

How to Redirect Authentication from a CloudGen Firewall to a Specific Authentication Server

<https://campus.barracuda.com/doc/96026651/>

Authentication redirection is used when a Control Center or a stand-alone firewall forwards user credentials to a dedicated authentication server, e.g., MSAD, RADIUS, LDAP, etc. This intermediary system serves as an authentication proxy.

The CloudGen Firewall, which handles the credentials, must be configured to send the credentials to the authentication proxy, which will then forward the data to the actual authentication server.

The authentication proxy can be of two types:

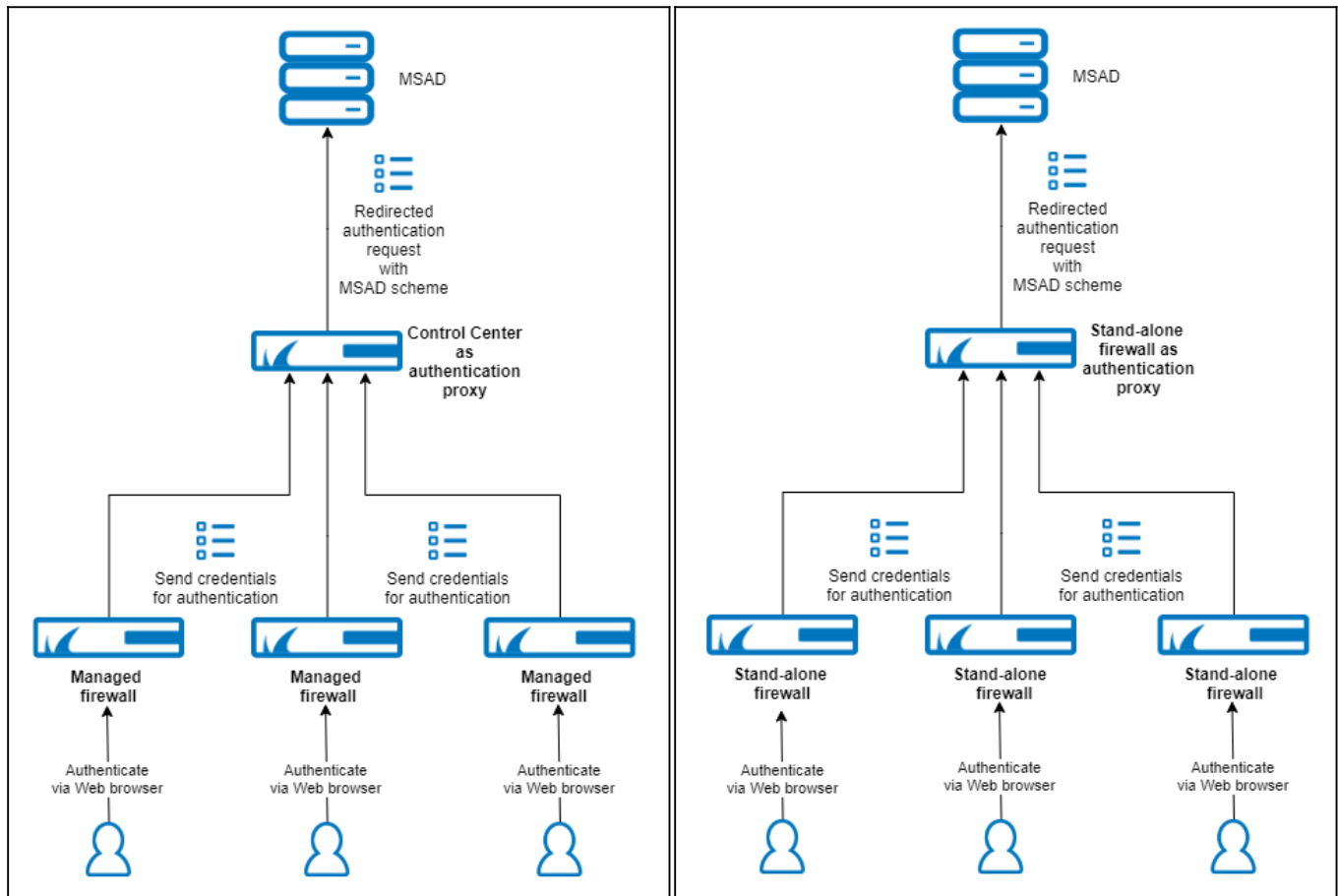
- If it is a Control Center (see image for *CC-Managed Setup* below), it already contains the necessary access rule for forwarding the credential.
- If it is a stand-alone CloudGen Firewall (see image for *Stand-alone Setup* below), an appropriate access rule must be configured on this forwarding system.

The firewall that receives and sends the credentials can be either a managed or a stand-alone firewall.

Use Case

In this example, a user enters credentials into a web-based form in a web browser that then sends the data to a CloudGen Firewall. This firewall is configured to redirect the authentication request to another CloudGen Firewall that effectively handles the authentication request.

Example 1: CC-Managed Setup	Example 2: Stand-Alone Setup
------------------------------------	-------------------------------------



According to various authentication systems available, the following target schemes can be redirected:

- NGFLocal
- MSAD
- LDAP
- TacPlus
- Radius
- RSASecurID

Authentication redirects are transmitted using the UDP protocol on port number 802.

Before You Begin

For a setup with a Control Center as an authentication proxy, ensure the following conditions are met:

- The Control Center must be configured so that it authenticates against a specific authentication server, e.g. MSAD.

For more information on this example, see [How to Configure MSAD Authentication](#).

For more information on other authentication methods, see [Authentication](#).

- The firewall, which handles the credentials, must be configured as a managed firewall and must be connected to its managing Control Center. For more information, see [How to Add a New CloudGen Firewall to the Control Center](#).

For a setup with a stand-alone firewall as an authentication proxy, ensure the following conditions are met:

- A stand-alone CloudGen Firewall must be configured so that it authenticates against a specific authentication server, e.g. MSAD.

For more information on this example, see [How to Configure MSAD Authentication](#).

For more information on other authentication methods, see [Authentication](#).

Example 1: Configure Authentication Redirection for a Managed CloudGen Firewall

When configuring authentication redirection for a managed CloudGen Firewall, the forwarding rule for protocol type UDP, port 802, is already preconfigured on the Control Center. Therefore, the Control Center already knows how to forward authentication requests.

The following steps apply to the use case as shown in the image above for the *CC Managed Setup*.

1. Log into the Control Center that manages the firewall in question.
2. Go to **CONFIGURATION > Configuration Tree > Multi-Range > your range > your cluster > Boxes > your managed box > Infrastructure Service > Authentication Service**.
3. In the left menu, click **Redirect Authentication**.
4. Click **Lock**.
5. For **Redirect Scheme**, select **Yes**.
6. For **Primary box type**, select **CC**. (Note: it is not necessary to enter an explicit IP address because the managed firewall already knows the IP address of its managing Control Center)
7. For **Target Scheme**, select the target scheme that you want to authenticate against, e.g., **MSAD**.

Redirect Information

Redirect Scheme	Yes	
Method	Redirect_Authentication	
User Info Helper Scheme		
Number of Processes	5	
Primary box type	CC	
Explicit Box Address		
Target Scheme	MSAD	<input type="checkbox"/> Other

When authenticating to a managed CloudGen Firewall, your credentials will now be forwarded to the authentication system (e.g., MSAD authentication server) by the Control Center that operates as an authentication proxy.

Example 2: Configure Authentication Redirection for a Stand-Alone CloudGen Firewall

The following steps apply to the use case as shown in the image above for the *Stand-Alone Setup*.

1. Log into the stand-alone firewall that receives the user credentials.
2. Go to **CONFIGURATION > Configuration Tree > Infrastructure Service > Authentication Service**.
3. In the left menu, click **Redirect Authentication**.
4. Click **Lock**.
5. For **Redirect Scheme**, select **Yes**.
6. For **Primary box type**, select **Explicit**.
7. For **Explicit Box Address**, enter the IP address of the forwarding stand-alone firewall.
8. For **Target Scheme**, select the target scheme that you want to authenticate against, e.g., **MSAD**.

Redirect Information

Redirect Scheme	Yes	
Method	Redirect_Authentication	
User Info Helper Scheme		
Number of Processes	5	
Primary box type	Explicit	
Explicit Box Address	10.0.10.1	
Target Scheme	MSAD	<input type="checkbox"/> Other

When configuring authentication redirection for a stand-alone CloudGen Firewall, an access rule must

also be configured to forward an authentication request.

1. Log into the firewall that forwards the authentication request.
2. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
3. Click **Lock**.
4. Click **+** to add a new access rule.
5. The **Edit Rule:New Rule** window is displayed.
6. For the access rule type, select **App Redirect**.
7. For the name of the access rule, enter **AuthRedirect**.
8. For source, enter **Any**.
9. For service, select **<explicit-srv>**.
10. Double-click the first empty line in the list.
11. The **Edit/Create Service Object** window is displayed.
12. Click **New Object**.
13. The **Service Entry Parameters** window is displayed.
14. For **IP Protocol**, select **017 UDP**.
15. For **Port Range**, enter **802**.
16. For **Service Label**, enter **phibs**.

Service Entry Parameters

IP Protocol: 017 UDP

Comment:

TCP & UDP

Port Range: 802

Dyn. Service:

Service Label: phibs

Client Port Used: 1024-65535 (client port range)

From: 1024 To: 65535

ICMP Echo

Max Ping Size: Min Delay: 10 ms

General

Session Timeout: 60 Balanced Timeout: 30

Plugin:

Available Plugins:

Port Protocol Protection

Action for prohibited Protocols: No Protocol Detection

Detection Policy: White Listing

Information

Allow Listing: Only protocols with a match to the Allow List are allowed. - Detected protocols not listed here including unknown protocols will be tagged prohibited.

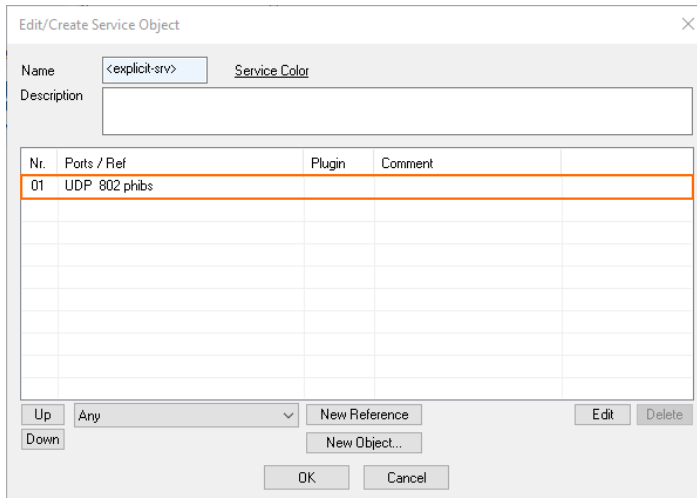
Block Listing: Protocols with a match to the Block List are prohibited. - Detected protocols not listed here will be ignored.

Allow Listed Protocols

- Business
- E-Mail
- Games
- Instant Messaging
- Media Streaming
- Remote Access
- Standard Network
- Tunneling
- VOIP

OK Cancel

17. Click **OK**.



Dialog box: Edit/Create Service Object

Name: <explicit-srv> Service Color

Description:

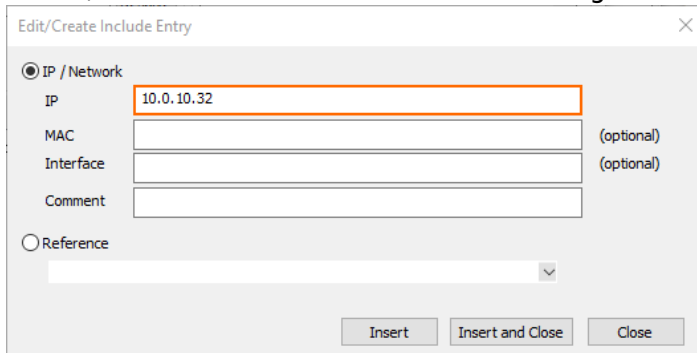
Nr.	Ports / Ref	Plugin	Comment
01	UDP 802 phibs		

Up Any New Reference Edit Delete

Down New Object...

OK Cancel

18. Click **OK**.
19. For **Destination**, select **<explicit-srv>**.
20. Double-click the first empty line in the list.
21. The **Edit/Create Network Object** window is displayed.
22. Click **+** right to **Include Entries**.
23. The **Edit/Create Include Entry** window is displayed.
24. For **IP**, enter the IP address of the forwarding firewall, e.g. 10.0.10.32.



Dialog box: Edit/Create Include Entry

☒ IP / Network

IP: 10.0.10.32

MAC: (optional)

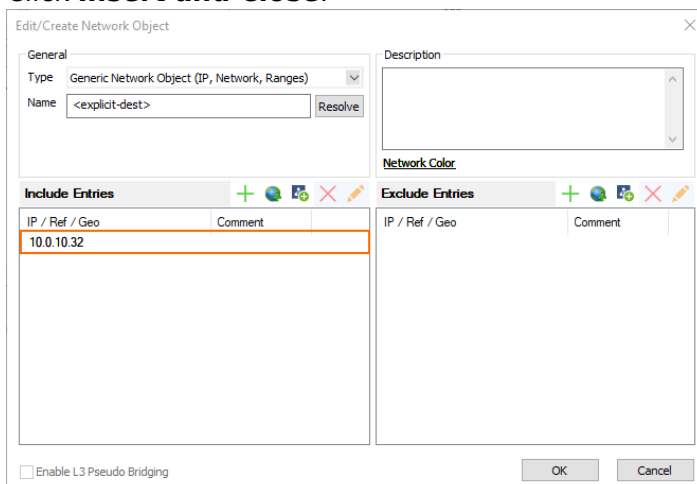
Interface: (optional)

Comment:

☐ Reference

Insert Insert and Close Close

25. Click **Insert and Close**.



Dialog box: Edit/Create Network Object

General

Type: Generic Network Object (IP, Network, Ranges)

Name: <explicit-dest> Resolve

Description:

Network Color:

Include Entries

IP / Ref / Geo	Comment
10.0.10.32	

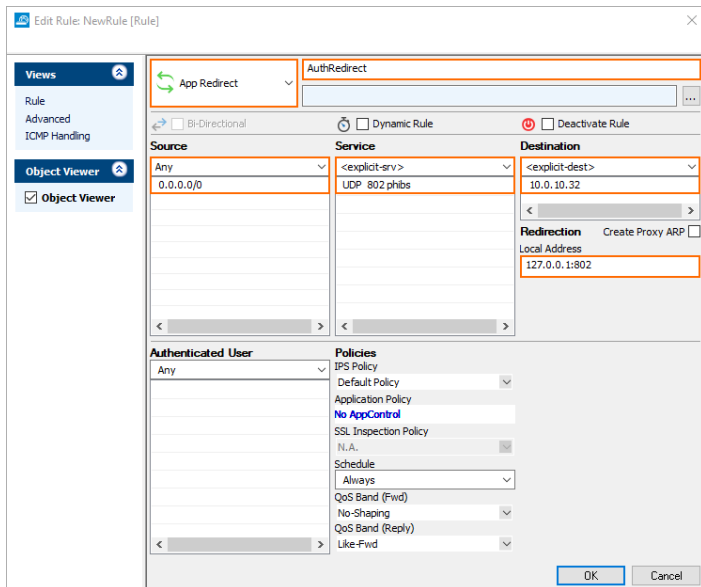
Exclude Entries

IP / Ref / Geo	Comment

☐ Enable L3 Pseudo Bridging

OK Cancel

26. Click **OK**.
27. For **Local Address**, enter 127.0.0.1:802.



28. Click **OK**.

When authenticating to the stand-alone CloudGen Firewall, your credentials will now be forwarded to the authentication system (e.g., MSAD authentication server) by the stand-alone CloudGen Firewall that operates as an authentication proxy.

Figures

1. auth_redirect_managed_cgfs.png
2. auth_redirect_standalone_cgfs.png
3. auth_redirect_configure_managed_box.png
4. auth_redirect_configure_standalone_box.png
5. service_entry_parameters.png
6. create_service_object.png
7. create_include_entry.png
8. create_network_object.png
9. create_new_rule.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.