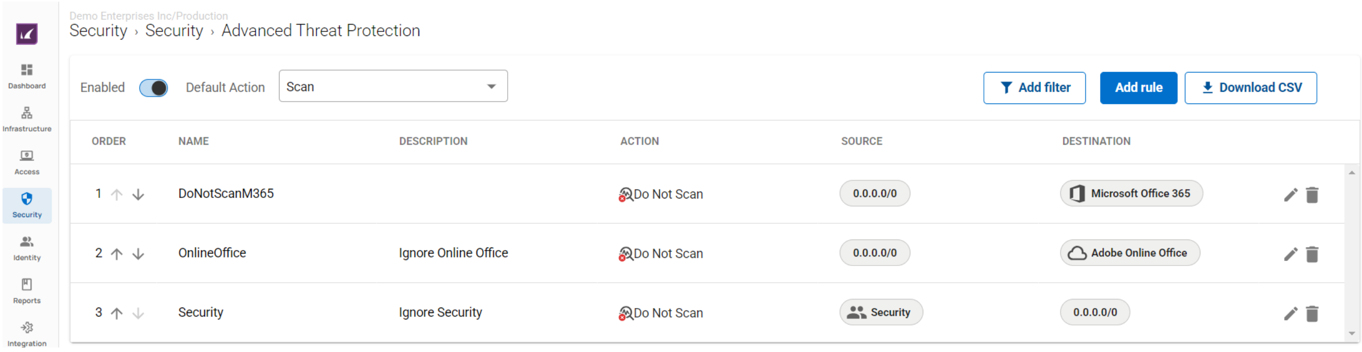
Advanced Threat Protection

https://campus.barracuda.com/doc/26689/

Advanced Threat Protection (ATP) offers protection against advanced malware, zero-day exploits, and targeted attacks not detected by the intrusion prevention system by scanning downloaded files. The user receives the downloaded file immediately after the hash DB lookup, which compares a hash of the file with the Barracuda database to see if it is a malicious file. Simultaneously, the file is uploaded to the Barracuda ATP cloud, but only if the file is 10 megabytes or less. Archives are unpacked and the files they contain are sent to the ATP cloud with the same restriction that only unpacked files 10 megabytes or less are sent to the ATP cloud for inspection. In the ATP cloud, those files are emulated in a virtual sandbox and their behaviour is analyzed. Depending on the behaviour of the file, it is assigned a threat level that is transmitted to the appliance. If the threat level exceeds the ATP threat level threshold, the file is blocked; otherwise, it is delivered.



Enabled ● Default Action: Scan

ORDER	NAME	DESCRIPTION	ACTION	SOURCE	DESTINATION
1	DoNotScanM365		Do Not Scan	0.0.0.0/0	Microsoft Office 365
2	OnlineOffice	Ignore Online Office	Do Not Scan	0.0.0.0/0	Adobe Online Office
3	Security	Ignore Security	Do Not Scan	Security	0.0.0.0/0

Advanced Threat Protection can be used for HTTP, HTTPS, FTP, and FTPS traffic. For HTTPS and FTPS, SSL Inspection must be activated.

The following file types are scanned by the Barracuda ATP cloud:

- **Microsoft Office files** – doc, docx, ppt, pps, pptx, ppsx, xls, xlsx
- **OpenOffice** – rtf, open office document extensions
- **Microsoft executables** – exe, msi, class, wsf
- **macOS executables**
- **PDF documents** – pdf
- **Android APK files** – apk
- **ZIP Archives** – 7z, lzh, bz, bz2, chm, cab, zip
- **RAR Archives** – rar4 and rar5
- **TAR Archives** – tar
- **GZ Content** – Content compressed with gzip

Risk Scores

The ATP service classifies all files in one of four categories:

- **High** – Files classified as high risk exhibit behavior normally only found in malware.
- **Medium** – Files classified as medium risk pose a potential risk.
- **Low** – Files classified as low risk are considered to be harmless. Some residual risk remains.
- **None** – No suspicious activity was detected.

Reporting

SecureEdge Reporting allows you to collect data for reports for your connected Sites when Web Filtering is enabled. The Reporting data is streamed according to your selected region. For more information on logs and reporting, see SecureEdge Reporting.

In addition, you can create reports and notifications using an Azure Log Analytics workspace. Your Barracuda SecureEdge service must be connected to the Azure Log Analytics workspace via the Azure Log Analytics Daemon.

For more Information, see:

- How to Configure Log Streaming to Microsoft Azure Log Analytics Workspace.
- How to Configure Log Streaming via the Azure Log Analytics Daemon in SecureEdge.

Maximum Number of Scans

Scale Units Gateway	Maximum Scans per Minute	Maximum Scans per Month
2	100	2 000 000
4	100	2 000 000
10	100	2 000 000
14	100	2 000 000
20	100	2 000 000
30	150	3 000 000
40	150	3 000 000
60	200	4 000 000
80	250	5 000 000

Before You Begin

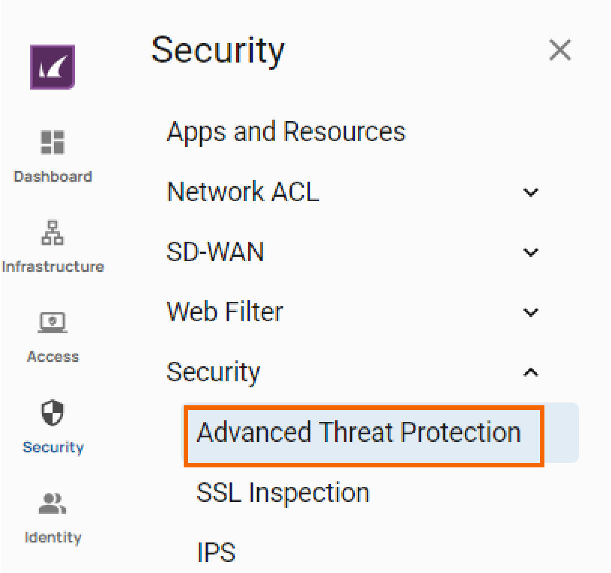
- If you want to use the users or groups from user directories (such as Microsoft Entra ID, LDAP, Google Workspace, Okta, SCIM, and Barracuda Cloud Control) in network policies, you must first connect your SecureEdge Identity Management in order to synchronize users and groups. For more information, see Identity Management.
- If you want to select users or groups from user directories such as BCC-linked Microsoft Entra ID or the BCC-linked LDAP directory in the policies, you must first connect your directory with

Barracuda Cloud Control in order to synchronize users and groups. For more information, see LDAP Active Directory and Microsoft Entra ID and How to Connect Microsoft Entra ID with Barracuda Cloud Control.

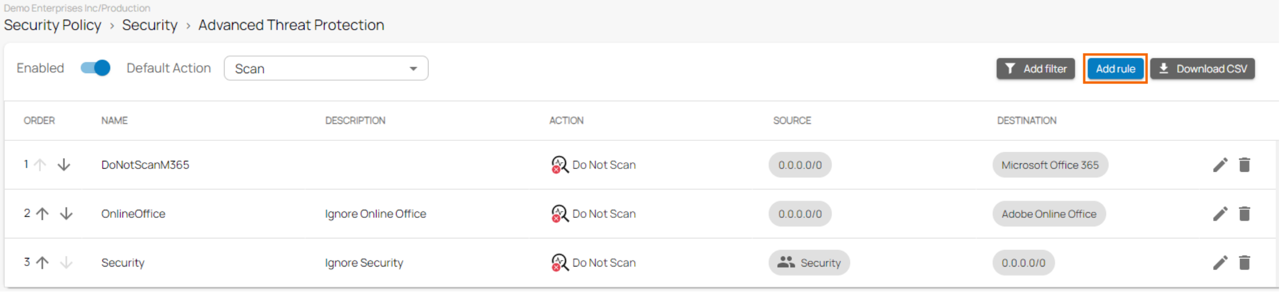
- Enable SSL Inspection.

Create Advanced Threat Protection Rules

1. Go to https://se.barracudanetworks.com and log in with your existing Barracuda Cloud Control account.
2. Go to **Security**.
3. Expand the **Security** menu on the left and select **Advanced Threat Protection**.



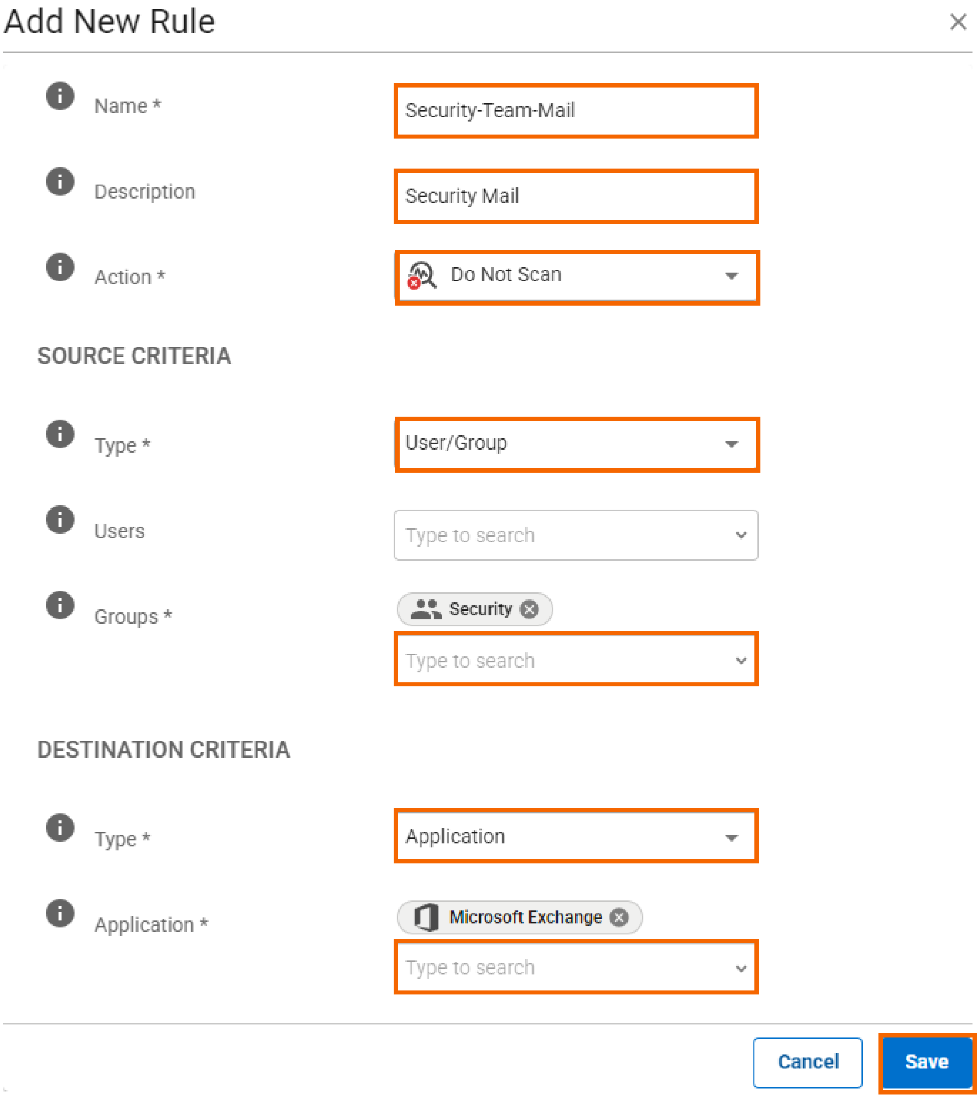
4. The **Advanced Threat Protection** window opens. To create a new rule, click **Add Rule**.


Demo Enterprises Inc/Production
Security Policy › Security › Advanced Threat Protection
Enabled
Default Action
Scan
Add filter
Add rule
Download CSV

ORDER	NAME	DESCRIPTION	ACTION	SOURCE	DESTINATION
1	DoNotScanM365		Do Not Scan	0.0.0.0/0	Microsoft Office 365
2	OnlineOffice	Ignore Online Office	Do Not Scan	0.0.0.0/0	Adobe Online Office
3	Security	Ignore Security	Do Not Scan	Security	0.0.0.0/0

5. The **Add New Rule** window opens. Specify values for the following:
   - **Name** – Enter a name for the rule.
   - **Description** – Enter a brief description for the rule.
   - **Action** – Select an action. You can choose either **Scan** or **Do not Scan**.
   - In the **SOURCE CRITERIA** section, specify values for the following:
     - **Type** – Select a source type. You can choose between **IP/Network**, **Site**, and **User/Group**.
       - If you select **Site**, the **All Sites** option is enabled by default. However, you can add a specific Site after disabling **All Sites**.

        - If you select **IP/Network**, specify values for the following:
            - **IP/Network** – Enter an IP or network address.
        - If you select **User/Group**, you must add one or more users/groups from the drop-down menu, or type to search.
    - In the **DESTINATION CRITERIA** section, specify values for the following:
        - **Type** – Select a destination type. You can choose between **Application**, **Domain**, **IP/Network**, and **Site**.
        - **Application** – Select an application. For more information, see [How to Create Custom Applications](#).



Add New Rule

Name * Security-Team-Mail

Description Security Mail

Action * Do Not Scan

SOURCE CRITERIA

Type * User/Group

Users Type to search

Groups * Security

Type to search

DESTINATION CRITERIA

Type * Application

Application * Microsoft Exchange

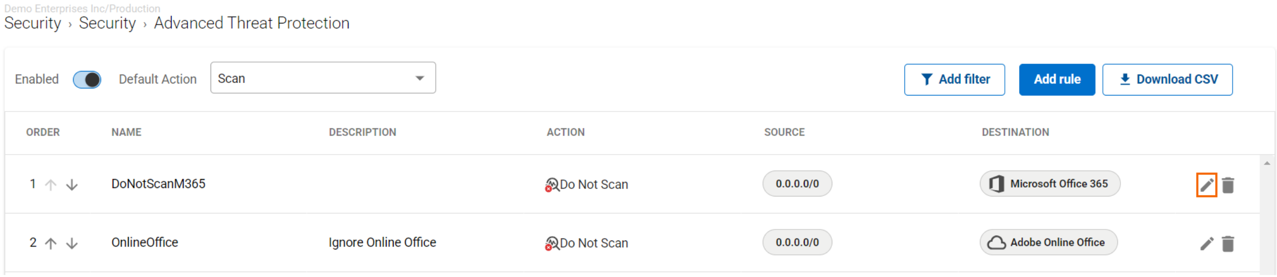
Type to search

6. Click **Save**.

Edit an Existing Rule

1. In the left menu, click **Security**.
2. Expand the **Security** menu on the left and select **Advanced Threat Protection**.

3. The **Advanced Threat Protection** window opens. Click on the pencil icon next to the rule you want to edit.



Demo Enterprises Inc/Production
Security › Security › Advanced Threat Protection

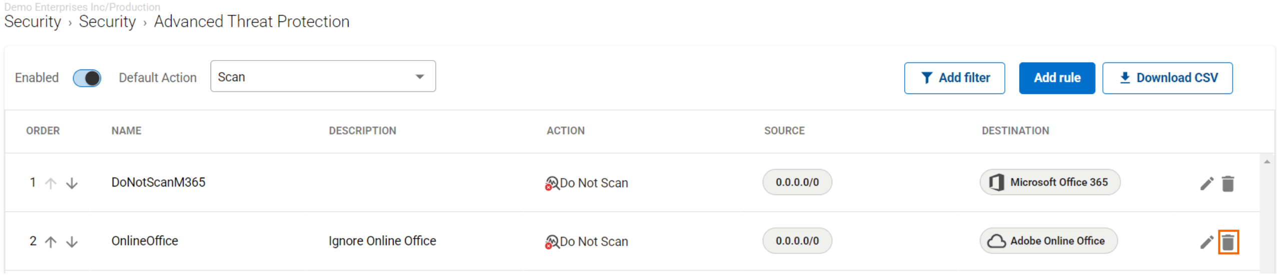
Enabled ● Default Action: Scan

ORDER	NAME	DESCRIPTION	ACTION	SOURCE	DESTINATION
1	DoNotScanM365		Do Not Scan	0.0.0.0/0	Microsoft Office 365
2	OnlineOffice	Ignore Online Office	Do Not Scan	0.0.0.0/0	Adobe Online Office

4. The **Edit Rule** window opens. Edit the value you are interested in.
5. Click **Save**.

Remove an Existing Rule

1. In the left menu, click **Security**.
2. Expand the **Security** menu on the left and select **Advanced Threat Protection**.
3. The **Advanced Threat Protection** window opens. Click on the trash can icon next to the rule you want to remove.

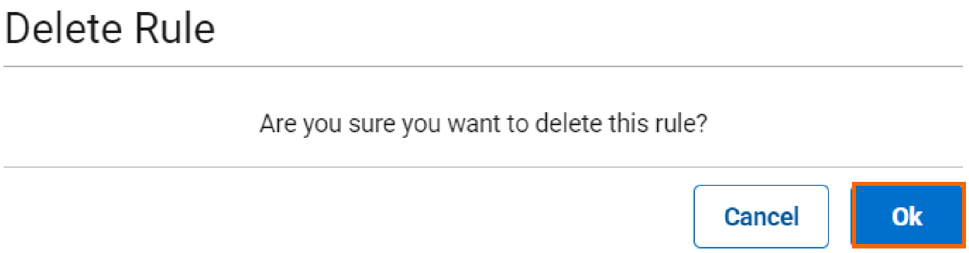


Demo Enterprises Inc/Production
Security › Security › Advanced Threat Protection

Enabled ● Default Action: Scan

ORDER	NAME	DESCRIPTION	ACTION	SOURCE	DESTINATION
1	DoNotScanM365		Do Not Scan	0.0.0.0/0	Microsoft Office 365
2	OnlineOffice	Ignore Online Office	Do Not Scan	0.0.0.0/0	Adobe Online Office

4. The **Delete Rule** window opens.



Delete Rule

Are you sure you want to delete this rule?

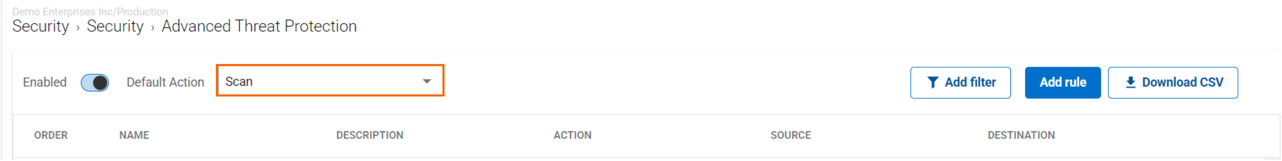
5. Click **OK** to confirm.

Select the Default Action

You can configure Advanced Threat Protection to either scan or not scan by default.

1. Go to https://se.barracudanetworks.com and log in with your existing Barracuda Cloud Control

account.
2. Go to **Security**.
3. Expand the **Security** menu on the left and select **Advanced Threat Protection**.
4. The **Advanced Threat Protection** page opens. Select the **Default Action**. You can choose either **Scan** or **Do not Scan**.



Further Information

- For more information on User and Groups, see How to Connect Microsoft Entra ID with Barracuda Cloud Control.

Figures

© Barracuda Networks Inc., 2025 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.