How to Configure SSL Interception in the Firewall

https://campus.barracuda.com/doc/48202687/

Most applications encrypt outgoing connections with SSL or TLS. SSL Interception decrypts SSL-encrypted HTTPS and SMTPS traffic to allow Application Control features (such as the Virus Scanner, ATP, 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. Clients using HTTP2, SPDY, or QUIC are not intercepted. To SSL intercept traffic from these browsers, block UDP 443 on your firewall or disable the protocol directly in the browser to allow the browsers to fall back to HTTPS. 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. The F-Series uses the following default cipher string: **HIGH:!aECDH:!ADH:!3DES:!MD5:!DSS:!RC4:!EXP:!eNULL:!NULL:!aNULL**. If necessary, you can also set a custom cipher string using the ciphers from the following list:

AES128-GCM-SHA256
AES128-SHA
AES128-SHA256
AES256-GCM-SHA384
AES256-SHA
AES256-SHA256
CAMELLIA128-SHA
CAMELLIA256-SHA
DHE-RSA-AES128-GCM-SHA256
DHE-RSA-AES128-SHA
DHE-RSA-AES128-SHA256
DHE-RSA-AES256-GCM-SHA384
DHE-RSA-AES256-SHA
DHE-RSA-AES256-SHA256
DHE-RSA-CAMELLIA128-SHA
DHE-RSA-CAMELLIA256-SHA
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA
ECDHE-ECDSA-AES128-SHA256
ECDHE-ECDSA-AES256-GCM-SHA384

ECDHE-ECDSA-AES256-SHA
ECDHE-ECDSA-AES256-SHA384
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES256-SHA
ECDHE-RSA-AES256-SHA384
PSK-AES128-CBC-SHA
PSK-AES256-CBC-SHA
SRP-AES-128-CBC-SHA
SRP-AES-256-CBC-SHA
SRP-RSA-AES-128-CBC-SHA
SRP-RSA-AES-256-CBC-SHA

Before You Begin

Enable Application Control. For more information, see How to Enable Application Control.

Step 1. 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** 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 SSL-encrypted connections. For HTTPS, the Barracuda NextGen Firewall F-Series uses the root certificate to present the client with an SSL certificate derived from this root CA.
   When changing the root certificate, go to **CONTROL > Server** and restart the Firewall service.
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 F-Series Firewall's certificate store, click the **Show CA Certificates** link.
6. Select the **Enable CRL Checks** check box to automatically check for revoked 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 include **mail.google.com**

8. Click **Send Changes** and **Activate**.

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

Step 2. 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
   - **Protocol Error Policy** – If the firewall cannot interpret the HTTP or SMTP connection this policy is enforced:
     - **continue** – The invalid HTTP or SMTP traffic is forwarded directly bypassing all further firewall policies such as virus scanner, URL Filter, etc...
     - **close** – The invalid HTTP or SMTP connection is closed.
   - **RSA Key Size** – Select the key size used for the dynamic SSL certificates.
   - **Log Verbosity** – You can select one of the following log granularity options: **debug, info, notice, warning,** or **error**.
   - **CRL Error Policy** – 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
     - **Ignore** – The F-Series creates a valid certificate for the client as long as the content of the server certificate is validated.
     - **Fail** – The F-Series 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, or remote mail servers, that are SSLv2 only.
     - **Allow (obsolete) SSLv3** – Enable if you must support clients, or remote mail

servers, that are SSLv3 only.
- **OpenSSL Cipher String** – You can set a custom cipher string. The F-Series uses the following default cipher string: **HIGH:!aECDH:!ADH:!3DES:!MD5:!DSS:!RC4:!EXP:!eNULL:!NULL:!aNULL**.

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

Certificate Management

The 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 the MS Windows **Trusted Root Certification Authorities** certificate store.

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

SSL Interception for SMTPS Traffic

The F-Series supports SSL Interception for incoming and outgoing SSL encrypted SMTP connections using the SSL certificate of your mail server.
For more information, see How to Configure Mail Security in the Firewall.

SSL Interception for HTTPS Traffic

The F-Series supports SSL Interception for incoming and outgoing SSL-encrypted HTTP connections.
For more information, see How to Configure Virus Scanning in the Firewall for Web Traffic.

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