How to Configure SSL Interception in the Firewall

https://campus.barracuda.com/doc/45026001/Most applications encrypt outgoing connections with SSL or TLS. SSL Interception decrypts SSL-encrypted traffic to allow Application Control features (such as the Virus Scanner, ATD, URL Filter, Safe Search, or File Content Scan) to inspect encrypted content that would otherwise not be visible to the Firewall service. To avoid certificate errors when the users use SSL-encrypted connections, you must install the SSL Interception root certificate on all client computers. If you are using CRL checks, the CRL/OCSP check is done once per 24h period to reduce the load on the CRL/OCSP server. If an error occurs during the CRL check, it is repeated after 10 minutes.
Applications with the application object property **not interceptable** cannot be intercepted and are automatically excluded from SSL Interception. Open the application object on the **Forwarding Rules > Applications** page to check if an application is interceptable. You can configure SSL Interception to use a cipher string of your choice.

Enable SSL Interception

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **Firewall** > **Security Policy**.
2. Click **Lock**.
3. Select the **Enable SSL Interception** checkbox.
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.
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** checkbox 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. Domains automatically include all subdomains.
   E.g., **google.com** will also includes **mail.google.com**
8. In the **Block Settings** section, enter a browser message that should be displayed when traffic is blocked.
9. Click **Send Changes** and **Activate**.

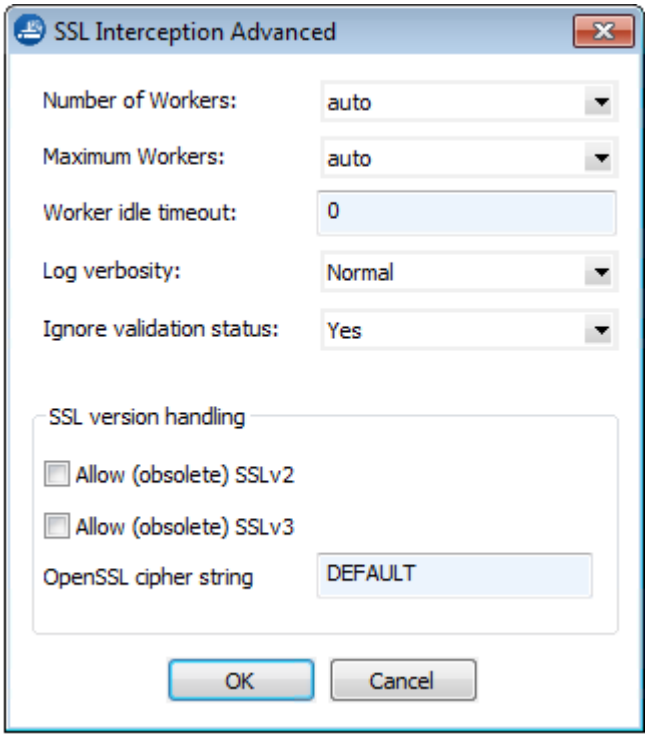
SSL Interception can now be enabled on a per-access or application rule basis.

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, CRL checks, or the used cipher string.

1. Go to **CONFIGURATION** > **Configuration Tree** > **Box** > **Virtual Servers** > ***your virtual server*** > **Assigned Services** > **Firewall** > **Security Policies**.
2. Click the **Advanced** link in the upper right of the **Security Policy** page. The **SSL Interception Advanced** window opens.

3. Change the advanced SSL Interception settings according to your requirements:
   - **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,** or **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. Default: Yes
     - **Yes** – The NG Firewall creates a valid certificate for the client as long as the content of the server certificate is validated.
     - **No** – The NG Firewall creates an invalid certificate to let the client know that CRL/OCSP checks could not be performed.
   - **SSL version handling**
     - **Allow (obsolete) SSLv2** – Enable if you must support clients that are SSLv3 only.
     - **Allow (obsolete) SSLv3** – Enable if you must support clients that are SSLv3 only.
     - **OpenSSL cipher string** – You can set a custom cipher string.The Barracuda NG Firewall uses the **DEFAULT** cipher string of the OpenSSL version used in the firmware by default.



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

Certificate Management

SSL Interception process breaks the certificate trust chain. To reestablish the trust chain, you must install the security certificate (root certificate) and, if applicable, intermediate certificates that are used by the SSL Interception engine. Install this certificate on every client in your network. To prevent browser warnings and allow transparent SSL interception, install the security certificate into the operating system's or web browser's certificate store.

1. On the **Security Policy** page, click the edit 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 the MS Windows certificate store.

Certificate Management with Intermediate Certificate Authorities

Intermediate CAs are not directly delivered from the Barracuda NG Firewall to the client. They 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** checkbox.
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.

SSL Interception for VPN Traffic

To use SSL Interception for traffic going through a VPN tunnel, you must create a VPN interface and

assign an IP address that is covered by the source route of the VPN tunnel.

SSL Interception on Bridged Interfaces

SSL Interception can only be used on routed Layer 2 and Layer 3 bridges. Additionally, a default route is needed to carry out CRL checks.

For more information, see Bridging.

Figures

1. ssl_int01.png
2. ssl_int02.png