

Internet Traffic Control

Edward Balas
ebalas@iu.edu

Advanced Network Management Laboratory

Overview

- ❑ Review of Internet Architecture and Technologies
- ❑ Macroscopic techniques to control traffic
- ❑ Microscopic techniques to control traffic
- ❑ What we have glossed over
- ❑ Examples

Internet Architecture Review

- ❑ Routing vs Bridging
- ❑ What is an Autonomous System(AS)
- ❑ Interior Gateway Protocols
- ❑ Exterior Gateway Protocols
- ❑ What is a Flow?

Routing Vs Bridging

- ❑ Routing examines the IP header.
- ❑ TTL in header is decremented.
- ❑ A routing device usually shows up in a traceroute.
- ❑ Bridging looks at the link layer header.
- ❑ IP portion is never modified.
- ❑ A bridging device is invisible in traceroute.

Interior Gateway Protocols

- ❑ Used to communicate connectivity information within an organization or AS
- ❑ Primary focus is on optimization of forwarding and failure recovery
- ❑ Modern protocols based on Shortest Path First (SPF) with Link State Database Algorithms vs Distance Vector.
- ❑ Examples include OSPF and ISIS

Exterior Gateway Protocols

- ❑ Exterior Gateway Protocols are used to communicate connectivity information between ASes.
- ❑ Focus is on enforcing peering agreements and administrative control.
- ❑ Currently BGP4 is king.
- ❑ How does it work?

What is a Flow?

- ❑ An abstraction used to denote a sequence or group of related IP packets.
- ❑ Variable granularity: SRC IP/PORT to DST IP/PORT, IP to IP, Net to Net, AS to AS.
- ❑ A TCP flow is a group of packets from the same TCP transaction.
- ❑ Routing devices strive to keep TCP based flows on the same forwarding path.

Macroscopic Traffic Control

- ❑ Accomplished by restricting route topology or connectivity information.
- ❑ Accomplished through the use of BGP and sometimes IGP.
- ❑ BGP implementations have per peer Announce and Accept filters
- ❑ Filters can consider the route prefix, AS path and other criteria.

Microscopic Traffic Control

- ❑ Controls traffic at the point of forwarding rather than at point of information propagation.
- ❑ Typically examines (TCP|UDP)/IP headers and sometimes payload.
- ❑ Firewalls
- ❑ Intrusion Detection Systems with active response mechanisms.

Firewalling

- ❑ A technique used by forwarding devices to filter traffic based on configuration.
- ❑ Examines (TCP|UDP)/IP packet headers, rarely examines payload.
- ❑ Stateless and Statefull variants exist.
- ❑ Statefull firewalls usually focused on TCP
- ❑ Dedicated devices, routers, and hosts can fulfill the role.

Intrusion Detection Systems

- ❑ Similar to statefull firewall but reassembles the payload, then examines contents.
- ❑ Use signatures of known attacks to perform pattern matching.
- ❑ Some implementations include active response to control the suspect traffic.
- ❑ Two responses: dynamic packet filtering or collapsing a TCP flow(set the RST bit).

What we have Neglected

- ❑ Rate Limiting.
- ❑ Queuing Strategies.

Rate Limiting

- ❑ Used to control bit rate or packet per second rate for a given flow on a per interface transmission basis.
- ❑ Can vary in level of enforcement, some drop packets instantly others will mark as drop eligible and drop if the link is Bandwidth constrained.
- ❑ Examples: Cisco's CAR, FreeBSD's Dummynet.

Queuing

- ❑ Routing Devices allow for different queuing techniques, each has an impact on traffic control.
- ❑ Some techniques are don't discriminate.
- ❑ Some allow for preferential treatment of traffic flows such as WFQ.
- ❑ Random Early Drop queuing designed to "interact" with TCP sessions.

BGP Routing Example

- ❑ BGP config for a Juniper
- ❑ This filters the routes we accept from a peer to whom we have applied this policy(filter).
- ❑ Filters can also match range on prefixes, AS path, etc.
- ❑ For more info:
<http://www.juniper.net/techpubs/software/junos50/swconfig50-routing/frameset.htm>

```
policy-statement internet-in {  
  term 1 {  
    from {  
      route-filter 192.168.231.0/24 exact accept;  
      route-filter 192.168.244.0/24 exact accept;  
      route-filter 192.200.198.0/24 exact accept;  
      route-filter 192.200.160.0/24 exact accept;  
      route-filter 192.200.59.0/24 exact accept;  
    }  
  }  
  term 2 {  
    then {  
      reject;  
    }  
  }  
}
```

Forwarding Example

- ❑ Firewalling example from FreeBSD

```
#--- Stateless IP exaple  
ipfw add allow ip from 156.56.103.0/24 to  
156.56.103.14
```

- ❑ Forwarding filters work with a host that is bridging or routing

```
#--- Stateless UDP exaple  
ipfw add allow udp from 156.56.0.0/16 to 156.56.103.14 666
```

- ❑ Filters have no effect on route information propagation

```
#--- Statefull TCP exaple  
ipfw add allow tcp from any to 156.56.103.14 80 keep-state
```

- ❑ Go to www.freebsd.org and search for ipfw

Rate Limiting

- ❑ Exaple of rate limiting using dummy net on FreeBSD
- ❑ Uses filters in conjunction with the pipe action to categorize traffic to send down a virtual "pipe"
- ❑ Can also induce latency and loss.
- ❑ Go to www.freebsd.org and search for dummynet.

```
#---rate limit each honeypot to 128kbs fullduplex
```

```
ipfw add pipe 1 ip from any to any recv fxp0
```

```
ipfw add pipe 2 ip from any to any recv fxp1
```

```
ipfw pipe 1 config mask dst-ip 0xffffffff bw 128Kbits/s
```

```
ipfw pipe 2 config mask src-ip 0xffffffff bw 128kbits/s
```

IDS Example

- ❑ Snort IDS config example
- ❑ This shows the disabling a TCP flow that matches the CodeRed v2 signature
- ❑ The response feature is rather new, I haven't even evaluated this implementation.
- ❑ Go to www.snort.org for more information.

```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80
(
  msg: "WEB-IIS CodeRed v2 root.exe access";
  flags: A+;

  #--- This causes snort to eval as HTTP and to
  #---examine the URI looking for a case insensitive #---
  match
    uricontent:"scripts/root.exe?";
    nocase;
    classtype: attempted-admin;
    sid: 1257;
    rev: 1;

  #--- This causes Snort to send RST messages
  #--- to both sides of the TCP flow
  resp: rst_all;
)
```