How to Enable Application Control 2.0, SSL Interception, URL Filtering, Virus Scanning and ATP

https://campus.barracuda.com/doc/41115750/

Before creating application rules, you must enable Application Control 2.0. You can also enable and configure the SSL Interception feature, Virus Scanning or ATP in the Firewall. Application Control 2.0 SSL Interception and Virus Scanning is only supported for IPv4 traffic.

Virus Scanning or SSL Interception can not be used on layer 2 bridging interfaces which is not assigned an IP address. Use routed layer 2 or layer 3 bridging interfaces instead.

In this article:

Supported NG Firewall Models

Feature	Supported NG Firewall Model
Application Control 2.0	Available on all Barracuda NG Firewall models with valid Energize Update subscription. On hardware models without valid Energize Update subscription or with a legacy phion license, Application Control 2.0 is limited to detecting applications only.
SSL Interception	Available on all Barracuda NG Firewall models with valid Energize Update subscription, except F10 and F100/F101.
URL Filtering	Available on all Barracuda NG Firewall models with valid Energize Update subscription, except F10.
Virus Scanning	Available on all Barracuda NG Firewall models with valid Energize Update and Malware subscription, except F10.
Advanced Threat Protection	Available on all Barracuda NG Firewall models with valid Energize Update, Malware and Advanced Threat Protection subscription, except F10 and F100/F101.

Enable Application Control 2.0

1. Open the **Forwarding Rules** page (**Configuration** > **Configuration Tree** > **Box > Virtual Server > *your virtual server*** > **Firewall**).
2. In the left menu, expand **Settings** and click **Setup**.
3. Verify that the correct **Feature Level** is selected:

- ***Release 6.0.0*** – Select for Application Control 2.0, SSL Interception, AV scanning and ATP
- **Release 5.4.3** – Select for Application Control 2.0, SSL Interception and AV scanning.
- **Release 5.4.2** – Select for Application Control 2.0, SSL Interception, and URL Filter.
- **Release 5.4.0** – Select for Application Control 2.0 and SSL Interception.

4. To enable the use of application rules, select *Use Application Ruleset* from the **Application Ruleset** list.
5. Click **OK**.
6. Click **Send Changes** and **Activate**.

Enable SSL Interception

1. Open the **Security Policy** page (**Config** > **Full Config** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **Firewall**).
2. Click **Lock**.
3. Select the **Enable SSL Interception** check box.
4. In the **Root Certificate** section, either select **Use self signed certificate** or add your certificate by clicking the plus sign (**+**). The root certificate is used to intercept, proxy, and inspect the HTTP/S session. The Barracuda NG Firewall can then intercept the HTTP/S connections by presenting the client with a CA that was derived from this root CA.
   When changing the root certificate, the firewall service must be restarted on the Server Page.
5. In the **Trusted Root Certificates** table, you can extend the default set of trusted root certificates by clicking the plus sign (**+**). To view the Barracuda NG Firewall's certificate store, click the **Show CA Certificates** link.
6. Select the **Enable CRL Checks** check box to automatically check for revoked CA certificates.
7. In the **Exception Handling** section, add domains that should be excluded from SSL Interception. SSL-encrypted traffic to and from these domains is not decrypted, although SSL Interception is globally enabled.
8. In the **Block Settings** section, enter a browser message that should be displayed when traffic is blocked.
9. Click **Send Changes** and **Activate**.

To ensure that SSL interception is activated, you must enable Application Control and SSL Interception in the settings of the forwarding firewall rules that it should apply to. For more information, see How to Create an Application Rule.

Enable the URL Filter

1. Open the **General Firewall Configuration** page (**Config** > **Full Config** > **Box** > **Infrastructure Services** > **General Firewall Configuration**).

2. Click **Lock**.
3. From the **Configuration** menu in the left pane, click **Application Detection**.
4. Set the **Working Mode** to *On*.
5. Click **Send Changes** and **Activate**.
6. Verify that the URL Filter service is properly configured and running. For more information on how to create and configure the URL Filter service, see URL Filter.
7. To verify if Application Control 2.0 is using the URL Filter service, review the following log file for according entries: **Box** > **Firewall** > *appid_urlcat*.

Configure Advanced SSL Interception Settings

For SSL Interception, you can also configure advanced settings such as the number of working instances that are involved in the SSL decryption process, log verbosity, or CRL checks.

1. To configure the advanced settings:
2. Click the **Advanced** link in the upper right of the **Security Policy** page.
3. In the **SSL Interception Advanced** window, you can specify the following settings:

Setting	Description
Number of Workers	The number of working instances to be involved in the SSL decryption and encryption process. Default: auto
Maximum Workers	The maximum number of working instances that decrypt and encrypt SSL connections. When all workers are used SSL connections are refused. Default: auto
Worker Idle Timeout	The timeout for the working instances involved in the SSL decryption and encryption process. Default: `0`
Log Verbosity	You can select one of the following log granularity options. ◦ **Normal** ◦ **Verbose** ◦ **Debug**
Ignore Validation Status	Since the clients cannot check the revocation status for server certificates of intercepted SSL connections, you can configure the default validation policy for all intercepted SSL connections for which CRL/OCSP checks could not be performed: ◦ **Yes** – The NG Firewall creates a valid certificate for the client as long as the content of the sever certificate validates. ◦ **No** – The NG Firewall creates an invalid certificate, to let the client know that CRL/OCSP checks could not be performed. **Default**: Yes

4. Click **OK**.
5. Click **Send Changes** and **Activate**.

Certificate Management

SSL Interception process breaks the certificate trust chain. To reestablish the trust chain it might be necessary to install the security certificate (root certificate) that is used by the SSL Interception engine. Install this certificate on computers in your network. If Application Control 2.0 and SSL Interception are enabled, and computers within your network are accessing SSL encrypted resources, users typically get a browser warning that the resource identity could not be verified. Access can even be blocked.

To prevent browser warnings and allow transparent SSL interception, install the security certificate either into the operating system's certificate store or directly in the web browser.

1. On the **Security Policy** page, click the pencil icon next to **(Self Signed) Certificate** and click **Export to file**.
2. Enter a name, select ***.cer** as file type, and click **Save**.
3. Deploy this certificate to the computers in your network. Either create a group policy object or install the certificate manually (MS Certificate Import wizard). Ensure that you deploy the certificate into MS Windows' **Trusted Root Certification Authorities** certificate store.

Mozilla Firefox does not automatically use trusted CA certificates installed in MS Windows' certificate store.

Certificate Management with Intermediate Certificate Authorities

Intermediate CAs are not directly delivered from the Barracuda NG Firewall to the client and must be deployed manually from the Microsoft Active Directory PKI.

1. Use Microsoft Internet Explorer and connect to your MS Active Directory Certificate Services server. For example, https://127.0.0.1/certsrv
2. Click **Request a Certificate** and select **advanced certificate request**.
3. Click **Create and submit a request to this CA** and answer all questions with *Yes*.
4. Select **Subordinate Certification Authority** from the Certificate Template.
5. Fill out the form below.
6. Select your key size in the **Key Options** section and select the **Mark keys as exportable** check box.
7. Click **Submit** and answer all questions with *Yes*.
8. Click **Install this certificate**.

After the certificate is installed successfully, start the MS Active Directory's management console.

1. Open the **Certificates - Current User** snap-in.
2. Right-click the **Intermediate Certification Authorities\Certificates** section and select your certificate.
3. Select **All Tasks > Export** in the upcoming window.
4. Click **Next** to proceed.
5. In the **Export Private Key** window, select *Yes, export the private key* and proceed.
6. Enter a password and click **Next**.
7. Select the export destination folder and enter a file name.
8. Click **Finish**.
9. After the certificate has been exported, rename the file extension from **.pfx* to **.p12* .
10. Use openssl to extract the private key from your *.p12 file. Enter the following command:
`openssl.exe pkcs12 -in <filename>.p12 -nocerts -nodes -out privateKey.pem`
11. Enter the password entered in step 6.
12. Use openssl to convert the key file to RSA. Enter the following command:
`openssl.exe rsa -in privateKey.pem -out yourPrivateKey.pem`
13. You can now import the certificate (**.p12*) and private key (**.pem*) pair to be used for SSL Interception.
14. Install the certificate (**.p12*) and Root CA from which the certificate was derived, on the certificate store of affected clients.