异常包攻击原理及入侵检测配置

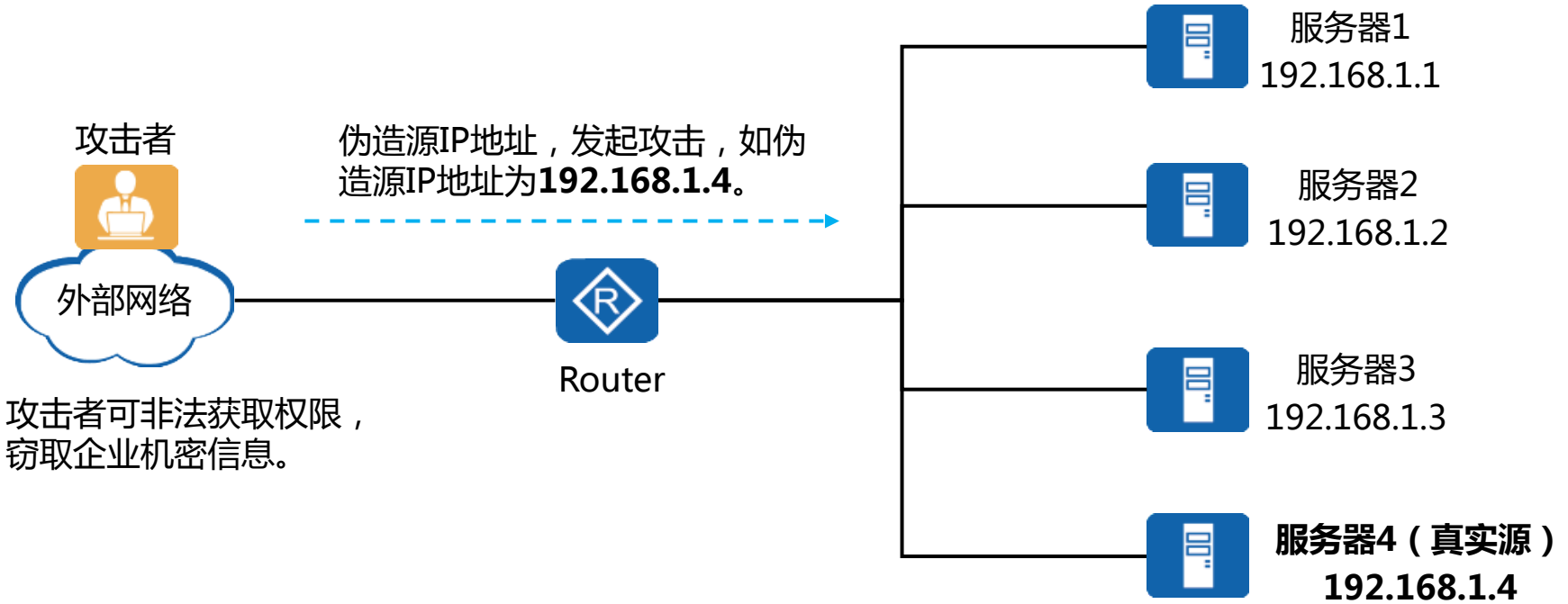
常见报文攻击

畸形报文攻击	特殊报文攻击
Smurf攻击	超大ICMP报文攻击
Land攻击	ICMP重定向报文攻击
Fraggle攻击	ICMP不可达报文
IP分片报文攻击	Tracert报文攻击
IP欺骗攻击	带源路由选项的IP报文攻击
Ping of Death攻击	带路由记录项的IP报文攻击
TCP报文标志位攻击	带时间戳选项的IP报文攻击
Teardrop攻击	

1 畸形报文攻击

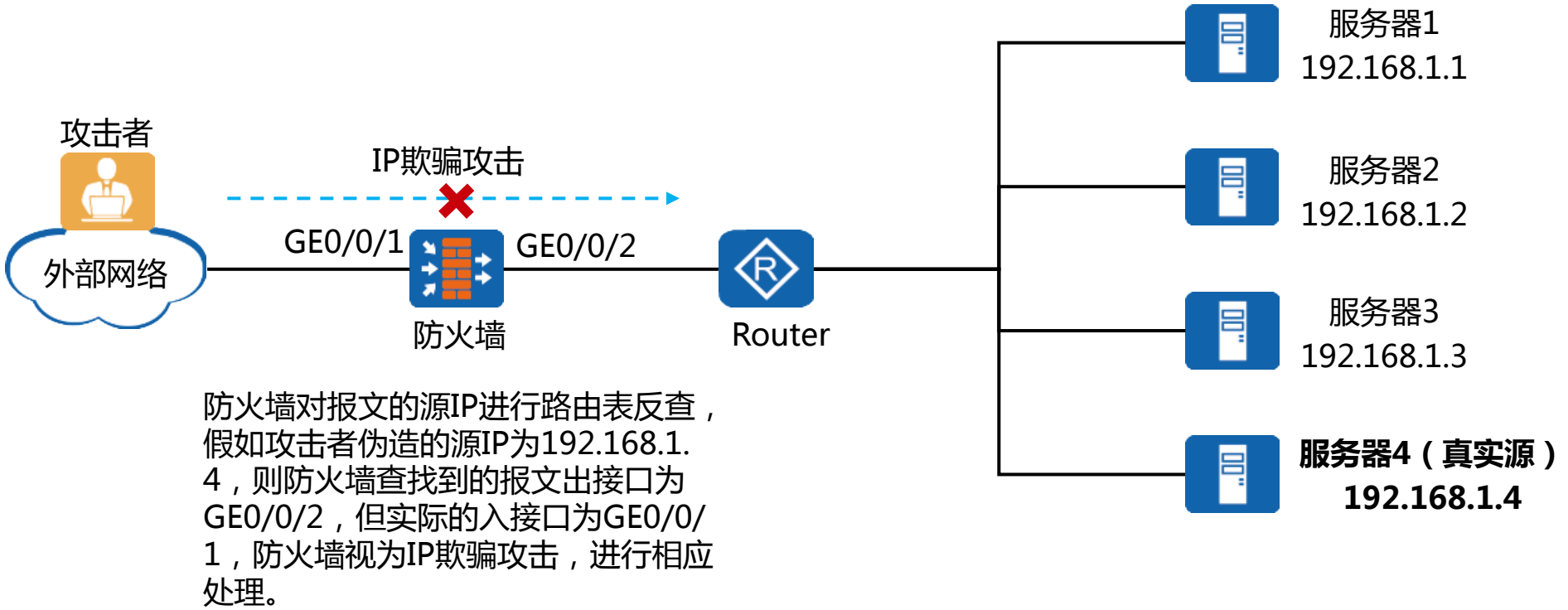
IP欺骗攻击原理

- IP欺骗攻击是一种常用的攻击方法，同时也是其他攻击方法的基础。攻击者通过向目标主机发送源IP地址伪造的报文，欺骗目标主机，从而获取更高的访问和控制权限。该攻击危害目标主机的资源，造成信息泄漏。



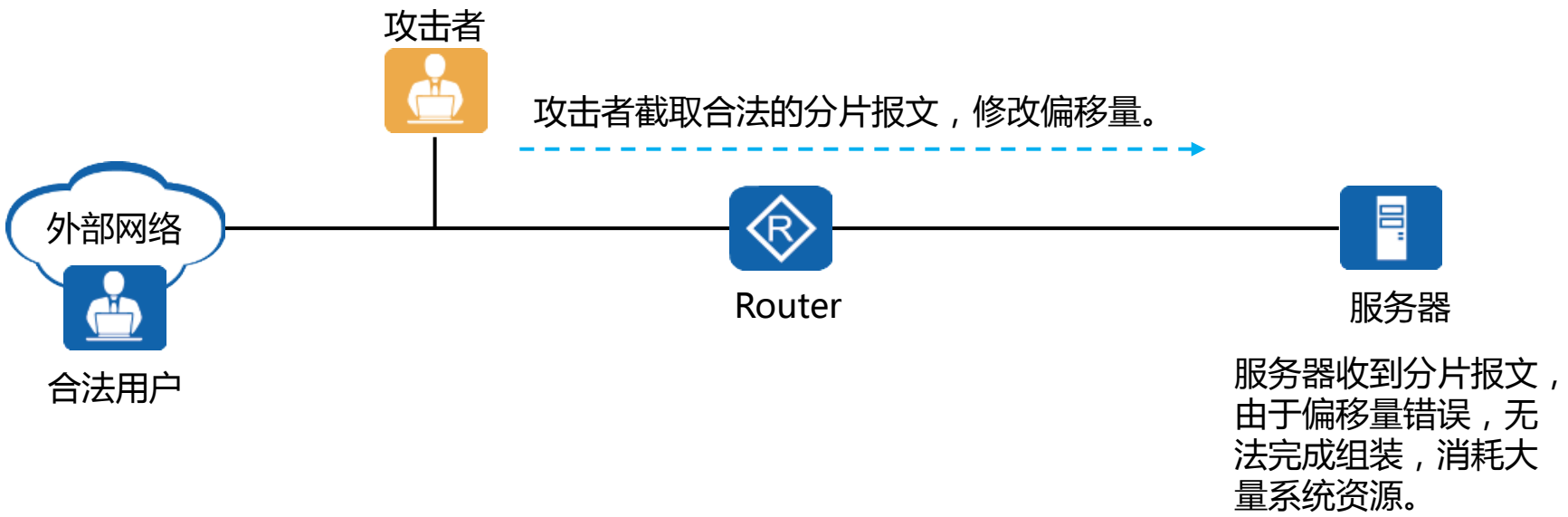
IP欺骗攻击防范原理

- 启用IP欺骗攻击防范后，设备对报文的源IP地址进行路由表反查，检查路由表中到源IP地址的出接口和报文的入接口是否一致。如果不一致，则视为IP欺骗攻击，并根据配置的动作处理该数据包。



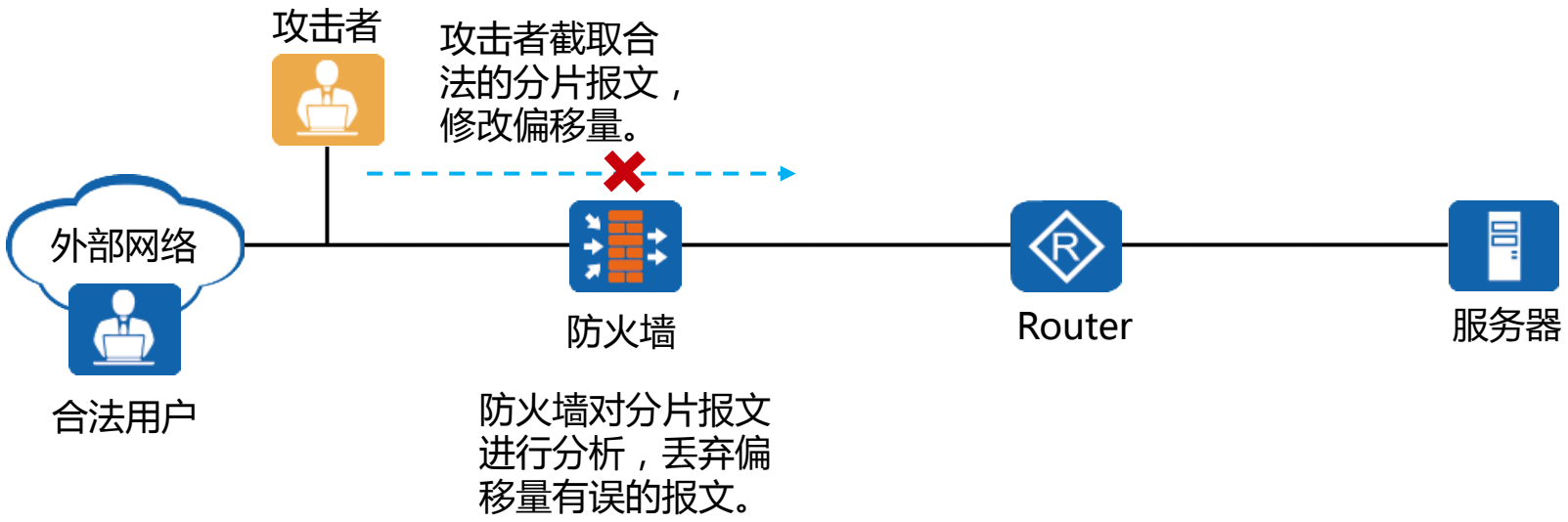
Teardrop攻击原理

- 为满足链路层MTU的要求，一些大的IP报文在传送过程中需要进行分片，被分片的报文在IP报头中会携带分片标志位和分片偏移量。如果攻击者截取分片报文后，对其中的偏移量进行修改，则数据接收端在收到分片报文后，无法组装为完成的数据包。接收端会不断进行尝试，消耗大量系统资源。



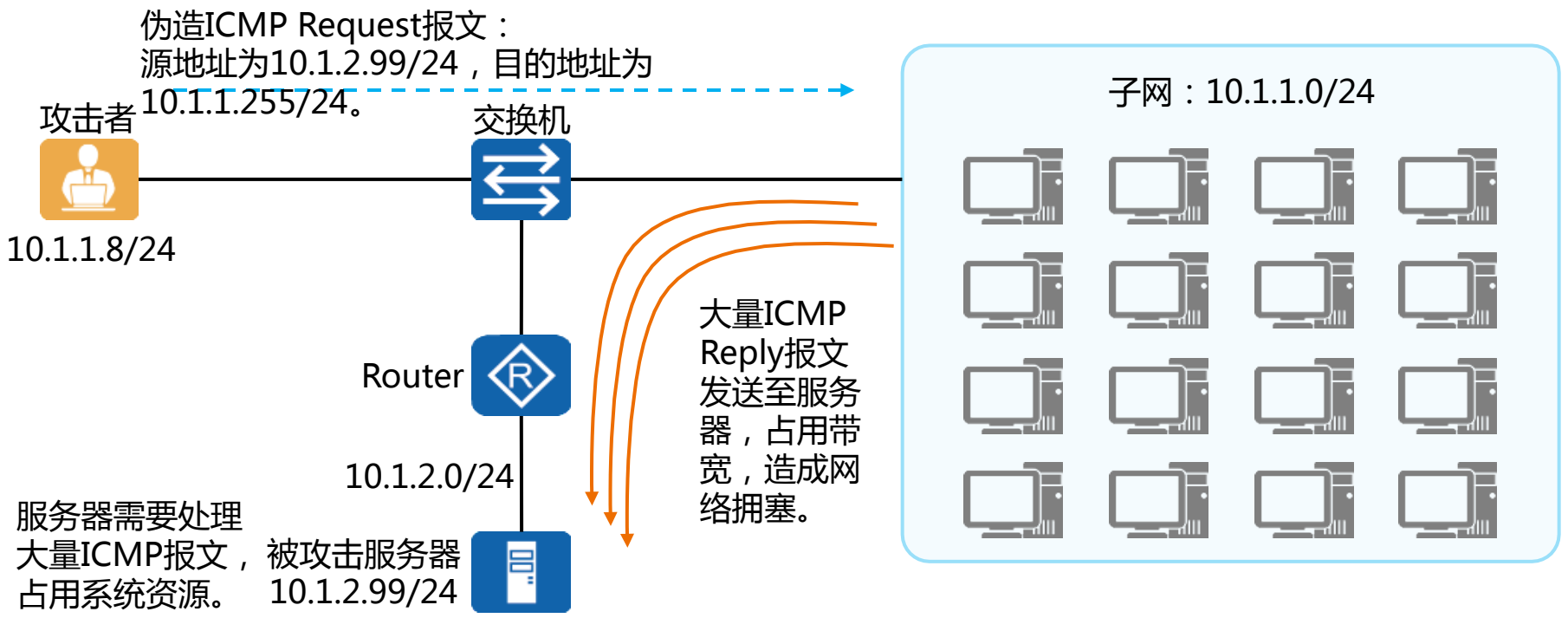
Teardrop攻击防范原理

- 启用Teardrop攻击防范后，设备会对接收到的分片报文进行分析，计算报文的偏移量是否有误。如果有误则直接丢弃该报文，并记录攻击日志。



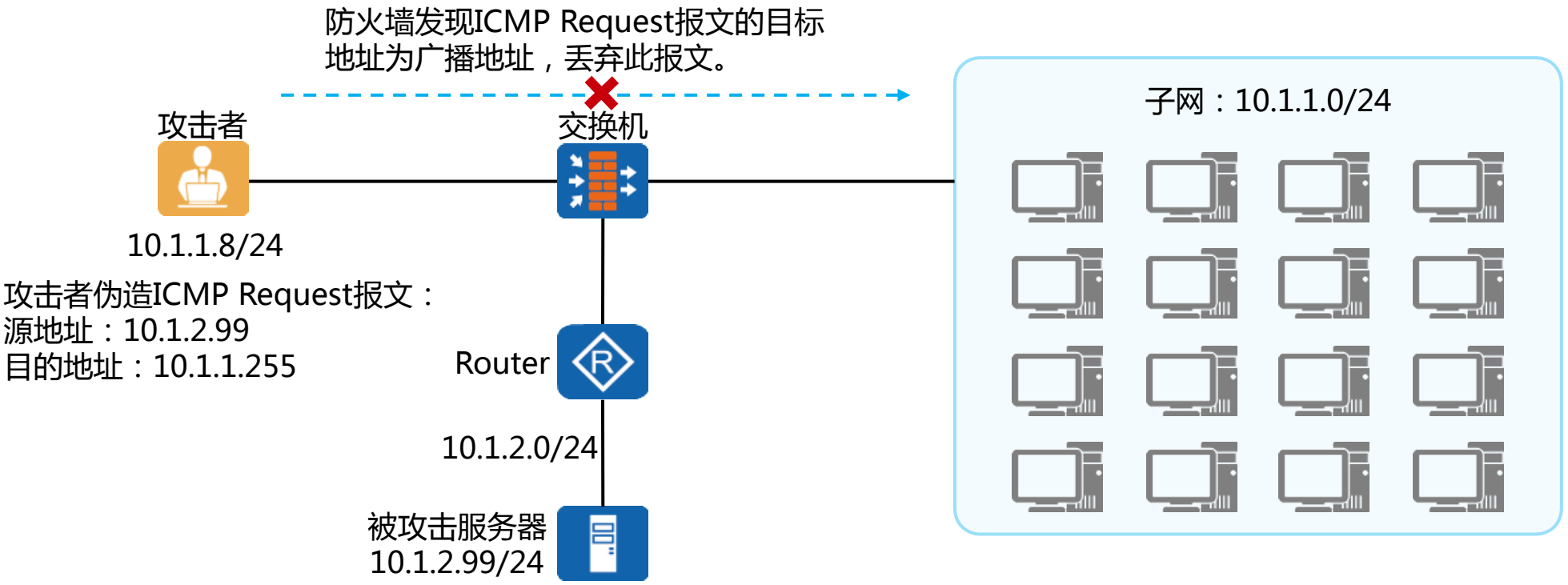
Smurf攻击原理

- 攻击者并不直接攻击目标服务器，而是通过伪造大量ICMP请求报文来实施网络攻击。伪造报文的源地址是被攻击服务器的地址，目的地址是某一个网络的广播地址，从而会造成大量主机向被攻击服务器发送ICMP应答报文，消耗网络带宽资源和服务器系统资源。此类攻击称为Smurf攻击。



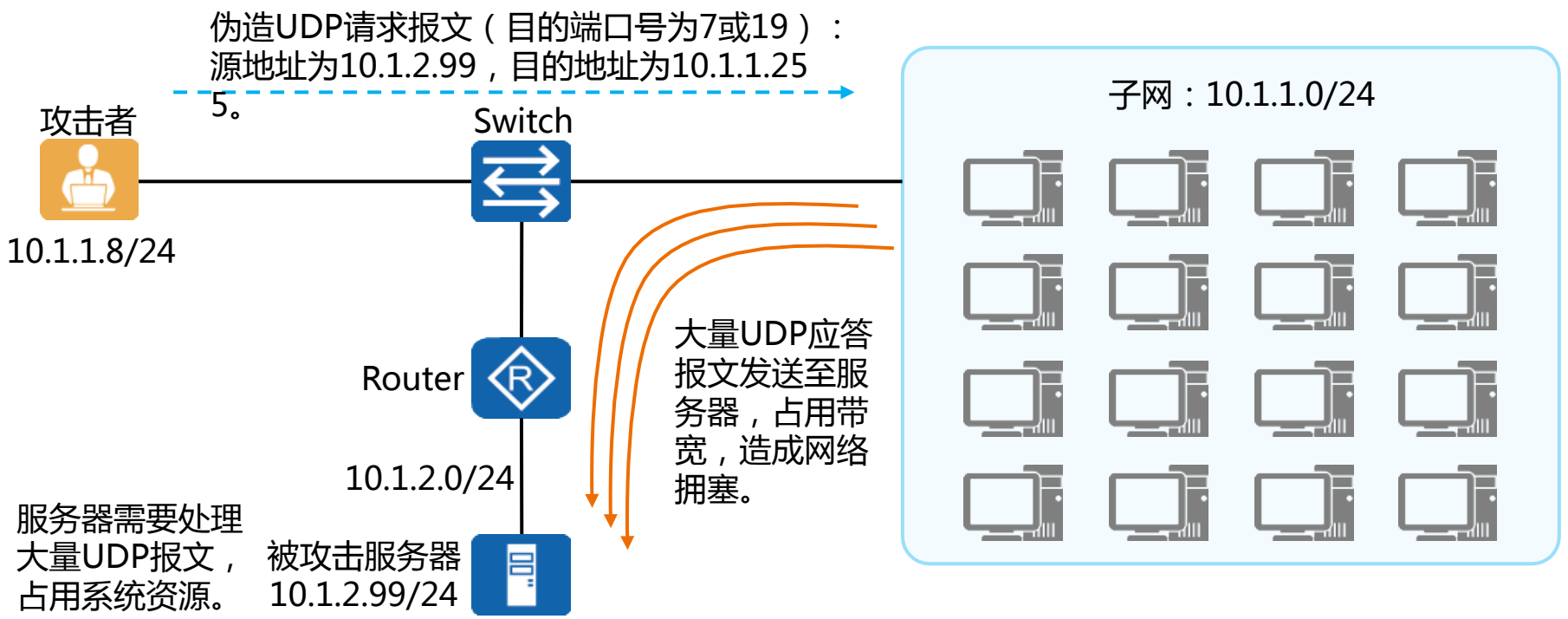
Smurf攻击防范原理

- 启用Smurf攻击防范后，防火墙会检查ICMP请求报文的目的地址是否为广播地址（即主机位全1）或网络地址（即主机位全0）。如果是则丢弃该报文，并记录攻击日志。



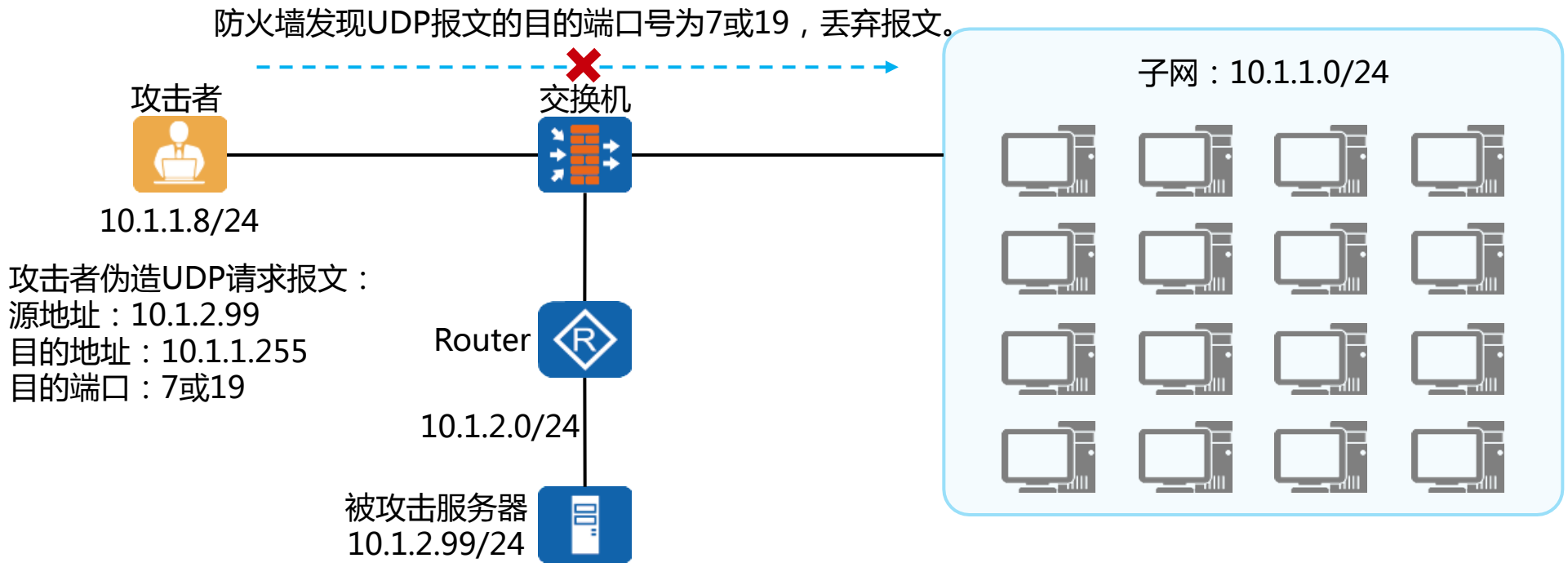
Fraggle攻击原理

- 类似于Smurf攻击，攻击者通过伪造大量UDP请求报文（目的端口号为7或19）来实施网络攻击。伪造报文的源地址是被攻击服务器地址，目的地址是某一个网络的广播地址，从而会造成大量主机向被攻击服务器发送UDP应答报文，消耗网络带宽资源和服务器系统资源。此类攻击称为Fraggle攻击。



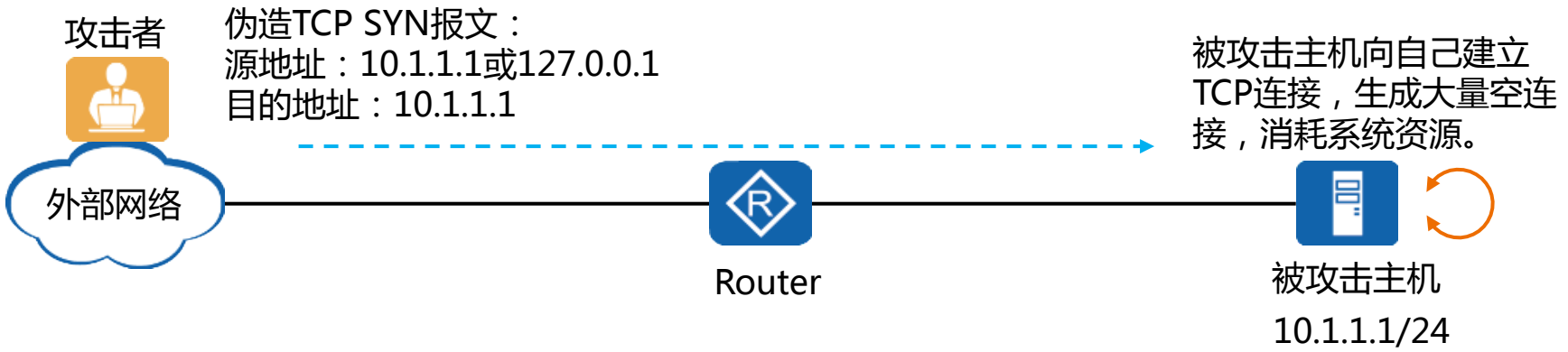
Fraggle攻击防范原理

- 启用Fraggle攻击防范后，设备会对收到的UDP报文进行检测。若目的端口号为7或19，设备拒绝该报文，并记录攻击日志。



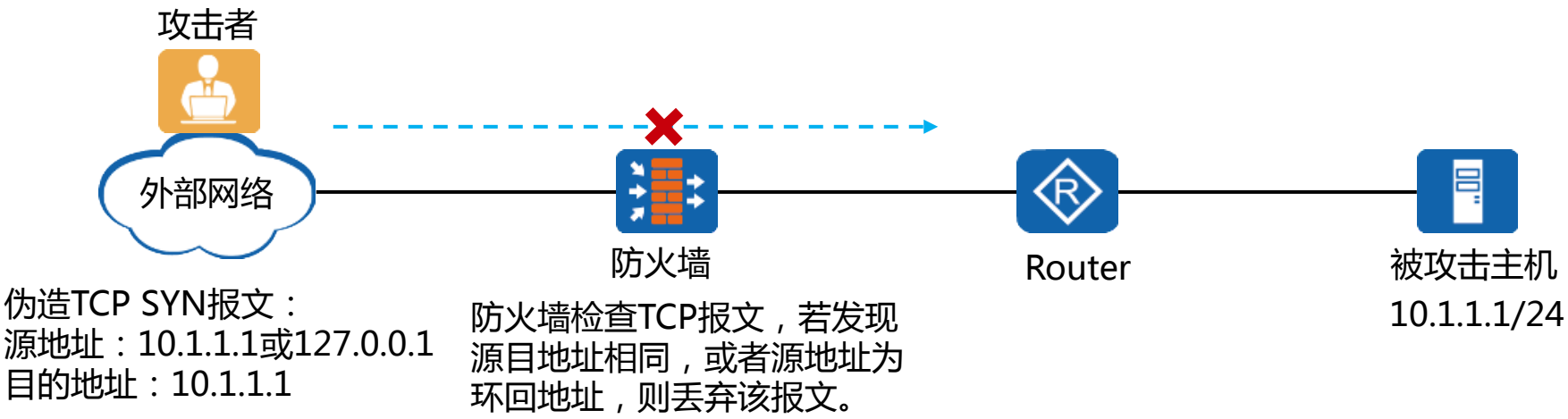
Land攻击原理

- 攻击者伪造TCP SYN数据包发送至被攻击主机，伪造报文的源地址和目的地址相同，或者源地址为环回地址（即127.0.0.0/8），导致被攻击主机向自己的地址发送SYN-ACK消息，产生大量的TCP空连接，消耗主机系统资源。此类攻击称为Land攻击，又称为环回攻击。



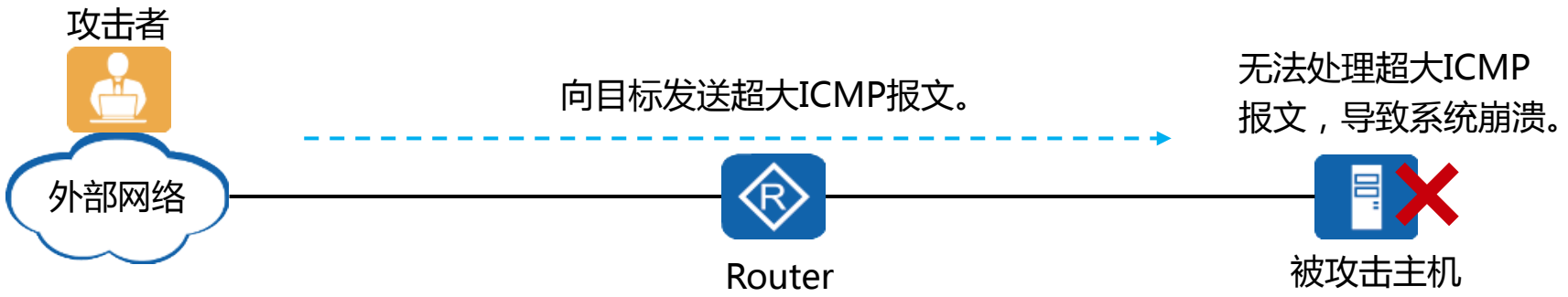
Land攻击防范原理

- 防火墙启用环回攻击防范后，设备会检查TCP报文的源地址和目的地址是否相同，或者TCP报文的源地址是否为环回地址。如果是则丢弃该报文，并记录攻击日志。



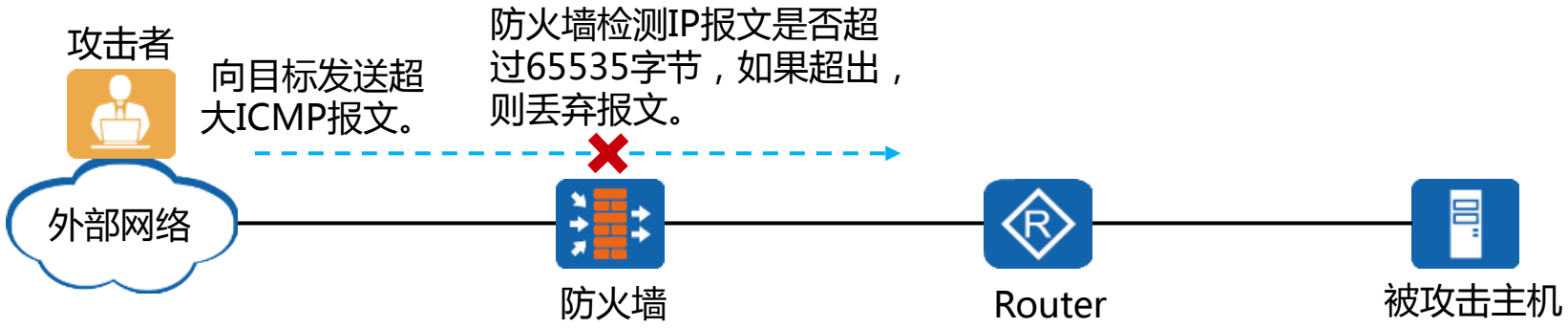
Ping of Death攻击原理

- IP报文的长度字段为16位，即IP报文的最大长度为65535字节。Ping of Death利用一些长度超大的ICMP报文对系统进行攻击。
- 对于某些网络设备或主机系统，在接收到超大ICMP报文后，由于处理不当，会造成系统崩溃、死机或重启。



Ping of Death攻击防范原理

- 防火墙启用Ping of Death攻击防范后，设备会检测IP报文的大小是否大于65535字节，对大于65535字节的报文直接丢弃，并记录攻击日志。



2 特殊报文攻击

ICMP不可达报文攻击原理

- 不同的系统对ICMP不可达报文的处理方式不同，有的系统在收到网络或主机不可达的ICMP报文后，对后续发往此目的地址的报文直接认为不可达，从而断开正常的业务连接。攻击者利用这一点，伪造不可达ICMP报文，切断受害者与目的地的连接，造成攻击。