SSL Certificate – SonicWALL

Installation Guide

webnic
accelerate your business

Please select your version

Installation Instructions for SonicWALL Offloaders

Installation Instructions for SonicWall SSL VPN Appliance

Installation Instructions for SonicWALL Offloaders

Step 1. Download the Intermediate CA Certificate

1. Download the Intermediate CA certificate.
   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
2. Copy the Intermediate CA certificate and paste it on a Notepad.
3. Save the file as **CertChain.pem**

Step 2. Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad
   The text file should look like:
   -----BEGIN CERTIFICATE-----

   [encoded data]

   -----END CERTIFICATE-----

3. Save the file with extansion **YourDomain.pem**

Step 3. Set up the chained Certificate

1. Now that you have the proper certificates, load the certificates into certificate objects.
2. These separate certificate objects are then loaded into a certificate group. This example demonstrates how to load two certificates into individual certificate objects, create a certificate group, and enable the use of the group as a certificate chain.

NOTE: In the example, the name of the Transaction Security device is myDevice. The name of the secure logical server is server1. The name of the PEM-encoded certificate for your domain name is YourDomain.pem; the name of the PEM-encoded certificate chain is CertChain.pem. The names of the recognized and local certificate objects are trustedCert and myCert, respectively. The name of the certificate group is CACertGroup.

3. Start the **configuration manager**
4. Attach the configuration manager and enter Configuration mode. (If an attach or configurationlevel password is assigned to the device, you are prompted to enter any passwords.)

   inxcfg> attach myDevice
   inxcfg> configure myDevice
   (config[myDevice])>

5. Enter SSL Configuration mode and create an Intermediate certificate named CACert, entering into Certificate Configuration mode. Load the PEM-encoded file into the certificate object, and return to SSL Configuration mode.

   (config[myDevice])> ssl
   (config-ssl[myDevice])> cert myCert create
   (config-ssl-cert[CACert])> pem CertChain.pem
   (config-ssl-cert[CACert])> end
   (config-ssl[myDevice])>

6. Enter Key Association Configuration mode, load the PEM-encoded CA certificate and private key files, and return to SSL Configuration mode.

   (config-ssl[myDevice])> keyassoc localKeyAssoc create
   (config-ssl-keyassoc[localKeyAssoc])> pem YourDomain.pem key.pem
   (config-ssl-keyassoc[localKeyAssoc])> end
   (config-ssl[myDevice])>

7. Enter Certificate Group Configuration mode, create the certificate group CACertGroup, load the certificate object CACert, and return to SSL Configuration mode.

   (config-ssl[myDevice])> certgroup CACertGroup create
   (config-ssl-certgroup[CACertGroup])> cert myCert
   (config-ssl-certgroup[CACertGroup])> end

(config-ssl[myDevice])>

8. Enter Server Configuration mode, create the logical secure server server1, assign an IP address, SSL and clear text ports, a security policy myPol, the certificate group CACertGroup, key association localKeyAssoc, and exit to Top Level mode.

   (config-ssl[myDevice])> server server1 create
   (config-ssl-server[server1])> ip address 10.1.2.4 netmask 255.255.0.0
   (config-ssl-server[server1])> sslport 443
   (config-ssl-server[server1])> remoteport 81
   (config-ssl-server[server1])> secpolicy myPol
   (config-ssl-server[server1])> certgroup chain CACertGroup
   (config-ssl-server[server1])> keyassoc localKeyAssoc
   (config-ssl-server[server1])> end
   (config-ssl[myDevice])> end
   (config[myDevice])> end
   inxcfg>

9. Save the configuration to flash memory. If it is not saved, the configuration is lost during a power cycle or if the reload command is used.

   inxcfg> write flash myDevice
   inxcfg>

Verify certificate installation using the Symantec Installation Checker.

Installation Instructions for SonicWall SSL VPN Appliance

Step 1. Obtain and Install the SSL Certificate

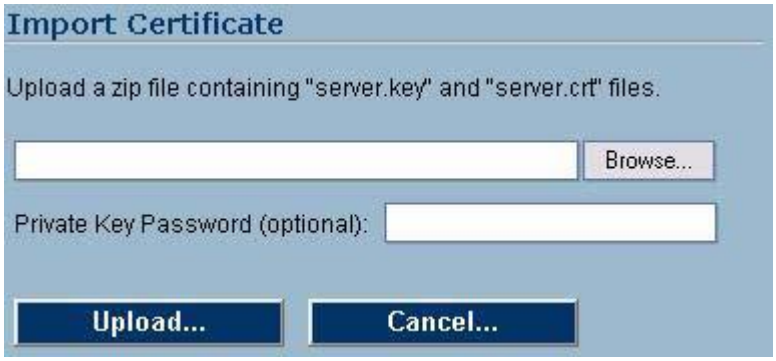
1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad
   The text file should look like:
   -----BEGIN CERTIFICATE-----

   [encoded data]

   -----END CERTIFICATE-----

3. Save the file as **server.crt**
4. Create a zipped file,that should contain a certificate file named **server.crt** and a certificate key file named **server.key**. The key and certificate must be at the root of the zip, or the zipped file will not be uploaded.
5. Navigate to the **System** > **Certificates** page.

5. Click **Import Certificate**. The Import Certificate dialog box is displayed.



6. Click **Browse**
7. Locate the zipped file that contains the private key and ssl certificate on your disk or network drive and select it. Any filename will be accepted, but it must have the "**.zip**" extension.
8. Click **Upload**
9. Once the certificate has been uploaded, the certificate will be displayed in the Certificates list in the **System > Certificates** page.

   NOTE: Private keys may required a password.
10. Select the imported certificate as the Default

Step 2. Download and Install the Intermediate CA Certificate

1. Download the Intermediate CA certificate. Select the appropriate Intermediate CA certificate for your SSL Certificate type.
2. Copy the Intermediate CA certificate and paste it on a Notepad.
3. Save the file as **intermediate.crt**.
4. Navigate to the **System > Certificates** page.
5. Click **Import Certificate** in the **Additional CA Certificates** section. The Import Certificate dialog box is displayed.
6. Click **Browse**
7. Locate the file saved as **intermediate.crt** on your disk or network drive and select it.
8. Click **Upload**
9. Once the certificate has been uploaded, the certificate will be displayed in the Certificates list in the **System > Certificates** page.

10. The web server needs to be restarted with the new certificate included in the CA certificate bundle.

Step 3. View Certificate and Certificate Authority (CA) Issuer Information

NOTE: The Current Certificates table in **System > Certificates** lists the currently loaded SSL certificates.

1. Click the **configure** icon for the certificate. The **Edit Certificate** dialog box is displayed showing issuer and certificate subject information.
2. From the **Edit Certificate** dialog box, you may view the issuer and certificate subject information.
3. Update the certificate common name by entering the correct IP address or string in the Common Name field.
4. Click **Submit** to submit changes.
5. You may also delete an expired or incorrect certificate. Delete the certificate by clicking the **Delete** button.

   NOTE: A certificate that is currently active cannot be deleted. To delete a certificate, upload and activate another SSL certificate, then delete the inactive certificate from **View Certificate** window.
6. Verify certificate installation using the Symantec Installation Checker.