Garbage Collection: Using Flow to Understand Private Network Data Leakage

Sid Faber
sfaber@cert.org

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Garbage Collection: Using Flow to Understand Private Network Data Leakage	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

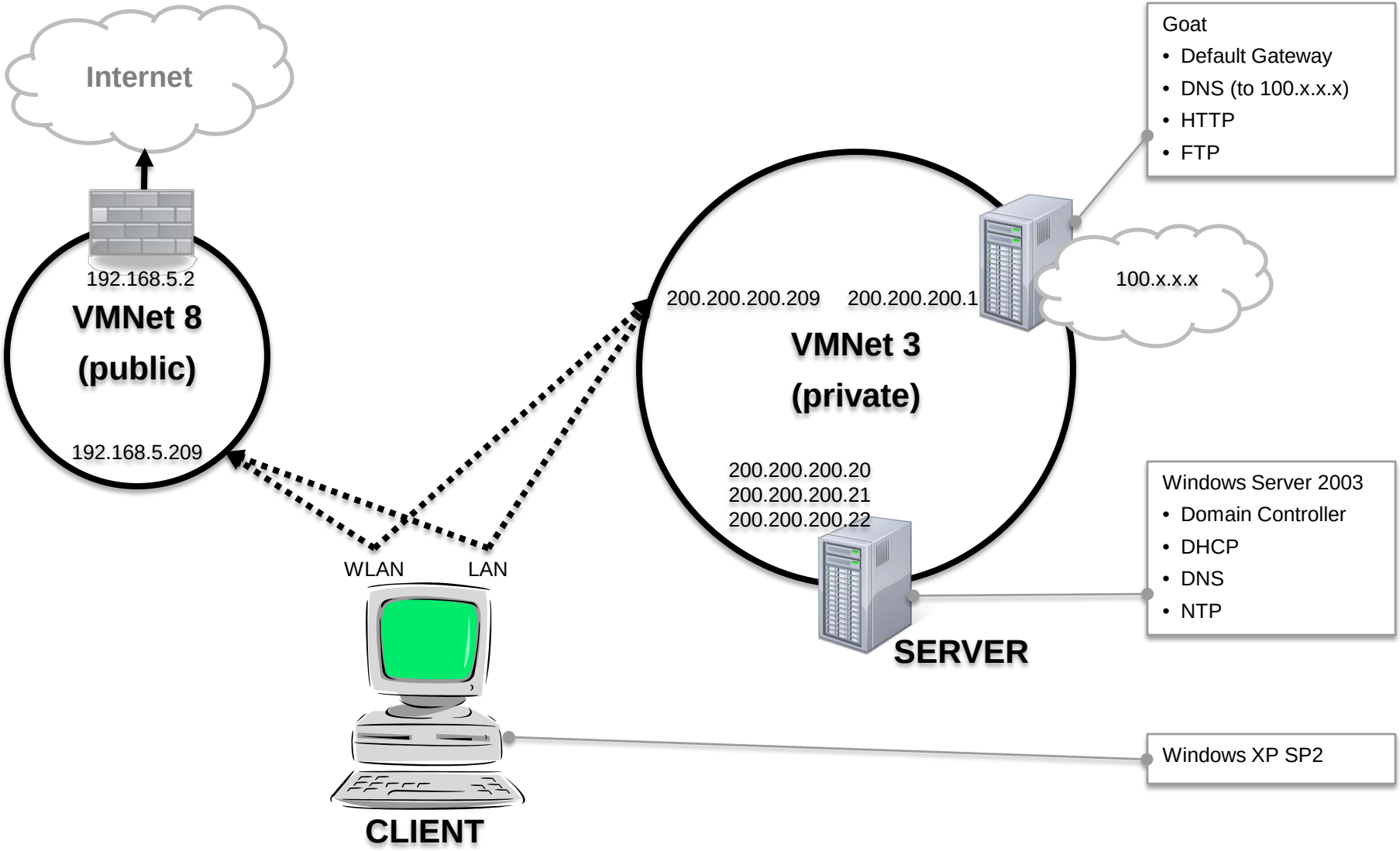
13. SUPPLEMENTARY NOTES
FloCon 2011, in Salt Lake City, Utah, on January 10-13, 2011.

14. ABSTRACT

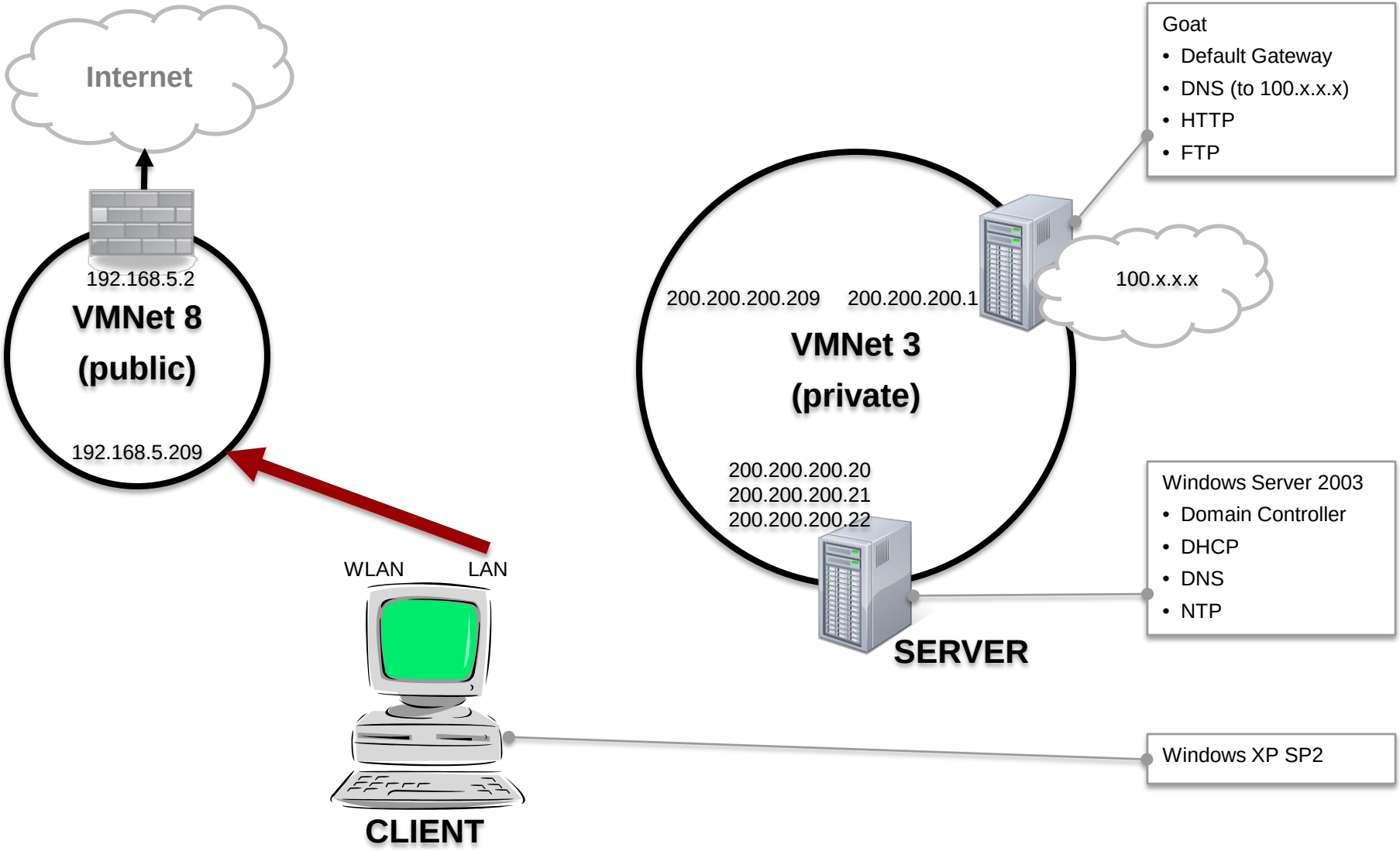
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**14**	

Virtual Layout



Experiment 1: Stand-alone boot



Experiment 1: Procedure

1. Start ethereal on HOST
2. Start ethereal on GOAT
3. Connect LAN on CLIENT to vmnet8
4. Start CLIENT
5. Verify internet connectivity: browse to www.cnn.com and get a legitimate web page
6. Stop packet capture on HOST and save as vmnet3.pcap.
7. Stop packet capture on GOAT and save as vmnet8.pcap.

Results 1: Stand-alone boot

```
|---------|------------------|------------------|------------------|------------------|
|Time     | 0.0.0.0          | 255.255.255.255  | 192.168.5.249    | 192.168.5.207    |
|---------|------------------|------------------|------------------|------------------|
|0.000    |         DHCP Request                |                  |                  |
|         |(68)     ----------------->  (67)    |                  |                  |
|0.000    |                  |                  |         DHCP ACK      - Tra      |
|         |                  |                  |(67)     ----------------->  (68)    |
|---------|------------------|------------------|------------------|------------------|
```

```
|---------|------------------|------------------|------------------|------------------|------------------|
|Time     | 192.168.5.207    | 192.168.5.2      | 192.168.5.255    | 224.0.0.22       | 207.46.232.182   |
|---------|------------------|------------------|------------------|------------------|------------------|
|2.746    |         NBNS     |                  |                  |                  |                  |NBNS: Multi-homed registration NB CLIENT<00>
|         |(137)    ----------------->  (137)    |                  |                  |                  |
|7.296    |         NBNS     |                  |                  |                  |                  |NBNS: Registration NB CLIENT<00>
|         |(137)    ------------------------------------>  (137)    |                  |                  |
|10.312   |         NBNS     |                  |                  |                  |                  |NBNS: Registration NB WORKGROUP<00>
|         |(137)    ----------------->  (137)    |                  |                  |                  |
|14.835   |         NBNS     |                  |                  |                  |                  |NBNS: Registration NB WORKGROUP<00>
|         |(137)    ------------------------------------>  (137)    |                  |                  |
|18.358   |         NBNS     |                  |                  |                  |                  |NBNS: Multi-homed registration NB CLIENT<20>
|         |(137)    ----------------->  (137)    |                  |                  |                  |
|25.888   |         NBNS     |                  |                  |                  |                  |BROWSER: Host Announcement CLIENT, Workstation, Serv
|         |(138)    ------------------------------------>  (138)    |                  |                  |
|26.726   |         DNS      |                  |                  |                  |                  |DNS: Standard query A time.windows.com
|         |(1025)   ----------------->  (53)     |                  |                  |                  |
|27.900   |         IGMP     |                  |                  |                  |                  |IGMP: V3 Membership Report / Join group 239.255.255.
|         |(0)      ------------------------------------------------------------>  (0)      |                  |
|---------|------------------|------------------|------------------|------------------|------------------|
```

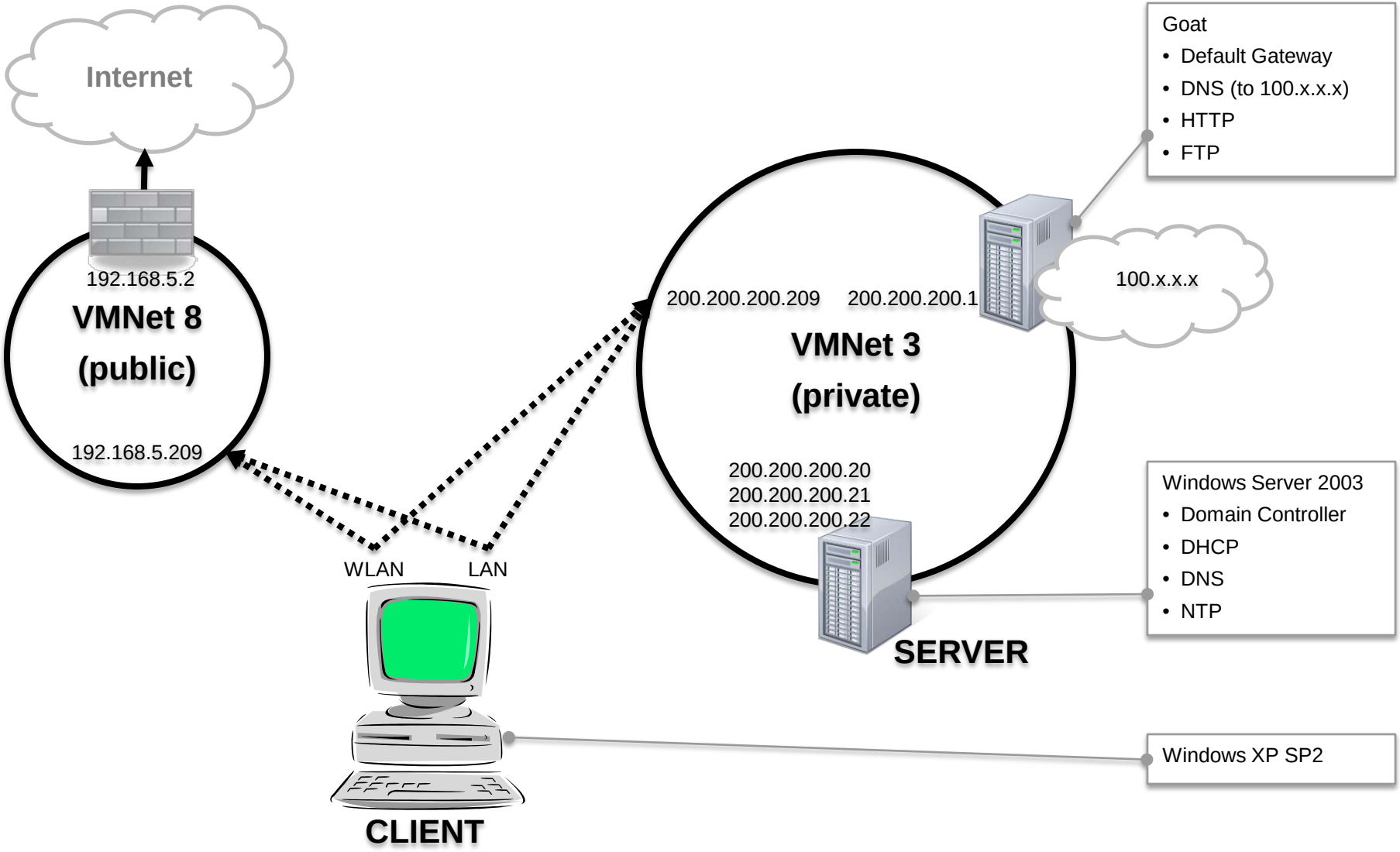
[continued]

Results 1: Stand-alone boot (2)

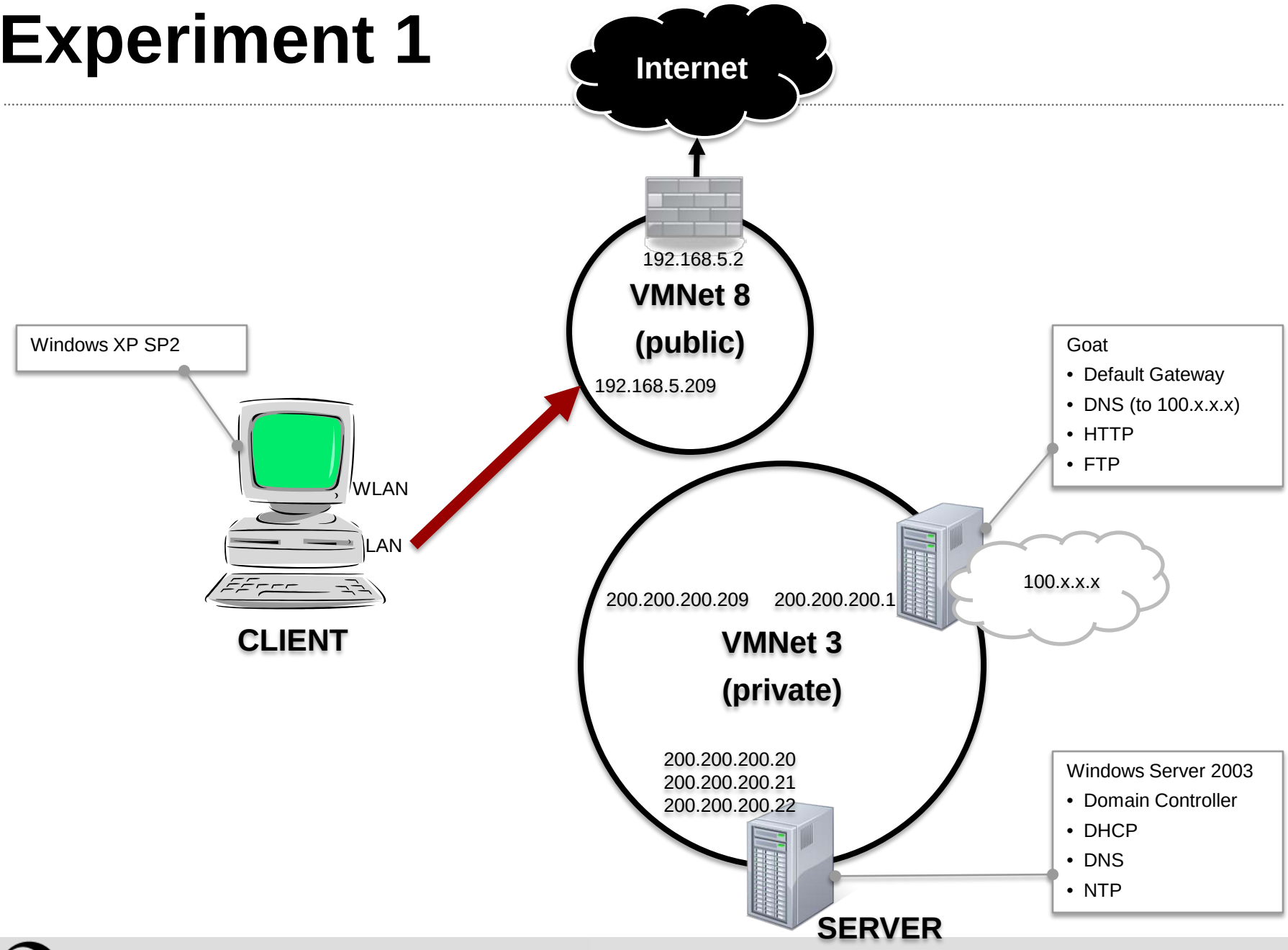
```
|---------|------------------|------------------|------------------|
|Time     | 192.168.5.207    | 192.168.5.2      | 207.46.232.182   |
|---------|------------------|------------------|------------------|
|28.807   |         DNS      |                  |                  |DNS: Standard query A time.windows.com
|         |(1025)   ------------------>  (53)    |                  |
|30.749   |         DNS      |                  |                  |DNS: Standard query response CNAME time.microsoft.akadns.net A 207.46.232.182
|         |(1025)   <------------------  (53)    |                  |
|30.822   |         NTP      |                  |                  |NTP: NTP symmetric active
|         |(123)    ------------------------------------->  (123)   |
|---------|------------------|------------------|------------------|
```

```
|---------|------------------|------------------|------------------|
|Time     | 192.168.5.207    | 192.168.5.2      | 157.166.226.25   |
|---------|------------------|------------------|------------------|
|72.489   |         Standard query A ww         |                  |DNS: Standard query A www.cnn.com
|         |(1025)   ------------------>  (53)    |                  |
|73.490   |         Standard query A ww         |                  |DNS: Standard query A www.cnn.com
|         |(1025)   ------------------>  (53)    |                  |
|74.491   |         Standard query A ww         |                  |DNS: Standard query A www.cnn.com
|         |(1025)   ------------------>  (53)    |                  |
|76.492   |         Standard query A ww         |                  |DNS: Standard query A www.cnn.com
|         |(1025)   ------------------>  (53)    |                  |
|76.604   |         Standard query resp         |                  |DNS: Standard query response A 157.166.226.25 A 157.166.226.26 A 157.166.255.18 A 157.166.25
|         |(1025)   <------------------  (53)    |                  |
|76.625   |         iad3 > http [SYN] S         |                  |TCP: iad3 > http [SYN] Seq=0 Win=64240 Len=0 MSS=1460
|         |(1032)   ------------------------------------->  (80)    |
|76.670   |         http > iad3 [SYN, A         |                  |TCP: http > iad3 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
|         |(1032)   <-------------------------------------  (80)    |
|76.682   |         iad3 > http [ACK] S         |                  |TCP: iad3 > http [ACK] Seq=1 Ack=1 Win=64240 Len=0
|         |(1032)   ------------------------------------->  (80)    |
|76.722   |         GET / HTTP/1.1              |                  |HTTP: GET / HTTP/1.1
|         |(1032)   ------------------------------------->  (80)    |
|76.722   |         http > iad3 [ACK] S         |                  |TCP: http > iad3 [ACK] Seq=1 Ack=455 Win=64240 Len=0
|         |(1032)   <-------------------------------------  (80)    |
|---------|------------------|------------------|------------------|
```

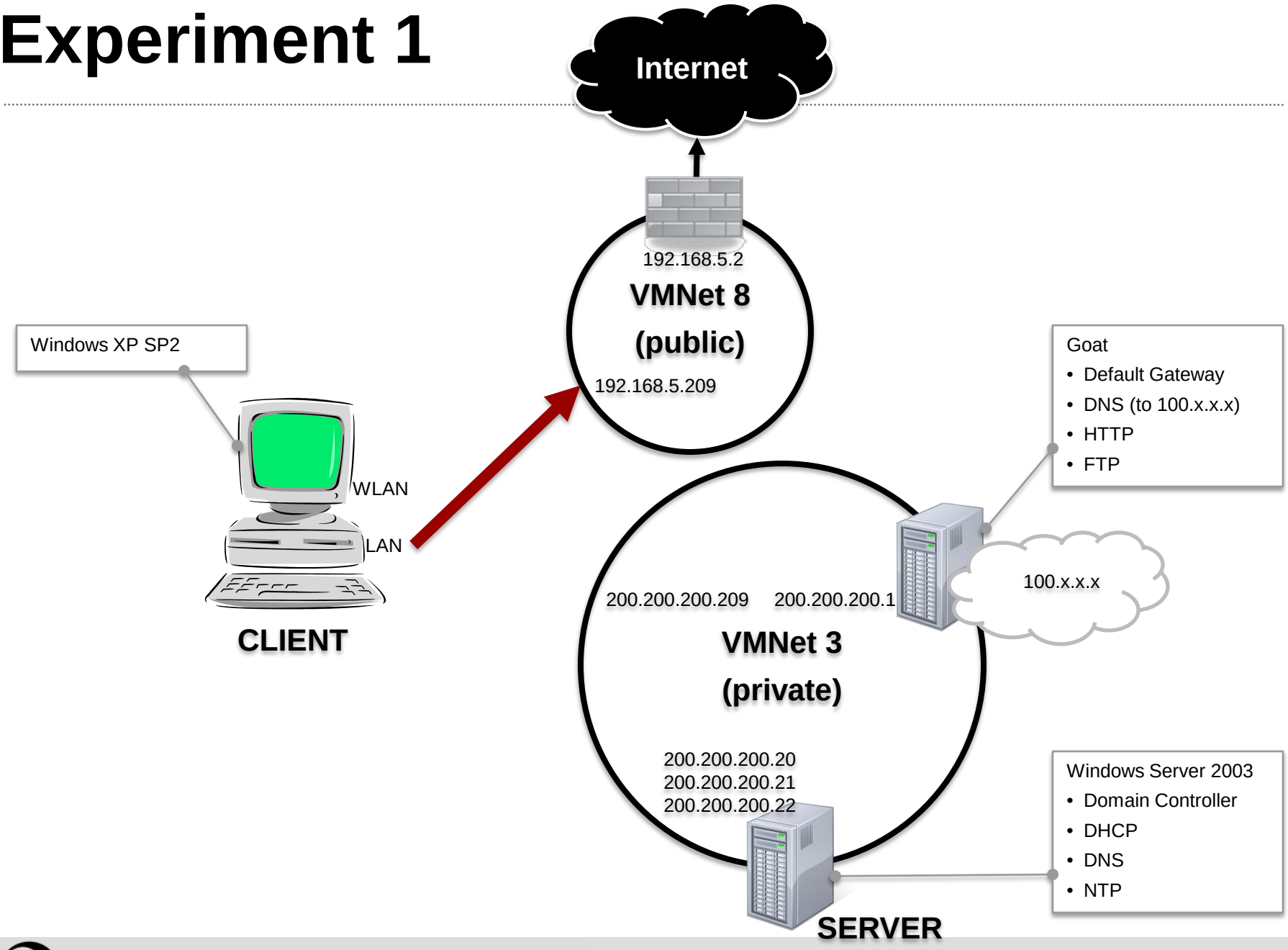
Scenario 2: Standalone boot on private



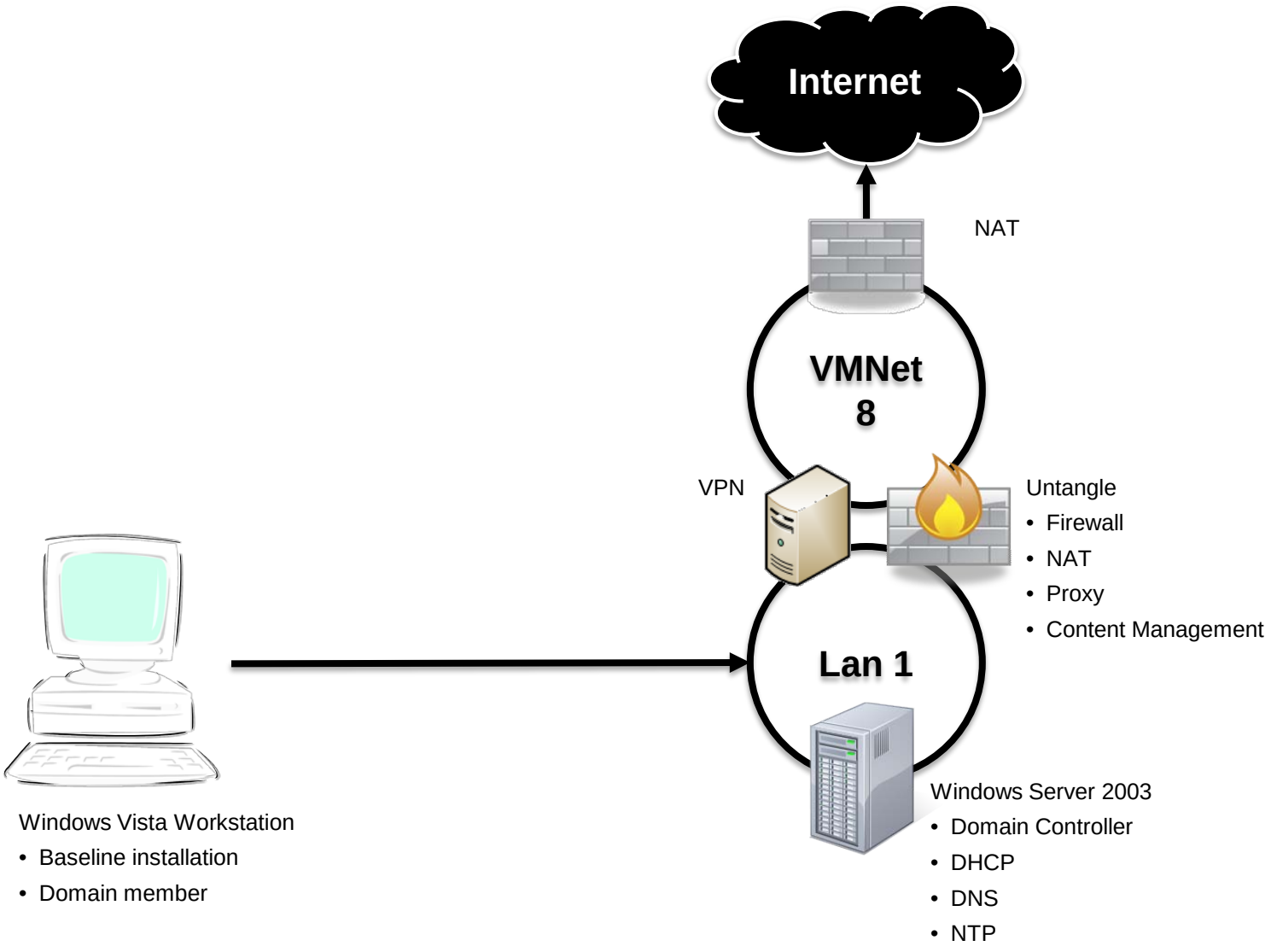
Experiment 1



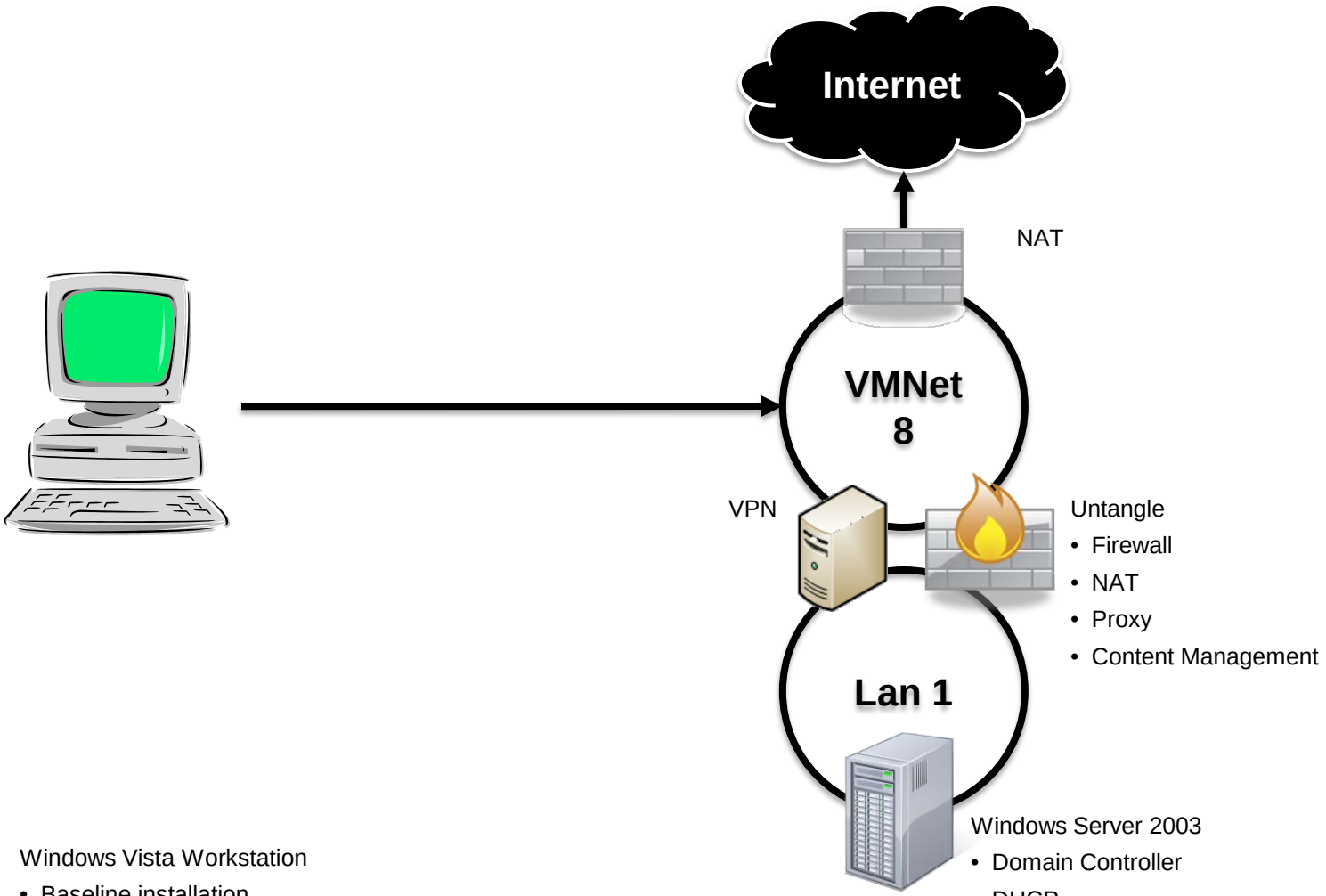
Experiment 1



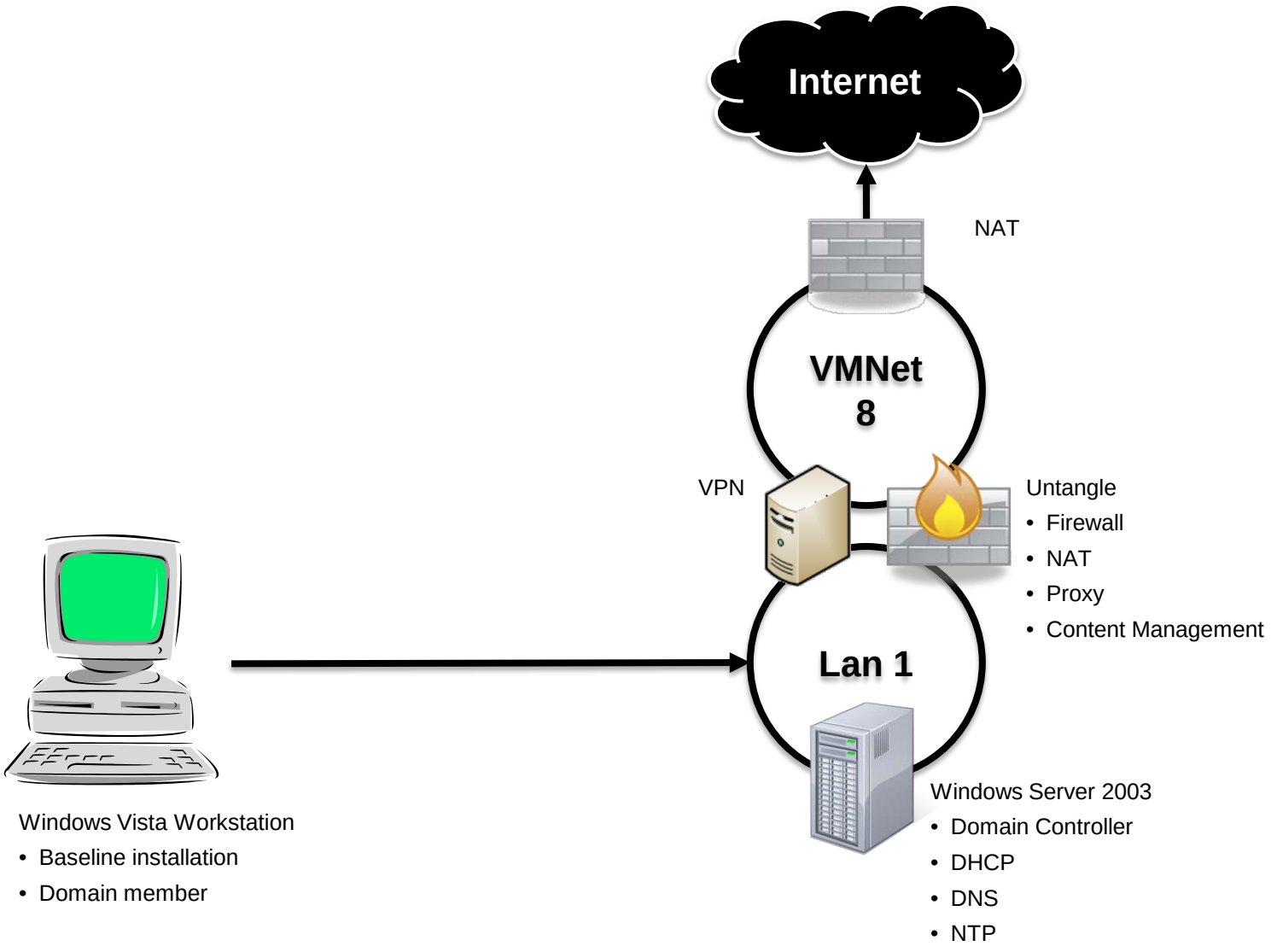
Scenario 1: Restart on Another Network



Scenario 1: Restart on Another Network



Scenario 2: Move to Another Network



Scenario 2: Move to Another Network