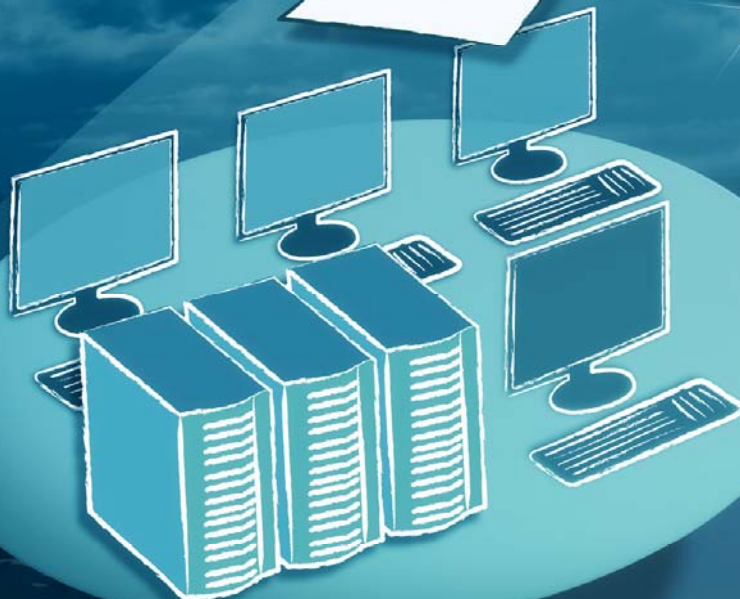


COLLECTIVE INTELLIGENCE

HYBRID
CLOUD





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	4
2.2 Scenario B – Panda GateDefender Performa LDAP User Database	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 2 - Explicit proxy	5
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.

System >> Domain users >> Local groups and users

Users

Name	Email address	Comment
Test User	test@mydomain.com	Local User Sample

Import Export Add Modify Delete

Groups

Name	Members	Comment
Test Group	Test User	Local Group Sample

Import Export Add Modify Delete Back

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 proxy for HTTP/HTTPS

Proxy IP address:

Netmask:

HTTP port:

HTTPS port:

Use authentication (Basic): [Select users](#)

The proxy will only be accessible from subnets defined in [internal networks](#)

Web page cache

Enable Web page cache in the proxy

Figure 2 - Explicit 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.

- 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 [Help](#)

User groups allowed for the explicit proxy

Local user groups

localusers - Test Group

Remote user groups

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 Help

System » Domain users » User authentication

Servers with validation

Lets you manage servers whose user validation will be performed through a defined LDAP server.


Name	Server/IP address	Protocol	LDAP server
HTTP Explicit Proxy	192.168.201.10	HTTP	localusers
HTTPS Explicit Proxy	192.168.201.10	HTTPS	localusers

Figure 4 - User authentication

4. Protection profile definition

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

Status Settings **Quarantine** Reports Tools Help

Protection » Profiles » List of settings 

Lets you create custom settings that can be used for the different profiles.

Name	Comment
block_all_settings	

Add Modify Delete

Back

Figure 5 - List of settings

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

Status Settings **Quarantine** Reports Tools Help

Profiles: Settings

Name:

Configurable modules:

- Anti-malware
- Content Filter
- Anti-spam
- IM/P2P/VoIP protocol and Web filter

Comments:

Edit settings

OK Cancel

Figure 6 - Profiles: Settings

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**



Figure 7 - Assign settings to local profiles

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



Figure 8 - Protection profile management

Next, choose the settings created from step 4 and finally click **OK** to apply the new profile.



Figure 9 - Protection profile settings



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:	<input type="text" value="SampleCompany"/>
Server/IP address:	<input type="text" value="192.168.201.2"/>
BaseDN:	<input type="text" value="cn=Users;dc=SampleCompany,dc=local"/>
Type of server:	<input type="text" value="Active Directory"/>
Schema	<i>Specify the names of the following schema classes</i>
User:	
ObjectClass:	<input type="text" value="user"/>
User ID	<input type="text" value="sAMAccountname"/>
Name:	<input type="text" value="name"/>
Email:	<input type="text" value="mail"/>
Description	<input type="text" value="description"/>
User group:	
ObjectClass:	<input type="text" value="group"/>
Group ID:	<input type="text" value="cn"/>
Member:	<input type="text" value="member"/>
Description	<input type="text" value="description"/>
Port:	<input type="text" value="389"/>
<input type="checkbox"/> Make connections via SSL	
Bind DN(*):	<input type="text" value="cn=Administrator,cn=users,dc=SampleCompany,dc=local"/>
Password (*):	<input type="password" value="....."/>
Repeat password (*):	<input type="password" value="....."/>

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 proxy for HTTP/HTTPS

Proxy IP address:

Netmask:

HTTP port:

HTTPS port:

Use authentication (Basic): [Select users](#)

The proxy will only be accessible from subnets defined in [internal networks](#)

Web page cache

Enable Web page cache in the proxy

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.

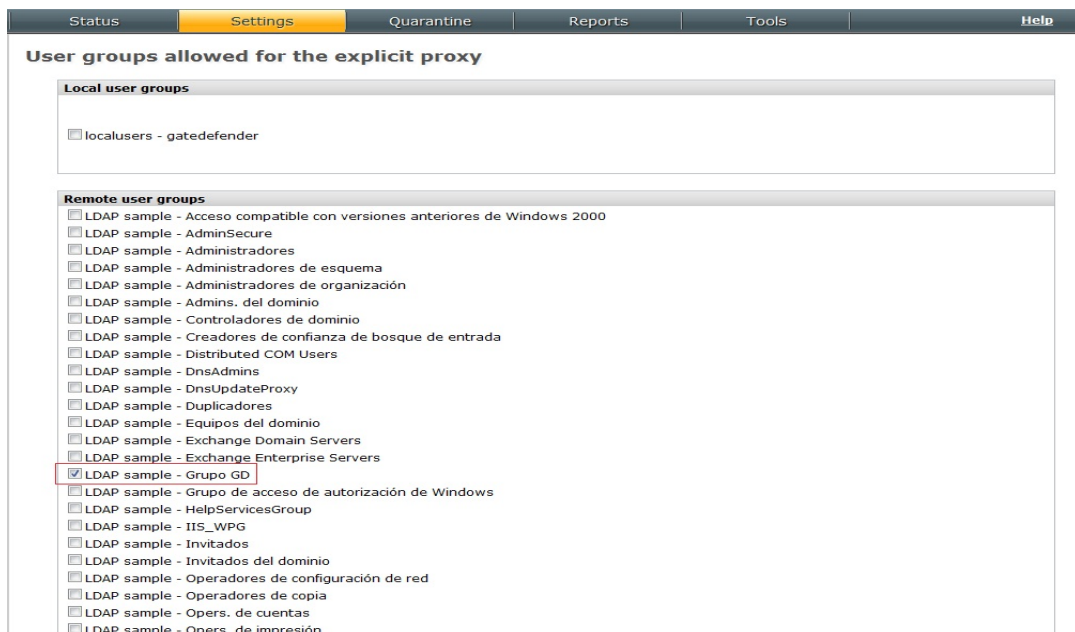


Figure 12 - User groups allowed for the explicit proxy

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.



System » Domain users » User authentication

Servers with validation

Lets you manage servers whose user validation will be performed through a defined LDAP server.

Name	Server/IP address	Protocol	LDAP server
HTTP Server	192.168.201.10	HTTP	SampleCompany
HTTPS Server	192.168.201.10	HTTPS	SampleCompany

Figure 13 - User authentication

6. Protection profile definition.

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

Protection » Profiles » List of settings

Lets you create custom settings that can be used for the different profiles.

Name	Comment
Block Social Net	
No Job Social Good	

Figure 14 - List of settings

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

Profiles: Settings

Name:

Configurable modules:

- Anti-malware
- Content Filter
- Anti-spam
- IM/P2P/VoIP protocol and Web filter

Comments:

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**

Protection » Profiles » Assign settings to local profiles

Lets you create profiles to which to assign custom settings.

Profile	Settings
GDTTest_Admin	Block Social Net

Figure 16 - Assign settings to local profiles



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

Protection profile management

Protection profile

Name:

Apply to:

Users:

User group:

Subtree/individual users:
Directories:
BaseDN:

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:

Modules configured:

- ✓ Anti-malware
- ✓ Content Filter
- ✓ 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 browser

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.

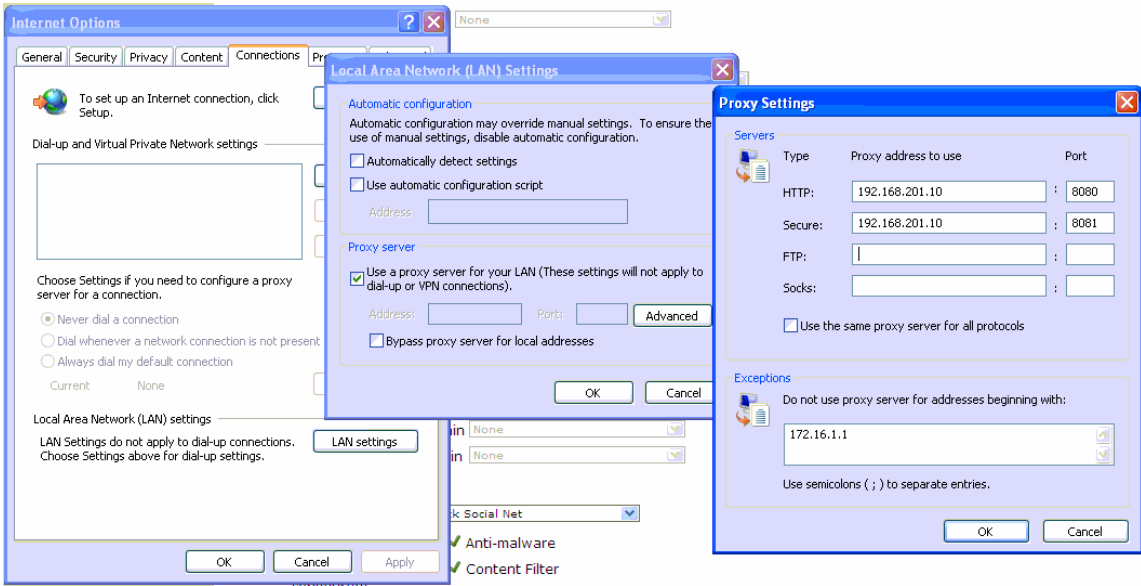


Figure 19 - Internet Explorer Lan Settings

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

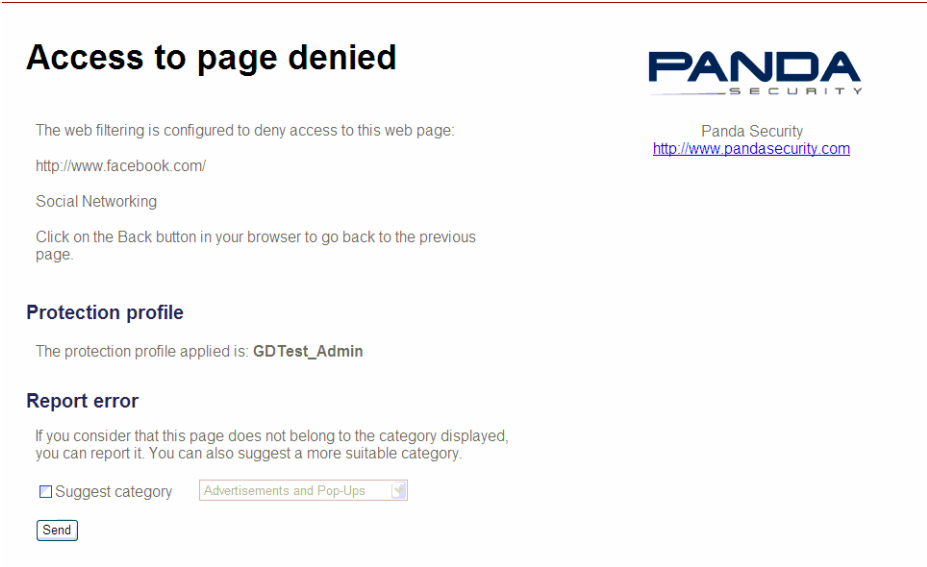


Figure 20 - Access to page denied



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.