SSL 证书 - SonicWALL

证书安装指南

webnic
accelerate your business

请选择您的版本

SonicWALL Offloaders SSL 安装指南

SonicWall SSL VPN SSL 安装指南

SonicWALL Offloaders SSL 安装指南

步骤 1：下载中级证书

1. 通过此链接下载中级 CA 证书。
2. 选择和你的 SSL 证书适合的中级 CA 证书。
3. 复制中级 CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 CertChain.pem。

步骤 2：获取 SSL 证书

1. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。
2. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

   证书正文的例子：

   -----BEGIN CERTIFICATE-----

   [加密数据]

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

3. 把证书存档为 YourDomain.pem。

步骤 3：设置证书链

1. 当你已经获取了上述证书，把证书导入各自的证书对象。
2. 把这些单独的证书对象导入证书群。这例子演示了如何加载两个证书入单独的证书对象，创建证书群，然后把证书群作为证书链使用。

注：在例子中，Transaction Security Device 的名字是 myDevice。Secure Logical Server 的名字是 server1。你的域名的 PEM-encoded certificate 的名字是 Yourdomain.pem。PEM-encoded certificate chain 的名字是 CertChain.pem。受认可的本地证书对象的名字是 trustedCert 和 myCert。证书群的名字是 CACertGroup。

3. 运行 **Configuration Manager**。
4. 连接 **Configuration Manager**，然后进入 **Configuration Mode**。

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

5. 进入 SSL Configuration 模式，然后创建中级证书，命名为 CACert，然后进入 Certificate Configuration 模式。把 PEM-encoded 文件导入证书对象，然后返回 SSL Configuration 模式。

```
(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. 进入 Key Association Configuration 模式，导入 PEM-encoded CA Certificate 和密钥文件，然后返回 SSL Configuration 模式。

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

7. 进入 Certificate Group Configuration 模式创建 CACertGroup 模式，然后导入 CACert 证书对象，然后返回 SSL Configuration 模式。

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

8. 进入 Server Configuration 模式，创建 Logical Secure Server server1，配置 IP 地址，SSL 证书和 Clear Text 端口，安全协议 myPol，证书群 CACertGroup，key association localKeyAssoc，然后返回到顶级模式。

```
(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. 把设置储存至闪存中，以防止设置在 Reload 命令时丢失。

```
inxcfg> write flash myDevice
inxcfg>
```

10. 要檢驗您的證書是否已正確安裝，請使用 Symantec 的證書檢查工具。

SonicWall SSL VPN SSL 安装指南

步骤 1：获取 SSL 证书

1. SSL 证书将会通过邮件发给用户。用户也可通过登入用户中心获取 SSL 证书。
2. 请把电邮中的正文复制并粘贴到 Vi 或 Notepad 等 TXT 文本编辑器。

   证书正文的例子：

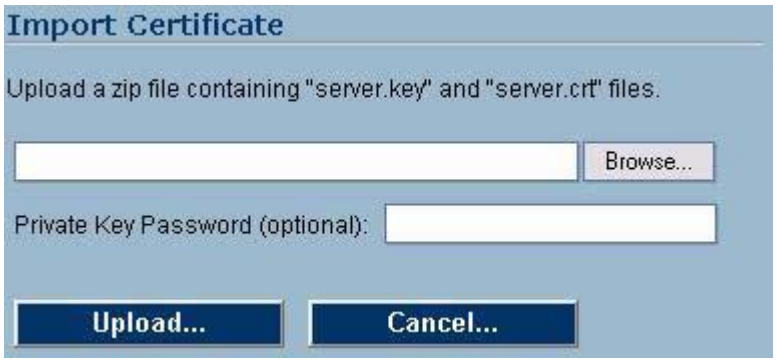
   -----BEGIN CERTIFICATE-----

   [加密数据]

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

3. 把证书存档为 server.crt。
4. 创建一个压缩文件，然后加入证书文件 server.crt 和密钥文件 server.key。这两个文件必须在压缩文件的最顶端，否则不会生效。
5. 导航到 System > Certificates 页面。

6. 点击 Import Certificate。导入证书的对话框将会出现。



7. 点击 Browse。
8. 点选刚刚创建的压缩（.zip）文件。
9. 点击 Upload。
10. 当证书已上传后，证书将会出现在 System > Certificates 页面的证书列表。
11. 选择导入证书为默认。

步骤 2：安装中级证书

1. 通过此链接下载中级 CA 证书。
2. 选择和你的 SSL 证书适合的中级 CA 证书。
3. 复制中级 CA 并粘贴至 Notepad 或其他 TXT 文本编辑器，并把文件存档为 Intermediate.crt。
4. 导航到 System > Certificates 页面。
5. 在 Additional CA Certificates 部分点击 Import Certificate。导入证书的对话框将会出现。
6. 点击 Browse。

7. 点选刚刚创建的 **Intermediate.crt** 文件。
8. 点击 **Upload**。
9. 当证书已上传后，证书将会出现在 **System** > **Certificates** 页面的证书列表。
10. 重启服务器。

步骤 3：查看证书和证书颁发机构（CA）发布者信息

1. 点击证书的配置图标，编辑证书的对话框将会出现并显示证书颁布者和证书的信息。
2. 在通用域名一栏，更新至正确的 IP 地址或通用域名。
3. 点击 Submit。
4. 你也可以使用删除功能删除过期或不正确的证书。

   注：激活中的证书不能删除。
5. 要检验您的证书是否已正确安装，请使用 Symantec 的证书检查工具。