清华永新统一安全网关 TN-SG5000 V5.0

脆弱性分析文档v1.0

**江苏清华永新安全科技有限公司**

**目 录**

[1.安全功能强度分析 3](#_Toc24419)

[2.脆弱性分析 3](#_Toc4733)

[2.1 TCP 端口443 3](#_Toc11931)

[2.2 TCP端口80 4](#_Toc16430)

[2.3 TCP端口22 4](#_Toc1824)

[2.4 TCP端口23 4](#_Toc30459)

[2.5用户登录口令方式 4](#_Toc29253)

[2.6 误操作分析 5](#_Toc5379)

# 安全功能强度分析

　　弱口令一直是数据泄露的一个大症结，因为弱口令是最容易出现的也是最容易被利用的漏洞之一。所谓弱口令就是非常简单的密码，比如“admin、123456、888888”等等。这类密码因为很方便记忆，所以被大量使用，但是也非常容易让他人猜测到，更容易被黑客暴力破解。

弱口令破解主要有两种方法：字典破解和暴力破解。

字典破解是指通过破解者对管理员的了解，猜测其可能使用某些信息作为密码，例如其姓名、生日、电话号码等，同时结合对密码长度的猜测，利用工具来生成密码破解字典。如果相关信息设置准确，字典破解的成功率很高，并且其速度快，因此字典破解是密码破解的首选。

暴力破解是指对密码可能使用的字符和长度进行设定后（例如限定为所有英文字母和所有数字，长度不超过8），对所有可能的密码组合逐个实验。随着可能字符和可能长度的增加，存在的密码组合数量也会变得非常庞大，因此暴力破解往往需要花费很长的时间，尤其是在密码长度大于10，并且包含各种字符（英文字母、数字和标点符号）的情况下。

所以防火墙应具备高强度密码策略，高强度密码规则参考：至少包含大写字母、小写字母、数字、符号中至少三种，至少8位以上。

# 2.脆弱性分析

## 2.1 TCP 端口443

功能：该端口是防火墙的Web界面默认管理端口；

脆弱性：对TOE不构成威胁；

说明：防火墙默认开放的443端口有3层防护：

* 1. 使用SSL协议，即必须使用https登录方式；
  2. 必须有防火墙的数字证书；
  3. 连接443的IP必须是防火墙指定的管理主机地址，否则该连接将被拒绝；

## 2.2 TCP端口80

功能：该端口是防火墙的web管理端口；

脆弱性：对TOE不构成威胁；

说明：防火墙80端口有3层防护：

1. 必须使用HTTP协议才能登录；
2. 防火墙必须开启HTTP登录方式，否则80端口默认不开放；
3. 连接80的IP必须是防火墙的管理主机地址，否则该连接将被拒绝；

## 2.3 TCP端口22

功能：该端口是防火墙的命令行管理端口；

脆弱性：对TOE不构成威胁；

说明：防火墙22端口有3层防护：

1. 必须使用SSH协议才能登录；
2. 防火墙必须开启SSH登录方式，否则22端口默认不开放；
3. 连接22的IP必须是防火墙的管理主机地址，否则该连接将被拒绝；

## 2.4 TCP端口23

功能：该端口是防火墙的命令行管理端口；

脆弱性：对TOE不构成威胁；

说明：防火墙23端口有3层防护：

1. 必须使用TELNET协议才能登录；
2. 防火墙必须开启TELNET登录方式，否则23端口默认不开放；
3. 连接23的IP必须是防火墙的管理主机地址，否则该连接将被拒绝；

## 2.5用户登录口令方式

功能：该端口是防火墙的用户认证端口；

脆弱性：对TOE不构成威胁；

说明：防火墙口令登录方式有如下防护：

1. 防火墙密码连续错误输入5次后，将账号锁定，必须在超时后解锁；
2. 防火墙密码长度不小于8位，且提供数字、字母及特殊符号的组合，密码加密方式传输；

## 2.6 误操作分析

防火墙管理误操作中主要存在以下几种：

1. 异常断电
2. 配置错误
3. 误删除配置

脆弱性：对TOE不构成威胁；

说明：防火墙针对异常情况提供了保存配置及配置导出的功能，当出现误操作或者出现异常情况时，可以重启恢复防火墙正确配置或者导入原先无误的配置。