

如何在linux中设置透明代理 PDF转换可能丢失图片或格式，
建议阅读原文

https://www.100test.com/kao_ti2020/145/2021_2022__E5_A6_82_E4_BD_95_E5_9C_A8I_c103_145272.htm

1.什么是透明代理？来源：www.examda.com 如果你问：我如何才能使得用户的浏览器不需要任何代理设置就能使用我的Squid cache代理服务器

上网？，此时你就需要使用透明代理。透明代理让你的客户端不需设置任何代理，当包经过透明代理服务器时实际上被重定向到squid代理服务器的代理端口（如8080），即由本地代理服务器向外请求所需数据然后拷贝给客户端。2.我需要什么样的环境才能实现透明代理？来源：www.examda.com

a.客户端的windows PC的网关必须设成Squid代理服务器，因为既然你的browser中没有任何代理设置,你要访问某个站点时，包必须经过squid代理服务器才能被重定向，故这是最基本的条件。b.客户端必须正确设置DNS服务器。因为既然现在不用设置任何代理。则DNS必须由browser来解析，也就是要由客户端的PC中TCP/IP中设置的DNS服务器来正确解析出某个站点的IP地址来c.服务器端可以安装squid代理服务器，1.x

or 2.x版本均可。3.配置Squid代理，启动透明代理功能Squid-2

加下面的行到你的/etc/squid/squid.conf中http_port

8080httpd_accel_host virtualhttpd_accel_port

80httpd_accel_with_proxy onhttpd_accel_uses_host_header

onSquid-1.1加下面的行到/etc/squid.confhttp_port

8080httpd_accel virtual 80httpd_accel_with_proxy

onhttpd_accel_uses_host_header on4. 重新启动squid. 用下面的命令：

#!/usr/sbin/squid -k reconfigure如提示内核不支持透明代理

。则需要重新编译内核，enable 透明代理的支持。下面是你需要启动的内核项目：[*] Network firewalls[] Socket Filtering[*] Unix domain sockets[*] TCP/IP networking[] IP: multicasting[] IP: advanced router[] IP: kernel level autoconfiguration[*] IP: firewalling[] IP: firewall packet netlink device[*] IP: always defragment (required for masquerading)[*] IP: transparent proxy support

5. 下面的命令针对linux 2.2.x内核：# Accept all on lookback/sbin/ipchains -A input -j ACCEPT -i lo# Accept my own IP, to prevent loops (repeat for each interface/alias)/sbin/ipchains -A input -j ACCEPT -p tcp -d 192.168.11.1/32 80# Send all traffic destined to port 80 to Squid on port 80/sbin/ipchains -A input -j REDIRECT 8080 -p tcp -s 192.168.11.0/24 -d 0/0 80

下面的命令针对linux 2.0.x内核：# Accept all on loopback ipfwadm -I -a accept -W lo# Accept my own IP, to prevent loops (repeat for each interface/alias) ipfwadm -I -a accept -P tcp -D 192.168.11.1/32 80# Send all traffic destined to port 80 to Squid on port 3128 ipfwadm -I -a accept -P tcp -S 192.168.11.0/24 -D 0/0 80 -r 8080

6. 应注意的问题：a. 这种透明代理只能针对http协议，不能针对FTP协议来源：www.examda.com b. PC的默认网关应设成squid 代理服务器c. 防火墙重定向规则在其它的input规则的前面，注意顺序。如：/etc/rc.d/rc.firewall:#!/bin/sh# rc.firewall linux kernel firewalling rulesFW=/sbin/ipfwadm# Flush rules, for testing purposesfor i in I O F # A # If we enabled accounting to do \${FW} - \$i -f done# Default policies:\${FW} -I -p rej # Incoming policy: reject (quick error) \${FW} -O -p acc # Output policy: accept \${FW} -F -p den #

Forwarding policy: deny# Input Rules:# Loopback-interface (local access, eg, to local nameserver):
`{FW} -I -a acc -S localhost/32 -D localhost/32`
 # Local Ethernet-interface:# Redirect to Squid proxy server:
`{FW} -I -a acc -P tcp -D default/0 80 -r 8080`
 # Accept packets from local network:
`{FW} -I -a acc -P all -S localnet/8 -D default/0 -W eth0`
 # Only required for other types of traffic (FTP, Telnet):
 # Forward localnet with masquerading (udp and tcp, no icmp!):
`{FW} -F -a m -P tcp -S localnet/8 -D default/0`
`{FW} -F -a m -P udp -S localnet/8 -D default/0`
 Here all traffic from the local LAN with any destination gets redirected to the local port 8080. Rules can be viewed like this:
 IP firewall input rules, default policy:

reject	type	prot	source	destination	ports	acc
	all	127.0.0.1	127.0.0.1			
n/a	acc/r	tcp	10.0.0.0/8	0.0.0.0/0	*	-> 80 => 8080
	acc	all	10.0.0.0/8	0.0.0.0/0		
n/a	acc	tcp	0.0.0.0/0	0.0.0.0/0	*	-> * 100

 Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com