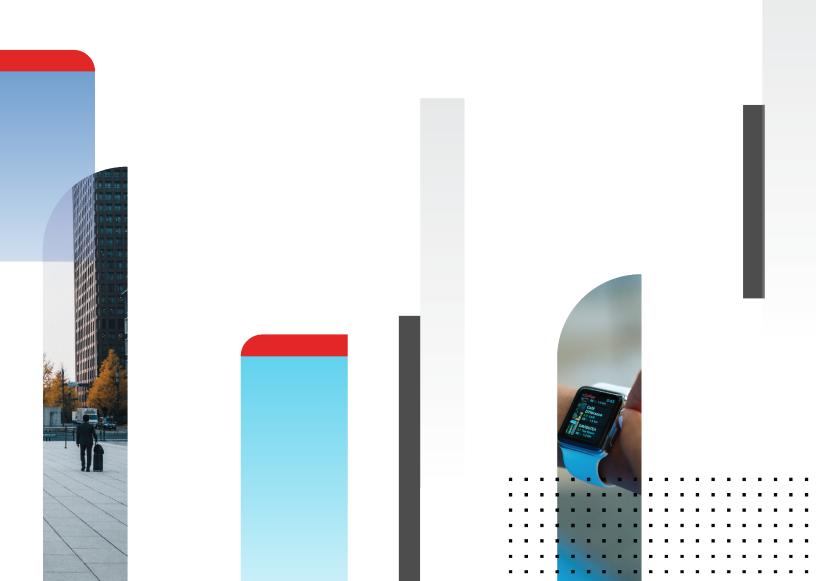
F**E**RTINET.

Administration Guide

Policy Analyzer MEA 1.0.0 Beta



FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE https://video.fortinet.com

FORTINET BLOG https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com



September 14, 2023 Policy Analyzer MEA 1.0.0 Beta Administration Guide 02-100-750937-20230914

TABLE OF CONTENTS

Change Log	4
Introduction	
Requirements	5
Key concepts	5
Device and logging requirements	
Policy Analyzer wizard process	
Types of policies generated by Policy Analyzer wizard	
How Policy Analyzer MEA works with FortiManager	7
Quick start	9
Configuring FortiGate	9
Setting NGFW to policy-based	
Configuring a Security Policy with Learn Mode enabled (7.2)	
Configuring a Security Policy with Learn Mode enabled (7.0)	
Enabling logging to FortiAnalyzer	
Configuring FortiAnalyzer	
Adding FortiGate to FortiManager	
Enabling Policy Analyzer MEA	
Opening Policy Analyzer MEA	16
Policy Analyzer modes	18
Blocking malicious traffic	18
Allowing learned traffic with permissive mode	21
Allowing learned traffic with restrictive mode	24
More information	28

Change Log

Date	Change Description
2021-10-20	Initial release of 1.0.0 Beta.
2021-10-22	Clarified the result of <i>Block malicious traffic</i> mode. Even though malicious traffic is leaned on a specific port, the policy block generated by Policy Analyzer MEA will block malicious traffic on all FortiGate interfaces. See Key concepts on page 5.
2022-03-31	Updated to support changes in FortiOS 7.2.0 and later. See Configuring FortiGate on page 9.
2023-06-06	Updated JSON API Access setting in FortiAnalyzer. See Configuring FortiAnalyzer on page 14.
2023-09-14	Updated Configuring FortiAnalyzer on page 14 with information about setting the HTTPS administrative access and Fabric Authorization settings.

Introduction

When enabled, Policy Analyzer MEA is installed on FortiManager. Policy Analyzer is a management extension application (MEA) that is released and signed by Fortinet to run on FortiManager.



You must be in ADOM version 7.0 or later to access Policy Analyzer MEA.

Policy Analyzer MEA is an automated tool with a wizard. It works with Security Policies in learn mode from a managed FortiGate to analyze logs sent to FortiAnalyzer. Based on the analyzed traffic, administrators can choose to automatically create a policy block to:

- Block malicious traffic
- Allowed learned traffic permissive mode
- Allowed learned traffic restricted mode

A policy block is automatically created and inserted in the policy package, and the policy package is installed to the target FortiGate.

Requirements

In order to use Policy Analyzer MEA, you must have the following products:

- FortiGate running FortiOS 7.0.2 or later
- FortiAnalyzer 7.0.2 or later
- FortiManager 7.0.2 or later
 - ADOM version 7.0 or later
 - FortiManager must manage FortiGate.
 - FortiManager must be able to communicate with FortiAnalyzer by its IP address, and the FortiManager administrator requires valid FortiAnalyzer credentials to authorize access to the logs.

Key concepts

This section describes the following key concepts for using Policy Analyzer MEA:

- Device and logging requirements on page 6
- Policy Analyzer wizard process on page 6
- Types of policies generated by Policy Analyzer wizard on page 6

Device and logging requirements

- FortiGate must have NGFW set to *policy-based* and be configured to use a Security Policy with *Learn Mode* enabled.
- FortiGate must send the logs to FortiAnalyzer, and you must configure FortiAnalyzer to allow communication to Policy Analyzer. See Configuring FortiAnalyzer on page 14. Allow the Security Policy to run for several days to generate traffic for analysis.
- FortiGate must be managed by FortiManager in a version 7.0 or later ADOM, with a synchronized configuration status. FortiManager must have Policy Analyzer MEA enabled.
- FortiManager must be able to communicate with FortiAnalyzer by its IP address, and the FortiManager administrator requires valid FortiAnalyzer credentials to authorize access to the logs.

Policy Analyzer wizard process

In Policy Analyzer MEA, you use a wizard to identify what FortiGate, FortiAnalyzer, and Security Policy to use for traffic analysis. Policy Analyzer MEA analyzes the traffic, and presents you with several options to handle the traffic. You choose an option, and Policy Analyzer MEA automatically creates a policy block. Policy Analyzer MEA also works with FortiManager to automatically insert the policy block into the Security Policy, and install the updated policy package to FortiGate.



You cannot edit the policy block in Policy Analyzer MEA. However after the policy block is automatically installed to the FortiGate, you can edit the policy block on the *FortiManager* > *Policy & Objects* pane, and then install the changes to FortiGate.

Types of policies generated by Policy Analyzer wizard

When using Policy Analyzer MEA wizard, you can choose one of the following modes:

- Block malicious traffic
- · Allowed learned traffic permissive mode
- · Allowed learned traffic restricted mode



Both *Allow learned traffic* modes also generate an implicit policy, and you must specify whether the implicit policy accepts or denies all traffic.

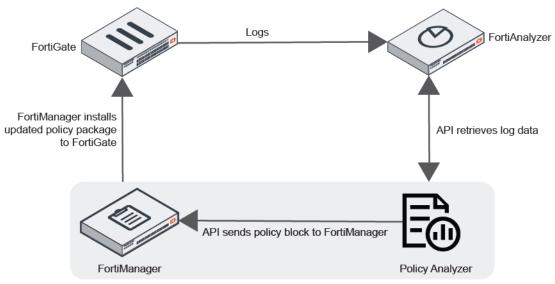
After you choose a mode, Policy Analyzer MEA automatically generates policies based on the selected mode. The following table summarizes the modes:

Mode	Description	Implicit Policy Generated?
Block malicious traffic	When the Policy Analyzer MEA wizard detects malware and applications rated high-risk, you can select the <i>Block</i> <i>Malicious Traffic</i> mode to create a policy block that will block the traffic on the FortiGate. Even though malicious traffic is leaned on a specific port, the policy block generated by Policy Analyzer MEA will block malicious traffic on all FortiGate interfaces.	No
Allowed learned traffic - permissive mode	You can use the <i>Allow Learned Traffic</i> - <i>Permissive Mode</i> setting to combine and allow traffic learned from different users and their detected applications. This method is based on Least Common Multiple concept. The wizard automatically creates a policy block with one policy to allow this traffic, and the policy block is followed by an implicit deny or allow policy. The policy block is inserted in the policy package above the Security Policy with Learn Mode enabled, and the updated policy package is automatically installed to the device.	Yes, and you choose whether the implicit policy denies or allows all traffic.
Allowed learned traffic - restricted mode	You can use the <i>Allow Learned Traffic</i> - <i>Restricted Mode</i> setting to allow the traffic learned for each user with their specific applications only. This method is based on Largest Common Denominator concept. The Policy Analyzer wizard automatically creates a policy block with one policy for each distinctive user, and the policy block is followed by an implicit deny or allow policy. The policy block is inserted in the policy package above the Security Policy with Learn Mode enabled, and the updated policy package is automatically installed to the device.	Yes, and you choose whether the implicit policy denies or allows all traffic.

How Policy Analyzer MEA works with FortiManager

Once FortiGate, FortiAnalyzer, FortiManager, and Policy Analyzer MEA are configured, FortiGate sends logs to FortiAnalyzer. Policy Analyzer uses the API to retrieve log data from FortiAnalyzer, and to provide policy changes to FortiManager for installation on the FortiGate.

Introduction



FortiManager with Policy Analyzer

Quick start

This section provides a summary of how to get started with Policy Analyzer MEA:

- 1. On FortiGate, configure FortiOS to provide logs for Policy Analyzer MEA to use. See Configuring FortiGate on page 9.
- 2. On FortiAnalyzer, configure an administrative account to use with Policy Analyzer MEA. See Configuring FortiAnalyzer on page 14.

The administrative account must have JSON API set to a minimum of Read to enable API communication between the products.

- **3.** On FortiAnalyzer, configure HTTPS administrative access, and the Authorization Address and Authorization port used for Fabric authorization. See Configuring FortiAnalyzer on page 14.
- 4. On FortiManager, add FortiGate for management, and import policy packages. See Adding FortiGate to FortiManager on page 15.
- **5.** On FortiManager, enable Policy Analyzer MEA. See Enabling Policy Analyzer MEA on page 15. Policy Analyzer MEA is downloaded from Fortinet Registry and installed on FortiManager.
- 6. Open Policy Analyzer MEA. See Opening Policy Analyzer MEA on page 16.
- 7. Use the Policy Analyzer wizard to analyze FortiGate traffic logs, and choose a mode for handling the traffic. See Policy Analyzer modes on page 18.

Policy Analyzer MEA automatically generates a policy block, inserts the policy block into the policy, and initiates installation of the updated policy package to FortiGate.

Configuring FortiGate

FortiGate must be configured with a Security Policy that has Learn Mode enabled. The Security Policy allows all services from all source and destination ports and logs all traffic for analysis. Learn Mode uses a special prefix in the policymode and profile fields in traffic and UTM logs for use by FortiAnalyzer and Policy Analyzer MEA. After configuring FortiGate, allow the device to run for several days to capture traffic in logs.

The following FortiGate limitations apply when Learn Mode is enabled in a Security Policy:

- Only interfaces with device-identification enable can be used as source interfaces in a Security Policy with Learn Mode enabled.
- Incoming and outgoing interfaces do not support any.
- Internet service is not supported.
- NAT46 and NAT64 are not supported.
- Users and groups are not supported.
- Some negate options are not supported.

The logs are sent to FortiAnalyzer, and then used by Policy Analyzer MEA to learn about the traffic needs of the FortiGate.

Following is an overview of how to configure FortiGate:

- 1. Set NGFW to policy-based. See Setting NGFW to policy-based on page 10.
- 2. Configure a Security Policy with Learn Mode enabled.
 - For FortiOS 7.2.0 and later, see Configuring a Security Policy with Learn Mode enabled (7.2) on page 10.
 - For FortiOS 7.0.2 to 7.0.x, see Configuring a Security Policy with Learn Mode enabled (7.0) on page 11.
- 3. Enable logging to FortiAnalyzer. See Enabling logging to FortiAnalyzer on page 13.

Although this section describes how to use FortiOS to configure FortiGate, you can also use FortiManager to configure FortiGate for Policy Analyzer MEA.

Setting NGFW to policy-based

On the FortiGate, NGFW must be set to policy-based.

To set NGFW to policy-based:

- **1.** Go to System > Settings.
- 2. Set NGFW Mode to Policy-based, and click Apply.

Configuring a Security Policy with Learn Mode enabled (7.2)

On the FortiGate, a Security Policy must be configured with Learn Mode enabled to provide the information that Policy Analyzer MEA requires to analyze traffic in logs.

Starting with FortiOS 7.2.0, you can enable Learn Mode in the GUI. In earlier releases of FortiOS, you must use the CLI to enable learning-mode after creating a Security Profile.

```
config firewall security-policy
  edit <policy name>
   set learning-mode enable
end
```

To configure a Security Policy with Learn Mode enabled:

- 1. Enable advanced policy options.
 - a. Go to System > Feature Visibility.
 - **b.** In the *Additional Features* column, toggle on *Policy Advanced Options*, and click *Apply*. Advanced policy options are enabled.
- 2. Create a Security Policy.
 - a. Go to Policy & Objects > Security Policy, and click Create New.
 - **b.** Set the following options:

Name	Type a name, such as <i>Learning Policy</i> .
Policy Mode	Select Learn Mode.
Incoming Interface	Select a port.
Outgoing Interface	Select a port.

New Policy					
					Additional Information
Name 🚯	Learning Policy				API Preview
Policy Mode 0	Standard Learn Mode				
Incoming Interface	im (port3)	×			⑦ Documentation
Outgoing Interface	m (port4)	×			 Online Help C Video Tutorials C
Source	💷 all	×			
	10 ali	<u></u>			
Destination	💷 all	×			
	io all +	×			
Schedule	Co always	~			
Service	App Default Specify				
	I ALL	ж			
Action	✓ ACCEPT Ø DEN	Y			
Firewall/Network Op	otions				
Protocol Options	PROT default	v			
Logging Options					
Log Allowed Traffic	O Security Events All	Sessions			
Comments Write	a comment //	0/1023			
Enable this policy C)				
			OK	Cancel	

c. Click OK.

A Security Policy is created.

A Security Policy with Learn Mode enabled automatically sets the action for all Security Policies to Monitor Only.

Dashboard	- ≡ Q		-							nbulld0220 • 🤶 • >_ 🕢 • 🔔
Network) <u> </u>	Add Filte								(*)
Policy & Objects	Date/Tin	e 9	Severity	Source	Protocol	User	Action	Count	Attack Name	Log Details
Security Profiles	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	General
	> Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Absolute Date/Time 2021/10/01 00:06:04
User & Authentication	> Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Time 00:06:04 Session ID 4776123
WiFi Controller	> Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Virtual Domain root
	> Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Source
Security Fabric	> Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	IP 10.3.144.41
Log & Report	Y Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Source Port 10014 Country/Region Reserved
Forward Traffic	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Source Interface Formation Formation Source ID FGVM08TM21003658
Local Traffic	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	User
Sniffer Traffic	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Destination
Events	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	IP 10.3.145.102
AntiVirus	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Port 80 Destination Interface nort4
Web Filter SSL	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Application Control
DNS Query	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Protocol 6
File Filter	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.SQL.Injection	Service HTTP
Application Control	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.SQL.Injection	Action
Intrusion Prevention	riday			10.3.144.1	6		detected		AlienVault.OSSIM.SQL.Injection	Action detected Threat 4096
Anomaly	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.Remote.Code.Execution	Policy ID 1
Log Settings	Friday			10.3.144.1	6		detected		AllenVault.OSSIM.Remote.Code.Execution	Security
	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.Remote.Code.Execution	Level
	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.Remote.Code.Execution	Threat Level Critical
	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.Remote.Code.Execution	Threat Score 50
	Friday			10.3.144.1	6		detected		AlienVault.USM.OSSIM.gauge.PHP.SQL.Injection	Cellular Service HTTP
	Friday			10.3.144.1	6		detected		AlienVault.USM.OSSIM.gauge.PHP.SQL.Injection	
	Friday			10.3.144.1	6		detected		AlienVault.USM.OSSIM.gauge.PHP.SQL.Injection	Intrusion Prevention
	Friday			10.3.144.1	6		detected		Alcatel-Lucent.OmniPCX.Office.MasterCGI.User.Command.Execution	Profile Isam-ips

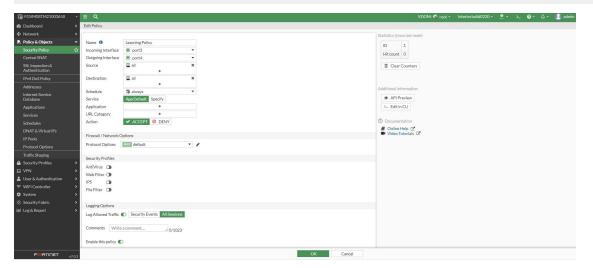
Configuring a Security Policy with Learn Mode enabled (7.0)

On the FortiGate, a Security Policy must be configured with Learn Mode enabled to provide the information that Policy Analyzer MEA requires to analyze traffic in logs.

To configure a Security Policy with Learn Mode enabled:

- 1. Enable advanced policy options.
 - **a.** Go to System > Feature Visibility.
 - **b.** In the *Additional Features* column, toggle on *Policy Advanced Options*, and click *Apply*. Advanced policy options are enabled.
- 2. Create a Security Policy.
 - a. Go to Policy & Objects > Security Policy, and click Create New.
 - **b.** Set the following options:

Name	Type a name, such as <i>Learning Policy</i> .
Incoming Interface	Select a port.
Outgoing Interface	Select a port.
Source	Select all.
Destination	Select all.



- **c.** Use the default settings for the remaining options, and click *OK*. A Security Policy is created.
- $\textbf{3. Edit the Security Policy to enable <math>\texttt{learning-mode by using the CLI}.$

```
config firewall security-policy
  edit <policy name>
   set learning-mode enable
```

end

A Security Policy with Learn Mode enabled automatically sets the action for all Security Policies to Monitor Only.

GVM08TM21003658	- = Q									imbuild0220 - 🤶 - >_ 🔗 - Д - 🙎
lashboard letwork	2 4 0/	Add Filter								()• 🗉
olicy & Objects	Date/Time	8	Severity	Source	Protocol	User	Action	Count	Attack Name	Log Details
ecurity Profiles	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	General
PN	> Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Absolute Date/Time 2021/10/01 00:06:04
ser & Authentication	> Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Time 00:06:04 Session ID 4776123
	> Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Virtual Domain root
	> Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Source
scurity Fabric	> Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	IP 10.3.144.41 Source Port 10014
g & Report	Y Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Country/Region Reserved
rward Traffic	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Source Interface Formation Formation Source ID FGVM08TM21003658
cal Traffic	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	User
iffer Traffic	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Destination
ents itiVirus	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	IP 10.3.145.102 Port 80
iti virus eb Filter	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Destination Interface m port4
L	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Application Control
~ NS Querv	Friday			10.3.144.41	6		detected		Oracle.Java.Applet.Remote.Code.Execution	Protocol 6
le Filter	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.SQL.Injection	Service HTTP
oplication Control	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.SQL.Injection	Action
trusion Prevention	🟫 Friday			10.3.144.1	6		detected		AlienVault.OSSIM.SQL.Injection	Action detected Threat 4096
nomaly	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.Remote.Code.Execution	Policy ID 1
g Settings	Friday			10.3.144.1	6		detected		AllenVault.OSSIM.Remote.Code.Execution	Security
	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.Remote.Code.Execution	Level
	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.Remote.Code.Execution	Threat Level Critical Threat Score 50
	Friday			10.3.144.1	6		detected		AlienVault.OSSIM.Remote.Code.Execution	Cellular
	Friday			10.3.144.1	6		detected		AllenVault.USM.OSSIM.gauge.PHP.SQL.Injection	Cellular Service HTTP
	Friday			10.3.144.1	6		detected		AllenVault.USM.OSSIM.gauge.PHP.SQL.Injection	
	Friday			10.3.144.1	6		detected		AlienVault.USM.OSSIM.gauge.PHP.SQL.Injection	Intrusion Prevention Profile
	Friday			10.3.144.1	6		detected		Alcatel-Lucent.OmniPCX.Office.MasterCGI.User.Command.Execution	Name learn-ips

Enabling logging to FortiAnalyzer

FortiGate must be configured to send logs to FortiAnalyzer. Policy Analyzer MEA will retrieve log data from FortiAnalyzer.

To enable logging to FortiAnalyzer:

- 1. In FortiAnalyzer, configure the authorization address and port.
 - **a.** Go to System Settings > Admin > Admin Settings.
 - **b.** In the *Fabric Authorization* section, enter an *Authorization Address* and *Authorization Port*. FortiOS uses this information to access the FortiAnalyzer login screen.
- 2. In FortiOS, go to Security Fabric > Fabric Connectors, and double-click the FortiAnalyzer Logging card.
- **3.** In the Server box, type the FortiAnalyzer IP, and click *OK*. The *FortiAnalyzer Status* (in the right-side gutter) is *Unauthorized*.
- 4. Click Authorize. You are redirected to a login screen.
- 5. Enter the username and password, and click Login.
- 6. Select Approve, and click OK to authorize the FortiGate.
- 7. In FortiOS, refresh the FortiAnalyzer Logging page. The FortiAnalyzer Status is Authorized.
- In FortiAnalyzer, go to FortiView > Applications & Websites > Top Applications to view log details. The following example identifies top applications and whether the risk level for the application is High, Medium, or Elevated.

tiView ৵ 🛛 🗏	FortiView Monitors							
~	🚔 All Devices 🗸	O Last 1 Week - Sep 27 2021 - Oct 04 2021						Dark Mo
sats	Application						Too: 1	.00 - 🗐 🗐 🕻
Лар	Add Eilter							
mised Hosts	Aug Tilles							
dbox Detection (Sessions 1.0M	<u></u>	Bio	ck -O- Pass				
	800.0k	Sep 29 08:00						
тэ	600.06	 Block : 0 Pass : 0 						
ions & Websites 🐱	400.0k			<u> </u>				
lications	200.0k							
site Domains	0 Sep 27 16:00 Sep 28 04:00	Sep 28 16:00 Sep 29 04:00 Sep 29 16:00	Sep 30 04:00 Sep 30 16:00	Oct 01 04:00 Oct 01 16:00	Oct 02 04:00	Oct 02 16:00 Oct 03 04:0	0 Oct 03 16:00	Oct 04 04:00
site Categories	# Application	Category	▼Risk	# of Clients	Sessions		Bandwidth	
using Users	1 🗵 BitTorrent	P2P	High	8	589,993		262.8 MB/193.6 ME	3
	2 🔍 RDP	Remote.Access	High	1	2		640.0 B/498.0 B	1
>	3 Telnet	Remote.Access	High	1	1		20.8 KB/3.7 KB	
	4 2 HTTP.BROWSER	Web.Client	Medium	32	1,515		9.6 MB/220.4 MB	
	5 😥 SMTP	Email/Not.Scanned	Medium	2	10		131.5 KB/8.8 KB	
	6 🛛 2 WebDAV	Network.Service	Medium	2	2		895.0 B/1.3 KB	
	7 😰 POP3	Email,Not.Scanned	Medium	1	2		1.2 KB/1020.0 B	1
	8 🙆 Usermin	Email	Medium	1	1		517.0 B/400.0 B	1
	9 tes GDB.Remote	Remote.Access	Medium	1	1		1.5 KB/1.4 KB	1
	10 📰 SSH	Network.Service,Not.Scanned	Elevated	26	185,514		291.2 MB/311.7 MB	3
	11 2 File.Upload.HTTP	Network.Service	Elevated	2	55		965.6 KB/38.2 KB	
	12 OFTP	Network.Service,Not.Scanned	Elevated	2	35		46.7 KB/45.0 KB	1
	13 😰 HTTPAudio	Video/Audio	Elevated	2	11		8.4 KB/69.9 KB	
	14 🗵 DNS	Not.Scanned	Elevated	2	10		80.3 KB/1.9 KB	
	15 😰 Sun.RPC	Network.Service	Elevated	2	8		88.8 KB/4.7 KB	
	16 😢 Ping	Network.Service	Elevated	1	6		2.7 KB/92.0 B	
	17 MS.RPC	Network.Service	Elevated	1	6		22.4 KB/2.3 KB	
	18 ₂ IRC	Collaboration, Not.Scanned	Elevated	1	4		81.0 KB/2.3 KB	
	19 😢 Portmap	Network.Service	Elevated	1	3		1.1 KB/1.1 KB	

Configuring FortiAnalyzer

FortiGate is configured to send logs to FortiAnalyzer.

When using Policy Analyzer MEA, you must log in to FortiAnalyzer to authorize use of the logs, and the administrative account must have JSON API access set to Read-Write to enable API communication between the products.

You must also enable HTTPS administrative access on the port used to communicate with FortiGate, and enter Authorization Address and Authorization Port information so that FortiOS can access the FortiAnalyzer login screen.

This section describes how to configure an administrator account to use with Policy Analyzer MEA.



In Policy Analyzer MEA, you specify a date range of log data to analyze. It's recommended to check your log storage policies in FortiAnalyzer to ensure log data is available in the database for the timeframe you would like to analyze.

To configure the FortiAnalyzer:

- 1. Go to System Settings > Administrators.
- 2. Double-click the administrator account to open it for editing.

Alternately you can create a new account for use with Policy Analyzer MEA.

- 3. Beside JSON API Access, select Read-Write.
- 4. Configure the remaining options as desired, and click OK.
- 5. Go to System Settings > Network > Interface. Ensure HTTPS Administrative Access is enabled on the port used for communication to Policy Analyzer.
- 6. Go to System Settings > Settings. In the Fabric Authorization section, enter an Authorization Address and Authorization Port.

Adding FortiGate to FortiManager

FortiGate must be managed by FortiManager to work with Policy Analyzer MEA. You must also import policy packages from FortiOS to FortiManager. You can import policy packages as part of using the *Add Device* wizard. Alternately you can import policy packages after you complete the wizard.

Policy Analyzer MEA automatically adds a policy block to the Security Policy in the policy package, so you must import the policy package to enable updates to it by FortiManager and Policy Analyzer MEA.

FortiManager must be synchronized with FortiGate to work with Policy Analyzer MEA.

To add FortiGate to FortiManager:

1. In FortiOS, configure the authorization address and port by using the following commands.

```
config system global
  set management-ip
  set management-port
```

- In FortiManager, ensure you are in a 7.0 or later ADOM.
 FortiGate must be running FortiOS 7.0.2 or later to work with Policy Analyzer MEA.
- 3. Go to Device Manager > Device & Groups, and click Add Device. The wizard opens.
- 4. Click Discover Device.
- 5. In the box, type the management port IP address for the device, and click Next.
- 6. Continue following the steps in the wizard, and select the *Import Policy Package* option when available.
- Complete the wizard to finish adding the device.
 FortiGate is managed by FortiManager, and the policy package for the device is imported to FortiManager.

Enabling Policy Analyzer MEA

You must enable Policy Analyzer MEA before you can use it. FortiManager provides access to Policy Analyzer MEA that is released and signed by Fortinet.



Only administrators with a *Super_User* profile can enable management extension applications. A CA certificate is required to install management extension applications on FortiManager.

To enable Policy Analyzer MEA in the GUI:

- 1. Ensure you are using a 7.0 or later ADOM.
- Go to *Management Extensions*, and click the grayed out tile for Policy Analyzer to enable the application. Grayed out tiles represent disabled Fortinet management extension applications. A confirmation dialog box is displayed.
- **3.** Click *OK* to confirm.

Policy Analyzer MEA is installed and enabled. It may take some time to install the application.

To enable Policy Analyzer MEA in the CLI:

```
config system docker
   set policyanalyzer enable
end
```

Opening Policy Analyzer MEA

After you enable Policy Analyzer MEA on FortiManager, you can open the MEA and use it.

To open Policy Analyzer MEA:

- 1. On FortiManager, ensure that Policy Analyzer MEA is enabled. See Enabling Policy Analyzer MEA on page 15.
- **2.** If ADOMs are enabled, ensure you are in the correct ADOM. Policy Analyzer MEA requires ADOM version 7.0 or later.
- 3. In FortiManager, go to *Management Extensions*, and click *Policy Analyzer*.



Policy Analyzer opens.

Policy Analyzer \checkmark \equiv			A	DOM: root	A admin ✓
. Select One device					_
. Select Learning-Mode Policies . Select One Policy Mode	Device	Select ~			
Review Discovered Traffic Create Policy Block	Policy Package				
	FortiAnalyzer status				
	FortiAnalyzer IP address	Å			
	FortiAnalyzer username				
	FortiAnalyzer password	٩			
		Validate Credentials			
	FortiAnalyzer ADOM	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~			
	Log date range	Start date – End date			
licyAnalyzer v1.0.0-build0007 (Beta)			Next >		Cancel

4. Use the Policy Analyzer wizard to select one of the Policy Analyzer modes. See Policy Analyzer modes on page 18.

Policy Analyzer modes

This section provides examples of how to use the following Policy Analyzer MEA modes to create policies:

- Block malicious traffic. See Blocking malicious traffic on page 18.
- Allow learned traffic with permissive mode. See Allowing learned traffic with permissive mode on page 21.
- Allow learned traffic with restricted mode. See Allowing learned traffic with restrictive mode on page 24.

Blocking malicious traffic

This example describes how to use Policy Analyzer MEA to create a policy block that blocks malicious traffic on FortiGates.

When the Policy Analyzer MEA wizard detects malware and applications rated high-risk, you can select the *Block Malicious Traffic* mode to create a policy block that will block the traffic on the FortiGate. Even though malicious traffic is leaned on a specific port, the policy block generated by Policy Analyzer MEA will block malicious traffic on all FortiGate interfaces.

For example, Policy Analyzer wizard can learn of a high-risk application on source port 1. When you select *Block Malicious Traffic* mode, Policy Analyzer creates a policy block that blocks high-risk applications for all ports. High-risk applications are not blocked only on the port used to learn traffic.

To block malicious traffic:

- Open Policy Analyzer MEA to access the first step in the wizard. Policy Analyzer opens, and the first pane of the wizard is displayed. The name of the first pane is 1. Select One device.
- 2. On the 1. Select One device pane, select a FortiGate.

Policy Analyzer 🗸 🛛 🗮		B A bolmin V
1. Select One device 2. Select Learning-Mode Policies	Device	FGVM08TM21003658[root]
3. Select One Policy Mode 4. Review Discovered Traffic	Policy package	new
5. Create Policy Block	FortiAnalyzer status	enable
	FortlAnalyzer IP address	10.3.143.72
	FortlAnalyzer username	admin
	FortiAnalyzer password	
		Validate Credentials
	FortlAnalyzer adom	root v
	Log date range	9/2/221 - 10/14/2021
Option		Description
Device		Select a managed FortiGate that uses a Security Policy with Learn Mode enabled.
Policy pac	kage	After selecting a FortiGate, the policy package for the selected FortiGate is displayed.
FortiAnaly	zer status	Displays whether logging from FortiGate to FortiAnalyzer is enabled.

Option	Description
FortiAnalyzer IP	After selecting a FortiGate, the IP address for the FortiAnalyzer that is receiving logs from the selected FortiGate is displayed.

3. On the 1. Select One device pane, complete the following options to validate credentials for FortiAnalyzer and select a date range of logs to analyze, and then click Next.

Option	Description
FortiAnalyzer username	Type the username for the administrator account for FortiAnalyzer. The administrator account must have JSON API set to a minimum of Read. See also Configuring FortiAnalyzer on page 14.
FortiAnalyzer password	Type the password for the administrator account.
Validate Credentials	After typing in the FortiAnalyzer username and password, click <i>Validate Credentials</i> to authenticate access to the logs on FortiAnalyzer.
FortiAnalyzer ADOM	Available after you validate the username and password for FortiAnalyzer. Select the ADOM on FortiAnalyzer that contains the logs for the selected FortiGate.
Log date range	 Available after you validate the username and password for FortiAnalyzer. Click the calendar icon to select a date range of logs for analysis. Policy Analyzer MEA needs to access online logs indexed in the FortiAnalyzer SQL database. Policy Analyzer MEA cannot analyze archived logs. For more information, see the <i>FortiAnalyzer 7.0.2 Administration Guide</i>.

The 2. Select Learning-Mode Policies pane is displayed.

4. On the 2. Select Learning-Mode Policies pane, select a Security Policy with Learn Mode enabled, and click Next. Policies are available for selection when they have Learn Mode enabled and have hit counts.

Policy Analyzer 🗸 🗮										A admin V
1. Select One device 2. Select Learning-Mode Policies	PolicyID	Name	From	То	Source	Destination	Hit Count	Action	Bytes (Sent/Received)	(
3. Select One Policy Mode 4. Review Discovered Traffic 5. Create Policy Block	1	learn	D port3	port4	IIa 🖀	IIe 🖾	3889085	LEARN	3.56TB/2.97TB	• •
o. orono r oncy brook										

The 3. Select One Policy Mode pane is displayed.

5. On the 3. Select One Policy Mode pane, select Block Malicious Traffic, and click Next.

Policy Analyzer ~	E De la companya de
1. Select One device 2. Select Learning-Mode Policies	Select One of These Policy Mode Below
Select One Policy Mode Select One Policy Mode Review Discovered Traffic S. Create Policy Block	Block Mailcox Traffic: When the Policy Analyzer detects malware traffic and high-risk rated application, you can select this mode to automatically block this traffic. As essuit, the Policy Analyzer Wizard will automatically create a Policy Block, insert It in the Policy Package. The Policy Package will be installed automatically one Trafficture or Fardina.
	Allow Learned Traffic - Permissive Mode: This permissive mode will combine and allow the straffic learned from different cases and the applications that have been detected for each of them. This method is based on the Least Common Multiple concept. The Policy Analyzer Witzerd will automatically create a Policy Block with one policy to allow this traffic matter to the Policy Policy Analyzer Witzerd will automatically create a Policy Block with one policy to allow this traffic matter to the Policy Policy Analyzer Witzerd will automatically create a Policy Block with one policy to allow this traffic matter to the Policy
	O Altor Learner Traffe - Residued Mode The studied mode will also the battle factor of the studied adjustment only. This method is based on the Largest Common Danominator concept. The Felloy Analyzer Weard will automatically create a Policy Block with one policy for each distinctive user to allow their traffic, Insert it in the Policy Plesdage. The Policy Plesdage will be installed usuandically on ForGote.

The Review Discovered Traffic pane is displayed.

6. On the *Review Discovered Traffic* pane, review discovered traffic, and click *Next*. In the following example, the *Top Applications* tab shows the high-risk applications in the logs. Click the *Top Users*, *Top Web Categories*, and *Top Threats* tabs to review traffic on those tabs. In the *Column Filter* box, type a string, and press *Enter* to filter results.

licy Analyzer ∽ 🛛 🚍												ADOM: root 🖉 🗛 a
ct One device ct Learning-Mode Policies ct One Policy Mode			op Users Top Web	Categories	Top Threats							
ew Discovered Traffic Ite Policy Block	Column	n Filter										
		App Group	App Category	DRisk	Risk	Number of Users	Bandwidth	Traffic In	Traffic Out	Session Block	Session Pass	App ID
	1	BitTorrent	P2P	4	High	61	784312835	332715197	451597638	0	967018	6
	2	Proxy.HTTP	Proxy	5	Critical	1	7889	5124	2765	0	2	107347980
	3	RDP	Remote.Access	4	High	1	2276	996	1280	0	4	15511
	4	Telnet	Remote.Access	4	High	1	25058	3762	21296	0	1	16091

The Create Policy Block pane is displayed.

Policy Analyzer 🗸 🛛 🚍								P 📣	ıdmin 🗸
. Select One device . Select Learning-Mode Policies I. Select One Policy Mode		Name	From	То	Source	Destination	Application	Action	
. Select Une Policy Mode . Review Discovered Traffic . Create Policy Block	1	BlockMalicious	🗖 any	any	2 all	🖀 all	BitTorrent RDP Elnet	deny	
				Upon clicking "Ok" button, a Polic	cy Block will be created and inserted in	the Policy Package above the learning	policies. The Policy Package will be au	tomatically installed to the F	ortiGate
Analyzer v1.0.0-build0005 (Beta)							< Back Ok	Cancel	

7. On the *Create Policy Block* pane, click *OK*. A confirmation dialog box is displayed.



8. In the confirmation dialog box, click OK.

Policy Analyzer MEA automatically creates the policy block, inserts the policy block in to the policy package, and the policy package is installed to the FortiGate.

Allowing learned traffic with permissive mode

This example describes how to use the Policy Analyzer MEA wizard to create a policy block and an implicit policy. During the wizard, you must choose whether to configure the implicit policy to deny or allow all traffic.

You can use the *Allow Learned Traffic - Permissive Mode* setting to combine and allow traffic learned from different users and their detected applications. This method is based on Least Common Multiple concept. The wizard automatically creates a policy block with one policy to allow this traffic, and the policy block is followed by an implicit deny or allow policy. The policy block is inserted in the policy package above the Security Policy with Learn Mode enabled, and the updated policy package is automatically installed to the device.



Only good, learned traffic is allowed. The malware and high-risk traffic is filtered out first.

To allow learned traffic with permissive mode:

- Open Policy Analyzer MEA to access the first step in the wizard. Policy Analyzer opens, and the first pane of the wizard is displayed. The name of the first pane is 1. Select One device.
- 2. On the 1. Select One device pane, select a FortiGate.

Policy Analyzer 🗸 🗮			A admin ~
Select Carring-Mode Policies Select Carring-Mode Policies Select One Policy Mode Raview Discovered Traffic Screate Policy Block	Device Policy padage Forthallyzer Halden Forthallyzer Paddesis Forthallyzer Username	FGVH08TH12103658(rost) new enable 10.3.143.72 admin	×
	FortiAnalyzer password		
		Validate Credentials	
	FortlAnalyzer adom	root	×
	Log date range	9/2/2021 - 10/14/2021	5

Option	Description
Device	Select a managed FortiGate that uses a Security Policy with Learn Mode enabled.
Policy package	After selecting a FortiGate, the policy package for the selected FortiGate is displayed.
FortiAnalyzer status	Displays whether logging from FortiGate to FortiAnalyzer is enabled.
FortiAnalyzer IP	After selecting a FortiGate, the IP address for the FortiAnalyzer that is receiving logs from the selected FortiGate is displayed.

3. On the 1. Select One device pane, complete the following options to validate credentials for FortiAnalyzer and select a date range of logs to analyze, and then click Next.

Option	Description
FortiAnalyzer username	Type the username for the administrator account for FortiAnalyzer. The administrator account must have JSON API set to a minimum of Read. See also Configuring FortiAnalyzer on page 14.

Option	Description
FortiAnalyzer password	Type the password for the administrator account.
Validate Credentials	After typing in the FortiAnalyzer username and password, click <i>Validate Credentials</i> to authenticate access to the logs on FortiAnalyzer.
FortiAnalyzer ADOM	Available after you validate the username and password for FortiAnalyzer. Select the ADOM on FortiAnalyzer that contains the logs for the selected FortiGate.
Log date range	Available after you validate the username and password for FortiAnalyzer. Click the calendar icon to select a date range of logs for analysis. Policy Analyzer MEA needs to access online logs indexed in the FortiAnalyzer SQL database. Policy Analyzer MEA cannot analyze archived logs. For more information, see the <i>FortiAnalyzer 7.0.2 Administration Guide</i> .

The 2. Select Learning-Mode Policies pane is displayed.

4. On the 2. Select Learning-Mode Policies pane, select a Security Policy with Learn Mode enabled, and click Next. Policies are available for selection when they have Learn Mode enabled and have hit counts.

Policy Analyzer V =										A admin V
1. Select One device 2. Select Learning-Mode Policies	PolicyID	Name	From	То	Source	Destination	Hit Count	Action	Bytes (Sent/Received)	1
3. Select One Policy Mode 4. Review Discovered Traffic 5. Create Policy Block	1	learn	D port3	port4	I all	II al	3889085	LEARN	3.56TB/2.97TB	••••••

The 3. Select One Policy Mode pane is displayed.

5. On the 3. Select One Policy Mode pane, select Allow Learned Traffic - Permissive Mode, and click Next.



The Review Discovered Traffic pane is displayed.

6. On the *Review Discovered Traffic* pane, review discovered traffic, and then click *Next*. In the following example, the *Top Applications* tab shows the high-risk applications in the logs. Click the *Top Users*, *Top Web Categories*, and *Top Threats* tabs to review traffic on each tab.

'olicy Analyzer ∽ ≣	•											ADOM: root 🖉 🗛 adm
lect One device lect Learning-Mode Policies	Тор А	pplications	Top Users Top Web	Categories	Top Threats							
lect One Policy Mode view Discovered Traffic eate Policy Block	Colum	n Filter										
to roncy block		App Group	App Category	DRisk	Risk	Number of Users	Bandwidth	Traffic In	Traffic Out	Session Block	Session Pass	App ID
	1	BitTorrent	P2P	4	High	61	784312835	332715197	451597638	0	967018	6
	2	Proxy.HTTP	Proxy	5	Critical	1	7889	5124	2765	0	2	107347980
	3	RDP	Remote.Access	4	High	1	2276	996	1280	0	4	15511
	4	Telnet	Remote.Access	4	High	1	25058	3762	21296	0	1	16091
er v1.0.0-build0008 (Deta)										< Back	Next >	Cancel

The Create Policy Block pane is displayed.

Policy Analyzer 🗸	Ξ									ADOM: root (🖗 🔺 admin 🗸
1. Select One device 2. Select Learning-Mode Policies		Name	From	То	Source Address	User	Source Group	Source Internet Service	Destination	Application	Action
Select One Policy Mode A. Review Discovered Traffic Create Policy Block	1	AllowAddr	D port3	port4	■ 10.3.144.1 ■ 10.3.144.23 ■ 10.3.144.12 ■ 10.3.144.13 ■ 10.3.144.14 ■ 10.3.144.14 ■ 10.3.144.15	L test			≌ all	AFP Apple.iPhone FTP FILe.Upload.HTTP GDB.Remote GDS.DB	accept
									Implicit Policy	Deny Any - Any O	-
					Upon dickin	g "Ok" button, a Policy Bl	ock will be created and inserted in the Polic	y Package above the learning po			
PolicyAnalyzer v1.0.0-build0008 (Beta)									< Back	Ok	Cancel

7. On the Create Policy Block pane, choose one of the following settings for the implicit policy, and click OK:

Option	Description
Deny Any - Any	Select to deny traffic on all source and destination ports.
Permit Any - Any	Select to permit traffic on all source and destination ports.

8. In the confirmation dialog box, click OK.

Policy Analyzer MEA automatically creates the policy block, inserts the policy block in to the policy package, and the policy package is installed to the FortiGate.

Policy Analyzer 🗸	=									ADOM: root	🖉 \land admin 🗸
1. Select One device 2. Select Learning-Mode Policies	æ	Name	From	То	Source Address	User	Source Group	Source Internet Servi	ce Destination	Application	Action
3 Salet One Policy Mode 4 Raview Discovered Traffic 5 Create Policy Block	1	AllowAddr	port3	Dport4	10.3.144.1 10.3.144.12 10.3.144.12 10.3.144.13 10.3.144.14 10.3.144.15	L test			I at	HAFP Apple.iPhone FTP FIIe.Upload.HTTF GDB.Remote GDS.DB	accept
			Install Policy	Package onto	FortiGate						
			Policy Block is cre	ated and inserted suc	cessfully		- 60				
			Policy Package is	installing to device			_				
			Policy Package is	installed successfully			- 60				
							- 100%				
						ок	-				
										cy 🔿 Deny Any - Any	
					Upon dicking	"Ok" button, a Policy Block will I	be created and inserted in the I	Policy Package above the learning	ing policies. The Policy Packag	e will be automatically insta	Illed to the FortiGate.
Reference and the South PANE (Resta)									< Back	Ok	Cancel

9. Go to *Policy & Objects > Policy Packages > Security Policy* to view the policy block created by Policy Analyzer MEA. The policy block and implicit policy are added above the rules in the policy package.

Policy & Objects 🗸 🗧	E 🖹 P	Policy Pac	kage 🗸 👌 Install 🗸	ADOM Revision	ns 🛛 Tools 🗸								ADOM: root 🔑 🤉	Aadm
🗄 Policy Packages 🗸	+	Create N	√ew ∽ 🖾 Edit ∽	🛱 Delete 🖽 Se	ection 🗸 📓 Policy B	lock ∽ 🖋 Collapse All 🚜	Column Settings ~							۹
La Search	a 🗆		Name	From	То	Source	Destination	Schedule	Service	Application	URL Category	Action	Security Profiles	Lo
■ € FGVM08TM21003658						 □ 10.3.144.41 □ 10.3.144.43 								
Security Policy						■ 10.3.144.46				Q Jonkins				
Security Virtual Wire Pair Policy						 10.3.144.47 10.3.144.48 				MS.RPC				
Central SNAT						10.3.144.49								
SSL Inspection & Authentication				🖬 port3	🖬 port4	■ 10.3.144.5 ■ 10.3.144.50	₩.at	G always						
Virtual Wire Pair SSL Inspection & Authentie	cati					■ 10.3.144.51								
Authentication Rules						10.3.144.52								
IPv4 Multicast Policy						■ 10.3.144.55								
IPv6 Multicast Policy						 10.3.144.59 10.3.144.60 								
IPv4 Local In Policy						10.3.144.7				SSH				
IPv6 Local In Policy						10.3.144.8				Sun RPC				
IPv4 DoS Policy						■ 10.3.144.17								
IPv6 DoS Policy						■ 10.3.144.28 ■ 10.3.144.31								
IPv4 Interface Policy						■ 10.3.144.10								
IPv6 Interface Policy						 10.3.144.11 10.3.144.20 								
Traffic Shaping Policy						■ 10.3.144.30								
Installation Targets						 10.3.144.33 10.3.144.34 								
FGVM08TM21003658_root						10.3.144.36								
⊕ ĝ default						 10.3.144.37 10.3.144.38 								
⊕ ■ Policy Blocks (9)						10.3.144.42								
Object Configurations >						 10.3.144.44 10.3.144.45 10.3.144.53 10.3.144.56 10.3.144.57 10.3.144.58 10.3.144.6 								
			Implicit accept	any any	any any	🖾 all	🖾 all	ahways				Accept	堂 default	C
			Learning_policy	D port3	D port4	2 all	🖾 all	ahvays				Ø Deny	🕏 default	
		▼ Implic	cit (4-4 / Total: 1)											
		4	Implicit Deny	🗖 any	any any	⊠ all 13 all	lle 10 Ile 10	G always	@ ALL			Ø Deny		0

Allowing learned traffic with restrictive mode

This example describes how to use the Policy Analyzer MEA wizard to create a policy block and an implicit policy. During the wizard, you must choose whether to configure the implicit policy to deny or allow all traffic.

You can use the *Allow Learned Traffic - Restricted Mode* setting to allow the traffic learned for each user with their specific applications only. This method is based on Largest Common Denominator concept. The Policy Analyzer wizard automatically creates a policy block with one policy for each distinctive user, and the policy block is followed by an implicit deny or allow policy. The policy block is inserted in the policy package above the Security Policy with Learn Mode enabled, and the updated policy package is automatically installed to the device.



Only good, learned traffic is allowed. The malware and high-risk traffic is filtered out first.

To allow learned traffic with restrictive mode:

1. Open Policy Analyzer MEA to access the first step in the wizard.

Policy Analyzer opens, and the first pane of the wizard is displayed. The name of the first pane is 1. Select One device.

2. On the 1. Select One device pane, select a FortiGate.

Policy Analyzer 🗸 🗮			
Solicel One device Select Learning-Mode Policies Select One Policy Mode Review Discovered Traffic Create Policy Block	Device Pelicy padage FortiAnalyzer status FortiAnalyzer IP address FortiAnalyzer usertame FortiAnalyzer gaswood	FGVH08TH22003658[root] • new enable 10.3.143.72 admin	
	FortlAnalyzer adom Log date range	Validute Credentials root 9/22021 - 10/14/2021	

Option	Description
Device	Select a managed FortiGate that uses a Security Policy with Learn Mode enabled.
Policy package	After selecting a FortiGate, the policy package for the selected FortiGate is displayed.
FortiAnalyzer status	Displays whether logging from FortiGate to FortiAnalyzer is enabled.
FortiAnalyzer IP	After selecting a FortiGate, the IP address for the FortiAnalyzer that is receiving logs from the selected FortiGate is displayed.

3. On the 1. Select One device pane, complete the following options to validate credentials for FortiAnalyzer and select a date range of logs to analyze, and then click Next.

Option	Description
FortiAnalyzer username	Type the username for the administrator account for FortiAnalyzer. The administrator account must have JSON API set to a minimum of Read. See also Configuring FortiAnalyzer on page 14.
FortiAnalyzer password	Type the password for the administrator account.
Validate Credentials	After typing in the FortiAnalyzer username and password, click <i>Validate Credentials</i> to authenticate access to the logs on FortiAnalyzer.
FortiAnalyzer ADOM	Available after you validate the username and password for FortiAnalyzer. Select the ADOM on FortiAnalyzer that contains the logs for the selected FortiGate.
Log date range	Available after you validate the username and password for FortiAnalyzer. Click the calendar icon to select a date range of logs for analysis.

Option	Description
	Policy Analyzer MEA needs to access online logs indexed in the FortiAnalyzer SQL database. Policy Analyzer MEA cannot analyze archived logs. For more information, see the <i>FortiAnalyzer 7.0.2 Administration Guide</i> .

The 2. Select Learning-Mode Policies pane is displayed.

4. On the 2. Select Learning-Mode Policies pane, select a Security Policy with Learn Mode enabled, and click Next. Policies are available for selection when they have Learn Mode enabled and have hit counts.

Policy Analyzer 🗸 🛛 🚍										A admin v
1. Select One device 2. Select Learning-Mode Policies	PolicyID	Name	From	То	Source	Destination	Hit Count	Action	Bytes (Sent/Received)	1
3. Select One Policy Mode 4. Review Discovered Traffic 5. Create Policy Block	1	learn	port3	D port4	≅ all	II all	3889085	LEARN	3.56TB/2.97TB	
o. Grouter andy broat										

The 3. Select One Policy Mode pane is displayed.

5. On the 3. Select One Policy Mode pane, select Allow Learned Traffic - Restricted Mode, and click Next.

	E ADD44 road β 🔕 Admin v
1. Select One device 2. Select Learning-Mode Policies	Select One of These Policy Mode Below
Select Conterpole Value Select Conterpole Value Arrivev Discovered Traffic S. Create Policy Block	O Block Malicious Traffic When the Policy Analyzer detects malware traffic and high-traik rated application, you can select this mode to automatically block this traffic. As result, the Policy Analyzer Witcard ell automatically create a Policy Block, insert is in the Policy Package. The Policy Package will be installed automatically or Policial or Portical or Portical or Portical or Policy Analyzer detects malware traffic and high-traik rated application, you can select this mode to automatically block this traffic. As result, the Policy Analyzer Witcard ell automatically create a Policy Block, insert is in the Policy Package. The Policy Package will be installed automatically or Policy
	O Alon Learners Tindle: - Pertission Mode: This pertission was well continues and when traffic learners from offerent users and the applications that have been distocted for each of them. This method is based on the Least Common Multiple concept. The Palicy Analyzer Witzerd will automatically create a Palicy Block with one palicy to allow the tartific, issue it is the Palicy parkage. The Palicy parkage will be installed automatically on FortGate.
	The restruct means the contrast means and the contrast means and the specific applications only. This method is based on the Largest Common Denominator concept. The Polcy Analyzer Witzerd will automatically creats a Polcy Block with one polcy for each districtive user to allow their traffic, Insert it in the Policy Package. The Policy Package will be installed automatically on FortGate.

The Review Discovered Traffic pane is displayed.

6. On the *Review Discovered Traffic* pane, review discovered traffic, and then click *Next*.

In the following example, the *Top Applications* tab shows the high-risk applications in the logs. Click the *Top Users*, *Top Web Categories*, and *Top Threats* tabs to review traffic on those tabs.

🟥 Policy Analyzer 🗸 🛛 🚍	1											ADOM: root 🖉 🔺 admin 🗸
1. Select One device 2. Select Learning-Mode Policies	Top A	Applications	ers Top Web	Categories	Top Threats							
Select One Policy Mode A. Review Discovered Traffic S. Create Policy Block	Colum	in Filter										
5. Create Policy block		App Group	App Category	DRisk	Risk	Number of Users	Bandwidth	Traffic In	Traffic Out	Session Block	Session Pass	App ID
	1	BitTorrent	P2P	4	High	61	784312835	332715197	451597638	0	967018	6
	2	Proxy.HTTP	Proxy	5	Critical	1	7889	5124	2765	0	2	107347980
	3	RDP	Remote.Access	4	High	1	2276	996	1280	0	4	15511
	4	Telnet	Remote.Access	4	High	1	25058	3762	21296	0	1	16091
PolsyAnabaser v1.0-Dauld3006 (Bea)										< Back	Next >	Cancel

The Create Policy Block pane is displayed.

ect One device ect Learning-Mode Policies	=	Name	From	То	Source Address	User	Source Group	Source Internet Service	Destination	Application	Action
ct One Policy Mode ew Discovered Traffic te Policy Block	1	AllowUsers1	D port3	port4		L test			II ali	FTP File.Upload.HTTP GDB.Remote GDS.DB HTTP.Audio HTTP.BROWSER	accept
	2	AllowSrcIP1	D port3	D port4	10.3.144.20				📱 all	HTTP.BROWSER	accept
	3	AllowSrciP2	D port3	D port4	■ 10.3.144.30				🖾 all	HTTP.BROWSER SSH Wget	accept
	4	AllowSrciP3	D port3	D port4	a 10.3.144.19				🖬 all	File.Upload.HTTP HTTP.Audio HTTP.BROWSER SSH	accept
	5	AllowSrciP4	D port3	D port4	₩ 10.3.144.22				🖾 all	File.Upload.HTTP HTTP.BROWSER SSH	accept
	6	AllowSrciP5	D port3	D port4	■ 10.3.144.60				🖾 all	 File.Upload.HTTP HTTP.BROWSER SSH 	accept
	7	AllowSrcIP6	D port3	D port4	10.3.144.33				🕮 all	HTTP.BROWSER	accept
	8	AllowSrcIP7	D port3	port4	10.3.144.36				🖾 all	HTTP.BROWSER	accept
	9	AllowSrcIP8	D port3	D port4	10.3.144.53				🖾 all	HTTP.BROWSER	accept
									Implicit Policy	Deny Any - Any	Permit Any -
					Upon clicking	g "Ok" button, a Policy Block w	ill be created and inserted in the Polic	y Package above the learning polic	ies. The Policy Package w	vill be automatically install	ed to the Forti

7. On the Create Policy Block pane, choose one of the following settings for the implicit policy, and click OK:

Option	Description
Deny Any - Any	Select to deny traffic on all source and destination ports.
Permit Any - Any	Select to permit traffic on all source and destination ports.

A confirmation dialog box is displayed.

Install Policy Package onto FortiGate	e	
Are you sure you want to create a new policy blo	ock and install policy package o	nto to the FortiGate?
	ОК	Cancel

- In the confirmation dialog box, click OK.
 Policy Analyzer MEA automatically creates the policy block, inserts the policy block in to the policy package, and the policy package is installed to the FortiGate.
- **9.** Go to *Policy & Objects > Policy Packages > Security Policy* to view the policy block created by Policy Analyzer MEA. The policy block and implicit policy are added above the rules in the policy package.

More information

Policy Analyzer is available as a management extension application with FortiManager. For information about Policy Analyzer MEA, see the FortiManager page on the Document Library.



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.