

# 文件安全网关使用手册



版权所有：深圳市中科网威科技有限公司

## 声明

本公司对本手册的内容在不通知用户的情况下有更改的权利。  
其版权归深圳市中科网威科技有限公司所有。  
未经本公司书面许可，本手册的任何部分不得以任何形式手段复制或传播。

## NOTICES

Shenzhen Anysec-Tech Company Limited reserves the right to make any changes in specifications and other information contained in this publication without prior notice and without obligation to notify any person or entity of such revisions or changes.

© Copyright 2009 -2012 by Anysec-Tech. Co., Ltd. All Right Reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical. Including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, without express written permission of Anysec Co., Ltd.

ANYSEC 是深圳市中科网威科技有限公司注册商标。所有其他商标均属于有关公司所有。

## 目录

一、前言 .....	4
二、文件安全网关功能特点 .....	5
2.1、使用方便、安全 .....	5
2.2、支持多种通讯协议 .....	5
2.3、文件深度检测 .....	5
2.4、MD5 校验 .....	5
2.5、多格式文件支持 .....	5
2.6、访问方式 .....	5
2.7、文件智能学习 .....	5
三、文件安全网关配置步骤 .....	6
3.1、登录设备 .....	6
3.2、设备配置 .....	6
3.3、系统配置 .....	7
说明：许可证一栏存在如下几种情况： .....	7
1、 恢复配置 .....	7
2、 备份配置 .....	7
3、 还原出厂配置 .....	7
3.4、网络配置 .....	8
3.5、用户管理 .....	10
3.6、文件管理 .....	12
3.7、磁盘映射 .....	13
3.8、摆渡管理 .....	14
3.9、文件同步 .....	15
3.10、应用映射 .....	16
3.11、访问策略 .....	17
3.12、病毒防护 .....	17
3.13、密码修改 .....	18
四、日志审计 .....	19
五、FTP 客户端使用说明 .....	21
5.1、下载 .....	21
5.2、安装 .....	21
5.3、用 ftp 软件登录文件安全网关 .....	21
六、常见问题处理 .....	24
6.1、输入正确的网络地址（IP）无法访问？ .....	24
6.2、 Web 界面显示紊乱，按钮无法点击？ .....	24
6.3、进入主界面无任何文件列表显示？ .....	24
6.4、进入 ftp 客户端发现文字乱码 .....	24
6.5、ftp 客户端不能下载某文件，错误是 553 服务器未知错误 .....	25
6.6、ftp 客户端不能上传某文件，错误是 550 不能存 .....	25
七、结束语 .....	26

## 一、前言

随着数字化、网络化技术的发展，国内各级电视台纷纷投入大量资金搭建了数字电视节目制作网络和播出网络，但是随之而来的病毒传播以及网络病毒攻击行为已经严重威胁电视台的正常运转。因为病毒等原因造成的停播、漏播等事故时有发生。计算机病毒和网络安全问题已经成为了工作人员正常工作的重大威胁，深圳中科网威已经有了近十年播出网和制作网病毒防范和网络安全设计、研发和实施经验。文件安全网关通过多种技术手段，最大程度保证了系统免受病毒的破坏。

文件安全网关是一款完全自主开发的安全隔离设备。它通过控制病毒传播途径，实现病毒隔离。它从源头上阻止了病毒的传播，在保障数据传输的同时，实现了数据资料的受控传输、格式检查、深度过滤等安全功能，确保整个传输过程高速、安全、可控。

## 二、文件安全网关功能特点

### 2.1、使用方便、安全

本产品安装、配置简单，接上文件安全网关就可以正常工作，降低了对相关人员专业性的要求。

### 2.2、支持多种通讯协议

文件安全网关支持多种通讯协议，包括 FTP、SAMBA、应用映射。

### 2.3、文件深度检测

内置了基于文件内容的深度检测算法，根据文件类型和格式进行深度检查，不简单停留在尾缀检测，能准确快速的识别病毒伪装文件，避免假冒文件通过。

### 2.4、MD5 校验

内置 MD5 校验协议，在传输文件的同时，将文件的 MD5 文件生成并将 MD5 文件以及正常文件一起上传到文件安全网关设备上。

### 2.5、多格式文件支持

支持广电常用的文件格式，新一代的文件检查过滤引擎检查比对速度更快运行效率更高，并且支持文件的格式众多

例如：视频：MPEG1、MPEG2、MPEG4(mp4 m4v m4a m4p 3gpp 3gp 3gpp2 3g2 k3g)、MPEG 传输流 (ts m2t m2s m4t m4s ts tp trp)、MOV、AVI、FLASH、Windows Media (ASF WMV WMA)、Real Media (RM RMVB RA)、mkv mka mks 等；音频：MP1、MP2、MP3、WAV、MIDI、OGG、ACC、AC3、DTS；图片：BMP、JPG、TGA、GIF、PNG、ICO、TIF；

其他格式：TXT；并且支持自定义的其他任意文件格式。

### 2.6、访问方式

提供了两种访问方式：ftp 访问和 web 访问。ftp 访问方式是图形 UI 的界面，方便进行目录整体迁移拷贝的功能，推荐常用的 ftp 客户端例如 filezilla 等，filezilla 是一款免费开源的 ftp 客户端软件，其客户端可以运行在 windows、mac、linux 等平台。Web 访问方式为浏览器访问。

### 2.7、文件智能学习

通过智能文件学习，将不在文件白名单里的后缀文件进行智能学习。以便开启深度检测。

## 三、文件安全网关配置步骤

### 3.1、登录设备

文件安全网关 E0 口默认 IP 地址 192.168.0.88 用户名/密码: admin/admin

E1 口默认 IP 地址是 192.168.1.99

E2 口默认 IP 地址是 192.168.2.99

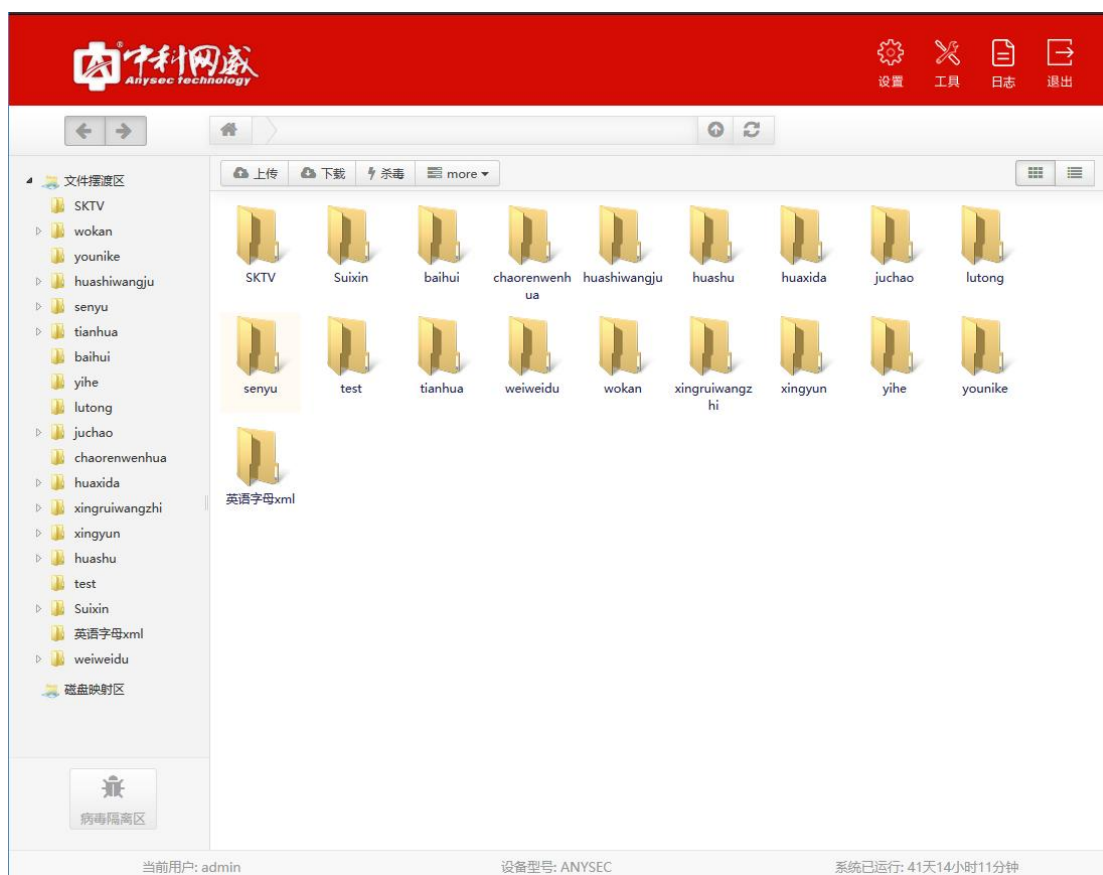
E3 口默认 IP 地址是 192.168.3.99

将配置用到的电脑 IP 地址修改成 192.168.0.X/24 网段, 连接到文件安全网关设备的 E0 口。打开浏览器输入 <http://192.168.0.88> 看到如下登录界面, 输入用户名和密码登录设备。



### 3.2、设备配置

登录设备后即可看到如下界面。Web 方式用管理员帐号进入主界面后, 右上角有配置按钮, 点击配置即可对当前系统进行配置 (如图)



### 3.3、系统配置

系统名称：即系统登录 logo 标题，可自定义建议 20 个字符以内。

设备型号：即该设备的型号。

设备序列号：设备的身份识别号。

许可证：设备的许可授权

**说明：许可证一栏存在如下几种情况：**

- 1、显示“正式授权许可证”，表示该文件安全网关里已经导入了正式授权许可文件。
- 2、显示“试用(过期日:年月日 时间 星期)”，表示文件安全网关处于试用状态以及到期的时间。
- 3、显示“没有许可证”，表示当前文件安全网关没有许可证，该状态下部分功能不可用。

软件版本：设备的软件的版本

硬件版本：设备硬件版本。

工作状态：正常运行

系统已运行：系统运行的时间。

资源状态：即设备系统的内存使用率、CPU 使用率、磁盘使用率等。

双机热备：是用于提供设备高可靠性服务的一种功能，通常的做法是提供 2 台或者多台设备模拟成一个虚拟设备，对外提供一个 IP 地址，来提供网络服务。

配置维护：

- 1、恢复配置
- 2、备份配置
- 3、还原出厂配置

### 3.4、网络配置

接口管理:配置文件安全网关的 IP 地址,子网掩码,以及网关,以便能通过局域网访问文件安全网关。  
 路由管理:添加默认路由、静态路由等。



**系统设置**

**选项**

- 系统设置
- 网络设置**
- 用户管理
- 文件管理
- 磁盘映射
- 摆渡管理
- 文件同步
- 应用映射
- 访问策略
- 病毒防护
- 密码修改

**网络设置**

接口管理 | 路由管理 | DNS服务器 | 高级选项

接口名	IP地址	子网掩码	状态	工作模式	操作
E0	192.168.0.88	255.255.255.0		route	<a href="#">编辑</a> <a href="#">速率</a>
E1	192.168.59.55	255.255.255.0		route	<a href="#">编辑</a> <a href="#">速率</a>
E2	192.168.2.88	255.255.255.0		route	<a href="#">编辑</a> <a href="#">速率</a>
E3	192.168.3.88	255.255.255.0		route	<a href="#">编辑</a> <a href="#">速率</a>



**系统设置**

**选项**

- 系统设置
- 网络设置**
- 用户管理
- 文件管理
- 磁盘映射
- 摆渡管理
- 文件同步
- 应用映射
- 访问策略
- 病毒防护
- 密码修改

**网络设置**

接口管理 | **路由管理** | DNS服务器 | 高级选项

目的IP	子网掩码	网关地址	跳数	接口	操作
192.168.0.0	255.255.255.0	0.0.0.0	0	E0	
192.168.2.0	255.255.255.0	0.0.0.0	0	E2	
192.168.3.0	255.255.255.0	0.0.0.0	0	E3	
192.168.59.0	255.255.255.0	0.0.0.0	0	E1	
<a href="#">+添加</a>					



路由添加：输入目的地址，子网掩码，以及下一跳地址或接口地址等。

192.168.123.0	255.255.255.0	0.0.0.0	0	E2	<input type="button" value="路由添加"/> <input type="button" value="取消"/>
<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="0.0.0.0"/>	<input type="text" value="6"/>	<input type="text" value="E7"/>	
+添加					

DNS 服务器：如果文件安全网关需要定时到公网更新病毒库之类的需要添加本地的 DNS 地址。一般电信可以输入 114.114.114.114 其它运营商可以输入：8.8.8.8

### 网络设置

接口管理
路由管理
DNS服务器

主DNS服务器:

从DNS服务器:

高级选项：允许数据包转发（打勾）

系统设置

## 选项

- 系统设置
- 网络设置
- 用户管理
- 文件管理
- 磁盘映射
- 摆渡管理
- 文件同步
- 应用映射
- 访问策略
- 病毒防护
- 密码修改

### 网络设置

接口管理
路由管理
DNS服务器
高级选项

允许数据包转发

TCP会话超时  (单位: 秒)

UDP会话超时  (单位: 秒)

ICMP会话超时  (单位: 秒)

登录失败最大值  (单位: 次)

防SYN Cookie攻击

防源IP欺骗攻击

防Ping of death攻击

远程日志

### 3.5、用户管理

用户管理： 用户点击管理员菜单，可以对文件安全网关的访问控制进行设置。管理员可以访问文件安全网关并配置其操作。在设备初始化安装完成后，默认的配置有一个用户名为 **admin** 的管理员账户，其初始默认密码为 **admin**；和用户名为 **audit** 的日志账户，其初始默认密码为 **audit**；通过连接到基于 **Web** 的管理器，用户也可以配置更多的管理员具有权限的文件安全网关的配置的管理访问。比如增加普通用户 **user**、**user1**.....

日志审计账户：



ID	时间	用户名	用户IP	文件名	传输方向	处理方式	备注
415	2020-06-12 07:28:30	admin	192.168.59.188	1.m4a	上传	通过	
414	2020-06-12 06:44:57	admin	192.168.59.139	test压缩.rar	上传	通过	
413	2020-06-12 03:24:35	admin	192.168.59.139	uploadadd.png	上传	通过	
412	2020-06-12 03:24:34	admin	192.168.59.139	upload.png	上传	通过	
411	2020-06-12 03:24:34	admin	192.168.59.139	synchronize.png	上传	通过	
410	2020-06-12 03:24:34	admin	192.168.59.139	speedlimits.png	上传	通过	
409	2020-06-12 03:24:34	admin	192.168.59.139	sitemanager.png	上传	通过	
408	2020-06-12 03:24:33	admin	192.168.59.139	remotetreeview.png	上传	通过	
407	2020-06-12 03:24:33	admin	192.168.59.139	refresh.png	上传	通过	
406	2020-06-12 03:24:33	admin	192.168.59.139	reconnect.png	上传	通过	

系统设置

### 选项

- 系统设置
- 网络设置
- 用户管理
- 文件管理
- 磁盘映射
- 摆渡管理
- 文件同步
- 应用映射
- 访问策略
- 病毒防护
- 密码修改

## 用户管理

用户管理
权限管理
添加权限
白名单
登录黑名单

用户名	权限	操作
admin	Administrator	默认权限不能操作
audit	audit	默认权限不能操作
user	user	<span style="background-color: #008080; color: white; padding: 2px 5px;">编辑</span> <span style="background-color: #008080; color: white; padding: 2px 5px;">删除</span>
+ 添加		

权限管理：建立权限组，可以设置不同的权限。

## 用户管理

用户管理
权限管理
添加权限
白名单
登录黑名单

权限	名称	操作
root	Administrator	默认权限不能操作
audit	audit	默认权限不能操作
user	user	<span style="background-color: #008080; color: white; padding: 2px 5px;">编辑</span> <span style="background-color: #008080; color: white; padding: 2px 5px;">删除</span>
+ 添加		

添加权限：添加权限组并定义相关权限。

## 用户管理

用户管理	权限管理	添加权限	白名单	登录黑名单
权限	<input type="text"/>	建议英文名, 不能重复		▲提示!
展示名称	<input type="text"/>	权限名描述		
上传下载	<input type="checkbox"/> 文件(夹)删除	<input type="checkbox"/> 文件上传	<input type="checkbox"/> 文件下载	上传大文件(>200M)时,请使用FTP或文件共享传输方式
修改密码	<input type="checkbox"/> 修改密码			
用户管理	<input type="checkbox"/> 列表查看	<input type="checkbox"/> 添加用户	<input type="checkbox"/> 编辑用户	<input type="checkbox"/> 删除用户
权限管理	<input type="checkbox"/> 列表查看	<input type="checkbox"/> 添加权限	<input type="checkbox"/> 编辑权限	<input type="checkbox"/> 删除权限
确定				全选/反选

权限：即定义的权限名称，建议为英文或拼音，不能重复

展示名称：针对权限名称的备注。

文件管理权限：包括：新建文件、新建文件夹、重命名、文件(夹)属性、移动(复制/剪切/粘贴/拖拽操作)

上传下载：文件(夹)删除、文件上传、文件下载

修改密码：允不允许修改各用户的密码

用户管理：列表查看、添加用户、编辑用户、删除用户

权限管理：列表查看、添加权限、编辑权限、删除权限

白名单：不添加默认所有电脑 ip 都是白名单，添加 IP 后只允许该 IP 通过，其它都是黑名单

黑名单：账号密码输错 5 次以上含 5 次自动加入黑名单

## 用户管理

用户管理	权限管理	添加权限	白名单	登录黑名单
登录IP	<input type="text"/>			操作
IP	<input type="text"/>			<input type="button" value="添加"/> <input type="button" value="取消"/>
+添加				

### 3.6、文件管理

文件管理即文件白名单，分为视频类、音频类、图片类、以及其它常见文件类型，勾选的话，是表示普通用户登录时，显示该类型的文件，但管理员登录的话，所有文件类型都会显示。系统默认 exe, dll, com, bat 不能通过。

自定义类型：输入文件后缀，每个后缀名中间用英文文件标点符号逗号“，”隔开。

深度检测：根据文件类型和格式进行深度检查，不简单停留在尾缀检测，能准确快速的识别病毒伪装

文件，避免假冒文件通过。

MD5 校验：开启后需要计算出所上传文件的 MD5 值文件并和源文件一起上传。设备会对每个文件的 MD5 进行比较。

目录自动删除：打勾后摆渡文件成功即将该目录自动删除（仅限摆渡方式）



文件智能学习：将没有在白名单里的文件，导入让设备自动学习。深度检测时能正常识别。导入文件后点开始学习即可。尽量文件不在太大。



### 3.7、磁盘映射

将内网磁盘映射出来，让客户端能正常访问并能对访问文件做病毒防护以及安全检查。



映射通道名：对外发布的文件名字

服务器 IP：内网服务器的 IP 地址

共享文件名：内网服务器的共享文件名（windows 共享目录名）

登录用户名：服务器登录的用户名

登录密码：服务器登录的密码

### 3.8、摆渡管理

配置好通过何种协议对需要传输到内网服务器的文件进行摆渡映射。



摆渡通道名：对外发布的摆渡文件夹名方便用户识别（不能与共享名一致）

传输方式：选择文件的传输方式，通过 FTP 或 SAMBA 方式（即 windows 文件共享方式）

服务器 IP：内网服务器 IP 地址。

传输路径:Windows 文件共享方式，填写共享名，FTP 方式，填目录名，若为 FTP 服务器根目录，请填写“/”。

登录用户名：服务器登录的用户名

登录密码：服务器登录的密码

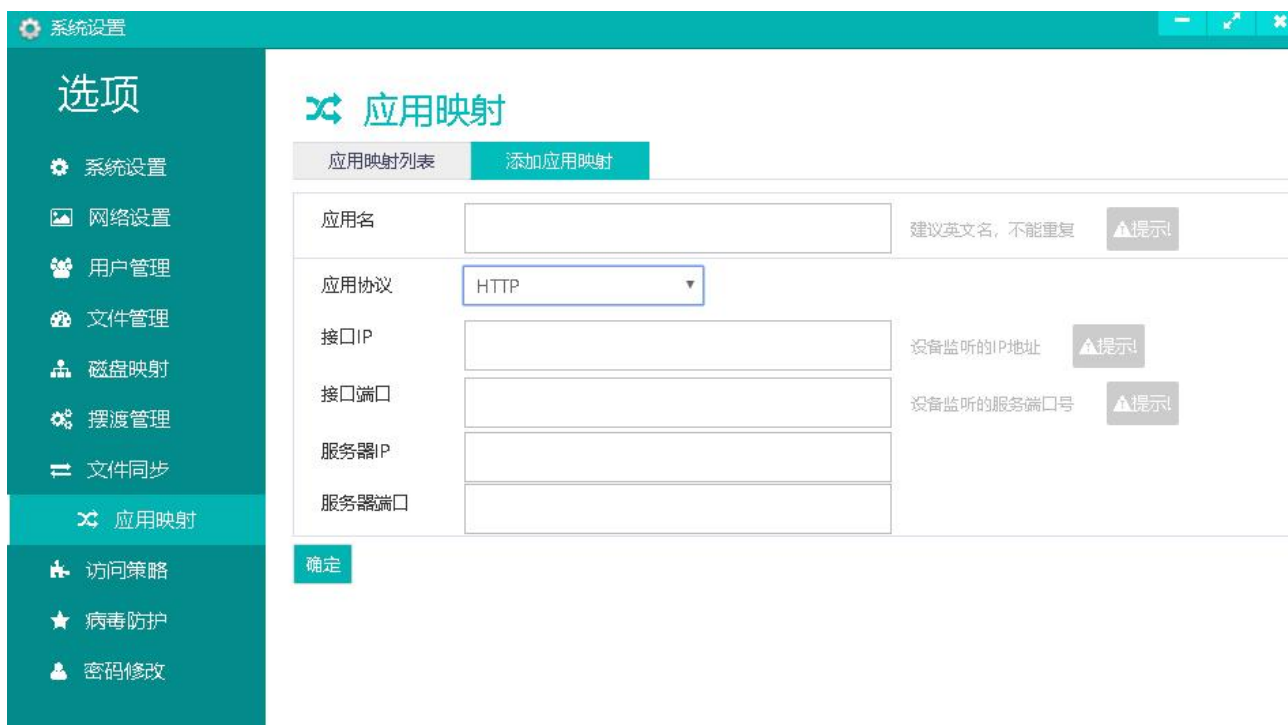
### 3.9、文件同步

文件同步：设置后传输的文件同步到设备里



### 3.10、应用映射

将内网某些应用映射到设备上。可以不用告诉用户内网服务器的真实 IP. 具体使用参数如下：



应用名：应用映射名用于区分每个映射的标识。

应用协议：应用映射的协议，包括：HTTP、FTP、SAMBA。



接口 IP: 设备监控的 IP 地址, 若监听设备所有接口的 IP, 请输入 0.0.0.0

接口端口: 设备监听的服务端口号, 该端口用于转发数据到服务器。

服务器 IP: 服务器的 IP 地址

服务器端口: 被映射服务器的端口。

### 3.11、访问策略



The screenshot shows the '访问策略' (Access Policy) configuration page. On the left is a sidebar with navigation options: 系统设置, 网络设置, 用户管理, 文件管理, 磁盘映射, 摆渡管理, 文件同步, 应用映射, 访问策略 (selected), 病毒防护, and 密码修改. The main content area is titled '访问策略' and contains a table for '访问策略列表' (Access Policy List).

包匹配	源IP	目的IP	协议	目的端口	控制	操作
	0.0.0.0/0		ALL		允许	确认 取消

Below the table is a '+添加' (Add) button.

### 3.12、病毒防护

对通过文件安全网关进行的文件传输, 进入病毒查杀处理。并且有相应的许可证文件。



The screenshot shows the '病毒防护' (Virus Protection) configuration page. The sidebar is the same as in the previous screenshot, with '病毒防护' (selected) highlighted. The main content area is titled '病毒防护' and contains several input fields for configuration:

- 防病毒许可证: [Input Field]
- 病毒库特征码: [Input Field]
- 病毒库更新时间: [Input Field]
- 许可过期时间: [Input Field]

At the bottom of the configuration area is a '确定' (Confirm) button.

防病毒许可证：病毒防护开启的许可证文件。

病毒库特征码：病毒库的特证码，定时升级处理之差的。

病毒库更新时间：病毒库更新的最新时间。

许可过期时间：病毒许可过期的时间。

### 3.13、密码修改

密码修改：修改设备登录密码。



## 修改密码

---

原密码

新密码

确认新密码

## 四、日志审计

为了响应二级等保将日志单独作为一个账户查看。

文件传输日志：包括 WEB 日志、FTP 日志、SAMB A 日志、摆渡日志、同步日志、病毒查杀日志、操作日志等。

### 日志审计

WEB日志	FTP日志	SAMB A日志	摆渡日志	同步日志	病毒查杀日志	操作日志	
当前记录总数: 415 ( 406 - 415 )							
ID	时间	用户名	用户IP	文件名	传输方向	处理方式	备注
415	2020-06-12 07:28:30	admin	192.168.59.188	1.m4a	上传	通过	
414	2020-06-12 06:44:57	admin	192.168.59.139	test压缩.rar	上传	通过	
413	2020-06-12 03:24:35	admin	192.168.59.139	uploadadd.png	上传	通过	
412	2020-06-12 03:24:34	admin	192.168.59.139	upload.png	上传	通过	
411	2020-06-12 03:24:34	admin	192.168.59.139	synchronize.png	上传	通过	
410	2020-06-12 03:24:34	admin	192.168.59.139	speedlimits.png	上传	通过	
409	2020-06-12 03:24:34	admin	192.168.59.139	sitemanager.png	上传	通过	
408	2020-06-12 03:24:33	admin	192.168.59.139	remotetreeview.png	上传	通过	
407	2020-06-12 03:24:33	admin	192.168.59.139	refresh.png	上传	通过	
406	2020-06-12 03:24:33	admin	192.168.59.139	reconnect.png	上传	通过	

### 日志审计

WEB日志	FTP日志	SAMB A日志	摆渡日志	同步日志	病毒查杀日志	操作日志	
当前记录总数: 130 ( 121 - 130 )							
ID	时间	用户名	用户IP	文件名	传输方向	处理方式	备注
130	2020-06-12 07:13:51	user	192.168.59.139	/transfer/12/1.rar	上传	通过	
129	2020-06-12 07:07:01	user	192.168.59.139	/transfer/123/1.rar	上传	通过	
128	2020-06-12 07:04:09	user	192.168.59.139	/transfer/123/test压缩.rar	下载	通过	
127	2020-06-12 07:02:13	user	192.168.59.139	/transfer/123/test压缩.rar	下载	通过	
126	2020-06-12 07:01:22	user	192.168.59.139	/transfer/123/test压缩.rar	下载	通过	
125	2020-06-12 07:01:12	user	192.168.59.139	/transfer/123/test压缩.rar	上传	通过	
124	2020-06-12 06:58:40	user	192.168.59.139	/diskmap/321/test压缩.rar	下载	通过	
123	2020-06-12 06:58:20	user	192.168.59.139	/diskmap/321/行为管理快速安装手册.pdf	上传	阻止	
122	2020-06-12 06:57:55	user	192.168.59.139	/diskmap/321/test压缩zip	上传	阻止	
121	2020-06-12 06:55:24	user	192.168.59.139	/diskmap/321/test压缩zip	上传	阻止	

## 日志审计

WEB日志	FTP日志	SAMBA日志	摆渡日志	同步日志	病毒查杀日志	操作日志	
当前记录总数: 361 (352 - 361)							
ID	时间	用户名	用户IP	文件名	传输方向	处理方式	备注
361	2020-07-17 14:14:58	user	192.168.59.186	transfer/123/培训.mp4	下载	通过	
360	2020-07-17 14:14:57	user	192.168.59.186	transfer/123/培训.mp4	下载	通过	
359	2020-07-17 14:14:15	user	192.168.59.186	transfer/123/培训.mp4	上传	通过	
358	2020-07-06 09:45:06	user	192.168.59.188	diskmap/test/1C3819F8.mxf	上传	通过	
357	2020-07-06 09:44:23	user	192.168.59.188	diskmap/test/5E56A973.mxf	上传	通过	
356	2020-07-06 09:43:56	user	192.168.59.188	diskmap/test/5E56A973.mxf	上传	通过	
355	2020-07-06 09:43:54	user	192.168.59.188	diskmap/test/5E56A973.mxf	上传	通过	
354	2020-07-06 09:43:53	user	192.168.59.188	diskmap/test/5E56A973.mxf	上传	通过	
353	2020-06-12 07:34:16	user	192.168.59.188	diskmap/321/2.m4a	上传	通过	
352	2020-06-12 07:34:15	user	192.168.59.188	diskmap/321/2.m4a	上传	通过	

## 日志审计

WEB日志	FTP日志	SAMBA日志	摆渡日志	同步日志	病毒查杀日志	操作日志			
当前记录总数: 7 (1 - 7)									
ID	时间	摆渡名	服务器IP	文件路径	文件名	传输方式	处理方式	传输用时	备注
7	2020-07-17 14:15:36	123	192.168.59.186	123	培训.mp4	samba	成功	63	传输完成
6	2020-06-12 07:13:52	12	192.168.59.188	12	1.rar	samba	成功	0	传输完成
5	2019-11-04 10:36:05	zkww	192.168.0.100	zkww	9g.jpg	samba	保留	0	可疑文件, 文件类型与后缀名不匹配
4	2019-11-04 10:36:05	zkww	192.168.0.100	zkww	9999m.jpg	samba	保留	0	可疑文件, 文件类型与后缀名不匹配
3	2019-11-04 06:32:43	zkww	192.168.0.100	zkww	2019529.mp4	samba	成功	113	传输完成
2	2019-11-04 06:31:10	zkww	192.168.0.100	zkww	201912114.mp4	samba	成功	87	传输完成
1	2019-11-04 06:28:53	zkww	192.168.0.100	zkww	2节98目调色系统 67演示.mpg	samba	成功	15	传输完成

## 五、FTP 客户端使用说明

常用的 ftp 客户端例如 filezilla 等，filezilla 是一款免费开源的 ftp 客户端软件，其客户端可以运行在 windows、mac、linux 等平台。

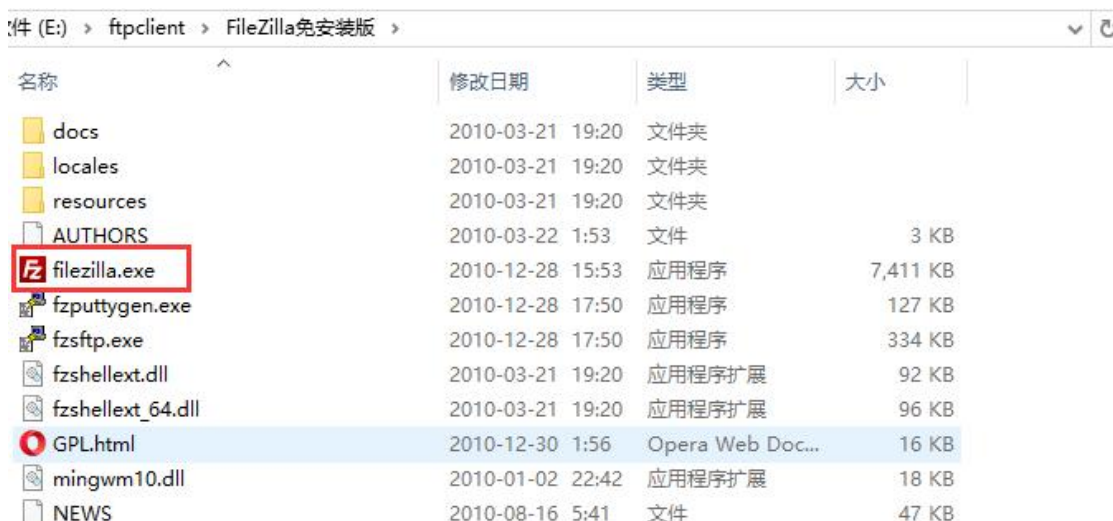
### 5.1、下载

登录设备后，点击右上角的“工具”即可下载 FileZilla Client 软件免安装绿色版。

或者点击 ANYSEC 官网下载链接：<http://www.anysec.com/upload/soft/ftp.exe>

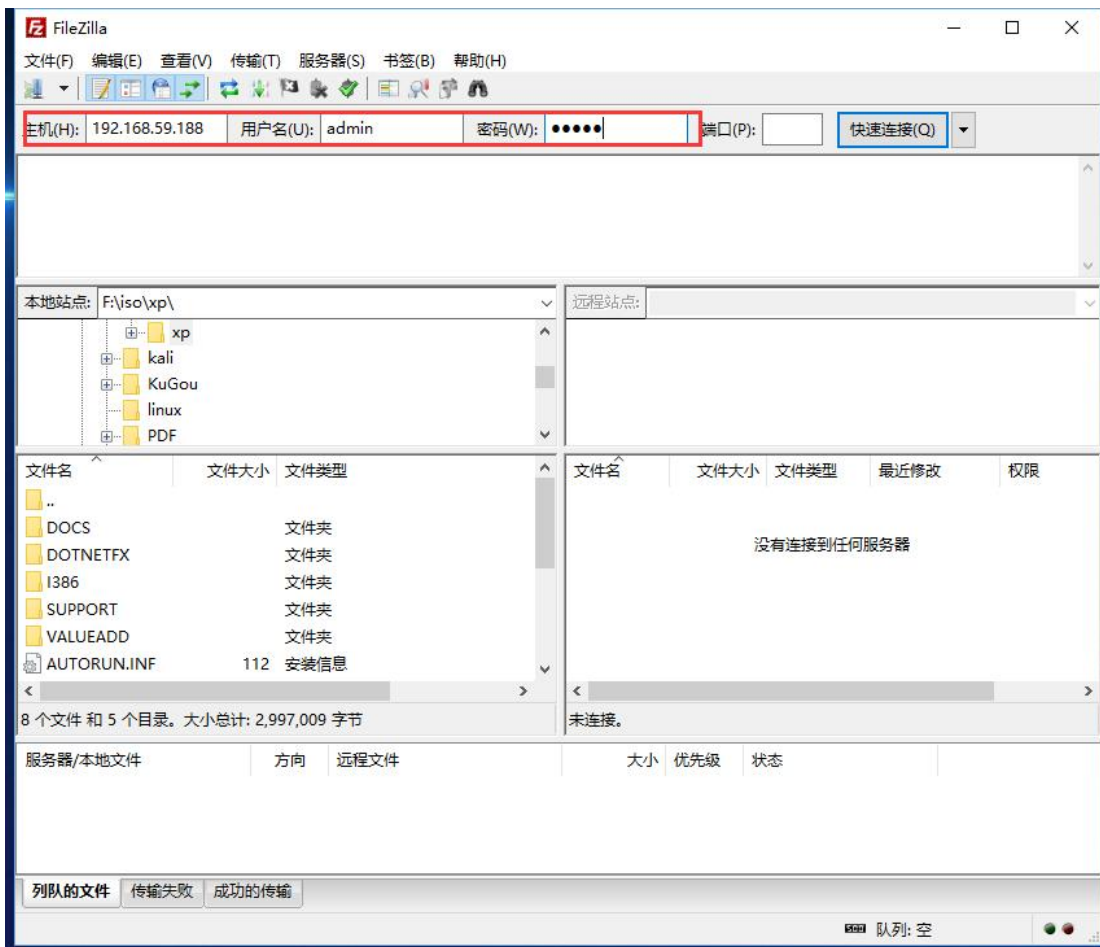
### 5.2、安装

将下载好的 ftp 客户端软件打开进行安装或解压，然后运行



名称	修改日期	类型	大小
docs	2010-03-21 19:20	文件夹	
locales	2010-03-21 19:20	文件夹	
resources	2010-03-21 19:20	文件夹	
AUTHORS	2010-03-22 1:53	文件	3 KB
<b>filezilla.exe</b>	2010-12-28 15:53	应用程序	7,411 KB
fzputtygen.exe	2010-12-28 17:50	应用程序	127 KB
fzsftp.exe	2010-12-28 17:50	应用程序	334 KB
fzshellext.dll	2010-03-21 19:20	应用程序扩展	92 KB
fzshellext_64.dll	2010-03-21 19:20	应用程序扩展	96 KB
GPL.html	2010-12-30 1:56	Opera Web Doc...	16 KB
mingwm10.dll	2010-01-02 22:42	应用程序扩展	18 KB
NEWS	2010-08-16 5:41	文件	47 KB

### 5.3、用 ftp 软件登录文件安全网关

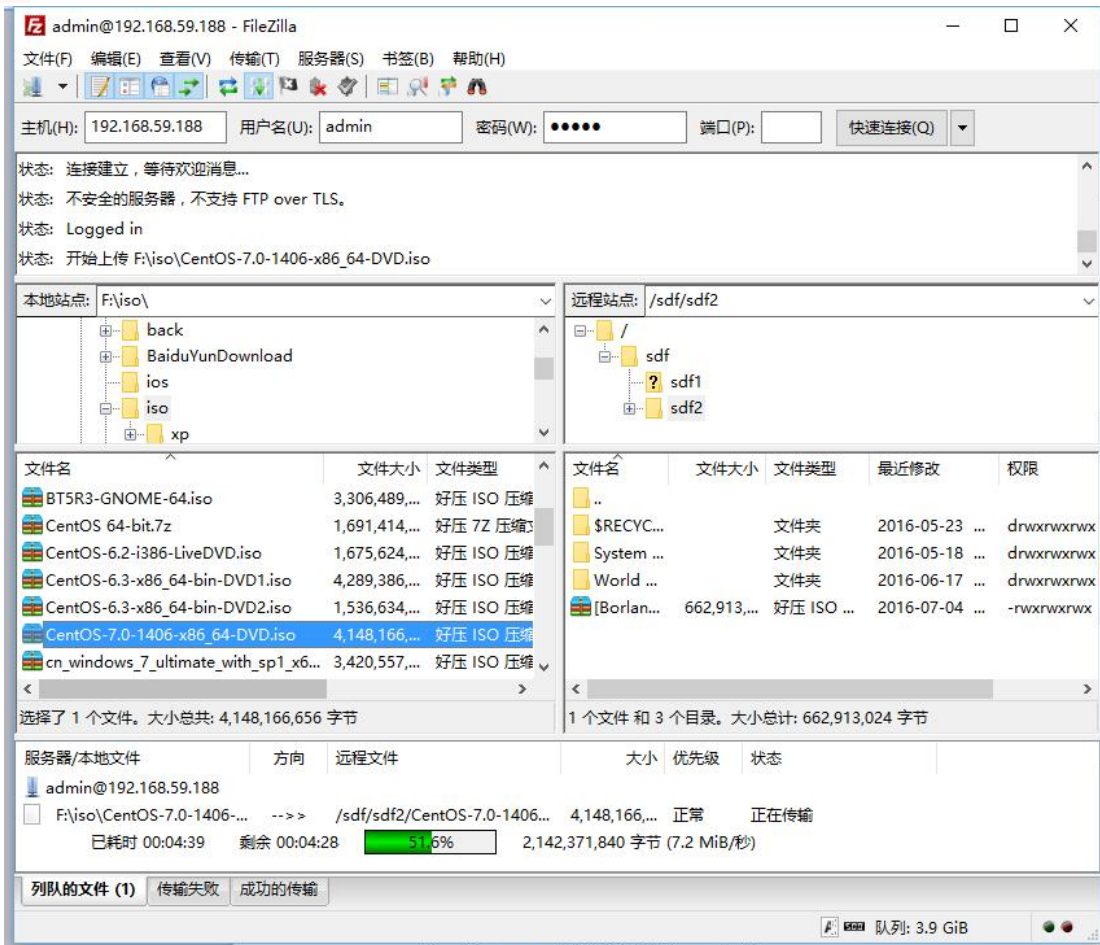


主机：文件安全网关的 IP 地址

用户名：文件安全网关中添加的用户，默认用户密码为 admin/admin

密码：文件安全网关中相对应用户的密码。

输入好以上三项后，点快速连接即可访问文件安全网关。



右边为远程站点：指的是连接文件安全网关的移动存储设备。

左边为本地站点：指的是本地计算机的存储空间。

例如：需要将本地计算机的文件拷贝到连接文件安全网关的移动存储时，直接将左边的文件拖曳到右边即可。

## 六、常见问题处理

本手册介绍设备在使用过程中可能遇到的问题和解决方法。

### 6.1、输入正确的网络地址（IP）无法访问？

解决方法：检查设备网线接口是否松动或者脱落，如果以上没有问题，请网络管理员检查访问者的 PC 是否和设备在同一网段。

### 6.2、 Web 界面显示紊乱，按钮无法点击？

解决办法：使用推荐的浏览器进行管理。

### 6.3、进入主界面无任何文件列表显示？

解决办法：插入外部存储设备或者 U 盘，请管理员进入“设置”查看“文件管理”设置，然后检查外部存储设备里面是否存在允许通过过滤的文件。

### 6.4、进入 ftp 客户端发现文字乱码

解决办法：进入 ftp 客户端配置，修改为 utf8 格式。





### 6.5、ftp 客户端不能下载某文件，错误是 553 服务器未知错误

解决办法：首先该文件可能有问题，不能通过过滤，可以通过浏览器访问“文件管理”中未通过文件日志查看该文件不能通过过滤原因。第二种可能是该种后缀不允许通过，关闭 ftp 客户端连接，浏览器进入“配置”->“文件管理”，确认该后缀需要进行下载，以及该后缀已经打勾或者在自定义后缀中并打勾。确认后重新打开 ftp 客户端连接再行下载。

### 6.6、ftp 客户端不能上传某文件，错误是 550 不能存

解决办法：关闭 ftp 客户端连接，用可写用户进入 ftp 客户端即可

## 七、结束语

如果您在使用过程中遇到问题，请参考本手册或及时联系深圳市中科网威科技有限公司的售后技术支持，协助您解决问题。

再次感谢您使用本产品。

手册内容及产品规格如有变更，恕不另行通知。

地址：深圳市龙华区观澜街道观光路 1301-80 号电子科技大学(深圳)高等研究院 3 号楼 1401

电话：0755-83658009

传真：0755-83656609 (FAX)

网址：www.anysec.com

技术热线：0755-83658229

24 小时值班手机：13510693536