2.7 拒绝服务攻击

拒绝服务攻击

Denial of Service（DoS），能导致服务器不能正常提供服务的攻击，都可以称为DoS攻击。

分布式拒绝服务攻击

Distributed Denial of Service（DDoS）指借助于客户/服务器模式，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DoS攻击，从而成倍地提高拒绝服务攻击的威力。

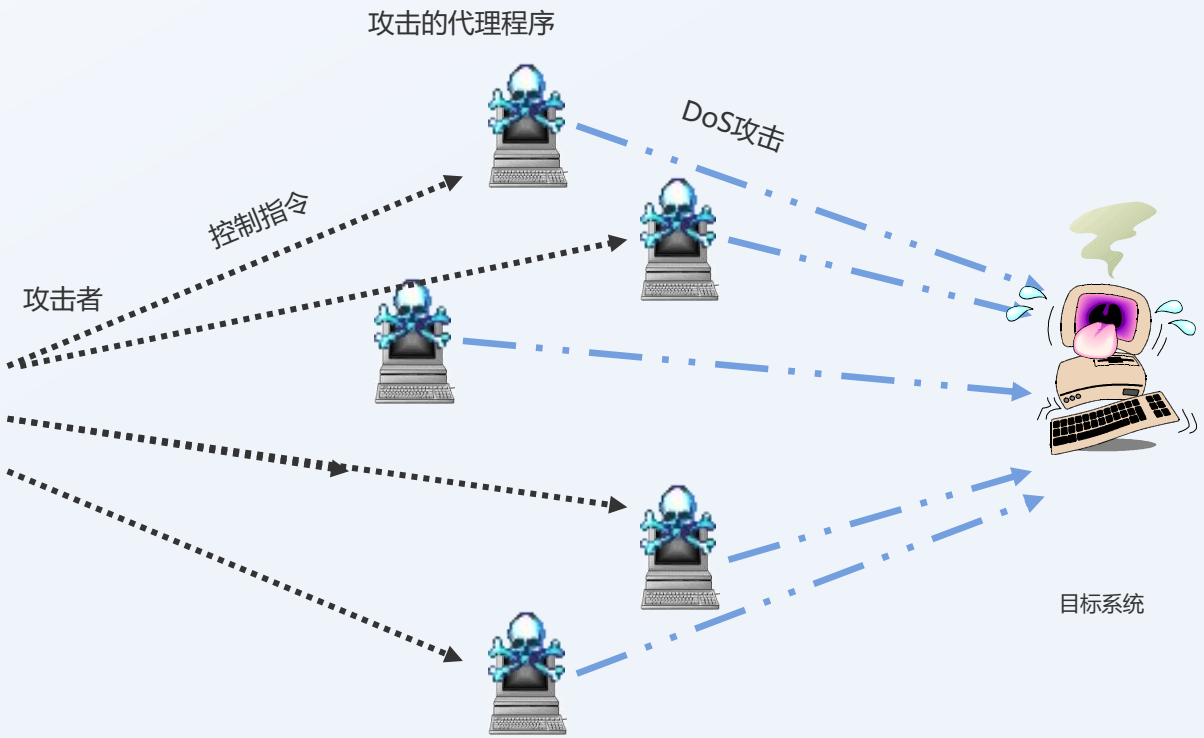
01 2.7 拒绝服务攻击

2018
201801	荷兰三大银
201802	GirHub遭
201803	Memcac
201804	欧洲最大DDoS服务
201805	美国监控到无线设备
201806	加密邮件服务商ProtonMail因遭到
201808	多家游戏公司遭到大规模DDoS
201810	阿里云主要节点全面上线IPv6 DDoS防护
201810	阿里云成功为某游戏客户抵抗峰值大于1Tbps的DDoS攻击
201811	柬埔寨全国频繁断网，因主要网络服务提供商遭到大规模DDoS攻击
201812	匿名者宣布对全球银行发动DDoS攻击

2.7.1 DDoS （分布式拒绝服务）攻击

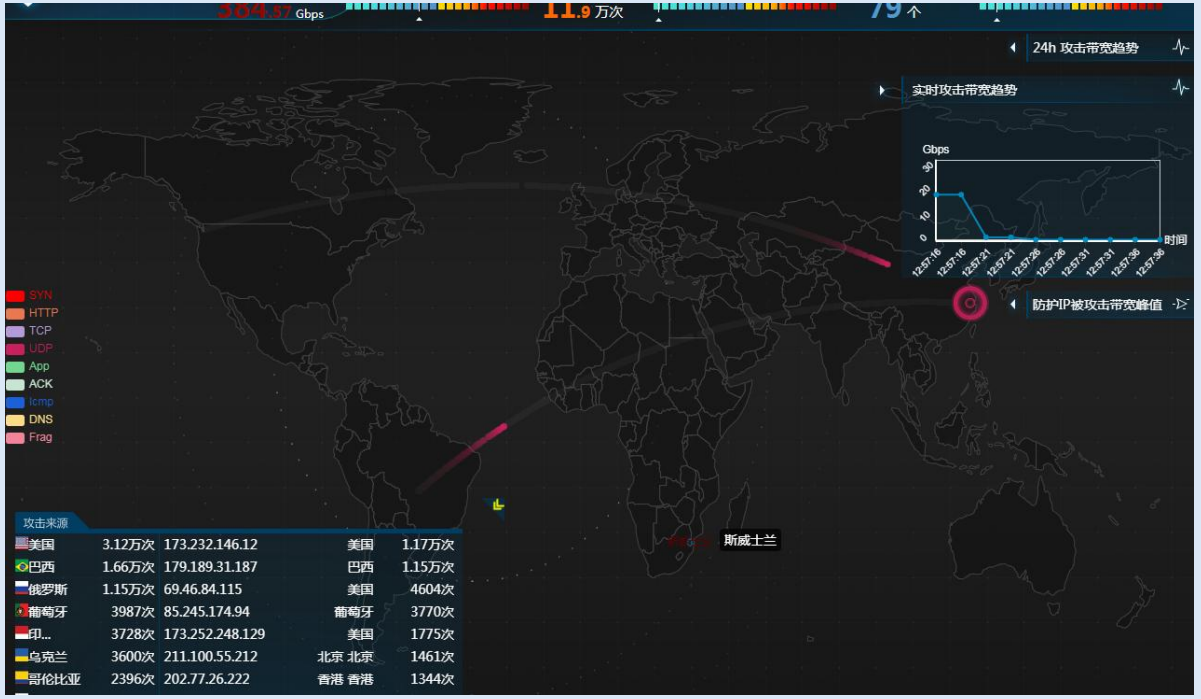
发起攻击

- 攻击者使他的全部代理程序同时发送由残缺的数字包构成的连接请求送至目标系统。
- 包括虚假的连接请求在内的大量残缺的数字包攻击目标系统，最终将导致它因通信淤塞而崩溃



2.7.1 DDoS （分布式拒绝服务）攻击

典型事件



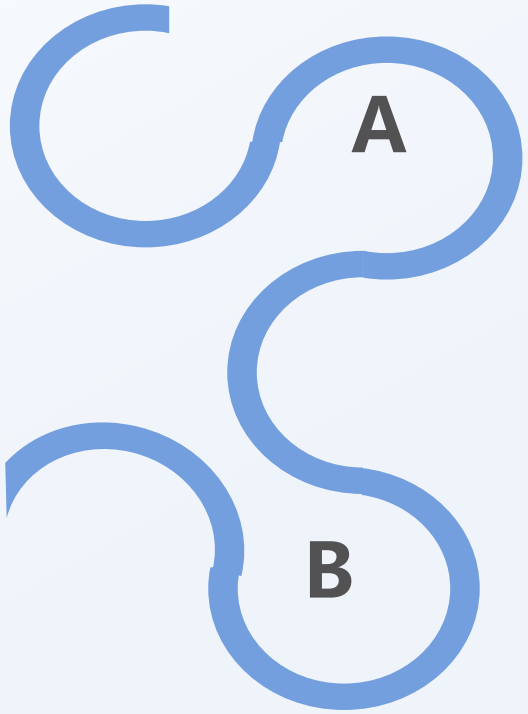
2.7.1 DDoS （分布式拒绝服务）攻击

2019年的第二季度，连续两个月DDoS攻击流量接近Tb级，6月份稍有下降。

DDoS攻击态势

2.7.1 DDoS （分布式拒绝服务）攻击

DoS攻击的对象与工具



攻击对象

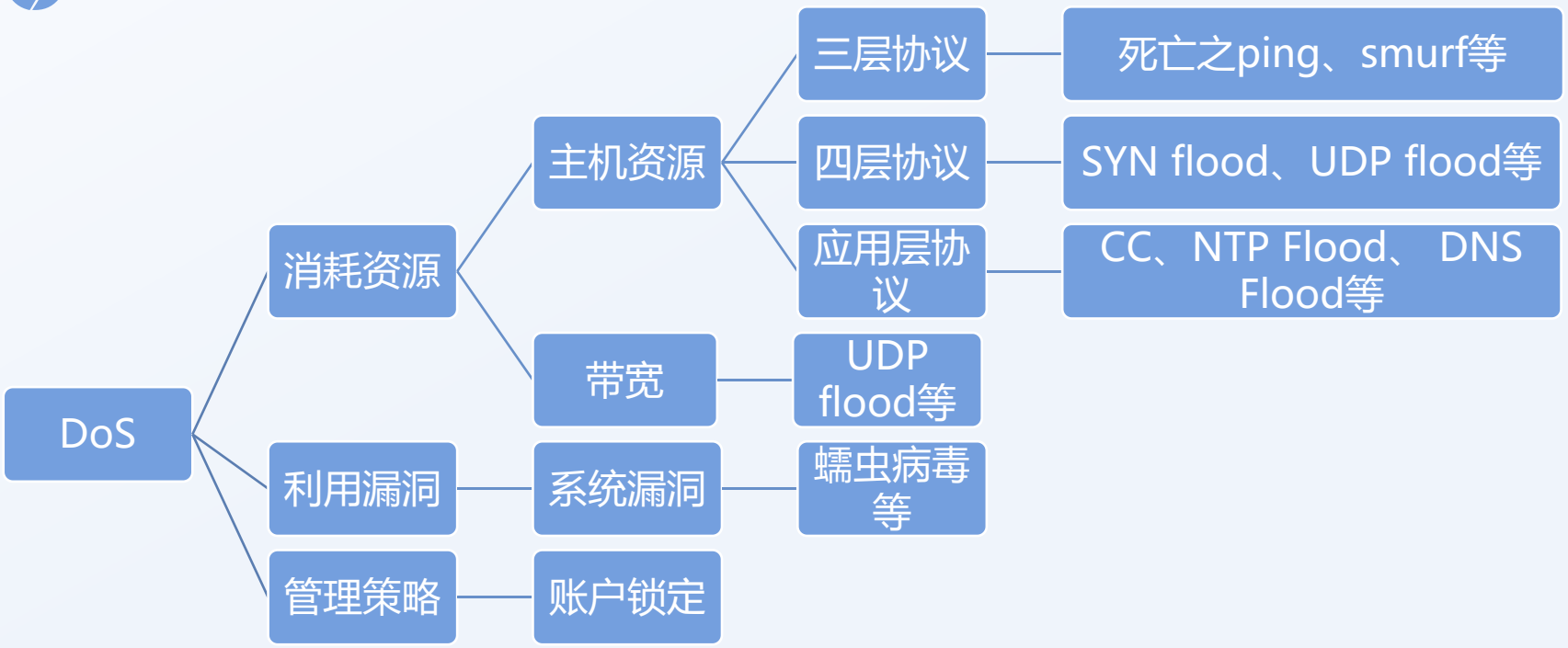
节点设备、终端设备，还可以针对线路

特点

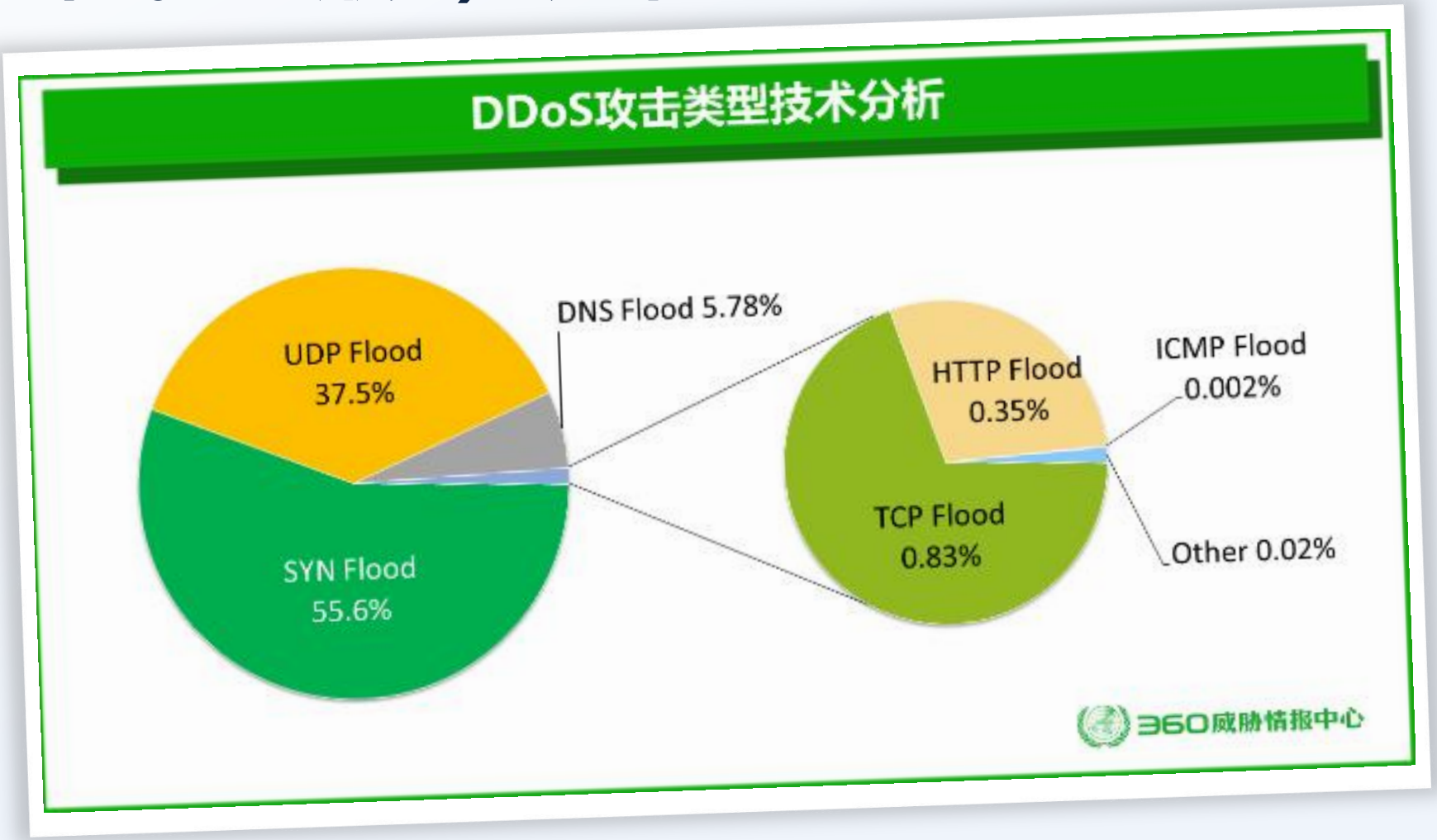
实时性

2.7.1 DDoS （分布式拒绝服务）攻击

DoS攻击的分类

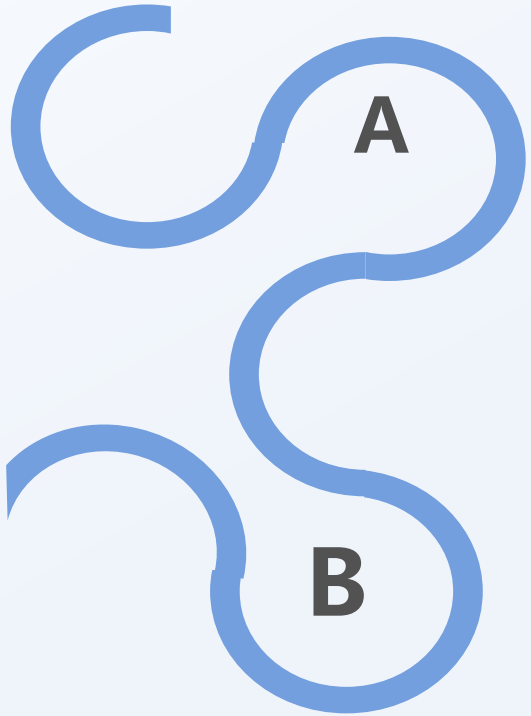


2.7.1 DDoS （分布式拒绝服务）攻击



2.7.1 DDoS （分布式拒绝服务）攻击

DoS攻击的分类



以消耗目标主机的可用资源为目的

死亡之ping、SYN洪水攻击、Land攻击、泪珠攻击等

以消耗链路的有效带宽为目的

UDP洪水攻击、Smurf攻击

2.7.1 DDoS （分布式拒绝服务）攻击

死亡之Ping

- 是由于单个包的长度超过了ICMP协议规范所规定的长度，从而导致操作系统崩溃的攻击。
- 防御：更新操作系统协议栈。

ICMP洪水攻击

- 向目标主机长时间、连续、大量的ping包，来减慢主机的响应速度和阻塞目标网络。
- 防御：对防火墙进行配置，阻断icmp协议的ECHO报文。

2.7.1 DDoS （分布式拒绝服务）攻击

泪珠攻击的原理

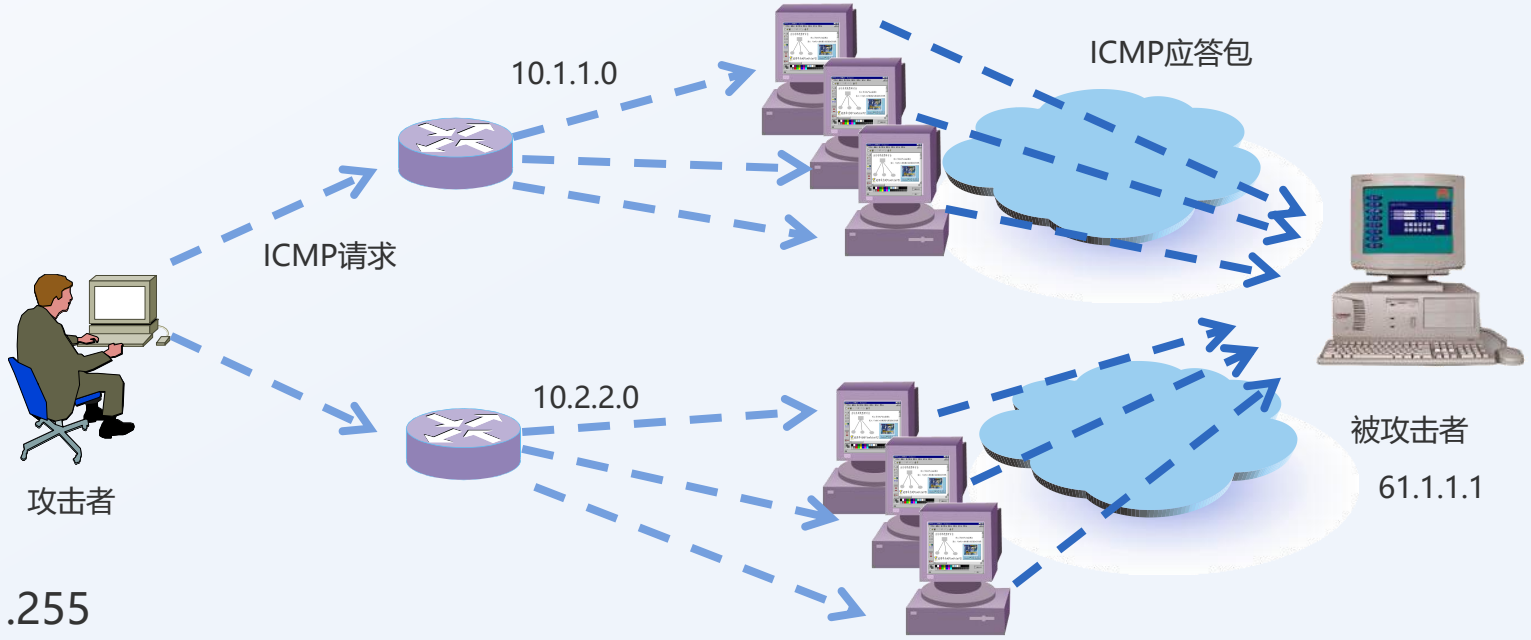
泪珠攻击（Tear Drop）：利用IP数据包分片重组时候，数据重叠，操作系统不能恰当处理，而引起的系统性能下降的攻击行为。

防御：更新操作系统协议栈。

2.7.1 DDoS （分布式拒绝服务）攻击

Smurf 攻击原理

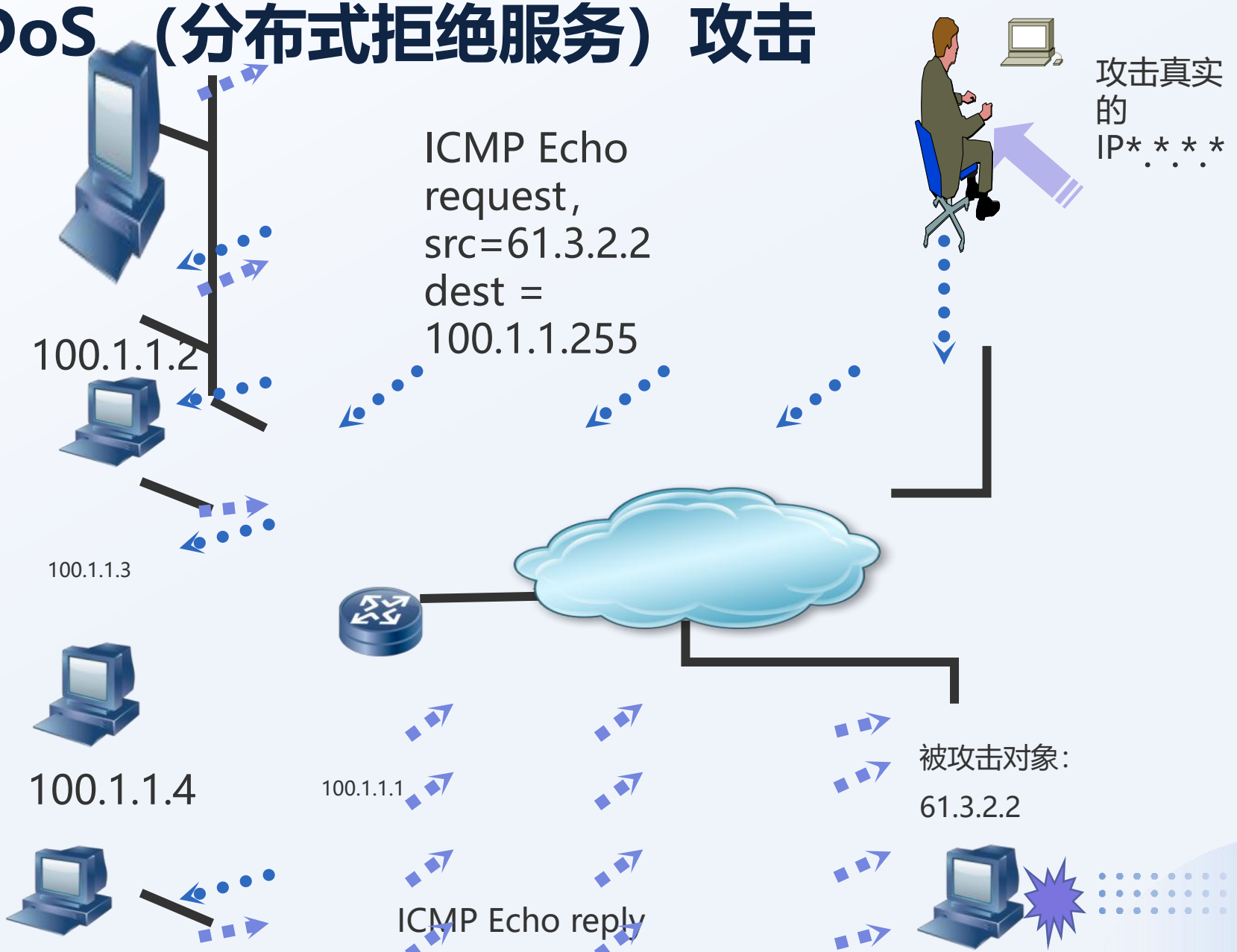
伪造Ping包的源IP：61.1.1.1



Ping 10.1.1.255
Ping 10.2.2.255

Smurf 攻击

2.7.1 DDoS（分布式拒绝服务）攻击

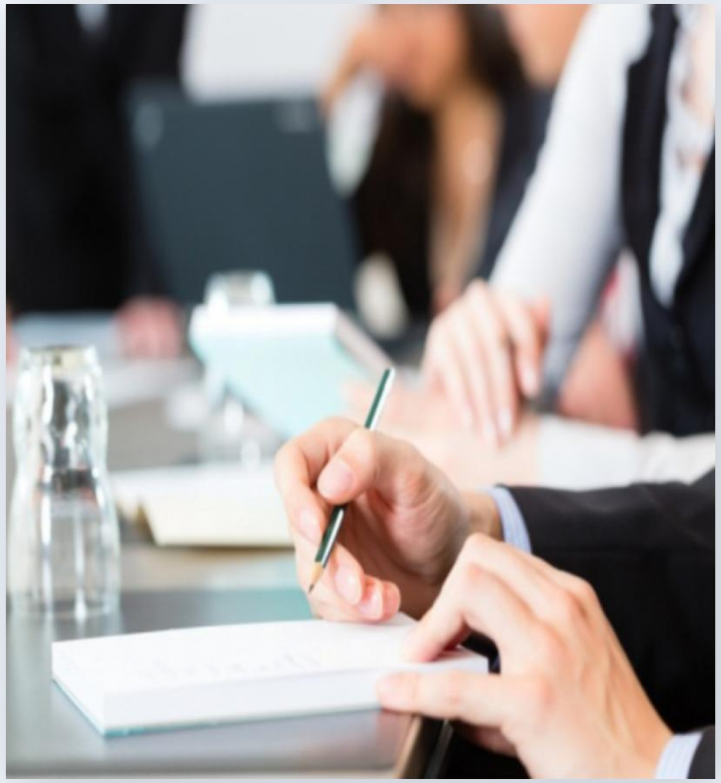


2.7.1 DDoS （分布式拒绝服务）攻击

Smurf 攻击的防御

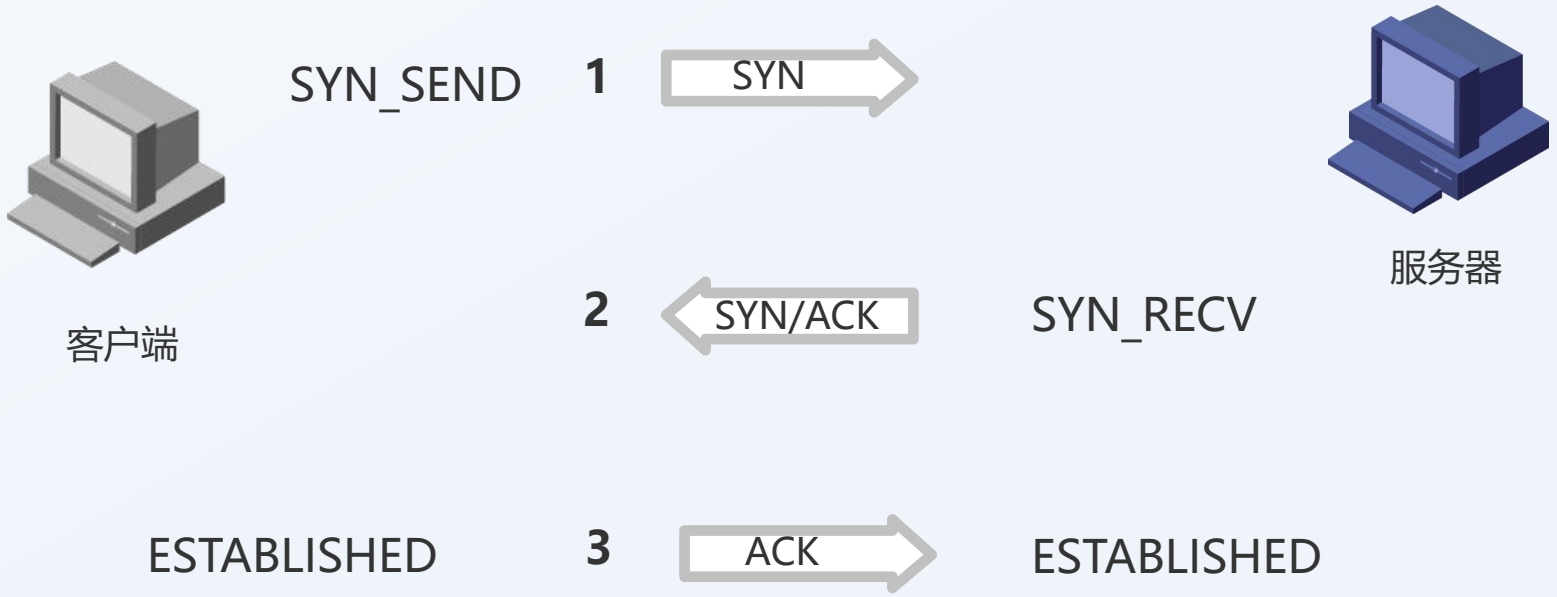
路由器接口不允许ping一个广播域。比如cisco路由器的接口默认no ip directed-broadcast

可以使用路由器的访问控制列表，保证内部网络中发出的所有信息都具有合法的源地址。



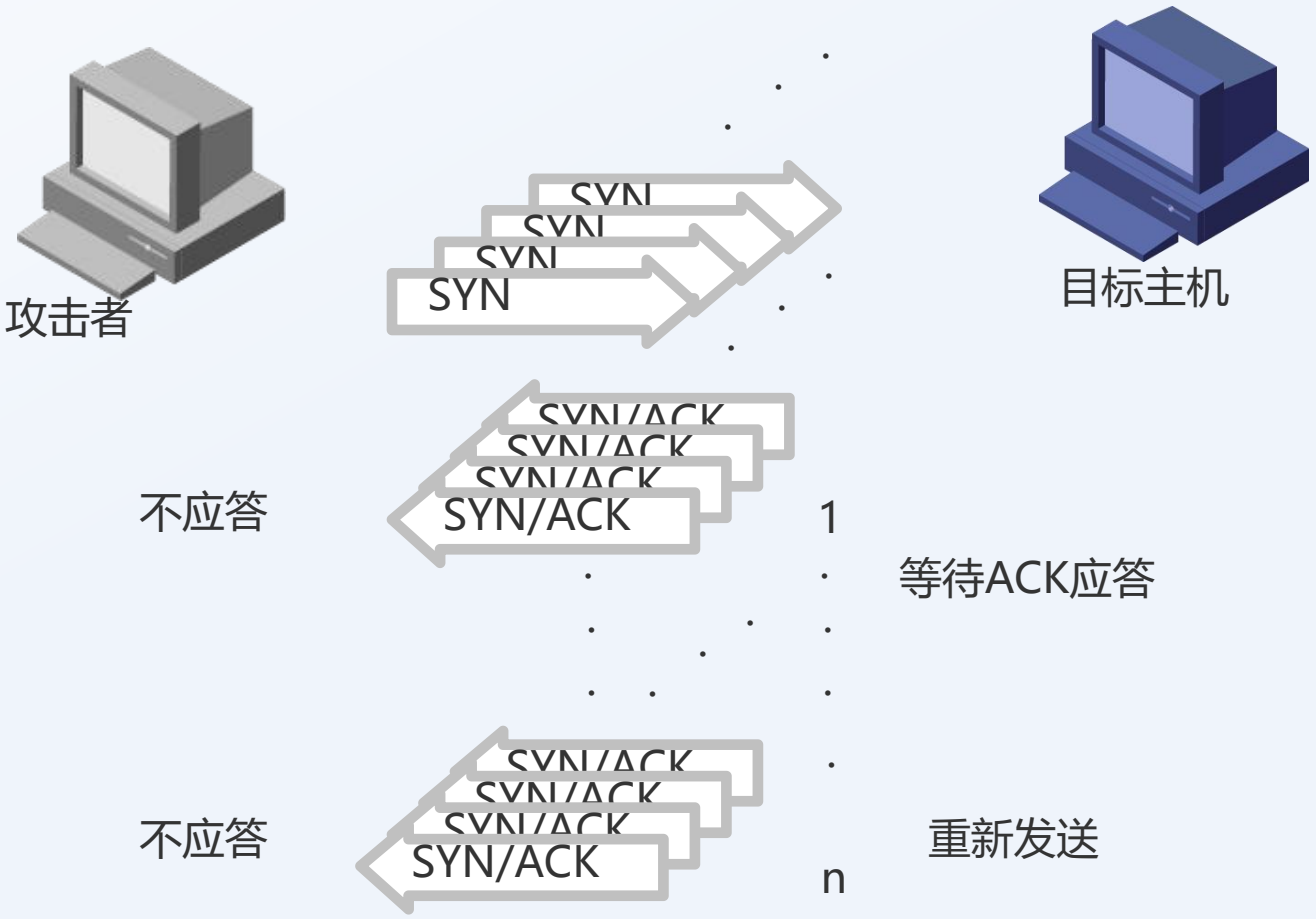
2.7.1 DDoS （分布式拒绝服务）攻击

TCP三次握手的原理



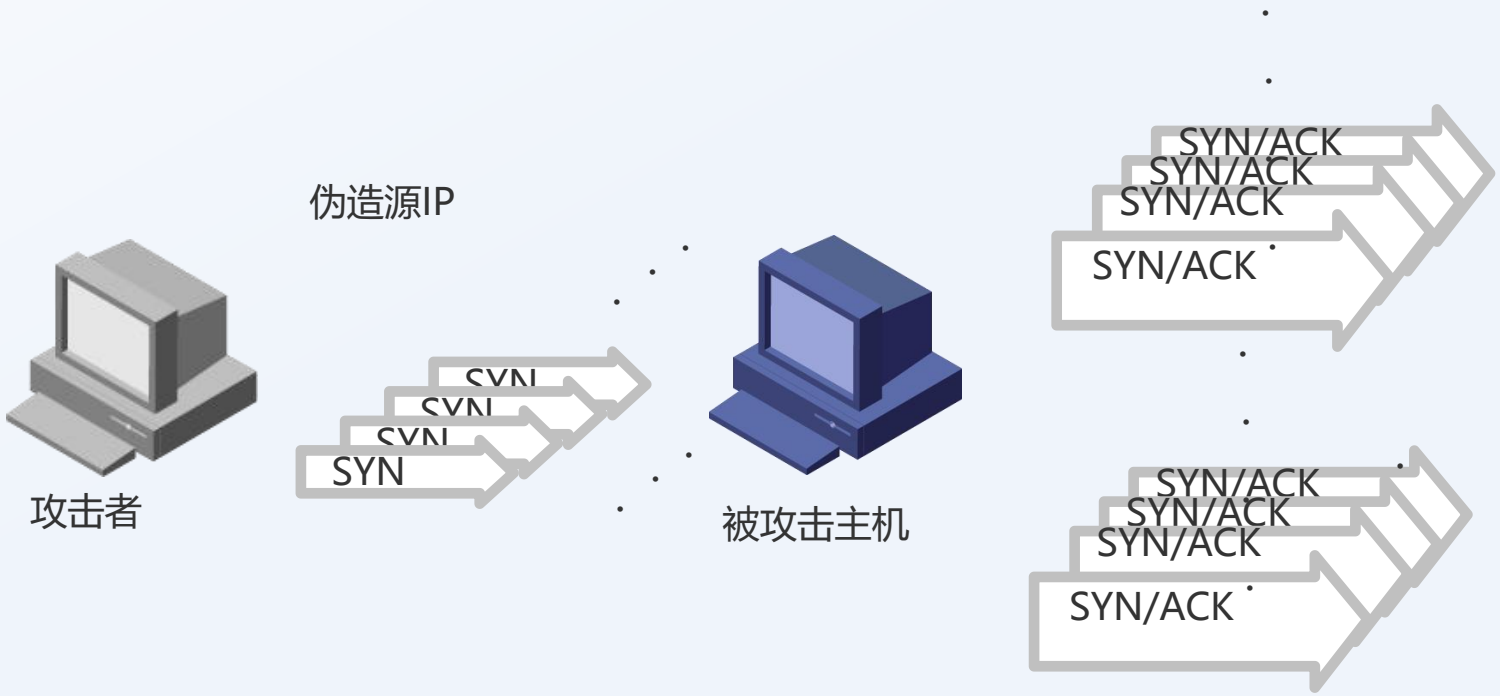
2.7.1 DDoS（分布式拒绝服务）攻击

SYN 洪水攻击—1



2.7.1 DDoS （分布式拒绝服务）攻击

SYN 洪水攻击—2



2.7.1 DDoS （分布式拒绝服务）攻击

以windows 为例SYN攻击

	花费时间（秒）	累计花费时间（秒）
第1次，失败	3	3
尝试第1 次，失败	6	9
尝试第2 次，失败	12	21
尝试第3 次，失败	24	45
尝试第4 次，失败	48	93
尝试第5 次，失败	96	189

2.7.1 DDoS （分布式拒绝服务）攻击

SYN洪水攻击案例

2.7.1 DDoS （分布式拒绝服务）攻击

Land攻击的原理

Land攻击是一种特别SYN攻击，把攻击包的源IP地址和目标IP地址都被设置成被攻击目标的地址。