

OPSWAT Quick Integration Guide

for PacketFence version 5.0.0

OPSWAT Quick Integration Guide

by Inverse Inc.

Version 5.0.0 - Mar 2015 Copyright © 2014 Inverse inc.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation; with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts. A copy of the license is included in the section entitled "GNU Free Documentation License".

The fonts used in this guide are licensed under the SIL Open Font License, Version 1.1. This license is available with a FAQ at: <u>http://</u><u>scripts.sil.org/OFL</u>

Copyright © Łukasz Dziedzic, http://www.latofonts.com, with Reserved Font Name: "Lato".

Copyright © Raph Levien, <u>http://levien.com/</u>, with Reserved Font Name: "Inconsolata".

inverse

Table of Contents

About this Guide	1
Assumptions	2
Quick installation	3
Step 1: Configure OPSWAT GEARS	3
Step 2: Developer account	3
Step 3: Gathering the install URL	3
Step 4: API access	4
Step 5: Configure PacketFence	4
Step 6: Add the necessary passthroughs	6
Step 7: Test	7
Compliance enforcement	8
Step 1: Configure OPSWAT GEARS	8
Step 2: Configure PacketFence	8
Step 3: Customize the template	9

About this Guide

This guide has been created in order to help sales engineers, product managers, or network specialists demonstrate the PacketFence capabilities on-site with an existing or potential customer. It can also provide guidelines to setup a proof of concept for a potential PacketFence deployment using OPSWAT GEARS to provide information about device compliance before and during network access.

Assumptions

- You have a configured PacketFence environment with working test equipment;
- You have, or will create, an OPSWAT GEARS account at http://www.opswatgears.com/.

Quick installation

Step 1: Configure OPSWAT GEARS

You will first need to create an OPSWAT GEARS account at <u>http://www.opswatgears.com</u> and configure your account according to OPSWAT's documentation.

Step 2: Developer account

Now that you have basic functionality for your OPSWAT GEARS account, you will need to create a GEARS developer account so PacketFence can access the OPSWAT GEARS API. You can do this here <u>https://gears.opswat.com/developers</u>.

Creating the application

Once this is done, click *Register a new application*. The only thing important here is to set the callback URL to <u>http://127.0.0.1/opswat</u>.

Once you created the application, note the client key and client secret for usage below.

Step 3: Gathering the install URL

From your OPSWAT GEARS console, click *+Devices* at the top. Then click on Enable *GEARS client on another device*. At the bottom you will see the URL to install the agent. Keep that URL in order to configure it in PacketFence

Step 4: API access

In order to configure OPSWAT GEARS in PacketFence you will need to generate an OAuth2 access and refresh token so PacketFence can access the OPSWAT GEARS API.

Generate the authorization code

First you will access this page using your browser (replace **-clientid-** by your client ID that you got when creating the application):

```
https://gears.opswat.com/o/oauth/authorize?client_id=-clientid-
&response_type=code&redirect_uri=http://127.0.0.1/opswat
```

Authorize the application and you will then be redirected to an unavailable page but the URL will contain the code in it's parameters (ex: http://127.0.0.1/opswat?code=wJ2RTE).

Generate the access and refresh token

We will now use the code at the end to generate the access and refresh token using another HTTP request that will be done in your browser. Replace **-clientid-** and **-clientsecret-** by the client id and secret of your application. Then add the code you got above at the end of this URL.

```
https://gears.opswat.com/o/oauth/token?client_id=-clientid-&client_secret=-
clientsecret-&grant_type=authorization_code&redirect_uri=http://127.0.0.1/
opswat&code=
```

You should now be presented with a JSON response that contains the access and refresh token. Take note of both of these values for the PacketFence configuration. Example:

```
{"access_token":"ab3aec71-fa6a-4752-8804-00c37f934059","token_type":"bearer",
    "refresh_token":"f9e7c698-4d88-42cb-b9ae-c067557e8385","expires_in":43199,
    "scope":"read","client_id":"1234567890"}
```

Step 5: Configure PacketFence

Create a new provisioner

Login in the PacketFence administration interface, then go in the *Configuration* tab, then in *Provisioners*. Click *Add provisioner* then select opswat.

ports Nodes Users Configu i	ration			
Provisioning	New Provisionin	g Entry	×	
android	Provisioning ID ()	opswat		Clone
-	Description	OPSWAT		
	Set role	Select a role		Clone Delete
mobileiron		Roles		Clone Delete
opswat	Client Id 🔒	1234567890		Clone Delete
	Client Secret 🔒	0987654321		
	Host	gears.opswat.com		
Add provisioner -	Port 🖲	443		
	Protocol	https •		
	Access token ()	b5275f8c-a22c-4260-8090-696c2b3		
	Refresh token ()	ec532cc4-0d78-426e-8c44-1411c5t		
	Agent download uri	https://gears.opswat.com/gears/a/dc		
			Close Save	

Now configure this new provisioner with the information you got above.

- The Provisioning ID is the friendly name of the provisioner.
- The Client Id is the ID of the application you created in the developer account.
- The Client Secret is the secret of the application you created in the developer account.
- The default host should work if you have a cloud account, if not adapt it to your local instance.
- The port and protocol should be left to default.
- The access and refresh token are the tokens you got at the end of step 4.
- The Agent download uri is the one you got in step 3.

Add the provisioner to the profile

Now that you have created the provisioner, go in the *Portal Profiles* menu on the left and select the default portal. Click *Add Provisioner* and select the new OPSWAT GEARS provisioner that was created earlier.

PacketFence 🕬 Status	Reports Nodes Users	Configuration	🛔 admin 🗸	0
Captive portal			concetorrort	
Advanced	Reuse dot1x credentials			
Web Services				
Portal Profiles	Enable Billing Engine			
Admin Access		When enabling the billing engine, all authentication sources bellow are ignored.		
NETWORK	Number of Registration	0		
Interfaces	Pages			
Switches				
WRIX	Languages	1 en_US •	(00
Floating devices				_
Firewall SSO				
USERS	Sources			
Roles		With no source specified, all internal and external sources will be used.		
Access Duration		Add a source.		
Sources		4		
Provisioners	Provisioners	1 opswat •	(00
COMPLIANCE				_
Violations				
Statement of Health	Mandatory Fields	1 firstname •	(00
IDENTIFICATION				
Fingerprints		2 lastname •		90
User Agents		3 phone •	(00
MAC Addresses		4 email •	(00

Step 6: Add the necessary passthroughs

Next, still in the PacketFence administration console, go in *Trapping* in the left menu, then scroll then to *Passthroughs*. Check the *Passthrough* box above the field and add the following domains to the passthrough list.

- gears.opswat.com
- software.opswat.com
- opswat-gears-cloud-clients.s3.amazonaws.com

PacketFence 🕬 Status	Reports Nodes Users	Configuration 🛓 admin 🔹 🕕
Provisioners		Choose between our supported IDS engine.
COMPLIANCE	Wireless IPS	
Violations		If enabled, we will act on wirelessIPS traps sent by Wireless controllers.
Statement of Health	Wireless IPS threshold	90
IDENTIFICATION		Decembran of matching you want to admin an a wireford IPS tran
Fingerprints		reitenage u maiuling you wain to aleit ure aunin on a wielessin s uap.
User Agents	Passthrough	Ø
MAC Addresses		When enabled, PacketFence uses pfdns if you defined Passthroughs or Apache mod-proxy if you defined Proxy passthroughs to allow trapped devices to reach web sites.
	Passthroughs	gears.gosval.com software.gosval.com
		Comma-delimited list of domains to be used as HTTP and HTTPS passthroughs to web sites. The configuration parameter passthrough must be enabled for passthroughs to be effective.
	Proxy Passthroughs	
		Comma-delimited list of domains to be used with apache passthroughs. The configuration parameter passthrough must be enabled for passthroughs to be effective.
	Proxy Interception	
		If enabled, we will intercept proxy request on the specified ports to forward to the captive portal.
	Denve Internetion Dent	
	Proxy Interception Port	autor 3128
		4

Step 7: Test

You can now test that the installation of the OPSWAT GEARS client is mandatory after the device registration. Connect a device to your test network and register like you normally would. At the end of the registration process you will be presented a page asking you to install the OPSWAT GEARS client on your device. After you install the client click continue. If your access is enabled than this means the connectivity between PacketFence and OPSWAT GEARS is good.

Compliance enforcement

PacketFence polls the OPSWAT GEARS API in order to trigger violations on noncompliant devices.

PacketFence uses the number of critical issues the device has to determine whether or not it needs to isolate it.

Step 1: Configure OPSWAT GEARS

First you need to configure what you consider as a critical issue in your OPSWAT GEARS console.

You will do that through the *Configure* menu. Then you'll see a column that allows you to flag what is considered as a critical issue.

Ĝ	EARS	Configure Managed Device	Policy								SAVE
	inverse	Protection	Unwanted Applications	System	Advanced Th	ireats					
	inverse	Consid	ler an issue		Crit	ical 🕜	All	Desktops	Laptops	VM's	Servers
Ch	Dashboard	Antiphishing					1	~	~	 Image: A set of the set of the	 Image: A start of the start of
		R	equire at least one antiphishing p	roduct to be enabled							
:=	Devices	Antivirus									
_		Antonius						•			
\bigcirc	Event Log	Ri	eport if no antivirus application is equire real time protection from a	installed t least one antivirus product		v					
*	Configure	Ri	Attempt to enable real time pro	otection in all antivirus product	s n 3 days old	 					
	Device Policy		Attempt to update all antivirus	definitions ast one antivirus in the last 7 d	avs						
	Account Settings	Report if at least one antivirus has detected any threats in the last 7 days									
	Summary Reports	Dealure									
	Heln Center	Васкир						~	 Image: A start of the start of		~
Q	help Gentel	RI RI	eport if no backup application is in eport if no backup activity in the la	nstalled ast 7 days							
	Log out			-		-					
		Encryption					1	v	v	~	~

Step 2: Configure PacketFence

Now in order to enforce the compliance of the devices using the flagged critical issues above, you will need to configure the provisioner you created above to activate the enforcement.

Back in the provisioner configuration, go in the Compliance tab.

You now have to configure the violation that is raised when a device is noncompliant. Using the violation *Generic* should fit your needs for now, and you can modify the template after.

Then configure the *Critical issues threshold* and put it at the minimum critical issues a device needs to have before it gets isolated.

Putting 1 into that field will isolate the device whenever there is at least one critical issue with the device.

Noeuds Utilisateurs Configuration			
Provisionnement			
ld D	Provisioning Entr	y opswat opswat ×	
	Settings Compliance		Cloner Supprimer
	Sealings Compliance		Cloner Supprimer
	Non compliance violation	Generic X 🗸	Cloner Supprimer
		detected	Cloner Supprimer
	Critical issues threshold	1	Cloner Supprimer
		Raise the non-compliance violation the number of critical issues is greater or equal than this. 0 deactivates it	
Add provisioner -		Format	
		Permer Sauveyaruer	

You can then hit Save and now the device will get isolated whenever it's found as noncompliant.

Step 3: Customize the template

You can now customize the template the violation is using in the *Portal Profile* section. Simply select your portal profile and then go in the *Files* tab.

You can then modify the template violations/generic.html so it displays additionnal information.

You can also customize this violation in the *Violations* section of the administration interface. Refer to the PacketFence Administration Guide for additionnal information about this.