COLLECTIVE INTELLIGENCE

HYBRID CLOUD

www

6

Panda GateDefende

http:/

http:

Ø



How to configure the Panda GateDefender Performa explicit proxy in a Local User Database or in a LDAP server

Copyright notice

© Panda Security 2010. All rights reserved. Neither the documents nor the programs that you may access may be copied, reproduced, translated or transferred to any electronic or readable media without prior written permission from Panda Security, c/ Gran Vía Don Diego López de Haro 4, 48001 Bilbao (Biscay) Spain.

Registered Trademark

Panda Security [™]. TruPrevent: Registered in U.S.A Patent and Trademark Office. Windows Vista and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and other countries. All other product names may be registered trademarks of their respective owners. D. L. BI-1915-07

© Panda Security 2010. All rights reserved.



Table of contents

1.	Introduction	. 4
2.	. Scenarios	. 4
	2.1 Scenario A – Panda GateDefender Performa Local User Database 2.2 Scenario B – Panda GateDefender Performa LDAP User Database	. 4 . 8
3.	. Steps to add the Web Proxy information into the web browse	12

Table of Figures

Figure 1 - Local groups and users	4
Figure 3 - User groups allowed for the explicit proxy	5
Figure 4 - User authentication	6
Figure 5 - List of settings	6
Figure 6 - Profiles: Settings	6
Figure 7 - Assign settings to local profiles	7
Figure 8 - Protection profile management	7
Figure 9 - Protection profile settings	7
Figure 10 - LDAP servers	8
Figure 11 -HTTP/HTTPS - Enable operation as proxy	9
Figure 12 - User groups allowed for the explicit proxy	9
Figure 13 - User authentication	10
Figure 14 - List of settings	10
Figure 15 - Profiles: settings	10
Figure 16 - Assign settings to local profiles	10
Figure 17 - Protection profile management	11
Figure 18 - Protection profile settings	11
Figure 19 - Internet Explorer Lan Settings	12
Figure 20 - Access to page denied	12



1. Introduction

This document describes the steps that need to be followed in order to enable and configure the Panda GateDefender Performa explicit proxy server.

The examples used in this documentation correspond to a network schema with the following general settings:

- GD Console IP: 172.16.1.1
- GD Network IP Defined: 192.168.201.199
- GD Explicit Proxy IP to be created: 192.168.201.10
- Default Network Gateway: 192.168.201.1

Depending on the customer's scenario, you will need to apply the configuration that best matches the network. In this document, the following scenarios are described:

- 1. Scenarios
 - a. Scenario A Panda GateDefender Performa Local User Database
 - b. Scenario B LDAP Server (Active Directory): 192.168.201.2
- 2. Steps to add the Web Proxy information into the web browser.

2. Scenarios

2.1 Scenario A – Panda GateDefender Performa Local User Database

1. Users' definition.

In order to define users, go to **Settings >> System >> Domain users >> Local groups and users** and add the required users and groups.

Status	Settings	Quarantine	Reports	Tools	E-1	He
stem » Dom	ain users » Lo	ocal groups and use	rs			
Name		Email address		Comment		
Test User		test@mydomain.com		Local User Sample		
Import E	port			Add	Modify	Delete
Import E:	port			Add	Modify	Delete
Import E roups Name	port	Members		Add	Modify	Delete
Import E: roups Name Test Group	port	Members Test User		Add Comment Local Group Sample	Modify	Delete
Import E rOUDS Name Test Group	port	Members Test User		Add Comment Local Group Sample	Modify	Delete

Figure 1 - Local groups and users



- 2. Explicit Proxy configuration.
 - a. Go to Settings >> System >> General >> Explicit proxy
 - b. Select the Enable operation as proxy for HTTP/HTTPS checkbox.
 - c. Enter the following data:
 - i. Proxy IP address
 - ii. Network mask
 - iii. HTTP and HTTPs ports on which the proxy will listen.

System » General » Explicit proxy				
🔽 Enable operation as pr	oxy for HTTP/HTTPS			
Proxy IP address:	192.168.201.10			
Netmask:	255.255.255.0			
HTTP port:	8080			
HTTPS port:	8081			
Use authentication	(Basic): <u>Select users</u>			
The proxy will only be a	accessible from subnets defined in <u>internal networks</u>			
Web page cache				
Γ Enable Web pag	ge cache in the proxy Clean			



If you configure the proxy with an IP that already exists on the network, a duplicated IP event is generated, which you will see in the **System Report** screen (a warning will also be displayed in the **Status** screen).

Note: To enable the explicit proxy you must have previously configured the internal networks.

d. Select **Use authentication** checkbox and click **Select users** to configure the groups that can use the internal proxy. Check the needed groups and save the configuration.

Status	Settings	Quarantine	Reports	Tools	<u>Help</u>
User groups a	llowed for the e	xplicit proxy			
Local user group	ps				
V localusers - T	est Group				
Remote user are	DUDS				

Figure 3 - User groups allowed for the explicit proxy

3. Server Authentication.



Configure Authentication through the Proxy. IP Address should be set as the Explicit Proxy's address. In the case below we are using HTTP and HTTPS protocols to authenticate.

Status	Settings	Quarantine	Reports	Tools	
em » Domain	users » Us	er authentication			
vers with validat	tion				
ats you manage servers	s whose user valida	tion will be performed through	a defined LDAP server.		
Name		Server/IP address	Protocol	LDAP server	
Name HTTP Explicit Proxy		Server/IP address 192.168.201.10	Protocol HTTP	LDAP server localusers	
Name HTTP Explicit Proxy HTTPS Explicit Proxy	r:	Server/IP address 192.168.201.10 192.168.201.10	Protocol HTTP HTTPS	LDAP server localusers localusers	
Name HTTP Explicit Proxy HTTPS Explicit Proxy	c	Server/IP address 192.168.201.10 192.168.201.10	Protocol HTTP HTTPS	LDAP server localusers localusers	
Name HTTP Explicit Proxy HTTPS Explicit Proxy	(Server/IP address 192.168.201.10 192.168.201.10	Protocol HTTP HTTPS	LDAP server localusers localusers	

- Figure 4 User authentication
- 4. Protection profile definition

Click Modify or New and set up your modules.

Status	Settings	Quarantine	Reports	Tools		<u>Help</u>
Protection » P	rofiles » List of storn settings that can be	settings used for the different prof	iles.			¥∃Ç¥
Name block_all_sett	ings	Comm	ent .			
				Add	Modify	Delete

Figure 5 - List of settings

To set specific information choose $\mbox{Edit}\ \mbox{Settings}$ to edit the protections for this profile.

Status	Settings	Quarantine	Reports	Tools		<u>Help</u>
Profiles: Settir	igs					
Name:	block_all	_settings				
Configurable m	odules: 🗹 Anti M Cont M Anti 	malware ent Filter spam				
Comments:	₩ IM/P:	PP/VoIP protocol and Web	n filter	Edit settings		
					ОК	Cancel

Figure 6 - Profiles: Settings

Back



Finally click **OK** to apply the new settings within the Settings Profile.

5. Apply the settings to a particular group of users: Assign settings to local profiles

Status	Settings	Quarantine	Reports	Tools		<u>Help</u>
Protection » P	rofiles » Assigr	n settings to loc	al profiles			
Profile		5	ettings			
block_all			block_all_settings			Up Down
				Add Modify	Delete	
						Back

Figure 7 - Assign settings to local profiles

In this exaple, a profile known as **BlockI_all** is created and it will be assigned to the User group **Localusers – Test Group**.

Status	Settings	Quarantine	Reports	Tools	<u>Help</u>
Protection pro	file managemer	nt			
Protection prof	le				
Name: b	lock_all	1			
Apply to:					
🗹 Users:					<u>User management</u>
O User g localus	roup: ers - Test Group 💽				
C Subtre	e/individual users:				
	Figur	e 8 - Protecti	on profile ma	nagement	
Next, choose t	ne settings crea	ited from step 4	and finally clic	k OK to apply th	he new profile.

Settings:	block_all_settings
	🗸 Anti-malware
Modules	🗸 Content Filter
configured:	🗸 Anti-spam
	🗸 IM/P2P/VoIP protocol and Web filte

Figure 9 - Protection profile settings

ОК

Cancel



2.2 Scenario B – Panda GateDefender Performa LDAP User Database

- 1. Define the LDAP Sources in: Settings >> System >> Domain users >> LDAP users.
- 2. In this example:

BaseDN: cn=Users; dc=SampleCompany, dc=local BindDN: cn=Administrator, cn=users, dc=SampleCompany, dc=local

LDAP servers				
Name:	SampleCompany			
Server/IP address:	192.168.201.2			
BaseDN:	cn=Users;dc=SampleCompany,d			
Type of server:	Active Directory			
Schema	Specify the names of the following			
User:				
ObjectClass:	user			
User ID	sAMAccountname			
Name:	name			
Email:	mail			
Description	description			
User group:				
ObjectClass:	group			
Group ID:	cn			
Member:	member			
Description	description			
Port: 389				
└── Make connections via SSL				
Bind DN(*):	cn=Administrator,cn=users,dc=§			
Password (*):	•••••			
Repeat password (*):	•••••			
Figure 10 - LDAP servers				

- 3. Explicit Proxy configuration.
 - a. Go to Settings >> System >> General >> Explicit proxy
 - b. Select the Enable operation as proxy for HTTP/HTTPS checkbox.
 - c. Enter the following data:
 - i. Proxy IP address
 - ii. Network mask



iii. **HTTP and HTTPs ports** on which the proxy will listen.

System » General	» Explicit proxy
Enable operation as pr	oxy for HTTP/HTTPS
Proxy IP address:	192.168.201.10
Netmask:	255.255.255.0
HTTP port:	8080
HTTPS port:	8081
Use authentication	(Basic): <u>Select users</u>
The proxy will only be a	accessible from subnets defined in <u>internal networks</u>
Web page cache	
┌ Enable Web pag	ge cache in the proxy Clean

Figure 11 -HTTP/HTTPS - Enable operation as proxy

If you configure the proxy with an IP that already exists on the network, a duplicated IP event is generated, which you will see in the **System Report** screen (a warning will also be displayed in the **Status** screen).

Note: To enable the explicit proxy you must have previously configured the internal networks.

4. Select **Use authentication** checkbox and click **Select users** to configure the groups that can use the internal proxy. Check the needed groups and save the configuration.

er groups a	llowed for the e	explicit proxy		
Local user grou	ps			
localusers - o	atedefender			
Remote user gr	oups			
LDAP sample	 Acceso compatible con 	versiones anteriores de V	Vindows 2000	
LDAP sample	- AdminSecure			
LDAP sample	- Administradores			
LDAP sample	 Administradores de ese 	quema		
LDAP sample	 Administradores de org 	janización		
LDAP sample	- Admins. del dominio			
LDAP sample	 Controladores de domi 	nio		
LDAP sample	- Creadores de confianz	a de bosque de entrada		
LDAP sample	 Distributed COM Users 			
LDAP sample	- DnsAdmins			
LDAP sample	- DnsUpdateProxy			
LDAP sample	- Duplicadores			
LDAP sample	- Equipos del dominio			
LDAP sample	- Exchange Domain Serv	ers		
LDAP sample	- Exchange Enterprise S	ervers		
LDAP sample	- Grupo GD			
LDAP sample	 Grupo de acceso de au 	torización de Windows		
LDAP sample	- HelpServicesGroup			
LDAP sample	- IIS_WPG			
LUAP sample	- Invitados			
LUAP sample	- Invitados del dominio			
LDAP sample	- Operadores de configu	racion de red		
LDAP sample	- Operadores de copia			
LUAP sample	- opers, de cuentas			

Figure 12 - User groups allowed for the explicit proxy

5. Server Authentication.

Configure Authentication through the Proxy. IP Address should be set as the Explicit Proxy's Address. In the case below HTTP and HTTPS protocols to authenticate is used.





6. Protection profile definition.

Click **Modify** or **New** and set up your modules.

Prote	ection » Profiles » List of sett ts you create custom settings that can be used i	i ngs for the different profiles.	
	Name Block Social Net No Job Social Good	Comment	

Figure 14 - List of settings

To set specific information choose Edit Settings to edit the protections for this profile.

Name:	Block Social Net	
Configurable modules:	✓ Anti-malware	
	Content Filter	
	🛱 Anti-spam	
	₩ IM/P2P/VoIP protocol and Web filter	
Comments:		1
	3	
	Edit settions	1
		OK Cance

Figure 15 - Profiles: settings

Finally click **OK** to apply the new settings within the **Settings Profile**.

7. Apply the settings to a particular group of users: **Assign settings to local profiles**

tection » Profiles » Assign settings to local profiles you create profiles to which to assign custom settings.		
Profile	Settings	
GDTest_Admin	Block Social Net	Up Down
	Add Modify Delete	
		B

Figure 16 - Assign settings to local profiles



In this case, a Profile known as GDTest_Admin is created and it will be assigned to the User group from the SampleCompany LDAP group known as GDTest_Admin.

Protection profile management				
Protection profile				
Name: GDTest_Admin				
Apply to:				
✓ Users:				
 User group: SampleCompany - GDTest_Adm Subtree/individual users: 				
Directories: None				

Figure 17 - Protection profile management

Next choose the **Settings** that you created from step 6 and finally click **OK** to apply the new profile.

Settings:	Block Social Net 💉
	🗸 Anti-malware
Modules	🗸 Content Filter
configured:	🗸 Anti-spam
	✓ IM/P2P/VoIP protocol and Web filter

Figure 18 - Protection profile settings

3. Steps to add the Web Proxy information into the web browse

Finally, regardless of the selected scenario, add the Web Proxy information into the web browser.

For Internet Explorer go to Internet **Options >> Connections >> LAN Settings** and check the box to use a **Proxy server**. Then click **Advanced** and add the proxy along with the ports.

In the case of this test environment, the Panda GateDefender Performa IP was added to the exceptions list.

Internet Options	None	<u></u>				
General Security Privacy Content Connections Pr	Local Area Network (LAN) Settings					
To set up an Internet connection, click Setup. Dial-up and Virtual Private Network settings	 Automatic configuration Automatic configuration may override manual settings. use of manual settings, disable automatic configuration Automatically detect settings 	To ensure the	Proxy Se	ttings Type	Proxy address to use	Port
	Use automatic configuration script Address Proxy server		Ş.	HTTP: Secure:	192.168.201.10 192.168.201.10	: 8080 : 8081
Choose Settings if you need to configure a proxy server for a connection.	Use a proxy server for your LAN (These settings wild dial-up or VPN connections).	I not apply to		FTP: Socks:		
Never dial a connection Dial whenever a network connection is not present Always dial my default connection	Bypass proxy server for local addresses	Mavancea		Use the	e same proxy server for all protocols	
Current None	ОК	Cancel	Exception	Do not use	e proxy server for addresses beginni	ng with:
LAN Settings do not apply to dial-up connections.	LAN settings in None in None	V		Use semic	.1 olons (;) to separate entries.	<
OK Cance	k Social Net K Apply Content Filter				ОК	Cancel

Figure 19 - Internet Explorer Lan Settings

Verify that the sites are being blocked. You should be presented with the Access Denied page.





Note: The Web filter engine works by querying a cache file. When a page is first visited the file is checked and the appropriate action is taken. If the URL is not in the cache, a query is sent to the servers to determine what type of site the URL is classified under. This query then feeds the cache, so that the information about the URL is available for future access attempts. This means that the first time a brand new website is tried within a network the user will be able to get to the home page. Each subsequent visit will choose the appropriate action as normal.