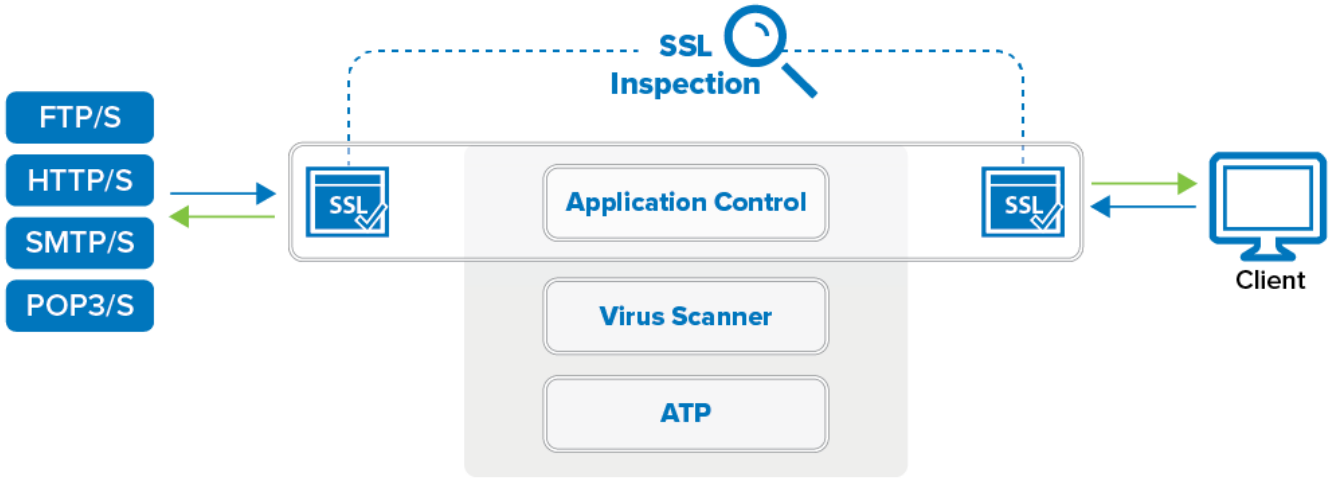
How to Configure ATP in the Firewall

https://campus.barracuda.com/doc/96026314/

Configure when and which types of files are uploaded to the Barracuda ATP Cloud. You can also configure if users will receive files immediately or have to wait until the file analysis is completed to continue with the download. Users who download files with a risk factor higher than the defined risk threshold are placed in quarantine. Create access rules to define what is blocked for the infected users and/or IP addresses. Malware and Advanced Threat Protection subscriptions are required. For more information, see How to License a CloudGen Firewall.



Before You Begin

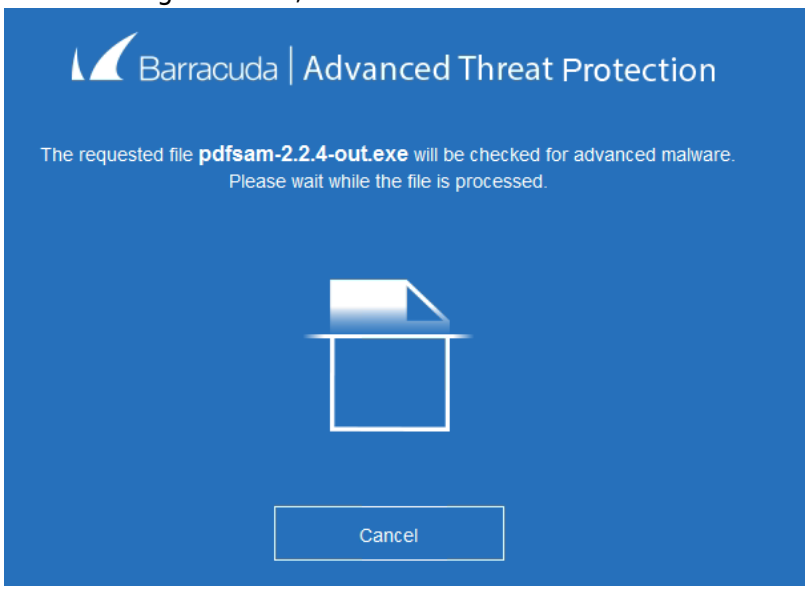
- Configure a **System Notification Email** address. For more information, see How to Configure System Email Notifications.
- Enable virus scanning in the firewall for web, mail, and/or FTP traffic. For more information, see How to Configure Virus Scanning in the Firewall for Web Traffic, How to Configure Mail Security in the Firewall, and How to Configure Virus Scanning in the Firewall for FTP Traffic.
- Verify that all file types you want to scan with ATP for are also listed in the scanned MIME types of the virus scanner. For more information, see How to Configure Virus Scanning in the Firewall for Web Traffic.
- (optional) Configure SSL Inspection. For more information, see SSL Inspection in the Firewall.

Step 1. Configure ATP Scan Policies and Risk Threshold

Configure the ATP scan policies for the desired type of connection. Depending on the policy, the user will have to wait for scanning to complete before the file is forwarded. FTP(S) traffic is always scanned

with the **deliver first, then scan** policy.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Virus-Scanner > Virus Scanner Settings**.
2. Click **Lock**.
3. In the left menu, click **ATP**.
4. In the **ATP HTTP and HTTPS Scan Policies** section, select the **Global Policy**:
   - **Deliver First, then Scan** – The user receives the file or email immediately. If malware is found, the quarantine policy applies.
   - **Scan First, then Deliver** – The user is redirected to a scanning page. If no malware is found during the scan, the download starts.



5. If needed, set the individual scan policies for each file type.
6. In the **ATP Email Scan Policies** section, select the **Global Policy** for email traffic.
   - **Deliver First, then Scan** – The user receives the email with the attachment immediately.
   - **Scan First, then Deliver** – The email attachment is scanned before it is forwarded to the user.
7. If needed, set the individual scan policies for each file type:
   - **Apply Global Policy (default)**
   - **Do Not Scan** – This file type is not scanned and immediately forwarded to the user.
   - **Deliver First, then Scan** – The user receives the file immediately. If malware is found, the quarantine policy applies.
   - **Scan First, then Deliver** – The user is redirected to a scanning page. After the scan is complete, the download starts.
8. In the **ATP Threats** section, select the **Block Threats** policy:
   - **High Only** – Files classified as high risk are blocked.
   - **High and Medium (Default)** – Files classified as high or medium risk are blocked.
   - **High, Medium and Low** – Files classified as high, medium or low risk are blocked. Only files with classification **None** are allowed.
9. Set **Send Notification Emails** to:

- **No** – No notification emails are sent when malware is found.
- **To System Notification Email (Default)** – A notification email is sent to the system notification email address. For more information, see How to Configure System Email Notifications.
- **To Explicit Address** – Enter the **Explicit Email Address** and **Explicit SMTP Server** the Barracuda CloudGen Firewall will use to send the notification emails.

10. (optional) Set the **ATP Data Retention** (in days). These values determine how long files are kept on the system before they are deleted.
11. Click **Send Changes** and **Activate**.

Step 2. Enable ATP in the Firewall and Configure Automatic Quarantine Policy

You must first enable ATP in the security policy of the Forwarding Firewall and enable the automatic block list policy for HTTP and HTTPS traffic.

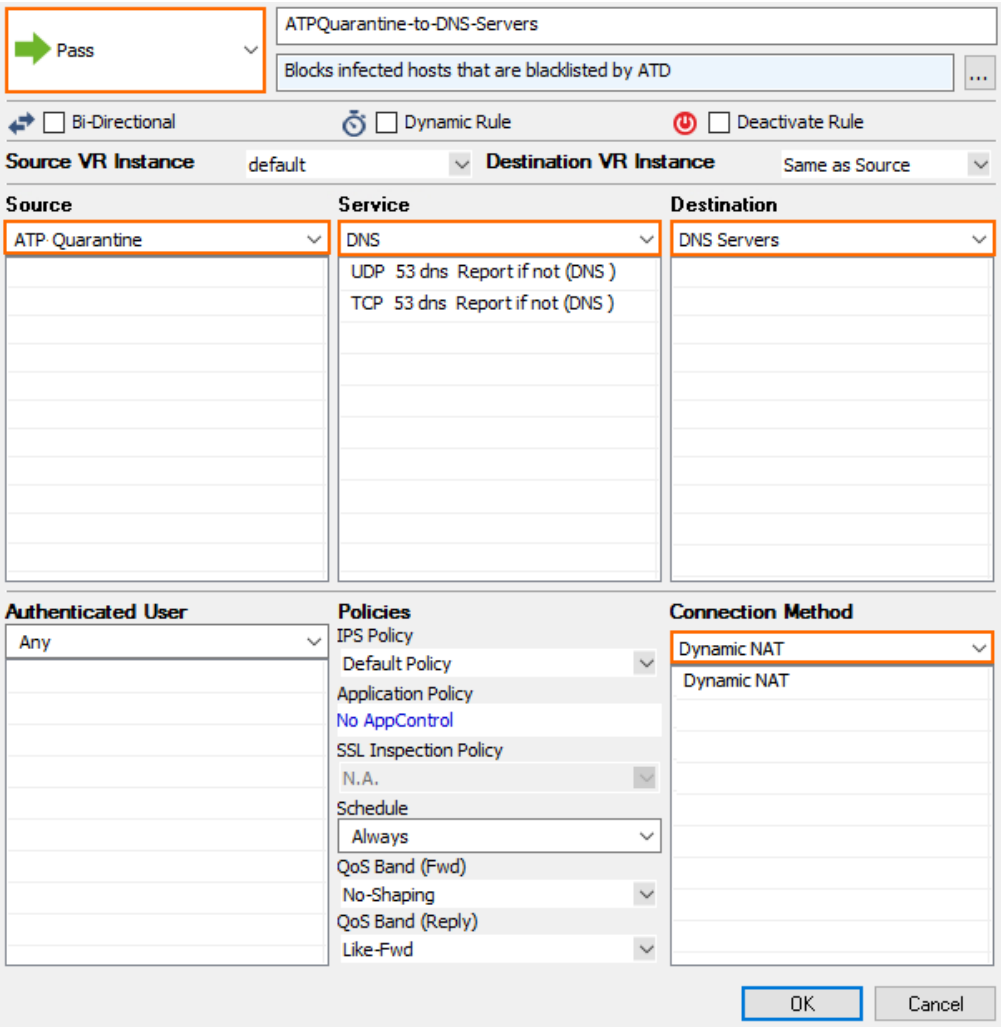
1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Security Policy**.
2. Click **Lock**.
3. In the **Advanced Threat Protection** section, click **Enable ATP in the firewall**.
4. Select the **Automatic Block List Policy**:
   - **No auto quarantining** – No connections are blocked.
   - **User only** – All connections by the infected user are blocked regardless of the source IP address.
   - **User@IP (AND)** – All connections originating from the infected source IP address and the infected user are blocked.
   - **User, IP (OR)** – All connections coming from the infected source IP address and/or the infected user are blocked.
5. Click **Send Changes** and **Activate**.

Step 3. Create two Quarantining Access Rules

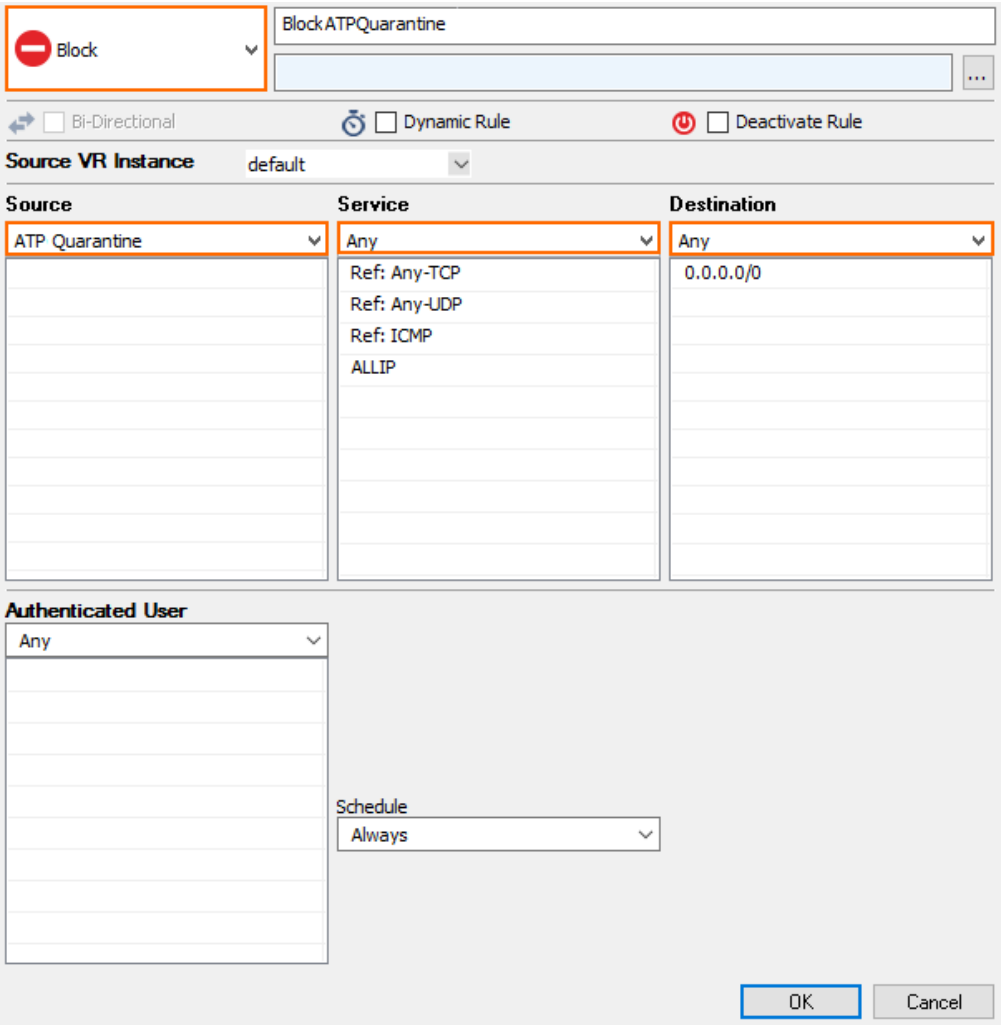
To block users and/or IP addresses, you must create access rules using the **ATP User Quarantine** network object. Place the Deny or Block rules before any other access rules handling traffic for these IP addresses and/or users. Enable **Transparent Redirect on Port 80** to redirect HTTP traffic from quarantined users or IP addresses to the custom quarantine block page. You must allow DNS queries from quarantined users to display the HTTP block page. Non-HTTP traffic is simply blocked or denied.

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Create a new access rule to allow DNS queries:

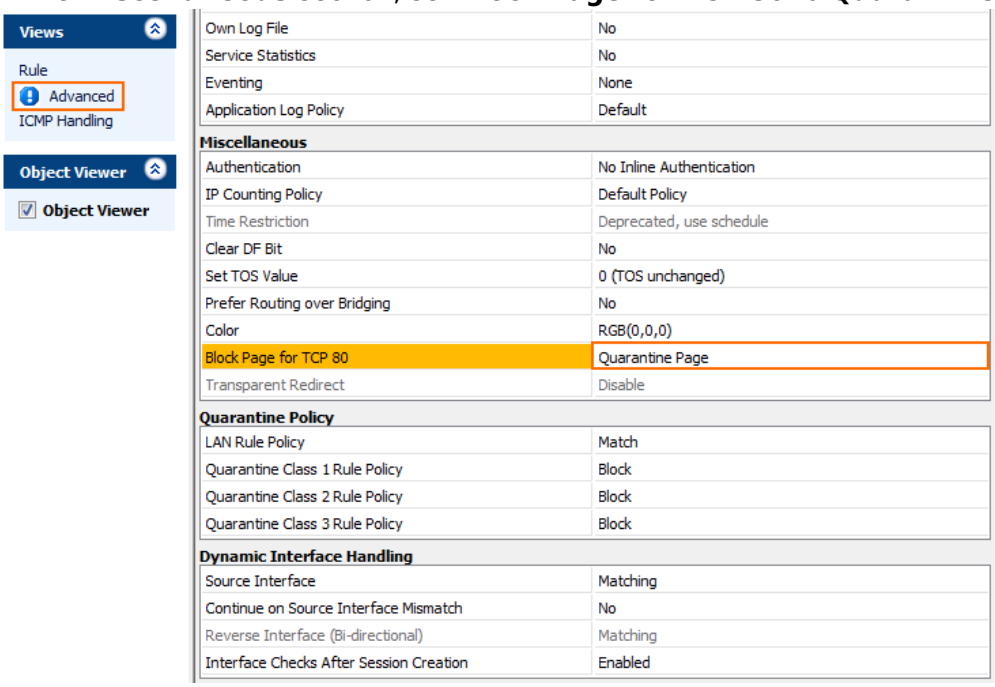
- **Action** – Select **Pass**.
- **Source** – Select **ATP Quarantine** network object.
- **Destination** – Enter the IP addresses of your DNS servers.
- **Service** – Select **DNS**.
- **Connection Method** – Select a connection object to allow you to connect to the DNS Server.



4. Click **OK**
5. Place the access rule so that no rule before it matches the same traffic.
6. Create a new access rule:
   - **Action** – Select **Deny** or **Block**.
   - **Source** – Select **ATP Quarantine** network object.
   - **Destination** – Select **Any (0.0.0.0/0)** network object.
   - **Service** – Select **Any**.

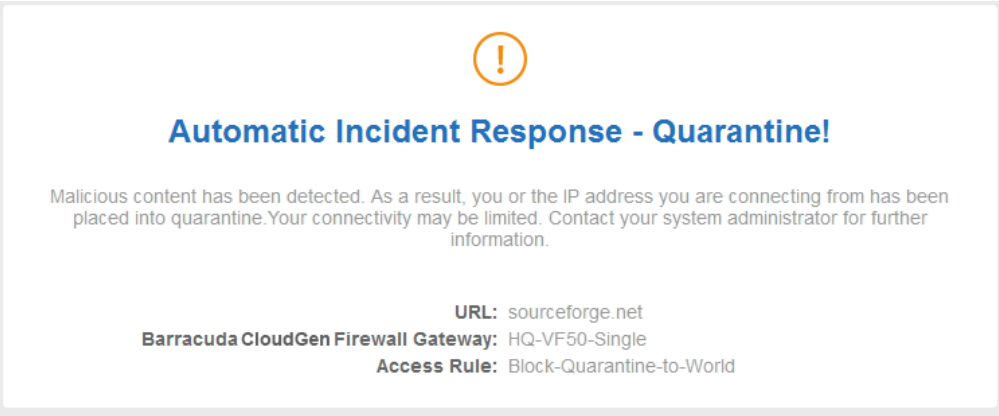


7. In the left menu, click **Advanced**.
8. In the **Miscellaneous** section, set **Block Page for TCP 80** to **Quarantine Page**.



9. Click **OK**.
10. Place the access rule directly below the rule allowing DNS queries from the quarantine so that no rule before it matches the same traffic.
11. Click **Send Changes** and **Activate**.

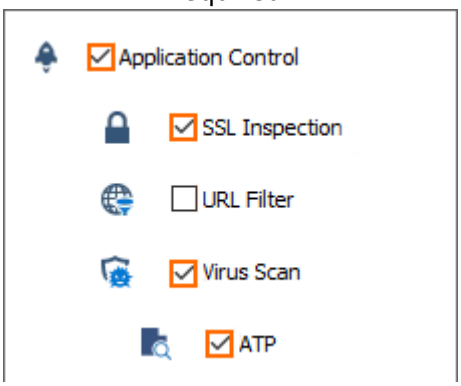
Quarantined users or users connecting via HTTP from quarantined IP addresses are automatically redirected to the customizable quarantine page. For more information, see [How to Configure Response Messages](#).



Step 4. Edit Access Rules to use ATP

Enable ATP by editing the access rules handling traffic you want to be scanned. E.g, LAN-2-INTERNET

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > Firewall > Forwarding Rules**.
2. Click **Lock**.
3. Edit the access rule handling the traffic you want analyzed by ATP.
4. Click the **Application Policy** link and select:
   - **Application Control** – required.
   - **SSL Inspection** – optional.
   - **Virus Scan** – required.
   - **ATP** – required.



5. If configured, select a policy from the **SSL Inspection Policy** drop-down list. For more

information, see SSL Inspection in the Firewall.
6. Click **Send Changes** and **Activate**.

All traffic handled by access rules with the **ATP** enabled are now scanned by the ATP service.

Quarantine Management

Manually Placing a User and/or IP Address in Quarantine

If you are not using automatic quarantine policy, the administrator can also place a user in quarantine manually.

1. Go to **FIREWALL > ATP**.
2. Click the **Scanned Files** tab.
3. Double-click the malicious file. The **ATP File Details** widow opens.
4. In the **File Download** section, select the user in the list.
5. Click **Quarantine**. The **Select Quarantine Policy** window opens.
6. Select the **Quarantine Policy**:
   - **Block only Users** – Place the user in quarantine, but not the source IP address.
   - **Block only IP Addresses** – Place the IP address in quarantine, but not the user.
   - **Block User @ IP (logic AND)** – Place user@IP address in quarantine. Both user and IP address have to match.
   - **Block User, IP (logic OR)** – Place the user and IP address in quarantine. Either user or IP address have to match.
7. Click **OK**.

The user and/or IP address are now in quarantine network object (Click the **Quarantine** tab to verify). Create an access rule using the ATP User Quarantine network object to block connection to and from the infected users and/or IP addresses.

Removing a User and/or IP Address from Quarantine

1. Go to **FIREWALL > ATP**.
2. Click the **Quarantine** tab.
3. Right-click the user or IP address you want to remove from quarantine.
4. Click **Remove from Quarantine**.

The user and/or IP address is removed from the quarantine network object.

Download a Scan Report

You can download a short or long version of scan report.

1. Go to **FIREWALL > ATP**.
2. Double-click the scanned file.
3. Click **Download Report** and select the report type:
    - **Summary Report**
    - **Full Report**

Figures