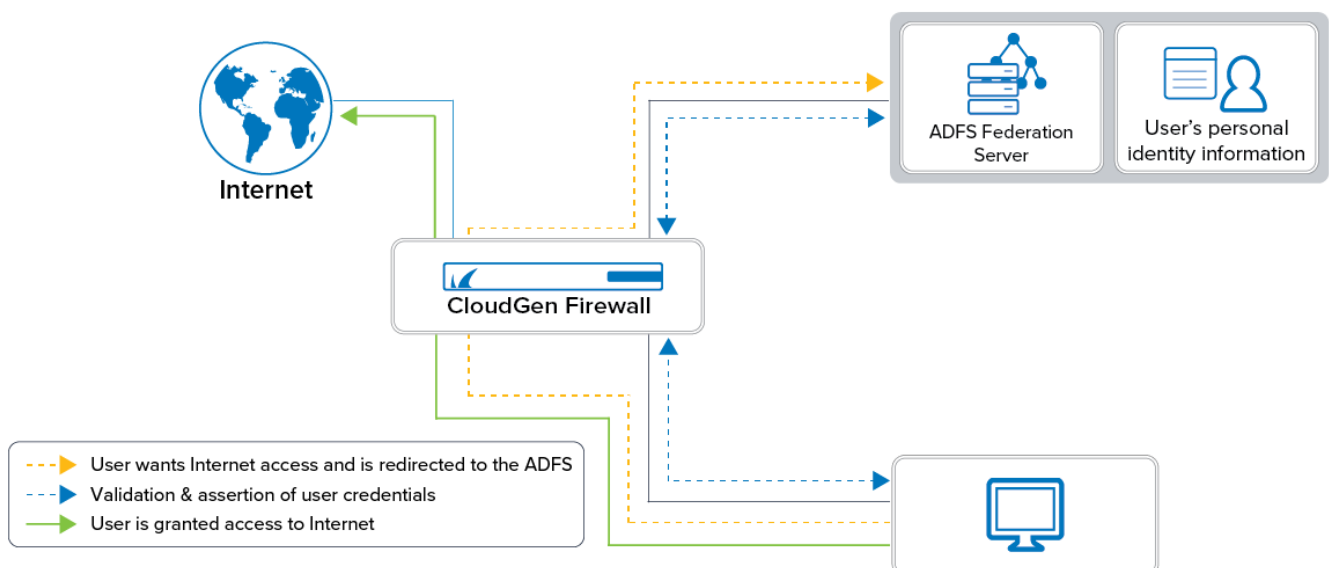


## How to Configure AD FS Authentication

<https://campus.barracuda.com/doc/96026648/>

The Active Directory Federation Service (AD FS) is a service provided by Microsoft that enables users to authenticate across multiple organizations. The credentials are not forwarded to the service provider. Rather, when users contact a service provider, they are forwarded to the AD FS that will provide a token. This token will then be used to verify with the identity provider that the user authenticated successfully. Using the token ensures that the service provider never has access to the actual user credentials. AD FS uses the Security Assertion Markup Language (SAML) for exchanging authentication and authorization information. AD FS is currently provided for HTTPs only. To use AD FS for Client-to-Site VPN, an Advanced Remote Access subscription is required.



AD FS enables transparent single sign-on (i.e., sign in to applications if the user is already signed in on the firewall, and vice versa). This requires a firewall rule to forward the traffic to fwauthd. AD FS authentication supports both offline authentication and inline authentication.

### Step 1. Enable AD FS Authentication on the Firewall

If you are making changes to this main Step 1, you must also execute Step 4 further below.

1. Go to **CONFIGURATION > Configuration Tree > Assigned Services > Firewall > Firewall Forwarding Settings**.
2. In the left menu, click **Authentication**.
3. In the **Authentication Server Configuration** section, import or create the **Default HTTPS Private Key** and **Default HTTPS Certificate**.

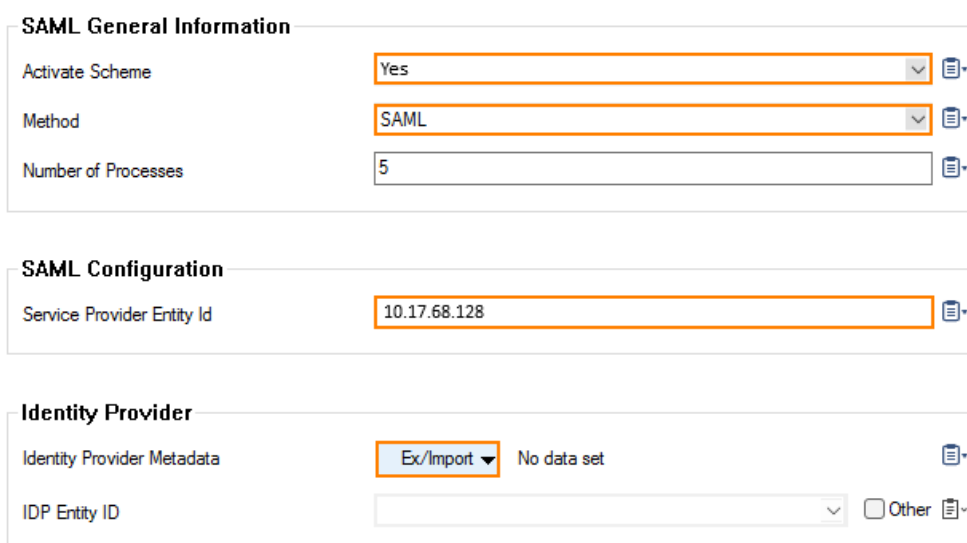
The **Name** of the certificate must be the IP address or an FQDN resolving to the IP

address of the Barracuda CloudGen Firewall. This value is used to redirect the client to the authentication daemon.




4. In the **Metadirectory Authentication** section, set the following values:
  - **Authentication Scheme** - Select **SAML/ADFS** from the list.
  - **Listen IP** - Enter the listening address of the CloudGen Firewall's authentication daemon.
  - **Request Timeout** - Set the value for the timeout for requests.
  - **User ACL Policy**
    - Set the value to **deny-explicit** if you want only domain users listed in User ACL to be blocked.
    - Set the value to **allow-explicit** if you want only domain users listed in User ACL to be allowed.
  - **User ACL** - Click **+** to add or **x** to remove users to or from the ACL list.
  - **URL Filter Overrid Users** - Click **Set/Edit** to configure user-specific credentials.

## Step 2. Configure General AD FS Settings for SAML, Identity Provider, and Certificates


1. Go to **CONFIGURATION > Configuration Tree > Infrastructure Service > SAML/ADFS Authentication**.
2. Set **Activate Scheme** to **yes**.
3. For **Method**, select **SAML**.
4. In the section **SAML Configuration**, enter the IP address for **Service Provider Entity ID**.
5. In the section **Identity Provider**, click **Ex/Import** to import the identity provider's metadata. The metadata in the imported XML file contains important information about the identity provider and the person's identity and is commonly generated by AD FS.





**SAML General Information**

Activate Scheme	Yes	
Method	SAML	
Number of Processes	5	

**SAML Configuration**

Service Provider Entity Id	10.17.68.128	
----------------------------	--------------	---

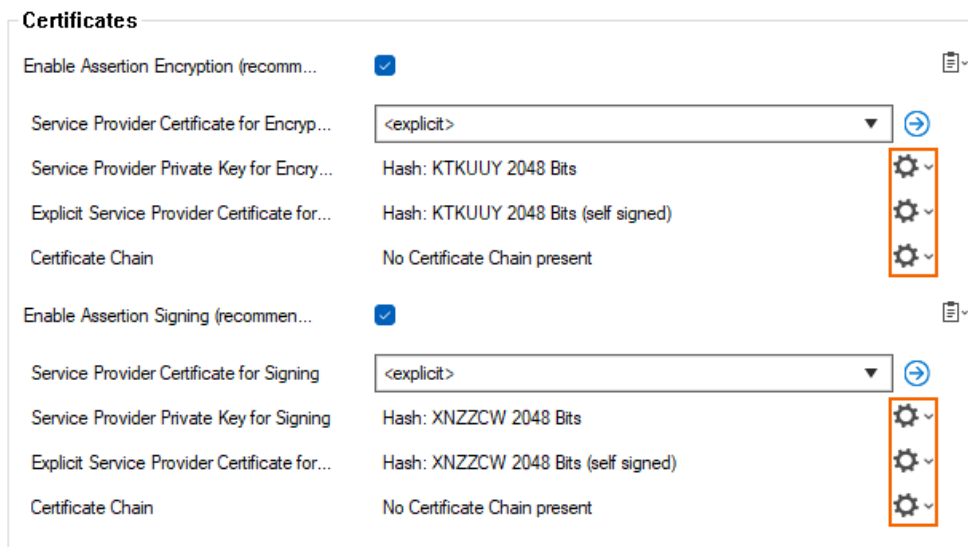
**Identity Provider**

Identity Provider Metadata	Ex/Import	No data set	
IDP Entity ID		<input type="checkbox"/> Other	

6. In the section **Certificates**, use the cogwheel icons on the right to configure certificates and keys:
  - **Service Provider Private Key for Encryption**
    - **Create New Key** - Click to create a new key.

- **Ex/Import** – Click to ex/import a key for encryption.
- **Service Provider Certificate for Encryption**
  - **Edit/Show** – Click to show the provider certificate.
  - **Ex/Import** – Click to ex/import a certificate for encryption.
- **Service Provider Private Key for Signing**
  - **Create New Key** – Click to create a new private key for signing.
  - **Ex/Import** – Click to ex/import a certificate for encryption.
- **Service Provider Certificate for Signing**
  - **Edit/Show** – Click to show the provider certificate for signing.
  - **Ex/Import** – Click to ex/import the service provider certificate for signing.

7. Click **Send Changes** and **Activate**.

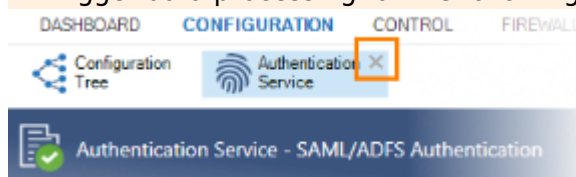


Certificates	
Enable Assertion Encryption (recomm...	<input checked="" type="checkbox"/>
Service Provider Certificate for Encryp...	<explicit> [gear icon]
Service Provider Private Key for Encry...	Hash: KTKUUY 2048 Bits [gear icon]
Explicit Service Provider Certificate for...	Hash: KTKUUY 2048 Bits (self signed) [gear icon]
Certificate Chain	No Certificate Chain present [gear icon]
Enable Assertion Signing (recommen...	<input checked="" type="checkbox"/>
Service Provider Certificate for Signing	<explicit> [gear icon]
Service Provider Private Key for Signing	Hash: XNZZCW 2048 Bits [gear icon]
Explicit Service Provider Certificate for...	Hash: XNZZCW 2048 Bits (self signed) [gear icon]
Certificate Chain	No Certificate Chain present [gear icon]

8. Click **Activate**.

9. Close the tab **Authentication Service**.

It is important to explicitly close the tab for Authentication Service because closing will trigger data processing for the following step.



After clicking **Activate** and closing the Authentication Service tab, the user's attributes stored in the **Identity Provider Metadata** will be extracted to the list for **IDP Entity ID**.

### Step 3. Configure a Specific Attribute for the Authentication of the Remote User

1. Click the field of the list for **IDP Entity ID**.
2. Select an attribute that optimally fits the configuration of the remote user.
3. Click **Send Changes** and **Activate**.

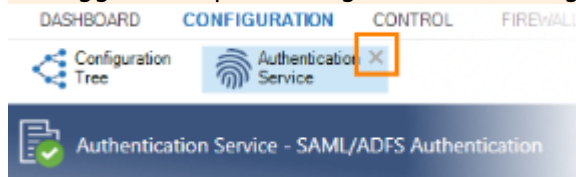
**Identity Provider**

Identity Provider Metadata Ex/Import ▾ No data set 📄

IDP Entity ID  ☒ Other 📄

4. Close the tab **Authentication Service**.

It is important to explicitly close the tab for Authentication Service because closing will trigger data processing for the following step.



## Step 4. Export the Service Provider Metadata

1. Click **Generate Data** in the section **Service Provider Metadata** to export the metadata.
2. Specify a location where to store the file.

**Service Provider Metadata**

📘 The service provider metadata will be available after activation of the SAML/ADFS configuration.

Generate Data

3. Click **Send Changes** and **Activate**.
4. Close the tab **Authentication Service**.

## Step 5. Create Access Rules for Authenticating with AD FS

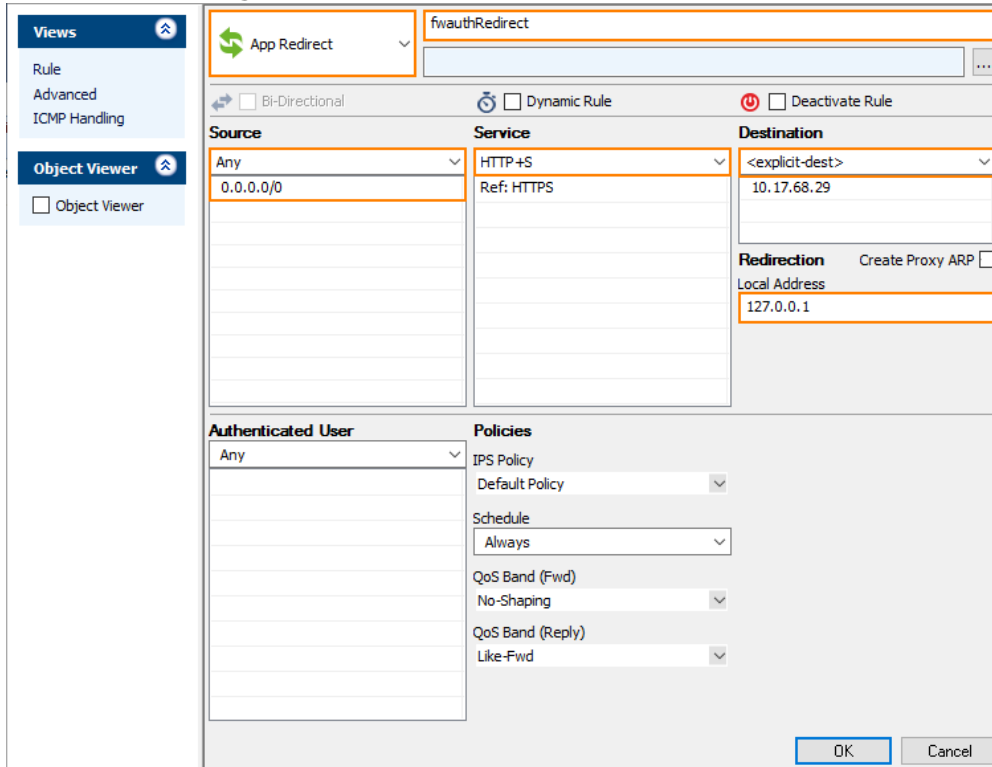
Create an access rule for redirecting users for authentication.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Either click the plus icon (+) in the top right of the ruleset, or right-click the ruleset and select **New > Rule**.



4. Select **App Redirect** as the action.
5. Enter a **Name** for the rule. For example, fwauthredirect.
6. Specify the following settings that must be matched by the traffic to be handled by the access rule:
  - **Source** – The source addresses of the traffic, e.g., 0.0.0.0/0.
  - **Service** – Select **HTTPS** from the list.
  - **Destination** – Enter the IP address of the CloudGen Firewall, e.g., 10.17.68.29.


7. Enter the **Redirection** IP address and optional port as the **Local Address**. For example, 127.0.0.1.
8. Click **OK**.
9. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located *above* the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.
10. Click **Send Changes** and **Activate**.



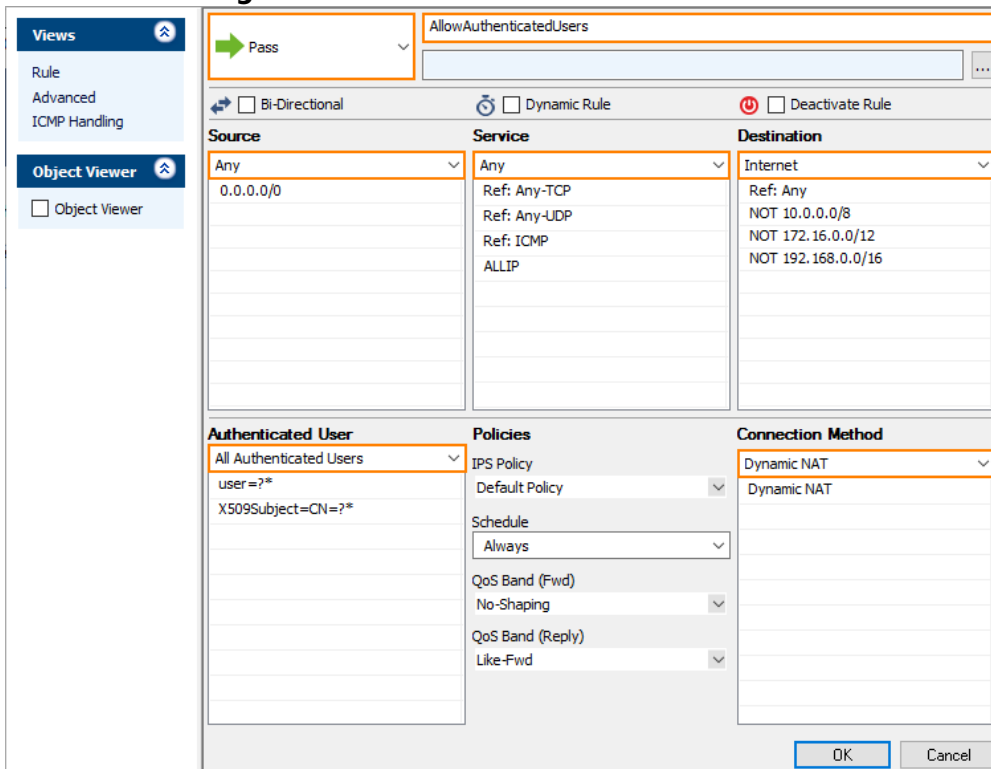
The screenshot shows the 'App Redirect' rule configuration window. The rule name is 'fwauthRedirect'. The 'Source' is set to 'Any' (0.0.0.0/0). The 'Service' is set to 'HTTP+S' with a reference to 'HTTPS'. The 'Destination' is set to '<explicit-dest>' (10.17.68.29). The 'Redirection' section shows 'Local Address' as '127.0.0.1'. The 'Authenticated User' is set to 'Any'. The 'Policies' section includes 'IPS Policy' (Default Policy), 'Schedule' (Always), 'QoS Band (Fwd)' (No-Shaping), and 'QoS Band (Reply)' (Like-Fwd). The 'OK' and 'Cancel' buttons are at the bottom right.

## Step 6. Create an Access Rule for Passing Authenticated Users

Authenticated users can be passed on when authenticated already.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
  2. Click **Lock**.
  3. Either click the plus icon (+) in the top right of the ruleset, or right-click the ruleset and select **New > Rule**.
- 
4. Select **Pass** as the action.
  5. Enter a **Name** for the rule. For example, AllowAuthenticatedUsers.
  6. Specify the following settings that must be matched by the traffic to be handled by the access rule:
    - **Source** - The source addresses of the traffic, e.g., 0.0.0.0/0.

- **Service** - Select **ANY** from the list.
  - **Destination** - Select **Internet**.
7. **Authenticated User** - Select **All Authenticated Users** from the list.
  8. **Connection Method** - Select **Dynamic NAT** from the list.
  9. Click **OK**.
  10. Drag and drop the access rule so that it is the first rule that matches the traffic that you want it to forward. Ensure that the rule is located *above* the BLOCKALL rule; rules located below the BLOCKALL rule are never executed.
  11. Click **Send Changes** and **Activate**.



Views: Rule, Advanced, ICMP Handling, Object Viewer

Object Viewer: ☐ Object Viewer

Pass

AllowAuthenticatedUsers

☐ Bi-Directional ☐ Dynamic Rule ☐ Deactivate Rule

Source	Service	Destination
Any 0.0.0.0/0	Any Ref: Any-TCP Ref: Any-UDP Ref: ICMP ALLIP	Internet Ref: Any NOT 10.0.0.0/8 NOT 172.16.0.0/12 NOT 192.168.0.0/16

Authenticated User	Policies	Connection Method
All Authenticated Users user=?* X509Subject=CN=?*	IPS Policy Default Policy Schedule Always QoS Band (Fwd) No-Shaping QoS Band (Reply) Like-Fwd	Dynamic NAT Dynamic NAT

OK Cancel

You can now authenticate against AD FS.

## Figures

1. adfs\_overview\_80.png
2. configure\_saml\_adfs\_authentication\_step1.png
3. configure\_saml\_adfs\_authentication\_scheme\_step1a.png
4. configure\_saml\_adfs\_authentication\_scheme\_step2a.png
5. configure\_saml\_adfs\_authentication\_step2.png
6. configure\_saml\_adfs\_authentication\_scheme\_step2a.png
7. configure\_saml\_adfs\_authentication\_step3.png
8. FW\_Rule\_Add01.png
9. fwauthRedirect\_access\_rule\_01.png
10. FW\_Rule\_Add01.png
11. allowAuthenticatedUsers\_access\_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.