[原创/转发] 标题 *//必有项。如果是原创，请在标题前加上字符串“[原创]”，如果是转发网上的文档，请在标题前加上字符串“[转发]”。居中排版*

单位 作者 *//必有项。多个不同单位作者可以多行。居中排版*

发布日期 *//必有项yyyymmdd，也起版本号作用。修改了文档内容后请修改此项。居中排版*

正文 *//必有项*

[参考文献] *//可有项。如果有参考文献，请在此列明。*

[原文网址] *//可有项。如果文档全文是转载网上的，必须在此注明。*

示例：

[原创]web服务器iptables防火墙设置

山东大学信息化工作办公室 陈军

20170408

用CentOs6.6自带的apache作web服务器，用iptables设置主机防火墙。防火墙规则如下：

1. TCP 80端口完全开放，允许ping本服务器。
2. 仅允许信息办办公网段192.168.100.0通过ssh访问本服务器。
3. 允许本服务器向外发送dns解析请求，允许本服务器向外发送时间同步请求。

通过shell脚本设置上述防火墙规则。firewall.sh代码如下：

#!/bin/bash

# Set firewall rules

DST="192.168.1.1"

# iptables rules:

iptables -P INPUT ACCEPT

iptables -F

iptables -A INPUT -i lo -j ACCEPT

iptables -A INPUT -p icmp --icmp-type echo-reply -j ACCEPT

iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT

iptables -A INPUT -s 192.168.100.0/24 –dport 22 -d $DST -j ACCEPT

iptables -A INPUT -p tcp --dport 80 -d $DST -j ACCEPT

# allow this host to visit other sever(dns,ntp) as client.

iptables -A INPUT -p tcp --sport 53 -j ACCEPT

iptables -A INPUT -p udp --sport 53 -j ACCEPT

iptables -A INPUT -p udp --sport 123 -j ACCEPT

iptables -P INPUT DROP

iptables -P FORWARD DROP

iptables -P OUTPUT ACCEPT

设置脚本可执行：

Chmod 755 firewall.sh //在fireall.sh脚本所在文件夹执行