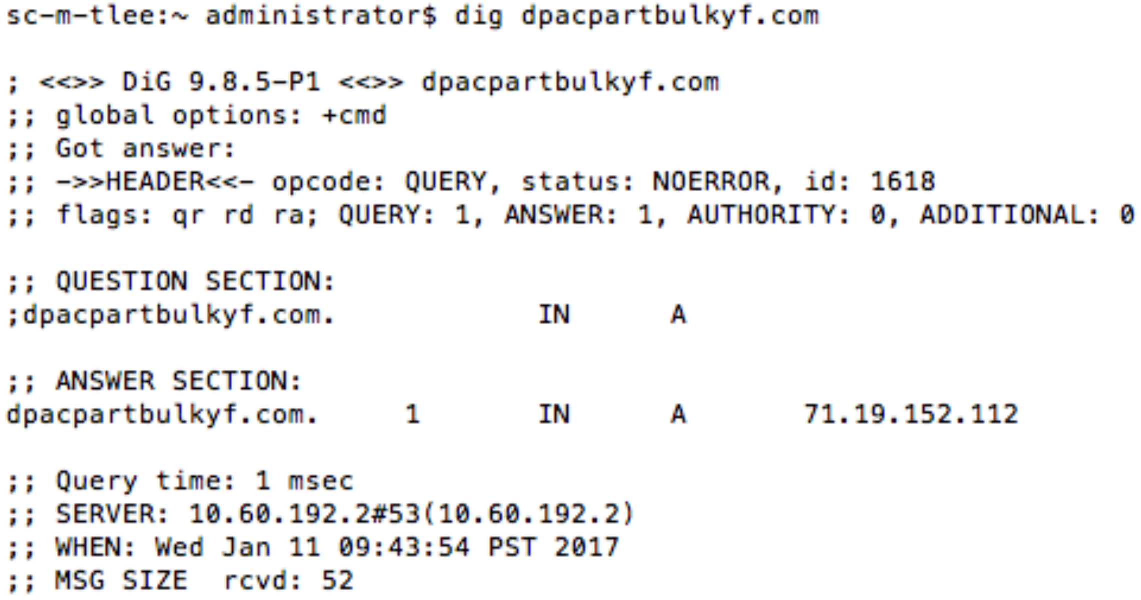
7. The output should look like this:



```
vsys1/url_list:
        Next update at        : Wed Jan 11 14:00:26 2017
        Source                : http://10.60.25.121/tide_url.txt
        Referenced            : Yes
        Valid                 : Yes

        Total valid entries   : 996
        Total invalid entries : 3
        Valid urls:
                apple.com.mbvjlu.yclscholarships.com/apple.de
                bestlagu.com/b/a9565d7d-8953-4177-9bd0-d17245df45de
                strapless.goodglobalsale.eu
                185a9776b.525762ff30108e.0bb52e3c8b52639e5e3.msgs-sc.com
```

## Test the Policies

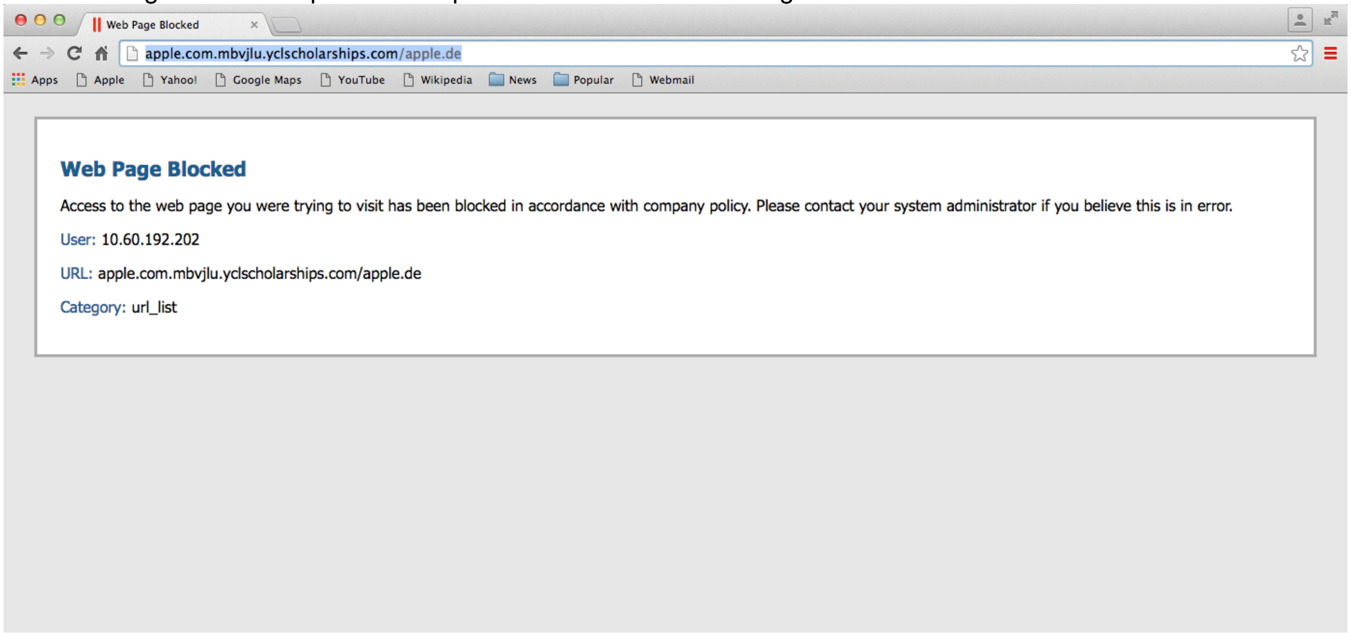
1. To test the IP list, run either ping on traceroute. You should not get any response from either command except for a timeout.
2. To test the domain list, run either nslookup or dig against an entry in the domain list.
3. You should get the following output. Notice the IP address? It is the default 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
```

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

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



**Web Page Blocked**

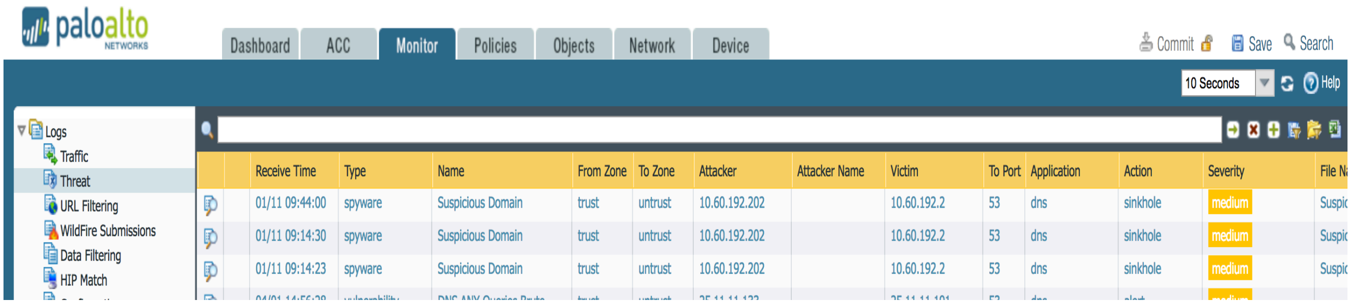
Access to the web page you were trying to visit has been blocked in accordance with company policy. Please contact your system administrator if you believe this is in error.

User: 10.60.192.202

URL: apple.com.mbvjlu.yclscholarships.com/apple.de

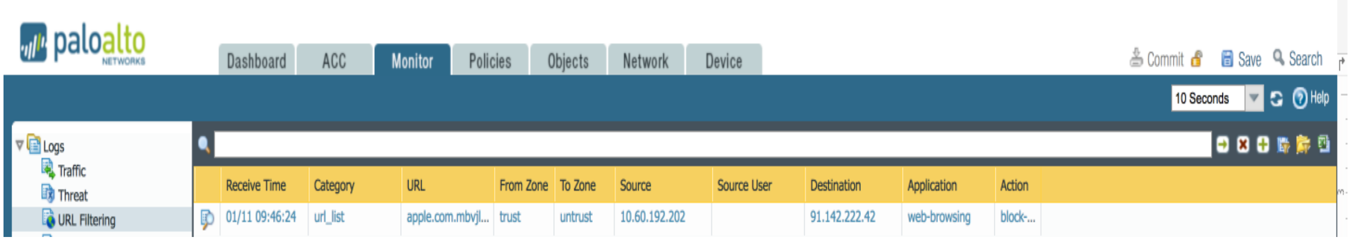
Category: url_list

6. Similarly, navigate to Monitor → Logs → Threat to see DNS sinkholing of a sinkholed domain.



| | Receive Time | Type | Name | From Zone | To Zone | Attacker | Attacker Name | Victim | To Port | Application | Action | Severity | File N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 01/11 09:44:00 | spyware | Suspicious Domain | trust | untrust | 10.60.192.202 | | 10.60.192.2 | 53 | dns | sinkhole | medium | Suspic |
| | 01/11 09:14:30 | spyware | Suspicious Domain | trust | untrust | 10.60.192.202 | | 10.60.192.2 | 53 | dns | sinkhole | medium | Suspic |
| | 01/11 09:14:23 | spyware | Suspicious Domain | trust | untrust | 10.60.192.202 | | 10.60.192.2 | 53 | dns | sinkhole | medium | Suspic |

7. Similarly, navigate to Monitor → Logs → URL Filtering to see the blocking of a URL in the URL block list.



| | Receive Time | Category | URL | From Zone | To Zone | Source | Source User | Destination | Application | Action |
|---|---|---|---|---|---|---|---|---|---|---|
| | 01/11 09:46:24 | url_list | apple.com.mbvjl... | trust | untrust | 10.60.192.202 | | 91.142.222.42 | web-browsing | block-... |