

DEPLOYMENT GUIDE

Implementing TIDE Feeds into Palo Alto Networks Firewalls

Table of Contents

Introduction	2
Infoblox Threat Intelligence Data Exchange Feeds	2
Requirements	2
Tested Hardware and Software	2
Sample Test Network for importing data feeds into Palo Alto firewall	3
Deployment Summary	3
Deployment Instructions	3
Obtain API Key from Infoblox's Cloud Services Portal	3
View TIDE filters and Generate API call	4
Use CURL to download feed(s) and modify the files for importing into Palo Alto firewall	4
Creating External Dynamic Lists	5
Create DNS Sinkholing entry for the domain list	6
Creating a URL Filtering entry for the URL List	8
Create the Security Policies	8
Showing the contents of each list	13
Test the Policies	15

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:
 - o Remove the quotes.
 - o Remove the field headers (i.e. IP, URL, host).
 - o Remove HTTP:// and HTTPS:// from the URLs.
 - o 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#<u>http://##g</u>' -e 's#<u>https://##g</u>'

Tested Hardware and Software

- Palo Alto Networks Firewall model 3020.
- PAN OS version 9.1.2.

Sample Test Network for importing data feeds into Palo Alto firewall



Infoblox TIDE website

Data Modifying Workstation

Palo Alto Networks 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 into the CSP at https://csp.infoblox.com
- 2. Upon logging in, hover over your username in the bottom-left corner and select User Preferences.



3. A popup will appear. 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.

API Keys	Show keys
edd3.ccor	

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 Filters" – You can use the "Apply Filters" 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, the select only the Data Type IP, then click on "Apply Filter", then click on Generate API Request.

Infoblex 💲 🧔	Apple Filter	5p. • 6	enerate API Recaent			Searcha		
Ed Manage E Policies M Reports Research Threat Lookup Desting	DATA TYPE Select all Ocar Escuel (0) Hash (0) Hash (0)	Generate A out & GET H	ilina Twara Typerio'	THRUT 00 80	i			
Active Indicators Resources	■ IF(159980) ■ URL(290240)	198.107.236.17	p	Palicy	Policy,NOCIEwst., 2025-021	24TOB. AISCOMM	80 80	
	THREAT CLASS/IPROVERTY Select all Cear > APT(SH69)	79.124.62.200 74.120.1447	р р	Scanner Scanner	Scanner,Generic 2023-02- Scanner,Generic 2023-02-	20116. ASCOMM	60 80	
	Bert (4003-4) CompromisedDomain (7) CompromisedHost (5382) CompromisedHost (5382)	220-58-245-101 220-191-237-31	р р	Palicy	Policy,NCCRwst., 2021-02- Policy,NCCRwst., 2021-02-	LTTOR: AISCOMM	80 80	
	SLoadmore	222.04.516.77	P	Palicy	Policy,NOCICNet., 2021-024	24T07 ASCOMM	00 80	
	Select al Clear ASCOMMI (2004) Exerciping/Treases (141292) Finisht/Security (2312000) Infolioas (2008204) Staffits (2302000)		-				Page 5	2.800

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

Creating External Dynamic Lists

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

paloalto	Dashboard ACC Monitor	Policies Objects Network [Device	🏝 Commit 💰 🔋 🗟 Save 🔍 Search
				Manual 🔽 😋 🔞 Help
Addresses	٩			3 items 🍯 🗙
Address Groups Regions	Name	Location Description	Source	Frequency
Applications				
Application Groups	domain_list		http://10.60.25.121/tide_host.bt	Hourly
Services	V Dynamic IP Lists			
Tags	ip_tide		http://10.60.25.121/tide_ip.txt	Hourly
V 🔇 GlobalProtect				
SHIP Objects	url_list		http://10.60.25.121/tide_url.txt	Hourly
🖲 External Dynamic Lists				

- 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.

External Dynamic Li	sts 💿
Name	
Туре	IP List
Description	
Source	http://
Repeat	Hourly
Test Source URL	OK Cancel

4. Click on the Commit button.

Create DNS Sinkholing entry for the domain list

1. Navigate to Objects \rightarrow Security Profiles \rightarrow Anti-Spyware.

V Security Profiles	1	sinkhole2		Rules: 4	simple-critical	any	critical	default	disable	disable
🐝 Antivirus	1				simple-high	any	high	default	disable	
Anti-Spyware					simple-medium	any	medium	default	disable	
Vulnerability Protection					simple-low	any	low	default	disable	
Ge URL Filtering		active trust domain list		Rules: 4	simple-critical	any	critical	default	disable	disable
WildFire Analysis					simple-high	any	high	default	disable	
Data Filtering					simple-medium	any	medium	default	disable	
Dos Protection					simple-low	any	low	default	disable	
Schedules										
	÷	Add 🖃 Delete 📧	Clone							

- 2. Click Add or Clone to create an entry.
 - I. Enter or modify the name.

II. Optionally, enter a description.

Anti-Spyware Profile				(0 🗆
Name	active trust d	lomain list			
Description					
Rules Exceptions	DNS Signa	atures			
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	
🕈 Add 🕞 Delate	C Move Up	🕽 Move Down 🛛 📀 Clone 🔍 Find Matching Sig	inatures		
				OK Cancel	

- 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.

	Name	active trust don	nain list							
	Description									
Rules	Exceptions	DNS Signatu	res							
Ex	ternal Dynamic	List Domains	Action o	on DNS Queries		Threat ID Exceptions				
Pa	lo Alto Network gnatures	s DNS	sinkhole	2		•	_		0 items	•
do	omain_list		sinkhole	9		Threat ID		Threat Name		
+ Add	d 🕒 Delete Sinkhole IPv4 🖡	alo Alto Network	s Sinkhole	e IP (71.19.152.112)	~					
€ Add S S	d Delete Sinkhole IPv4 [Sinkhole IPv6]	'alo Alto Network: Pv6 Loopback IP	s Sinkhole (::1)	9 IP (71.19.152.112)	*					
S Par	d Delete Sinkhole IPv4 F Sinkhole IPv6 J cket Capture	'alo Alto Network: Pv6 Loopback IP lisable	s Sinkhole (::1)	₂ IP (71.19.152.112)	*					
€ Add S S Par	d Delete Sinkhole IPv4 F Sinkhole IPv6 J cket Capture	Palo Alto Networks Pv6 Loopback IP lisable Enable Passive	s Sinkhole (::1) DNS Mor	• IP (71.19.152.112) hitoring	* *	Threat ID	0	Add 🗨 Delete		

3. Click on the Commit button.

Creating a URL Filtering entry for the URL List

1. Navigate to Objects \rightarrow Security Profiles \rightarrow URL Filtering.

URL Filtering			0	auctions business-and-economy computer-and-internet-info more		
Bos Protection Scourity Profile Groups Log Forwarding Occupation Profile Schedules	active trust un test	alert	abortion abused-drugs adult alcohol-and-tobacco auctions business-and-economy computer-and-internet-info		url_list +	
			more			
	🛨 Add 🔳 Delete 🚳 Clone					

- 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.

	Name	active trust url test			
	Description				
Categories	Settings				
Block List				ip	66 items 🔿 🗙
				Category	Action
				swimsuits-and-intimate-apparel	allow
				training-and-tools	allow
Action	alert	•		translation	allow
				travel	allow
Allow List				unknown	allow
				weapons	allow
				web-advertisements	allow
				web-based-email	allow
				web-hosting	allow
	For the block list and allow list with a newline. Each entry sho	enter one entry per row, separating the rows uld be in the form of "www.example.com"	V	url_list +	block
	and without quotes or an IP at included). Use separators to sp "www.example.com/" will mat "www.example.com.hk"	ddress (http:// or https:// should not be becify match criteria - for example, ch "www.example.com/test" but not match	* ind Che	icates a custom URL category, + indicates externa ack URL Category	ıl dynamic list

3. Click on the Commit button.

Create the Security Policies

- 1. Navigate to Policies \rightarrow 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 Po	olicy Rule	3/11 - 100						0		
General	Source	User	Destination	Application	Service/URL Category	Actions				
	Name IP-List-1									
	Rule Type	universal (default)					V		
D	Description									
	Tags							▼		
							ОК	Cancel		

- V. Click on the Source tab.
- VI. Add a Source Zone. In this example, the trust zone is entered.

Security Po	olicy Rule						
General	Source	User	Destination	Application	Service/URL Category	Actions	
🔲 Any					🗹 Any		
Source	ce Zone 🔺				Source Address		
🔲 🕅 ti	rust						
🕂 Add	😑 Delete				🕂 Add 🗖 Delete		
					Negate		
							OK Cancel

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.

Security Po	olicy Rule						0			
General	Source	User	Destination	Application	Service/URL Category	Actions				
select		~			Any					
🔲 Desti	nation Zone	A			Destination Address	; 🔺				
🔲 🕅 u	intrust				🔲 🔙 ip_tide					
Add	Doloto				Add Dalata		_			
Auu			-		+ Add Delete					
					Negate					
	_						OK Cancel			

IX. Click on the Actions tab.

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

Security Po	olicy Rule						0
General	Source	User	Destination	Applicat	ion	Service/URL Category	Actions
Action	Setting					Log Setting	
	Ac	tion	Drop			Log at Session Start	
		(Send ICMP Unro	eachable			Log at Session End
Profile	Setting					Log Forwarding	None
	Profile T	ype	Profiles			Other Settings	
	Antiv	irus	default			Schedule	None
Vulne	erability Protec	tion	default			QoS Marking	None
	Anti-Spyw	are	None		▼		Disable Server Response Inspection
	URL Filte	ring	None		▼		
	File Block	king	None		▼		
	Data Filte	ring	None		▼		
	WildFire Anal	ysis	default		▼		
							OK Cancel

- 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.

Security Po	olicy Rule						0		
General	Source	User	Destination	Application	Service/URL Category	Actions			
🔲 Any					🗹 Any				
Source	e Zone 🔺				Source Address 🔺				
🔲 🎮 tr	rust								
Add	🗖 Delete				🕂 Add 🗖 Delete		_		
					Negate				
							OK Cancel		

- VI. Click on the Destination tab.
- VII. Add a destination zone. In this example the untrust zone is entered.

General	Source	User	Destination	Application	Service/URL Category	Actions	
select					Nov.		
Desti	nation Zone				Destination Address		
	otruct						
i jed n	nuusi						
	nuusi						
	nuusi						
	nu usi						
	nu usu						
	nu usu						
Add	Delete				Add ■ Delete		
Add	Delete				Add Delete Negate		

- VIII. Click on the Actions tab.
- IX. Select allow for the action setting to allow.

Χ.	Select the entr	v for the	Anti-Spyware	and URI	Filtering.
/ .		y 101 ti 10	/ and opymano		i ntoring.

Security Po	licy Rule							0
General	Source	User	Destination	Application	Service/URL Category	Actions		
Action	Setting				Log Setting			
Action Allow]	🗹 Log at Se	ssion Start	
			Send ICMP Unr	eachable		🗹 Log at Se	ssion End	
Profile	Setting				Log Forwarding	None		•
	Profile	Туре	Profiles		Other Settings			
	Anti	ivirus	default	~	Schedule	None		
Vulne	erability Prote	ection	default	~	QoS Marking	None		
	Anti-Spy	ware	active trust domain	list 💌		Disable S	erver Response Inspect	ion
	URL Filt	ering	active trust url test	~				
	File Blo	cking	None	~				
	Data Filt	ering	None	~				
	WildFire Ana	alysis	default	~				
							OK Can	cel

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:

<pre>vsys1/ip_tide:</pre>		
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:		
zzpyanerratica	aľ	lyqozaw.com
zzpyfordlinnet	a	vox.com
zzqallaabettir	ngl	k.com
zzqavinskycatt	e	derifg.com
zzpxvinskycatt	e	derifg.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.mbv;	jl	u.yclscholarships.com/apple.de									
bestlagu.com/)/a	a9565d7d-8953-4177-9bd0-d17245df45de									
strapless.good	strapless.goodglobalsale.eu										
185a9776b.525	76	2ff30108e.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.
- 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
                                        А
;; ANSWER SECTION:
dpacpartbulkyf.com.
                        1
                                IN
                                        А
                                                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.



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

paloalto	[Dashboard	ACC Mo	nitor Policie	s Objects	Network	Device					🏝 Com	nit 💣 🖥 Save	9, Search
_													10 Seconds 💌	😋 🔞 Help
	٩												→ × +	🛯 🖏 🖗
Threat		Receive Time	Туре	Name	From	Zone To Zone	Attacker	Attacker Name	Victim	To Port	Application	Action	Severity	File Ni
URL Filtering	Þ	01/11 09:44:0	0 spyware	Suspicious Doma	in trust	untrust	10.60.192.202		10.60.192.2	53	dns	sinkhole	medium	Suspic
WildFire Submissions	Þ	01/11 09:14:3	0 spyware	Suspicious Doma	in trust	untrust	10.60.192.202		10.60.192.2	53	dns	sinkhole	medium	Suspic
Data Filtering	Þ	01/11 09:14:2	3 spyware	Suspicious Doma	in trust	untrust	10.60.192.202		10.60.192.2	53	dns	sinkhole	medium	Suspic
	B	04/01 14/50/0	0	DAIC ANY Ounde	Dauka karak	contra out	25 11 11 122		35 11 11 101	52	dan	alast		

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

paloalto		Dashboard	ACC	Monitor Poli	cies	Objects	Network	Device				🍰 Commit 💰 📑 Save 🔍 Search	ľ
												10 Seconds 🔻 😌 🕑 Hel	p -
▼ 🗟 Logs	٩											🕀 🗶 🕀 🛤 🎥	i -
Traffic		Receive Time	Category	URL	From Zone	To Zone	Source	Source User	Destination	Application	Action		m.
QURL Filtering	Þ	01/11 09:46:24	url_list	apple.com.mbvjl	trust	untrust	10.60.192.202		91.142.222.42	web-browsing	block		



Infoblox is the leader in modern, cloud-first networking and security services. Through extensive integrations, its solutions empower organizations to realize the full advantages of cloud networking today, while maximizing their existing infrastructure investments. Infoblox has over 12,000 customers, including 70 percent of the Fortune 500.

in f y D

Corporate Headquarters | 2390 Mission College Boulevard, Ste. 501 | Santa Clara, CA | 95054 +1.408.986.4000 | info@infoblox.com | www.infoblox.com

© 2021 Infoblox, Inc. All rights reserved. Infoblox logo, and other marks appearing herein are property of Infoblox, Inc. All other marks are the property of their respective owner(s).