



奇安信

新一代网络安全领军者

上网行为管理行为分析技术



CONTENTS

■ 应用识别技术

■ 内容识别技术

■ 行为阻断技术

■ 旁路干扰技术

■ 策略控制逻辑

■ 其他管控策略

行为主体是指发起上网行为，在网络中产生数据流量包的源，通常指发起人的身份信息，另外结合工具和位置的多维度定义，实现对网络行为更精确的溯源。

行为客体是指上网行为访问的目的对象，如淘宝，京东，王者荣耀，百度，搜狐等。通过对客体数据包特征的预分析和提取，形成对客体的定义，预置在系统中。

准确识别主体、客体是行为管理的基础

定义： 行为客体是指上网行为访问的目的对象，如淘宝，京东，王者荣耀，百度，搜狐等。通过对客体数据包特征的预分析和提取，形成对客体的定义，预置在系统中。

识别： 对于输入流量，由识别模块**对数据包实时特征提取**，通过**匹配内置特征库**，确定该数据包的目的属性，从而实现相应管控需求。

- 输入：数据包
- 输出：mark、URL类别

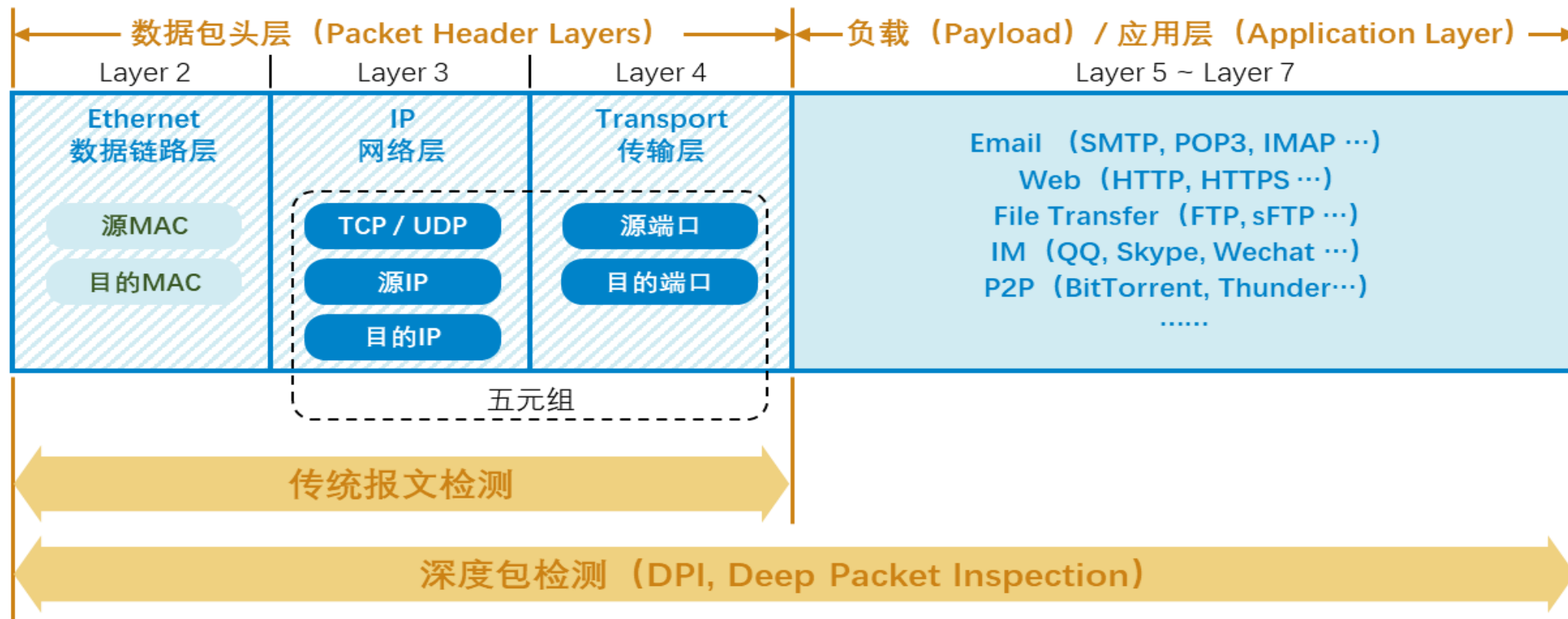
```
GET /passApi/js/uni_login_wrapper.js?cdnversion=1383270362303 HTTP/1.1
Host: passport.baidu.com
Connection: keep-alive
Accept: */*
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, l
Referer: http://www.baidu.com/
Accept-Encoding: gzip,deflate,sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: BAIDUID=477F7C6CB7826DC58AE1D82AC7296511:FG=1; PASSID=fi_aJhVPBPaiSM

HTTP/1.1 200 OK
Content-Type: text/javascript
ETag: "2970232409"
Accept-Ranges: bytes
Last-Modified: Wed, 30 Oct 2013 09:28:17 GMT
Expires: Fri, 01 Nov 2013 01:56:08 GMT
Cache-Control: max-age=600
Vary: Accept-Encoding
Content-Encoding: gzip
```

客体识别的方法-应用协议识别



- **协议识别**：融合了多种应用识别技术，进行最终应用判断和输出的独立功能模块。
 - **端口识别**：基于五元组的识别，应用识别最初所依赖的是端口识别：例如对于网页，识别80端口作为网页的特征，相应的封堵也是依赖于端口。
 - **DPI**：即(Deep Packet Inspection)深度包检测技术，通过检测包中的**特殊字段（或签名）**来判定应用。

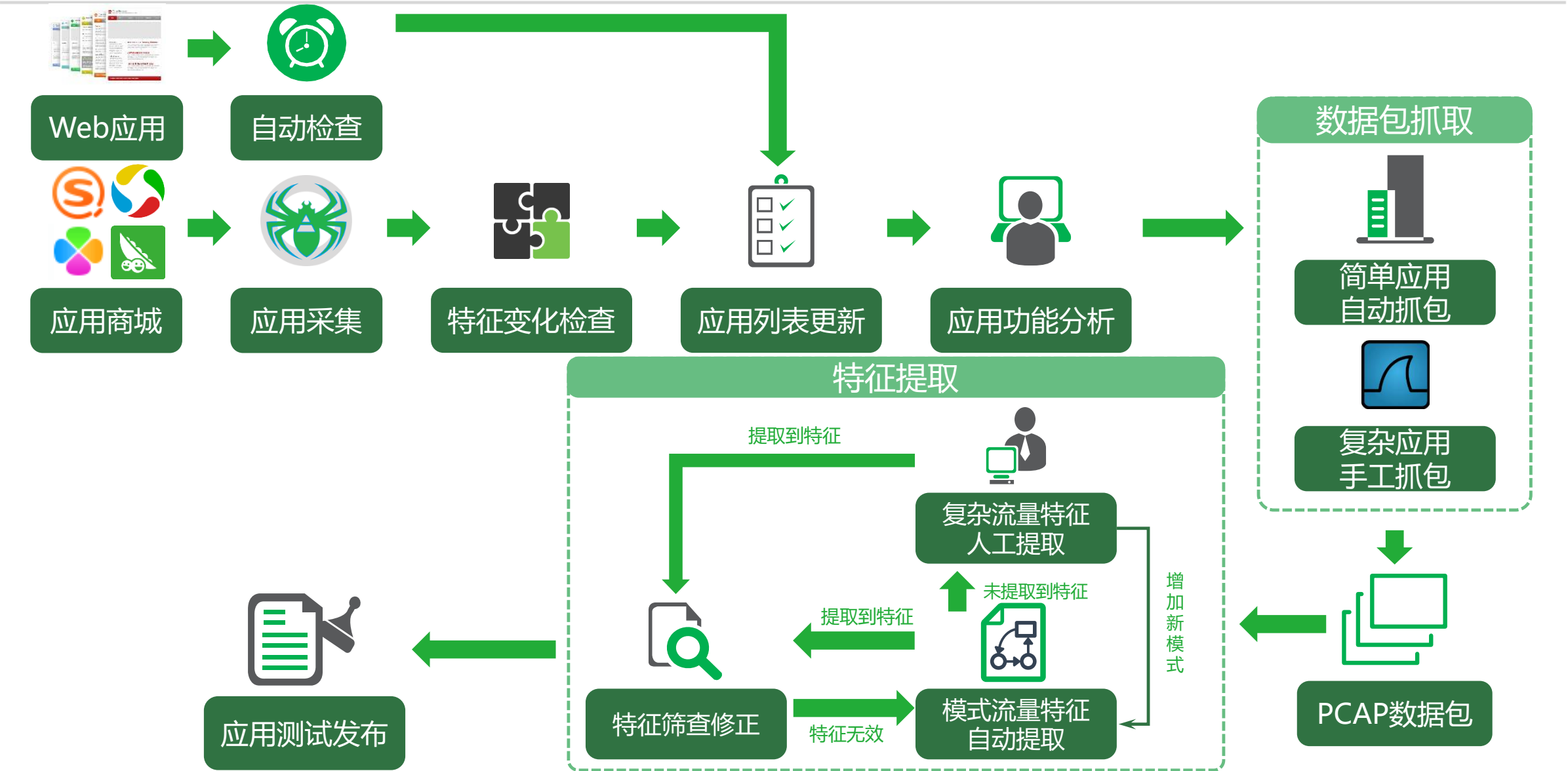


- **DFI:** (Deep/DynamicFlow Inspection, 深度/动态流检测)是通过分析网络数据流量**行为特征**来识别网络应用的。如下图所示:

流量特征	VOIP	P2P
数据包大小	130-220 byte	>1000byte
传输速率	20-90kbit/s	较高, 视带宽而定
连接持续时间	较长	较长
连接目标地址	单一目标地址	多个目标地址
所用协议	主要是 UDP	主要是 TCP

- **XAI** (extensive application inspection) : 拓展应用识别技术, 实现跨包、跨链接、跨应用的全面识别技术。
- 可以识别子应用, 比如QQ, DPI只知道在用QQ; 但XAI可以知道, 是在用QQ聊天, 还是在用QQ传文件。
- **XAI**识别包括了应用识别、应用元信息分析识别、拓扑识别、用户识别。

应用协议库生成流程

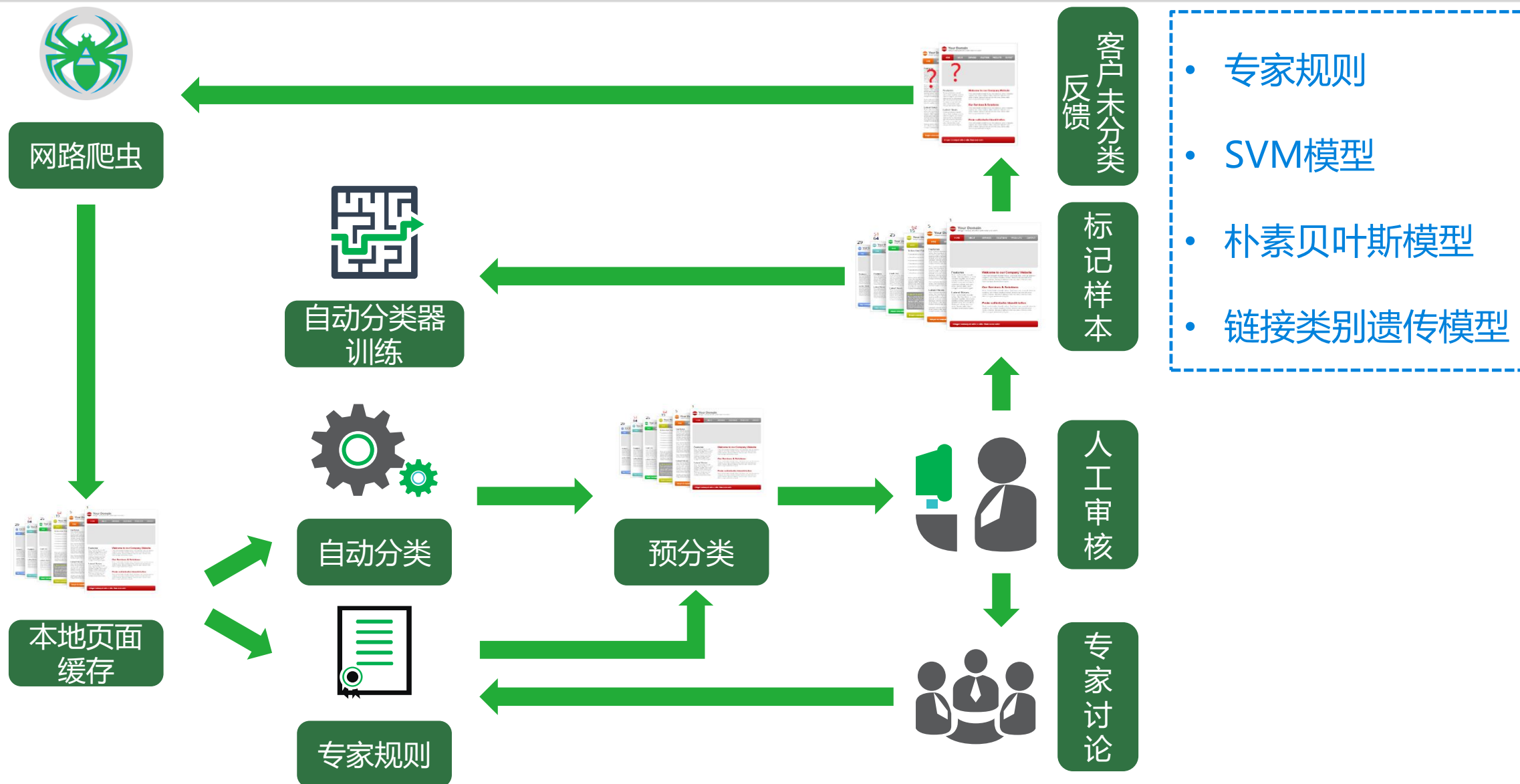




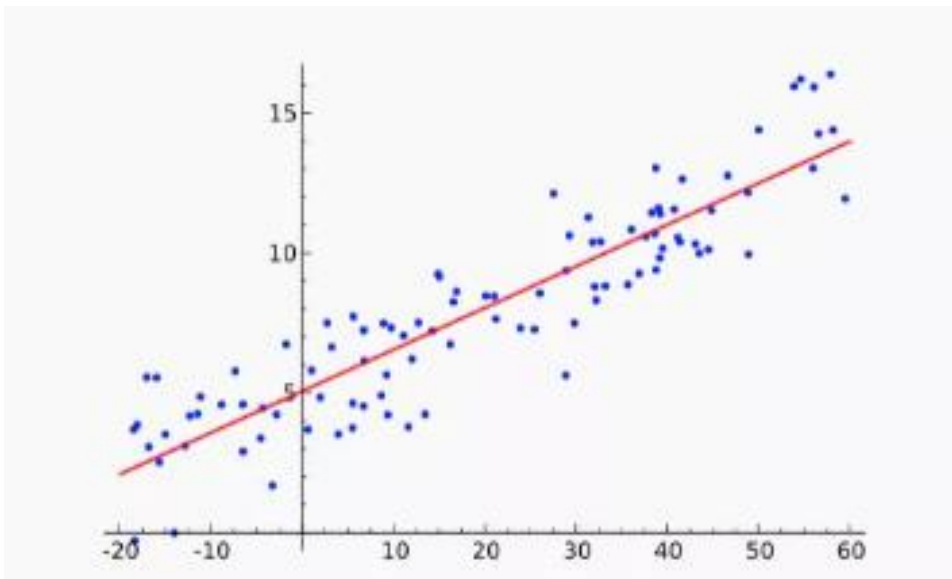
CONTENTS

- 应用识别技术
- 内容识别技术
- 行为阻断技术
- 旁路干扰技术
- 策略控制逻辑
- 其他管控策略

URL库生产流程



- 是一种统计学上分析数据的方法，目的在于了解两个或多个变量间是否相关、相关方向与强度
- 并建立数学模型以便观察特定变量来预测研究者感兴趣的变量
- 更具体的来说，回归分析可以帮助人们了解在只有一个自变量变化时因变量的变化量
- 一般来说，通过回归分析我们可以由给出的自变量估计因变量的条件期望



在安全领域，有一种思想是利用滑动时间窗口方法将各个离散时间监测点的网络安全态势值构造成部分线性相关的多元回归数据序列,以其做为样本集输入到改进广义回归神经网络加以训练,进而得到网络安全态势预测模型，实现网络安全态势预测的功能。

- **正则表达式**，又称规则表达式。(英语:Regular Expression，在代码中常简写为regex、regexp或RE)。
- 常用来检查一个字符串中是否包含某种子串，将匹配的子串替换，或者从某个串中取出符合某个条件的子串。
- 正则表达式由以下组成：由普通字符(0-9、a-z、A-Z、标点符号)和特殊字符（含有特殊含义的字符）组成的文字模式，它将某个字符模式与所搜索的字符串进行匹配。

➤ 部分使用方法摘要，不完整

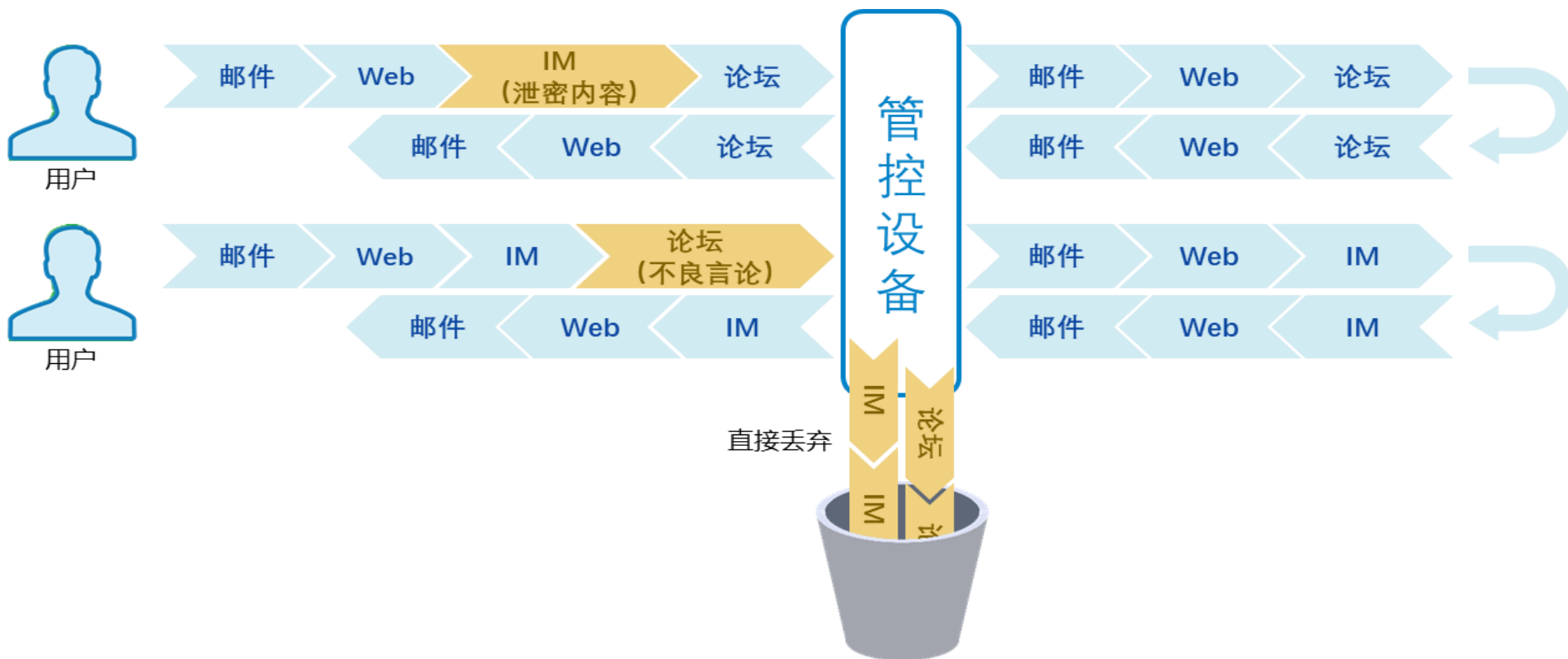
字符	说明
\	将下一字符标记为特殊字符、文本、反向引用或八进制转义符。例如，“n”匹配字符“n”。“\n”匹配换行符。序列“\\”匹配“\”，“\(\"匹配“(“。
^	匹配输入字符串开始的位置。如果设置了 RegExp 对象的 Multiline 属性，^ 还会与“\n”或“\r”之后的位置匹配。
\$	匹配输入字符串结尾的位置。如果设置了 RegExp 对象的 Multiline 属性，\$ 还会与“\n”或“\r”之前的位置匹配。
*	零次或多次匹配前面的字符或子表达式。例如，zo* 匹配“zo”和“zoo”。* 等效于 {0,}。
+	一次或多次匹配前面的字符或子表达式。例如，“zo+”与“zo”和“zoo”匹配，但与“z”不匹配。+ 等效于 {1,}。
?	零次或一次匹配前面的字符或子表达式。例如，“do(es)?”匹配“do”或“does”中的“do”。? 等效于 {0,1}。
{n}	n 是非负整数。正好匹配 n 次。例如，“o{2}”与“Bob”中的“o”不匹配，但与“food”中的两个“o”匹配。
{n,}	n 是非负整数。至少匹配 n 次。例如，“o{2,}”不匹配“Bob”中的“o”，而匹配“fooooood”中的所有 o。‘o{1,}’ 等效于 ‘o+’。‘o{0,}’ 等效于 ‘o*’。
{n,m}	m 和 n 是非负整数，其中 n <= m。至少匹配 n 次，至多匹配 m 次。例如，“o{1,3}”匹配“fooooood”中的头三个 o。‘o{0,1}’ 等效于 ‘o?’。注意：不能将空格插入逗号和数字之间。



CONTENTS

- 应用识别技术
- 内容识别技术
- 行为阻断技术
- 旁路干扰技术
- 策略控制逻辑
- 其他管控策略

- 阻断是最常见的控制手段之一，与防火墙传统的ACL（Access Control List，访问控制列表）功能类似，是对管理员所不希望发生的行为进行的阻断。
- 丢包阻断是最简单的阻断方式，当流经行为安全管理设备的数据包经过主客体识别，匹配了阻断策略后，行为安全管理设备直接将数据包丢弃，使得客户端（主体）与服务端（客体）之间无法正常通信，从而实现阻塞。



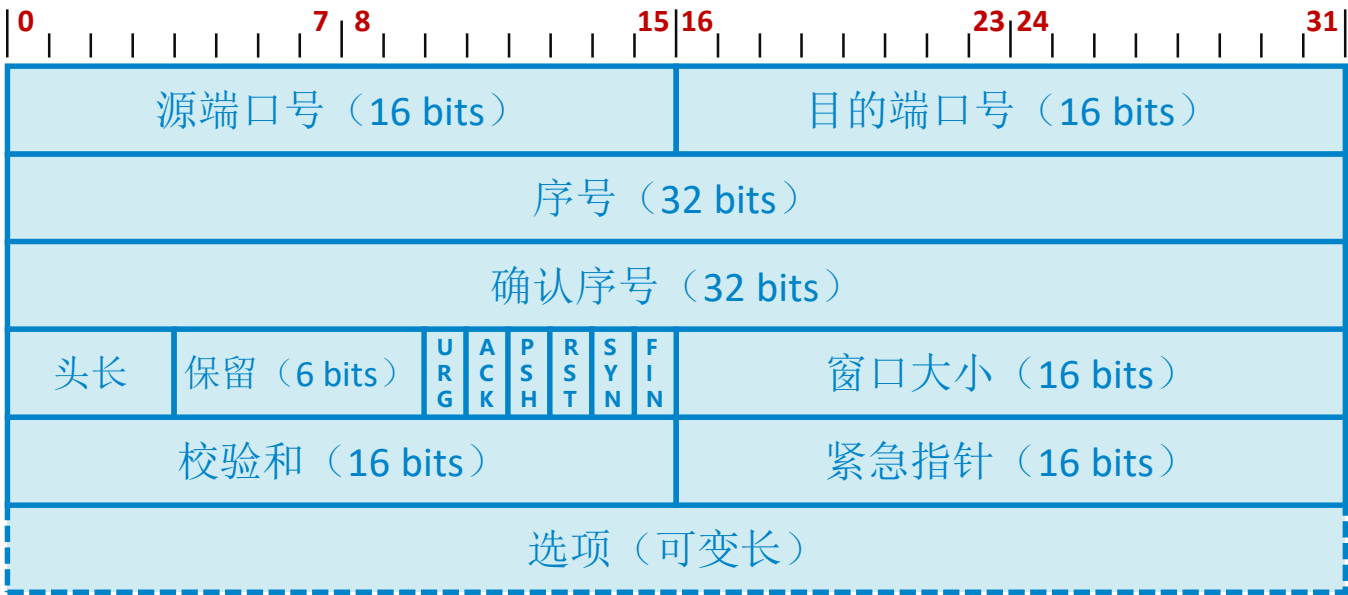
- “丢包”是指管控设备根据安全管理策略，选择性的针对命中阻断策略的数据包不做转发处理，即这些数据包进入管控设备后，不会被转发出去；表面上看起来，就像是被管控设备“丢弃”了。

```
bri0    Link encap:Ethernet  HWaddr BA:██████:83
        inet addr:172.██████.24  Bcast:172.██████.255  Mask:255.255.255.0
        inet6 addr: fe80::b83a:2ff:fe4b:fa83/64 Scope:Link
        UP BROADCAST RUNNING NOARP MULTICAST  MTU:1500  Metric:1
        RX packets:924078 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:42507588 (40.5 MiB)  TX bytes:0 (0.0 b)
```

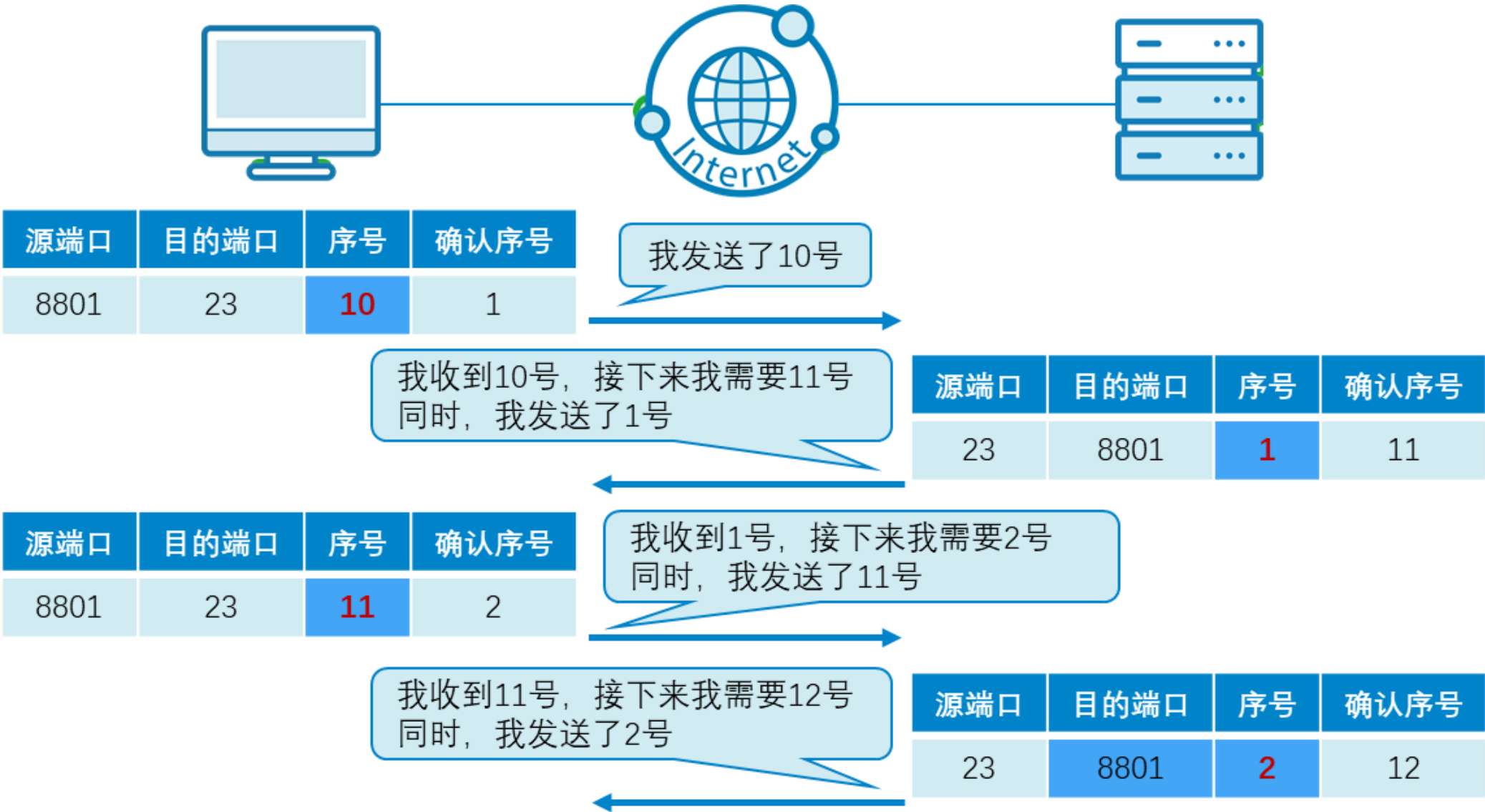
TCP协议的源端口和目的端口：“五元组”中的“两元”，用来唯一标识进程。源端口标识发起端到端通信的进程，目的端口标识接受端到端通信的那个进程。

序号：TCP为传送字节流的每一个字节进行顺序编号，序号是本报文段的第一个字节编号；

确认号：确认号就是期望收到对方的下一个报文段的第一个数据字节的序号；当确认号位N，则表示N-1之前的数据都已经收到了。头部长度：TCP报文段的头部长度，4个比特（bits），十进制取值范围5~15，单位为4字节（4 bytes），所以首部长度范围也就是20字节（5 x 4 bytes）~ 60字节（15 x 4 bytes）；



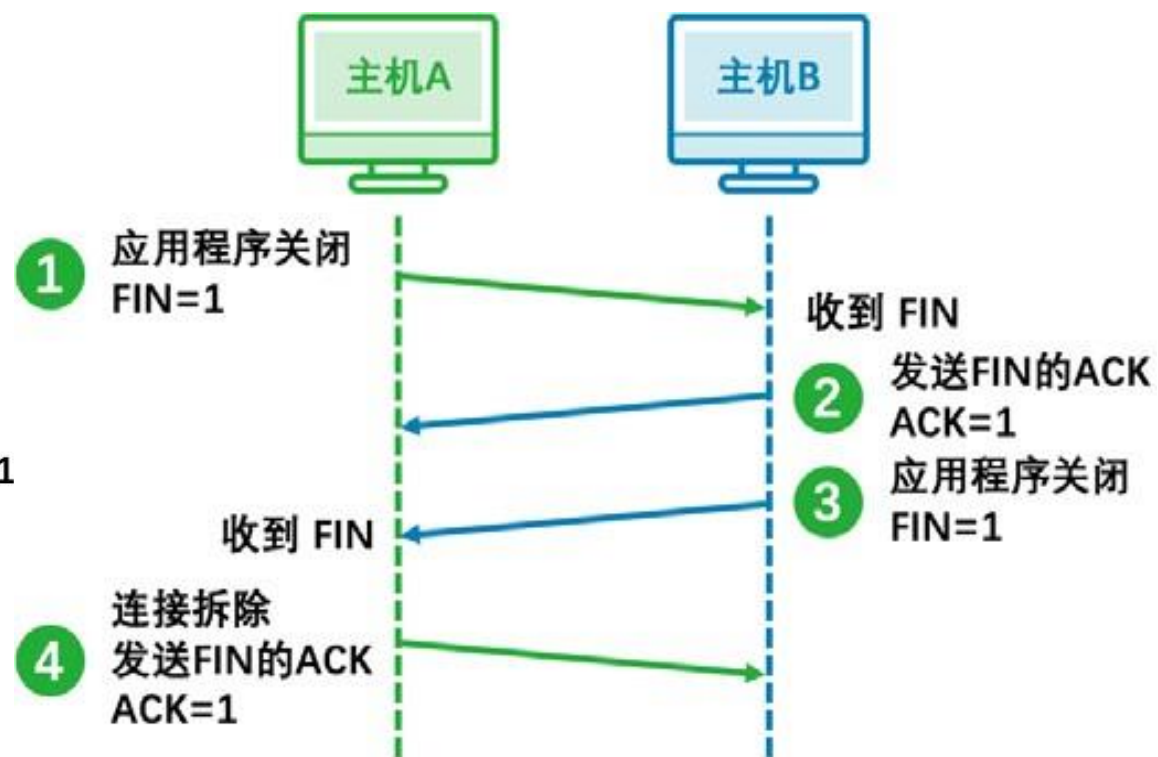
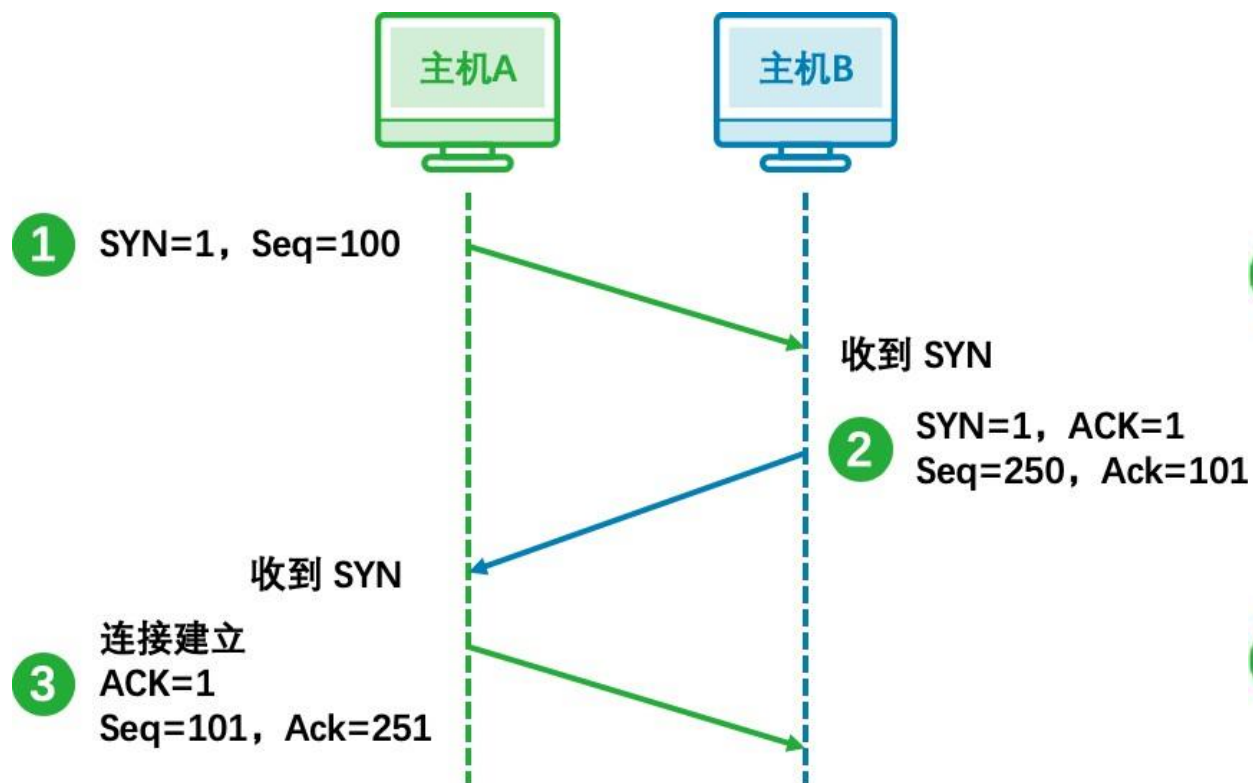
连接重置阻断——序号与确认号



连接重置阻断——三次握手与四次挥手



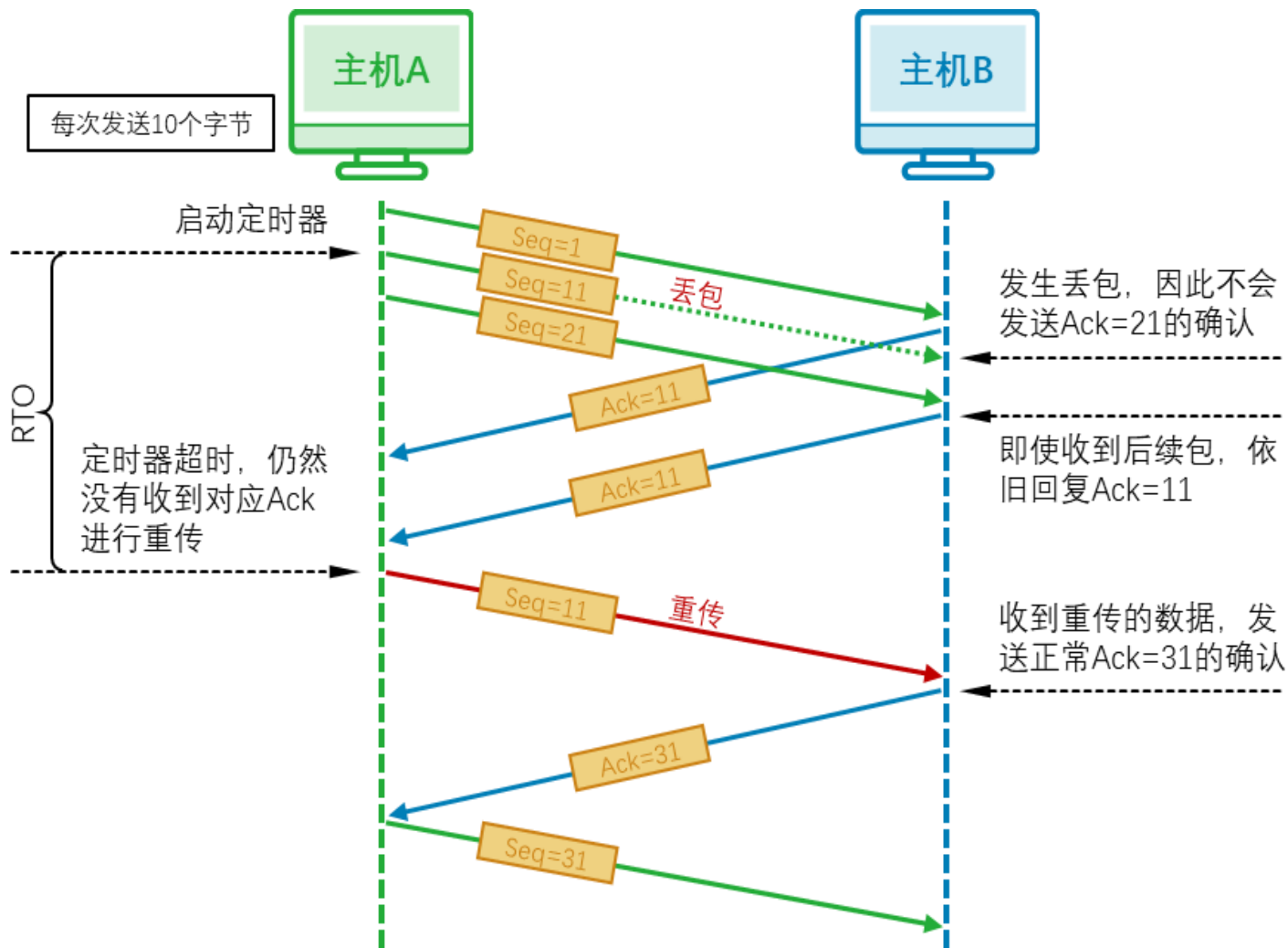
- TCP 连接的建立和拆除被形象的称之为“三次握手”（建立连接过程）和“四次挥手”（连接拆除过程）。



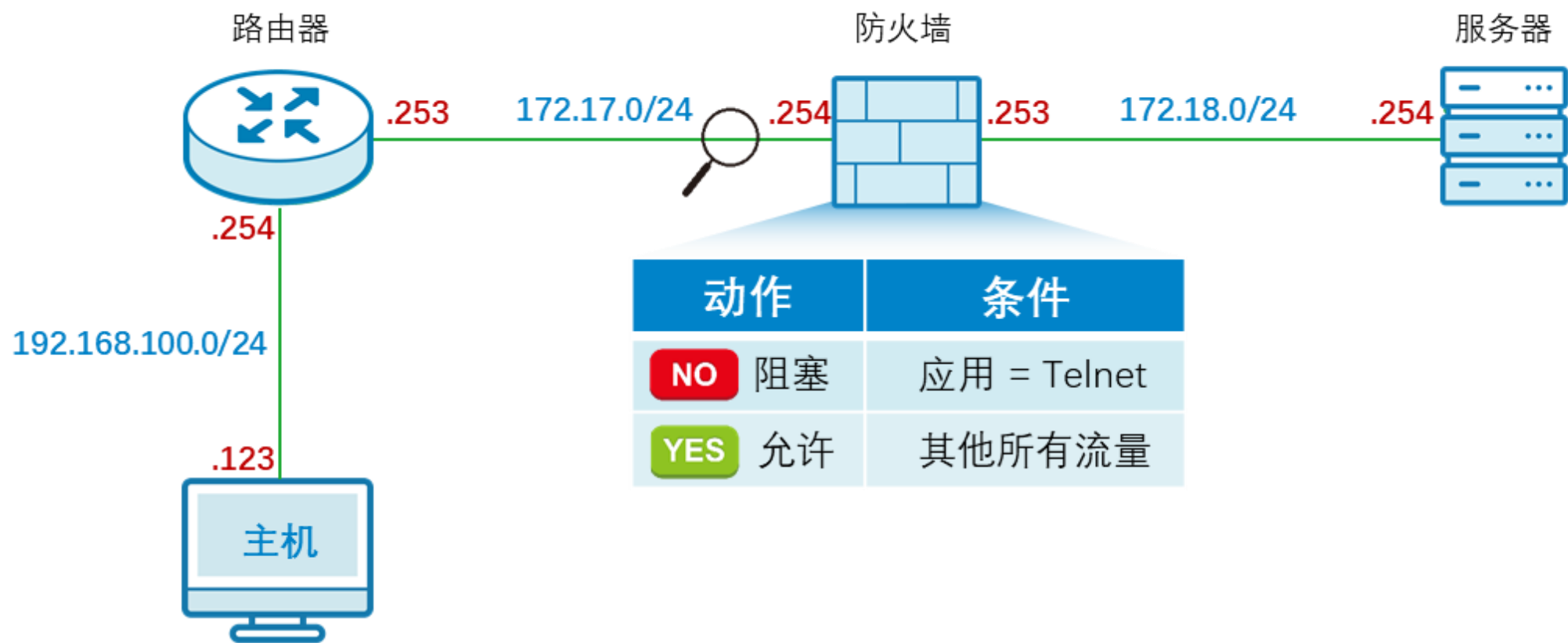
连接重置阻断——超时和重传



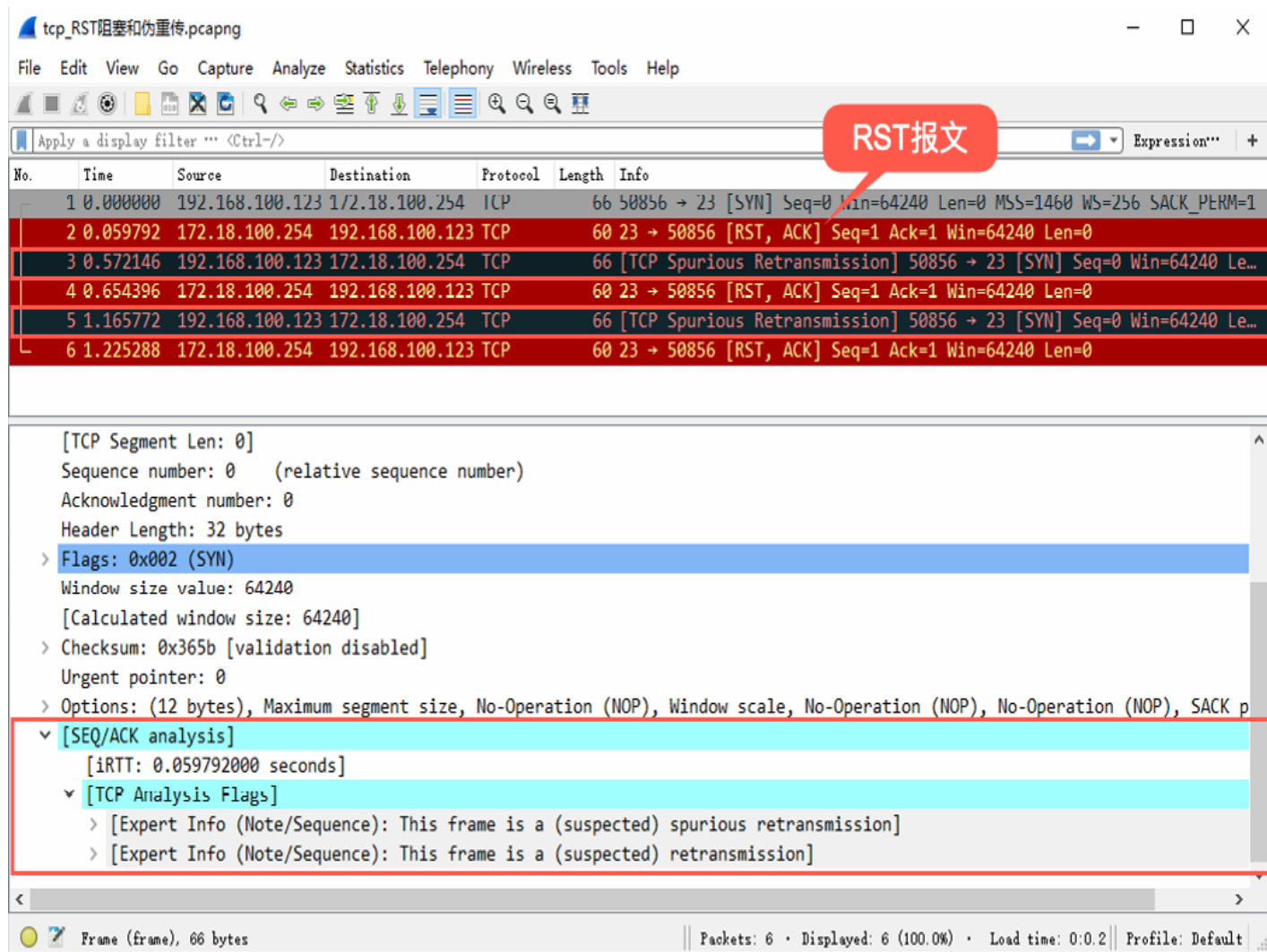
- TCP协议要求发送端每发送一个报文段，就启动一个定时器并等待确认信息；接收端成功接收新数据后返回确认信息（ACK=1）。
- 若在定时器超时前数据未能被确认，TCP就认为报文段中的数据已经发生丢失或损坏，需要对报文段中的数据重新组织和重传。



- 用户体验降低：**当采用简单丢包阻断方式的安全管理设备发现需要阻塞的数据报文时，将直接把这些报文丢弃，TCP协议无法区分造成“丢包”的原因，将无差别的启动定时器，等待超时后进行重传，这将大大降低用户体验。



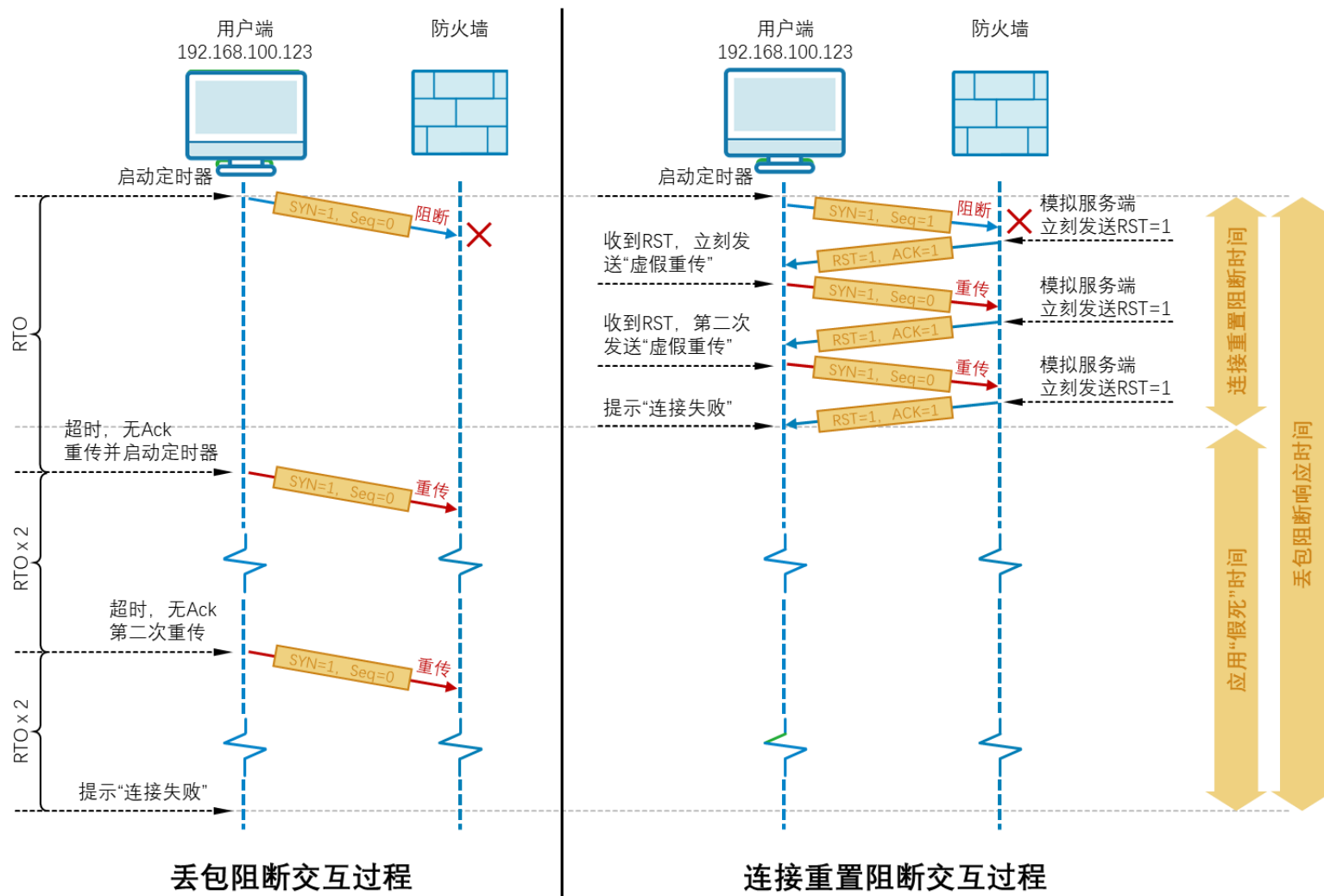
- 安全管理设备在丢弃数据包的同时会模拟接收端向发起端发送一个 RST=1 的连接重置报文，这样发送端会认为对方“拒绝”了连接请求，立刻将计时器超时，而进行后续的动作



连接重置阻断



- 1、防火墙代替真实服务器（使用服务器 IP 地址 172.18.100.254）发送 RST=1 的重置报文；
- 2、用户主机收到重置报文后进行了“虚假重传”（Spurious Retransmission）；
- 3、对于用户端来说，当用户发起 Telnet 请求后，会立刻得到“连接失败”提示，而无需长时间等待。



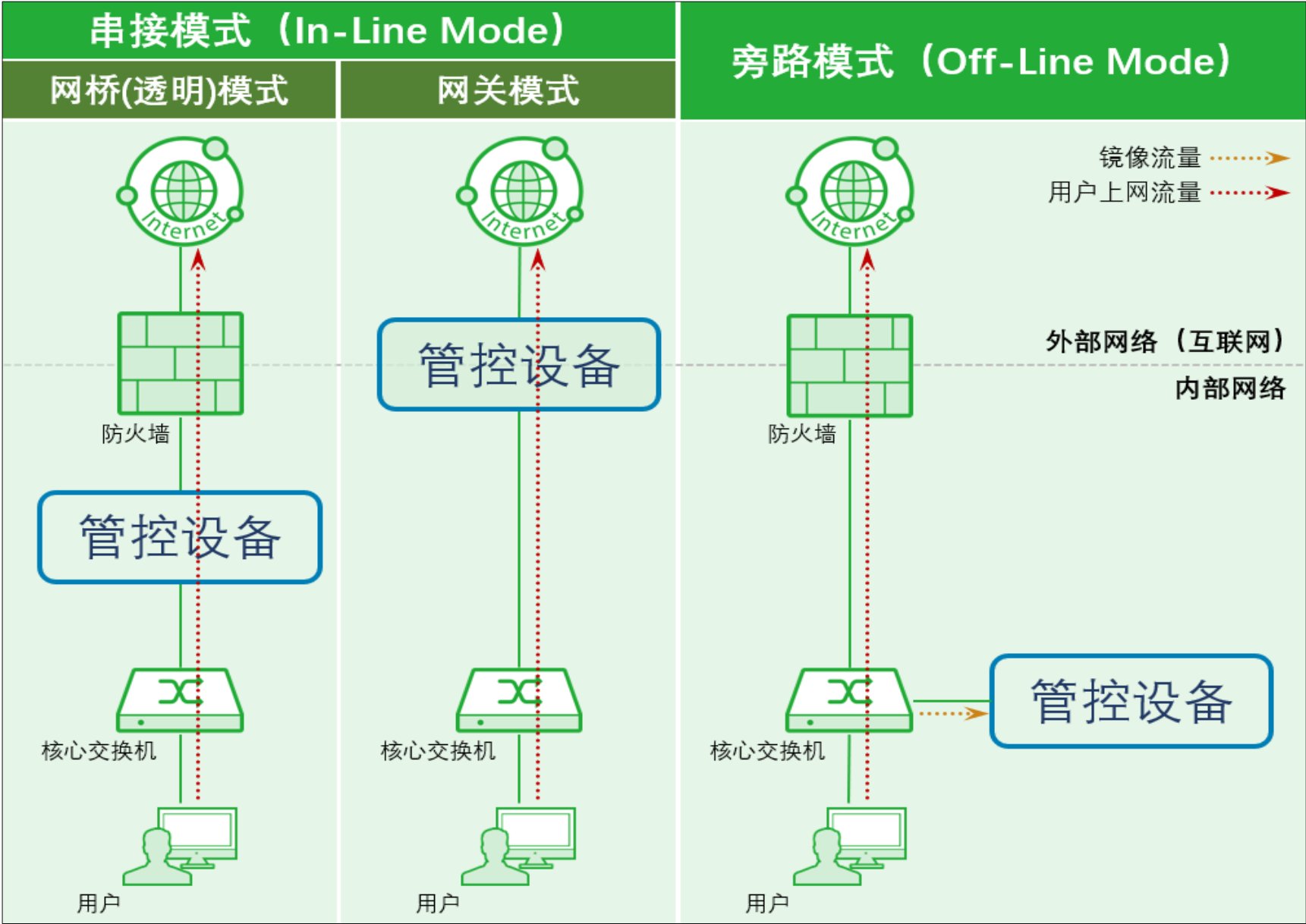


CONTENTS

- 应用识别技术
- 内容识别技术
- 行为阻断技术
- 旁路干扰技术
- 策略控制逻辑
- 其他管控策略

旁路模式与串接模式的显著区别：

- 用户的上网流量不直接经过管控设备，而是通过核心交换机或其他网络分析设备镜像后到达管控设备。
- 管控设备收到的是真实流量的一份“拷贝”，并对其进行识别、分析；用户原始上网流量不会受到任何影响
- 管控设备只能对网络流量进行分析，无法阻断。这种部署由于对原始流量无任何影响。
- 常用于可靠性要求较高且无明显控制需求的场景，如运营商等大流量环境。



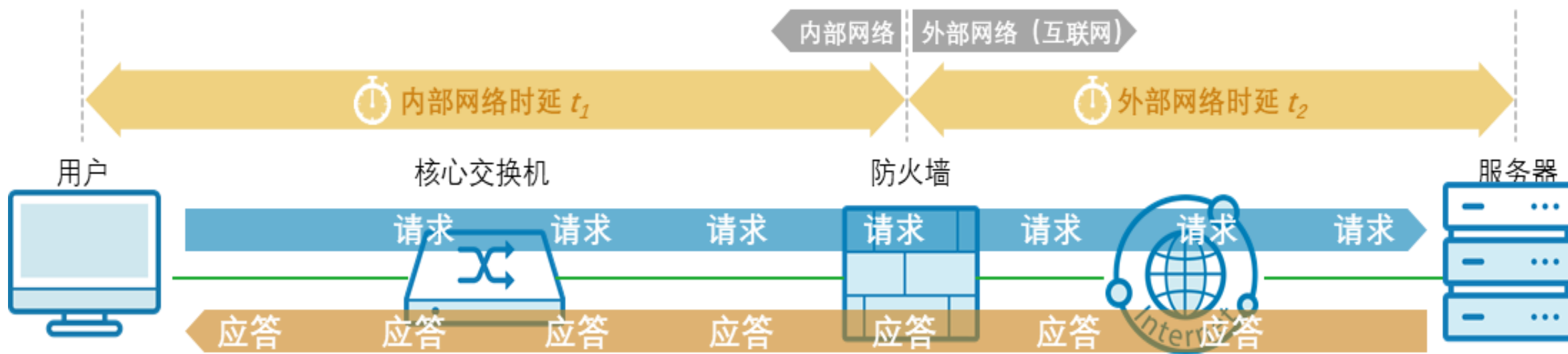
部署形态	网络变更	单点故障	功能		适用场景
			审计	控制	
串接网桥（透明）模式	有	有	●	●	最常见的部署模式，适用于大多数场景
串接网关模式	有	有	●	●	适用于小型网络组网场景，通过一台设备完成所有功能
旁路模式	无	无	●	○	适用于对可靠性要求较高、控制需求较低的网络场景

- 旁路模式下控制能力的实现原理与串接模式不同：由于设备无法对原始流量进行操作，因此也不能通过阻断的方式实现控制，而是需要本章我们要讨论的“旁路干扰”技术。

旁路干扰的基本原理



- 用户端与服务器端通常以“一问一答”的形式进行交互，即用户端发送请求，服务器收到来自用户端的请求后做出响应并发送应答。
- 不论是请求数据包，还是应答数据包在网络中传输以及被端到端路径上的各类网络设备处理都是需要时间的，这些时间我们称之为“时延”。
- 为了讨论方便，我们将端到端通信中的时延简化为四个部分；以边界网络设备（如：防火墙）作为分界点，将网络分为内部、外部两部分。



旁路干扰的基本原理



- 图中可以看到，通常外部网络的时延是内部网络时延的几倍甚至十几倍，如果服务器端位于不同的国家或运营商，外部网络时延甚至可以达到数十毫秒。
- 旁路干扰的基础：利用内、外部网络时延的显著差异，在来自外部服务器的真实应答到达用户端之前，由管控设备“冒充”服务器伪造虚假的应答发送给用户，对其正常通信进行干扰。

```
Administrator: Windows PowerShell
PS C:\Windows\system32> ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64
Reply from 192.168.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
PS C:\Windows\system32> ping www.163.com

Pinging www.163.com.lxdns.com [43.243.234.234] with 32 bytes of data:
Reply from 43.243.234.234: bytes=32 time=4ms TTL=51
Reply from 43.243.234.234: bytes=32 time=37ms TTL=51
Reply from 43.243.234.234: bytes=32 time=5ms TTL=51
Reply from 43.243.234.234: bytes=32 time=6ms TTL=51

Ping statistics for 43.243.234.234:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 37ms, Average = 13ms
PS C:\Windows\system32> ping www.163.com

Pinging www.163.com.lxdns.com [43.243.234.234] with 32 bytes of data:
Reply from 43.243.234.234: bytes=32 time=4ms TTL=51
Reply from 43.243.234.234: bytes=32 time=5ms TTL=51
Reply from 43.243.234.234: bytes=32 time=5ms TTL=51
Reply from 43.243.234.234: bytes=32 time=4ms TTL=51

Ping statistics for 43.243.234.234:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 4ms, Maximum = 5ms, Average = 4ms
PS C:\Windows\system32>
```

内部网络时延

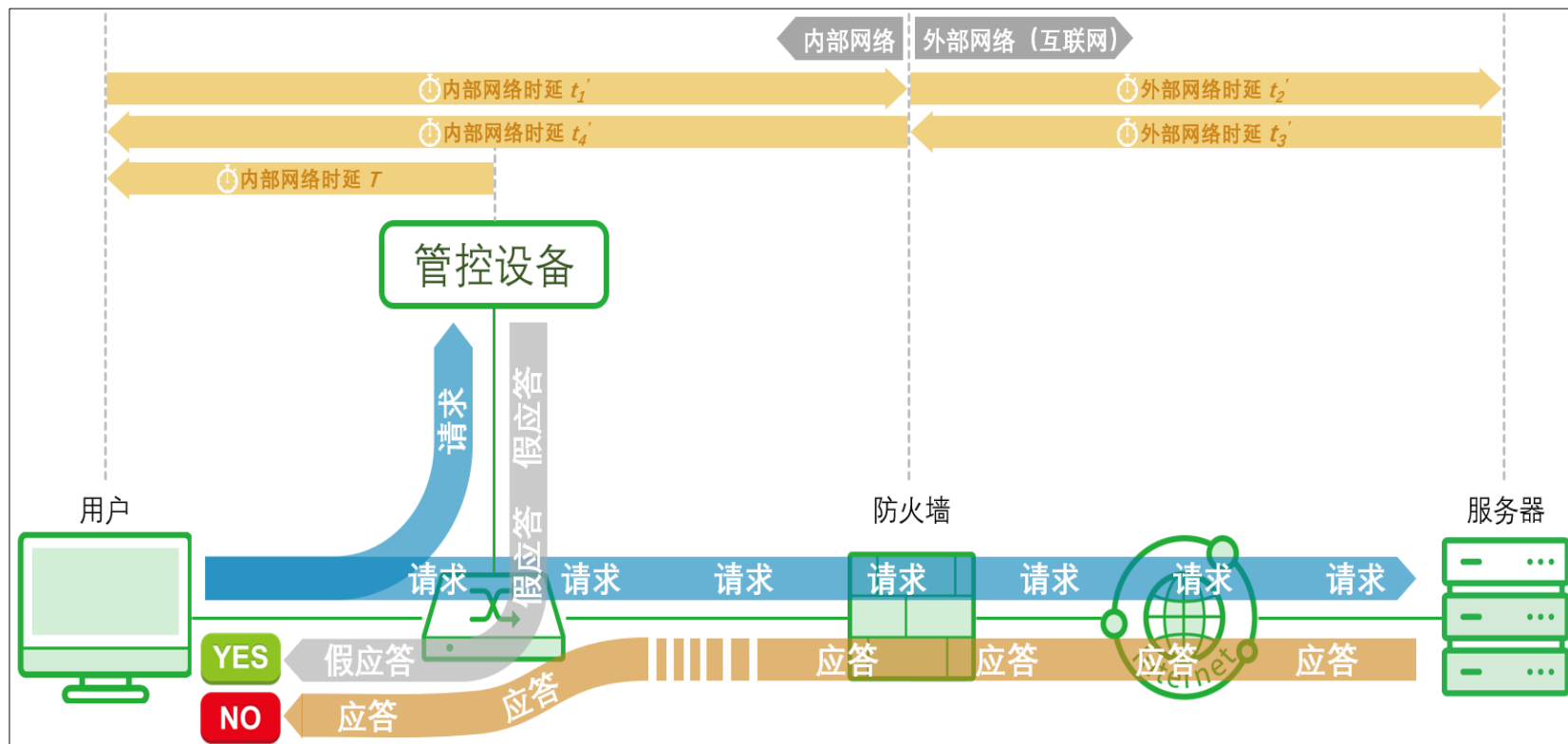
外部网络时延 (第1次测试)

外部网络时延 (第2次测试)

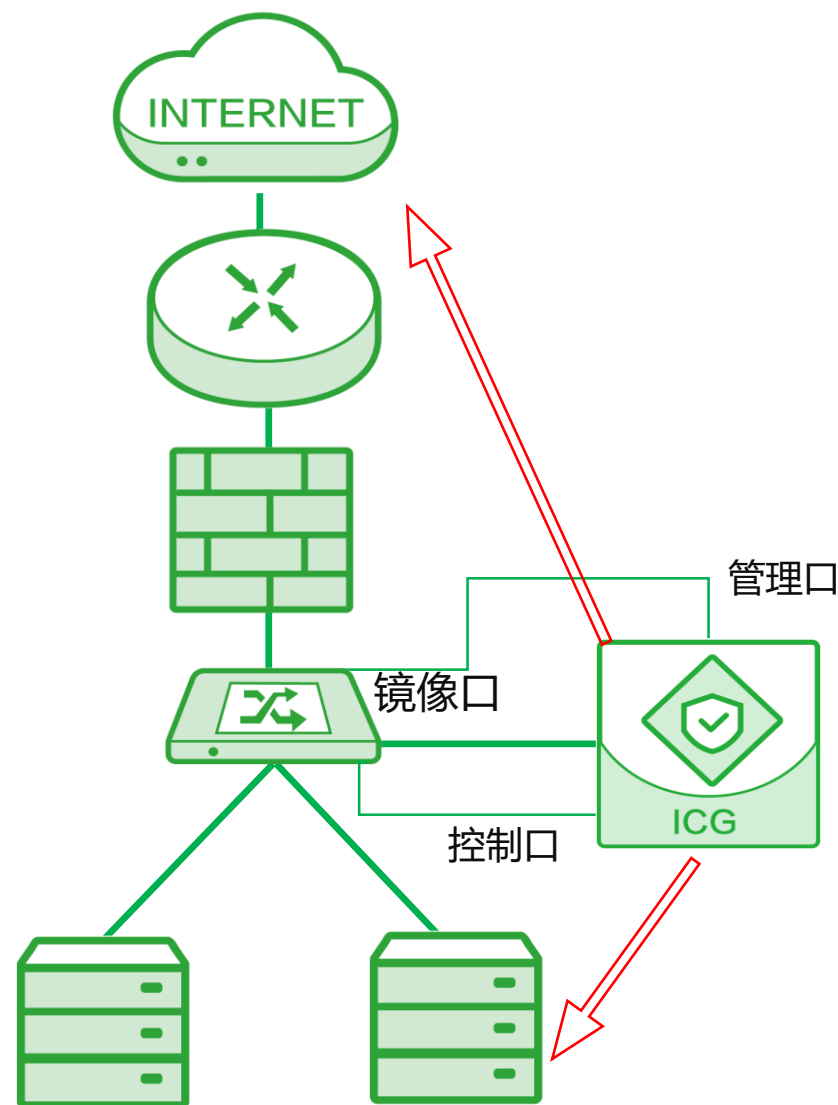
旁路干扰的基本原理

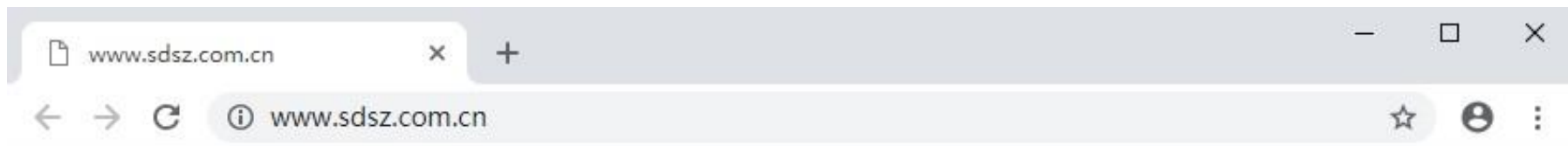


- 1) 用户发出的请求数据包经过交换机镜像，发送给管控设备；原始流量正常转发给服务器；
- 2) 管控设备对镜像流量进行分析，并进行策略匹配；
- 3) 若流量命中“控制”策略，管控设备模拟服务器（伪造数据包参数，如源 IP 地址等）发送虚假应答数据包；
- 4) 由于管控设备位于内部网络，虚假应答总会优先于真实应答到达用户；用户接收到虚假应答后，其正常的通信被干扰，达到“控制”的效果。



- 1) 用户访问某一个包含有特定关键字的域名（如，www.sdsz.com.cn），发出 HTTP 请求报文；该报文在被转发的同时，也被镜像给了管控设备；
- 2) 管控设备收到该 HTTP 请求后进行策略匹配，并成功命中一条阻塞策略；
- 3) 管控设备随即模拟用户及服务器（根据数据包中的源目的 IP 地址），向对方发送 RST 标记置位的数据报文，强制终止连接；
- 4) 用户的 HTTP 请求被强制终止，无法正常访问页面；浏览器提示“连接被重置”错误。





This site can't be reached

The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_RESET

Reload

Details

旁路干扰——页面重定向



Wireshark · Follow TCP Stream (tcp.stream eq 0) · tcp_旁路控制...

<</div>
</div>

您(192.168.100.123)访问的教育类页面 <u>www.sdsz.com.cn/</u> 已被禁止!
禁止原因如下:

网站访问_阻塞

单击浏览器的 "后退" 按钮返回上一页

若有任何疑问,请与管理员联系。

</div>
</body>

2 client pkt(s), 0 server pkt(s), 0 turns.

61.49.8.144:80 → 192.168.100.123:59756 (14) Show data as UTF-8 Stream 0

Find: Find Next

Hide this stream Print Save as*** Close Help

tcp_旁路控制口推送页面_客户机抓包_sdsz.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.stream eq 0

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.100.123	61.49.8.144	TCP	66	59756 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=2
3	0.138474	61.49.8.144	192.168.100.123	TCP	66	80 → 59756 [SYN, ACK] Seq=0 Ack=1
4	0.138570	192.168.100.123	61.49.8.144	TCP	54	59756 → 80 [ACK] Seq=1 Ack=1 Win=66304 Len=0
5	0.141497	192.168.100.123	61.49.8.144	HTTP	655	GET / HTTP/1.1
8	0.201687	61.49.8.144	192.168.100.123	TCP	1454	[TCP segment of a reassembled PDU]
9	0.212396	61.49.8.144	192.168.100.123	HTTP	536	HTTP/1.1 200 OK (text/html)
10	0.212514	192.168.100.123	61.49.8.144	TCP	54	59756 → 80 [ACK] Seq=602 Ack=1883 Win=66304 Len=0
11	0.213872	192.168.100.123	61.49.8.144	TCP	54	59756 → 80 [FIN, ACK] Seq=602 Ack=
12	0.223686	61.49.8.144	192.168.100.123	TCP	60	80 → 59756 [FIN, ACK] Seq=1883 Ack=
13	0.223829	192.168.100.123	61.49.8.144	TCP	54	59756 → 80 [ACK] Seq=603 Ack=1884 Win=66304 Len=0
14	0.234817	61.49.8.144	192.168.100.123	TCP	60	80 → 59756 [RST, ACK] Seq=1884 Ack=602 Win=0 Len=0
15	0.490821	61.49.8.144	192.168.100.123	TCP	60	80 → 59756 [ACK] Seq=1 Ack=602 Win=66304 Len=0
20	1.324717	61.49.8.144	192.168.100.123	TCP	1466	[TCP Spurious Retransmission] 80 → 59756 [ACK] Seq=1
21	1.335582	61.49.8.144	192.168.100.123	TCP	1466	[TCP Retransmission] 80 → 59756 [ACK] Seq=1
30	4.308081	61.49.8.144	192.168.100.123	TCP	1466	[TCP Spurious Retransmission] 80 → 59756 [ACK] Seq=1
32	10.208221	61.49.8.144	192.168.100.123	TCP	1466	[TCP Spurious Retransmission] 80 → 59756 [ACK] Seq=1

> Frame 9: 536 bytes on wire (4288 bits), 536 bytes captured (4288 bits) on interface 0

> Ethernet II, Src: c2:02:39:f0:00:00 (c2:02:39:f0:00:00), Dst: Vmware_f6:6a:d5 (00:0c:29:f6:6a:d5)

> Internet Protocol Version 4, Src: 61.49.8.144, Dst: 192.168.100.123

> Transmission Control Protocol, Src Port: 80 (80), Dst Port: 59756 (59756), Seq: 1401, Ack: 602, Len: 482

> [2 Reassembled TCP Segments (1882 bytes): #8(1400), #9(482)]

> Hypertext Transfer Protocol

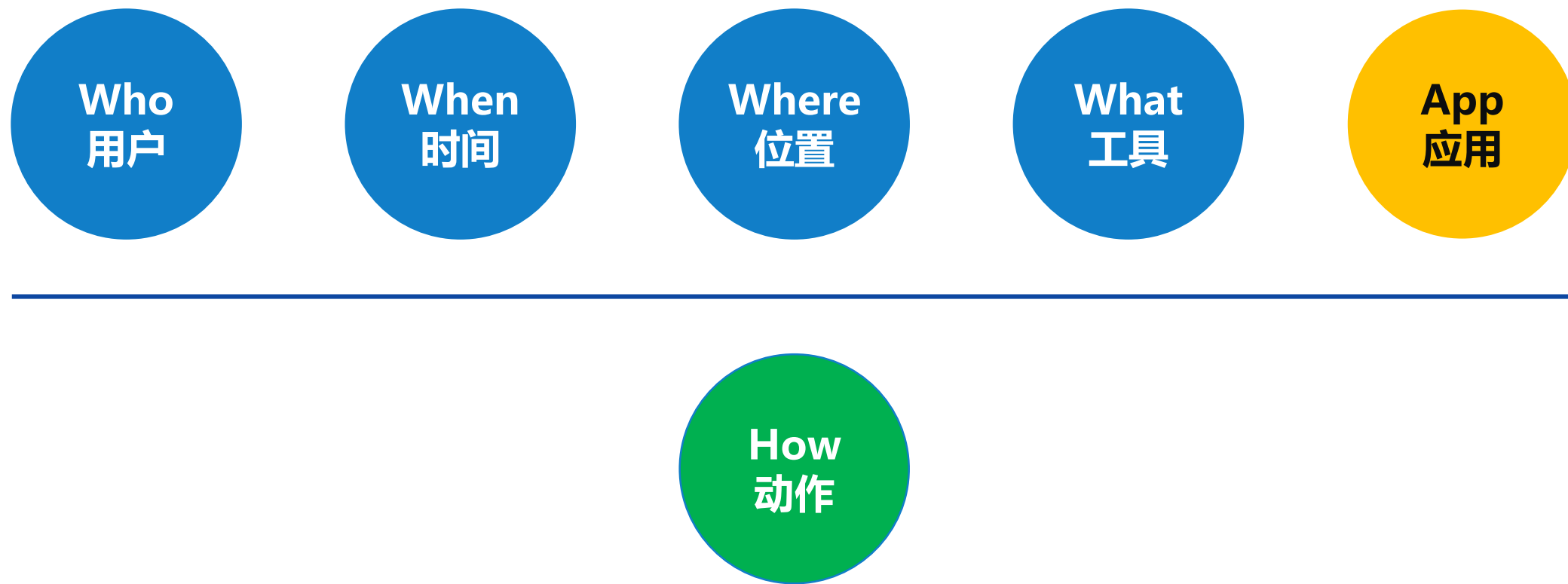
> Line-based text data: text/html

tcp_旁路控制口推送页面_客户机抓包_sdsz | Packets: 33 · Displayed: 16 (48.5%) · Load time: 0:0.31 | Profile: Default



CONTENTS

- 应用识别技术
- 内容识别技术
- 行为阻断技术
- 旁路干扰技术
- 策略控制逻辑
- 其他管控策略



➤ 动作：允许、阻塞

- **策略**就是为了实现某一个目标，预先根据可能出现的问题制定的若干对应的方案。在ICG中，策略是指到达为管控目标而设定的各种上网规则。
- **对象**是一个抽象的概念，是要操作的目标。是人们要进行研究的任何事物。在ICG中，对象为策略服务，是策略的作用目标。

控制逻辑——策略顺序匹配逻辑



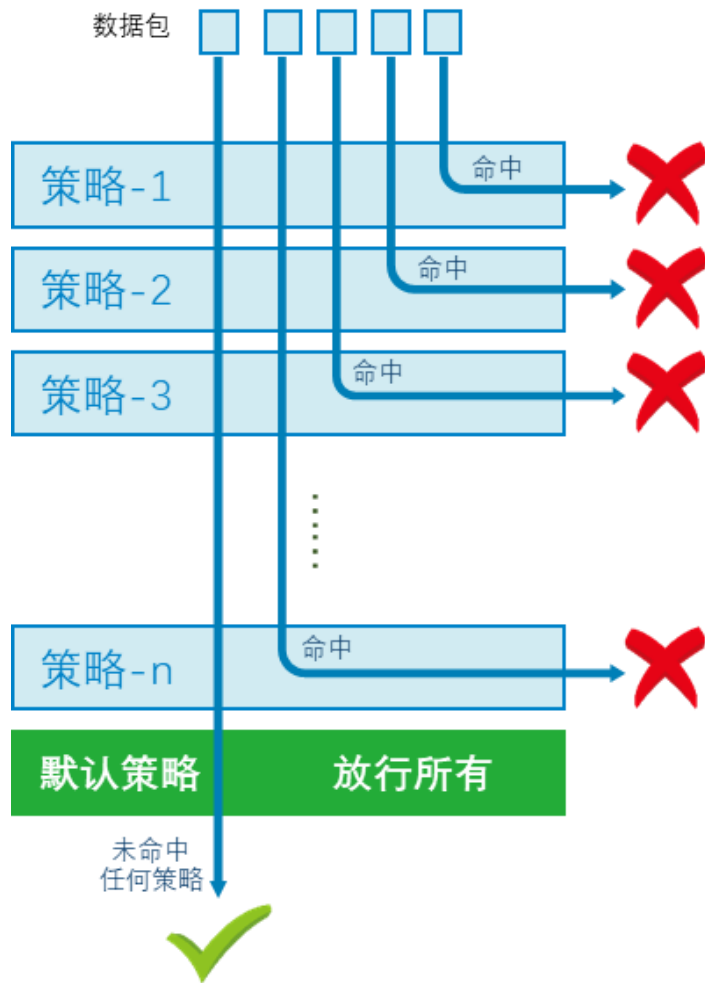
- 从上到下
- 匹配即停
- 默认放行

<input type="checkbox"/>	优先级	状态 ▾	类型 ▾	名称	描述	时间	用户	动作 ②
<input type="checkbox"/>	↓ 0	● 启用	FTP	ftp审计		所有时间	[未共享] 所有用户	✓
<input type="checkbox"/>	↑ ↓ 1	● 启用	网安应用行...	网安审计策略		所有时间	[未共享] 所有用户	
<input type="checkbox"/>	↑ ↓ 2	● 启用	文件	文件审计		所有时间	[未共享] 所有用户	✓
<input type="checkbox"/>	↑ ↓ 3	● 启用	IM聊天	IM审计		所有时间	[未共享] 所有用户	✓
<input type="checkbox"/>	↑ ↓ 4	● 启用	发帖	发帖审计		所有时间	[未共享] 所有用户	✓
<input type="checkbox"/>	↑ ↓ 5	● 启用	搜索	[缺省]网页搜索策略	缺省网页搜索策略	所有时间	[已共享] 所有用户	✓
<input type="checkbox"/>	↑ ↓ 6	● 启用	发帖	[缺省]发帖审计全记录	缺省发帖审计全记录	所有时间	[已共享] 所有用户	✓
<input type="checkbox"/>	↑ ↓ 7	● 启用	网页	[缺省]网站访问全记录	缺省网站访问策略	所有时间	[未共享] 所有用户	✓
<input type="checkbox"/>	↑ ↓ 8	● 禁用	IM聊天	飞信聊天	飞信聊天	所有时间	[已共享] 所有用户	
<input type="checkbox"/>	↑ ↓ 9	● 禁用	文件	飞信文件	飞信文件	所有时间	[已共享] 所有用户	
<input type="checkbox"/>	↑ ↓ 10	● 禁用	IM聊天	飞信其它	飞信其它	所有时间	[已共享] 所有用户	
<input type="checkbox"/>	↑ ↓ 11	● 禁用	IM聊天	QQ聊天	QQ聊天	所有时间	[已共享] 所有用户	✓
<input type="checkbox"/>	↑ ↓ 12	● 禁用	文件	QQ文件	QQ文件	所有时间	[已共享] 所有用户	✓
<input type="checkbox"/>	↑ ↓ 13	● 禁用	邮件	接收邮件审计	接收邮件审计	所有时间	[已共享] 所有用户	✓
<input type="checkbox"/>	↑ ↓ 14	● 禁用	FTP	FTP审计	FTP审计	所有时间	[已共享] 所有用户	✓
<input type="checkbox"/>	↑ ↓ 15	● 禁用	TELNET	TELNET审计	TELNET审计	所有时间	[已共享] 所有用户	✓
<input type="checkbox"/>	↑ 16	● 禁用	HTTPS	HTTPS审计	HTTPS审计	所有时间	[已共享] 所有用户	✓

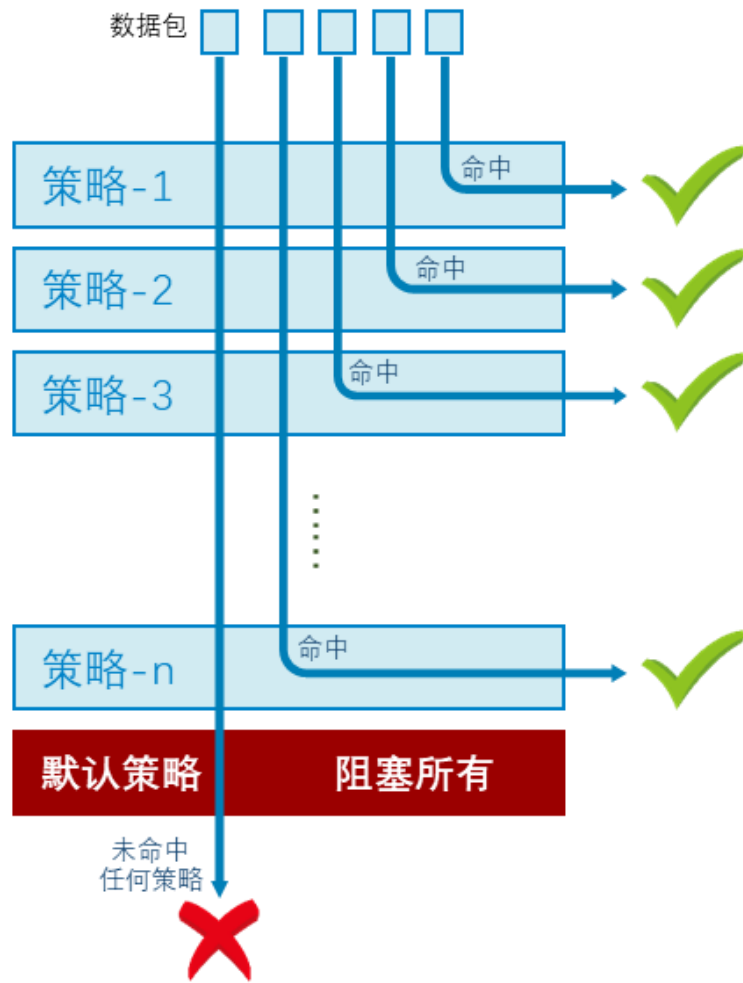
控制逻辑——默认放行逻辑



- 默认放行是指如果网络数据包没有命中任何管控策略，会被行为安全管理设备直接转发，如右图a。
- 与防火墙等网络安全设备的逻辑有着本质的区别，网络安全设备采用“默认阻塞，显式放行”逻辑，即如果网络数据包没有匹配到任何策略，会被安全设备阻塞，如右图b



(a)



(b)



网络安全设备

- 如防火墙等，其核心功能是保证网络安全。
- 在这种情况下管理员必须清晰的明确哪些流量可以被放行；因此防火墙默认策略（优先级最低的策略）为阻塞所有，这就使得所有没有被管理员明确放行的流量被全部阻塞；尽管在有的时候，这样做会造成连通性问题；但为了确保安全，这种“宁可错杀一千，也不放过一个”的控制逻辑是必要的



行为安全管理设备

- 此类设备更多时候是在确保网络可用的前提下为网络管理者提供增值功能，保证网络可用性具有更高的优先级。
- 因此这类设备默认策略（优先级最低的策略）一般为放行所有，所有没有被管理员明确阻塞的流量会被放行；另一方面，不论设备识别能力有多么强大也都会出现“误识别”现象，这会导致策略匹配的失效，若使用“默认阻塞”逻辑，会造成比安全设备更大概率的“错杀”。对于一个非安全类设备来说，这种“错杀”会大大增大网络维护成本，是应该尽量避免的。

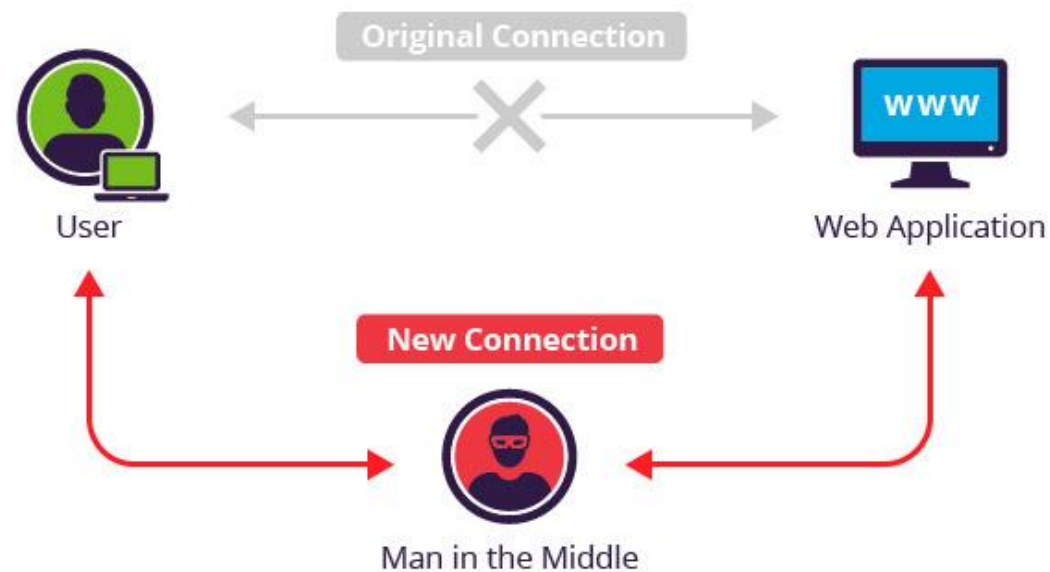
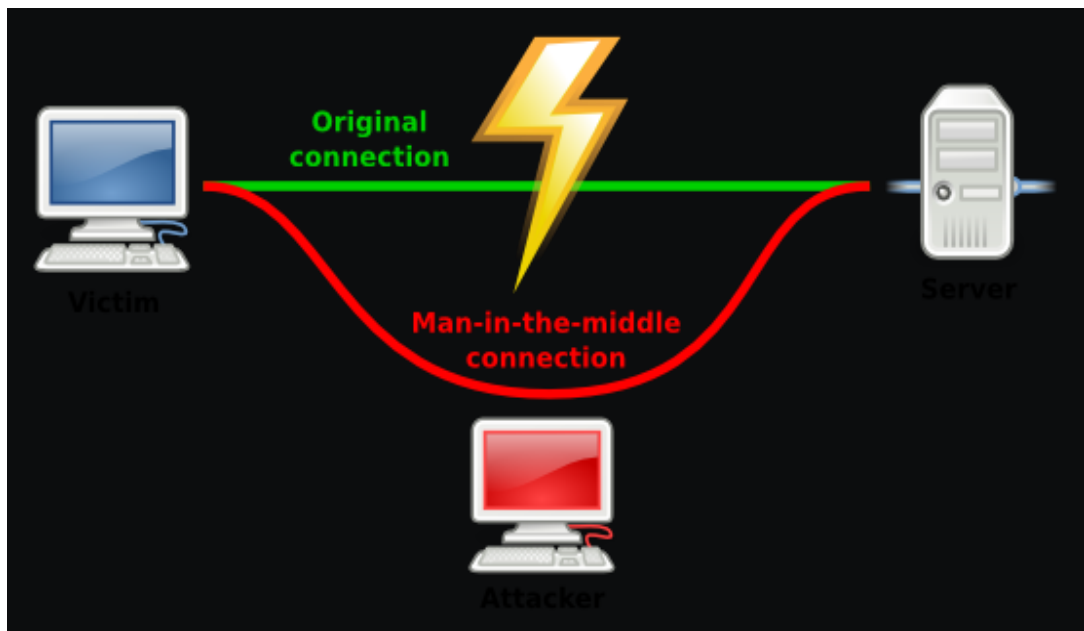


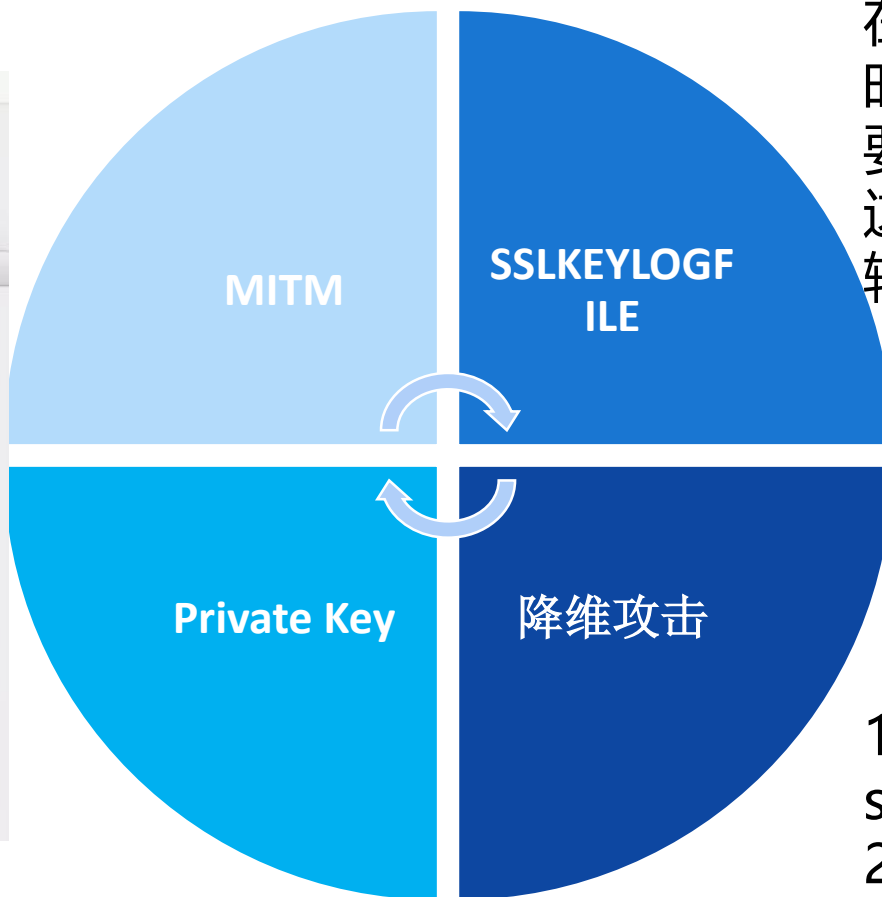
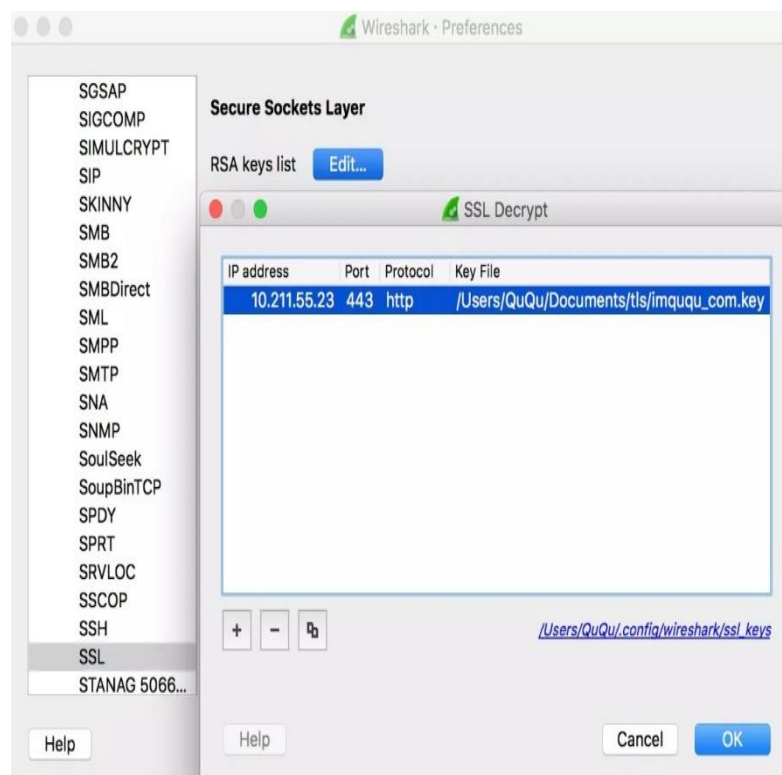
CONTENTS

- 应用识别技术
- 内容识别技术
- 行为阻断技术
- 旁路干扰技术
- 策略控制逻辑
- 其他管控策略

“在密码学和计算机安全领域中，中间人攻击（*Man-in-the-middle attack, MITM*）是指攻击者与通讯的两端分别建立独立的联系，并交换其所收到的数据，使通讯的两端认为他们正在通过一个私密的连接与对方直接对话，但事实上整个会话都被攻击者完全控制。在中间人攻击中，攻击者可以拦截通讯双方的通话并插入新的内容。”

----来自维基百科的定义





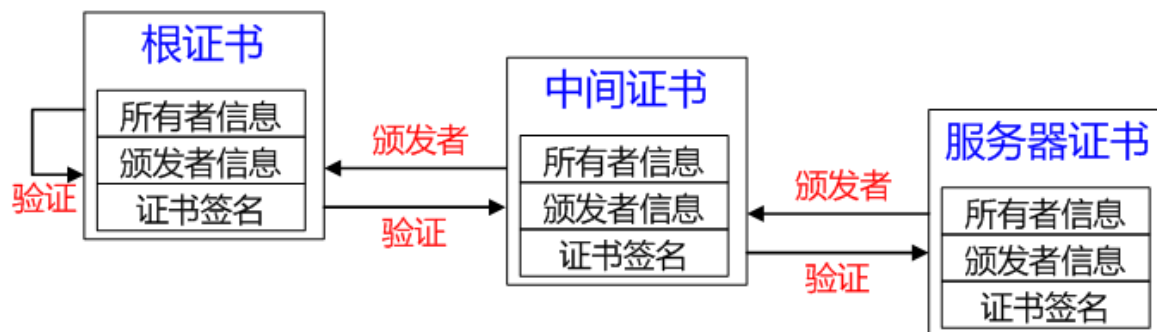
Firefox 和 Chrome 会在系统环境变量存

在 SSLKEYLOGFILE 文件路径时，将每个 HTTPS 链接最重要的加密信息保存在此。有了这个文件，Wireshark 就可以轻松解密 HTTPS 流量。

1 HTTPS---->HTTP(比如 sslstrip 工具)

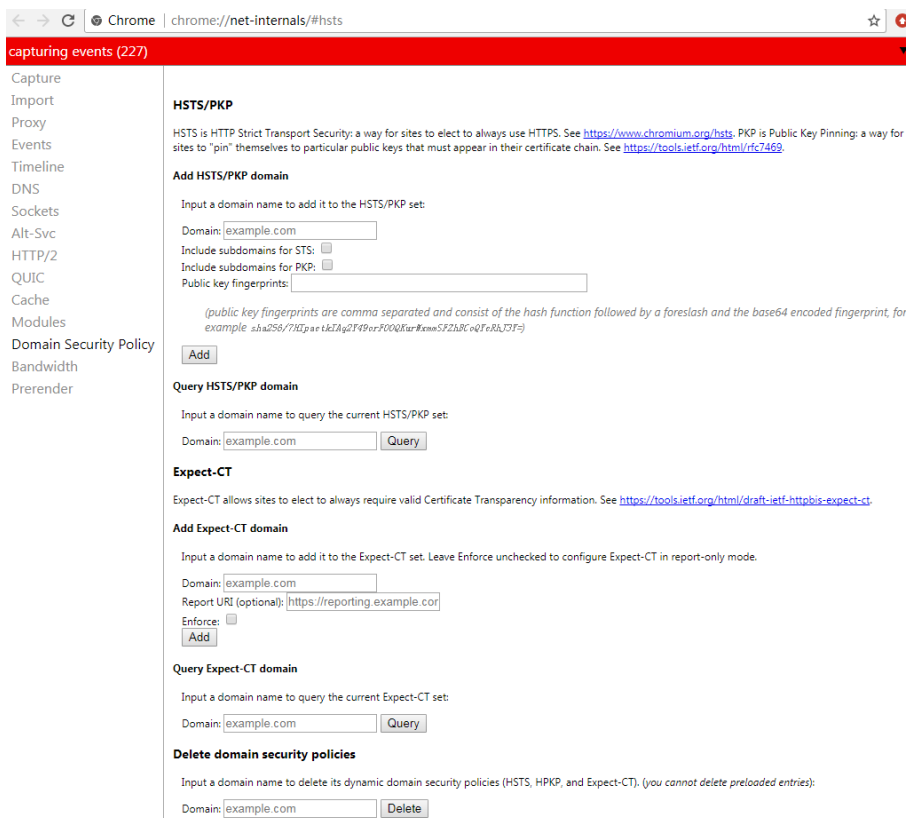
2 QUIC---->HTTPS

PKI (Public Key Infrastructure) 即"公钥基础设施", 是一种遵循既定标准的密钥管理平台,它能够为所有网络应用提供加密和数字签名等密码服务及所必需的密钥和证书管理体系, 简单来说, PKI就是利用公钥理论和技术建立的提供安全服务的基础设施。PKI技术是信息安全技术的核心, 也是电子商务的关键和基础技术。



完整的PKI系统必须具有权威认证机构(CA)、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口 (API) 等基本构成部分, 构建PKI也将围绕着这五大系统来着手构建。

HTTP严格传输安全（HTTP Strict Transport Security, *HSTS*）是一套由互联网工程任务组发布的互联网安全策略机制。网站可以选择使用HSTS策略，来让浏览器强制使用HTTPS与网站进行通信，以减少会话劫持风险。



The screenshot shows the Chrome DevTools 'capturing events (227)' panel. The left sidebar lists various network events: Capture, Import, Proxy, Events, Timeline, DNS, Sockets, Alt-Svc, HTTP/2, QUIC, Cache, Modules, Domain Security Policy, Bandwidth, and Prerender. The main panel displays the 'HSTS/PKP' section, which includes a description of HSTS and PKP, and a form to 'Add HSTS/PKP domain'. The form has fields for 'Domain' (example.com), 'Include subdomains for STS' (checked), 'Include subdomains for PKP' (checked), and 'Public key fingerprints' (empty). Below the form is a 'Query HSTS/PKP domain' section with a 'Domain' field (example.com) and a 'Query' button. The 'Expect-CT' section follows, with a description and a form to 'Add Expect-CT domain'. The form has fields for 'Domain' (example.com), 'Report URI (optional)' (https://reporting.example.com), and 'Enforce' (checked). Below this is a 'Query Expect-CT domain' section with a 'Domain' field (example.com) and a 'Query' button. At the bottom is a 'Delete domain security policies' section with a 'Domain' field (example.com) and a 'Delete' button.

HTTP/1.1 307 Internal Redirect
Location: <https://www.baidu.com/>
Non-Authoritative-Reason: HSTS

HTTP/1.1 302 Moved Temporarily
Date: Mon, 08 Jan 2018 08:15:33 GMT
Content-Type: text/html
Connection: Keep-Alive

.....
Location: <https://www.baidu.com/>
Server: BWS/1.1
X-UA-Compatible: IE=Edge,chrome=1
Content-Length: 225

➤需求背景：

- 运营商希望能够对接入网络的设备做观察、控制，能够控制一个用户后的终端数量，以达到运营商多开账号的目的。
- 企业则希望对接入网络的做严格的限制，保障网络接入在企业边界内部，控制私接无线等设备以保障企业内部网络安全。

➤ **共享接入策略** 的核心功能是能够**识别出使用同一个IP上网的终端数量**，不论是采用分时分段上网，还是采用NAT路由上网，或是使用代理同时上网。在此基础上，通过策略对共享接入的终端类型及数量进行控制，以达到防止网络私接的目的。

共享接入模块能够对接入网络的设备做观察、控制，能够检测到一个用户的终端数量，做策略控制，以达到掌控用户终端数量的目的。

实现效果

- ✓ 主机个数（PC及终端管理）的识别，并可分别配置允许共享接入的数量
- ✓ 对识别到的终端进行控制，并对命中的用户推送阻塞提示页面
- ✓ 可配置是否封堵非80端口的流量
- ✓ 对私接状况进行监控和记录日志
- ✓ 允许在线升级私接特征库（跟随协议库一同更新）

- 不同终端的网络流量中会携带有不同的特征，共享接入模块依靠不同终端的不同流量特征来判别是否具有私接行为，当一个用户（IP）的上网流量中包含多个不同特征时，即可判定为其私接。
- ICG共享接入模块分析特征列表
 - 1、UA特征识别
 - 2、数据包识别（pkt）
 - 3、应用特征识别
 - 4、account流量特征
 - 5、手机imei特征码识别
 - 6、Wi-Fi 接入识别

抓取内网ip用户上网流量进行分析

分析流量中所带的流量特征

一个ip用户流量中有多种特征即判定为该用户为私接

User-Agent识别方法



- Pc UA: 区分 windows mac ubuntu;
- 手机UA: iPhone, 不同品牌的android;

```
⊕ Internet Protocol, Src: 192.168.60.118 (192.168.60.118), Dst: 119.75.218.77 (119.75.218.77)
⊕ Transmission Control Protocol, Src Port: optimanet (2408), Dst Port: http (80), Seq: 1, Ack: 1, Len: 715
⊖ Hypertext Transfer Protocol
  ⊖ GET /index.php?tn=utf8kb_oem_dg HTTP/1.1\r\n
    ⊖ [Expert Info (Chat/Sequence): GET /index.php?tn=utf8kb_oem_dg HTTP/1.1\r\n]
      [Message: GET /index.php?tn=utf8kb_oem_dg HTTP/1.1\r\n]
      [Severity level: Chat]
      [Group: Sequence]
      Request Method: GET
      Request URI: /index.php?tn=utf8kb_oem_dg
      Request Version: HTTP/1.1
      Host: www.baidu.com\r\n
      Connection: keep-alive\r\n
      Cache-Control: max-age=0\r\n
      User-Agent: Mozilla/5.0 (windows NT 5.1) AppleWebKit/537.13 (KHTML, like Gecko) Chrome/24.0.1284.2 Safari/537.13\r\n
      Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8\r\n
      Accept-Encoding: gzip,deflate,sdch\r\n
      Accept-Language: zh-CN,zh;q=0.8\r\n
      Accept-Charset: GBK,utf-8;q=0.7,*;q=0.3\r\n
      [truncated] Cookie: BAIDUID=04F3769855180A557E65EA2B6808EC4F:FG=1; Hm_lvt_9f14aaa038bbba8b12ec2a4a3e51d254=13502852910\r\n
```

➤Pc特征id: 本地ip, 本机mac, 唯一id;

➤手机特征id: imei;

```
> Frame 1: 553 bytes on wire (4424 bits), 553 bytes captured (4424 bits)
> Ethernet II, Src: Vmware_bd:79:6d (00:50:56:bd:79:6d), Dst: Vmware_bd:13:03 (00:50:56:bd:13:03)
> Internet Protocol Version 4, Src: 175.16.114.81, Dst: 111.206.23.96
> Transmission Control Protocol, Src Port: 49976, Dst Port: 80, Seq: 2037491528, Ack: 1434936955, Len: 499
▼ Hypertext Transfer Protocol
  ▼ [truncated]GET /b?t=21&pf=201&p=11&p1=114&rpge=search&bstp=1&ce=0&channelid=sogou&de=4c678ea9f13e4b1e5a4ec5e593921a8d&list=0&macid=00:50:56:BD:79:6D&ppuid=&pu=&purl=http://www.iqiyi.com/lib/pps/tu:
    > [ [truncated]Expert Info (Chat/Sequence): GET /b?t=21&pf=201&p=11&p1=114&rpge=search&bstp=1&ce=0&channelid=sogou&de=4c678ea9f13e4b1e5a4ec5e593921a8d&list=0&macid=00:50:56:BD:79:6D&ppuid=&pu=&purl
      Request Method: GET
    > Request URI [truncated]: /b?t=21&pf=201&p=11&p1=114&rpge=search&bstp=1&ce=0&channelid=sogou&de=4c678ea9f13e4b1e5a4ec5e593921a8d&list=0&macid=00:50:56:BD:79:6D&ppuid=&pu=&purl=http://www.iqiyi.com
      Request Version: HTTP/1.1
  Host: msg.iqiyi.com\r\n
  User-Agent: Qiyi List Client PC 6.2.57.5300\r\n
  Accept-Encoding: gzip\r\n
  Pragma: no-cache\r\n
  Cache-Control: no-cache\r\n
  Connection: close\r\n
  Accept: */*\r\n
  \r\n
  [Full request URI [truncated]: http://msg.iqiyi.com/b?t=21&pf=201&p=11&p1=114&rpge=search&bstp=1&ce=0&channelid=sogou&de=4c678ea9f13e4b1e5a4ec5e593921a8d&list=0&macid=00:50:56:BD:79:6D&ppuid=&pu=&p
  [HTTP request 1/1]
```

手机连接WIFI的时候会发出特定的探测信号

```
<!-- iPhone WIFI接入识别 -->
<process featype="ios_wifi" length="0" platform="IPHONE">
  <feature>
    <id value="1940"/>
    <useragent condition="CaptiveNetworkSupport"/>
    <host condition=""/>
    <reg source="GET" regx=""/>
  </feature>
</process>
```

```
> Frame 4: 182 bytes on wire (1456 bits), 182 bytes captured (1456 bits)
> Ethernet II, Src: Tp-LinkT_e8:45:3d (08:57:00:e8:45:3d), Dst: HuaweiTe_45:2f:9c (d0:d0:4b:45:2f:9c)
> Internet Protocol Version 4, Src: 10.208.206.199, Dst: 218.58.101.229
> Transmission Control Protocol, Src Port: 13948, Dst Port: 80, Seq: 3457513441, Ack: 156137168, Len: 128
▼ Hypertext Transfer Protocol
  > GET /library/test/success.html HTTP/1.0\r\n
    Host: www.apple.com\r\n
    Connection: close\r\n
    User-Agent: CaptiveNetworkSupport-346 wispr\r\n
    \r\n
    [Full request URI: http://www.apple.com/library/test/success.html]
    [HTTP request 1/1]
    [Response in frame: 6]
```

- 强特征的定义在于能单独标识一种类型的设备。多种强特征取最大值。
- 弱特征不能唯一标识一种类型的设备，但是多种弱特征联合可以表征设备。弱特征取小。

```
#method weak feature
FEA_METHOD_TYPE=2
UA_METHOD_TYPE=1
FLASH_METHOD_TYPE=2
IP_METHOD_TYPE=2
PACKET_METHOD_TYPE=1
ACCOUNT_METHOD_TYPE=1
IOS_WIFI_METHOD_TYPE=2
WEAK_FEATURE_NUM=2
INCOGNITOMODE=1
```


1、某公司IT管理员希望对员工的聊天内容进行审计，以下说法正确的是？

- ☒ A、ICG可以审计PC端的QQ和微信，但是需要安装客户端
- ☐ B、ICG可以审计PC端的QQ和微信，而且不需要安装客户端
- ☐ C、微信网页版由于是加密的，所以无法审计
- ☐ D、ICG可以审计手机端的QQ和微信内容

THANKS!

让网络更安全
让世界更美好