原创 一个不是程序员的程序猿 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。

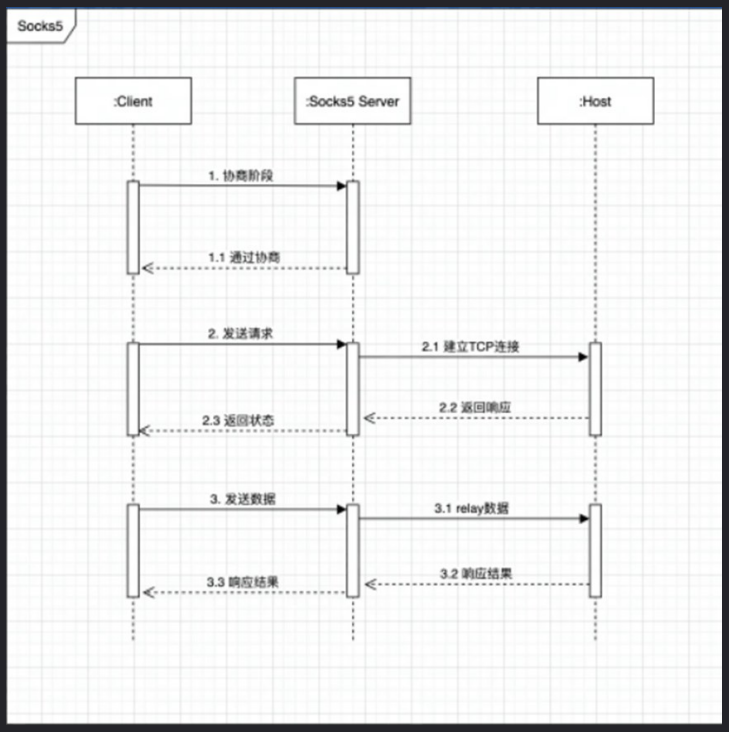

图 1 SOCKS5原理

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：

```
+----+----------+----------+
|VER | NMETHODS | METHODS  |
+----+----------+----------+
| 1  |    1     | 1 to 255 |
+----+----------+----------+
```

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

```
+----+--------+
|VER | METHOD |
+----+--------+
| 1  |   1    |
+----+--------+
```

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

```
+----+-----+-------+------+----------+----------+
|VER | CMD |  RSV  | ATYP | DST.ADDR | DST.PORT |
+----+-----+-------+------+----------+----------+
```

分类专栏

- 群晖NAS 5篇
- WampSever
- Winsows Server 3篇
- Ecshop 4篇
- 网络安全 2篇

```
+----+-----+-------+------+----------+----------+
|VER | REP |  RSV  | ATYP | BND.ADDR | BND.PORT |
+----+-----+-------+------+----------+----------+
| 1  |  1  | X'00' |  1   | Variable |    2     |
+----+-----+-------+------+----------+----------+
```

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：

```
+----+-----+-------+------+----------+----------+
|VER | REP |  RSV  | ATYP | BND.ADDR | BND.PORT |
+----+-----+-------+------+----------+----------+
| 1  |  1  | X'00' |  1   | Variable |    2     |
+----+-----+-------+------+----------+----------+
```

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需要先向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。

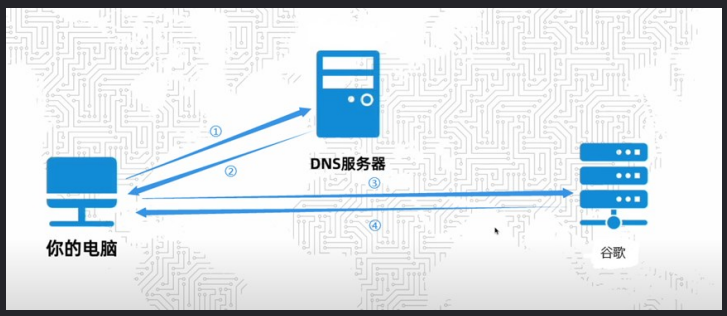

图 6

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。

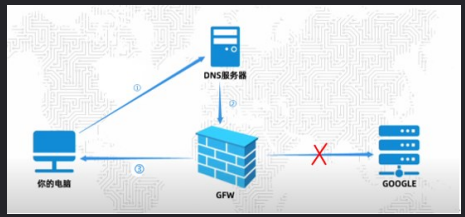

图 7

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。

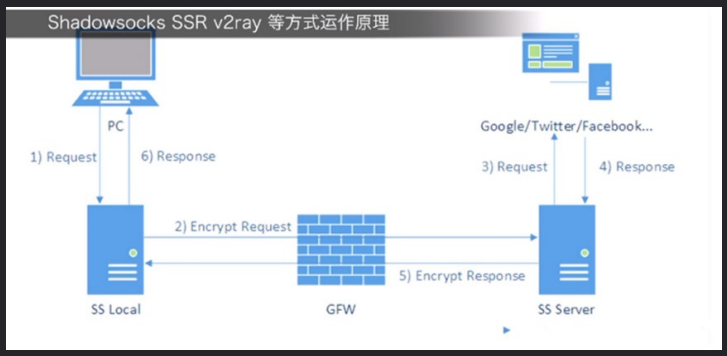

图 8

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。

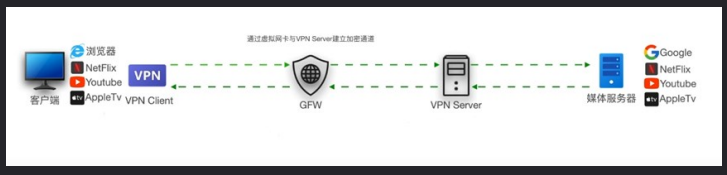

图 9

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