TECHNOLOGY PARTNER PROGRAM

USE CASE DOCUMENTATION

Author: mnemonic

Contents

Partner Information

Partner information	
Date	May 28 2019
Partner Name	Mnemonic
Web Site	www.mnemonic.no
Product Name	Mnemonic Nordic threat feed for Palo Alto Networks
Partner Contact	Richard Jensen, richard@mnemonic.no, +4741451331
Support Contact	portal.mnemonic.no, support@mnemonic.no, +4723204741
Partner Product for Integration	External Dynamic Lists
Product Description	Dynamic URL, IP and domain lists focusing on threats targeted at the Nordics.

Use cases for integration into Palo Alto Networks Next Generation Security Operating Platform

Customer wants to block locally targeted threats from their networks:

Mnemonic Nordic Threat Feed provides real-time data that dynamically updates the URL filter capabilities of Palo Alto Networks NGFW.

Palo Alto Networks Products for Integration

Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	Mnemonics versions tested
AutoFocus			
Cortex XDR			
Cortex XDR Analytics			
MineMeld			
NGFW		9.0.1	7,8,9
Panorama			
Prisma Access			
Prisma Public Cloud			
Prisma SaaS			
Traps			

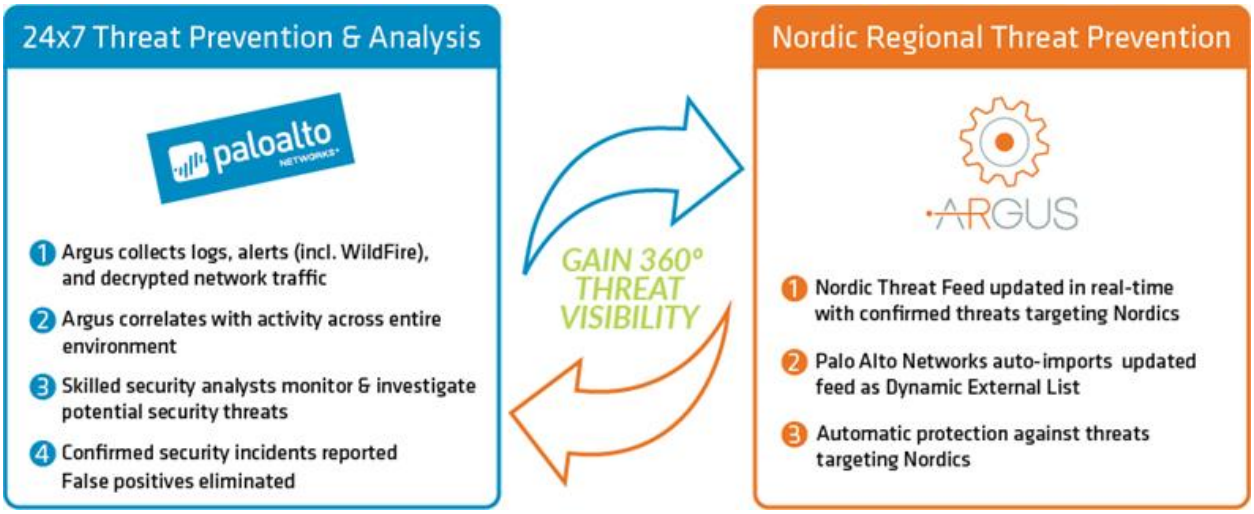
Palo Alto Networks Product	Integration Status	Palo Alto Networks versions tested	Mnemonics versions tested
VM-Series		9.0.1	7,8,9
WildFire			
Other			

Integration Benefits

Mnemonic Nordic Threat Feed integration between Palo Alto Networks and mnemonic's Argus defends your business against Nordic targeted and global threats.

Enhance your existing Palo Alto Networks investment with the Nordic Threat Feed for Palo Alto Networks. With setup taking a matter of minutes, you can ensure your Palo Alto Networks firewall is automatically and continuously updated with live threat intelligence.

Integration Diagram



Before you begin

Make sure your PAN NGFW can access the following host over HTTPS to download the feed:

https://urlfilter.mnemonic.no
(Please send an email to **support@mnemonic.no** with the subject “Nordic Threat Feed for Palo Alto Networks”, containing your public IP address from where the requests for downloading the feed originate.)

Palo Alto Networks Configuration

1)Adding External Dynamic Lists

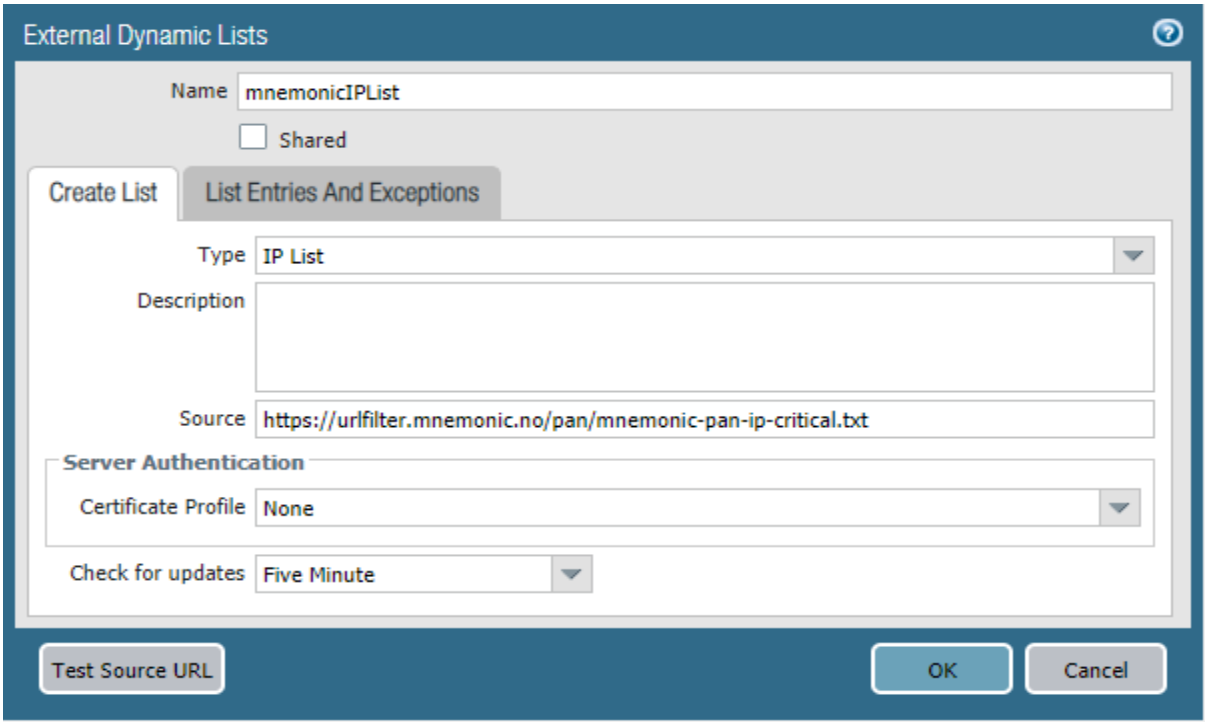
Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/configure-the-firewall-to-access-an-external-dynamic-list.html#

Examples:

Under “Objects” -> “External Dynamic Lists” click “Add” and enter the relevant feed URLs.

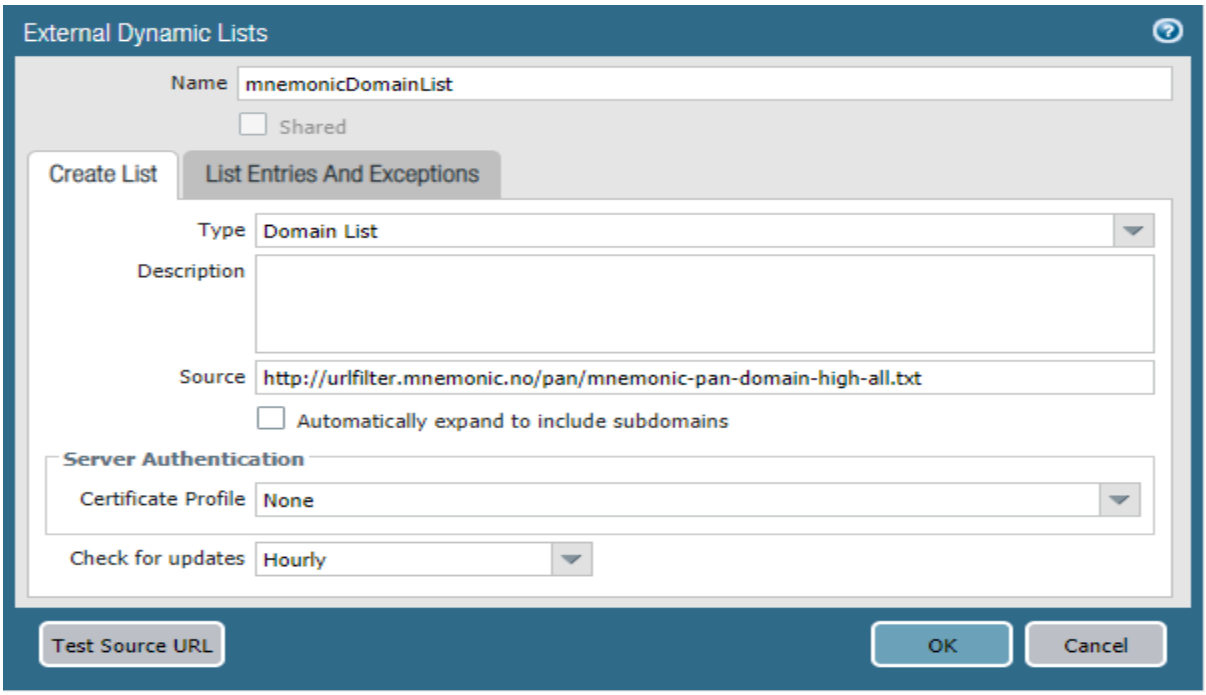
IP list:

https://urlfilter.mnemonic.no/pan/mnemonic-pan-ip-critical.txt

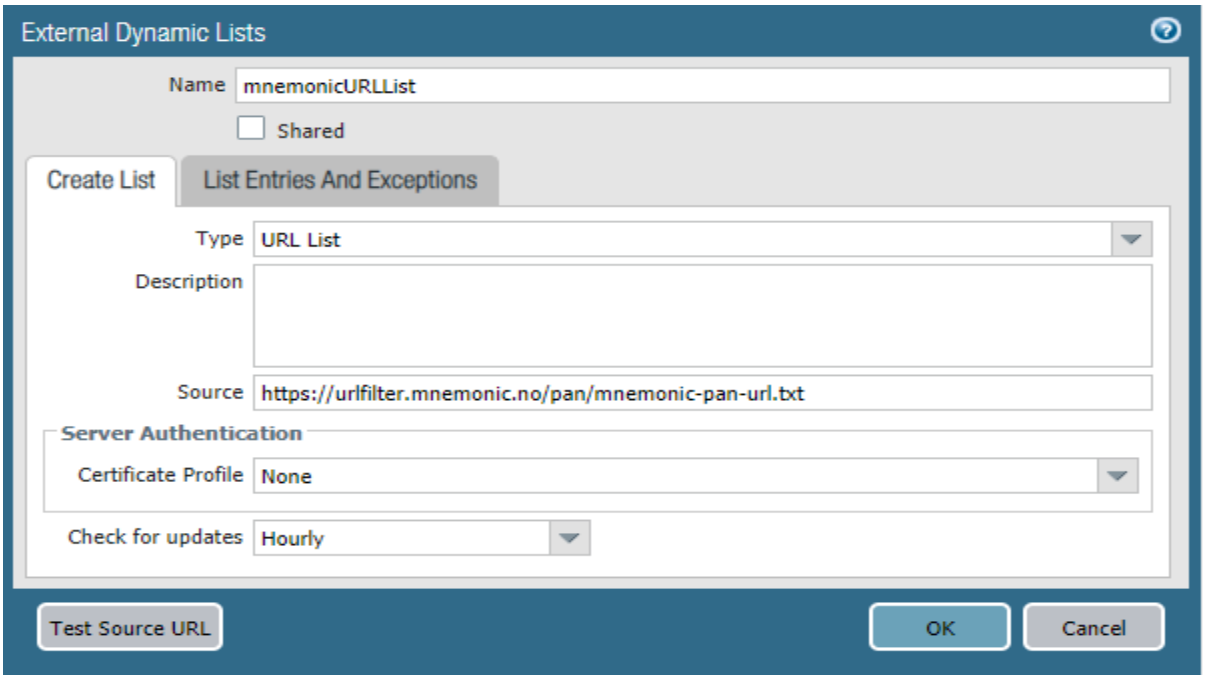


Domain list:

https://urlfilter.mnemonic.no/pan/mnemonic-pan-domain-high-all.txt



URL list:
https://urlfilter.mnemonic.no/pan/mnemonic-pan-url.txt



Provide a name for the External Dynamic List and select the default update interval.

Click OK to save your changes.

(Any manual exceptions can be added to “List Entries and Exception” and If you need to perform server certificate validation please select a certificate profile.)

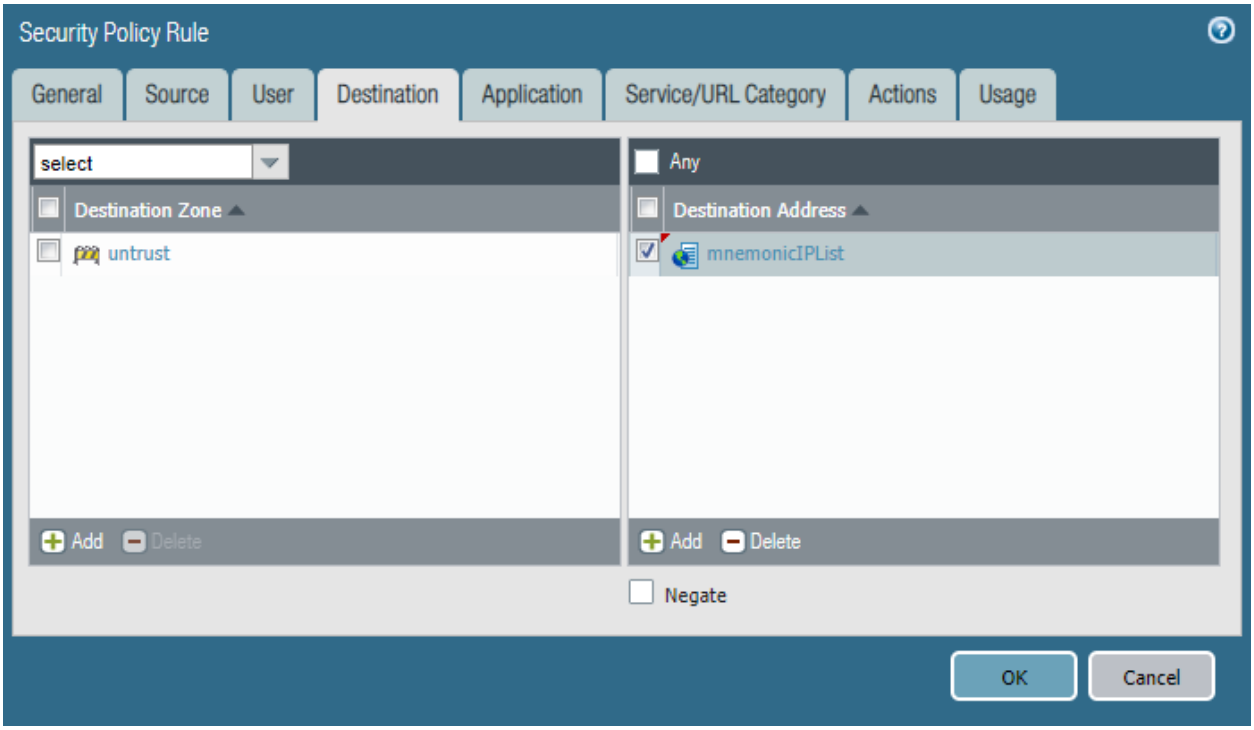
2)Enforce policy on the entries in External Dynamic List

Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/enforce-policy-on-an-external-dynamic-list.html

Examples:

Create an IP based filtering policy

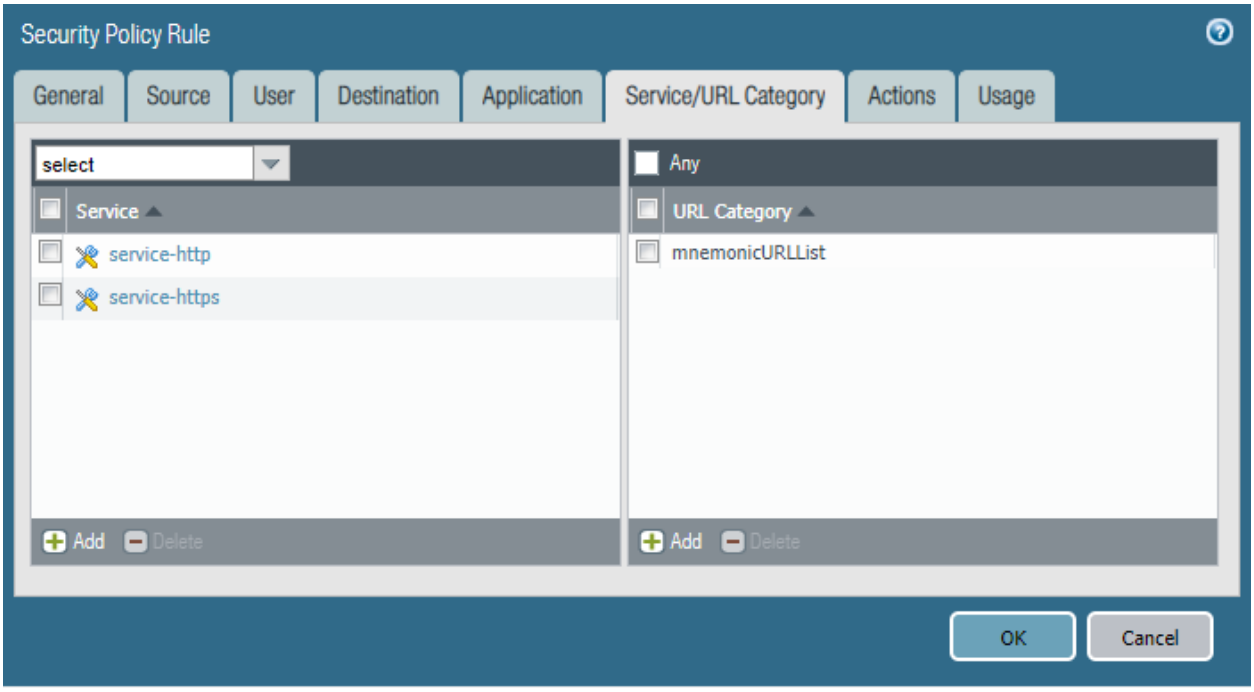
Create a new rule or edit an existing rule and input desired information about source, destination and application. From the “Destination” tab select the list(s) under “Destination Address”.



Select action drop or deny and save the new rule and commit your changes.

Create a URL Category based policy

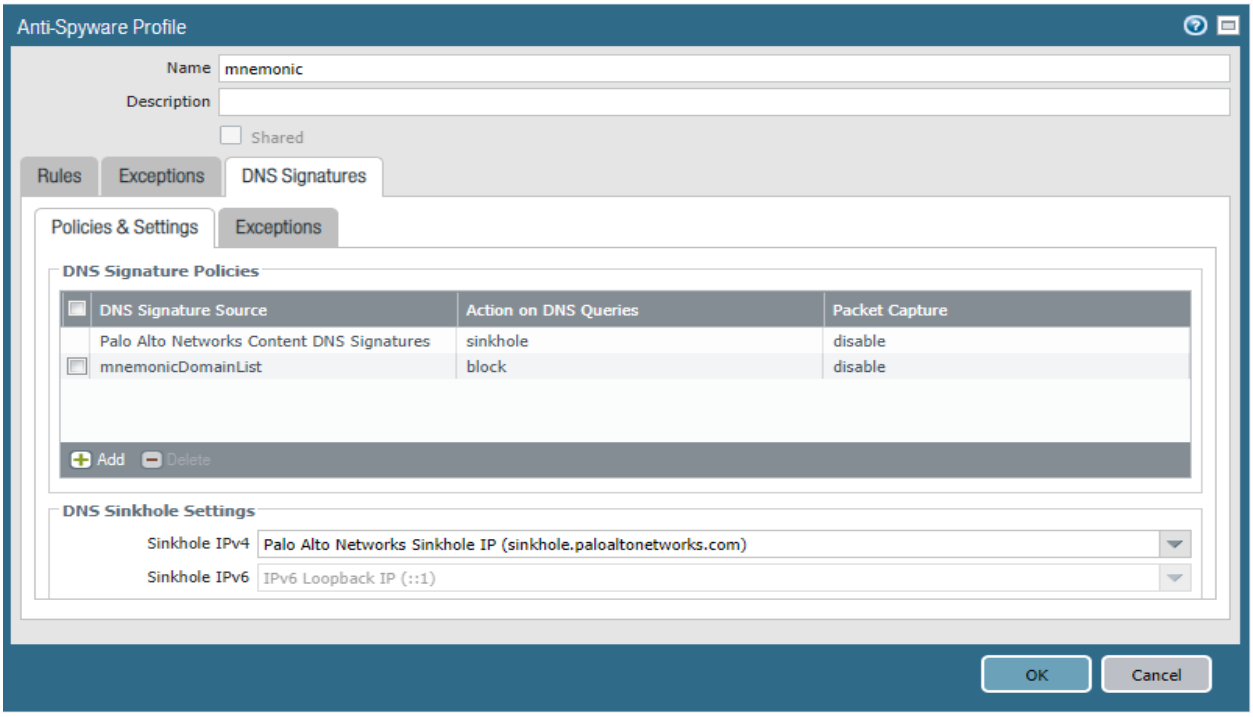
Create a new rule or edit an existing rule and input desired information about source, destination and application. From the “Service/URL Category” tab add the list under “URL Category”.



Select action drop or deny and save the new rule and commit your changes.

Configure DNS Sinkholing (Domain List)

Add the domain list to an Anti-Spyware profile under DNS Signatures -> Policies & Settings



Add the Anti-Spyware profile to a rule in the policy and commit.

Partner Product Configuration

The feeds are hosted on at: *https://urlfilter.mnemonic.no*
(Please send an email to **support@mnemonic.no** with the subject "Nordic Threat Feed for Palo Alto Networks", containing your public IP address from where the requests for downloading the feed originate.)

Troubleshooting

Test if the Nordic Threat Feed can be downloaded by using the "Test Source URL" button on the External Dynamic List object.

If this test fails, please ensure you have connectivity to urfilter.mnemonic.no on port 443.

HOW TO CONTACT SUPPORT 24/7

Customer portal	https://portal.mnemonic.no
Email	support@mnemonic.no
Phone	+47 23 20 47 41
Alternative phone numbers (in case primary is offline)	+47 23 20 28 25 (SOC hotline) +47 90 57 65 63 (Support hotline)

Mnemonic is a TSANet member, level Limited EMEA.

Technical Details

The Nordic Threat Feed database is regularly maintained and kept below 50,000 entries in order to be compatible with all Palo Alto Networks devices.

Mnemonic provides access to the Nordic Threat Feed over encrypted channel (HTTPS).

Nordic Threat Feed can be utilized by the following functions in PANOS:

- URL Filtering

- DNS Sinkhole
- Port based filtering

Product description

Nordic Threat Feed for Palo Alto Networks:

https://www.mnemonic.no/managed-detection-and-response/applied-threat-intelligence/nordic-threat-feed-for-palo-alto-networks/