USER GUIDE V1.0.0

SlashNext Threat Intelligence Integration Guide PAN-OS Firewall

1	EXTERNAL DYNAMIC LISTS (EDL)	2
2	EDLS IN PAN-OS FIREWALL	2
	Creating an EDL of type IP addresses	2
	Creating an EDL of type Domains	4
	Creating an EDL of type Wildcard URLs	5
3	POLICIES IN PAN-OS FIREWALL	5
	Creating a Policy based on IPs EDL	5
	Creating a Policy based on Domains EDL	7
	Creating a Policy based on Wildcard URLs EDL	10
4	RESULTS	12
5		14

1 | EXTERNAL DYNAMIC LISTS (EDL)

An External Dynamic list is a text type of file hosted on an external web server. A firewall can import objects such as IP Addresses, Domain names and URLs from the EDL and enforce the required policies on the incoming traffic. The EDL can be modified in real-time and the firewall is able update its policies correspondingly. In case the EDL becomes unreachable due to network issues, the firewall uses the most recently imported EDL. Thus EDLs provide a convenient way to enforce network policies on a firewall without manual labor. The Palo Alto Networks Firewall supports four different types of EDLs:

- 1. IP Address: The policy can be applied for a source or destination IP address present as a static object in the EDL.
- 2. Predefined IP Address: A predefined IP address list is referred to the Palo Alto Networks Malicious IP Address Feeds.

These feeds can be used to enforce policies on the network traffic if you have an active Threat Prevention license.

- 3. **Domain:** An EDL of domain type can be used to import custom domain names to enforce a network policy based on an Anti-Spyware profile.
- 4. URL: An external dynamic list of URL type can be used to filter the network traffic from malicious URLs.

2 | EDLS IN PAN-OS FIREWALL

Below we elaborate on how to create EDLs of all the above mentioned types.

2.1 | CREATING AN EDL OF TYPE IP ADDRESSES

Log into Palo Alto Networks Firewall by typing your username and password.

Username Password	Log In
Figure 1: Login to PAN-OS Firewall managem	ient portal

Click on **Objects** from the top menu-bar and **External Dynamic Lists** option from the left menu. Click on **Add** button from the bottom menu-bar to create a new EDL.

, paloalto									
NETWORKS'	Dashboard ACC	Monitor Polici	es Objects	Network	Device			🏯 Commit 💰 🔰 Co	ntig - Q Search
	_							Manual	💌 🖸 🔞 Help
Sa Addresses	۹.								0 items 📑 🗙
Address Groups	Name 🔺	Location	(1)	Description		Source	Certificate Profile	Frequency	
Regions			$\overline{}$						
Application Groups									
Application Filters									
X Services									
Service Groups									
🎨 Tags									
V ClobalProtect									
HIP Objects									
Conternal Demonstration									
T Custom Objects									
Data Patterns									
Spyware									
Vulnerability									
URL Category									
V Security Profiles									
Antivirus									
Anti-Spyware									
Vulnerability Protection									
Eie Blocking									
WidFire Analysis									
🔒 Data Filtering									
EDoS Protection									
Construction Security Profile Groups									
Log Forwarding									
12 Authentication	3								
Decryption Decryption	1ī								
Schedules									
and southeaters a	♥								
	AM Debte Stars	EDDEUNSV 🔔 konnert Now 🔽 Li	et Canacities						
admin Langet Last Lonin Time: DR/11	U2019 1841 20							= 1	Tarks Language
amen 1 Third 1 rear collecture: nov 11	12010-10/11/20								20 uaxo 1 raubrate
Figure 2: Steps to crea	ite a new EDL in PAN	I-OS Firewall							

A new dialog box to create the EDL will open up. Type the desired **Name** and **Description**. Select **IP List** as the type of the new EDL from the Type drop-down menu. Use the SlashNext Plaintext type feed for Phishing IPs pointed to by:

Important Note

Please note that if the user wants to use MineMeld output for the EDL, use the FEED BASE URL from output node for IP intel here instead of the above SlashNext threat intelligence API here.

Finally select **Hourly** option from the Repeat drop-down menu which refers to the update interval at which the EDL retrieves the feed from SlashNext endpoint and updates itself. You can also click on **Test Source URL** to verify the status of the source used for the new EDL.

External Dynamic Lis	ts
Name	SlashNextIntel-PhishingIPs-EDL
Create List List	Entries And Exceptions
Туре	IP List
Description	External Dynamic List for SlashNext Phishing IPs feed.
0	
Source	https://intel.slashnext.cloud/api/intel/ips?authkey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Server Authentica	tion
Certificate Profi	e None 💌
Repeat	Hourly
Test Source URL	OK
igure 3: Configur	ation settings for SlashNext Phishing IPs EDL

Click on the List Entries And Exceptions menu from the top menu-bar to see all the entries of the EDL fetched from the selected feed source. Please note that at this point, the List Entries will be empty and an EDL in PAN-OS Firewall is only updated if it is used in at-least one Policy so, you have to create a new policy using this newly created EDL. Click on **OK** to finish the creation of EDL. In section 3, we explain how to create policies based on different types of EDLs created in this section.

2.2 | CREATING AN EDL OF TYPE DOMAINS

Similarly we create an EDL for malicious domains provided by SlashNext domains feed according to the settings shown in Figure 4.

External Dynamic List	IS	0
Name s	SlashNextIntel-PhishingFQDNs-EDL	
Create List List	Entries And Exceptions	
Туре	Domain List	V
Description	External Dynamic List for SlashNext Phishing Domains feed.	
Source	https://intel.slashnext.cloud/api/intel/domains?authkey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx	xx
Server Authentica	tion	
Certificate Profile	e None	r
Repeat	Hourly	
Test Source URL	OK	
Figure 4: Configure	ation settings for SlashNext Phishing Domains EDL	

The Type of the EDL in this case is selected to be **Domain List** and the Source URL is given as:

Important Note

Please note that if the user wants to use MineMeld output for the EDL, use the **FEED BASE URL** from output node for FQDN intel here instead of the above SlashNext threat intelligence API here.

2.3 | CREATING AN EDL OF TYPE WILDCARD URLS

Finally, we create an EDL to cater Widlcard URLs from SlashNext Wildcard URLs feed. The source of the EDL is given to be as:

() Important Note

Please note that if the user wants to use MineMeld output for the EDL, use the **FEED BASE URL** from output node for wildcard URL intel here instead of the above SlashNext threat intelligence API here.

External Dynamic Lists 💿
Name SlashNextIntel-PhishingWildcardURLs-EDL
Create List List Entries And Exceptions
Type URL List
Description External Dynamic List for SlashNext Phishing Wildcard URLs feed.
Source https://intel.slashnext.cloud/api/intel/wildcardurls?authkey=xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Server Authentication
Certificate Profile None
Repeat Hourly
Test Source URL OK Cancel
igure 5: Configuration settings for SlashNext Phishing Wildcard URLs EDL

3 | POLICIES IN PAN-OS FIREWALL

In this section we explain the procedure to create different policies to block malicious traffic, based on the EDLs created in the previous section.

3.1 | CREATING A POLICY BASED ON IPS EDL

Click on **Policies** from the top menu-bar and select **Security** from the left menu then, click on the **Add** button from the bottom menu-bar to create a new policy based on IPs EDL.

paloalto	Dashboard ACC	Monitor Polici	es Objec	ts Network	Device					& Con	ımit 💰 🎑 Contig 🕶 🔍 S	learch
		4									0	() Help
📾 Security 🗲 🔁												
NAT		~				Source		D	estination		Rule Usage	
Policy Based Forwarding	Name	Tags	Туре	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First Hit
d Decryption	1 Forward	none	interzone	(M) Trusted	any	any	any	(20) NonTrusted	any	1689	2019-06-11 21:40:34	2019-05
Application Override	2 Reverse	none	interzone	(M) NonTrusted	any	any	any	(22) Trusted	any	334356	2019-06-11 21:43:44	2019-05
& Authentication	3 intrazone-default	 none 	intrazone	any	any	arry	any	(intrazone)	arry	0		
DoS Protection	4 interzone-default	 none 	interzone	any	BOY	any	алу	my	any	0		
Tag Browser												
Fiber by first tag in rule Rule Order Alphabetical Dibject : Addresses		ends 🍨 Reset. 🖾 Dabb	Charles Mo	wa • 🏘PDF/CSV	Highlight Urus	d Rules Reset Rule	Hit Counter •		_	_		
and a manager of control of the own that												

Figure 6: Steps to create a new policy in PAN-OS Firewall

SLASHNEXT THREAT INTELLIGENCE INTEGRATION GUIDE PAN-OS FIREWALL | USER GUIDE 1.0.0

A new dialog box by the name **Security Policy Rule** will open up. In the **General** tab, select a suitable name for your policy.

Security Po	Security Policy Rule												
General	Source	User	Destination	Application	Service/URL Category	Actions							
Name SlashNextIntel-PhishingIPs-Policy													
	Rule Type	universal (default)					-					
D	escription												
	lags												
								Cancel					

Then go to the **Source** tab and check **Any** checkbox for **Source Zone** and **Source Address** panel. This means that you are applying no filter on outgoing traffic from your network.

Security Po	olicy Rule					0
General	Source	User	Destination	Application	Service/URL Category	Actions
🗹 Any					🗹 Any	
Source	e Zone 🔺				Source Address 🔺	
🗭 Add	Delete				🗭 Add 🛛 🗖 Delete	
					Negate	
						OK Cancel

Now go to the **Destination** tab and select **any** option from the drop-down list in the **Destination Zone**. In the **Destination Address** panel, select the Phishing IPs EDL created in the previous sections. By doing so, you are restricting the users on your network to access anything on the internet that is malicious and present on our Phishing IPs EDL.



Finally, go to the **Actions** tab to select the desired action in case the firewall detects any packet that is coming from a source marked as malicious in our IPs EDL. In our case we want to deny any such traffic so select **Deny** from the **Action** drop-down list. For a complete understanding of different actions, please refer to Security Policy Actions. Click **OK** to save our newly created policy.

Security Policy Rule			0
General Source Us	er Destination Application	Service/URL Category Actions	
Action Setting Action	Deny Allow Drop	Log Setting Log at Session V Log at Session Log Forwarding None	n Start n End
Profile Setting Profile Type	Reset client Reset server Reset both client and server None	Other Settings Schedule None QoS Marking None	Pasponea Inspaction
			OK Cancel

3.2 | CREATING A POLICY BASED ON DOMAINS EDL

To blocks access to malicious domains, first we need to create an Anti-Spyware profile based on our previously create EDL. This profile can then be attached in a security policy to enforce the necessary restrictions. PAN-OS Firewall also allows DNS Sinkholing for malicious domains to a Palo Alto Networks' or a user defined sinkhole server.

Let us first create an Anti-Spyware profile based on malicious domains EDL. Go to the **Objects** tab and select **Anti-Spyware** from the **Security Profiles** sub menu on the left as shows in Figure 7.

paloalto		Dashboa	ard ACC	Monitor	Policies Object	ts Netwo	rk Device				🍰 Commit 💣 👰 Config = 🔍 Search
					4						S ())ie
San Addresses	•					_					2 items 🖃
Regions	E	Name	Location	Count	Rule Name	Threat Name	Severity	Action	Packet Capture	DNS Packet Capture	
Application Groups	E	detauit	Predefined	Rules: 4	simple-critical	any	critical	default	disable	disable	
Application Filters					simple-high	any	high	default	disable		
1 Services					simple-medium	any	medium	default	disable		
Service Groups					simple-low	any	low	default	disable		
Tags .	E	strict	Predefined	Rules: 5	simple-critical	any	oritical	reset-both	disable	disable	
GlobalProtect					simple-high	any	high	reset-both	disable		
HIP Objects					simple-medium	any	medium	reset-both	disable		
HIP Profiles					simple- informational	any	informational	default	disable		
External Dynamic Lists					simple-low	any	low	default	disable		
Constantiants Constan	-2)] ↓									
Schedules	1	Add 🖬 🖬	enn 🥘 Clare 🛛 💏 POF/	CSV Threat Pr	evention License required to	x artivirus, arti-spyw	are, and vulnerability p	rotection to function.			
min Loopet Last Looin Time: 05/	11/201										📼 🚟 Tasis Lanua
and the second se		100000000									- 1 . 1 mar

Figure 7: Steps to create a new Anti-Spyware profile

A new dialog box by the name of Anti-Spyware Profile will open up. Add a friendly name for the profile and then click on the **DNS Signatures** tab. Click on the **Add** button to select our Phishing Domains EDL from the drop-down list. Select the appropriate **Action on DNS Queries** option according to your own need. In this case, we can simply block the malicious domains. Click on **OK** to finally save the new profile.

	Name Description	SNXIntel-Phis	hingFQDNs-Profile			
Rules	Exceptions	DNS Signat	ures			
Ext	ernal Dynamic	List Domains	Action on DNS Queries		•	0 items 📑 😫
Pal	o Alto Network natures	s DNS	sinkhole		DNS Threat ID Exceptions	Threat Name
Sla ED	Delete	ishing FQDNs-	block alert allow block sinkhole	-		
SI	nkhole IPv4	Palo Alto Networ	ks Sinkhole IP (72.5.65.111)	Ŧ		
Pac	ket Capture	Pv6 Loopback II lisable	9 (::1)	*	DNS Threat ID	🗣 Add 🖨 Delete

Next, we go the **Policies** tab to create a new policy for malicious domains. After selecting a suitable name for your policy in the **General** tab, go to the **Source** tab and check the **Any** checkbox for both **Source Zone** and **Source Address**.

Security Policy Rule	0
General Source User Destination Application Service/URL Category Actions	
🗾 Any	
Source Zone 🔺 🖉 Source Address 🔺	
	_
wegate	
ОК	Cancel

Similarly, for the Destination we select the Any option for both Destination Zone and Destination Address.

Security Policy Rule	0
General Source User Destination Application	Service/URL Category Actions
any	Any
any	Destination Address
select	
🛨 Add 🛛 🗖 Delete	🛨 Add 🗖 Delete
	Negate
	OK

Finally, go to the **Actions** tab and from the **Profile Setting** pane, choose **Profiles** as the **Profile Type** from the drop-down list.

Security Policy Rule					0
General Source Us	er Destination	Application	Service/URL Category	Actions	
Action Setting			Log Setting		
Action	Allow	-		Log at Session Start	
	Send ICMP Unre	achable		Log at Session End	
			Log Forwarding	None	~
			Other Settings		
Profile Setting			Schedule	None	V
Profile Type	None	~	QoS Marking	None	V
	Profiles			Disable Server Response Inspecti	on
	Group				
				ОК Сал	cel

Some further options will appear in the **Profile Setting** pane. Select the recently created Anti-Spyware profile from the **Anti-Spyware** drop-down list. Finally, click on OK to save the malicious domains policy.

General	Source	Use	r Destination	Applicatio	n	Service/URL Category	/ Actions	
Action S	etting					Log Setting		
	А	ction	Allow		•		Log at Session Start	
			Send ICMP Unr	eachable			Log at Session End	
Profile S	etting					Log Forwarding	None	•
	Profile	Туре	Profiles		~	Other Settings		
	Antivirus	None			•	Schedule	None	Ŧ
v	ulnerability	None			-	QoS Marking	None	-
	Protection						Disable Server Response Inspection	on
An	ti-Spyware	None			-			
UF	RL Filtering	None defaul	t					
Fi	le Blocking	SNXI	tel-PhishingFQDNs	s-Profile				
Da	ata Filtering	strict			_			
WildFi	re Analysis	New	💭 Anti-Spyware					

3.3 | CREATING A POLICY BASED ON WILDCARD URLS EDL

PAN-OS firewall also supports direct protection against malicious URL via a URL Filtering profile based on our URL EDLs. These URL Filtering profiles can then be used to create a new policy to block malicious traffic. Therefore, let us first create profiles Wildcard URL EDLs to be later used in creating policies.

Go to Objects \rightarrow Security Profiles \rightarrow URL Filtering and click on the Add button present at the bottom as demonstrated by Figure 8.

paloalto	Dashboard	ACC Monitor	Policion	Notwork	Dovice			🔹 Commit 🥒 🎯 Config = 🙆 Search
NETWORKS*	Dashboard	AGG Monitor	Policies		Device			S OHelp
Addresses	٩		(1 item 🔿 🗙
Address Groups	Name	Location	Block List	Action for Block List	Allow List	Site Access	User Credential Submission	HTTP Header Insertion
Applications Application Groups Application Filters Services Service Groups Tans	m default	Predefined		block		Allow Categories (57) Alert Categories (0) Continue Categories (0) Block Categories (9) Override Categories (0)	Allow Categories (66) Alert Categories (0) Continue Categories (0) Block Categories (0)	
GlobalProtect								
Custom Objects Data Patterns Spyware Vulnerability URL Category								
▼ 3 Security Profiles Antivirus Anti-Spyware Vulnerability Protection								
URL Filtering								
Security Profile Groups Log Forwarding Authentication Oecryption Decryption Profile Schedules	3 ↓ Add ■ Delete €) Clane 🙀 PDF/CSV Lic	ense required for URL Filterin	g to function (* indicates custor	n URL category, + indicat	es external dynamic list)		
Figure 8: Steps to cre	eate a new URI	L Filtering profile	2					

Use a suitable name for the Profile and select our Phishing Wildcard URLs EDL from **Category** list in the **Categories** tab. Finally, select suitable action for the firewall to take from the drop-down list under **Site Access** as show in Figure 9.

Name SN. Description	XIntel-Phishir	ngWCURLs-Profile					
ategories Overrides URL Filterin	g Settings	User Credential Detection	HTTP Header Inser	rtion			
٩	_			_	_	68 items	- ×
Category						User Credenti Submission	
Translation				allow		allow	
T travel				allow		allow	
m unknown				allow		allow	
weapons				allow		allow	
web-advertisements				allow		allow	
web-based-email				allow		allow	
web-hosting				allow		allow	
				allow		allow	
SlashNextIntel-PhishingWildcardURL	s-EDL +			allow	v	allow	
indicates a custom URL category, + indicates exte	rnal dynamic list	t		alert			
Check URL Category				allow			
				block			
				continue			
				override		OK	Cancel

Figure 9: Configuration Settings for Wildcard URLs Profile

Finally, we can use our recently created URL Filtering Profiles in creating a new policy. Go to **Policies** \rightarrow **Security** and click on **Add** to create a new policy.

Select a suitable name and use the **Any** option for both **Source** and **Destination** as done in Section 3.2 Next, select **Profiles** from the **Profile Type** drop-down list in **Profile Setting** pane. In the URL Filtering option, select the recently created URL Filtering Profile and click on **OK** to create the new policy.

ieneral Source	Use	er Destination	Applicatio	on	Service/URL Category	/ Actions	
Action Setting					Log Setting		
	Action	Allow		-		Log at Session Start	
		Send ICMP Ur	nreachable			Log at Session End	
Profile Setting					Log Forwarding	None	•
Profil	е Туре	Profiles		~	Other Settings		
Antivirus	None			-	Schedule	None	-
Vulnerability	None			-	QoS Marking	None	-
Protection						Disable Server Response Inspec	tion
Anti-Spyware	None			•			
URL Filtering	SNXI	ntel-PhishingWCU	RLS-Profile	-			
File Blocking	None	dr.					
Data Filtering	uciau						
WildFire Analysis	SNXI	ntel-PhishingWCU	RLs-Profile				
	New	URL Filtering					

Once you are done creating all the policies and objects, click on the **Commit** button to deploy all the changes on the firewall as shown in Figure (Please note that it is recommended to commit after making any substantial change in your firewall configurations. To maintain the continuity of this document, we committed the configurations in the end only).

												9	Help
Security	•											7 item	0
Se NAT													
Policy Based Forwarding		Name	Tags	Туре	Zone	Address	User	HIP Profile	Zone	Address	Hit Count	Last Hit	First
Decryption Decryption Competition Application	1	Forward	none	interzone	(#R Trusted	any	any	any	(IN) NonTrusted	any	1740	2019-06-12 19:23:38	2019-
	2	Reverse	none	interzone	FR NonTrusted	any	any	any	pag Trusted	any	349704	2019-06-12 19:58:36	2019-
& Authentication	3	SlashNextIntel-PhishingIPs-Policy	none	universal	any	any	any	any	any	SlashNextIntel	+	*	-
DoS Protection	4	SlashNextIntel-PhishingFQDNs-Policy	none	universal	any	any	any	any	any	any			
	5		none	universal	any	any	any	any	any	any			
	6	SlashNextIntel-PhishingWildcardURLs-Po	none	universal	any	any	any	any	any	any			
	7	intrazone-default	none	intrazone	any	any	any	any	(intrazone)	eny	0		*
	8	interzone-default	none	interzone	any	any	any	any	any	any	398	2019-06-12 19:57:21	2019-0
ag Browser													

A dialog bar showing the progress and Status of your commit will appear on the screen. Once the configurations are successfully committed, the dialog box will look something like this (Ignore all the warnings at the moment).



4 | RESULTS

Once the policies are deployed, you can see the EDLs getting updated as they fetch data from SlashNext Threat Intelligence Platform feeds. These List entries will keep on updating as new items are fetches.

Go to **Objects** \rightarrow **External Dynamic Lists** and click on one of the EDLs. Then go to **List Entries And Exceptions** tab to see the **List Entries** as shown in Figure 10, 11, and 12.

External Dynamic Lists				0
Name SlashNextIntel-PhishingIPs-EDL	4			
Create List List Entries And Exceptions				
List Entries		Manual Exceptions		
€86 items		•	0 ite	ms 🔿 🗙
List Entries		List Entries		
178.62.243.240/32				
104.248.191.14/32				
159.65.11.18/32				
138.197.150.225/32	_			
18.209.247.231/32	→			
68.183.190.222/32				
178.128.192.204/32				
139.59.216.126/32				
37.44.212.2/32				
157.230.64.150/32		🕂 Add 🔲 Delete		
Test Source URL			ОК	Cancel

Figure 10: List Entries of IPs EDL



Figure 11: List Entries of Domains EDL



Figure 12: List Entries for Wildcard URLs EDL

5 | TROUBLESHOOTING

You might face an error while committing your changes to the firewall as shows in Figure 13.

Commit Status	• •
Operation	Commit
Status	Completed
Result	Failed
Details Warnings	Warning: No Valid Threat License vsy1 Warning: Rule 'SlashNext-URLs-Policy': No valid URL filtering license, Security Policy: Rule 'SlashNext-FQDNs-Policy' shadows rule 'SlashNext-URLs-Policy' Rule 'SlashNext-FQDNs-Policy' shadows rule 'SlashNext-URLs-Policy' Rule 'SlashNext-FQDNs-Policy' shadows rule 'SlashNext-WildcardURLs-Policy' Rule 'SlashNext-GDNs-Policy' shadows rule 'SlashNext-WildcardURLs-Policy' Rule 'SlashNext-URLs-Policy' shadows rule 'SlashNext-WildcardURLs-Policy' Rule 'SlashNext-URLs-Policy' shadows rule 'SlashNext-WildcardURLs-Policy' Rule 'SlashNext-URLs-Policy' shadows rule 'SlashNext-WildcardURLs-Policy' Rule 'SlashNext-WildcardURLs-Policy' shadows rule 'SlashNext-WildcardURLs-Policy' Policy' SlashNext-WildcardURLs-Policy' Policy' SlashNext-WildcardURLs-EDL url) Exceeded maximum number of urls at line 11878
	Close
Figure 13: Frequ	iently occurring Commit Error

This can be circumvented by rebooting the firewall device (Please note that all your changes which are not yet committed will be gone. To save and load a snapshot of the firewall, refer to Save and Export Firewall configurations). To reboot the firewall, Go to **Device** \rightarrow **Setup** \rightarrow **Reboot Device** as shown in Figure 14.

paloalto	Dashboard (C)C Monitor Policies Objects Network Device	👗 Commit 💣 🎯 Config 🗸 Q. Search
	I	S (0)140
Setup -2	Management Operations Services Interfaces Telemetry Content-ID WildFire S	
Config Audit	Configuration Management	Device Operations
Administrators	Revert Revent to last saved configuration	as Reboot Device 🗲 4
Admin Roles	Revent to running configuration Save Save named configuration snapshot	as Shutdown Device
Authentication Sequence	Save candidate configuration	
User Identification	Load configuration snapshot Load configuration version	
The Certificate Management	Export Export named configuration snapshot	Miscellaneous
Certificates	Export configuration version	Custom Logos
OCSP Responder	Import Import named configuration snapshot	Ma areas assis
SSL/TLS Service Profile	Import device state	
SSL Decryption Exclusion		
Response Pages		
V Server Profiles		
SNMP Trap		
Email		
HTTP Number		
RADIUS		
TACACS+		
Rerberos		
SAML Identity Provider		
V Database		
S Users -		
admin Logout Last Login Time: 06/11/2	2019-21:40:56	📼 🚼 Tisks Langanga
Figure 14: Steps to res	start PAN Firewall	