

FortiToken 介绍及使用

版本	1.0
时间	2011 年 12 月
作者	胡丹丹(ddhu@fortinet.com)
支持的版本	FortiOS v4.3
状态	草稿

目录

1.目的	3
2.环境介绍	3
3. FortiToken 用户添加与同步	4
3.1 添加 FortiToken 至 FortiGate.....	4
3.2 Fortitoken 的同步	5
4. FortiToken 的认证.....	6
4.1 管理员 FortiToken 双向认证	6
4.2 SSLVPN FortiToken 双向认证.....	8
5.批量的 FortiToken 导入	10

1.目的

FortiToken 是一种基于时间同步技术的动态令牌身份认证设备, 用于为应用系统提供高安全性的身份认证功能, 保护用户的身份认证安全, 防止攻击者通过身份盗用、身份冒用以及身份欺诈等方式实施非法操作, 损害合法用户的利益。

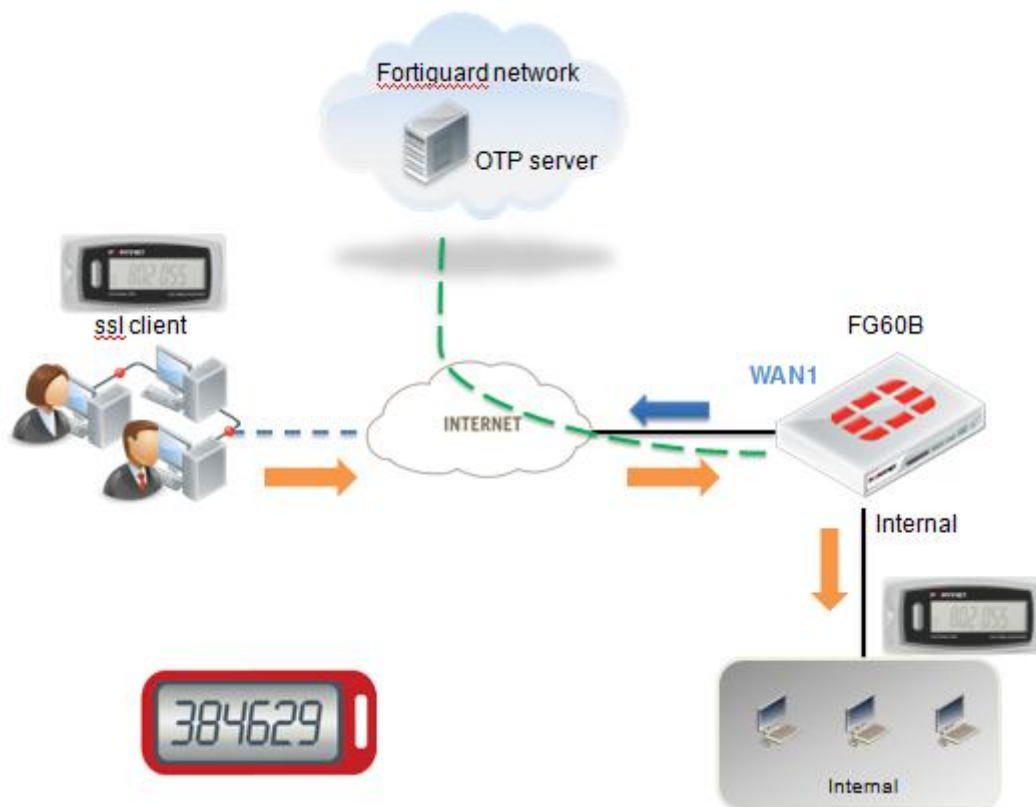
FortiToken 采用时间同步方式的 OTP 技术, OTP 全称叫 One-time Password, 也称动态口令, 是根据专门的算法每隔 60 秒生成一个与时间相关的、不可预测的随机数字组合, 每个口令只能使用一次, 每天可以产生 43200 个密码。其原理是基于动态令牌和动态口令验证服务器的时间比对, 基于时间同步的令牌, 一般每 60 秒产生一个新口令, 要求服务器能够十分精确的保持正确的时钟, 同时对其令牌的晶振频率有严格的要求, 这种技术对应的终端是硬件令牌。

动态口令是一种安全便捷的帐号防盗技术, 可以有效保护交易和登录的认证安全, 采用动态口令就无需定期更换密码, 安全省心, 这是这项技术的一个额外价值, 对企事业内部应用尤其有用。

本文就 FortiToken 结合 FortiGate 的实际应用进行说明。

2.环境介绍

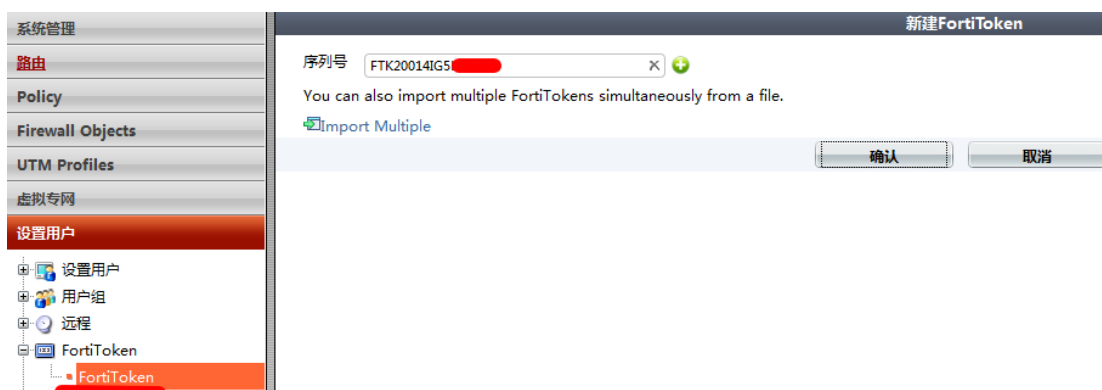
本文使用 1 台 FortiGate 310B 与 FortiToken 200 进行说明, 本文使用的系统版本为 FortiOS v4.0MR3 Patch3。同时进行批量扫描所用到的 android 系统为 2.3.7, 条码扫描器软件版本 4.6.2。



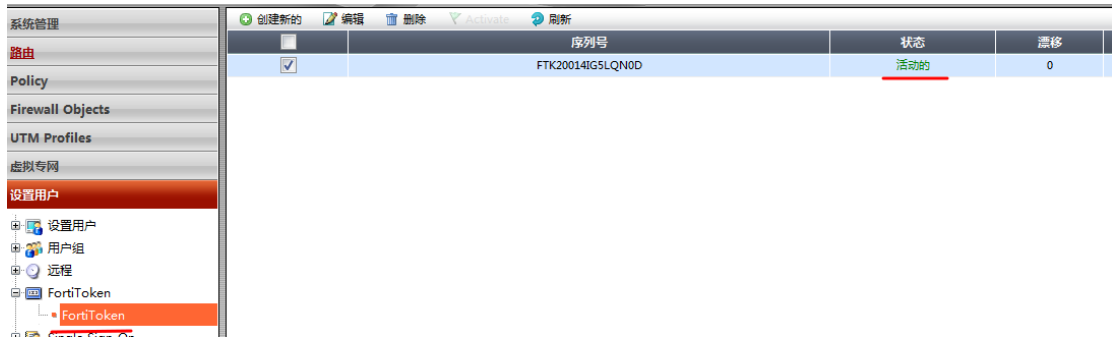
3. FortiToken 用户添加与同步

3.1 添加 FortiToken 至 FortiGate

设置用户—fortitoken—新建用户—在序列号一栏中输入 fortitoken 令牌背面的 15 位字符序列号



添加后 FortiGate 会激活该 Fortitoken



3.2 Fortitoken 的同步

新添加的 FortiToken 在同步之前还无法正常工作,由于本地 FortiToken 的每分钟的密码同 FDN 远端 OTP 服务器的密码不同步,以此在使用 FortiToken 之前必须与远端 OTP 服务器进行同步。



输入 2 个连续的 Token 码,即第一分钟一个,第二分钟一个。



同步 FortiToken

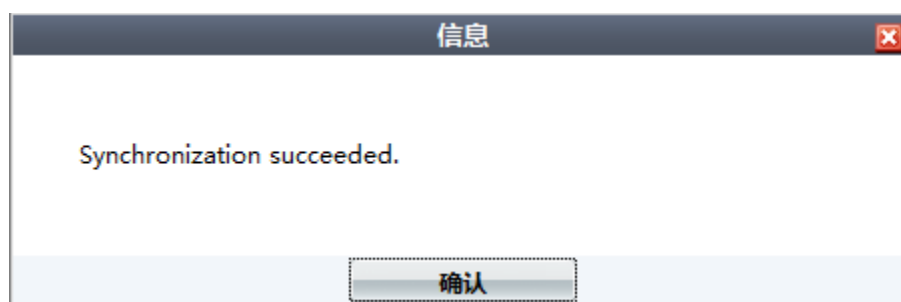
请输入两个FortiToken 码：

码1

码2

确认 取消

完成后会显示同步状态是否成功。



信息

Synchronization succeeded.

确认

4. FortiToken 的认证

FortiToken 的认证可以用于多种场景,如管理员登陆,SSLVPN 登陆验证,策略验证,同时也可以结合数字证书进行认证,以下我们就常用的场景进行介绍。

4.1 管理员 FortiToken 双向认证

添加系统管理员,启用双向认证,选择之前建立的 FortiToken 用户。

系统管理

- 面板
- 网络
- 配置
- 管理员设置
 - **管理员**
 - 访问内容表
- 设置
- 证书
- 监视器

路由

Policy

Firewall Objects

UTM Profiles

虚拟专网

设置用户

WAN优化和缓存

新建管理员

管理员	<input type="text" value="token"/>
类型	<input checked="" type="radio"/> 普通 <input type="radio"/> 远程 <input type="radio"/> PKI
输入密码	<input type="password" value="•••••"/>
确认密码	<input type="password" value="•••••"/>
访问表	<input type="text" value="super_admin"/>
范围	全局

启用双向认证

由 发送令牌码

FortiToken

邮件地址

SMS (移动服务提供商) (电话号码)

Restrict this Admin Login from Trusted Hosts Only

若同步成功仅需要输入一次 Token 码。否则需要输入两次连续的 Token 码

请输入您的FortiToken

用户名	<input type="text" value="token"/>
密码	<input type="password" value="•••••"/>
FortiToken	<input type="text"/>

FortiToken clock drift detected. Please input the next code and continue.

用户名	<input type="text" value="token"/>
密码	<input type="password" value="•••••"/>
FortiToken	<input type="password" value="•••••"/>
Next Code	<input type="text"/>

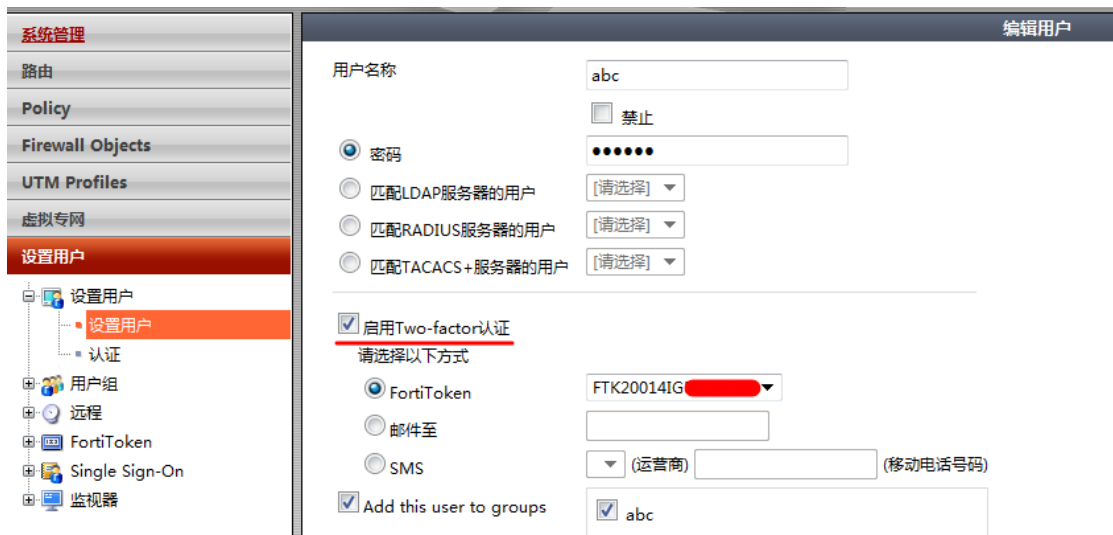
4.2 SSLVPN FortiToken 双向认证

本文仅对涉及到 FortiToken 中的相关步骤进行介绍,如需了解 SSLVPN 的配置方法请参考[如何配置 SSL VPN 4.2](#)。

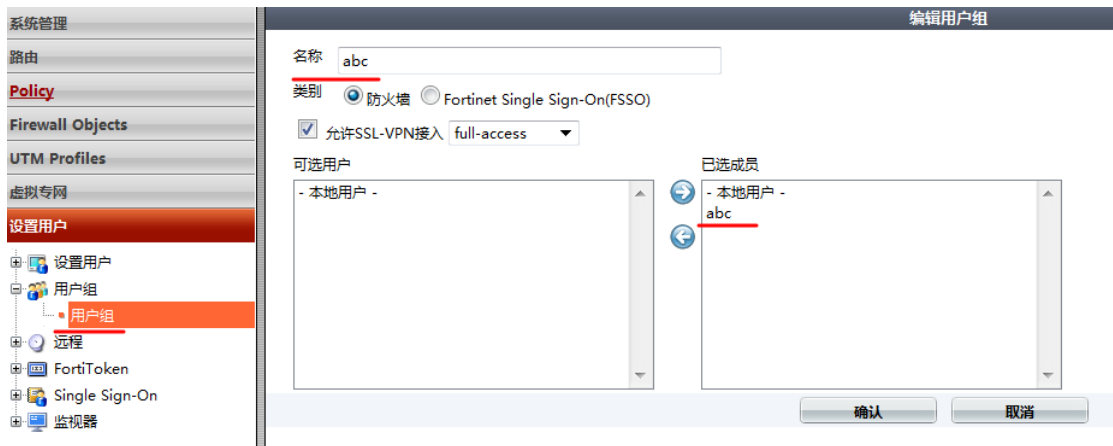
添加 SSL 用户 abc



启用双向认证



创建 abc 的用户组



创建 SSL VPN 策略,启用 abc 用户组进行认证

新建认证规则

用户组

+

服务

+

时间表

+

记录允许流量
 UTM
 流量控制

系统管理

路由

Policy

- 策略
 - 策略
 - DoS策略
 - 探测策略
 - 协议选项
- 监视器

Firewall Objects

UTM Profiles

虚拟专网

设置用户

WAN优化和缓存

新建输出策略

源接口/区

源地址

+

目的接口/区

目的地址

+

动作

SSL客户端认证限制
 加密强度

配置SSL-VPN用户

规则ID	用户组	服务	时间表	UTM	Logging
1	abc	ANY	always		

注释 0/63

之后在使用 SSL VPN WEB 登陆时,除输入 abc 账号密码外,需额外输入

Token 码

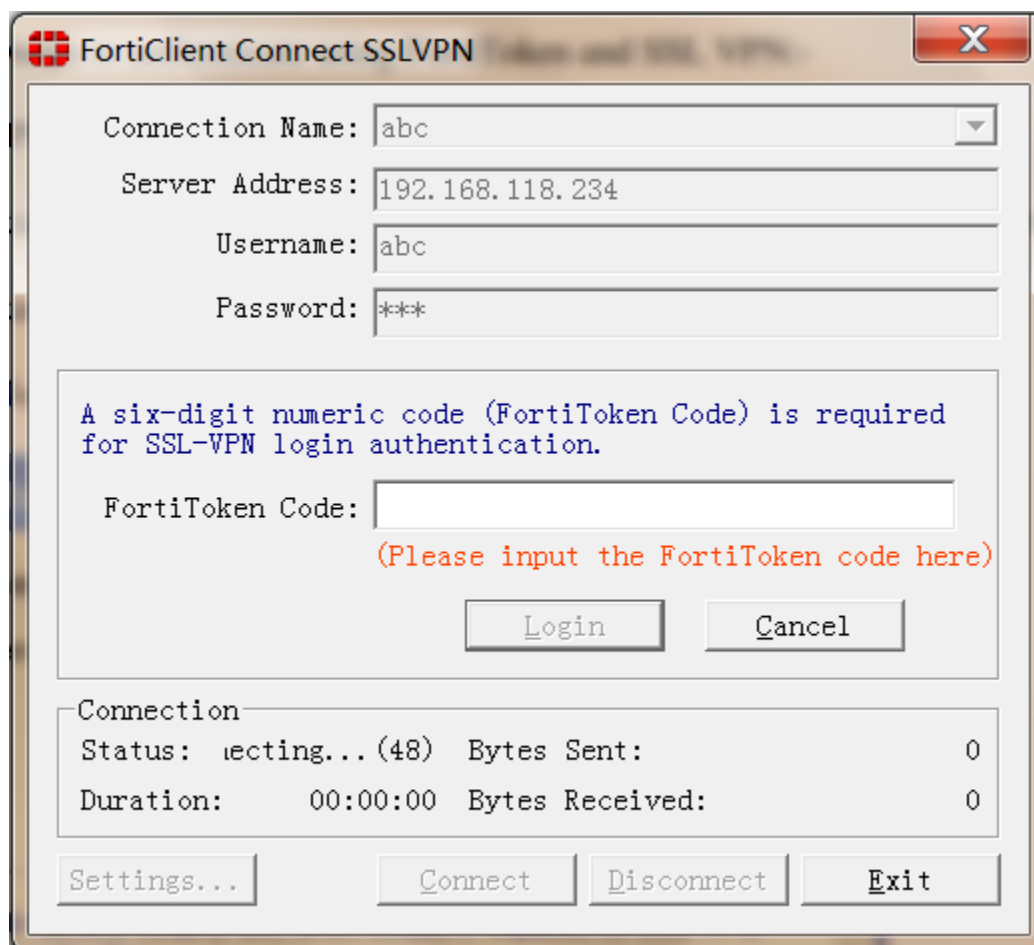
Please Login

Name:

Password:

FortiToken Code:

FortiToken 同时也支持 SSL Tunnel 模式的认证,如下



5.批量的 FortiToken 导入

大量的 FortiToken 进行部署时,逐个进行新建 FortiToken 用户是件很痛苦的事情,FortiNet 也提供批量 FortiToken 的导入方式,本文以 android 系统及条码扫描器为例,对批量导入 FortiToken 进行简单介绍。

首先安装条码扫描器软件,将软件模式在设置中开启批量扫描模式



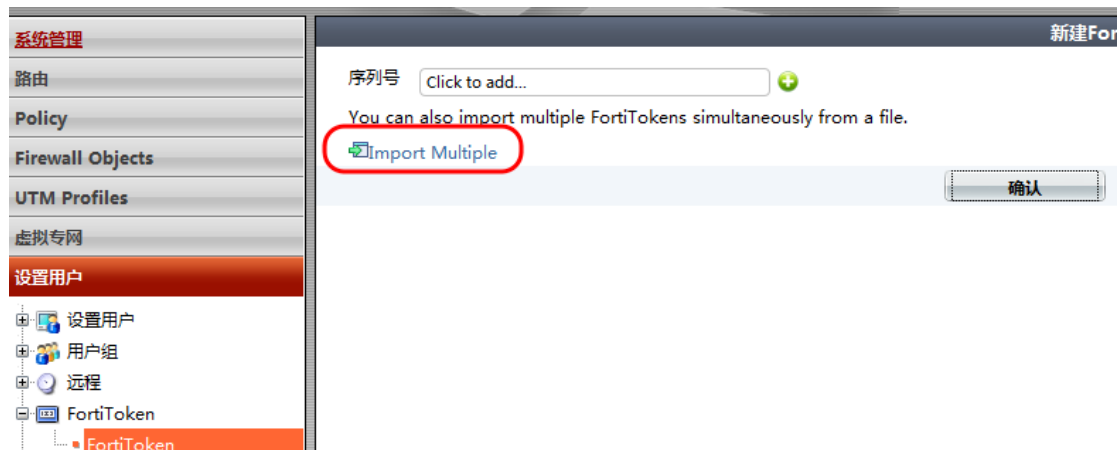
对 FortiToken 进行扫描

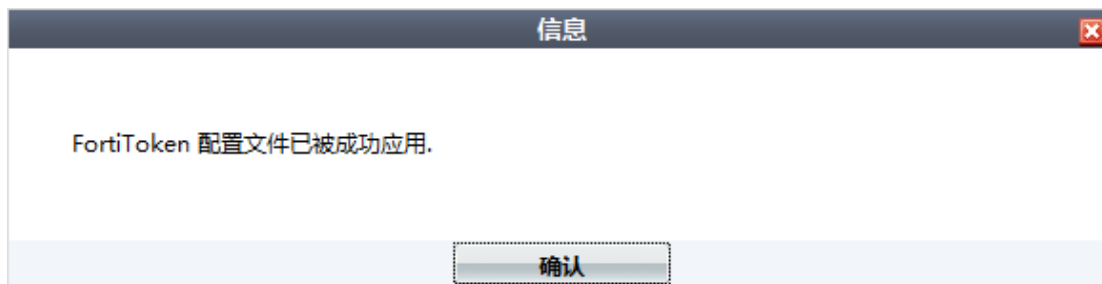


对于历史扫描的所有条码,条码扫描器会生产一个后缀为.csv 的文件,可将其以 Email 形式发送至邮箱



在收到 csv 文件后即可对 FortiToken 进行批量导入





至此, FortiToken 的批量导入即以完成。

目前, FortiToken 可以通过联系 Fortinet 的销售代表或者在[官方网店](#)进行购买。