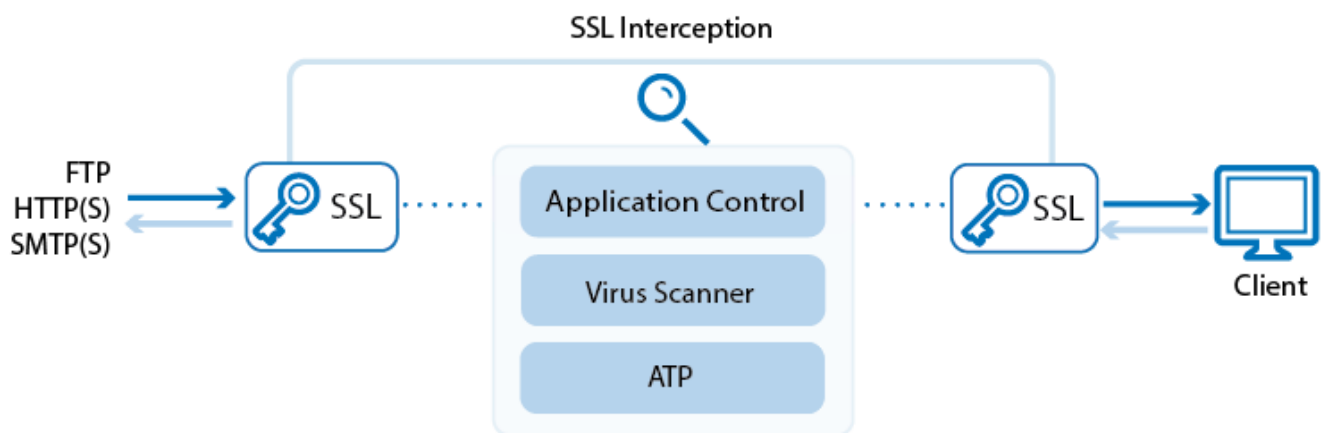


How to Configure ATP/ATD in the Firewall

<https://campus.barracuda.com/doc/49746347/>

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 downloaded 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.



Before you begin

- Configure a **System Notification Email** address. For more information, see [How to Configure Email Notifications](#).
- Enable virus scanning in the firewall for web, mail, and/or FTP traffic. For more information, see [How to Configure Virus Protection 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 HTTP and SMTP connections are also listed in the scanned MIME types of the virus scanner. For more information, see [How to Configure Virus Protection in the Firewall for Web Traffic](#).

Step 1. Enable ATD in the firewall and configure scan policies

Enable ATD and configure the ATD scan policies for HTTP, HTTPS, SMTP and SMTPS connections. Depending on the policy, the user will have to wait for scanning to complete before the file is forwarded. FTP traffic is always scanned with the **Deliver before scan complete** policy.

1. Go to the **FIREWALL > Settings** page.

2. In the **Advanced Threat Detection** section, enable **Advanced Threat Detection**.
3. Next to **Deliver before scan complete**, select the global scan policy:
 - **Yes** – The user receives the file or email immediately. If malware is found, the quarantine policy applies.
 - **No** – The user is redirected to a scanning page. If no malware is found during the scan, the download starts.
4. Select the **Block Threats** policy:
 - **High only** – Files classified as high risk are blocked.
 - **High and Medium only** – 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.
5. Configure automatic blacklisting for HTTP and HTTPS traffic:
 - From the **Quarantine Policy** drop down, select the policy for automatic blacklisting:
 - **No automatic blacklisting** – No connections are blocked.
 - **User** – All connections by the infected user are blocked regardless of the source IP address.
 - **IP** – All connections by the infected source IP address are blocked regardless of the user.
 - **User AND IP** – All connections originating from the infected source IP address and the infected user are blocked. If a different user logs in to the infected computer, all connections are allowed because only one criteria, the source IP address, matches. If the username for the connection is unknown, only the IP address is blocked.
 - **User OR IP** – All connections coming from the infected source IP address and/or the infected user are blocked. If a different user logs into the infected computer, all connections are blocked because the source IP is blocked. If the infected user logs in to a different workstation, connections are blocked because the infected user is blocked.
6. Click **Save**.

Step 2. Configure advanced scan settings

If needed, set the individual scan policies for each file type:

1. Go to the **FIREWALL > Settings** page.
2. In the **Advanced Threat Detection** section, select **Show** next to **Advanced Options**.
3. In the **General** section, configure the following settings:
 - **Encrypted Archives handling** – Specify what happens if encrypted archives were detected. Default: **Report only**
 - **Max. Archive size** – Maximum allowed archive size. Default: 1024. Set to 0 to disable.
 - **Large Archives handling** – Specify what happens if **Max. Archive size** is exceeded. Default: **Report only**
 - **Send Notification E-mails** – **To system settings Address** sends a notification mail for every malicious file found by ATP.

- **ATD Report Page size** – Select the page format for ATP reports.
4. If needed, set the individual HTTP and HTTPS scan policies for each file type:
 - **Apply Global Policy (default)** – This file type is scanned according to the policy configured in the basic ATD settings.
 - **Do not scan** – The file 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.
 5. Click **Save**.

After specifying the ATD settings, click **Save** to save your configuration changes.

Step 3. Create two quarantining access rules

To block users and/or IP addresses, you must create access rules using the **ATD User Quarantine** network object. Place the Block rules before any other access rules handling traffic for these IP addresses and/or users. Enable **HTTP Block Page** 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.

Create a new access rule to allow DNS queries:

1. Go to **FIREWALL > Firewall Rules**.
2. Click **Add Access Rule** to create a new access rule.
3. In the **Add Access Rule** window, enter a name and description for the rule.
4. Specify the following settings:

Action	Connection	Service	Source	Destination
Allow	Select a connection object to allow you to connect to the DNS server.	DNS	Select ATD Quarantine network object.	Enter the IP addresses of your DNS servers.

General Advanced

Action:

Allow

Name:

ATDQuarantine-to-DNS

Bi-directional:

☐ Yes ☒ No

Description:

Connection:

Dynamic SNAT

Adjust Bandwidth:

Internet

The interface must have bandwidth management enabled on the **NETWORK > IP Configuration** page for this policy to be applied.

Disable:

☐ Yes ☒ No

IPS:

☒ Yes ☐ No

Application Control:

☐ Yes ☒ No

SSL Inspection:

☐ Yes ☒ No

URL Filter:

☐ Yes ☒ No

Virus Protection:

☐ Yes ☒ No

ATD:

☐ Yes ☒ No

Mail Blacklist Checks:

☐ Yes ☒ No

Safe Search:

☐ Yes ☒ No

Source

3G Local IP

+

Ref: ATD Quarantine

-

Network Services

Any-VPN

+

DNS

-

Destination

ATD Quarantine

+

Ref: DNS Servers

-

☒ Network Objects ☐ IP Address ☐ Geo Loc.

☒ Network Objects ☐ IP Address ☐ Geo Loc.

5. Click **Save**.

6. Place the access rule so that no rule before it matches the same traffic.

Create a second access rule:

- Go to **FIREWALL > Firewall Rules**.
- Click **Add Access Rule** to create a new access rule.
- In the **Add Access Rule** window, enter a name and description for the rule.
- Specify the following settings:

Action	Connection	Service	Source	Destination
Block	Select a connection object to allow you to connect to the DNS server.	Select Any .	Select ATD Quarantine network object.	Select Any (0.0.0.0/0) network object.

General **Advanced**

Action: Block

Name: Block-ATDQuarantine

Bi-directional: ☐ Yes ☒ No

Disable: ☐ Yes ☒ No

Description:

Connection: Dynamic SNAT

Adjust Bandwidth: Internet

*The interface must have bandwidth management enabled on the **NETWORK > IP Configuration** page for this policy to be applied.*

Source

3G Local IP +

Ref: ATD Quarantine -

☒ Network Objects ☐ IP Address ☐ Geo Loc.

Network Services

Any-EMAIL +

Any -

Destination

Internet +

Ref: Any -

☒ Network Objects ☐ IP Address ☐ Geo Loc.

DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.
Bi-directional - Source and destination networks are interchangeable.

- In the **Add Access Rule** window, click the **Advanced** tab.
- In the **Other** section, set **HTTP Block Page** to **Quarantine Page**.

General **Advanced**

Valid For Users

All Authenticated Users +

If no users are added to this rule, then any user information in the traffic will be ignored.

Apply only during this time

None ▼

Select or create new time objects to define a time frame this rule shall be applied. One time object may be selected.

Denial of Service and Spoofing Protection

Interface Group: Matching ▼

*Select the interface(s) the rule applies to or select **Any** to match all interfaces. **Matching** automatically determines the interface.*

SYN Flood Protection: ☒ Automatic ☐ Always On

Automatically detects SYN flood attacks and switches to a different TCP handshake mode to protect the network. Default: Automatic

Other

HTTP Block Page: Quarantine Page ▼

Show the access block page if a HTTP request gets blocked by the firewall rule. If set to 'None; SYN Block' the SYN request will be silently blocked and the browser will time out. Default: 'None; SYN Block'

- Click **Save**.
- Place the access rule directly below the rule allowing DNS queries from the quarantine so that no rule before it matches the same traffic.

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



Automatic Incident Response - Quarantine!

Malicious content has been detected. As a result, you or the IP address you are connecting from has been placed into quarantine. Your connectivity may be limited. Contact your system administrator for further information.

URL: sourceforge.net
Barracuda NG Firewall Gateway: HQ-VF50-Single
Access Rule: Block-Quarantine-to-World

Step 4. Edit access rules to use ATP

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

1. Go to **FIREWALL > Firewall Rules**.
2. Create or edit an access rule.
3. Edit the access rule handling the traffic you want analyzed by ATP.
4. On the **General** page, select the following options:
 - **Application Control** - required.
 - **SSL Inspection** - optional.
 - **Virus Protection** - required.
 - **ATD** - required.

Edit Access Rule

General	Advanced
Action: <div>Allow</div>	
Name: <div>LAN-2-INTERNET</div>	
Description: <div>Allows internet access from Trusted LAN for typical applications.</div>	
Connection: <div>Dynamic SNAT</div>	
Adjust Bandwidth: <div>Internet</div>	
Bi-directional: <input type="radio"/> Yes <input checked="" type="radio"/> No	
Disable: <input type="radio"/> Yes <input checked="" type="radio"/> No	
IPS: <input checked="" type="radio"/> Yes <input type="radio"/> No	
Application Control: <input checked="" type="radio"/> Yes <input type="radio"/> No	
SSL Inspection: <input checked="" type="radio"/> Yes <input type="radio"/> No	
URL Filter: <input checked="" type="radio"/> Yes <input type="radio"/> No	
Virus Protection: <input checked="" type="radio"/> Yes <input type="radio"/> No	
ATD: <input checked="" type="radio"/> Yes <input type="radio"/> No	
Mail Blacklist Checks: <input checked="" type="radio"/> Yes <input type="radio"/> No	
Safe Search: <input checked="" type="radio"/> Yes <input type="radio"/> No	

DNAT (port forwarding) - Redirect traffic to a specific IP address.
Redirect to Service - Redirect traffic to a service on the Barracuda Firewall.
Bi-directional - Source and destination networks are interchangeable.

*The interface must have bandwidth management enabled on the **NETWORK > IP Configuration** page for this policy to be applied.*

5. Click **Save**.

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

files are listed on the **BASIC > Recent Threats** page. To view scan results, go to **BASIC > ATD**.

File scanning on the ATD page

The **ATD** page displays results and processes file scanning via Advanced Threat Protection. Use the global filter settings to adjust the amount of displayed files. To access the information about the files scanned by ATP, click the tabs.

Files in Progress tab

This tab displays all files that are currently scanned or waiting in the queue. The information displayed on this page is listed in columns. The **State** column shows the ATP scan status.

ADVANCED THREAT DETECTION

Help

Files in Progress

Scanned Files

Malicious Files

Quarantine

0 Files and 0 Compressed HTTP Files queued, 1 File(s) scanning

Files scanned this month: 5 of 1000000

Manual Upload

State	Hash	File	Start Time	Scan Policy	File Type	URL	Orig
Scanning	5dc7783a5fd9a80ce65ba7a81d6a706dec53caab	VDA_1-0.zip	2016-06-16 02:21:57	Deliver first, then scan	zip	http://tenet.dl.sourceforge.net/project/Migdicattack/VS2010/Project/VDA_1-0.zip	http://
Queued	5dc7783a5fd9a80ce65ba7a81d6a706dec53caab	VDA_1-0.zip	2016-06-16 02:22:02	Deliver first, then scan	zip	http://tenet.dl.sourceforge.net/project/Migdicattack/VS2010/Project/VDA_1-0.zip	http://

<

Showing 1 to 2 of 2 entries

>

Scanned Files tab

Clicking this tab queries the ATP list and displays all files that were scanned by ATP.

ADVANCED THREAT DETECTION

Files in Progress

Scanned Files













Malicious Files

Quarantine

0 Files and 0 Compressed HTTP Files queued, 0 File(s) scanning
Files scanned this month: 11 of 1000000

Remove all entries on this page

Manual Upload

Action	Risk	Scan Policy	Start Time	File	File Type	Origin	Information	Delivered	Blocked	Hash
 	None	Deliver first, then scan	2016-06-16 02:32:10	rPE.exe	.exe	http://https	http://jaist.dl.sourceforge.net/project/repox/Version_0.7.4.04/rPE.exe	Yes	0	f9f990c2cda2a175da1a9a
 	None	Deliver first, then scan	2016-06-16 02:31:49	showtraf-1.7.0-setup.exe	.exe	http://https	http://heanet.dl.sourceforge.net/project/showtraf/showtraf1.7.0/showtraf-1.7.0-setup.exe	Yes	0	63040aa109b1451b2aa9d
 	None	Deliver first, then scan	2016-06-16 02:28:22	nsis-2.51-setup.exe	.exe	http://https	http://heanet.dl.sourceforge.net/project/nsis/NSIS-2.51/nsis-2.51-setup.exe	Yes	0	2d321c3ba700eee4e2ca2
 	None	Deliver first, then scan	2016-06-16 02:23:53	VDA_1-0.zip	zip	http://https	http://tenet.dl.sourceforge.net/project/vigdicattack/VS2010/Project/VDA_1-0.zip	Yes	0	5dc7783a5fd9a80ce65ba7
 	None	Deliver first, then scan	2016-06-16 02:17:52	willpassworddecryptor.zip	zip	http://https	http://gsf-ct.softonic.com/215ebba43d8602ac205c8bf1dc761ba546c2a238/willpassworddecryptor.zip	Yes	0	215ebba43d8602ac205c8
 	None	Deliver first, then scan	2016-06-16 02:12:50	processhacker-2.39-setup.exe	.exe	http://https	http://jaist.dl.sourceforge.net/project/processhacker/processhacker2/processhacker-2.39-setup.exe	Yes	0	162b08b0b11827cc024e6b
	None	Deliver first, then scan	2016-06-16 02:06:56	beecrypt-1.1.2-ppro.zip	zip	http://https	http://master.dl.sourceforge.net/project/beecrypt/OldFiles/beecrypt-1.1.2-ppro.zip	Yes	0	4b926d0ec7f8e85e63d2ca
	None	Deliver first, then scan	2016-06-16 01:54:00	real.exe	.exe	http://https	http://214.51.2.80/real.exe	Yes	0	9d8cb02122d3a0d6b23b6
	Medium	Deliver first, then scan	2016-06-16 02:10:31	LOIC-1.0.8-binary.zip	zip	http://https	http://tenet.dl.sourceforge.net/project/loic/loic-1.0.8/LOIC-1.0.8-binary.zip	Yes	4	f0068b03f7b6c785284bd
	Low	Deliver first, then scan	2016-06-16 02:36:47	usbdrvinstall.exe	.exe	http://https	http://tenet.dl.sourceforge.net/project/usbdrv/usbdrvinstall.exe	Yes	0	be6609e941420e012a4e9

The **Action** column provides a set of icons, offering the following options:







- **Details** – Opens the **ATD File Details** window.
- **Download** – Offers the option to download a scan report.

- **Move to Quarantine** – Moves the file to the **Quarantine** page.
- **Delete Entry** – Deletes the file entry.

Download a scan report

Scanned files are displayed on the **Scanned Files** page. You can download a basic or detailed version of the scan report.

1. Go to **BASIC > ATD**.
2. Select the scanned file.
3. From the **Action** menu, select the **Download Report** icon.
4. Select the report type:
 - **Summary Report** – Download a basic summary report
 - **Full Report** – Download a detailed report

Action	Risk	Scan Policy	Start Time	File	File Type
	None	Deliver first, then scan	2016-06-16 02:23:53	VDA_1-0.zip	.zip
					
					
					
					
	None	Deliver first, then scan	2016-06-16 01:54:00	real.exe	.exe

5. Save the report to your desired location.

Malicious Files tab

This tab displays all files that were blocked by ATP.

ADVANCED THREAT DETECTION

Help

Files in Progress

Scanned Files

Malicious Files

Quarantine

0 Files and 0 Compressed HTTP Files queued, 0 File(s) scanning

Files scanned this month: 11 of 1000000

Remove all entries on this page

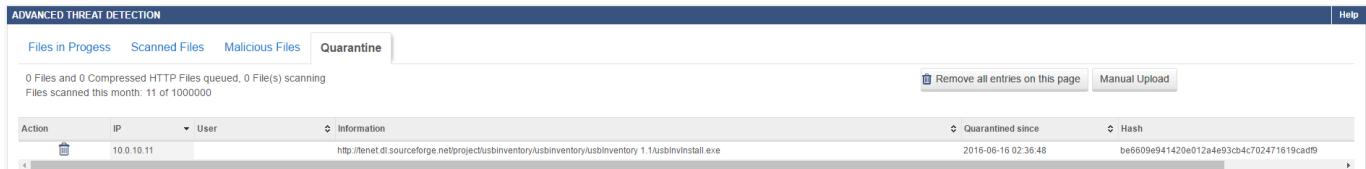
Manual Upload

Action	Risk	Scan Policy	Start Time	File	File Type	Origin	Information	Delivered	Blocked	Hash
<div><div><div></div><div></div><div></div></div></div>	Medium	Deliver first, then scan	2016-06-16 02:10:31	LOIC-1.0.8-binary.zip	.zip	http/https	http://net.dl.sourceforge.net/project/loic/loic-1.0.8/LOIC-1.0.8-binary.zip	Yes	4	80088b0377b9c785284ab95a
<div><div><div></div><div></div><div></div></div></div>	Low	Deliver first, then scan	2016-06-16 02:36:47	usbinstall.exe	.exe	http/https	http://net.dl.sourceforge.net/project/usbinventory/usbinventory/1.1/usbinstall.exe	Yes	0	be6609e941420e0124e93cb4

The **Action** column provides the same options as on the **Scanned Files** tab. If you want to remove a file from the list, click the trash can icon and choose the action **Delete Entry** to delete the file entry. To remove all files, select **Remove all entries on this page**.

Quarantine tab

Displays all files that are quarantined due to the **Quarantine Policy**.



Action	IP	User	Information	Quarantined since	Hash
	10.0.10.11		http://tenet.dl.sourceforge.net/project/usbinventory/usbinventory/1.1/usbinstall.exe	2016-06-16 02:36:48	be6609e941429e012a4e93cb4c702471619cadf9

If you want to remove a file from the quarantine, click the trash can icon and choose the action **Remove from Quarantine**. To remove all files from the list, select **Remove all entries on this page**.

Quarantined users and/or IP addresses are also shown on the **BASIC > Status** page.

QUARANTINE			All		Help
User	IP	Since			
	10.0.10.11	2016-06-16 02:36:48			

Manual File upload

If you want to manually check a local file using ATP, you can upload the file to the ATP Cloud. After the file has been scanned, you are mailed a report with the scan results.

For more information, see [How to Manually Upload Files to ATP/ATD](#).

Next step

(Optional) To protect SMTP and SMTPS traffic, enable ATD in the Mail Security settings. For more information, see [Mail Security in the Firewall](#).

Figures

1. virus_scanning_https_traffic_ATP-01.png
2. atd_quarantine_01.png
3. atd_quarantine_02.png
4. atd_quarantine_03.png
5. atd_quarantine_block_page.png
6. atd_rule.png
7. atd_fp.png
8. atd_sf.png
9. atd_report.png
10. atd_mf.png
11. atd_qu.png
12. atd_qustat.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.