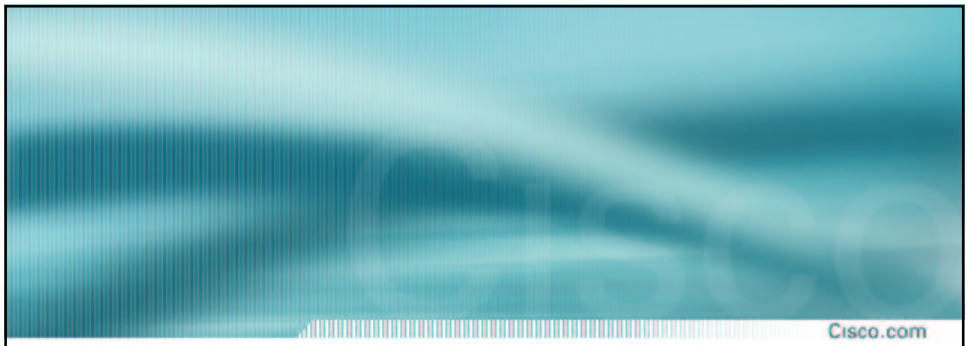


Scalable Defense against DoS Attacks

DFN-CERT Workshop, 27. 2. 2002

Michael Behringer <mbehring@cisco.com>

News - January 22,2002

Cloud-Nine Officially Closes ISP!

Cisco.com

By:mark.j @ 10:44:AM - Comments (35) - SendNews [HERE] / PrintNews [HERE]

Today looks set to be a sad and frustrating one for anybody who was ever a customer of the once popular unmetered dialup and broadband ISP Cloud-Nine.

At precisely 10:16am a few minutes ago Emeric Miszti (CEO) and John Parr (Operations Director) of the C9 ISP posted what's likely to be their final announcement on our forums. C9 is now the latest ISP to close, although it's the first we've ever seen to go from a hack attack!:

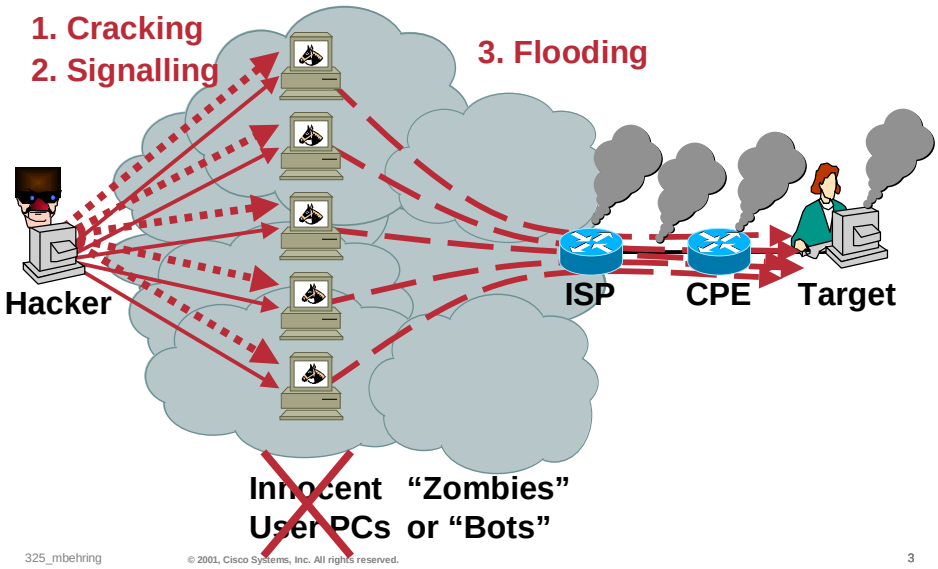
Cloud Nine regret to announce that at 7:45 this morning the decision was taken to shut down our Internet connections with immediate effect.

We tried overnight to bring our web servers back online but were seeing denial of service attacks against all our key servers, including email and DNS. These were of an extremely widespread nature.

http://www.ispreview.co.uk/cgi-bin/ispnews/printnews.cgi?newsid1011696274,91619,

DoS: The Procedure

Cisco.com



DoS: The Mechanisms Used

Cisco.com

1. **Cracking:**

   Manually, through viruses, worms (code red), …; always exploiting host vulnerabilities

2. **Signalling:**

   IRC, specific ICMPs, through "relays"…

3. **Flooding:**

   TCP SYN flood, UDP, ICMP, other IP protocols, …

Attacking a Line: Big packets (bandwidth!)

Attacking a Host/Router: Small packets (pps!)

DoS in an Enterprise Environment

Cisco.com

- Typically few entry points
- Mostly punctual defense on routers / firewalls:
  - Packet filters (ACLs)
  - Firewalling
  - TCP Intercept (against SYN attacks)
  - Rate limiting of attacking traffic (CAR)
- If the above doesn't help, contact ISP

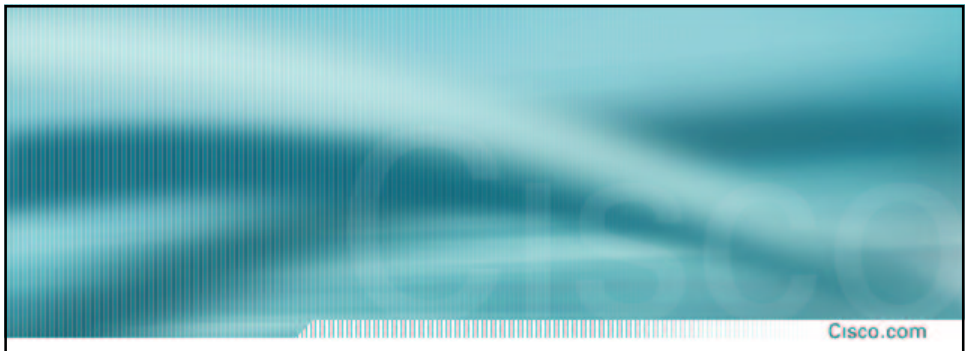
  -> This is the rest of the presentation

Agenda

Cisco.com

- First Steps: Detection, Classification and Back Tracing
- Scalable Defense Mechanisms

Notes:
- DoS is a research topic! Please contribute your experience!
- Most attacks today are distributed, therefore: DoS = dDoS for this presentation



First Steps: Detection, Classification, Back Tracing

Ways to Detect and Classify DoS Attacks

- Customer Call
- SNMP: Line/CPU overload, Drops
- Netflow: Counting Flows
- ACLs with Logging
- Backscatter
- Sniffers

Detecting DoS through CPU Load

Cisco.com

router>sh proc cpu

CPU utilization for five seconds: A% B% one minute: C%; five minutes: D%

CPU total utilisation

CPU at interrupt level

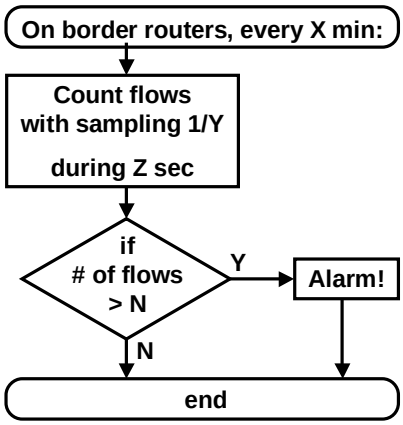
- A: Total CPU load
- B: CPU at Interrupt level (note: B <= A)
- A-B: Process switched traffic, CPU processes

(See: http://www.cisco.com/warp/public/63/highcpu.html)

Detecting DoS Attacks with Netflow

Cisco.com

- Basis: Have Netflow running on the network



DANTE uses:
X=15 min, Y=200,
Z=10 sec, N=10

Values are empirical

How does a DoS Attack Look Like?

Cisco.com

Potential DoS attack (33 flows) on router1
Estimated: 660 pkt/s 0.2112 Mbps
ASxxx is: ...
ASddd is: ...

src_ip	dst_ip	in_if	out_if	s_port	d_port	pkts	bytes	prot	src_as	dst_as
192.xx.xxx.69	194.yyy.yyy.2	29	49	1308	77	1	40	6	xxx	ddd
192.xx.xxx.222	194.yyy.yyy.2	29	49	1774	1243	1	40	6	xxx	ddd
192.xx.xxx.108	194.yyy.yyy.2	29	49	1869	1076	1	40	6	xxx	ddd
192.xx.xxx.159	194.yyy.yyy.2	29	49	1050	903	1	40	6	xxx	ddd
192.xx.xxx.54	194.yyy.yyy.2	29	49	2018	730	1	40	6	xxx	ddd
192.xx.xxx.136	194.yyy.yyy.2	29	49	1821	559	1	40	6	xxx	ddd
192.xx.xxx.216	194.yyy.yyy.2	29	49	1516	383	1	40	6	xxx	ddd
192.xx.xxx.111	194.yyy.yyy.2	29	49	1894	45	1	40	6	xxx	ddd
192.xx.xxx.29	194.yyy.yyy.2	29	49	1600	1209	1	40	6	xxx	ddd
192.xx.xxx.24	194.yyy.yyy.2	29	49	1120	1034	1	40	6	xxx	ddd
192.xx.xxx.39	194.yyy.yyy.2	29	49	1459	868	1	40	6	xxx	ddd
192.xx.xxx.249	194.yyy.yyy.2	29	49	1967	692	1	40	6	xxx	ddd
192.xx.xxx.57	194.yyy.yyy.2	29	49	1044	521	1	40	6	xxx	ddd
192.xx.xxx.202	194.yyy.yyy.2	29	49	1840	345	1	40	6	xxx	ddd
192.xx.xxx.90	194.yyy.yyy.2	29	49	1327	176	1	40	6	xxx	ddd
192.xx.xxx.164	194.yyy.yyy.2	29	49	1451	1343	1	40	6	xxx	ddd

....

Detecting DoS with ACLs

Cisco.com

- **Requires ACLs to be in place (for detection)**

Extended IP access list 169

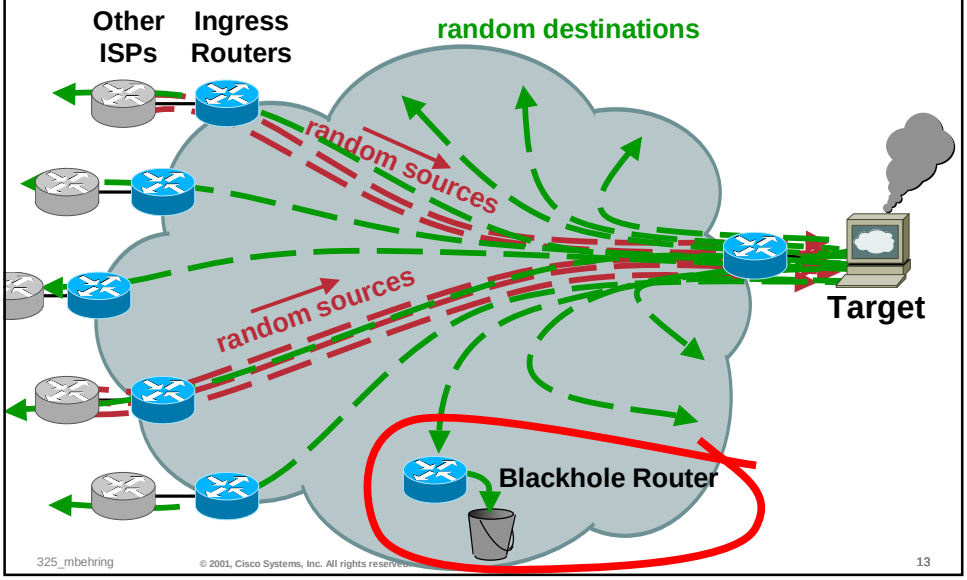
permit icmp any any echo (2 matches)
permit icmp any any echo-reply (21374 matches)
permit udp any any eq echo
permit udp any eq echo any
permit tcp any any established (150 matches)
permit tcp any any (15 matches)
permit ip any any (45 matches)

Found:
- attack type
- interface

-> Watch performance impact
-> Normally only on demand, not pro-active
-> More used for checking than for detection
-> Use key-words “log” “log-input” for details

Backscatter Analysis

Cisco.com



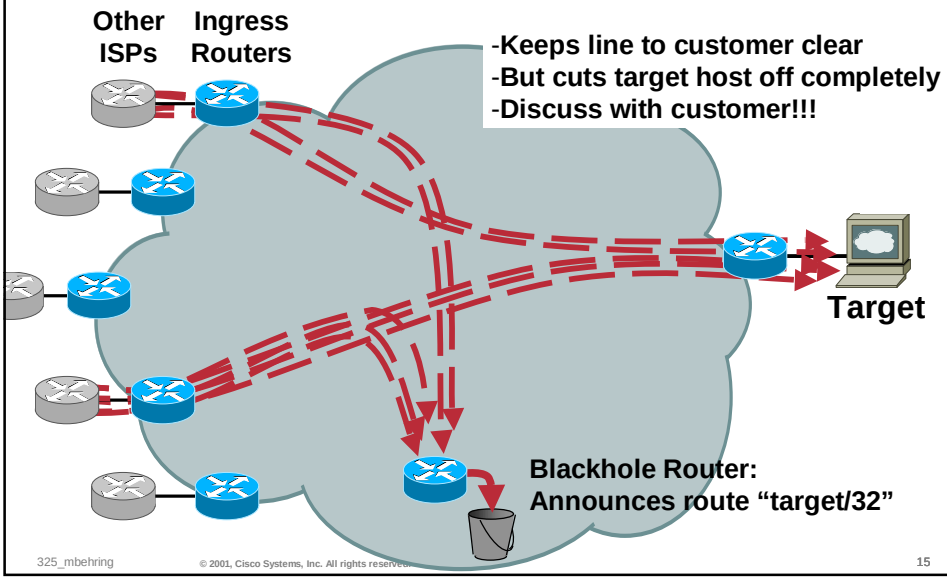
Backscatter Analysis

Cisco.com

- **Blackhole router:**
  Statically announce *unused* address space (1/8, 2/8, 5/8)
  (see http://www.iana.org/assignments/ipv4-address-space)
- **Victim replies to random destinations**
- **-> Some backscatter goes to blackhole router, where it can be analysed**

Re-Directing Traffic from the Victim

Cisco.com



Tracing DoS Attacks

Cisco.com

- If source prefix is not spoofed:

  -> Routing table
  -> Internet Routing Registry (IRR)
  -> direct site contact

- If source prefix is spoofed:

  -> Trace packet flow through the network
  -> Find upstream ISP
  -> Upstream needs to continue tracing

Tracing Back with Netflow

Cisco.com

- Routers need Netflow enabled

Victim

router1#sh ip cache flow | include <destination>

Se1 <source> Et0 <destination> 11 0013 0007 159

.... (lou re flows to the same destination)

The flows come from serial 1

Find the upstream router on serial 1

router1#sh ip cef se1

Prefix	Next Hop	Interface
0.0.0.0/0	10.10.10.2	Serial1
10.10.10.0/30	attached	Serial1

Continue on this router

Tracing Back with ACLs

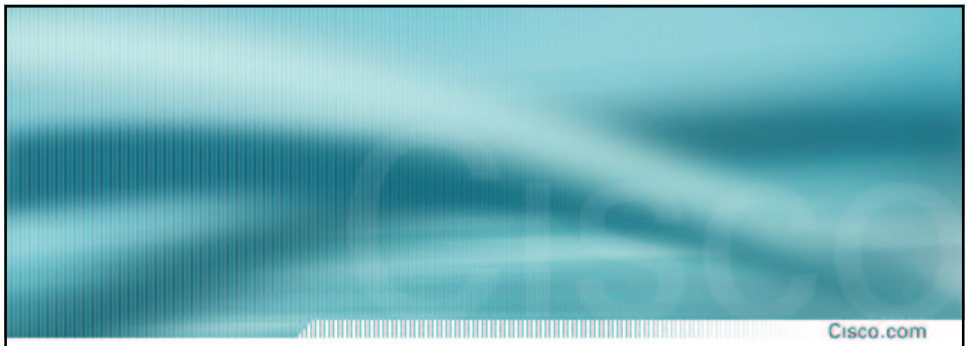
Cisco.com

- **Create ACL:**
  access-list 101 permit ip any <target> log-input
- **Apply to interface for a few seconds:**
  interface xxx
  ip access-group 101 in
  (wait a few seconds)
  no ip access-group 101
- **Log shows interface the attack comes from**

14:17:21: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 105.12.73.84(0) (FastEthernet0/0 0006.d780.2380) -> 192.168.1.1(0), 1 packet
14:17:22: %SEC-6-IPACCESSLOGP: list 101 permitted tcp 166.159.237.65(0) (FastEthernet0/0 0006.d780.2380) -> 192.168.1.1(0), 1 packet

mac address

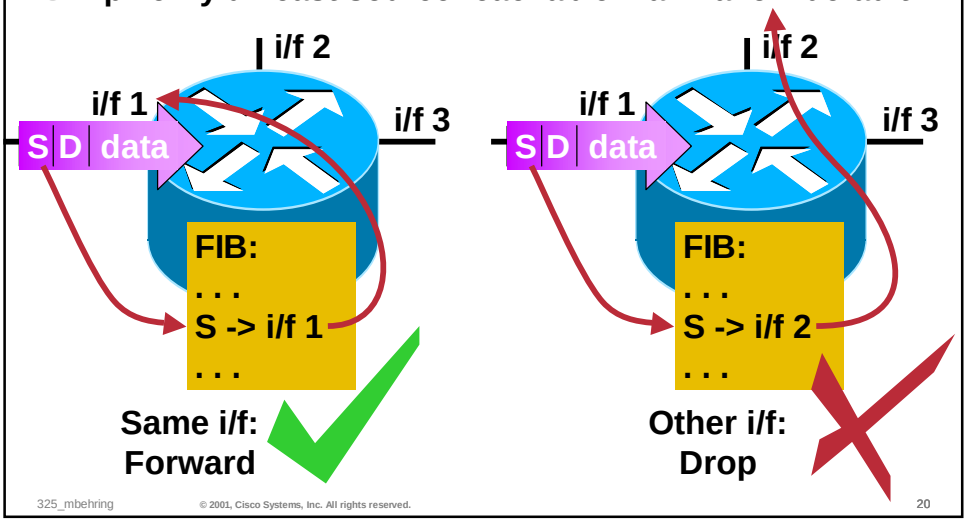
src interface



Scalable Defense Mechanisms

Strict uRPF Check (Unicast Reverse Path Forwarding)

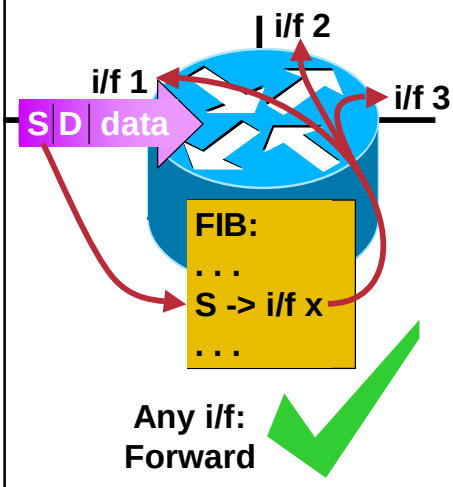
router(config-if)# ip verify unicast reverse-path
or: ip verify unicast source reachable-via rx allow-default

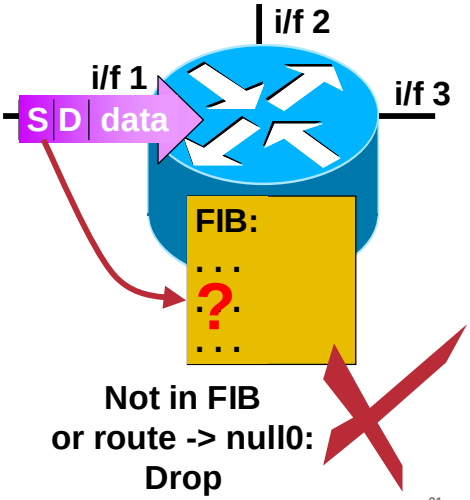


Loose uRPF Check (Unicast Reverse Path Forwarding)

Cisco.com

router(config-if)# **ip verify unicast source reachable-via any**

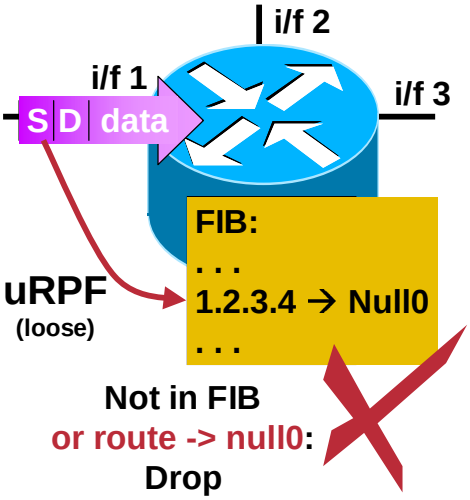




Deleting Traffic *from* a Source Address

Cisco.com

- Goal: Delete all packets *from* 1.2.3.4
- Static route: 1.2.3.4 → Null0
- Loose uRPF: "reachable-via any"
- Minimal CPU impact (2-3%), CEF based
- Alternative to ACL



Shunning with uRPF and BGP

Cisco.com

- ip route x.x.x.x null0 is manual :-(
- BGP cannot send “next-hop null0”… but:
- BGP can send “next-hop 192.0.2.1”
- And on each border router:
  ip route 192.0.2.1 null0
- Router receives iBGP routing update:
  “Route x.x.x.x next-hop 192.0.2.1” (comm: local-AS)
  and it has an ip route 192.0.2.1 null0
  Thus: x.x.x.x -> null0 (note: CEF required!)
- With uRPF: Source x.x.x.x also -> null0

Effect of BGP Remote Trigger

Cisco.com

- Traffic to/from a specific subnet will be sent to null0
- Automatically, on all border routers
- No attack traffic on backbone
- But… *Where is the attack coming from??? Which upstream ISPs to notify???*

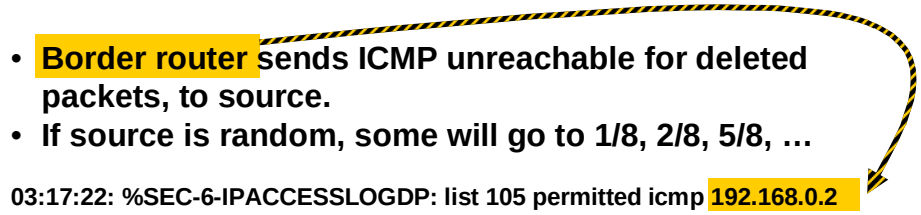
ICMP Backscatter

Cisco.com

On black hole router:

- Static routes for 1/8,2/8,5/8 (will attract 3/256 of packets)
- access-list 105 permit icmp any any log-input
  access-list 105 permit ip any any

- Border router sends ICMP unreachable for deleted packets, to source.
- If source is random, some will go to 1/8, 2/8, 5/8, …

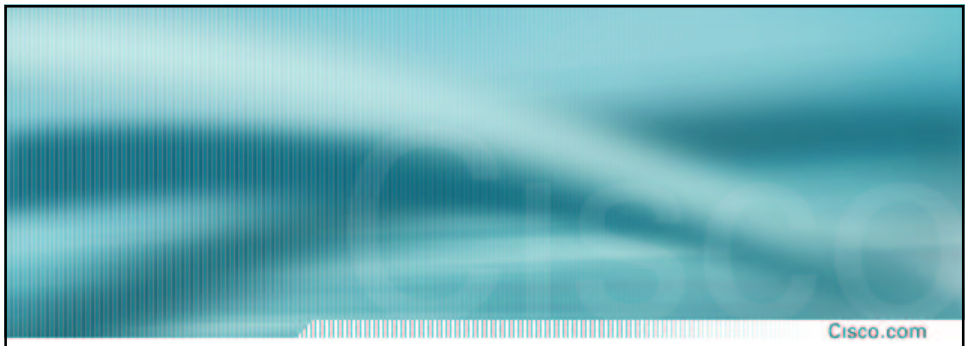


```
03:17:22: %SEC-6-IPACCESSLOGDP: list 105 permitted icmp 192.168.0.2
   (Serial0/0 *HDLC*) -> 5.52.203.66 (0/0), 1 packet
03:17:38: %SEC-6-IPACCESSLOGDP: list 105 permitted icmp 192.168.0.2
   (Serial0/0 *HDLC*) -> 1.167.111.47 (0/0), 1 packet
03:17:52: %SEC-6-IPACCESSLOGDP: list 105 permitted icmp 192.171.12.5
   (Serial0/1 *HDLC*) -> 2.153.59.34 (0/0), 1 packet
…
```


Summary: Containing DoS Attacks

Cisco.com

- **ACLs:**
  - Manual, performance impact
- **uRPF:**
  - Stops non-existing sources
  - Automated with BGP for specific shunning
- **CAR:**
  - Limit attack flow, performance impact
  - Manual or automated via QPPB (BGP)



Wrap Up

What we can do now

Cisco.com

- Detect DoS Attacks (SNMP, Netflow, ACL)
- Trace back random packet floods (Netflow, ACLs)
- Shun a source (uRFP, ACL)
- Shun a destination (routing, ACL)
- Limit attacking traffic (CAR)
- And update all routers via iBPG

Tip: scheduler allocate

Cisco.com

- **Schedules CPU time spent on processes versus interrupts**

Syntax:
`scheduler allocate <interrupt> <processes>`

`<interrupt>`: 3000-60000 Microseconds handling network interrupts
`<processes>`: 1000-8000 Microseconds running processes

Example:
`router(config)#scheduler allocate 8000 8000`

Very useful under heavy load!
Recommended Standard Config!

Recommendations for ISPs

Cisco.com

- **Preventive Meassures: ACLs, uRPF, CAR, …**
  - See ISP Essentials
- **Monitor your routers and alarm on:**
  - CPU, line load, memory, …
- **Use Netflow plus Collector s/w:**
  - Usage statistics, DoS detection, DoS tracing through the network
- **Be prepared:**
  - Technically: Understand the routers
  - Operationally: Have procedures in place, know your upstream/downstream contacts, have a CERT

Other Types of DoS :-)

Cisco.com

“The first day of summer vacations is a DoS attack against the highway system.”

(What can we do if future DoS attacks use many PCs to send millions of perfectly legal HTTP request?)

References (non-Cisco)

Cisco.com

DoS Detection:

- “Tackling Network DoS on Transit Networks”: David Harmelin, DANTE, March 2001 (describes a detection method based on netflow) [http://www.dante.net/pubs/dip/42/42.html]
- “Inferring Internet Denial-of-Service Activity”: David Moore et al, May 2001; (described a new method to detect DoS attacks, based on the return traffic from the victims, analysed on a /8 network; very interesting reading) [http://www.caida.org/outreach/papers/backscatter/index.xml]
- “The spread of the code red worm”: David Moore, CAIDA, July 2001 (using the above to detect how this worm spread across the Internet) [http://www.caida.org/analysis/security/code-red/]

DoS Tracing:

- “Tracing Spoofed IP Addresses”: Rob Thomas, Feb 2001; (good technical description of using netflow to trace back a flow) [http://www.enteract.com/~robt/Docs/Articles/tracking-spoofed.html]

Other:

- “DoS attacks against GRC.com”: Steve Gibson, GRC, June 2001 (a real life description of attacks from the victim side; somewhat disputed, but fun to read!) [http://grc.com/dos/grcdos.htm]

References (Cisco - public)

Cisco.com

Product Security:

- Cisco's Product Vulnerabilities; A page that every SE MUST know!!! [http://www.cisco.com/warp/public/707/advisory.html]
- Security Reference Information: Various white papers on DoS attacks and how to defeat them [http://www.cisco.com/warp/public/707/ref.html]

ISP Essentials:

- Technical tips for ISPs every ISP should know [http://www.cisco.com/public/cons/isp/]

Technical tips:

- Troubleshooting High CPU Utilization on Cisco Routers [http://www.cisco.com/warp/public/63/highcpu.html]
- The "show processes" command [http://www.cisco.com/warp/public/63/showproc_cpu.html]

Mailing lists:

- cust-security-announce: All customers should be on this list.
- cust-security-discuss: For informal discussions.

CISCO SYSTEMS

EMPOWERING THE INTERNET GENERATION℠