



TZNOG 2014

Systems & Network Security
Welcome

Instructors

Simon Balthazar

TZNIC

- Tanzania

Damas Makweba

TERNET

- Tanzania

Cleven Mmari

NSRC

- USA / Tanzania

Hans Kuhn

NSRC

- USA

Bryton Focus

-Tanzania

Schedule

Original Plan

Session I	09:00 – 10:45
Break	10:45 – 11:15
Session II	11:15 – 13:00
Lunch	13:00 – 14:00
Session III	14:00 – 15:45
Break	15:45 – 16:15
Session IV	16:15 – 18:00+

Potential evening sessions. See Agenda for further details

Agenda:

Monday

- Session 1 Welcome, Introductions,
Workshop Details
Accessing the virtual environment
- Session 2 Security: threats, risks, and attacks
security life cycle
- Session 3 demo: dsniff, metasploit, DNS hijack
buffer overflow, SQL injections
- Session 4 Cryptography applied: using SSH
SSH labs

Tuesday

- Session 1 Cryptography basics
- Session 2 Cryptography labs (incl. SSH keys)
Encryption with GPG and OpenSSL
- Session 3 Authentication & Authorization
- Session 4 Labs (permissions, local vs
centralized auth)
TACACS
- Evening (if time) Discussion: Hardening hosts

Wednesday

- Session 1 Logging and Auditing
- Session 2 Logging & auditing Labs (logging, analysis)
Host Security, Network Security
- Session 3 Labs: ACLs, firewalls
- Session 4 IDS: methods and tools
Labs: snort, netflow, building an NFR
- Evening (if time) Discussion: Physical security & threats

Thursday

- Session 1 Labs continued
- Session 2 Securing network applications: SSL
- Session 3 Labs: SSL web server, TLS
- Session 4 DNS security: recursion, DNSSEC, TSIG
- Evening (if time) Discussion: Mitigating software flaws
(perms, DB model, jail/chroot)

Friday

- Session 1 Netflow
- Session 2 Labs: host analysis: AIDE
- Session 3 Network and vulnerability scanning

Administrative Items

- **Agenda**
 - <http://noc.ws.nsrc.org/>
- **During the course**
 - Please ask questions as you have them.
 - Your experiences are valuable. Please share them.
 - The schedule is somewhat flexible.
- **Course Materials**
 - Available in electronic format during the week:
<http://noc.ws.nsrc.org/>
 - Will be available permanently here:
<http://nsrc.org/workshops/20XX/...>

Virtual machine access

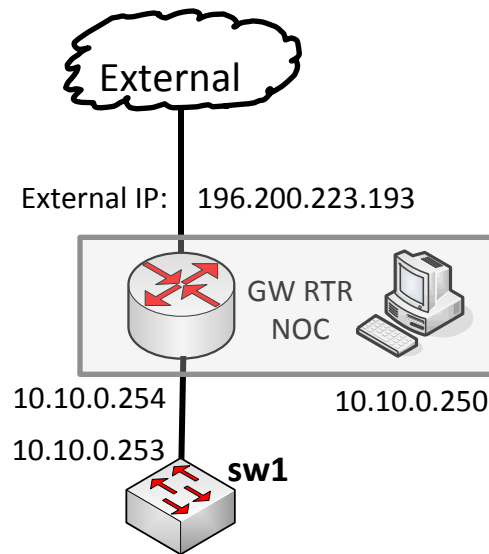
There are two users on your virtual machines

General User
sysadm

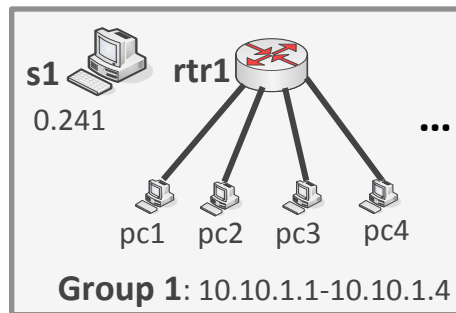
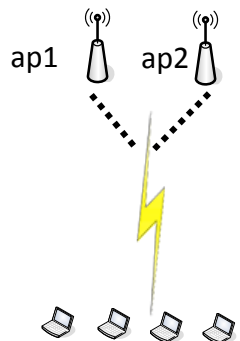
Administrative User
root

Passwords are or will be written down in class

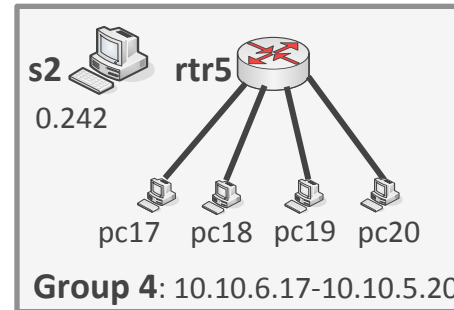
Logical Network Diagram



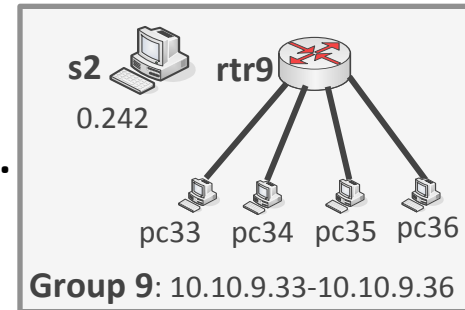
10.10.0.0/24
Classroom backbone



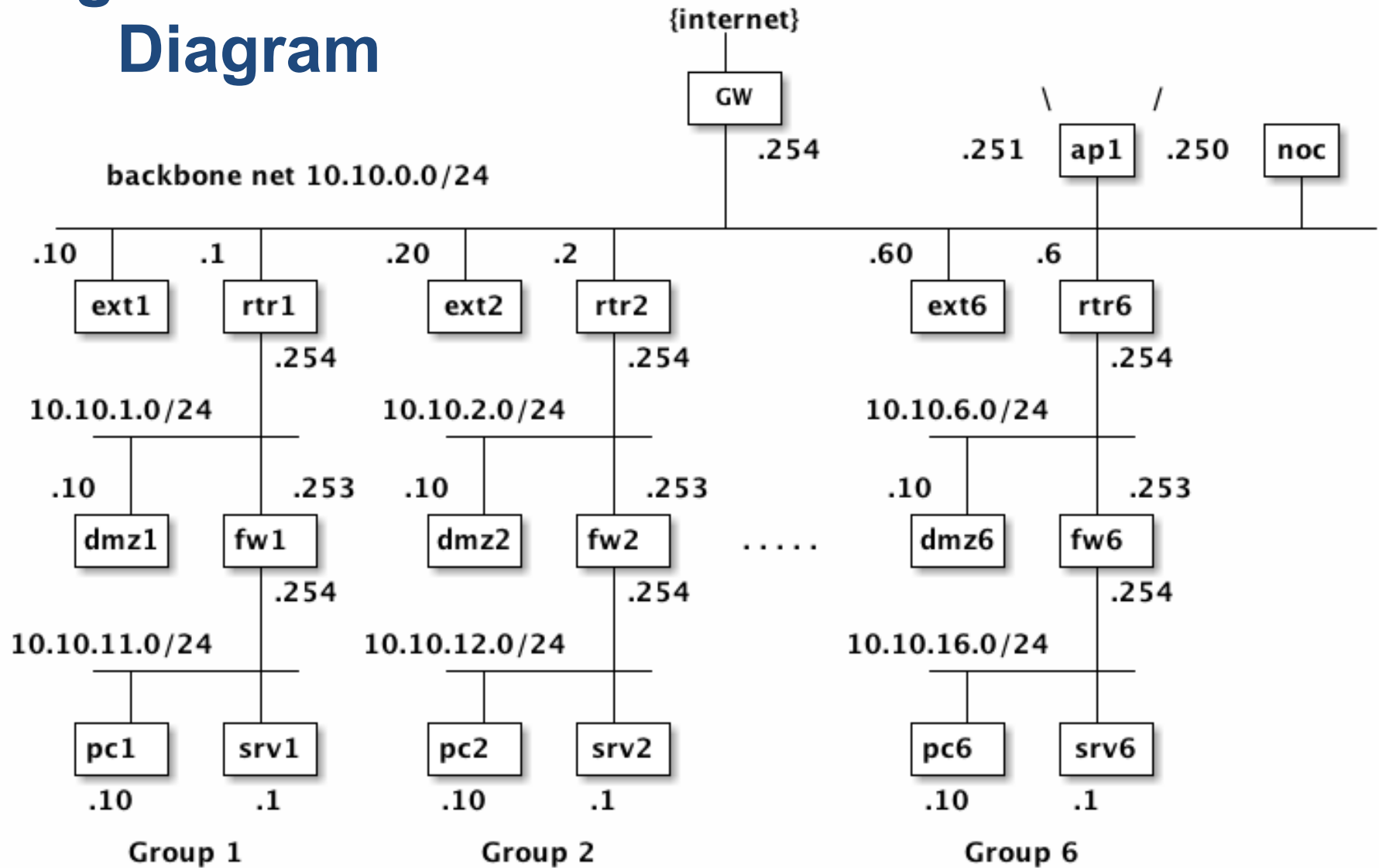
...



...

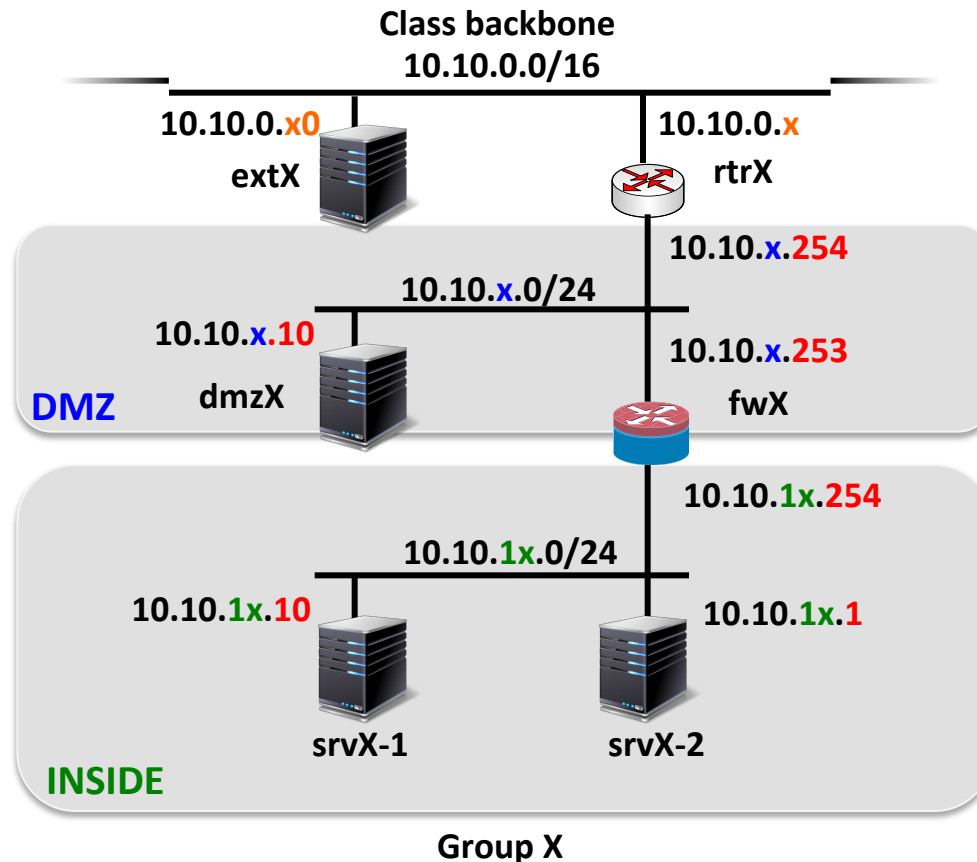


Logical Network Diagram



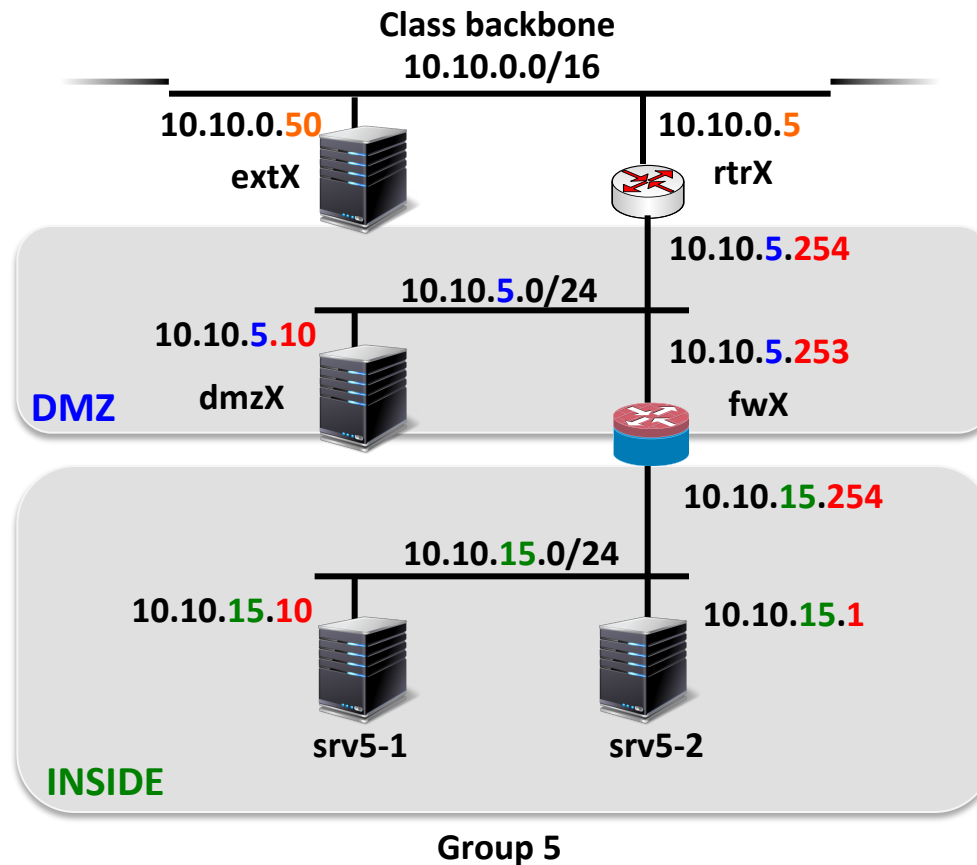
Virtual machine groups

- 6 groups of virtual machines
- Each group is built up as follows:



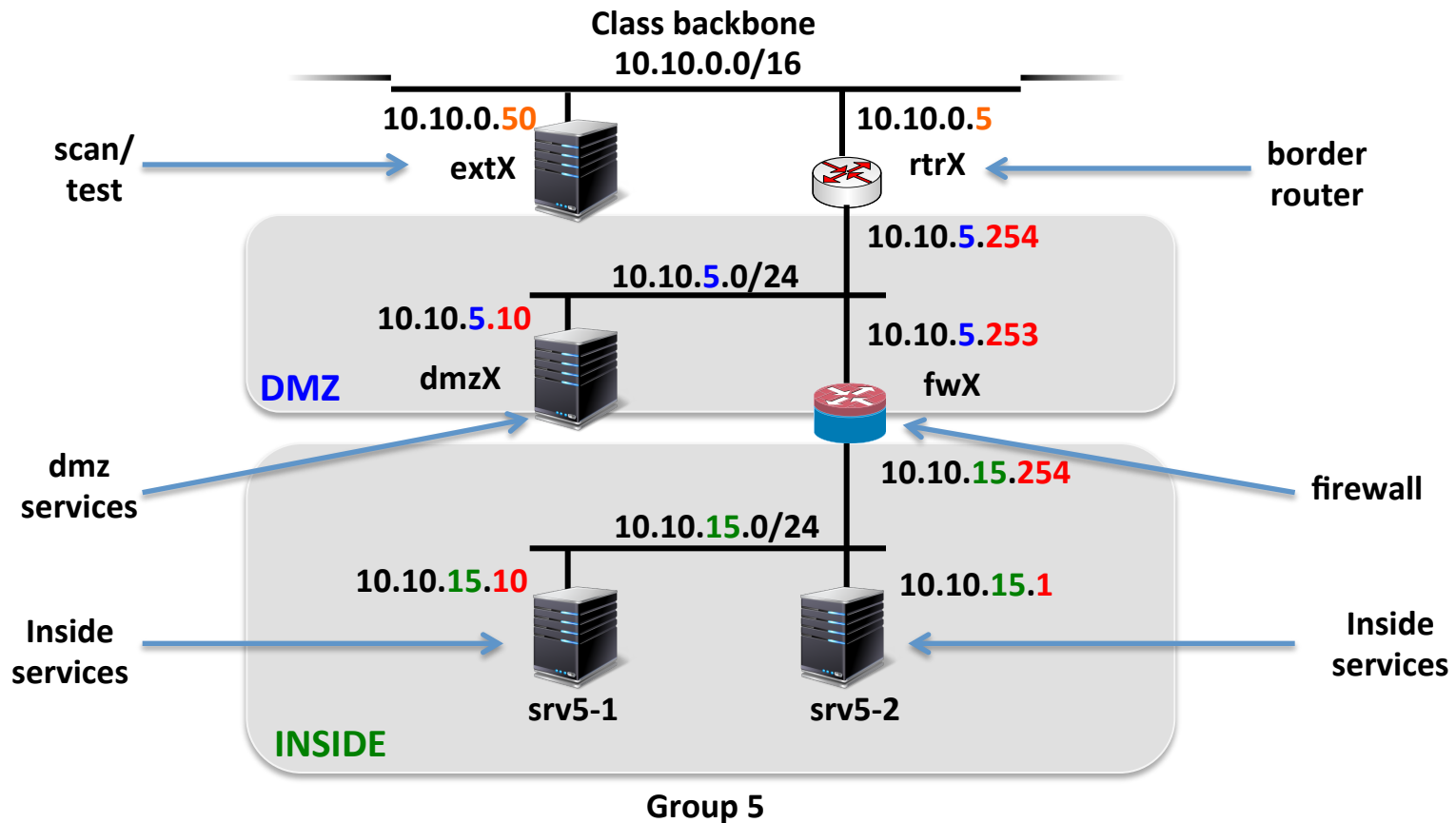
Virtual machine groups

- Example for group 5



Virtual machine groups

- Example for group 5



Assigning your group now

You will work as groups on some exercises. We will assign groups now. Please use the same group/virtual machines during the whole week.

Questions

Do you have any questions?

