SSL 證書 – SonicWALL

證書安裝指南

webnic
accelerate your business

請選擇您的版本

SonicWALL Offloaders SSL 安裝指南

SonicWall SSL VPN SSL 安裝指南

SonicWALL Offloaders SSL 安裝指南

步驟 1：下載中級證書

1. 通過此鏈接下載中級 CA 證書。
2. 選擇和你的 SSL 證書適合的中級 CA 證書。
3. 複製中級 CA 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為 CertChain.pem。

步驟 2：獲取 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。
2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

證書正文的例子：

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

[加密數據]

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

3. 把證書存檔為 YourDomain.pem。

步驟 3：設置證書鏈

1. 當你已經獲取了上述證書，把證書導入各自的證書對象。
2. 把這些單獨的證書對象導入證書群。這例子演示瞭如何加載兩個證書入單獨的證書對象，創建證書群，然後把證書群作為證書鏈使用。

   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。受認可的本地證書對象的名字是 trustedCert 和 myCert。證書群的名字是 CACertGroup。

3. 運行 Configuration Manager。
4. 連接 Configuration Manager，然後進入 Configuration Mode。

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

5. 進入 SSL Configuration 模式，然後創建中級證書，命名為 CACert，然後進入 Certificate Configuration 模式。把 PEM-encoded 文件導入證書對象，然後返回 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. 進入 Key Association Configuration 模式，導入 PEM-encoded CA Certificate 和密鑰文件，然後返回 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. 進入 Certificate Group Configuration 模式創建 CACertGroup 模式，然後導入 CACert 證書對象，然後返回 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. 進入 Server Configuration 模式，創建 Logical Secure Server server1，配置 IP 地址，SSL 證書和 Clear Text 端口，安全協議 myPol，證書群 CACertGroup，key association localKeyAssoc，然後返回到頂級模式。

(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. 把設置儲存至閃存中，以防止設置在 Reload 命令時丟失。

```
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 安裝指南

步驟 1：獲取 SSL 證書

1. SSL 證書將會通過郵件發給用戶。用戶也可通過登入用戶中心獲取 SSL 證書。
2. 請把電郵中的正文複製並粘貼到 Vi 或 Notepad 等 TXT 文本編輯器。

證書正文的例子：

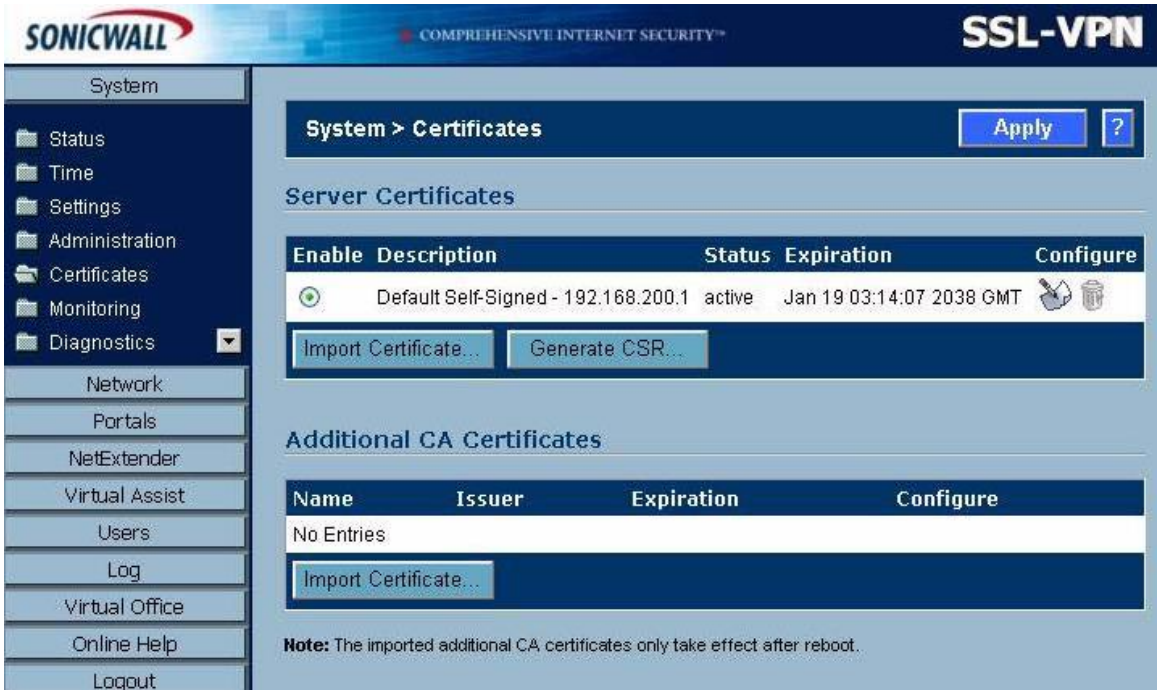
-----BEGIN CERTIFICATE-----

[加密數據]

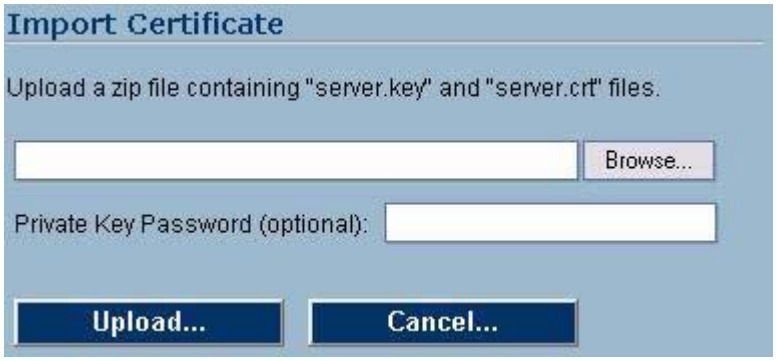
-----END CERTIFICATE-----

3. 把證書存檔為 server.crt。
4. 創建一個壓縮文件，然後加入證書文件 server.crt 和密鑰文件 server.key。這兩個文件必須在壓縮文件的最頂端，否則不會生效。

5. 導航到 System > Certificates 頁面。



6. 點擊 Import Certificate。導入證書的對話框將會出現。



7. 點擊 Browse。

8. 點選剛剛創建的壓縮（.zip）文件。

9. 點擊 Upload。

10. 當證書已上傳後，證書將會出現在 System > Certificates 頁面的證書列表。

11. 選擇導入證書為默認。

步驟 2：安裝中級證書

1. 通過此鏈接下載中級 CA 證書。
2. 選擇和你的 SSL 證書適合的中級 CA 證書。
3. 複製中級 CA 並粘貼至 Notepad 或其他 TXT 文本編輯器，並把文件存檔為 Intermediate.crt。
4. 導航到 System > Certificates 頁面。
5. 在 Additional CA Certificates 部分點擊 Import Certificate。導入證書的對話框將會出現。
6. 點擊 Browse。
7. 點選剛剛創建的 Intermediate.crt 文件。
8. 點擊 Upload。
9. 當證書已上傳後，證書將會出現在 System > Certificates 頁面的證書列表。
10. 重啟服務器。

步驟 3：查看證書和證書頒發機構（CA）發布者信息

1. 點擊證書的配置圖標，編輯證書的對話框將會出現並顯示證書頒布者和證書的信息。
2. 在通用域名一欄，更新至正確的 IP 地址或通用域名。
3. 點擊 Submit。
4. 你也可以使用刪除功能刪除過期或不正確的證書。

   注：激活中的證書不能刪除。
5. 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。