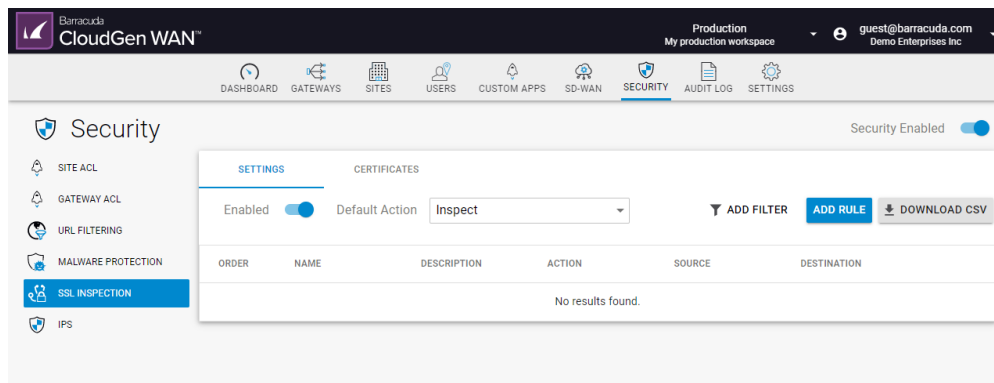


SSL Inspection

<https://campus.barracuda.com/doc/93882903/>

SSL Inspection decrypts both SSL and TLS connections so the appliance can allow features, such as [Malware Protection](#) and [IPS](#), to scan traffic that would otherwise not be visible to the service.



Before You Begin

- If you want to select users or groups in the policies, you must first connect your Azure Active Directory. For more information, see [How to Connect Your Azure Active Directory with Barracuda Cloud Control](#).
- SSL Inspection does not support the QUIC protocol used by Google Chrome and therefore will not inspect traffic using QUIC. If you want to use SSL Inspection for all traffic, you must block the QUIC protocol on the corresponding CloudGen Firewall. For instructions, see Step 3 in [How to Configure Google Accounts Filtering in the Firewall](#) in the CloudGen Firewall documentation.

Settings

In this section, you can add explicit rules, such as exemptions for traffic that should not be scanned. For example: financial traffic. In addition, you can specify the default action for SSL Inspection.

Add a Rule

1. Open <https://cloudgenwan.barracudanetworks.com/> and log in with your existing Barracuda Cloud Control account.
2. Go to **SECURITY > SSL INSPECTION > SETTINGS**.
3. Click **ADD RULE**.
4. The **Add New Rule** window opens. Specify values for the following:
 - **Name** – Enter a name.

- **Description** – Enter description.
- **Action** – Select either **Inspect** or **Do Not Inspect**.

SOURCE CRITERIA

- **Type** – Select a type. You can choose between IP/Network, Site, and User/Group. If you want to select users or groups in the policies, you must first connect your Azure Active Directory. For more information, see [How to Connect Your Azure Active Directory with Barracuda Cloud Control](#).
- **IP/Network** – Enter an IP or network address.

DESTINATION CRITERIA

- **Type** – Select a type. You can choose between **Application**, **URL Category**, **Domain**, **IP/Network**, and **Site**.
- **Application** – Select an application. For more information, see [How to Create Custom Applications](#).

Add New Rule ×

i Name *

IgnoreFinancials

i Description

i Action *

Do Not Inspect ▼

SOURCE CRITERIA

Type *

Site ▼

All Sites

☒

DESTINATION CRITERIA

Type *

URL Category ▼

i Category *

Finance & Investment ×

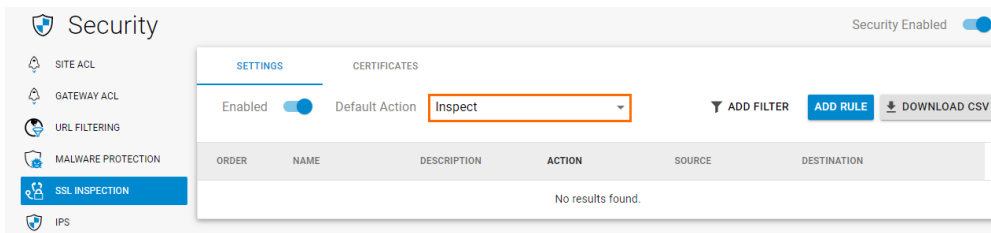
▼

CANCEL **SAVE**

5. Click **SAVE**.

Select the Default Action

1. Open <https://cloudgenwan.barracudanetworks.com/> and log in with your existing Barracuda Cloud Control account.
2. Go to **SECURITY > SSL INSPECTION > SETTINGS**.
3. Select the default action.

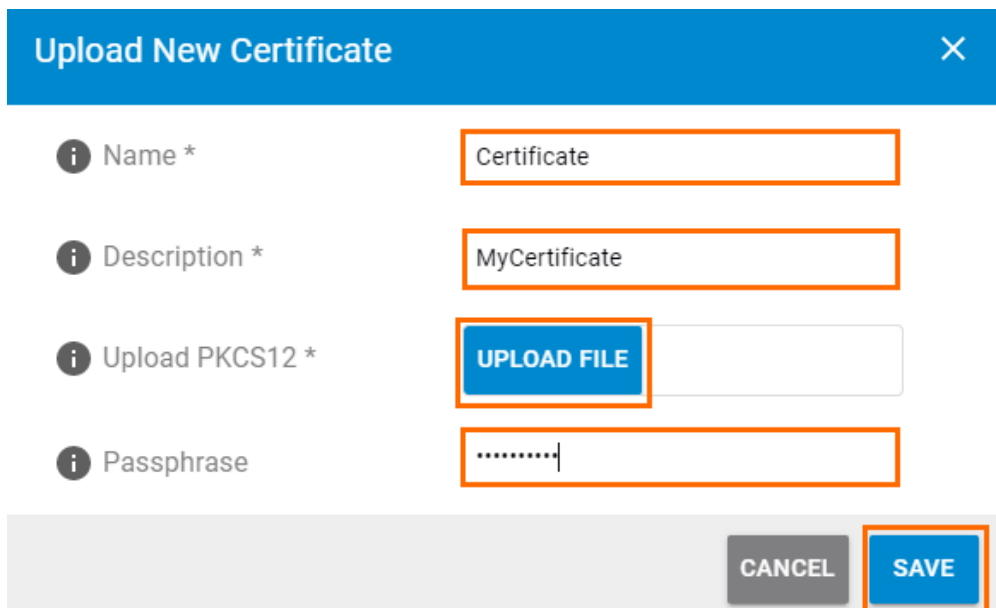


Certificates

In this section, you can add, edit, and activate SSL Inspection certificates and trusted root certificate authorities.

Add SSL Inspection Certificate

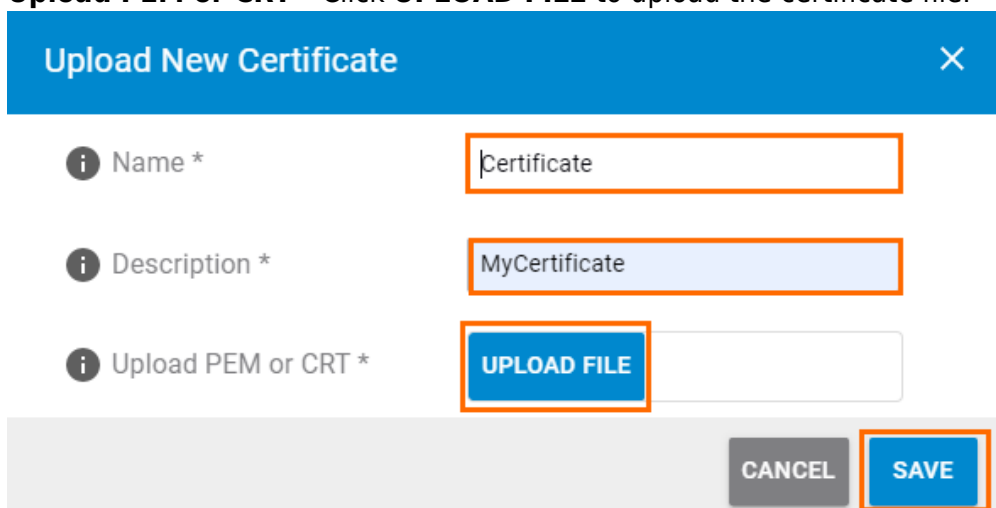
1. Open <https://cloudgenwan.barracudanetworks.com/> and log in with your existing Barracuda Cloud Control account.
2. Go to **SECURITY > SSL INSPECTION > CERTIFICATES**.
3. In the **SSL INSPECTION CERTIFICATES** section, click **ADD CERTIFICATE**.
4. The **Upload New Certificate** window opens. Specify values for the following:
 - **Name** – Enter a name.
 - **Description** – Enter a description.
 - **Upload PKCS12** – Click **UPLOAD FILE** to upload the certificate file.
 - **Passphrase** – Enter the passphrase of the certificate.



5. Click **SAVE**.

Add Trusted Root Certificate Authorities

1. Open <https://cloudgenwan.barracudanetworks.com/> and log in with your existing Barracuda Cloud Control account.
2. Go to **SECURITY > SSL INSPECTION > CERTIFICATES**.
3. In the **TRUSTED ROOT CERTIFICATE AUTHORITIES** section, click **ADD CERTIFICATE**.
4. The **Upload New Certificate** window opens. Specify values for the following:
 - **Name** – Enter a name.
 - **Description** – Enter a description
 - **Upload PEM or CRT** – Click **UPLOAD FILE** to upload the certificate file.



5. Click **SAVE**.

Edit, Delete, or Activate an Existing Certificate

Note that only certificates added in the SSL Inspection section can be activated.

- **MAKE ACTIVE** – Click on the button next to the certificate you want to activate.
- Edit – Click on the pencil icon next to the certificate you want to edit.
- Delete – Click on the **X** icon next to the certificate you want to delete.

Further Information

- For more information on Malware Protection, see [Malware Protection](#).
- For more information on Intrusion Prevention, see [IPS](#).

Figures

1. ssl_82.png
2. explicit_ignore_financial.png
3. sssl_default_82.png
4. cert82_upload1.png
5. cert82_upload2.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.