TECH.CON.07

PBS.

Security Challenges in the Face of Convergence

Matt Burrough, *NPR Labs*
Scott Gebhardt, *PBS*
Ken Walters, *PBS*

Security of HD Radio Broadcast Systems

Areas of Concern and Mitigation Strategies

Acknowledgements

- NPR Labs
- Rochester Institute of Technology

Why conduct this study?

- Concern for the safety of stations' equipment as their resources become Internet-enabled.

Why…Cont.

- A desire to improve the quality of future products and updates by raising awareness.
- General curiosity on the part of the researcher.

Specific goals

- To find out whether:
  - Equipment in the broadcast chain is susceptible to attack or exploit.
  - Guides or best practices to prevent attacks.

A Few Definitions

- PAD – Program Associated Data; used to display text on HD radios
- TCP – A Networking Protocol used by software connecting to the Importer

Methodology

- Testing performed on importers and exciters from two major vendors, as well as a number of other related products both directly and remotely.

Methodology cont.

- Tests were conducted from Windows and Linux-based systems using both hand-coded and off-the-shelf tools.

Points of Concern

- Security of Program Associated Data (PAD).
- Security of multicast audio feeds.
- Authentication security.

Points of Concern cont.

- Importer/Exciter safety from malware.
- Attacks against default, non-radio related services.

Exploiting PAD

- Attacks were performed as both an “outsider” and an “insider” on Importer 1.1.2 software.

Exploiting PAD cont.

- PAD for multicast channels can be shut down remotely and illegitimate text can be injected.

Example PAD Attack

1. Attacker finds the IP address of an importer and the source sending PAD information.

Example PAD Attack cont.

2. Attacker forges sender IP and sequence number and sends RESET packets.

Example PAD Attack cont.

3. Importer drops its connection to the legitimate sender.
4. Attacker sends Importer custom PAD.

Protecting PAD

- Run PAD applications directly on the Importer and firewall PAD Ports.
- Directly connect the Importer to the Exciter using a crossover network cable.

Protecting PAD cont.

- If PAD ports must be Internet-accessible, move them to non-standard ports and apply restrictive firewalls.

Multicast Audio

- Same issues as PAD.
- Slightly harder to attack due to format of file transfer.
- Can benefit from same methods of protection.

Changes in v2

- Username/Password required, but sent as plain text.
- Former Importer ports all mapped through TCP port 1010.

Changes in v2 cont.

- PAD moved from Importer to media provider.

Authentication

- Some services (i.e., PAD) don’t require authentication.
- On services like SSH, disable root account logons.

Authentication cont.

- Disable telnet, rsh, and other non-encrypted services.
- Use smart password policies.

Beware of Malware

- Since Importers & Exciters are PCs, they are susceptible to viruses.
- Don’t use them for daily tasks.

Beware of Malware cont.

- Keep them patched and updated, and consider antivirus & firewall software (carefully).

Non-Radio Services

- The operating systems used on Importers and Exciters run standard PC services.
- These can contain vulnerabilities or other weaknesses.

TECH.CON.07

Services to Consider

Importers: Web (80), SMTP (25), RPC (135)

Exciters: Telnet (23), VNC (5900+), SSH (22), Shell (514), RPC (111), X11 (6000), Web (80)

Conclusion

- Security measures designed for PCs have a place in HD broadcasting.
- Risk can be minimized by removing unneeded point of attack.

Conclusion cont.

- Thoughtful design & setup can help further mitigate risk.

Protecting Broadcast Network Segments

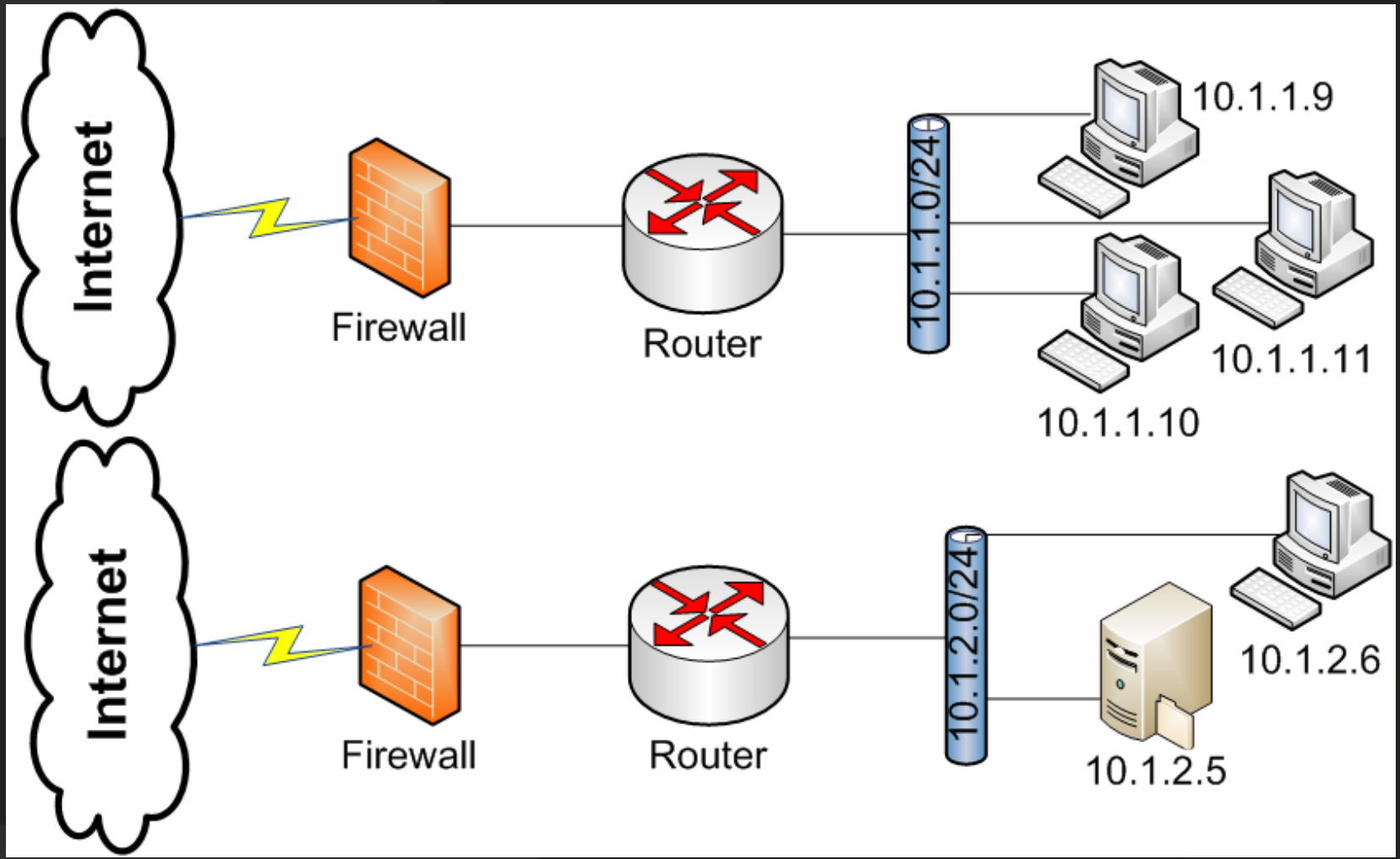
Strategies That Work

Tech.Con.07

PBS.

Isolated Broadcast and IT Networks

TECH.CON.07


Internet
Firewall
Router
10.1.1.0/24
10.1.1.9
10.1.1.11
10.1.1.10
Internet
Firewall
Router
10.1.2.0/24
10.1.2.6
10.1.2.5

Isolated “Pros”

- Least chance of cross-contamination
- Separation of policies for Broadcast and IT

Isolated “Pros”

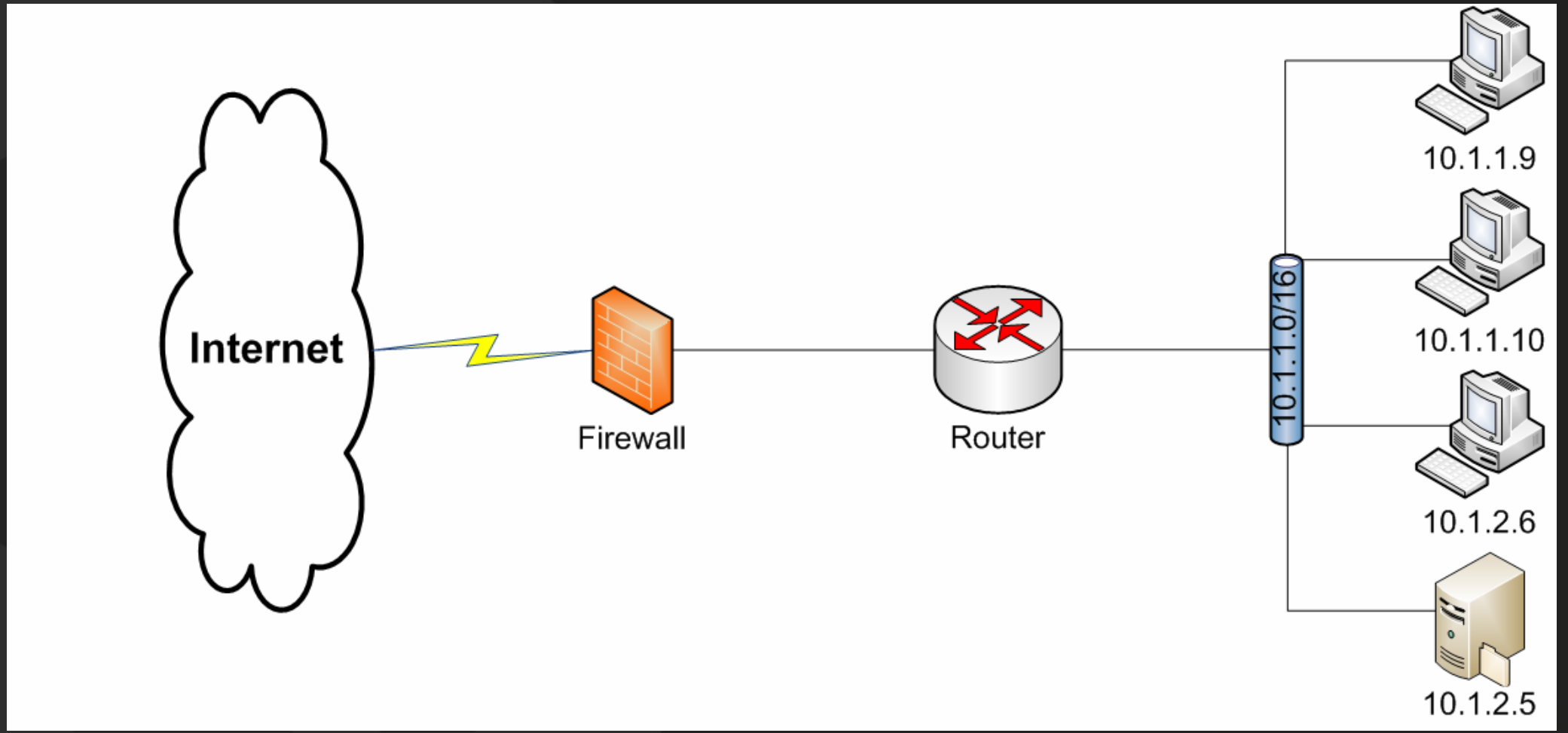
- Network and system designs specific to environmental needs

Isolated “Cons”

- Increased cost
- Departmental segregation
- Difficult file sharing
- More network administration

Fully Connected Broadcast and IT Networks

TECH.CON.07


Internet
Firewall
Router
10.1.1.0/16
10.1.1.9
10.1.1.10
10.1.2.6
10.1.2.5

Fully Connected “Pros”

- Reduced cost
- Departmental integration
- Uncomplicated file sharing

Fully Connected “Pros”

- Policy uniformity
- Less network administration

Fully Connected “Cons”

- Highest risk of cross contamination
- Policy decision making more complex
- Priorities for use of network

Limited Access Between Broadcast and IT Networks

Limited Access “Pros”

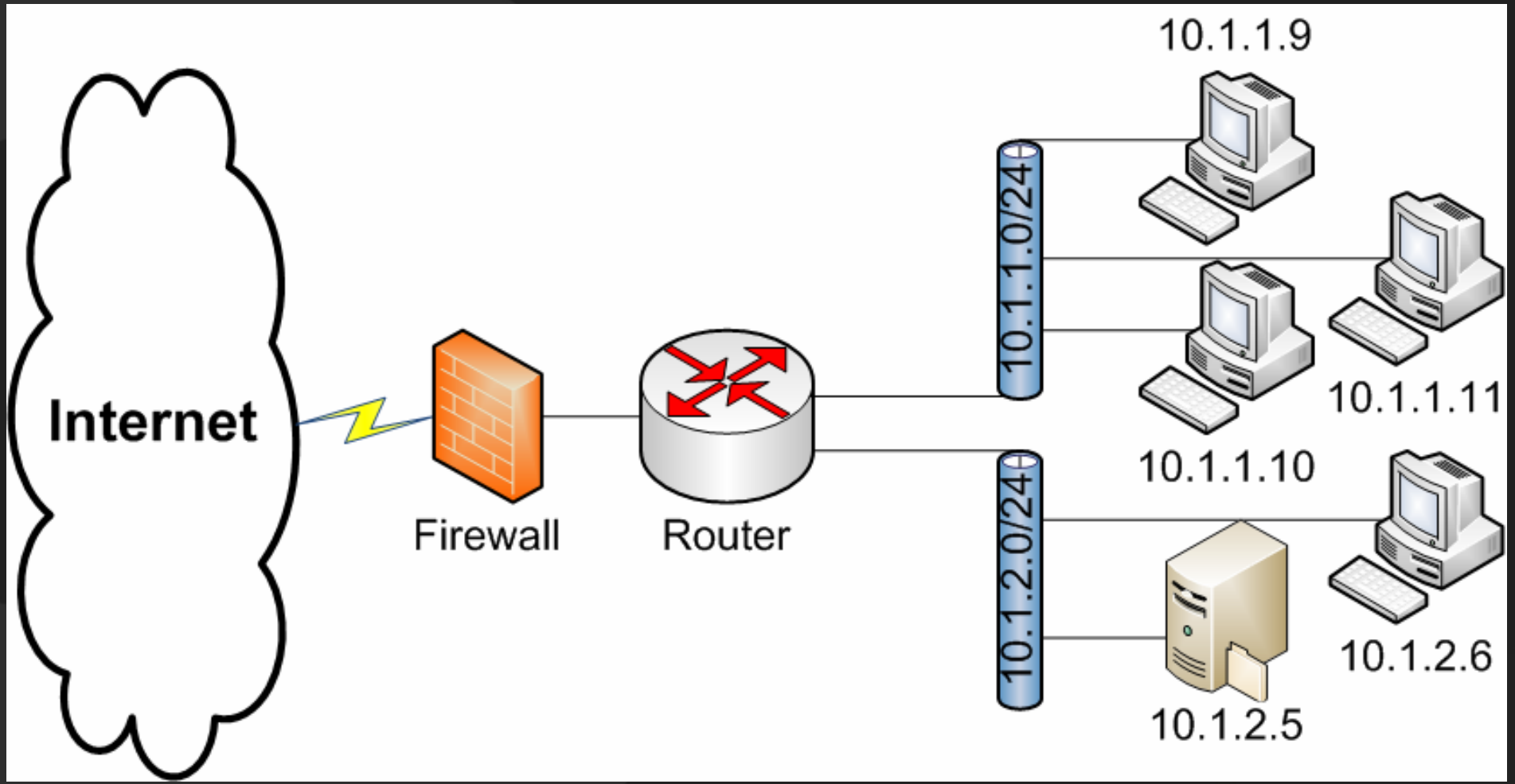
- Reduced cost
- Decreased chance of cross contamination
- Departmental integration
- Controlled file sharing

Limited Access “Cons”

- Defining boundaries
- Security vs. Functionality
- More complex network administration

Controlling Limited Access

- Access Control Lists (ACL) are a common way to control limited access between networks on firewall or router interfaces


10.1.1.9
Internet
10.1.1.0/24
10.1.1.11
10.1.1.10
Firewall
Router
10.1.2.0/24
10.1.2.6
10.1.2.5

Some attributes to control limited access include:

- Source address of the traffic
- Destination address of the traffic
- Upper-layer protocols

Implementing Limited Access

- Create the Access Control List
- Apply the ACL to an interface

Example - Access-list

```
ip access-list extended moc
permit ip host 10.1.1.9 host 10.1.2.5
```

Example Continued

permit tcp host 10.1.1.10 host 10.1.2.5 eq 20

permit tcp host 10.1.1.10 host 10.1.2.5 eq 21

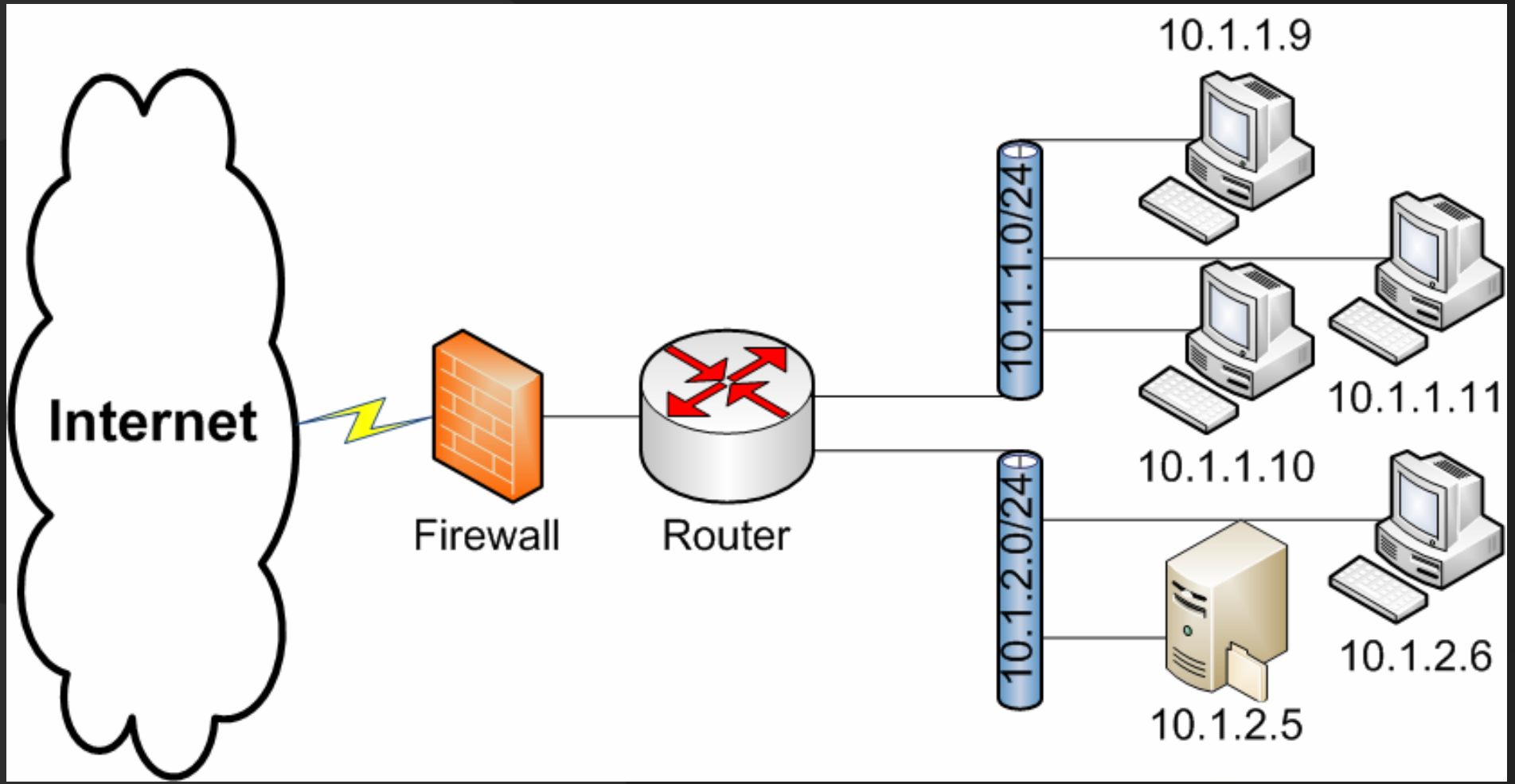
deny ip any any

Applying ACL to an Interface

```
interface Vlan10
Ip address 10.1.1.1 255.255.255.0
ip access-group moc-isolation out
```

ACLs

- For more access control, ACLs can be applied both inbound and outbound


10.1.1.9
Internet
10.1.1.0/24
10.1.1.11
10.1.1.10
Firewall
Router
10.1.2.0/24
10.1.2.6
10.1.2.5

Summary

1. Isolated Broadcast and IT networks
2. Fully connected Broadcast and IT networks

Summary Continued

- Limited access between Broadcast and IT networks

Misconception

- There is a fair amount of misinformation about firewalls and the like (ACLs) slowing things down.

IT Infrastructure in the Broadcast Environment

Strategies for Safe Integration

Tech.Con.07

PBS.

What's Been Happening

- Information Technology is driving advancements in audio and video
- Ingest, edit, playout are file based this changing workflow, processes, and behavior

What's Been Happening

- Security is the new challenge
  - Application
  - Network
  - Server OS

Benefits

- More time spent on content means more *creativity*
- Less time spent on mechanics
- Cost containment?

Benefits

- Leverage IT resources within organization
- Network connectivity enables integration

Challenges

- Landscape constantly changing
  – operating systems, software
- Constantly evolving standards and practices to meet new security threats

Challenges

- Budgeting
  - Software and integration are now capitalized
  - Hardware relatively cheap

Perfect World

- Fully networked
- Firewall in place
- AV solution
- Critical patches
- With No performance impact

Reality

- Anti-Virus, maybe
- Scanning exclusions
- Delayed critical OS patches

Reality

- Firewall, maybe
- Controlled network access
- Policies and procedures

Reducing The Risks

- Leverage both IT and Eng strengths - respect what each brings to the mix:
  - –Experience in *the wild*
  - –Broadcast Operations

Reducing The Risks

- Vendor “encouragement”
  - –AV, OS patches, best practices
- Policies and procedures
- Network control

IT should keep in mind

- Broadcast apps and what they produce are business critical
- Broadcast applications can be “delicate”

IT should keep in mind

- Impact of impaired system can be great
- B’cast vendors can be different than IT vendors

B’cast should keep in mind

- Many vectors
  - –OS, services, applications
  - –Peripherals
  - –IP network
  - –People

B’cast should keep in mind

- Anti-Virus critical
- OS critical patching mandatory

“Encourage” Vendors

- Understand vendor’s commitment to security - *before you buy*
- Certify an Anti Virus solution and stay current

“Encourage” Vendors

- Support OS critical patch application
- Staying current with OS releases

“Encourage” Vendors

- Harden the operating system
- Encryption & Strong passwords
- Use modern programming practices
  - –Programs as Services

Policies and Procedures

- No Web access, IM, FTP, etc.
- No email
- Beware of USB, floppy or CD drives

Policies and Procedures

- Business work only
- Use a file proxy
- Beware of service laptops

Anti-Virus In Depth

- You need it
- Each product is a little different
- Test drive them

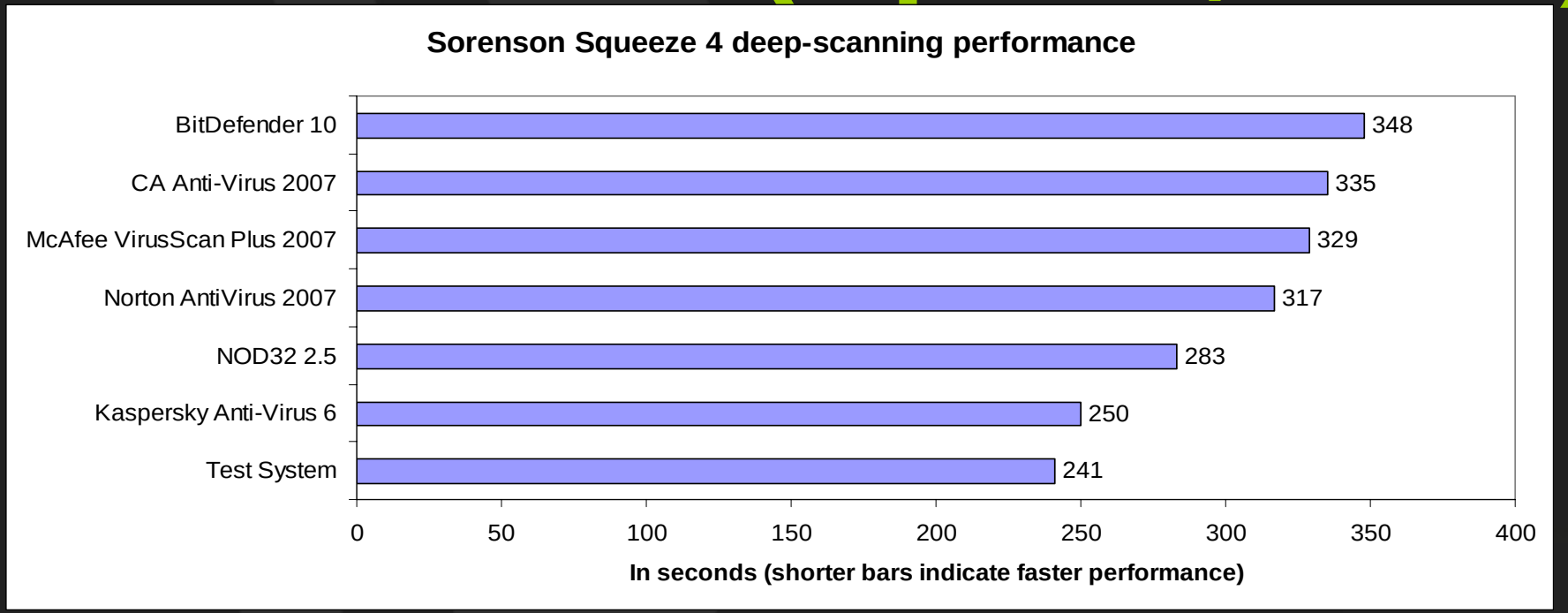
Anti-Virus In Depth

- Exclusions
  - Processes
  - File type or Location
- Keep tuning until you get it right

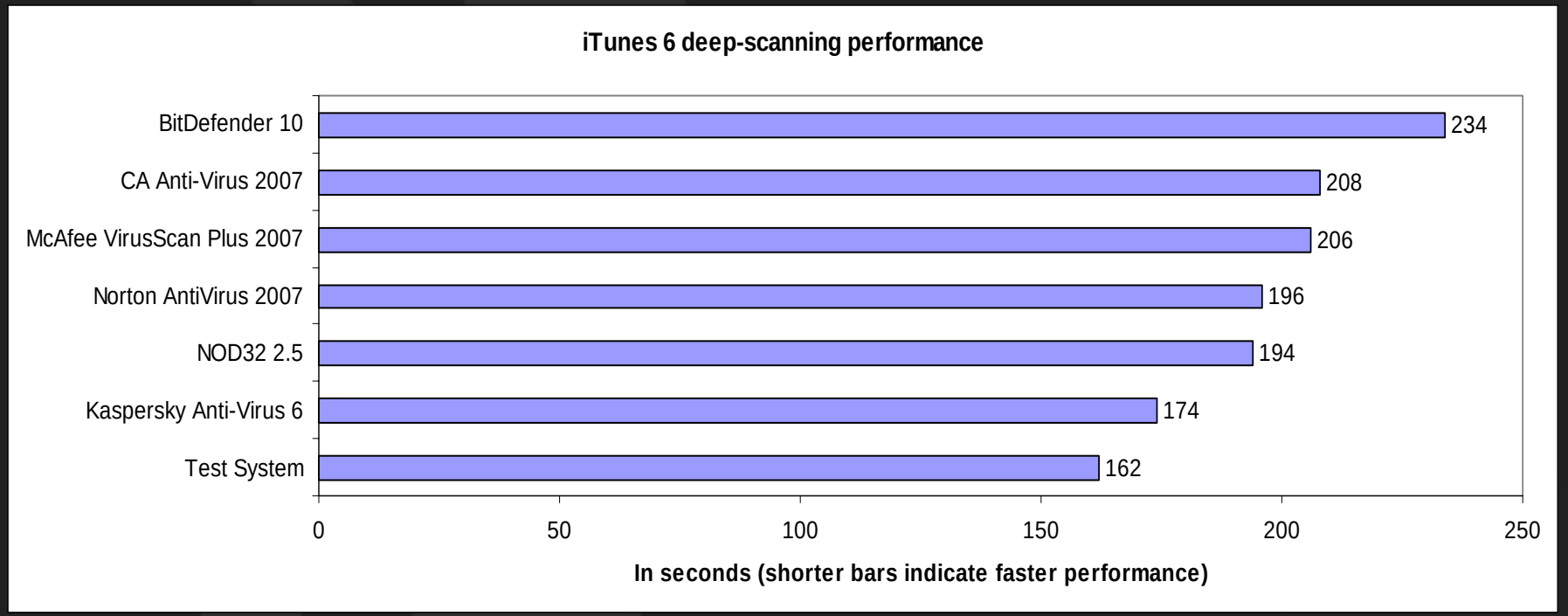
Anti-Virus In Depth

- Check system requirements
- Performance:
  - –Boot speed, scan speed
  - –On access vs. full scan
  - –Impact on applications

CNET Labs (April 7, 2006)



CNET Labs (April 7, 2006)



Web Resources

- www.virusbtn.com VB100 Award and Logo Program
- http://www.av-comparatives.org/

Summary

- IT is fueling productivity and creativity
- Security cannot be an afterthought

Summary

- Modern programming practices and current versions
- Defense in Depth – Network, AV, Firewalls, OS Hardening

Questions?

mburrough@npr.org
sgebhardt@pbs.org
kwalters@pbs.org

PBS.

TECH.CON.07

PBS.