Wireshark vs. „The Cloud“: Capturing packets in virtual environments

Jasper Bongertz
Airbus Defence and Space CyberSecurity
Topics

• General virtualization basics
• Virtual Switches (vSwitch/dvSwitch)
• Capture Scenarios
• Best practises

• See also my blog posts at:
  • https://blog.packet-foo.com/category/vm/
Virtual Machines

• Two basic platforms:
  • Desktop virtualization: VirtualBox, VMware Workstation, Parallels Desktop, etc
  • Enterprise virtualization: Hyper-V, VMware vSphere, XEN Server, KDE, etc.

• Here, we’ll look at VMware vSphere as an example
  • All others should behave more or less the same
VMs and virtualization hosts

- Virtualization host runs multiple Virtual Machines on a single NIC
- The host may use the NIC for its own data communication, too
- Potentially dozens of virtual servers showing up with their own virtual MAC address on the physical NIC
Internal communication

• There may also be “internal only“ switches making things complicated
• Data on internal switches never leaves the virtualization host
• No physical pickup possible
NIC teaming

• NIC teaming means that a VM can use more than one physical adapter
  • some virtualization hosts have dozens of NICs
  • virtual machines are balanced over multiple NICs
Clustering virtualization hosts

• Groups of virtualization hosts are usually combined into a cluster
  • provides automatic load balancing and "high" availability features
Capturing virtual servers

• In virtual/cloud environments
  • virtual servers, applications, services may run everywhere
  • multiple virtual servers on physical hosts may share a network card

• If you have access to the virtualization host you can SPAN/TAP its connections

• Challenges:
  • Find and capture the correct NIC
  • Isolate traffic for the virtual server/application
  • Servers with 10GBit or even faster links
  • Blade Centers
Migrating VMs

• Virtual Machines may move from host to host while running
Reasons for VMs changing hosts

• High Availability (sort of)
  • Restart virtual machines on other hosts if there is a host crash

• Real High Availability
  • Running an “invisible” hot standby VM on a secondary host that is kept in sync

• Fully automatic live VM moving
  • Load Balancing virtual machines across virtualization hosts
Capture Strategies
Wireshark on the problem VM

- Install Wireshark on the virtual system of interest

- Advantages:
  - Can capture, even on VMs with internal only NICs
  - Sometimes your only option

- Disadvantage:
  - Changes the environment
  - Gets funny results (way too often)
  - May crash the VM
Capturing the host uplink (1)

- Capture at virtualization host uplink (TAP/SPAN)
- Maybe your only option when you have no better access to the virtual infrastructure

- Advantages:
  - Easy to do in simple setups
  - Usually gets good data
  - Most familiar way to get data since its similar to physical captures
Capturing the host uplink (2)

• Disadvantages:
  • May get you tons and tons of data to sort
  • Server uplink may be too fast for your capture device or the SPAN port
  • VM may be live-moved off the server, interrupting the capture
  • Worst case: you don’t even know where to capture!
Virtual capture setups (1)

- VMware virtual switches come in two flavors:
  - vSwitch (always available)
  - Distributed virtual switch/dvSwitch (E+ license only)
- Virtual switch features helping with captures:
  - "Promiscuous mode" on port groups
  - SPAN sessions (dvSwitch only)
Best Practises
Scenarios

• Problem with a single/a few VMs
  • SPAN the problem VM traffic (if on dvSwitch)
  • isolate problem VM on a port group with a capture VM
  • run dumpcap/tcpdump inside problem VM (only as last resort)

• Intermittent problems concerning multiple VMs
  • e.g. trouble with a Citrix farm running virtualized on a cluster
  • SPAN/Promiscuous mode is usually no option
  • instead, capture physical uplinks
Virtual capture heads-up

• Promiscuous mode on vSwitches puts packets on the NICs of all VMs on the same port group
  • keep security in mind; all VMs see everything (like a hub)
• Storage of packets
  • where? NAS, SAN, local storage?
  • do **NOT** overload the NAS/SAN links with capture I/O
• Keep capture VM and problem VM on the same hosts
  • or you'll not be able to capture the packets you want
Too much data

• Ways to handle „too much data“ (a.k.a „dropped frames“) on physical captures:
  • use frame slicing if possible
  • SPAN only as few affected ports or VLANs as possible
  • use a filtering TAP
  • Capture Filters on the Wireshark itself may help, too
  • Use dumpcap on command line
Thanks. Questions?

Blog: https://blog.packet-foo.com
eMail: jasper@packet-foo.com
Twitter: @packetjay