

# AXI系列路由器最大限度地降低DoS攻击的影响

Juniper 网络公司，爱立信公司，2001 年 3 月

内容提要 .....	2
角度 .....	2
SMURF 攻击.....	2
跟踪和阻止 SMURF 攻击.....	3
SYN 攻击 .....	5
跟踪 SYN 攻击 .....	6
发现和防止对 AXI 系列路由器的 SYN 攻击.....	6
发现、最大限度地降低及跟踪流经 AXI 系列路由器的 SYN 攻击.....	9
反向跟踪 SYN 攻击的入口点.....	10
防止假冒信源地址.....	11
积极地最大限度地降低 DOS 攻击的影响 .....	12
积极封锁 DoS 攻击 .....	12
限制分组速率 .....	12

## 内容提要

拒绝服务 (DoS) 攻击是Internet上常见的攻击方法。许多DoS攻击都基于分组泛滥或基于反复发送分组流，如smurf 和 SYN 攻击。本文描述了这两种DoS攻击方法，以及怎样采用Internet Processor II™ ASIC的过滤、采样和限速功能，跟踪和最大限度地降低这些攻击的影响。

## 角度

对世界各地的企业来说，其面临的一大挑战是既要允许甚至鼓励希望的流量，同时还要排斥不希望甚至有害的流量。关键是在不限制性能或扩充能力的情况下，提高网络的安全性。尽管在DoS攻击发生前完全阻止DoS攻击几乎是不可能的事，但通过使用AXI系列路由器上Internet Processor II ASIC提供的过滤和限速技术，可以最大限度地降低此类攻击的影响。此外，这种ASIC在实现上述功能时，不会阻碍转发或路由性能，同时提供了一个可扩充的解决方案。

## Smurf 攻击

Smurf 攻击是有人向包含大量主机的网络执行广播 ping 的结果。攻击者的 IP 地址并不是这个广播 ping 的信源地址，而是使用假的信源 IP 地址。接到这个广播 ping 的所有主机都会向攻击者标明的主机作出回应，结果导致受攻击的主机超载，与该主机相连的多条链路都会饱和。

Figure 1: Smurf Attack

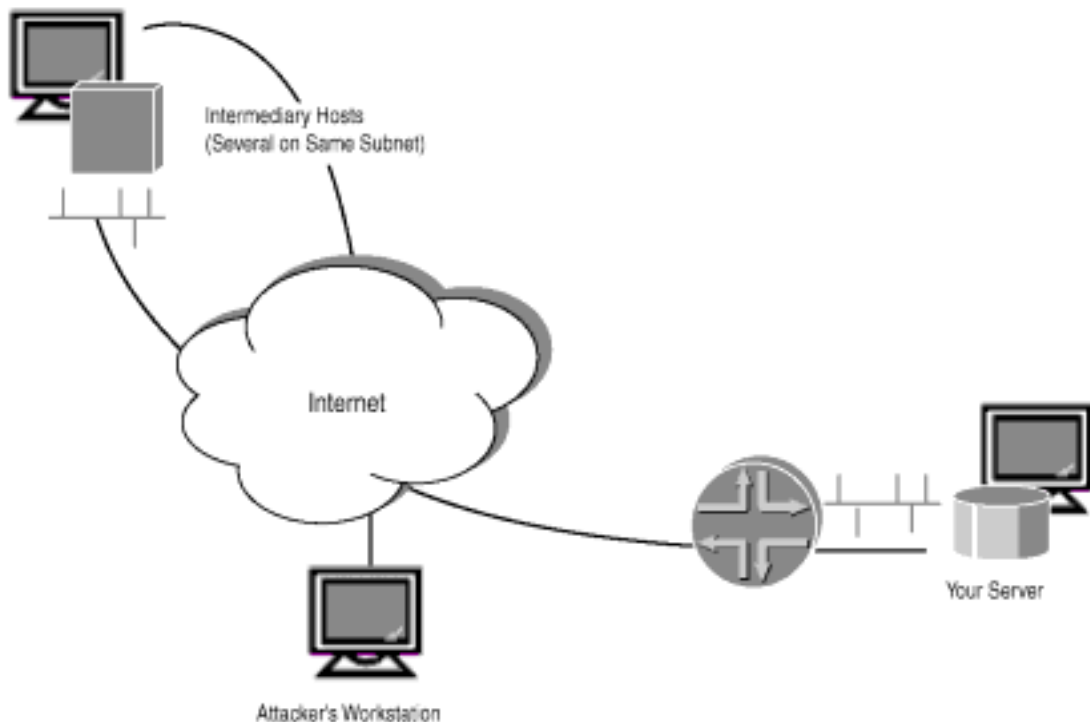


图 1：Smurf 攻击

Intermediary Hosts (Several on Same Subnet)：中间主机（多台中间主机位于同一个子网上）

Attacker's Workstation：攻击者的工作站

Your Server：你的服务器

Smurf攻击分成两种类型：对路由器的攻击和对网络上主机的攻击。此外，smurf攻击目标路由器的方式也有两种：路由器可以是中间路由器，也可以是真正的攻击目标。AXI系列路由器不能作为中间路由器，因为其默认值取消了定向广播功能。

当黑客把 smurf 攻击指向一台 AXI 系列路由器时，来自多个信源的 ICMP 回应会轰炸路由引擎。在默认状态下，AXI 系列路由器会限制指向路由器的 ICMP 回应请求速率，这样，到达路由引擎上的回应请求速率不会超过每秒 1,000 个。这种限速功能使得路由器即使在遭受攻击时，仍能继续进行正常工作。

## 跟踪和阻止 Smurf 攻击

1. 对防火墙过滤器进行配置，计数和记录指向遭受攻击的服务器的ICMP回应。

实例： [edit firewall filter detect-icmp]

```
term a {
  from {
    destination-address {
      10.1.1.1/32;
    }
    protocol icmp;
  }
  then {
    count icmp-counter;
    log;
    accept;
  }
}
term b {
  then accept;
}
```

2. 对与受影响的服务器相连接口的出局端应用过滤器。

实例： [edit interfaces fxp0]

```
unit 0 {
  family inet {
    filter {
      output detect-icmp;
    }
  }
}
```

```

        address 10.10.10.1/24;
    }
}

```

3. 查看计数器。如果分组和字节计数器迅速增加，表明发生了 smurf 攻击。

实例： root@ballpark> show firewall

```

Filter/Counter          Packet          Byte
                        count            count
detect-icmp             78,516         5,025,000
    icmp-counter
root@ballpark>

```

4. 查看路由引擎防火墙日志，确定攻击的媒介。大多数 ICMP 分组只源自少量的子网。

实例：

root@ballpark> show firewall log

Time	Filter	A Interface	Pro Source address	Destination address
23:09:09	-	A at-2/0/0.301	TCP 10.2.0.25	211.211.211.1:80
23:09:07	-	A at-2/0/0.301	TCP 10.2.0.25	211.211.211.1:56
23:09:07	-	A at-2/0/0.301	ICM 10.2.0.2	211.211.211.1:49552
23:02:27	-	A at-2/0/0.301	TCP 10.2.0.25	211.211.211.1:56
23:02:25	-	A at-2/0/0.301	TCP 10.2.0.25	211.211.211.1:80
23:01:22	-	A at-2/0/0.301	ICM 10.2.2.101	211.211.211.1:23251
23:01:21	-	A at-2/0/0.301	ICM 10.2.2.101	211.211.211.1:16557
23:01:20	-	A at-2/0/0.301	ICM 10.2.2.101	211.211.211.1:29471
23:01:19	-	A at-2/0/0.301	ICM 10.2.2.101	211.211.211.1:26873

5. 为确定地址所有者及相关的联络信息，查找相应的路由数据库（例如 whois -h radb.ra.net 192.68.20.1）。

6. 与所有者联系，请他或她通过过滤或消除定向广播从该端停止攻击。

7. 为了缓解攻击和恢复服务器运行，在 Then 语句中把过滤器的接收操作改为丢弃操作。通过这种修改，可以丢弃指向这台服务器的 ICMP 回应。在这种应用中使用丢弃而不是拒收非常重要，因为拒收会生成 ICMP 不可达信息，而丢弃则不会生成此信息。然而，黑客的流量仍在网络上的带宽资源。由于 smurf 攻击是一种分布式攻击，进入网络对等点的流量绝大部分都可能是假的流量，因此建议对服务器所在的所有自治系统（AS）边界应用过滤器。你可以对所有边缘路由器应用过滤器，而不会带来消极影响，也不会害怕丢弃合法的流量。

SYN 攻击

SYN 攻击可能会指向 AXI 系列路由器，也可能指向 AXI 系列服务器相连的主机。SYN 攻击的工作方式是攻击的主机建立半个 TCP 会话。所谓半个 TCP 会话，是指服务器从客户机上收到 SYN，应答为 SYN\_ACK，但服务器从不会接到客户机发回的 ACK。而正确的信息交换过程应该是：

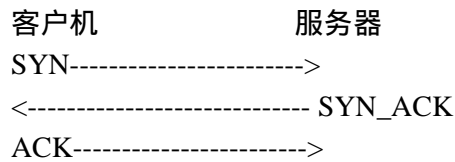
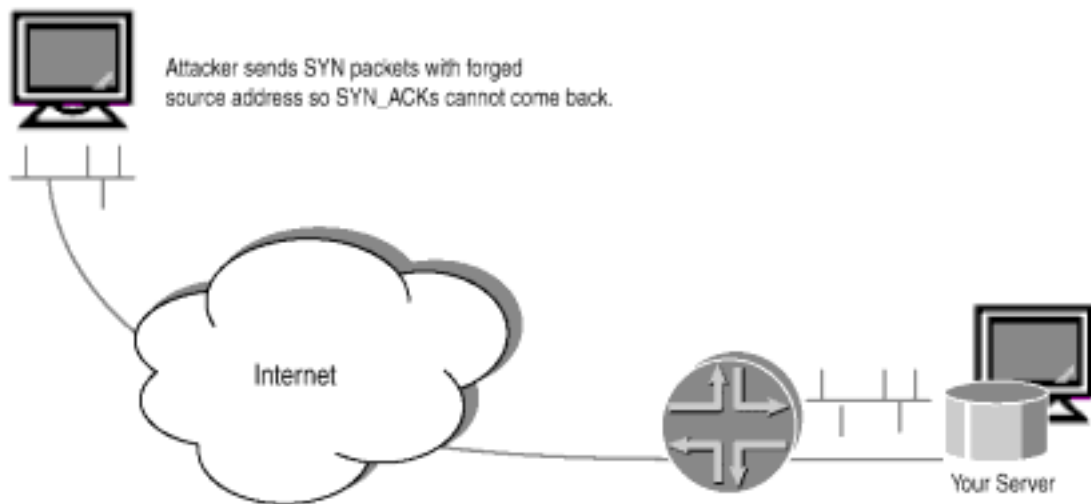


Figure 2: SYN Attacks



图示内容：

图二：SYN 攻击

攻击者使用伪造的信源地址发送SYN分组，因此不会返回SYN\_ACK。

Your Server：你的服务器

一般来说，半个会话不会导致重大损害，因为服务器会认为会话超时，继续进行正常的处理工作。在 SYN 泛滥的情况下，假冒客户机发起半个会话，因此不能完成三方询问。攻击者以非常快的速度发起这些 SYN 攻击，操作系统会预留资源，等待永远不会到来的最终 ACK，其对服务器的影响包括耗尽内存，导致系统瘫痪，直至使用所有可用服务，从而拒绝能够建立连接的合法用户。

AXI系列路由器以多种方式最大限度地降低了对主机的SYN攻击：

- 它限制了路由器上实现的服务数量；
- 在正确配置的路由器上，你只能从信任的地址建立服务；
- 即使从保护的地址上发起SYN泛滥，但它限制了内核允许的连接数量，因此不会出现内存耗尽的问题。

## 跟踪 SYN 攻击

有多种方法可以最大限度地降低和跟踪指向AXI系列路由器及与AXI系列路由器相连的主机的SYN攻击。注意，尽管这些方法不能保证路由器永远不会受到攻击，但这些方法确实有助于最大限度地降低此类攻击的影响。

如果发生 SYN 攻击，阻止 SYN 攻击的选项是有限的。任何企图阻止 SYN 攻击的方法都必须至少丢弃发往该主机的部分合法流量。如果 SYN 流量没有采取分布方式，那么最好是在攻击过程中封锁 SYN 攻击，丢弃部分合法流量，从而允许来自所有其它进入点的合法流量到达主机。为了确定 SYN 泛滥是不是分布式攻击，需要对攻击进行跟踪；如果它只通过一个对等点进入网络，那么就不是分布式攻击。但需要注意的是，大多数攻击都是分布式的。

## 发现和防止对 AXI 系列路由器的 SYN 攻击

1. 从命令行环境中，输入下面这条命令。如果有多个会话处在SYN\_RECEIVED状态，那么表明有人发起了对路由器的SYN泛滥攻击。

```
netstat -a -f inet
```

2. 对环回接口应用防火墙过滤器，确保只允许从信任的地址空间上建立连接。

实例： 对所有路由器上的lo0应用防火墙过滤器。

```
firewall {
    filter hostprotect {
        term ssh-permit {
            from {
                source-address {
                    10.1.1.0/24;
                }
                protocol tcp;
                destination-port ssh;
            }
            then {
                count ssh-permitted;
                accept;
            }
        }
        term ssh-deny {
            from {
                protocol tcp;
                destination-port ssh;
            }
        }
    }
}
```

```
        then {
            count ssh-denied;
            log;
            discard;
        }
    }
term telnet-permit {
    from {
        source-address {
            10.100.100.0/24;
            10.200.0.0/16;
        }
        protocol tcp;
        destination-port telnet;
    }
    then {
        count telnet-permitted;
        accept;
    }
}
term telnet-denied {
    from {
        protocol tcp;
        destination-port telnet;
    }
    then {
        count telnet-denied;
        log;
        discard;
    }
}
term snmp-permit {
    from {
        source-address {
            10.100.100.0/24;
            10.200.0.0/16;
        }
        protocol udp;
        destination-port snmp;
    }
    then {
        count snmp-permitted;
        accept;
    }
}
```

```
    }
    term snmp-denied {
        from {
            protocol udp;
            destination-port snmp;
        }
        then {
            count snmp-denied;
            log;
            discard;
        }
    }
    term ntp-permit {
        from {
            source-address {
                10.100.100.0/24;
                10.200.0.0/16;
            }
            protocol udp;
            destination-port ntp;
        }
        then {
            count ntp-permitted;
            accept;
        }
    }
    term ntp-denied {
        from {
            protocol udp;
            destination-port ntp;
        }
        then {
            count ntp-denied;
            log;
            discard;
        }
    }
    term permit-everything-else {
        then {
            count other-permitted;
            accept;
        }
    }
}
```

}

## 发现、最大限度地降低及跟踪流经 AXI 系列路由器的 SYN 攻击

1. 为了发现流经AXI系列路由器的SYN攻击，请遵循下述步骤之一：

- 配置防火墙过滤器，计数和比较TCP和TCP SYN流量。

实例： [edit firewall filter detect-syn-attack]

```
term a {
  from {
    protocol tcp;
    tcp-flags SYN;
  }
  then {
    count syn-packets;
    log;
    sample;
    accept;
  }
}
term b {
  from {
    protocol tcp;
  }
  then {
    count tcp-packets;
    accept;
  }
}
root@ballpark#
```

- 在转发选项中启动过滤。

```
实例： forwarding-options {
  sampling {
    input {
      family inet {
        rate 100;
        run-length 2;
      }
    }
  }
  output {
```

```

        file filename sampled-pkts files 5 size 2m world-readable stamp;
    }
}
}

```

- 对连接主机的接口应用过滤器。

```

实例： [edit interfaces fxp0]
      unit 0 {
        family inet {
          filter {
            output detect-syn-attack;
          }
          address 10.10.10.1/24;
        }
      }
[edit]

```

2. 查看计算的分组数量，确定带有TCP标记SYN集合的分组数是否异常高。比较detect-syn-attack过滤器中配置的计数器，其中包括tcp分组数和syn分组数。在正常情况下，syn分组数应该不到其它tcp分组数的一半。如果发生SYN泛滥，SYN分组数会非常高，可能达到TCP分组总数的50%以上。

```

实例： root@ballpark# run show firewall
Filter/Counter      Packet count      Byte count
count-icmp-echo
echo-reply-counter      0                  0
detect-syn-attack
tcp-packets           0                  0
syn-packets           0                  0
[edit firewall filter detect-syn-attack]
root@ballpark#

```

## 反向跟踪 SYN 攻击的入口点

1. 检查输出文件sampled-pkts。

```

实例：
scapshaw@ballpark> file show /var/tmp/sampled-pkts

```

Time	Dest Addr	Src Addr	Dest Port	Src Port	Proto	TOS	Pkt Le	Intf Num	IP Fra	TCP Flags
Sept 27	5:48:54	10.10.9.1	10.10.9.1	0	0	1	0x00	84	8	0x0
Sept 27	15:48:55	10.10.9.1	10.10.9.1	0	0	1	0x00	84	8	0x0

Sept 27	15:48:56	10.10.9.19	10.10.9.195	0	0	1	0x00	84	8	0x00
Sept 27	15:48:57	10.10.9.19	10.10.9.195	0	0	1	0x00	84	8	0x00
Sept 27	15:48:58	10.10.9.19	10.10.9.195	0	0	1	0x00	84	8	0x00

2. 仔细找出指向攻击主机的假冒信源地址。一旦确定参与攻击的假冒信源地址，那么你应该注意相应的进入接口。通过 Intf Num 字段可以识别进入接口。在 show interface extensive 命令输出中，可以查看这个接口指标。

3. 对上行路由器的出局端应用过滤器 detect-syn-attack。使用“发现、最大限度地降低和跟踪流经 AXI 系列路由器的 SYN 攻击”一节中说明的 detect-syn-attack 过滤器。应用这个过滤器，直到到达网络边缘。

4. 与你的网络之外的路由器所有者联系，通知他或她发生了这种攻击。

5. 为丢弃网络入口的流量，把 detect-syn-attack 过滤器中 Term A 的接收操作改为丢弃操作。对面向你的网络之外路由器的接口入局端（发起攻击的地方）应用这种操作。

## 防止假冒信源地址

1. 对只接收客户网络发起的流量的所有客户电路应用入局分组过滤。通过应用过滤，它可以传送带有合法客户信源 IP 地址的所有流量，并计数、记录和丢弃带有非法信源地址的所有流量。这种过滤器可以防止黑客使用假冒的信源地址。

实例：本实例用于位于 10.1.0/24 网络上的客户。

```

filter source-addr-verification {
    term a {
        from {
            source-address {
                10.1.1.0/24;
            }
        }
        then accept;
    }
    term b {
        then {
            count invalid-source-addr;
            log;
            discard; }
    }
}
[edit]
root@ballpark#

```

2. 对与客户相连的接口应用过滤器。

```
实例： [edit interfaces fxp0]
      unit 0 {
        family inet {
          filter {
            input source-addr-verification;
          }
          address 216.44.149.19/29;
        }
      }
root@ballpark#
```

### 积极地最大限度地降低 DoS 攻击的影响

我们强烈推荐积极地最大限度地降低DoS攻击的影响。方法之一是监视具体的分组，配置过滤器，在分组数量达到用户规定的门限时丢弃分组。另一种方法是使用Internet Processor II ASIC的限速功能。

### 积极封锁 DoS 攻击

1. 确定你希望把哪些分组划分成潜在的DoS分组。例如，你可能希望跟踪ICMP、UDP或TCP-SYN分组。你甚至可以划分信宿是具体地址的分组。
2. 创建过滤器，与划分为潜在DoS分组的分组相匹配。使用“Smurf攻击”和“SYN攻击”中描述的程序，把过滤器配置成计数、记录或接收分组。
3. 使用网络管理站上运行的脚本，监视计数器和系统日志文件，确定日志告警操作关联的项目。当脚本发现计数器或日志项目超过用户规定的门限时，可以重新配置路由引擎防火墙过滤器，把接收操作改为丢弃操作。

### 限制分组速率

可以在所有边缘限制网络接纳的ICMP分组数量，从而降低smurf攻击的影响。例如，如果把所有对等限定为发送200 Kbps的ICMP分组，那么smurf攻击可能暂时破坏了目标，但其几乎不会给带宽等网络资源带来任何压力。

```
实例： [edit firewall]
      filter limit-icmp {
        policer p1 {
          if-exceeding {
            bandwidth-limit 200k;
            burst-size-limit 20k;
          }
        }
      }
```

```
    }
    then {
        discard;
    }
}
term one {
    from {
        protocol icmp;
    }
    then {
        policer limit-icmp;
        accept;
        count count-icmp;
    }
}
}
```