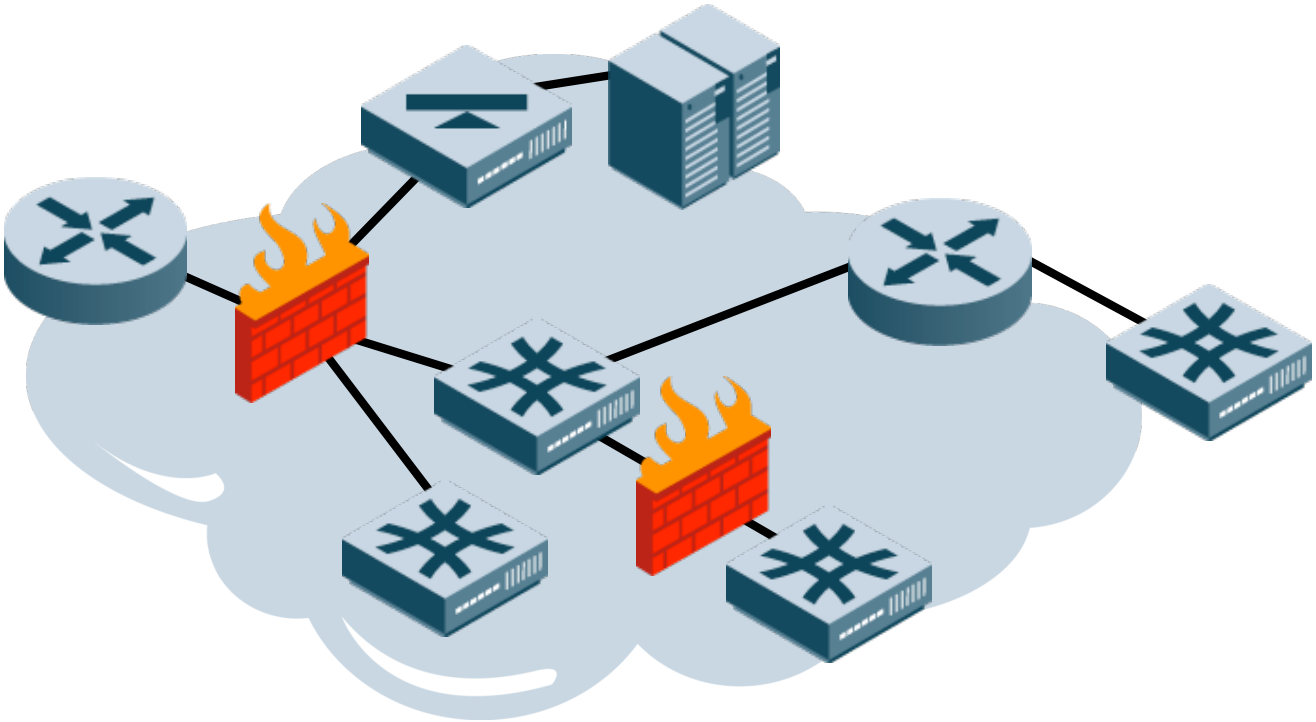
Increasing Security using Routers and Switches

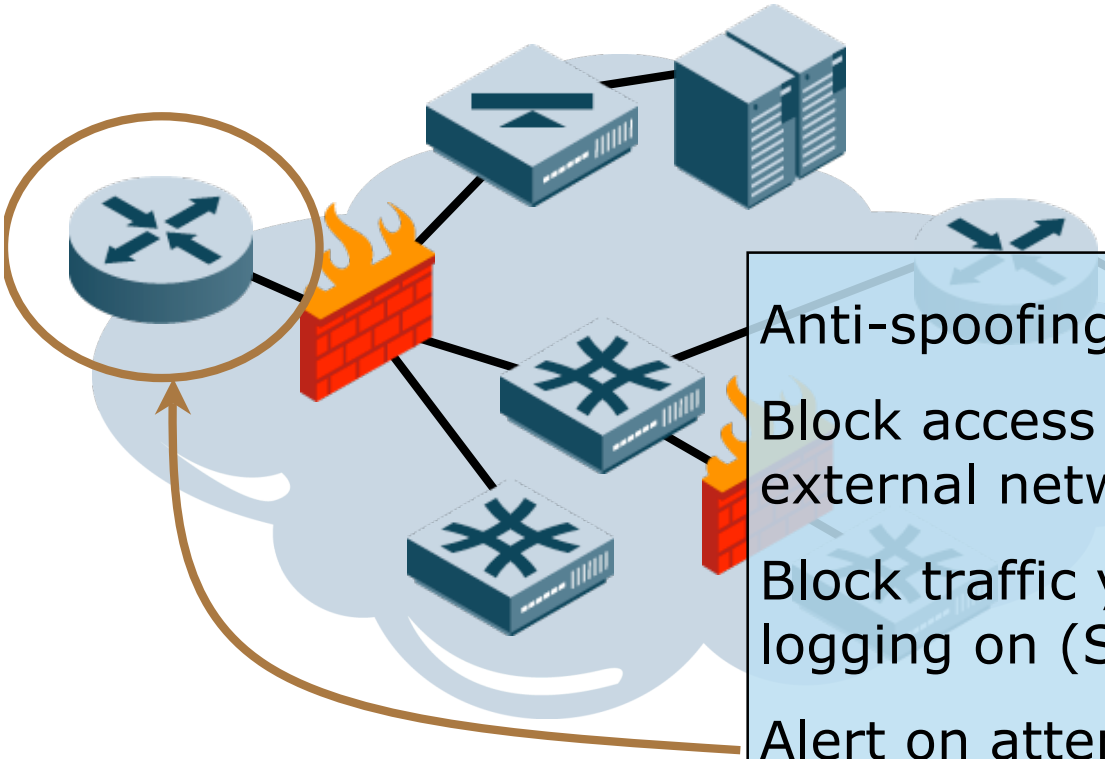
Joel M Snyder
Senior Partner
Opus One
jms@opus1.com

Spring/2007

Your network already has lots of security control points… use them!

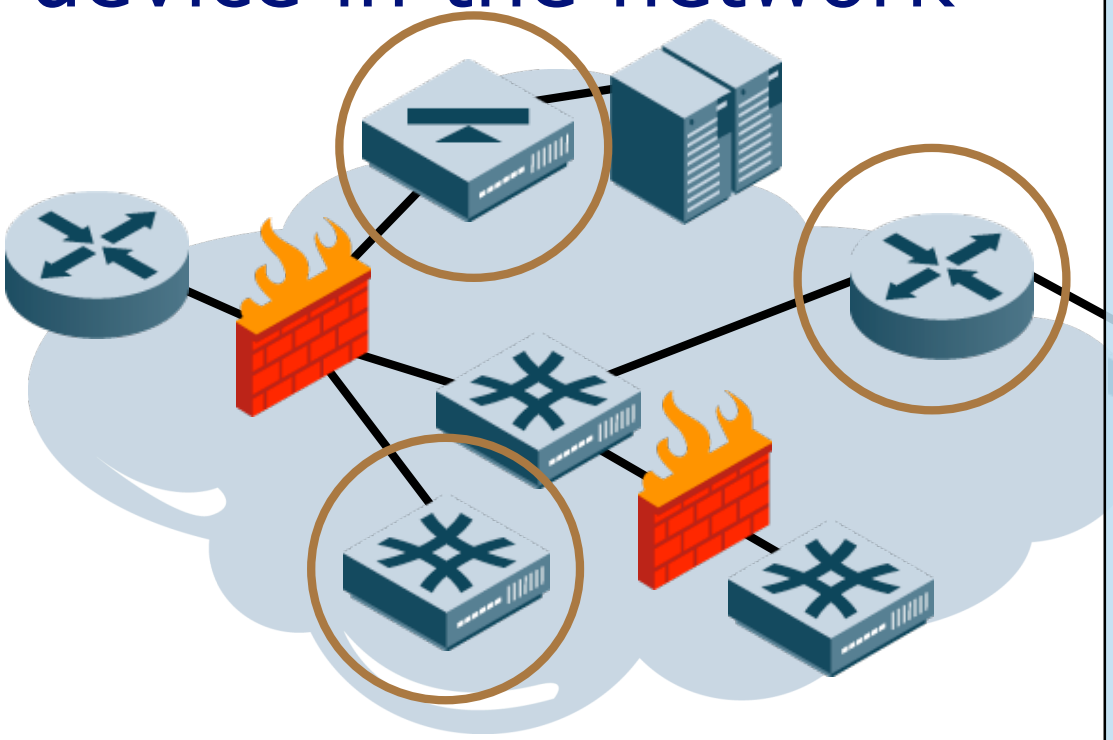


Your external router is a good first cleaner for traffic



- Anti-spoofing ACL starts here
- Block access to control plane on external network
- Block traffic you don’t want to waste logging on (Slammer, etc.)
- Alert on attempted control plane access
- Consider sending blocked traffic out to a monitoring port for your IDS to watch

Control traffic TO and THRU each device in the network



<u>Control plane management:</u> either a separate management network (best) or ACLs (good)

<u>Traffic management:</u> block and alert on common errors and worms; install anti-spoofing ACLs

16 Recommendations for Increasing Internal Security

- **Basic Physical Security and Settings**
- **Overall System Management Security**
- **Protecting the Device**
- **Integrating Securely with your Network**
- **Controlling Traffic Through the Network**

Part I: Physical Security and Settings

- **Basic Physical Security and Settings**
  - **Assume physical security is weak**
  - **For switches, turn off unused ports**
- **Overall System Management Security**
- **Protecting the Device**
- **Integrating Securely with your Network**
- **Controlling Traffic Through the Network**

1. Assume Physical Security is Weak

```
user jms privilege 1 password <pass>
line con 0
 password <pass>
 exec-timeout 10 0
 login local
 transport input none
line aux 0
 access-class 21 in
 exec-timeout 0 0
 transport input none
 no exec
```

"10 0" means timeout in 10 minutes, 0 seconds.

```
access-list 21 remark Nobody Gets In
access-list 21 deny any log
```

(…1) Physical Security Extends into your NOC/SOC

- **Do you have a password book updated and locked up somewhere?**
- **Do you have documentation on your routing infrastructure (including design documents)?**
- **Do you have documentation on your security infrastructure (including design)?**

- **Do you actually update and refer to this documentation?**
- **Do you have a change control process which includes documentation updates?**

2. For Switches, Turn off Unused Ports

```
interface range FastEthernet0/1 - 24
description UNUSED PORT
no ip address
shutdown
```

If you're really into security, you can use MAC address limits.

```
interface range FastEthernet0/1 - 24
switchport port-security
switchport port-security violation shutdown
switchport port-security maximum 1
```

… and then after a while …

```
switchport port-security mac-address sticky
write
```

Semi-Advanced 2: DHCP-based security controls

- **DHCP Snooping**
  - **You tell the switch which ports DHCP servers are on, and which have users. Switch enforces that only valid DHCP servers get to pass out addresses**
- **IP Source Guard**
  - **The switch enforces IP address on ingress based on what it learned via DHCP snooping**
- **Dynamic ARP Inspection**
  - **The switch enforces IP-to-MAC bindings in ARP requests/responses based on what it learned via DHCP snooping**

Part II: Overall System Management Security

- Basic Physical Security and Settings
- **Overall System Management Security**
  - **Log Everything Somewhere**
  - **Save Your Configs**
  - **Know What Time It Is**
  - **Talk SNMP Only To Your Friends**
  - **Use AAA Services If You Have Them**
- Protecting the Device
- Integrating Securely with your Network
- Controlling Traffic Through the Network

3. Log Everything Somewhere

Every device that has more than one IP address should have a "loopback0" set up that represents a canonical IP for the device

```
logging on
logging host 1.2.3.4
logging host 5.6.7.8 xml
logging trap level informational
logging source-interface loopback0
logging userinfo
!
service timestamps log datetime
```

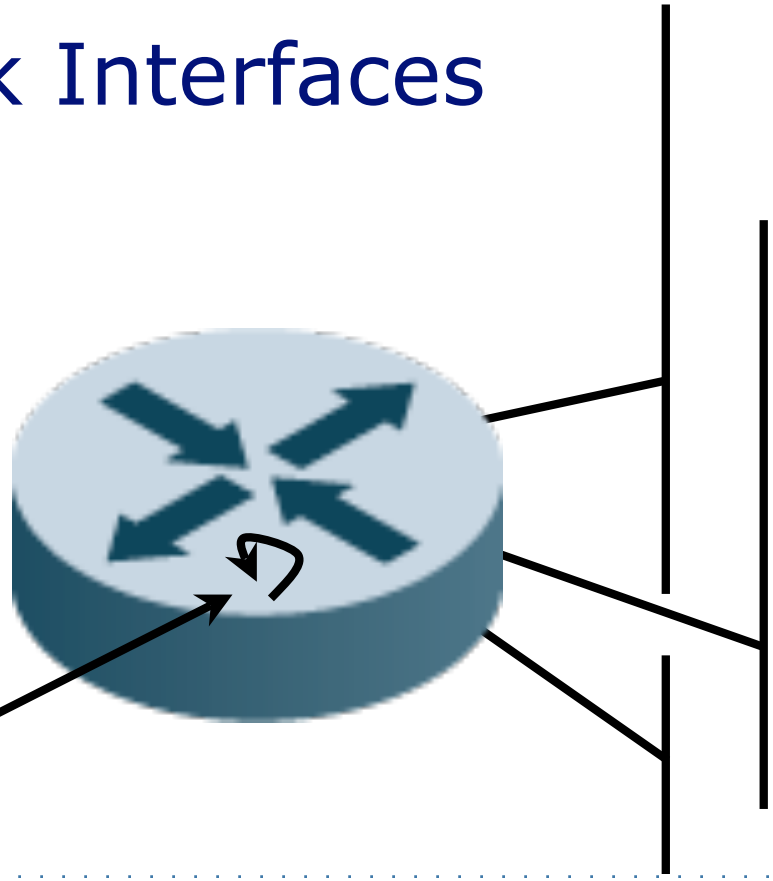
Assuming you have NTP, which we'll get to soon.

Logging has many more options, such as filtering and enabling/disabling specific streams of data. This will get you started.

Diversion: Loopback Interfaces

Question: What IP does traffic from the router itself use?

Answer: Unpredictable based on routing-du-jour, unless you try and make it predictable



```
interface loopback0
description Address for traffic sourced to/from this router
ip address 207.182.63.117 255.255.255.255
```

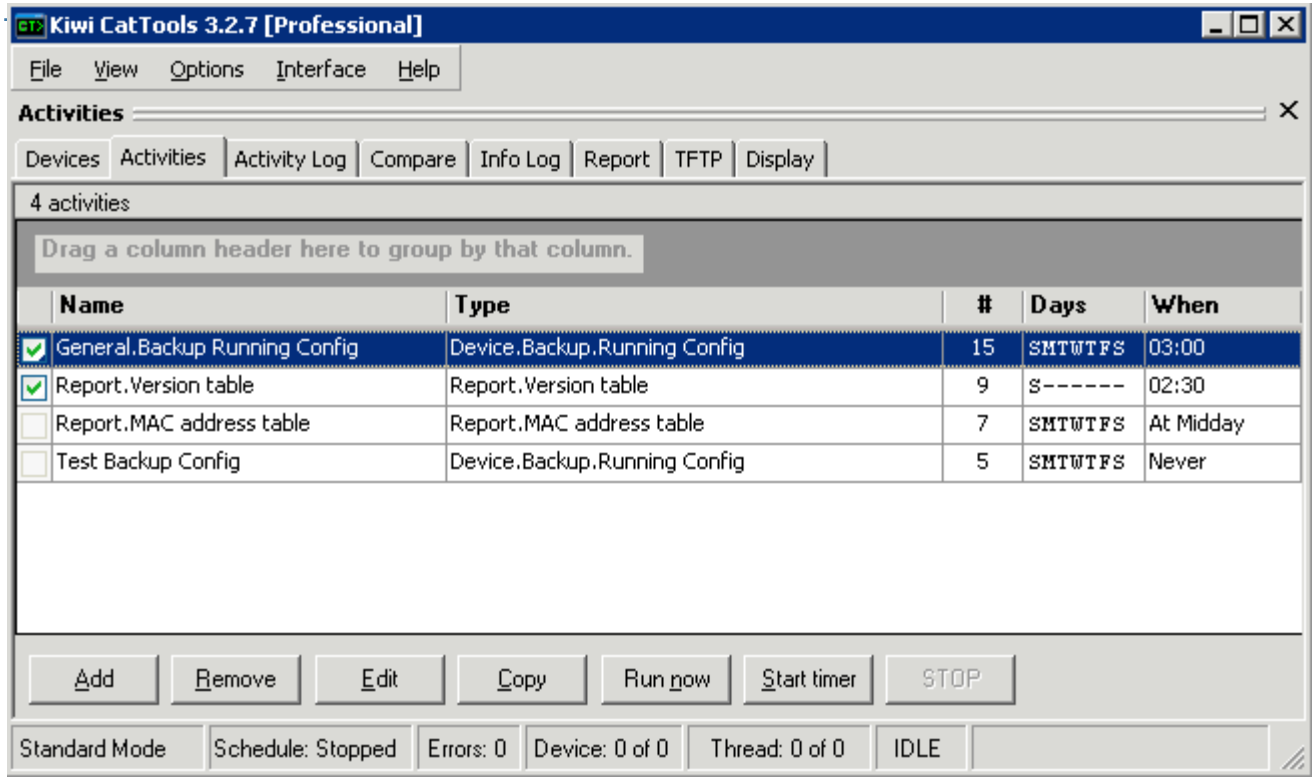
Services that can be bound to the loopback address should be

4. Save your configs!

```
DSL-GW3#copy running-config tftp:
Address or name of remote host []? 192.245.13.7
Destination filename [dsl-gw-confg]? dsl-gw3.config
32993 bytes copied in 16.932 secs (1949 bytes/sec)
DSL-GW3#
```

Good

Better



See also the very popular RANCID - Really Awesome New Cisco config Differ at http://www.shrubbery.net/rancid/

(…4) Audit Your Configuration

- **Outside help is always a good idea once in a while. Extra eyes never hurt!**
- **Center for Internet Security tools can score your configurations against the NSA security guidelines (slightly outdated, but invaluable nevertheless!)**
- **`http://www.cisecurity.org/bench_cisco.html`**

5. Know what time it is

```
ntp server 192.245.12.21 source Loopback0 prefer

ntp authenticate
ntp authentication-key 21 md5 <ntp-password>
ntp trusted-key 21
ntp server 192.245.12.21 key 21 prefer
```

If you are running NTPv3, use authenticated NTP

Unless you intend to be an NTP server, you can turn off service per-interface. WAN interfaces to Internet probably should be off.

```
interface serial3/0
ntp disable
```

6. Talk SNMP Only To Your Friends

```
access-list 6 remark Our Management Nets
access-list 6 permit 192.245.12.0 0.0.0.255
access-list 6 deny any log
```

```
no snmp-server community public RO
no snmp-server enable traps
no snmp-server system-shutdown
no snmp-server trap-auth
no snmp-server
!
snmp-server community notpublic RO 6
snmp-server location Where-is-the-box
snmp-server host 192.245.12.117 traps notpublic
```

This is SNMP v1/v2; you want SNMP v3 (authenticated!) if you can get it on your management station.

7. Use AAA Services If You Have Them

This one is a little too complicated to put in a simple snippet of code. However, the following general strategy should work:

1) Turn on AAA services (`aaa new-model`) and define RADIUS servers and keys

2) Define local users and enable secrets for emergency access when RADIUS is down

3) Create `aaa authentication`, `aaa authorization`, and `aaa accounting` statements to define AAA

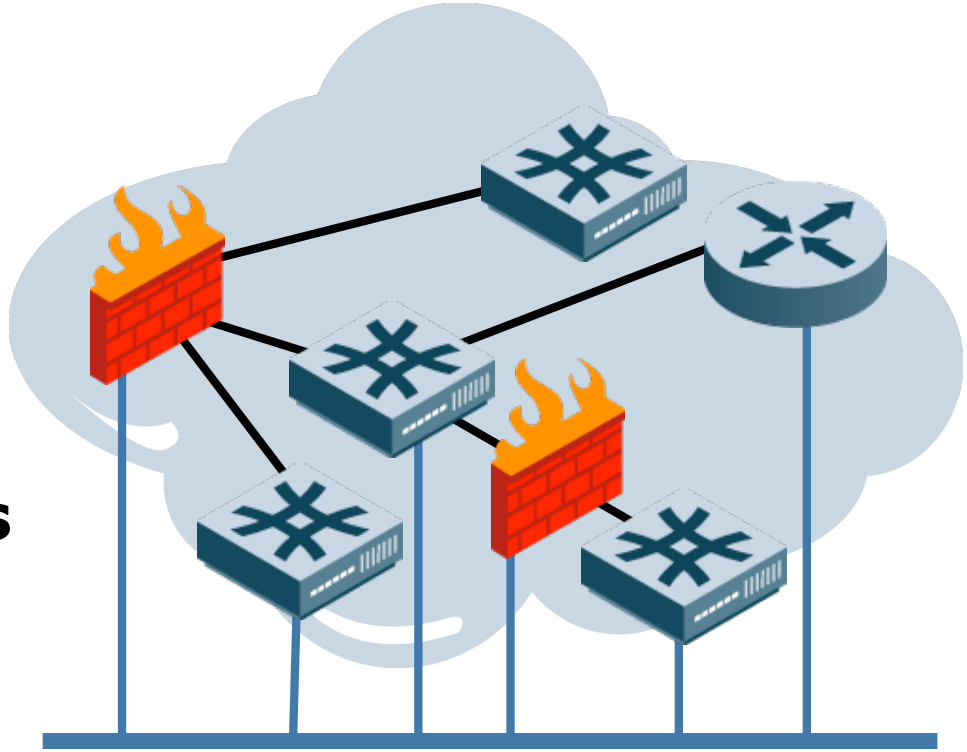
4) Apply login rules to access methods, such as VTY logins

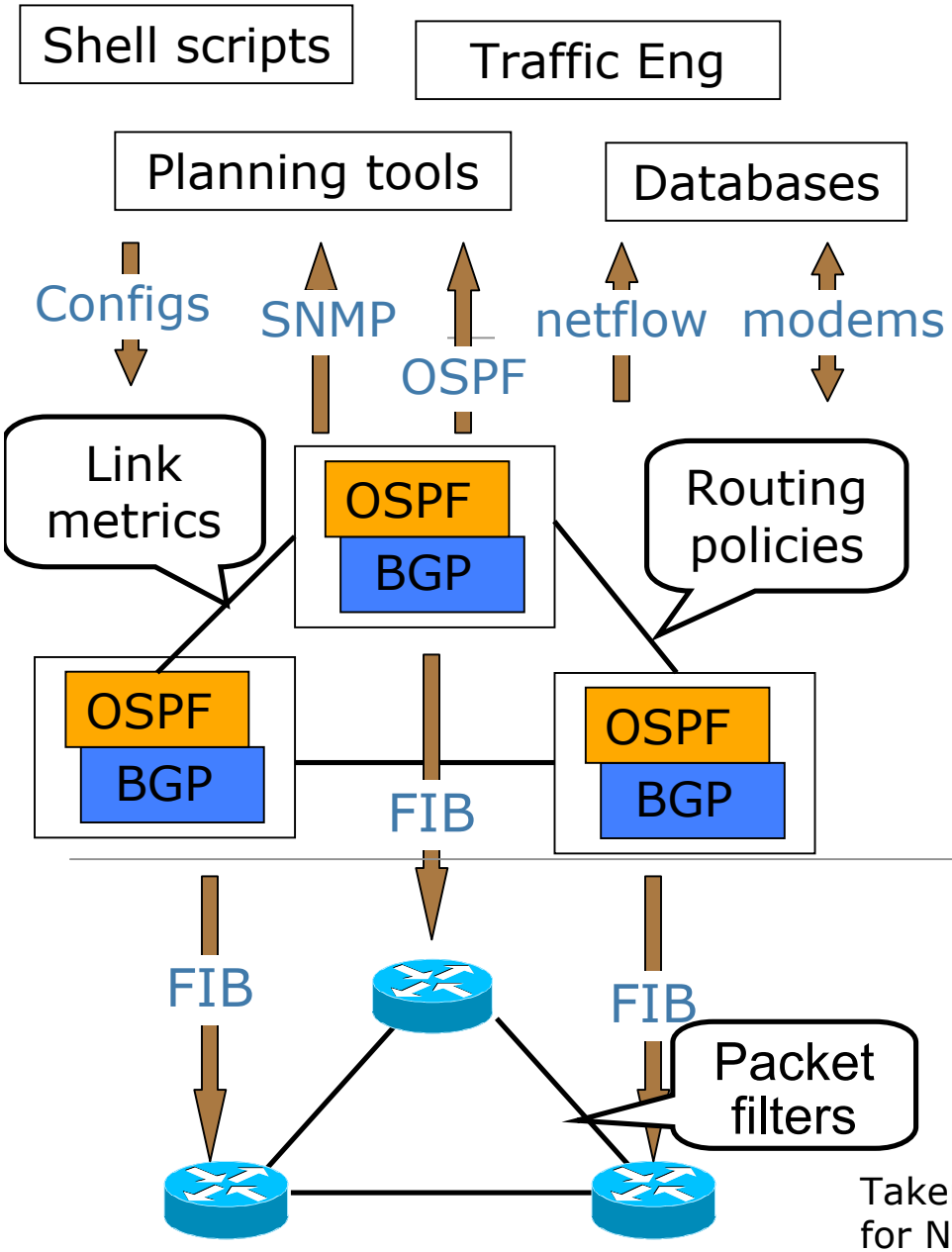
Part III: Protecting The Device

- Basic Physical Security and Settings
- Overall System Management Security
- **Protecting the Device**
  - **Separate your management plane from data & control planes**
  - **Disable everything you don't use**
  - **Use SSH if you can**
  - **Put ACLs on access**
- Integrating Securely with your Network
- Controlling Traffic Through the Network

8. Separate Your Management Plane from your Data Plane

- **Don't use VLAN 1 for management**
- **Dedicated a physical Ethernet port for management and run separate "access" network for management**
- **Same for console ports**
- **For larger networks, separate control (routing) and management as well**





Management Plane

- Figure out what is happening in network
- Decide how to change it

Control Plane

- Multiple routing processes on each router
- Each router with different configuration program
- Huge number of control knobs: metrics, ACLs, policy

Data Plane

- Distributed routers
- Forwarding, filtering, queueing
- Based on FIB or labels

Taken from: Maltz, *et al.*, "Rethinking the Systems for Network Control"

(…8) Switches are easy because they don't need IP addresses for anything else

```
vlan 21
name MANAGEMENT-VLAN
!
interface vlan 21
description Connection to MANAGEMENT network
ip address 192.245.12.117 255.255.255.0
ip access-group 6 in
!
interface fastethernet0/22
description Management Plane Access Port
switchport mode access
switchport access vlan 21
```

```
access-list 6 remark Our Management Nets
access-list 6 permit 192.245.12.0 0.0.0.255
access-list 6 deny any log
```

(…8) Remember that Switches and Routers are often Interchangeable

- **Many enterprises are using "L3 switches"**
- **If so, don't forget to separate out control plane (routing) from management as well**

- **"Routing interfaces are for routing. Management interfaces are for managing."**

Advanced 8: Use Control Plane Policing

- **"The Control Plane Policing feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of routers and switches against reconnaissance and denial-of-service (DoS) attacks."**
- **http://www.cisco.com/en/US/products/sw/iosswrel/ps1838/products_feature_guide09186a008052446b.html**

9. Disable Everything You Don't Use

```
no service tcp-small-servers
no service udp-small-servers
no ip bootp server
no ip finger
no service finger
no service config
no boot host (network, system)
no service pad
no ip source-route
no ip proxy-arp (per interface on routers)
no mop enabled (per interface, routers only)
no ip directed-broadcast
no ip domain-lookup (depends…)
ip http access-class 21
no ip http server (almost certainly)
no snmp-server (probably not)
```

```
access-list 21 remark Nobody Gets In
access-list 21 deny any log
```

Note that not all of these services are present in every IOS/CatOS release

9a. Common, but poor advice: turn off ICMPs

- **ICMPs are necessary for proper operation of routing systems. If you're scared of them, disable on untrusted interfaces only**

```
interface serial3/0
description I/F between us and bad guys
no ip unreachables
no ip redirects
no ip mask-reply
no ip directed-broadcast (this is valid for all I/Fs)
```

10. Use SSH if you can

- **Not every version of IOS supports SSH**
  - **What in the hell was Cisco thinking?**

```
hostname routerfoo
ip domain-name opus1.com
crypto key generate rsa
... several lines of output; suggest 1024 or 2048 bit keys ...
!
line vty 0 4
transport input ssh
access-class 6 in
```

11. Put ACLs on access

- **We've been putting ACLs on as we go**
- **Make sure you have ACLs on**
  - **VTY (Telnet, SSH)**
  - **HTTP server**
  - **SNMP**
  - **Anything else listening!**

```
bogus-gw#show ip socket
Proto    Remote        Port       Local        Port  In Out Stat TTY
OutputIF
 17 192.245.13.50      514 207.182.36.78    57564   0   0   20   0
 17 0.0.0.0              0 207.182.53.49       67   0   0 2211   0
 17 192.245.13.8      4609 207.182.53.49      161   0   0    1   0
 17   --listen--           207.182.53.49      162   0   0   11   0
 17   --listen--           207.182.53.49    51268   0   0    1   0
 17   --listen--           207.182.53.49      123   0   0    1   0
 17 192.245.13.250     514 207.182.36.78    55087   0   0   20 162
```

A Digression: How many VTYs?

```
DSL-GW#show line vty 0 100
    Tty Typ      A Modem  Roty AccO AccI    Uses   Noise  Overruns    Int
*   130 VTY      -     -      -    -   28     346       0      0/0      -
    131 VTY      -     -      -    -   28       3       0      0/0      -
    132 VTY      -     -      -    -   28       0       0      0/0      -
    133 VTY      -     -      -    -   28       0       0      0/0      -
    134 VTY      -     -      -    -   28       0       0      0/0      -
    135 VTY      -     -      -    -    -       0       0      0/0      -
    136 VTY      -     -      -    -    -       0       0      0/0      -

DSL-GW#config term
Enter configuration commands, one per line.  End with CNTL/Z.
DSL-GW(config)#no line vty 5
DSL-GW(config)#^Z
DSL-GW#
```

Gets rid of 5 and all higher numbered ones

11a. More on ACLs

- **Simple Security Rule:**

- **Every IP datagram aimed at your router or switch should go through an ACL before it hits the device**
- **That ACL should have a "default deny" policy on traffic aimed at the router**

- **The closer your device is to the Internet, the more critical this is**

Part IV: Integrating Safely

- Basic Physical Security and Settings
- Overall System Management Security
- Protecting the Device
- **Integrating Securely with your Network**
  - **All routing updates should be authenticated**
  - **Understand CDP**
  - **Use static VLAN config if at all possible**
  - **Disable Spanning Tree if at all possible**
- Controlling Traffic Through the Network

12. All routing updates should be authenticated

- **OSPF**

```
int fastethernet0/1
ip ospf message-digest-key 1 md5 <goodpassword>
```

- **RIP**
  - **Don't use RIP. Come on, this is 2007.**
- **EIGRP, IS-IS**
  - **More complex than OSPF, but same idea: point to a key to be used for authentication on each interface running the routing protocol**
- **BGP**

```
router bgp 6373
neighbor 192.245.14.117 remote-as 701
neighbor 192.245.14.117 password <goodpassword>
```

12a. Miscellaneous Routing Notes

- **Mark interfaces as "passive" if they shouldn't be blabbing multicast routing (OSPF, RIP, etc.)**
- **Use distribute lists to ensure you don't get routing updates from your ISP for yourself**
  - **And you may want to filter lots of other things too**
  - **Try not to send a default route out if your ISP is dumb**
  - **Beware lingering stability issues w/ OSPF distribute lists**
- **BGP Dampening can help to secure your routing fabric**
- **Unicast Reverse-Path Verification is dangerous**
  - **If you use it, use it with care**

13. Understand CDP

- **CDP is officially a bad thing**
  - `no cdp run`
- **CDP is often a nice thing**

```
cdp run
interface range fastethernet0/1 - 24
no cdp enable
interface fastethernet0/15
cdp enable
!

bogus-gw#show cdp neigh
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID    Local Intrfce     Holdtme    Capability  Platform  Port ID
AuntHollis   Ser 0/0            167          R         3640      Ser 0/1
main-gw      Fas 2/0            138         R S        3845      Fas 0/0
backup-gw    Fas 2/0            164          R         7140-2FE  Fas 0/0
```

14. Use Static VLAN Configuration Unless You Have No Choice

```
no vtp mode
no vtp password
no vtp pruning
!
interface fastethernet0/1
description Normal Device Interface
switchport mode access
switchport nonegotiate
!
interface fastethernet0/2
description 802.1q interface
switchport mode trunk
switchport nonegotiate
switchport trunk allowed vlan 21, 22, 23, 25
switchport trunk native vlan 999
```

VTP can be used safely, but most networks don't need it

DTP is always a bad idea. Ports are either 802.1q or not.

List all legal VLANs explicitly

```
vlan 999
name BLACKHOLE-VLAN
interface vlan 999
description Packets check in…
shutdown
```

15. Spanning Tree should be off unless you plan to have loops

- **Spanning tree configuration was supposed to be easy and automatic and safe**
  - **It's not and it's not and it's not**
- **Networks that need spanning tree protocol should use it**
  - `bpduguard` **and** `root guard` **can help protect against topology meltdowns**
  - `spanning-tree portfast bpdufilter default` **turns on BPDU filtering for all ports with portfast on (i.e., device ports which should not be playing in your spanning tree in the first place)**

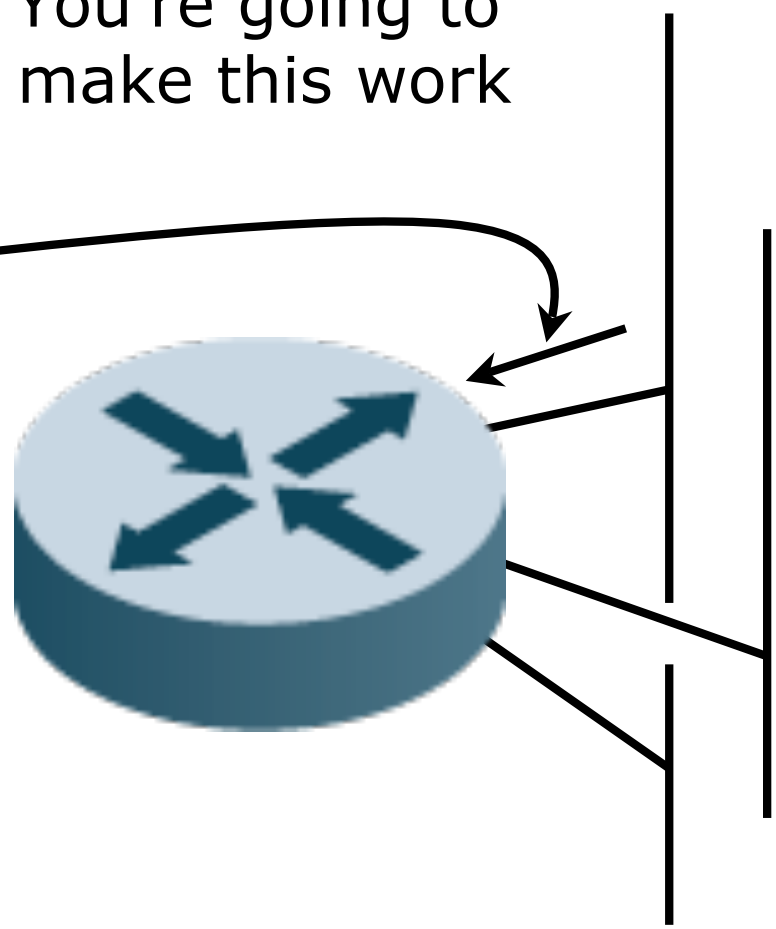
Part V: Applying ACLs Control Traffic

- **Basic Physical Security and Settings**
- **Overall System Management Security**
- **Protecting the Device**
- **Integrating Securely with your Network**
- **Controlling Traffic Through the Network**
  - **Use ACLs to apply controls on traffic**

16. Apply ACLs to control traffic

Sorry: no recipes here. You're going to have to engage brain to make this work

- **Each IP interface should have input ACLs to**
  - **Block spoofed packets**
  - **Block "impossible" packets**
  - **Block inappropriate packets**
  - **Block services you never want to see**



Border Router Starting Points: Filtering IN from Internet

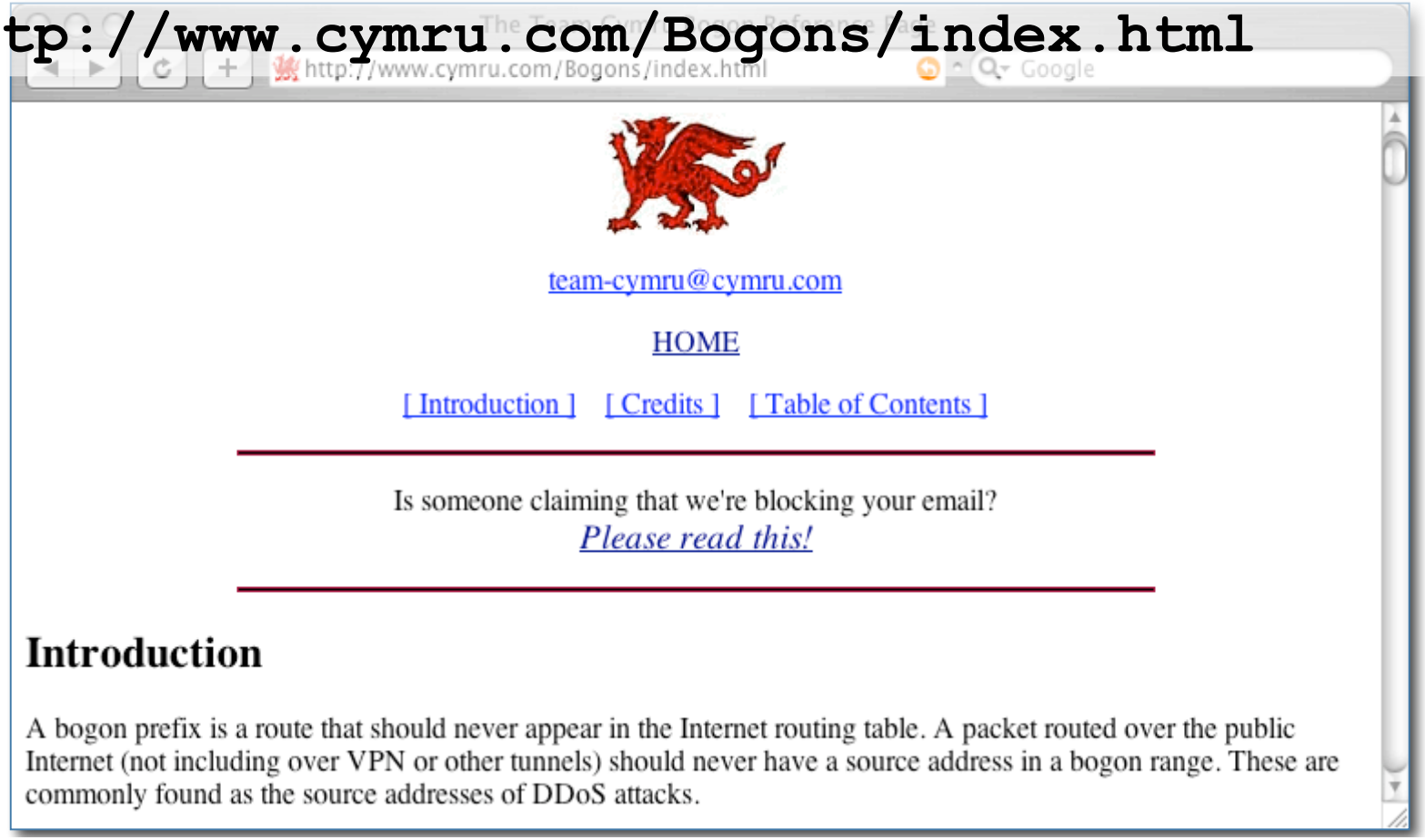
- **Block RFC1918 IP addresses in both directions**
  - `deny ip 10.0.0.0 0.255.255.255 any log`
  - `deny ip 192.168.0.0 0.0.255.255 any log`
  - `deny ip 172.16.0.0 0.15.255.255 any log`
  - `deny ip any 10.0.0.0 0.255.255.255 log`
  - `deny ip any 192.168.0.0 0.0.255.255 log`
  - `deny ip any 172.16.0.0 0.15.255.255 log`
- **Block packets to the "NSA List of Risky Services" (if you have a fast router)**
  - `1/tcp,udp; 7/tcp,udp; 9/tcp,udp; 11/tcp; 13/tcp,udp; 15/tcp; 19/tcp,udp; 37/tcp,udp; 43/tcp; 67/udp; 69/udp; 95/tcp,udp; 111/tcp,udp; 135/tcp,udp; 137/tcp,udp; 138/tcp,udp; 139/tcp,udp; 177/udp; 445/tcp; 512/tcp; 515/tcp; 517/udp; 518/udp; 540/tcp; 1434/udp; 1900,5000/tcp,udp; 2049/udp; 6000-6063/tcp; 6667/tcp; 12345-6/tcp; 31337/tcp,udp`
  - `79/tcp; 161/tcp,udp; 162/tcp,udp; 513/tcp,udp; 514/tcp,udp; 550/tcp,udp`

Border Router Starting Points (pt 2): Filtering IN from Internet

- **Block Spoofed Packets**
  - `deny ip 192.245.12.0 0.0.0.255 any log`
- **Block Impossible Packets**
  - `deny ip 127.0.0.0 0.255.255.255 any log`
  - `deny ip 0.0.0.0 0.255.255.255 any log`
  - `deny ip host 255.255.255.255 any log`
  - `deny ip 224.0.0.0 15.255.255.255 any log`
  - `deny ip 169.254.0.0 0.0.255.255 any log`

Border Router Starting Points (pt 3): Filtering IN from Internet

- **Use Bogon Filtering**
  - **Your ISP should be doing this already!**
- **`http://www.cymru.com/Bogons/index.html`**



Border Router Starting Points: Filtering OUT to Internet

- **Assuming your network is 207.182.32.0/19**

```
ip access-list extended DISALLOWTOOUTSIDE
deny ip any host <badguy> log
permit ip 207.182.32.0 0.0.31.255
deny ip any any log
!
!
interface FastEthernet0/1
description Main connection to ISP
ip access-group DISALLOWTOOUTSIDE out
```

All Router Possibilities: Common Exploits to be Blocked

- **Land Attack**
  - **Block IP packets where source and dest are same as the router's IP addresses**
- **Smurf Attack**
  - **Block IP packets addressed to a subnet broadcast address**
  - **Can also be handled with "no ip directed-broadcast"**

- **Value of these is low nowadays**

All Router Possibilities: Coarse Access Controls

- **A router or switch should not be used where you need a firewall**
- **Not all threats require a firewall**

- **Coarse access controls can be helpful**
  - **E.g. "block access from VoIP to Printer network"**
  - **E.g. "block outbound connects from Printer VLAN"**
  - **E.g. "block Internet traffic that shouldn't exist"**
- **Nothing wrong with layered defenses**
- **Generally a "default deny" policy shows you've figured out what should be going on**

Some routers support true stateful firewalling

- **Technologically, router firewalls are weaker than firewall firewalls**
- **Performance may be an issue. <u>Be careful!</u>**
- **The real kicker is management**

- **Advanced Topics:**
  - **Cisco IOS CBAC (stateful access controls)**
  - **Cisco IOS IDS/IPS**
  - **Cisco IOS brand new firewall feature set (12.4 T-train feature on ISRs) including zone-based firewall, IM/P2P/ HTTP inspection, stateful failover, ingress rate-limiting, and SNMP monitoring**

Thanks!

Joel Snyder
Senior Partner
Opus One
jms@opus1.com

Huge thanks to members of the Cisco-NSP list who gave up their time on the weekend to help with this presentation: Adrian Chadd, Roland Dobbins, Richard Golodner, Brad Henshaw, Gniewomir Przemyslaw Krol, Alan Buxey, Matthew Lange

The following resource slides taken from:

http://www.nanog.org/mtg-0602/greene.html

By Barry Greene and Roland Dobbins (Cisco)

SP Security Primer 101

Peers working together to battle Attacks to the Net
Version 1.3

Where to go to get more?

- NANOG Security Curriculum
  - **Sessions recorded over time which builds a library for all SPs to use for their individual training, staff empowerment, and industry improvements.**
- **http://www.nanog.org/ispsecurity.html**

Remote Triggered Black Hole Filtering

- **Remote Triggered Black Hole Filtering is the most common ISP DOS/DDOS mitigation tool.**
- **Prepare your network:**
  - ftp://ftp-eng.cisco.com/cons/isp/essentials/ **(has whitepaper)**
  - ftp://ftp-eng.cisco.com/cons/isp/security/ **(has PDF Presentations)**
  - **NANOG Tutorial:**
    - http://www.nanog.org/mtg-0110/greene.html **(has public VOD with UUNET)**

Ingress Packet Filtering

- **BCP 38/ RFC 2827**
- **Title: Network Ingress Filtering: Defeating Denial of Service Attacks which Employ IP Source Address Spoofing**
- **Author(s): P. Ferguson, D. Senie**
- **`http://www.ietf.org/rfc/rfc2827.txt`**

NetFlow—More Information

- **Cisco NetFlow Home—http://www.cisco.com/warp/public/732/Tech/nmp/netflow**
- **Linux NetFlow Reports HOWTO—http://www.linuxgeek.org/netflow-howto.php**
- **Arbor Networks Peakflow SP—http://www.arbornetworks.com/products_sp.php**

More Information about SNMP

- **Cisco SNMP Object Tracker—http://www.cisco.com/pcgi-bin/Support/Mibbrowser/mibinfo.pl?tab=4**
- **Cisco MIBs and Trap Definitions—http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml**
- **SNMPLink—http://www.snmplink.org/**
- **SEC-1101/2102 give which SNMP parameters should be looked at.**

RMON—More Information

- **IETF RMON WG—**http://www.ietf.org/html.charters/rmonmib-charter.html
- **Cisco RMON Home—** http://www.cisco.com/en/US/tech/tk648/tk362/tk560/tech_protocol_home.html
- **Cisco NAM Product Page—**http://www.cisco.com/en/US/products/hw/modules/ps2706/ps5025/index.html

BGP—More Information

- **Cisco BGP Home—**http://www.cisco.com/en/US/tech/tk365/tk80/tech_protocol_family_home.html
- **Slammer/BGP analysis—** http://www.nge.isi.edu/~masseyd/pubs/massey_iwdc03.pdf
- **Team CYMRU BGP Tools—** http://www.cymru.com/BGP/index.html

Syslog—More Information

- **Syslog.org - http://www.syslog.org/**
- **Syslog Logging w/PostGres HOWTO— http://kdough.net/projects/howto/syslog_postgresql/**
- **Agent Smith Explains Syslog— http://routergod.com/agentsmith/**

Packet Capture—More Information

- **tcpdump/libpcap Home—** **http://www.tcpdump.org/**
- **Vinayak Hegde's Linux Gazette article—** **http://www.linuxgazette.com/issue86/vinayak.html**