VIRTUALIZATION-ASSISTED TESTING OF NETWORK SECURITY SYSTEMS FOR NPPS

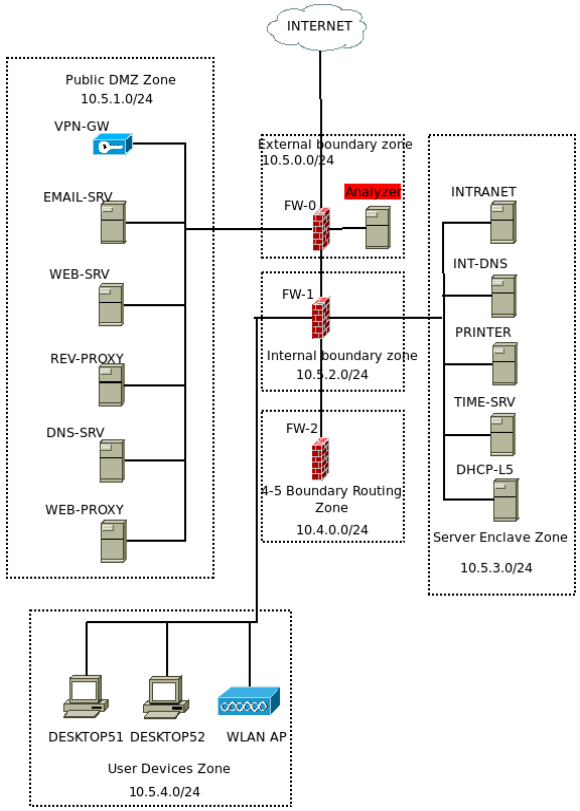
Tamás Holczer[1] Gustavo Berman[2]
Sebastian M. Darricades[2] Péter György[1]
[1]BME, CrySyS Lab, Hungary [2]CNEA, Argentina
holczer@crysys.hu
CRP-J02008

© 2020 CrySyS Lab, BME

Basic idea

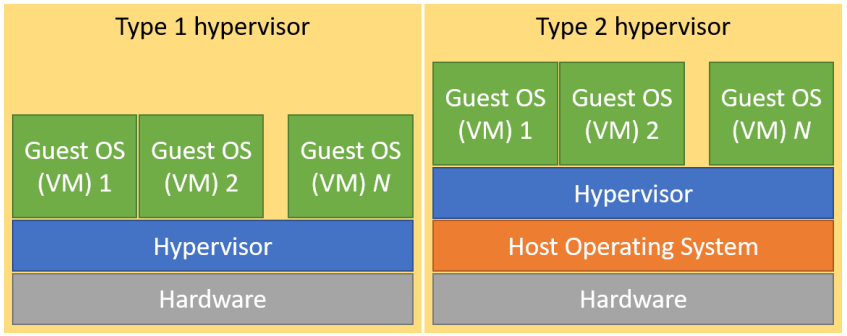
- Devices must be tested before deployment
- Focus on network security devices (e.g. firewalls)
- Complex scenarios
- Reproducible test cases
- Complex networks required to be realistic
- Interaction of many hosts
- Virtual users also needed

- Solution: use virtualization



Virtualization

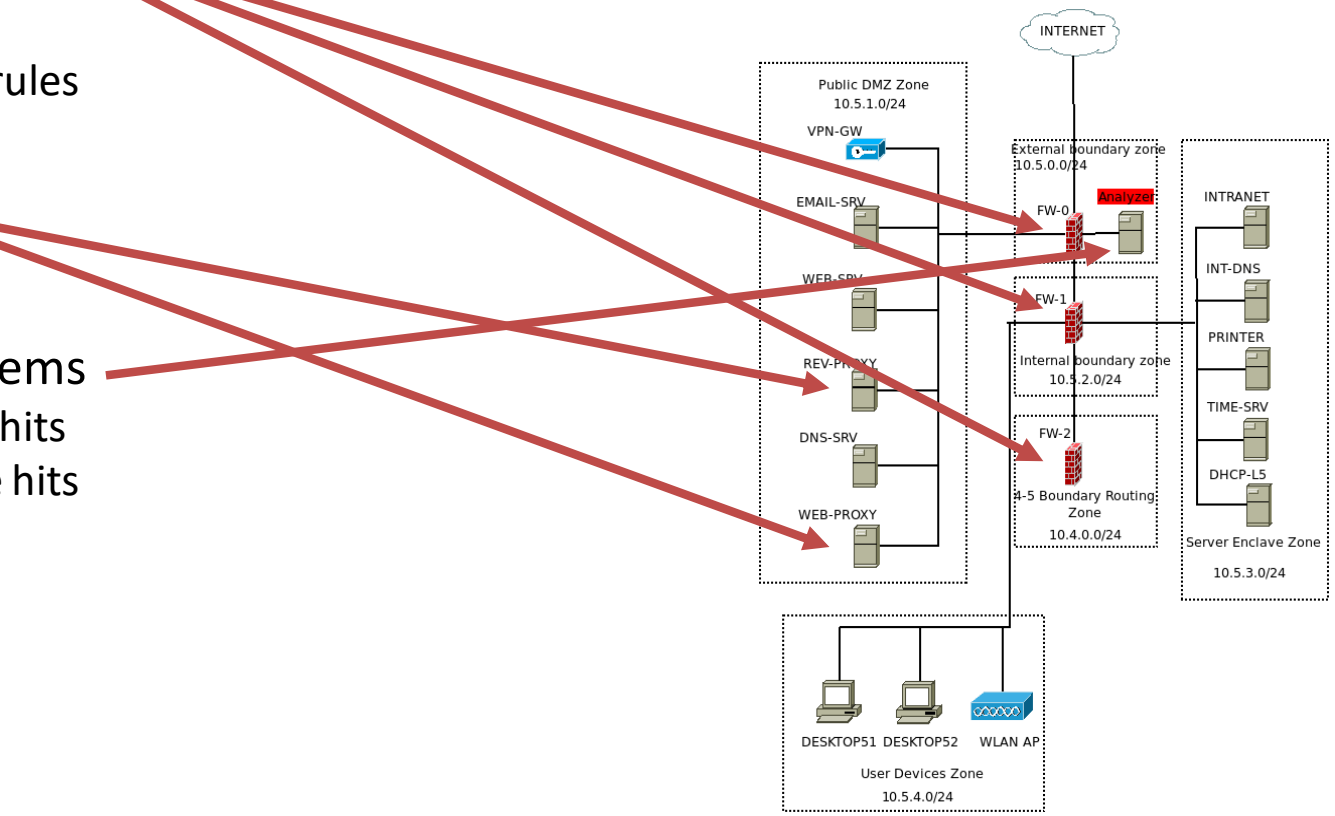
- Use virtual hardware to operate:
  - Computers
  - Networks
  - Storage
  - Etc.



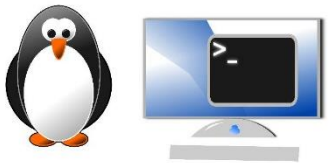
- Advantages of virtualization:
  - Fewer physical hosts
  - Reproducible test cases (snapshots)
- Disadvantages and limitations of virtualization:
  - Performance penalty
  - Another tool must be learnt
  - No straightforward way to virtualize every special devices (e.g. PLCs)

Controls under test

- Zones and segregation
  - Inter zone communication
  - Required flows
- Firewalls
  - Test ruleset
  - Missing rules
  - Unnecessary rules
  - Performance
- Proxy
  - Ruleset
  - Performance
- IDS and IPS systems
  - False positive hits
  - False negative hits
- SIEM
  - Performance
  - Usability
  - Fine tuning



Firewall test



- Free and Open-Source Software

- IPTables / Netfilter:
  - part of Linux kernel
  - IPTables: user space application to manage rules
  - Command line interface

- pfSense:
  - Based on freeBSD
  - Contains web GUI

- Endian Firewall Community:
  - Based on RedHat
  - Contains web GUI
  - Based on iptables

Evaluation

- Based on IEC 63096 Nuclear power plants - Instrumentation, control and electrical power systems - Security controls
- More than 60 tests
- Some of the main categories:
  - Access control
  - Operational security
  - Protection from malware
  - Logging and monitoring
  - Control of operational software
  - Vulnerability management
  - Network security management
  - Cybersecurity and architecture

Example test cases and summary

	IPTables	pfSense	Endian
Unused ports of network interface cards or communication equipment should be either physically locked or disabled.	YES	YES	NO
Teleworking or other remote access to I&C equipment should not be allowed.	YES	YES	YES
Implementing controls that prevent or detect the use of unauthorized software (e.g. application whitelisting);	NO	NO	NO

- The 3 firewalls are quite similar
  - In most cases none or all can implement the control
  - Small differences, e.g.:
    - » IPTables: Easier to lock down, easier code signature verification
    - » pfSense & EFC: automatic file scan for malware

Thank you for your attention