火龙果•整理
uml.org.cn

ChinaDDOS Anti-DDOS Service
高级防御策略使用说明

中国DDOS防御实验室

目　　录

引　言.....3
1 常用名称解释.....4
1.2　Bit.....4
1.4　bps.....4
1.5　Bps.....4
1.6　pps － 包转发率.....4
2 网络常用传输协议.....5
2.1　TCP.....5
2.2　UDP.....5
2.3　ICMP.....5
3 网络中常见的攻击的种类.....6
3.1　Syn 攻击.....6
3.2　UDP 攻击.....6
3.3　ICMP 攻击.....6
3.4　CC 攻击.....6
3.5　洪水攻击.....6
4 各类数据包组成介绍.....7
4.1　IP 首部.....7
4.2　UDP 首部.....7
4.3　TCP 首部.....8
4.4　ICMP 首部.....8
5 高级防御策略使用说明.....8
5.1　刷新.....9
5.2　新增规则.....9
5.2.1　IP 包部首内容.....10
5.2.2　TCP 包部首内容.....14
5.2.3　UDP 包部首内容.....19
5.2.4　ICMP 包部首内容.....20
5.2.5　处理方式.....22
5.2.6　选择逻辑关系.....23
5.3　删除规则.....23
5.4　规则属性.....24
5.5　清空所有规则.....24
5.6　降低优先级、提高优先级别.....24

引　言

1 常用名称解释

在介绍高级防御策略使用功能之前，首先对要求用户了解一定的 TCP/IP 协议的一些相关知识。以下就针对该相关知识进行阐述。

1.2 Bit

电脑记忆体中最小的单位，在二进位电脑系统中，每一 bit 可以代表 0 或 1 的数位讯号。

1.3 Byte

字节单位，一般表示存储介质大小的单位，一个 B（常用大写的 B 来表示 Byte）可代表一个字元(A~Z)、数字(0~9)、或符号(,.?!%&+-*/)，但中文字需要 2 个 Byte。

1 Byte = 8 bits
1 KB = 1024 Bytes
1 MB = 1024 KB
1 GB = 1024 MB
在计算存储介质大小时，需要用 2 的 n 次方来换算（1KB = 2^10 Bytes）。

1.4 bps

“bits per second”常用于表示数据机及网络通讯的传输速率。

1.5 Bps

“Byte per second”电脑一般都以 Bps 显示速度，但有时会跟传输速率混淆，例如 ADSL 宣称的带宽为 1Mbps ，但在实际应用中，下载速度没有 1MB ，只有 1Mbps/8 = 128kBps
也就是说与传输速度有关的 b 一般指的是 bit。
与容量有关的 B 一般指的是 Byte。

1.6 pps – 包转发率

包转发率标志了交换机转发数据包能力的大小。单位一般位 pps（包每秒），一般交换机的包转发率在几十 Kpps 到几百 Mpps 不等。包转发速率是指交换机每秒可以转发多少百万个数据包（Mpps），即交换机能同时转发的数据包的数量。
包转发率以数据包为单位体现了交换机的交换能力。例如：
1 个千兆端口的线速包转发率是 1.4881MPPS,
百兆端口的线速包转发率是 0.14881MPPS，这是国际标准，但是如何得来的呢？
具体的数据包在传输过程中会在每个包的前面加上 64 个（前导符）preamble 也就是

一　个 64 个字节的数据包，

原本只有 512 个 bit,但在传输过程中实际上会有 512+64+96=672bit,也就是这时一个数据包的长度实际上是

有 672bit 的千兆端口线速包转发率=1000Mbps/672=1.488095Mpps，约等于 1.4881Mpps,　兆除于 10 为 0.14881Mpps

那么以后很简单了，其实直接用设备参数中的 pps 数值乘以 672 那么就转化成我们比较能理解的大众化的 bps 概念了。

2 网络常用传输协议

网络传输过程中主要分为 TCP（传输控制协议）、UDP（用户数据报协议）、ICMP（Ineternet 控制报文协议）、等主要的传递方式。

2.1　TCP

提供一种面向连接的、可靠的字节流服务。TCP 传输的方式是采取三次握手　　的方式。由发送端象目的端发送一个连接请求，目的端再回应请求端的连接　　请求，此时发送端再次确认连接请求过程。

TCP 包主要包括网页浏览等网络操作内容

2.2　UDP

是一个简单的面向数据包的运输层协议。UDP 把应用程序传给 IP 层的数据发送，但是并不保证他们能到达目的地。

UDP 包主要包括 QQ、聊天室等这类网络操作形式。

2.3　ICMP

它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

3 网络中常见的攻击的种类

3.1 Syn 攻击

SYN 攻击是利用 TCP 协议的三次握手的漏洞进行攻击。如同上述介绍。在正常情况下，一次 TCP 连接需要完成三次握手的情况下实现。而 SYN 攻击是通过伪造大量的虚假 IP，在向服务器端发送连接请求。当服务器端接　　收到请求并给予回应时，由于客户端访问 IP 都是伪造 IP，因此无法回应服务器的连接。以至于服务器端在等待大量回复信息而消耗服务器的使用资源，最后导致系统繁忙而无法响应正常的服务连接请求。

3.2 UDP 攻击

UDP 是一种无连接的协议，而且它不需要用任何程序建立连接来传输数据。当攻击者随机地向受害系统的端口发送 UDP 数据包的时候，就可能发生了 UDP 淹没攻击。当受害系统接收到一个 UDP 数据包的时候，它会　　确定目的端口正在等待中的应用程序。当它发现该端口中并不存在正在等待的应用程序，它就会产生一个目的地址无法连接的 ICMP 数据包发送给该伪造的源地址。如果向受害者计算机端口发送了足够多的 UDP 数据包的时候，整个系统就会瘫痪。

3.3 ICMP 攻击

可以利用操作系统规定的 ICMP 数据包最大尺寸不超过 64KB 这一规定，向主机发起“Ping of Death”（死亡之 Ping）攻击。“Ping of Death” 攻击的原理是：如果 ICMP 数据包的尺寸超过 64KB 上限时，主机就会出现内存分配错误，导致 TCP/IP 堆栈崩溃，致使主机死机。

3.4 CC 攻击

CC 主要是用来攻击页面的。大家都有这样的经历，就是在访问论坛时，如果这个论坛比较大，访问的人比较多，打开页面的速度会比较慢，对不？！ 一般来说，访问的人越多，论坛的页面越多，数据库就越大，被访问的频率也越高，占用的系统资源也就相当可观。当 CC 攻击模拟成百上千的用户同时去访问页面数据库资源时，足以消耗服务器的使用资源而是正常用户无法访问。

3.5 洪水攻击

之前的攻击方式都是以各类协议的漏洞进行攻击，从而造成服务器资源的耗尽，使正常用户无法进行访问。而达到拒绝服务器的目的。但随着服务器硬件设备的提高和防御手段的加强，同时攻击机器的攻击能力也得到了加强，原有的服务器资源损耗方式逐步转变为带宽资源损耗的拒绝服务。洪水攻击方式就是利用更多的资源进行攻击从而沾满被攻击者的网络

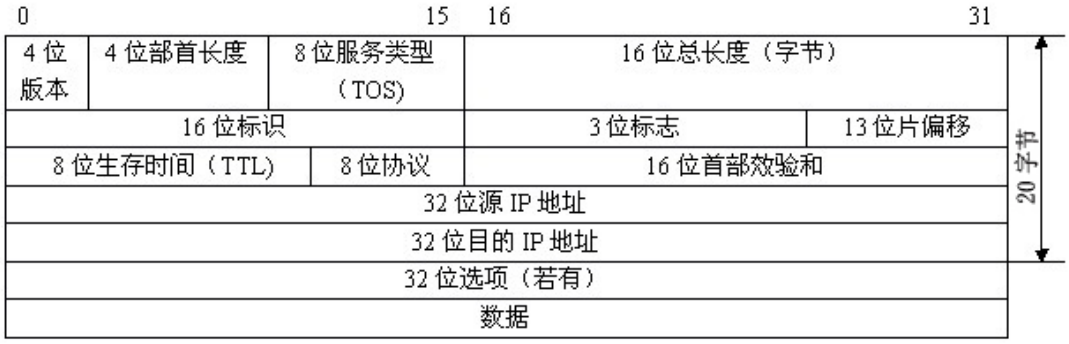
带宽资源，同样使正常用户因访问带宽被沾满的情况下无法访问到服务器。

注：洪水攻击并不是泛指一种攻击，它既可以是 syn 攻击也可以是 UDP 攻击，甚 至是多种混合型攻击。攻击者通过加大对被攻击者的数据流量从而达到拒绝服务的目的。

4 各类数据包组成介绍

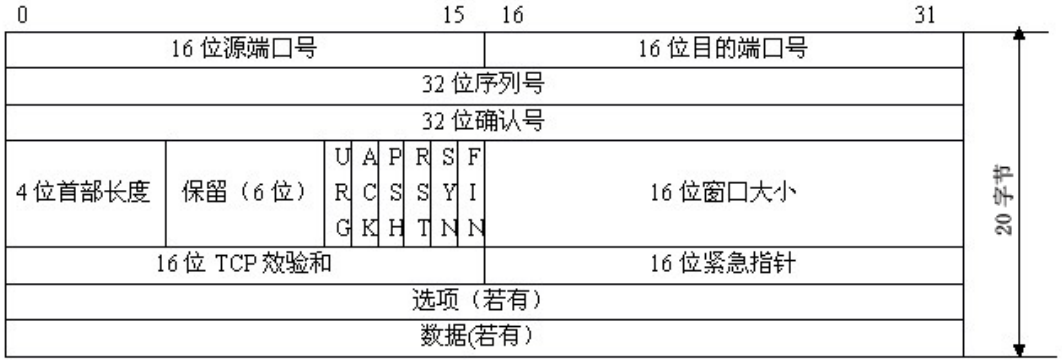
针对 IP 协议、TCP 协议、UDP 协议以及 ICMP 协议的网络是数据包作一个简单介绍。

4.1 IP 首部



4.2 UDP 首部

4.3 TCP 首部



4.4 ICMP 首部

0	15	16	31	
8 位类型	8 位代码	效验和		8字节
标识符		序列号		
数据（若有）				

5 高级防御策略使用说明

在介绍完以上的部分基础知识以后，将对 ChinaDDOS 防火墙的高级防御规则作详细介绍。

高级防御策略是在《安全配置中心》——《高级防御策略》

单击高级防御策略库见下图

在高级防御策略库中有以下几个功能按钮：

5.1 刷新

单击刷新当前高级防御策略库中的所有策略内容

5.2 新增规则

单击新增规则可以制定高级防御规则策略。如下图

新增规则窗口中分为过滤数据包的类型、处理方式以及逻辑关系三种。

过滤数据包类型：是分为 IP/TCP、IP/UDP、IP/ICMP 等三种数据包的处理，针对于不同的数据包分别有不同的策略条件。

5.2.1 IP 包部首内容

窗口内容中，左侧是属于 IP 包部首内容。如下图

右侧则显示 TCP、UDP、ICMP 的包部首内容后面将会详细介绍。

5.2.1.1 源 MAC 地址

指 IP 包部首包含发送端的硬件地址。

5.2.1.2 目的 MAC 地址

指 IP 包部首中含由 48 比特长(6 字节),16 进制的数字组成的接收端的硬件地址。

注:

1. MAC 地址是指的网卡的物理地址，它如同我们身份证上的号码是具有唯一性，但是可以通过软件的方式进行修改。
2. MAC 地址是是由 48 比特长(6 字节),16 进制的数字组成.0-23 位叫做组唯一标志符。例如：44-45-53-54-00-00 表示一个硬件地址。
3. 该条件通常是用于控制受保护机器只接收或发送固定机器的 TCP 数据包。如果不填写 MAC 地址，则表示策略不受该条件的限制。

5.2.1.3 源 IP 地址

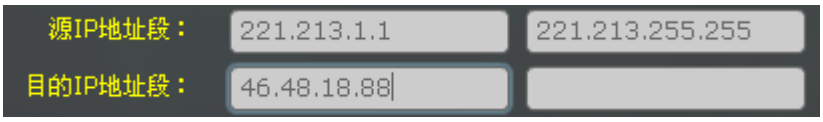
指 IP 包部首中含有发送端的网络 IP 地址地址。

5.2.1.4 目的 IP 地址

指 IP 包部首中含有接收端的网络 IP 地址地址。

注：

1. IP 地址是指互联网地址或 Internet 地址。是用来唯一标识互联网上计算机的逻辑地址。每台连网计算机都依靠 IP 地址来标识自己。就很类似于我们的电话号码样的。
2. IP 地址是由 4 个以小数点隔开的十进制整数。例如：202.130.11.211
3. 一般情况下，设置受保护的服务器的 IP 地址为目的地址，再通过其他的条件进行策略防御，这样可以实现每个单独服务器的安全使用策略。
4. 在源 IP 地址和目的 IP 地址栏中分别有两个数字填写框，改填写框主要是用于填写源 IP 和目的 IP 地址段的功能。如下图



表示：IP 包部首中还有 221.213.1.1 至 221.213.255.255 段内所有的 IP 在访问 46.48.18.88 的目的服务器时的条件。

5.2.1.5 IP 包长度

一个 IP 数据包最大可达 65535 字节。如果数据包的总长度大于大于这个数值，大多数链路层采取分片的形式进行数据传输。

注：

1. 分片攻击方式是有意将超过包的最大字节数。当机器碰到该类型的数据包时，原有的老系统会因为数据包的溢出而造成系统崩溃。现在的操作系统基本上都已经解决这个方面的问题。
2. IP 包长度填写方式如同 IP 地址的填写方式，输入一个包的最小最大的范围。通过填写包的长度，可以控制超出包长度的 IP 访问情况的处理。如下图

5.2.1.6 16 位的标识起始

标识起始更可以看作成一个数据包的身份证，也就是说每个数据包都具有唯一的 16 位标识起始内容。

注：一般情况下，正常数据包的标识是不一样的。如果发现大量相同的标识则可能是攻击伪造的标识的值，通过设置标识的值来防止这类攻击的出现。

5.2.1.7 生存时间

是指数据包在到达目的地址时所经过路由的数值。每经过一个路由初始数值减一，直到目的地或初始值为 0 则表示这个数据包的结束。. 当初始值减至为 0 时，则自动丢弃该数据包。

注：

1. 随着操作系统的不同生存时间初始值也不同。例如 windowsNT/2000系统的生存

时间（即 TTL 值）为128，Linux/Unix 操作系统的生存时间（即 TTL 值）为64/255，windows95/98操作系统的生存时间（即 TTL 值）为32。

2. 生存时间条件方式同上也是填写一个时间范围值。如下图

表示满足于 TTL 为0－255之间的数值条件的 IP 访问情况处理。

5.2.1.8 IP 部首长度

在网络传输过程中，用户数据都是采取封装的形式进行打包。而数据包在传递过程中时，需要建立一个类似于邮寄信件的封面内容，告诉邮递员该信件的一些基本内容（如：邮寄双方的地址——目的双方的 IP、经过的路程时限——TTL）情况，而这类数据都全部封装在 IP 首部内容中。

注：

1. 通常情况下 IP 部首长度为20字节，如果含有选项字段，则 IP 部首长度会大于20个字节。

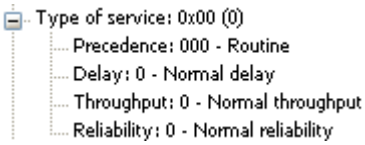
2. TCP 部首长度最少为20字节。

3. IP 部首长度作为策略条件同样也是采取的长度范围。如下图

同样可以通过定义 IP 部首长度条件进行相应的防御策略。

5.2.1.9 服务类型

字段包括一个3bit 的优先权字段，4bit 的 TOS 子字段分别代表：最小时延、最大吞吐量、最高可靠性和最小费用。如果所有4bit 均为0，则意味着是一般服务。不过现在大多数 TCP/IP 协议都不支持 TOS 特性。因此再这里将不再作过多介绍。用户仅作一般了解即可。如下图



5.2.1.10 分片标记

链路层具有最大传输单元 MTU 这个特性，它限制了数据帧的最大长度，不同的网络类型都有一个上限值。例如以太网的 MTU 是1500，一般 IP 首部为20字节，UDP 首部为8字节，数据的净荷（payload）部分预留是1500-20-8=1472字节。如果数据部分大于1472字节，就会出现分片现象。

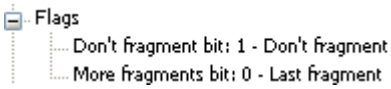
保留位(Reserved)：6位值域，这些位必须是0。为了将来定义新的用途所保留

不分片(Don't fragment bit)：如果数据包的不分片标记为1时，则表示该数据包

不分片，例如上例也就是说数据包的数据净荷小于1472个字节。（勾上则表示针对于不分片的数据包的设置条件）

分片(More fragments bit)：如果数据包的分片标记为1时，则表示该数据包进行分片处理。（勾上则表示针对于分片的数据包的设置条件）

实例见下图



改数据包不分片位置为1，则表示该数据包是一个完整的数据包内容。

注：如果是数据包的内容数据包过大，而采取分片的形式时，每个数据包都含有形同的标识字段内容，这样是为了当分片以后的数据包在到达目的地时，进行重组时以便让链路层了解到哪些分片内容是属于同一个数据包内容。除了最后一片外，其他的每个组成数据包的片都要把 more fragments bit 置1。

5.2.1.11 分片偏移

通过上面分片标记，我们了解到数据包的数据内容比较大的时候，数据包在传递过程中会采取分片的形式进行传输。而此时的问题就是当数据包达到目的地以后进行包的重组时，是如何将数据包内容按照何种顺序进行组合的呢？分片偏移就是数据包在重组时顺序的重要依据。

为了便于描述分片偏移情况，下面举例说明：在一个以太网上，数据帧的最大长度是1500字节，其中1472字节留给数据，假定 IP 首部为20字节，UDP 首部为8字节。我们分别以数据长度为1471、142、1473和1474字节运行 sock 程序。

```
Bsdi % sock -u -i -nl -w1471 svr4 discard
Bsdi % sock -u -i -nl -w1472 svr4 discard
Bsdi % sock -u -i -nl -w1473 svr4 discard
Bsdi % sock -u -i -nl -w1474 svr4 discard
```

输出结果如下：

```
1   0.0                    bsdi.1112 > svr4.discard : udp 1471
2   21.008303    (21.0083) bsdi.1114 > svr4.discard : udp 1472
3   50.449704   (29.4414) bsdi.1116 > svr4.discard : udp 1473 (frag 26304:1480@0
+)
4   50.450040    ( 0.0003) bsdi > svr4:( frag 26304: 1@1480)
5   75.328650    (24.8786) bsdi.1118 > svr4.discard : udp 1474   (frag
26313:1480@0+)
6   75.328982    ( 0.0003) bsdi > svr4:( frag 26313: 2@1480)
```

通过上面输出结果可以了解数据长度为1471、1472的数据都能直接装入以太网数据帧中，没有被分片。而对于1473和1474的数据包长度为1501和1502，所以需要进行分片处理。在第3和第5句中：

（**frag 26304**:1480@0＋）：是指 IP 部首部中的标识字段值。

（frag 26304:**1480**@0＋）：则表示除 IP 首部外的分片长度（ip 首部20字节＋udp 部首8字节＋数据内容1472字节＝正好为1500字节）。

（frag 26304:1480@**0**＋）：表示当前偏移值为0。

（frag 26304:1480@0**＋**）：表示当前数据包作分片处理。

在第4和第6句中：

（frag 26304：1@1480）：表示当前之包含1字节的用户数据。

（frag 26304：1@1480）：表示挡墙偏移值从1480的位置开始进行数据分片（因为上句中用户数据1472字节＋udp8字节）

在了解什么是偏移量后，我们同样可以在高级防御策略中设置偏移量的范围值，从来可以将它作为限制数据分片数据两的一个选择条件。

注：在分片时，除最后一片外，其他的每个片中的数据部分必须是8字节的整数倍。本例中的1480是8的整数倍

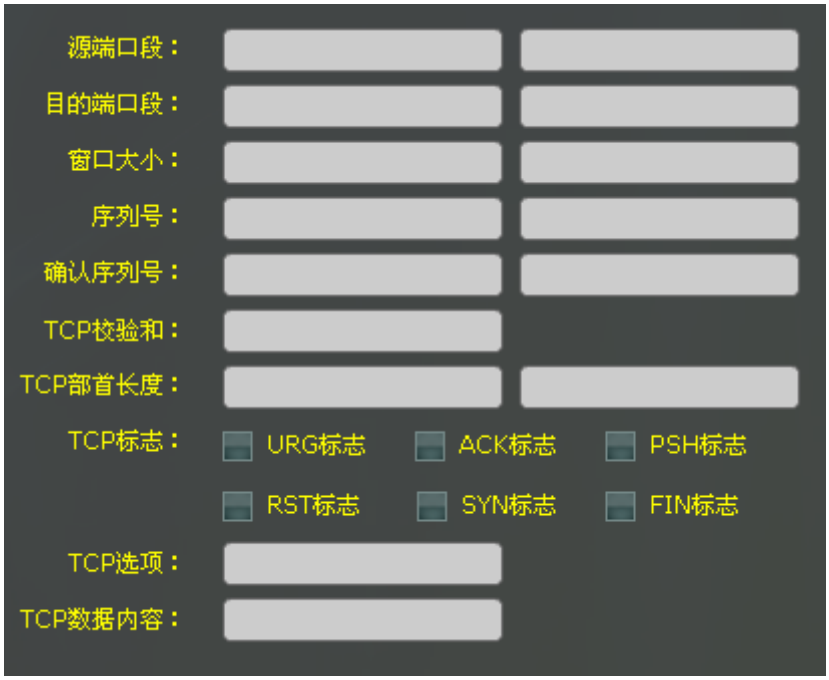
5.2.1.12 IP 效验和

依据 IP 数据对象内容而定的涵数运算后得出该值，并和数据对象一起储存或传送，以便检测数据变动。

注：一般情况下，正常数据包的效验和是不一样的。如果发现大量相同的效验和则可能是攻击伪造的效验和的值，通过设置效验和的值来防止这类攻击的出现。

5.2.2 TCP 包部首内容

在介绍完 IP 部首设置的相关条件参数以后，我们再来看看高级策略右侧内容中的 TCP 设置参数。如下图



5.2.2.1 源端口段

指 TCP 部首中含有的发送端的端口号

5.2.2.2 目的端口段

指 TCP 部首中含有的接收端的端口号

注：

1. 如果把 IP 地址比作房子，那么端口就是门。一个房子可以有多个门。一个服务器也就可以开启多个端口。端口范围是从 0－65535
2. 服务端的所提供的端口服务是固定的。如：FTP 服务器的 TCP 端口号都是 21，每个 Telnet 服务器的 TCP 端口号都是 23，每个 TFTP(简单文件传送协议)服务器的 UDP 端口号都是 69。任何 TCP/IP 实现所提供的服务都用知名的 1～1023 之间的端口号。
3. 高级防御策略中，端口填写的方式也同样是采用的范围填写。也就是说可以设置任意范围内的端口的策略条件。通过设置端口条件可以。

5.2.2.3 窗口大小

16 个字节，接受方用来通知发送方，我的接受 buffer 的大小，发送方不能过分的发送，导致接受方的 buffer 溢出。 单位是字节。

5.2.2.4 序列号

32 位的序列号由接收端计算机使用，重新分段的报文成最初形式。当 SYN 出现，序列码实际上是初始序列码（ISN），而第一个数据字节是 ISN+1。这个序列号（序列码）是可以补偿传输中的 不一致。

5.2.2.5 确认序列号

确认序列号是指在收到对方机器发过来的序列号(ISN)的第一个字节＋1 进行回复确认。

5.2.2.6 TCP 效验和

16 位，用来表示想收到的每个 TCP 数据段的大小。16 位 TCP 头。源机器基于数据内容计算一个数值，收信息机要与源机器数值结果完全一样，从而证明数据的有效性。

5.2.2.7 TCP 部首长度

TCP 部首长度是指 TCP 部首长度和 TCP 数据长度的字节长度. TCP 包的部首长度最少为 20 字节.

注意：最小 TCP 部首长度是指不带 TCP 选项内容的长度。一般情况下，带有 SYN 标记的 TCP 数据包都含有 TCP 选项内容. TCP 部首长度会大于 20 字节。

5.2.2.8 TCP 标志

6 位标志域。表示为：紧急标志、有意义的应答标志、推、重置连接标志、同步序列号标志 、完成发送数据标志。按照顺序排列是：URG、ACK、PSH、RST、SYN、FIN。

标志控制功能

URG：紧急标志
紧急(The urgent pointer) 标志有效。紧急标志置位，

ACK：确认标志
确认编号(Acknowledgement Number)栏有效。大多数情况下该标志位是置位的。TCP 报头内的确认编号栏内包含的确认编号(w+1，Figure：1)为下一个预期的序列编号，同时提示远端系统已经成功接收所有数据。

PSH：推标志
该标志置位时，接收端不将该数据进行队列处理，而是尽可能快将数据转由应用处理。在处理 telnet 或 rlogin 等交互模式的连接时，该标志总是置位的。

RST：复位标志
复位标志有效。用于复位相应的 TCP 连接。

SYN：同步标志
同步序列编号(Synchronize Sequence Numbers)栏有效。该标志仅在三次握手建立 TCP 连接时有效。它提示 TCP 连接的服务端检查序列编号，该序列编号为 TCP 连接初始端(一般是客户端)的初始序列编号。在这里，可以把 TCP 序列编号看作是一个范围从0到4，294，967，295的32位计数器。通过 TCP 连接交换的数据中每一个字节都经过序列编号。在 TCP 报头中的序列编号栏包括了 TCP 分段中第一个字节的序列编号。

FIN：结束标志
带有该标志置位的数据包用来结束一个 TCP 回话，但对应端口仍处于开放状态，准备接收后续数据。

5.2.2.9 TCP 选项

TCP 选项如同 TCP 协议中的附加协议一般，它常用的协议一般是：

MSS(Maximum Segment Size)：在服务器和客户端连接建立时(SYN)双方都会通告自己的 MSS，否则默认为 5 3 6 字节。它的长度为 4 个字节如下图所示：

Kind=2	len=4	最大报文长度
1 字节	1 字节	2 字节

Kind 表示选项的类型 2 通常表示最大报文段长度
len 表示该 kind 类型的总长度
最大报文长度表示该数据包能接收的最大报文长度

Window Scale 通过定义一个窗口扩大因子，使 TCP 的窗口从 1 6 bit 增加到 3 2 bit。同样 w 只出现在含有（SYN)标志的报文里。长度为 3 个字节如下图所示：

Kind= 3	len= 3	移位数
1 字节	1 字节	1 字节

Tcp 用窗口比例因子选项扩展窗口值。窗口比例因子表示原来 16 位的窗口值向左移位的次数，每次 1 次，窗口值翻一番。窗口比例因子的最大值为 14。窗口最大可以扩大 2^{14}＝16384 倍。

Timestamp：发送方在报文中放置一个时间戳值，接受方在确认时返回这个值以及接受的时间戳值，以此来计算 RTT 值。不一定出现在含有 SYN 标志的报文里。长度为 10 字节。

Kind=8	len=10	时间戳值	时间戳回显应答
1 字节	1 字节	4 字节	4 字节

Sack（Selective Acknowledgment，选择性确认）：TCP 通信时，如果发送序列中间某个数据包丢失，TCP 会通过重传最后确认的包开始的后续包，这样原先已经正确传输的包也可能重复发送，急剧降低了 TCP 性能。使用 sack 技术以后使 TCP 只重新发送丢失的包，不用发送后续所有的包，而且提供相应机制使接收方能告诉发送方哪些数据丢失，哪些数据重发了，哪些数 据已经提前收到等。

SACK 信息是通过 TCP 头的选项部分提供的，信息分为两种，一种标识是否支持 SACK，是在 TCP 握手时发送的；另一种是具体的 SACK 的信息。

SACK 允许选项

Kind=4	len=2

注：该选项只允许在有 SYN 标志的 TCP 包中，即 TCP 握手的前两个包中，分别表示各自是否支持 SACK。

SACK 选项

Kind=5	length

注：SACK 选项类型为 5。而选项长度是可变，但整个 TCP 选项长度不超过 40 字节，实际最多不超过 4 组边界值。

Kind=5	length

Left Edge of 1st Block

Right Edge of 1st Block

……

Left Edge of nth Block

Right Edge of nth Block

* Left Edge of Block

不连续块的第一个数据的序列号。

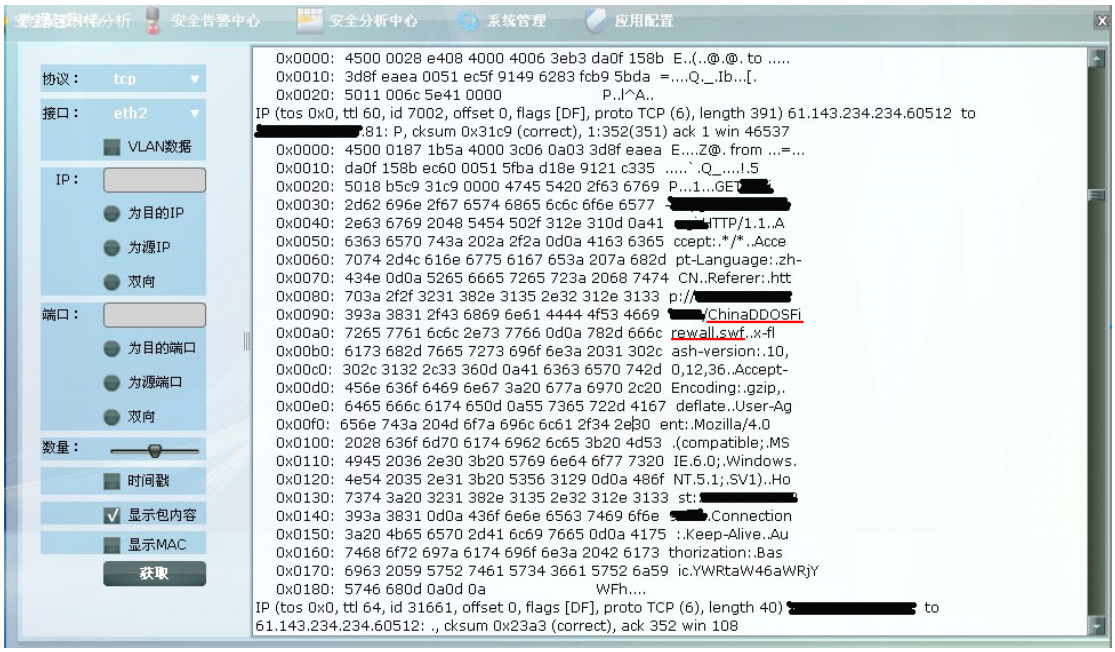
* Right Edge of Block

不连续块的最后一个数据的序列号之后的序列号。表示(Left Edge)和(Right Edge －1)处序列号的数据没能接收到。

注意：该选项参数告诉对方已经接收到并缓存的不连续的数据块，注意都是已经接收的，发送方可根据此信息检查究竟是哪个块丢失，从而发送相应的数据块。

5.2.2.10 TCP 数据内容

当建立正常的 TCP 三次握手协议以后，就开始传递需要访问的数据内容。TCP 数据内容包含所有的用户所需要了解的信息传递。例如：运用防火墙提供的分析工具如下图所示：



现在设置的条件为捕获所有经过 ETH2 网口的 TCP 协议内容。如上图红线所标记的内容，在

捕获的 TCP 数据内容中，包含有调用 ChinaDDOSFiewall.swf 的内容部分等相关信息内容。

注意：TCP 数据内容指的是 TCP 数据包中实际传递的内容数据，在有一些特殊攻击类型中，攻击源控制网络的肉鸡带有特殊的内容去攻击服务器的情况，我们可以通过分析工具利用抓包的形式将带有许多 TCP 数据内容关键字作为筛选条件。以防止这类特殊攻击的情况出现。

5.2.3 UDP 包部首内容

UDP 是一个简单的面向数据报的运输层协议：进程的每个输出操作都正好产生一个 UDP 数据报，并组装成一份待发送的 IP 数据报。简单的说 UDP 协议就好像短信功能一样。在不需要得道对方确认的情况下，直接可以发送短信给对方，因此 UDP 数据在传递过程中数据具有不可靠性。且不保证接收方能够接受到发送方的数据内容。UDP 参数设置如下：

注意：图片中 TCP 数据内容实为 UDP 数据内容。这个 BUG 将会在后续的版本中修正。

5.2.3.1 源端口段

源端口段：同 TCP 设置参数一样，指 UDP 部首中发送方的端口段

5.2.3.2 目的端口段

目的端口段：同 TCP 设置参数一样，指 UDP 部首中目的方的端口段

5.2.3.3 UDP 长度

UDP 长度是指 UDP 部首和 UDP 数据的字节长度。该字段的最小值为 8 字节。

5.2.3.4 UDP 效验和

UDP 效验和是指 16 位用于硝烟数据双方的正确性。UDP 的效验和覆盖 UDP 首部和 UDP 数据。

注：UDP 的效验和是可选的，而 TCP 效验和是必须的。

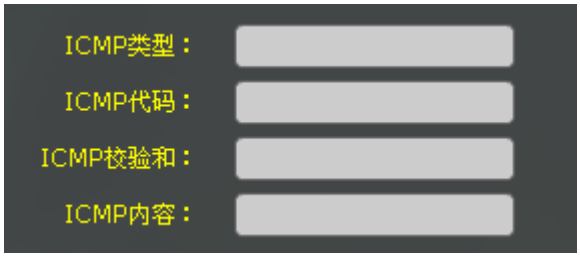
UDP 和 TCP 的效验和都覆盖了他们的首部和数据的效验和，而 IP 效验和仅仅只覆盖 IP 的部首，并不覆盖 IP 数据报中的任何数据。

5.2.3.5 UDP 数据内容

UDP 数据内容是指在 UDP 数据传递过程中的 UDP 数据内容.

5.2.4 ICMP 包部首内容

ICMP 是传递差错报文以及其他需要注意的信息。ICMP 通常被 IP 层或更高层协议使用。一些 ICMP 报文把差错报文返回给用户进程。用于在 IP 主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。ICMP 参数设置如下：



由于 ICMP 主要是用来控制差错报文的传递。因此各种类型的 ICMP 报文是由不同字段类型和代码字段来共同决定的。

5.2.4.1 ICMP 类型和代码

类型标识生成的错误报文，它是 ICMP 报文中的第一个字段；代码标识是进一步地限定生成 ICMP 报文。该字段用来查找产生错误的原因；详细内容如下表

类型	代码	描述
0	0	回应应答（Ping 应答，与类型 8 的 Ping 请求一起使用）
3		目的不可达
	0	网络不可达
	1	主机不可达
	2	协议不可达
	3	端口不可达
	4	需要进行分片但设置了不分片比特
	5	源站选路失败
	6	目的网络不认识
	7	目的主机不认识
	8	源主机被隔离（作废不用）
	9	目的网络被强制禁止
	10	目的主机被强制禁止

	11	由于服务器类型 TOS，网络不可达
	12	由于服务器了性 TOS，主机不可达
	13	由于过滤，通信被强制禁止
	14	主机越权
	15	优先权中止生效
4	0	源消亡
5		重定向
	0	对网络重定向
	1	对主机重定向
	2	对服务类型和网络重定向
	3	对服务类型和主机重定向
8	0	回应请求（Ping 请求，与类型 8 的 Ping 应答一起使用）
9	0	路由器公告（与类型 10 一起使用）
10	0	路由器请求（与类型 9 一起使用）
11		超时
	0	传输期间生存时间为 0
	1	在数据报组装期间生存时间为 0
12		参数问题
	0	坏的 IP 部首
	1	缺少必须的选项
13	0	时标请求（与类型 14 一起使用）
14	0	时标应答（与类型 13 一起使用）
15	0	信息请求（与类型 16 一起使用）
16	0	信息应答（与类型 15 一起使用）
17	0	地址掩码请求（与类型 18 一起使用）
18	0	地址掩码应答（与类型 17 一起使用）

5.2.4.2 ICMP 校验和

存储了 ICMP 所使用的校验和值。ICMP 的效验和是必须的。

5.2.4.3 ICMP 数据内容

包含了所有接受到的数据报的 IP 报头。还包含 IP 数据报中前 8 个字节的数据；

5.2.5 处理方式

处理方式主要是指将设置的高级策略条件作什么方面的操作处理。

5.2.5.1 丢弃数据包

当选择丢弃数据包的处理方式时，满足于当前设置策略的所有数据包都将直接作丢弃处理。

注意：如果是设定为一些禁止访问的策略时，请采用丢弃数据包的处理方式，从而避免降低防火墙使用性能。

5.2.5.2 允许通过

当选择允许通过的处理方式时，满足于当前设置策略的所有数据包都将直接作放行通过的处理。

5.2.5.3 源地址加黑名单

当选择允许通过的处理方式时，满足于当前设置策略的所有源地址 IP 数据包都将被加入到动态黑名单中。

注意：一般情况下，如果攻击者利用肉鸡的方式进行攻击时，建议使用加黑名单的处理方式。

5.2.5.4 目的地址加黑名单

当选择允许通过的处理方式时，满足于当前设置策略的所有目的地址 IP 数据包都将被加入到动态黑名单中。

注意：一般情况下，如果攻击者利用肉鸡的方式进行攻击时，建议使用加黑名单的处理方式。

5.2.5.5 源地址加白名单

当选择允许通过的处理方式时，满足于当前设置策略的所有源地址 IP 数据包都将被加入到动态白名单中。

5.2.5.6 目的地址加白名单

当选择允许通过的处理方式时，满足于当前设置策略的所有目的地址 IP 数据包都将被加入到动态白名单中。

5.2.6 选择逻辑关系

逻辑关系主要是指策略条件满足的判断方式。它分为以下几个方面

5.2.6.1 所有条件成立

所有条件成立：指在高级防御策略必须在满足所有的条件情况下，该策略才得以生效。

5.2.6.2 任意条件成立

任意条件成立：指在高级防御策略中只要有一项条件满足的情况下，该策略将生效。

5.2.6.3 所有条件不成立

所有条件不成立：指在高级防御策略必须在满足所有的条件不成立的情况下，该策略才得以生效。

5.2.6.4 任意条件不成立

任意条件不成立：指在高级防御策略中只要有一项条件不成立的情况下，该策略将生效 。

5.3 删除规则

删除规则是指删除当前不用的规则策略。单击要删除的规则，选择删除规则。此时规则窗口中的内容已删除。

注意：在操作删除规则的时候一定要注意。规则删除时是没有提示信息的。

5.4 规则属性

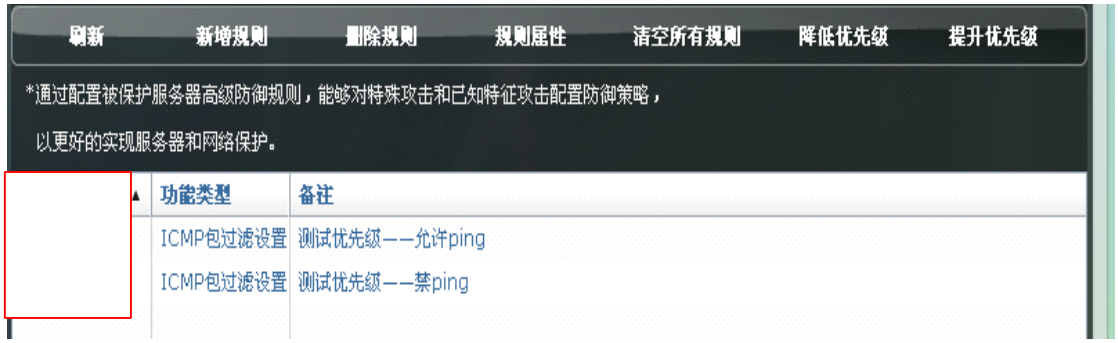
规则属性主要是用于修改当前已经建立的策略内容。

5.5 清空所有规则

清空所有规则是指一次性清空所有的规则策略。

5.6 降低优先级、提高优先级别

高级防御策略采用的是优先级别的使用法则，在默认情况下同等条件的策略排前的规则优先于排后的规则使用。例如



现在建立两条高级防御规则，一条是允许指定 IP 具有 ping 的功能，一条是禁止指定 IP 具有 ping 的功能。

允许 ping 功能

禁止 ping 功能

通过签名我们建立的条件来看，允许 ping 的优先级别高于禁 ping 级别。

```
C:\Documents and Settings\yh>ping 192.168.1.27

Pinging 192.168.1.27 with 32 bytes of data:

Reply from 192.168.1.27: bytes=32 time<1ms TTL=64
Reply from 192.168.1.27: bytes=32 time<1ms TTL=64
Reply from 192.168.1.27: bytes=32 time<1ms TTL=64
Reply from 192.168.1.27: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.27:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

所以在测试过程中，192.168.1.15 的 IP 可以 ping 通 192.168.1.27 的地址
我们现在将禁 ping 策略提高优先级别（记得一定要进行应用才有效）

再次通过以上测试发现，此时 192.168.1.15 的 IP 已经策略规则所限制无法 ping 通 192.168.1.27 的 IP

```
C:\Documents and Settings\yh>ping 192.168.1.27

Pinging 192.168.1.27 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.27:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

通过以上实例相信用户朋友可以很清楚的了解到优先级别的使用方式。