

原创

一个不是程序员员的程序猿

于 2022-11-11 16:29:45 发布

328

收藏 2

版权

分类专栏:

网络安全

文章标签:

网络

服务器

代理模式

网络安全

专栏收录该内容

0 订阅

2 篇文章

订阅专栏

引言

SOCKS全称是SOCKet Secure，是一种网络传输协议，主要用于客户端与外网服务器之间通讯的中间传递。在OSI模型中，SOCKS是会话层的协议，位于表示层与传输层之间，最新协议是SOCKS5。

正文

一、SOCKS5原理

- ①首先客户端向代理服务器发出请求信息，用以协商版本和认证方法。随后代理服务器应答，将选择的方法发送给客户端。
- ②客户端和代理服务器进入由选定认证方法所决定的子协商过程，子协商过程结束后，客户端发送请求信息，其中包含目标服务器的IP地址和端口。代理服务器验证客户端身份，通过后会与目标服务器连接，目标服务器经过代理服务器向客户端返回状态响应。
- ③连接完成后，代理服务器开始作为中转站中转数据。

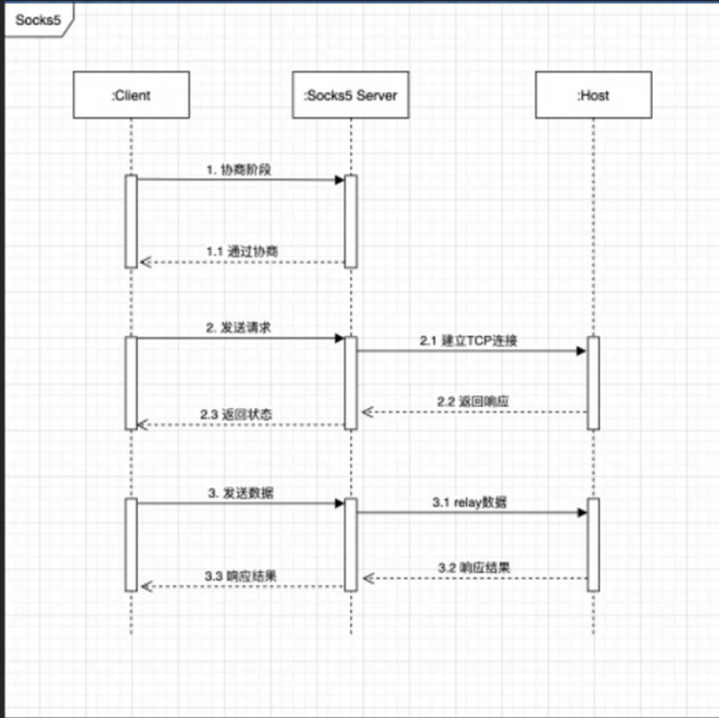


图 1 SOCKS5原理

二、SOCKS5 协议交互具体过程

2.1 认证

①客户端向代理服务器发送代理请求，其中包含了代理的版本和认证方式：

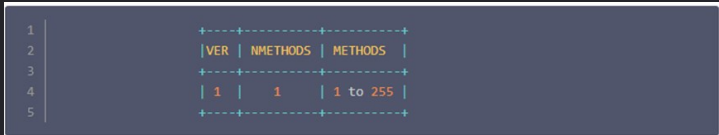


图 2

VER（1字节）：版本号,固定为0x05,代表使用SOCKS5协议

NMETHODS（1字节）：方法数目，表示后面的方法编号列表（METHODS字段）中有多少种客户端支持的认证方法

METHOD（1-255字节）：方法编号列表，存储客户端支持的认证方法的编号

②代理服务器从给定的方法编号列表中选择一个方法并返回选择报文

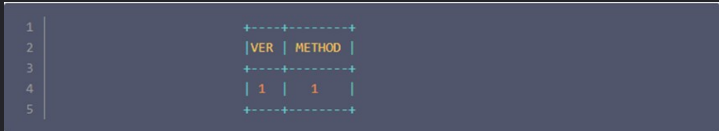


图 3

METHOD字段用来返回选择的方法编号

支持的认证方式有：

0x00: 不需要认证

0x01: GSSAPI认证

0x02: 用户名和密码方式认证

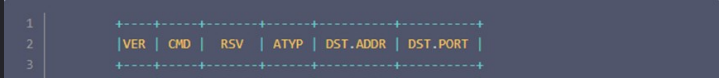
0x03: IANA认证

0x80-0xfe: 保留的认证方式

0xff: 不支持任何认证方式，当客户端收到此信息必须关闭连接。

2.2请求

①协商完成后，客户端就可以向代理服务器发送代理请求，客户端会向代理服务器发送下面格式的请求



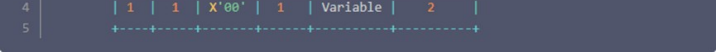


图 4

CMD:指令编号,0x01 CONNECT 指令,用于 TCP 代理

0x02 BIND 指令,一般用于要客户端主动接受来自服务器连接时

0x03 UDP ASSOCIATE 指令,用于 UDP 代理

RSV:保留字段:必须为 0

ATYP:地址类型: 0x01 表明地址为 (DST.ADDR字段) IPv4 地址,长度为4字节

0x03域名,表明地址为域名,第一个字节用作域名的长度标识

0x04 表明地址为IPv6 地址,长度为16字节

DST.ADDR:目标地址:要访问的目标服务器的地址或域名,类型由ATYP字段决定

DST.PORT:目标端口号:于目标地址对应的端口号。

②SOCKS 服务端会根据请求类型和源、目标地址,执行对应操作,并且返回对应的一个或多个报文信息,格式如下:

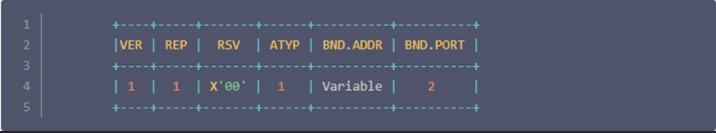


图 5

REP:请求的结果,0x00 成功

0x01常规 SOCKS 服务故障

0x02 规则不允许的连接

0x03 网络不可达

0x04 主机无法访问

0x05 拒绝连接

0x06 连接超时

0x07 不支持的命令

0x08 不支持的地址类型

RSV:保留字段:必须为 0

ATYP:地址类型

BND.ADDR:绑定地址:即请求成功后客户端需要连接的代理服务器的地址或域名,客户端之后的通信均通过改地址对应的服务器

BND.PORT:绑定端口号:绑定地址对应的端口号

2.3 通信

当代理服务器返回成功消息,则后续客户端通过绑定地址和绑定端口号与代理服务器通信,由代理服务器转发客户端的请求到目标服务器,并将目标服务器的响应转发给客户端。

三. SOCKS5的特点

1.SOCKS5相比于SOCKS4,加入了UDP协议支持,在框架上加入了**强认证功能**,并且地址信息也加入了**域名和IPv6**的支持。

1. SOCKS5服务器在将通讯请求发送给真正服务器的过程中,对于请求数据包本身**不添加任何改变**,只是传递数据包,而不关心是何种应用协议,所以SOCKS代理服务器比应用层代理服务器**更快**。

3.与VPN(虚拟专用网络)相比,SOCKS5可以**代理应用层的某些应用**,而不是代理全局网络,而VPN控制的是你电脑的整个网络,只要需要连接到互联网的流量都会经过VPN。

四. SOCKS5的应用场景

SOCKS5目前常被用于访问被**GFW屏蔽的网络内容**,以及作为代理服务器**为用户提供不同位置的IP**,帮助用户**隐藏真实IP**访问一些可能存在安全隐患的网络内容。

下面以SOCKS5应用于访问GFW阻断的内容为例,描述SOCKS5的主要应用场景。

GFW全称是Great Firewall,官方名称为数据跨境安全网关,阻断不符合中国政府要求的互联网内容传输。

如图6,假设没有GFW,正常访问谷歌,①需要向DNS服务器发送谷歌的域名,之后②DNS服务器解析域名之后,向电脑发送回google的IP。③电脑通过IP访问google,④google向电脑传回数据。



图 6

把这个过程比作写信,有了GFW之后,你的信件会被GFW所审查,当被审查出信件中的内容是不符合要求的时候时,GFW会返回给你一个错误的IP地址,因此再无法访问到google这是GFW主要的阻断方法之一: **DNS域名污染**。初次之外,GFW还有多种方式进行阻断:直接舍弃数据包、IP地址或传输层端口封锁、TCP连接重置等等。

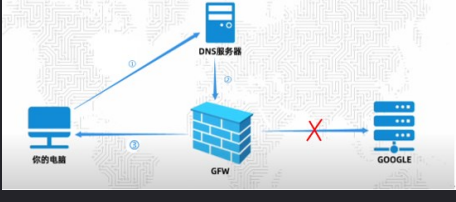


图 7

如图8,目前基于SOCKS5的代理软件,会先在本地(SS Local)对数据进行加密处理,再通过GFW,由于数据进行了加密,所以GFW无法得知内容,也就不能确定阻断,因此数据可以通过GFW,随后到达境外服务器(SS Server),经过解密,发送数据请求到google等网站,

用户便可以访问。

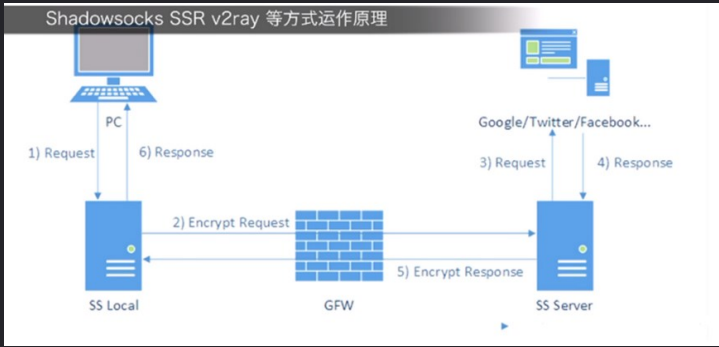


图 8

而对比图9，使用VPN访问GFW阻断的内容，VPN在客户端和VPN服务器之间先发送一个建立加密通道的明文数据包，GFW看到是VPN服务器，则不会进行阻断。加密通道建立后，客户端便可以通过VPN服务器来访问google等网站。但这种方式由于会在开始发送明文数据包，所以时间一长，特征非常明显，会经常被GFW所阻断。所以SOCKS5协议的优势是非常明显的。



图 9

参考文献

- [1] Wikipedia. SOCKS[E]. <https://zh.m.wikipedia.org/zh-hans/SOCKS#SOCK5>
- [2] M. Leech. Username/Password Authentication for SOCKS V5[E]. <https://datatracker.ietf.org/doc/pdf/rfc1929.pdf>. 1996.3
- [3] M. Leech, M. Ganis, Y. Lee. SOCKS Protocol Version 5. <https://datatracker.ietf.org/doc/pdf/rfc1928.pdf>. 1996.3

内网渗透之Socks代理简介	墨鱼菜鸡	148
目录 Socks代理简介 01什么是Socks 02什么是Socks代理 Socks代理工具简介 01EarthWorm 02FRP 03ProxyChains 04other Socks代理简介 01什么是S...		
手把手教你建立sock5代理服务器		12-22
文档非常详细的介绍了sock5服务器的搭建过程，并对搭建过程中的细节进行了详细说明		
什么是SOCKS5协议_dianbalao8154的博客		1-9
Socks5代理服务器则是把你的网络数据请求通过一条连接你和代理服务服务器之间的通道,由服务器转发到目的地。你没有加入任何新的网络,只是http/socks数...		
socks5 代理服务服务器项目_一条傻傻的二哈的博客		1-16
class SockServer { public: SockServer(int port) : EpollServer(port) {} //安全认证和建立连接 int AuthHandle(int fd); int Establishm...		
go get 使用 proxy 最新发布	云满笔记	238
在使用 grafcp 过程中出现了 HTTPS 无法握手的现象。polipo 虽然旧, 而且不再维护了, 但确是一种非常可靠隐妥的工具。用 C 语言编写的代理程序, 通过...		
java 抓包_关于抓包的碎碎念	weixin_39712705的博客	460
本文为看雪论坛优秀文章看雪论坛作者ID: ChenSem抓包是作为apk分析的首要切入点，获取apk的通信协议的必要手段。常见的抓包手段是基于中间人攻...		
socks5代理服务器-SOCKS5篇_wx19866222的博客		1-13
sock5代理服务器-SOCKS5篇(2008-07-05 07:41) 分类:Proxy 1.安装SOCKS5 # tar -zxvf socks5-v1.0r11.tar.gz # cd socks5-v1.0r11 # patch -p0 < socks-...		
sock5代理工作原理_头像好看吗的博客		1-6
sock5支持UDP和TCP,但两种代理是有区别的,以下分类说明 如何用代理TCP协议 1. 向服务器的1080端口建立tcp连接。 2. 向服务器发送 05 01 00 (此为...		
sock5基础	西凉刀客	1万+
什么是socks5 socks是'SocketS'的缩写，因此socks5也叫sockets5。 socks是一种网络传输协议，主要用于客户端与外网服务器之间通讯的中间传递。根...		
sock5简单理解	qq_45300786的博客	2233
通俗来说，可以用DNS服务器来理解 A主机上安装sock, 然后在相应的配置文件里设置本地ip和端口，或者其他sock服务器的p和端口 以后你的一切请...		
SOCKS5协议	HK_server的博客	723
SOCKS5 是一种代理协议，充当前端机器和服务端机器之间的中介。它使用TCP/IP协议进行通信，使内网的前端机器可以访问Internet网络中的服务器，...		
Socks5工作原理与搭建	CZD__CZD的博客	7807
Socks5协议是一款广泛使用的代理协议，它在使用TCP/IP协议通讯的客户端和服务端之间扮演一个中介角色，使得内部网中的客户端能够访问Interne...		
socks5代理服务协议的说明 向连接	liujay2的专栏	3万+
socks5 socks5代理和socks4 socks4a比，多了一个验证功能和udp代理的功能。 socks5的tcp代理几乎和socks4 socks4a一样简单，但是udp却比较复杂...		
socket 5协议详解	qq_36963214的博客	2904
认证 首先客户端向服务端发送认证信息，结构如下 +-----+ VER METHODS METHODS +-----+ 1 1 1 1 to 255 ...		
socks5协议详细说明	小野(xpc)	1506
由浅入深带大家详细了解socks5协议。 首先会对socks协议进行简单介绍 然后介绍它的工作工程 最后介绍协议的细节		
SOCKS5	QQ1289671197的博客	690
SOCKS5发展及现状：网络发展到今天，SOCKS5也历经了几次大的修改。 现在SOCKS5通过特殊方法，可以实现以下功能： 1.局部指定进程使用SOCK...		
SOCKS5代理的特性和测试教程	hhhhhyyyyy1的博客	1141
一：Socks5的特性：Socks5是一种代理，也就是先所有的交互数据都先经过另一台主机（网卡），这个过程中用户访问其他网络都是使用的代理服务...		
SOCKS5中的UDP穿透	whatday的专栏	2万+
socket5是一种代理协议，如果防火墙禁止所有的计算机发送udp包，代理也没用。 http tunnel是在防火墙禁止了udp的数据包，可以把数据封装在http包...		
socks5代理工作流程和原理	好记性不如烂笔头	2607
一、socks5协议 socks5协议是一款广泛使用的代理协议，它在使用TCP/IP协议通讯的前端机器和服务端机器之间扮演一个中介角色，使得内部网中的前...		
Socks5协议详解	suffengdeshtou的博客	1万+
Socks5协议详解 由于项目需求，最近需要了解一些代理的知识，因此看了一下sock5协议。主要还是RFC1928,也参考了网上的一些翻译。 防火墙的使用，...		
SOCKS 5协议详解	legion8169的专栏	3136
SOCKS 5协议详解 笔者在实际学习中，由于在有些软件用到了socks5(如Icicq,icq等)，对其原理不甚了解，相信很多朋友对其也不是很了解，于...		
SOCKS5代理	KwokY的博客	5429
SOCKS协议 SOCKS：防火墙安全会话转换协议 (Socks: Protocol for sessions traversal across firewall securely) SOCKS协议提供一个框架，为在 TC...		
sock5	weixin_33985507的博客	137
SOCKS5 是一个代理协议，它在使用TCP/IP协议通讯的前端机器和服务端机器之间扮演一个中介角色，使得内部网中的前端机器变得能够访问Internet网...		

“相关推荐”对你有帮助？

非常没帮助

没帮助

一般

有帮助

非常有帮助

©2022 CSDN 皮肤主题：鲸 设计师：meimeilei 返回首页

关于我们 招贤纳士 商务合作 寻求报道 400-660-0108 kefu@csdn.net 在线客服 工作时间 8:30-22:00

一个不是程序员的...

关注

1

2

0

专栏目录

一个不是程序员的程序员猿

码龄14年

暂无认证

VIP

14

4万+

7万+

2万+

等级

原创

周排名

总排名

访问

等级

164

33

2

0

16

积分

粉丝

获赞

评论

收藏

私信

关注

热门文章

群晖如何添加第三方源 8967

群晖NAS 升级DSM7.0以后PLEX无法启动的解决方案 4753

(更新) 群晖 DSM 7.0 系统上更新、安装 Plex Media Server 2655

Windows 新增远程桌面会话连接数(可多人同时远程桌面，互不影响) 2246

Transmission 3.0-19 如何升级WebUI套件 (群晖NAS升级DSM7.0以后) 1856

您愿意向朋友推荐“博客详情页”吗？

😞

😐

😐

😐

😐

强烈不推荐

不推荐

一般般

推荐

强烈推荐

最新文章

Wampserver 3.2.6 切换中文报错处理方法

ecshop用户会员必须注册登录以后才可以浏览访问商城网站

ECSHOP开源系统的文件结构

2022年 10篇 2021年 5篇

Beta

🔍

📄

🔍

🔍

🔍