Virtualization: Enough Holes to Work Vegas

Defcon 15
Las Vegas, 2007

D.J. Capelis
University of California, San Diego

Introductory Notes

- Mostly known issues
- Mostly design flaws, not entirely bugs
- Documented behavior
- (So slightly less testing)
  - VMWare Server, not ESX or VI3.
- This is still untenable

Overview

- Review
- Isolation isn't
- Covert channels
- Virtual machines on a network
- Virtual machines changing the network
- Live migration
- Questions, heckling, grandiose proposals and accusations of hating freedom

Overview of Technologies

Technology	Example
• OS Level Virt	→ Zones/UML/openVZ
• Paravirtualization	→ Xen
• Full Virt w/ HW	→ KVM, Xen
• Full Virt w/o HW	→ VMWare, KQEmu
• Full Emulation	→ QEmu, Bochs

The Features

- Freeze / Thaw / Snapshotting
- Decoupled Hardware
- Another Layer of Protection
- Live Migration
- Dynamic Deployment / Creation

The Hype

- Reliability
  - No longer bound to hardware, who cares about failures!
- Consolidation
  - Take many machines, use less of them. Better utilization of physical hardware.
- Isolation
  - Take many tasks, isolate them from each other. Don't you feel more secure already?

Attacking Isolation

- Shared hardware attacks
  - Thought the SMT attacks were old news?
  - Similar things on other shared hardware
- Attacking the host scheduler
- Did you want to actually... use that video card? (Or other hardware device? USB?)
  - Moment you pass real hardware, you can wedge the entire box.
- Covert Channels

More on Covert Channels

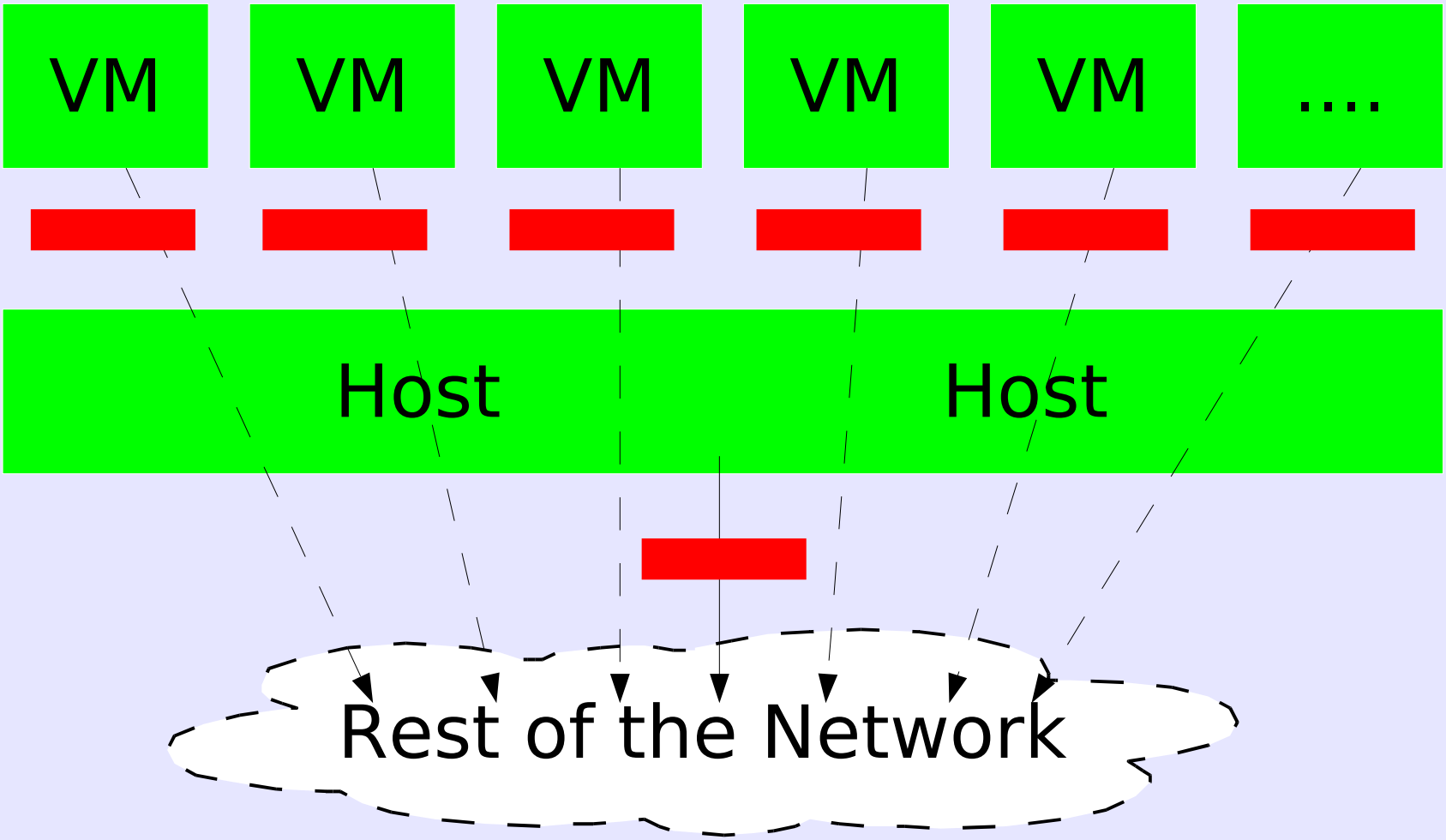
- Use Resources
  - Use something on one
  - Detect on another
    - RDTSC can help (or any half-decent timesource)
- Pass data in Layer 2
  - Turns out... very few of us use EBTables.
  - Mess with Novell, use IPX
  - More of an Apple hater? Use appletalk!
  - Old School? Want to try DECNet?

Networking Issues

- Bypass host firewall
  - Pick whatever IP you'd like
  - VMWare bypasses by default in bridged mode
- Promiscuous Mode
- MAC impersonation
- Spoofing is easier again

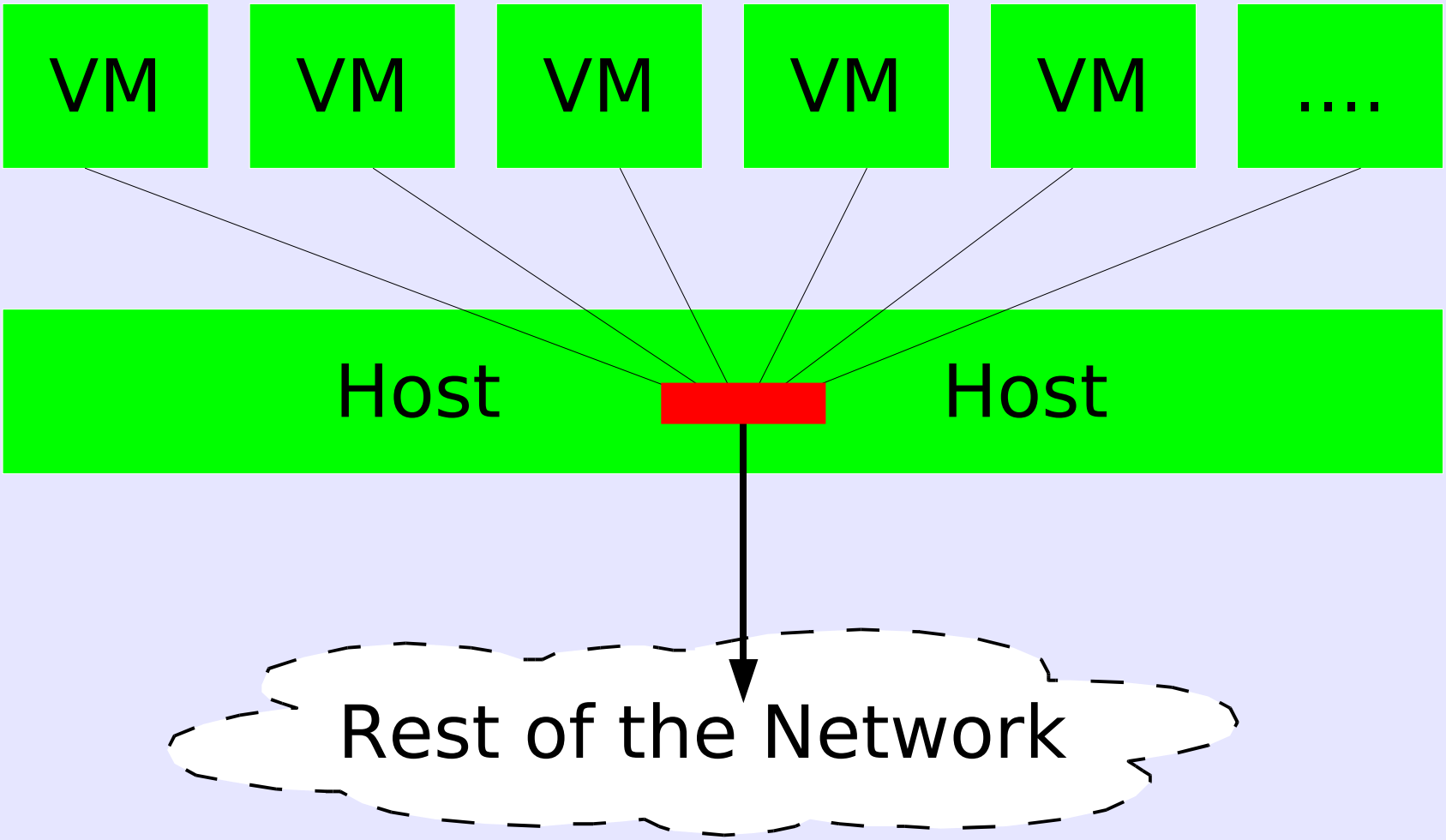
The VMWare Model

(Default)

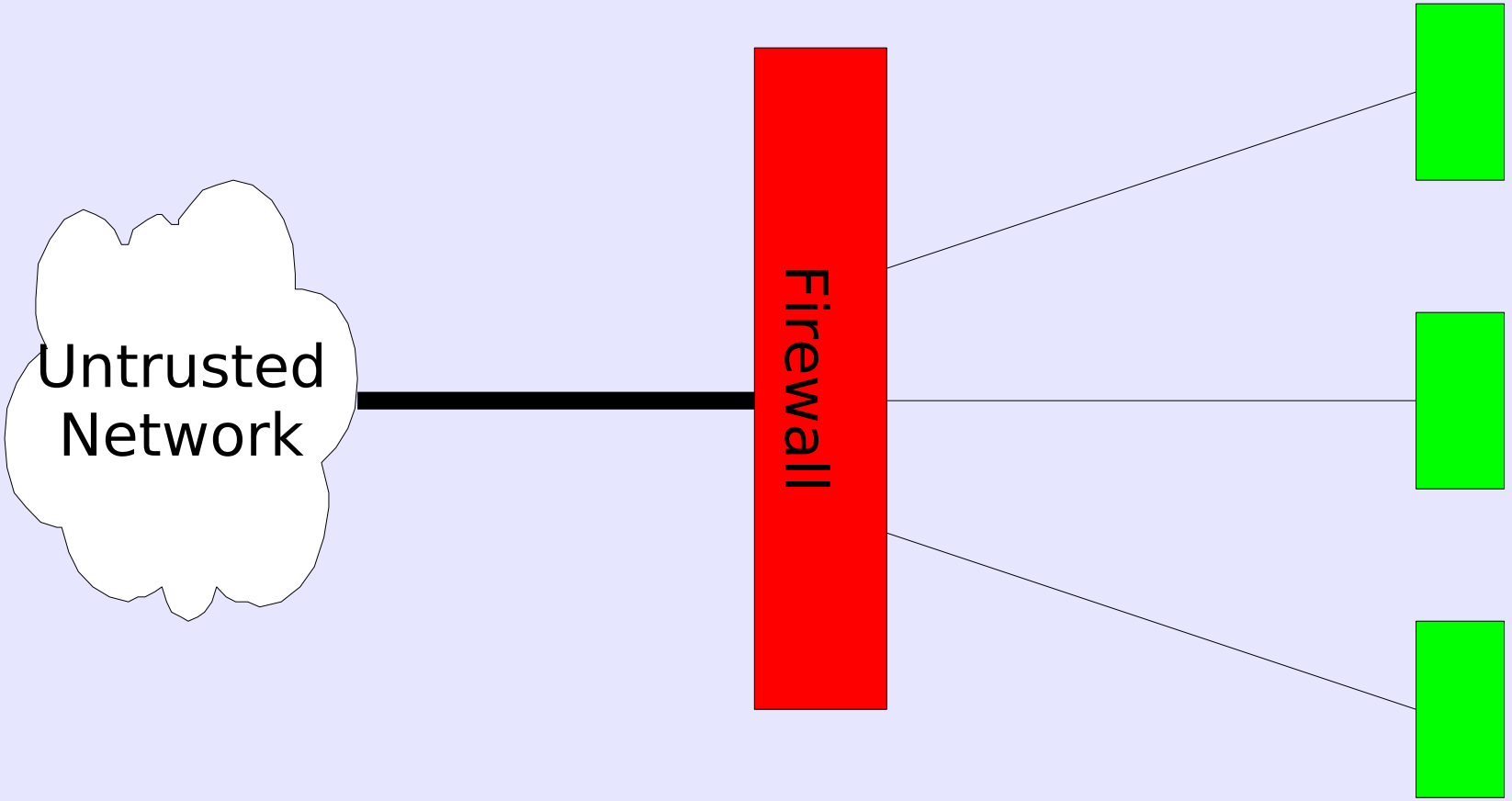


The Xen Model

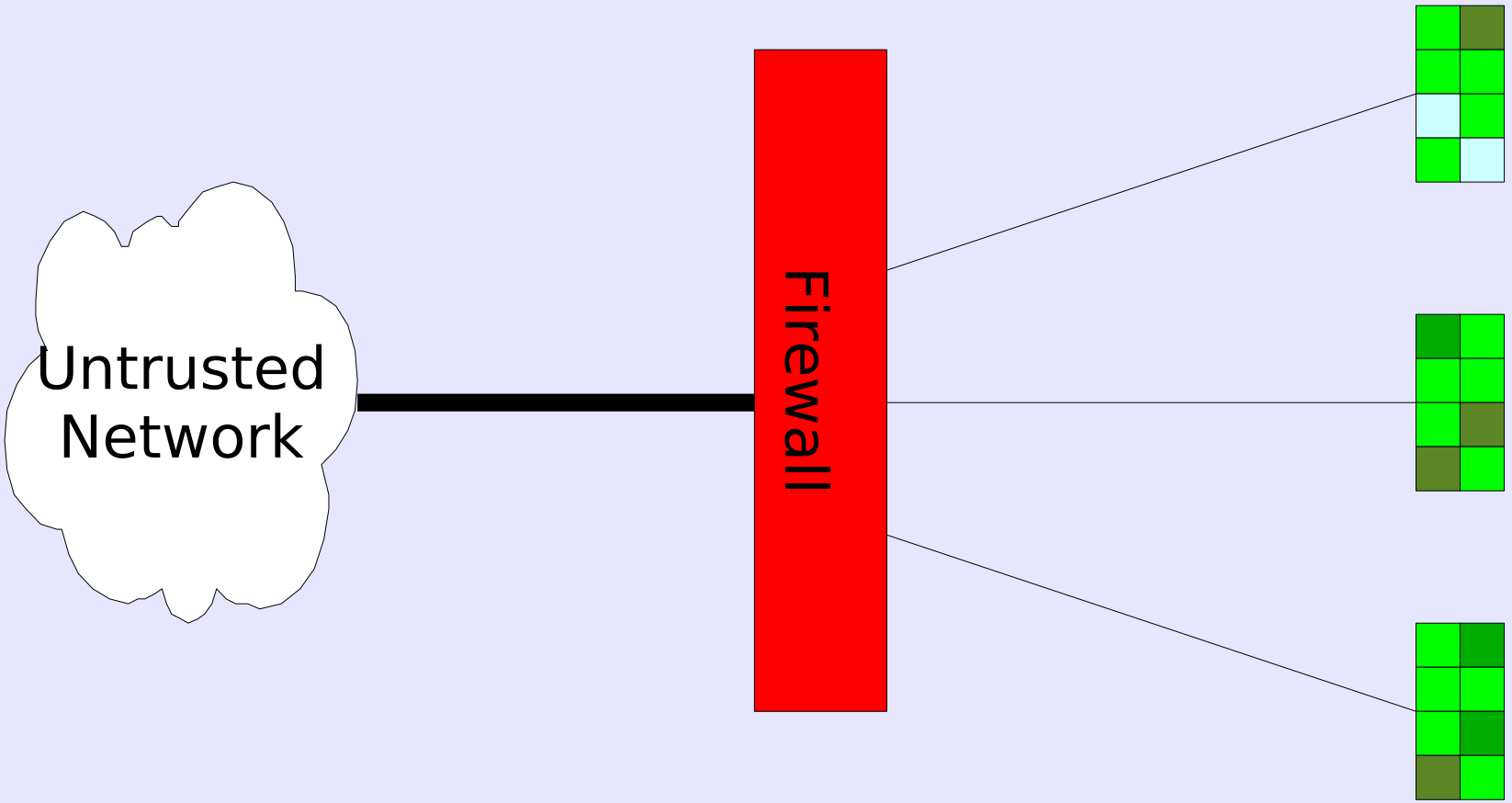
(Default)



The Traditional Firewall



Network Firewall with VMs



Live Migration

The Products

- Xen
- VMWare
- OpenVZ
- IBM's VM stuff

Status

- No encryption
- opt. hw based SSL
- Uses SSH! ...root. :(
- We'll find out end of '07.

Tool

Tool is a rather strong word, but it's available here:

http://sdcc21.ucsd.edu/~dcapelis/vmnet.sh

Puts VMWare's networking and allows you to use a real linux bridging system instead. This gets rid of quite a few of the lamer things VMWare does.

Summary

- VMs are still neat
- The people who make VM software live in a world without attackers
- The world is full of attackers
- Trivial issues rarely become more trivial
- Folks pushing VM technology need to think about the changes deployment brings. Leaving security as an implementation detail is lame.

Questions?
Heckling?
Grandiose Proposals?
Accusations?