Digital Security
Research Group

DNS for EVIL

Alexey Sintsov

ConfidencE 2011

Digital Security
Research Group

I am…

Playing with SAP

ERPScan
Security Scanner for SAP NetWeaver

Do research

Digital Security
Research Group

Write articles

BUT my JOB is PENETRATION TESTER

Common work

Task: Test employees awareness of IT policies and common security risks

Tools: Metasploit/SET

Action: Spam e-mail messages with attached PDF or link

Idea: Tempt employers to open a malicious email attachment or visit malicious web-site

Common work

Task: Test employees awareness of IT policies
and common security risks

Tools: Metasploit/SET

Action: Spam e-mail messages with attached PDF or link

Idea: Tempt employers to open a malicious email attachment
or visit malicious web-site

vs.

Antivirus - block known exploits with PDF
Firewall - block traffic to attacker
Awareness - make employer smarter)

Common work

Task: Test employees awareness of IT policies
and common security risks

Tools: Metasploit/SET

Action: Spam e-mail messages with attached PDF or link

Idea: Tempt employers to open a malicious email attachment
or visit malicious web-site

VS.

Antivirus - block
Firewall - block traffic to attacker
Awareness - make employer smarter)

Common work

Task: Test employees awareness of IT policies
and common security risks

Tools: Metasploit/SET

Action: Spam e-mail messages with attached PDF or link

Idea: Tempt employers to open a malicious email attachment
or visit malicious web-site

VS.

Antivirus - block kn… s wi…
Firewall - block traffic to attacker
Awareness - ma… …orter)

Obfuscation

0day

Social Engineering

Common work

Task: Test employees awareness of IT policies
and common security risks

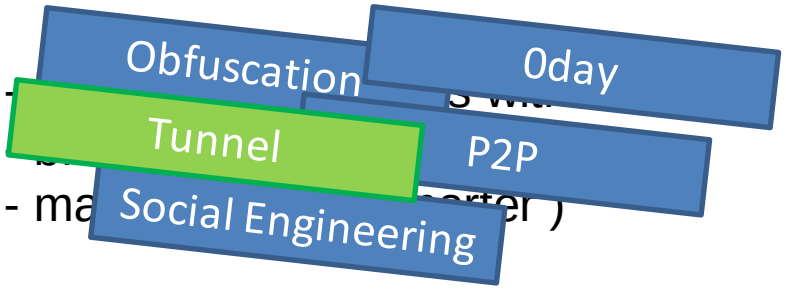
Tools: Metasploit/SET

Action: Spam e-mail messages with attached PDF or link

Idea: Tempt employers to open a malicious email attachment
or visit malicious web-site

VS.

Antivirus
Firewall
Awareness



Tunnel

ICMP	HTTP	DNS
ICMP traffic must be allowed	Web proxy with black-list or without *OR* HTTP traffic must be allowed	DNS service must forward client's requests

Tunnel

Do not forget about mail, ftp, ntp …

ICMP	HTTP	DNS
ICMP traffic must be allowed	Web proxy with black-list or without *OR* HTTP traffic must be allowed	DNS service must forward client's requests

Tunnel

ICMP	HTTP	DNS
ICMP traffic must be allo	Web proxy with	DNS service must fo
Rarely	Often / Sometimes	Always / Often
	HTTP traffic must be allowed	

Tunnel

ICMP

ICMP traffic must be allo

Rarely

HTTP

Web proxy with

Often / Sometimes

HTTP traffic must be allowed

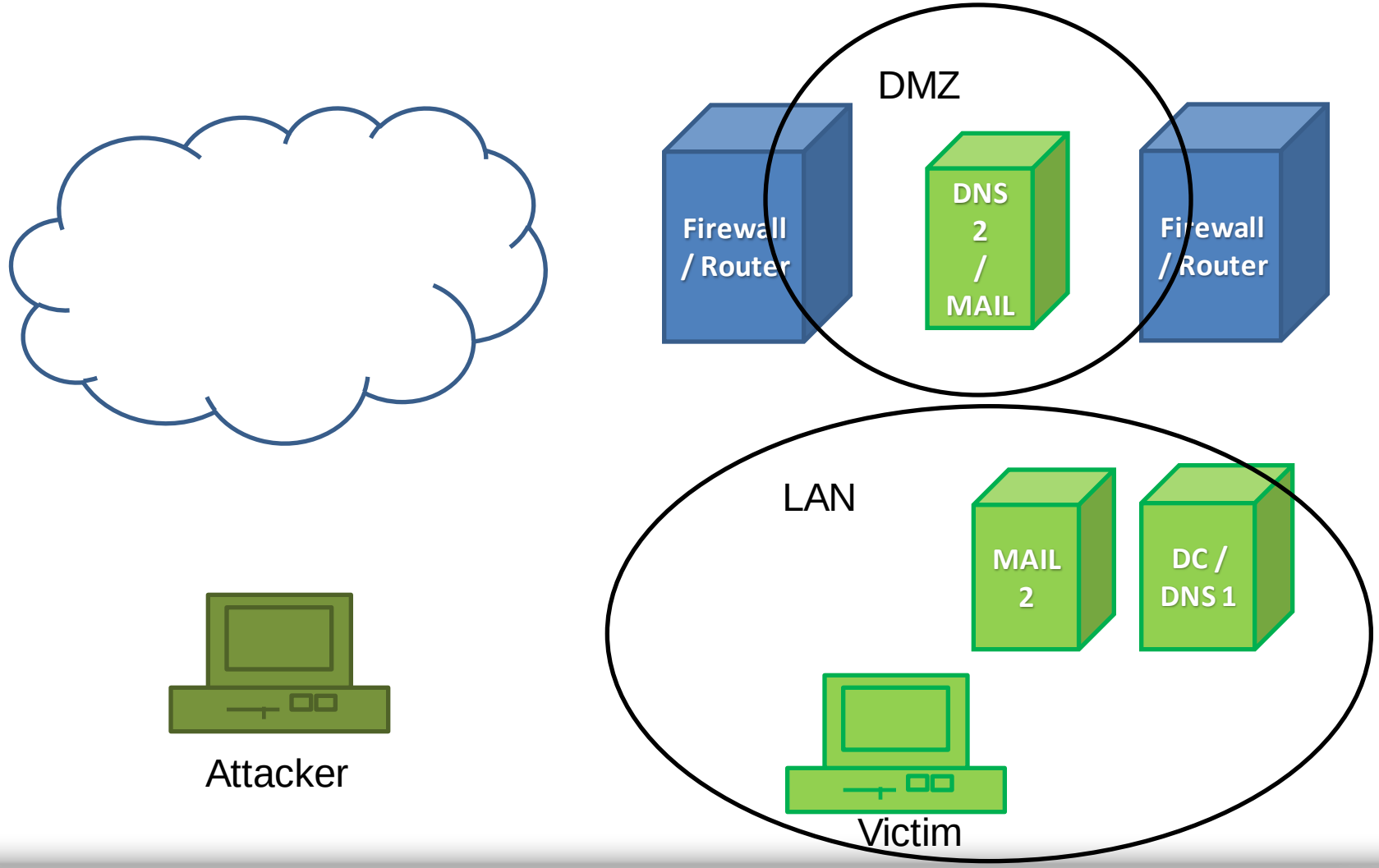
DNS

DNS service must fo

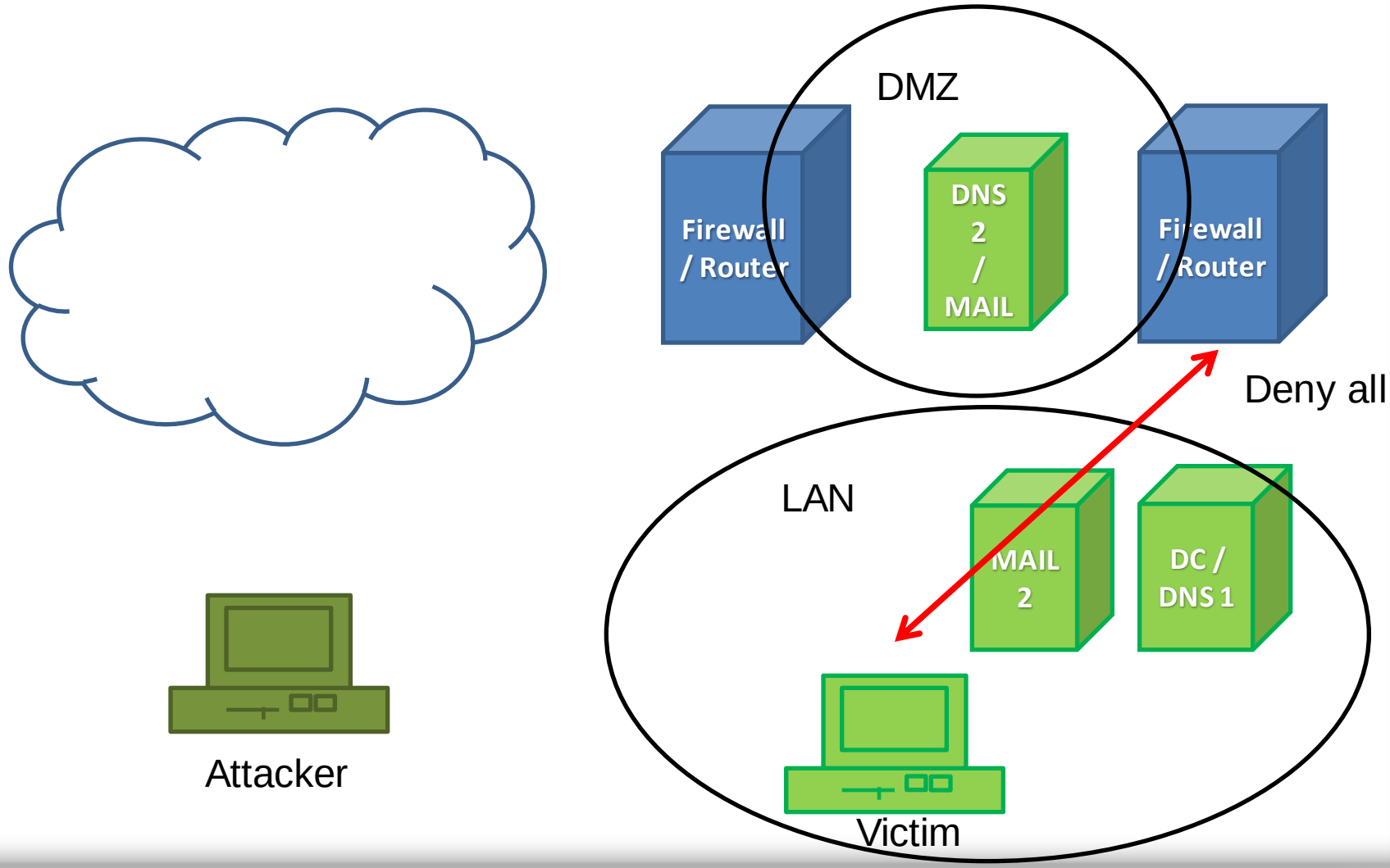
Always / Often

Most realistic scenario

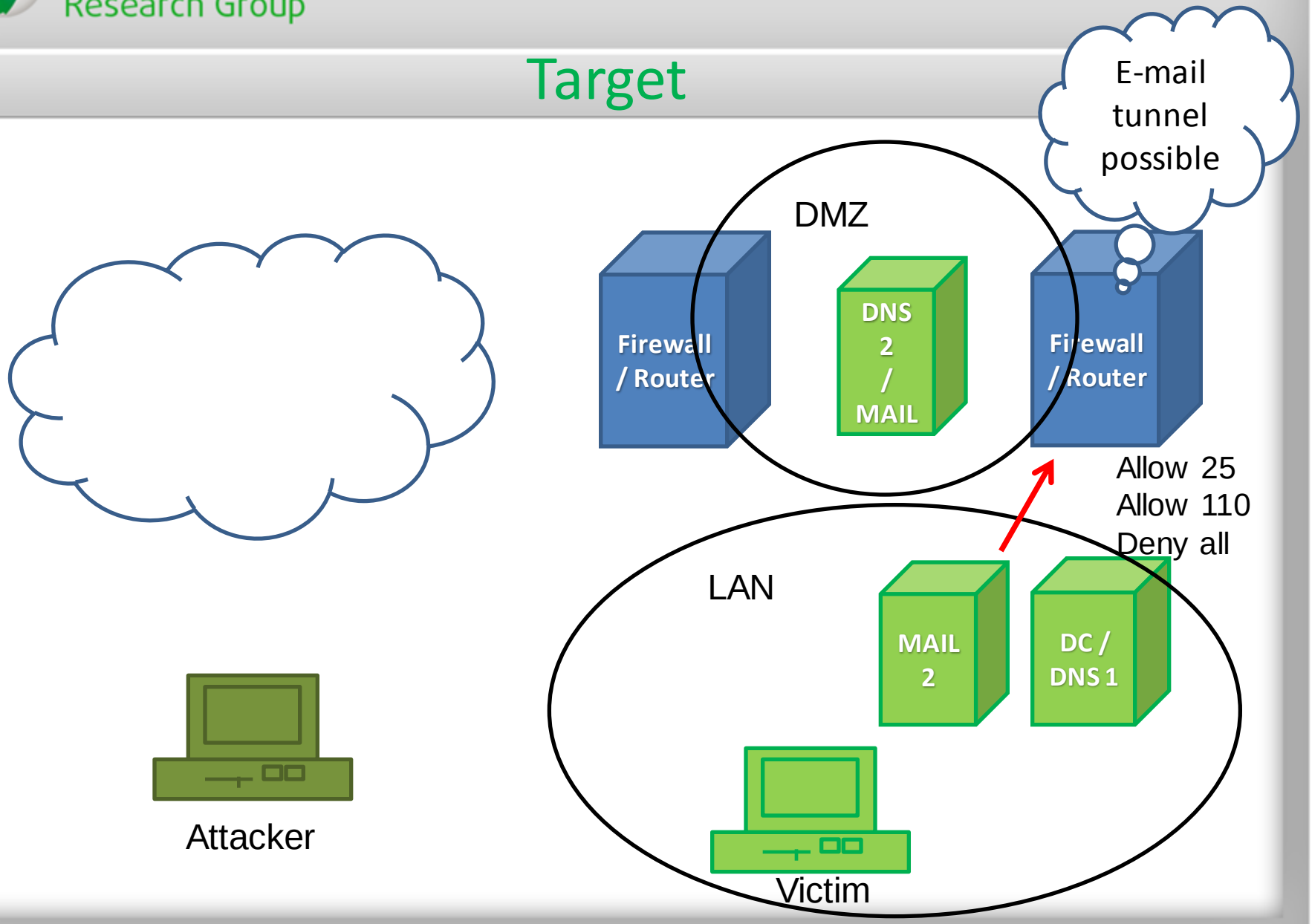
Target



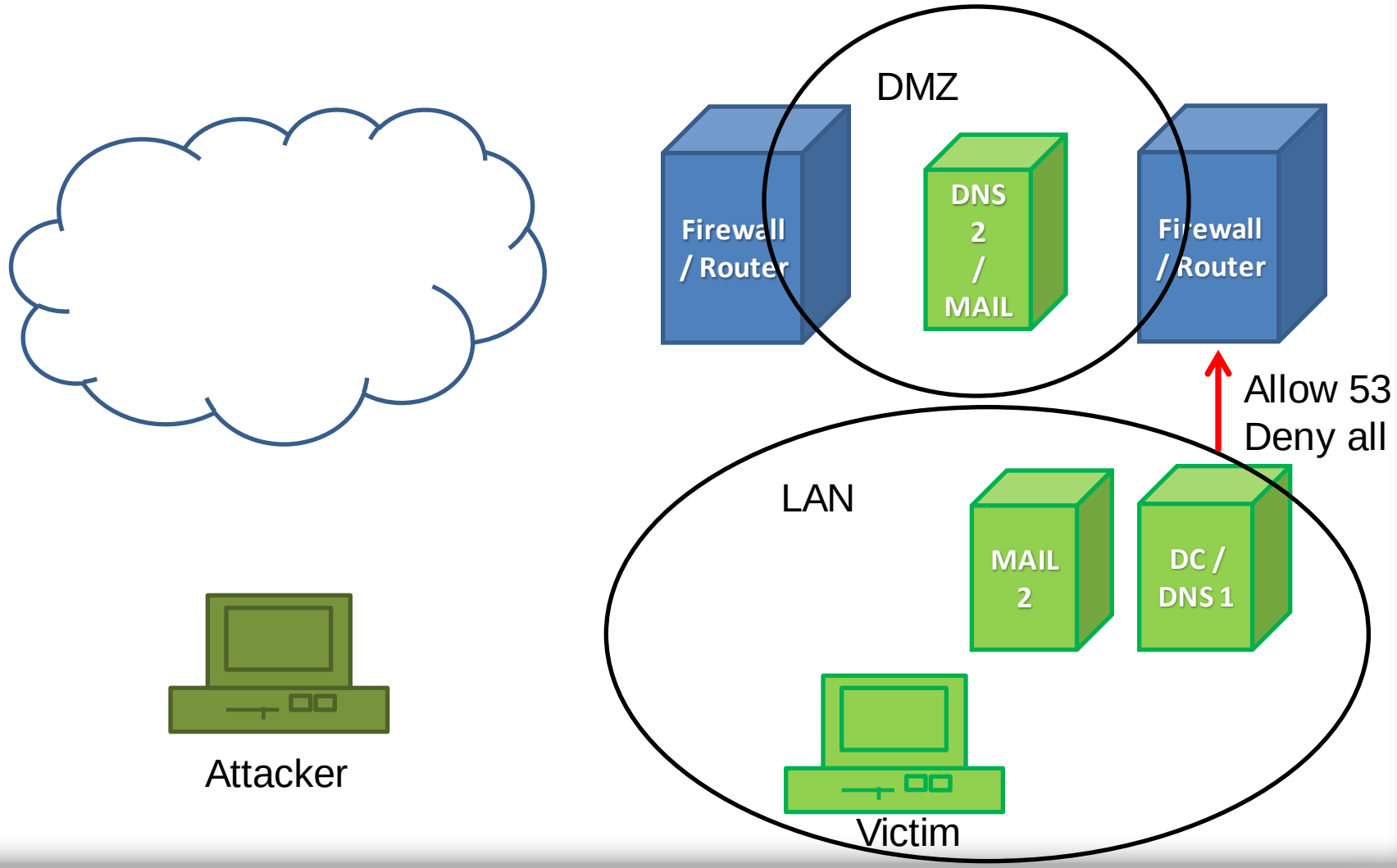
Target



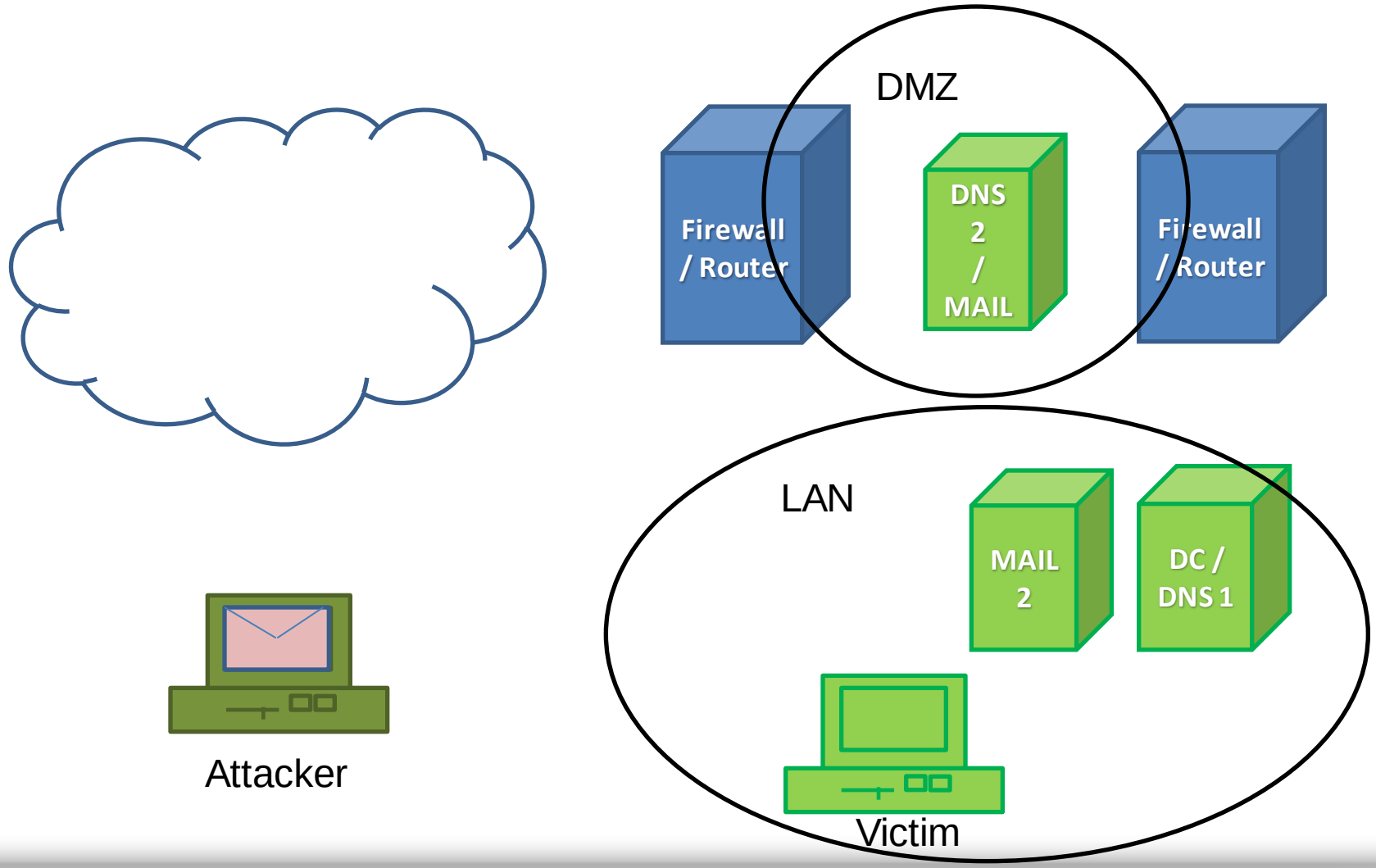
Target



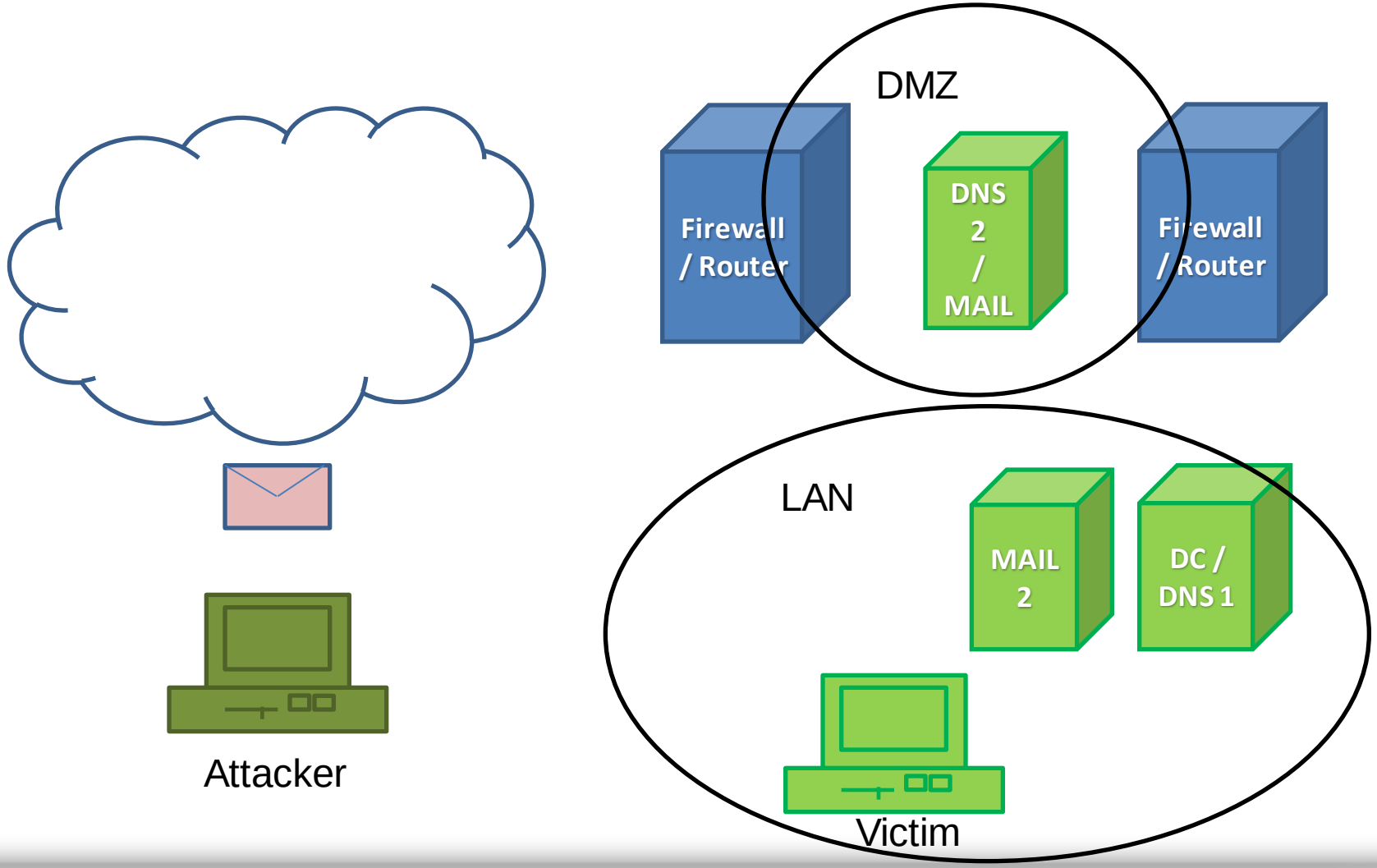
Target



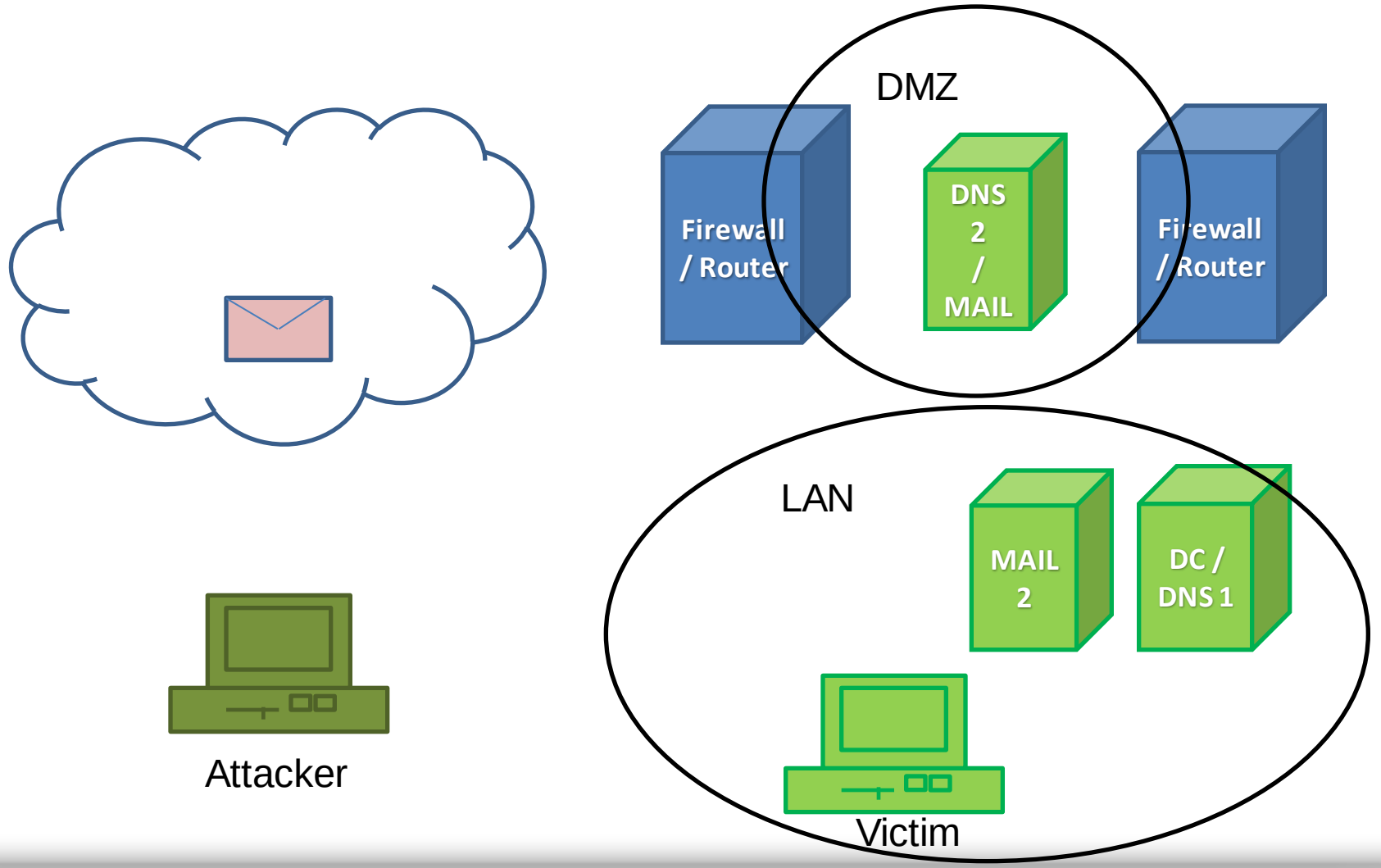
Step one – send mail



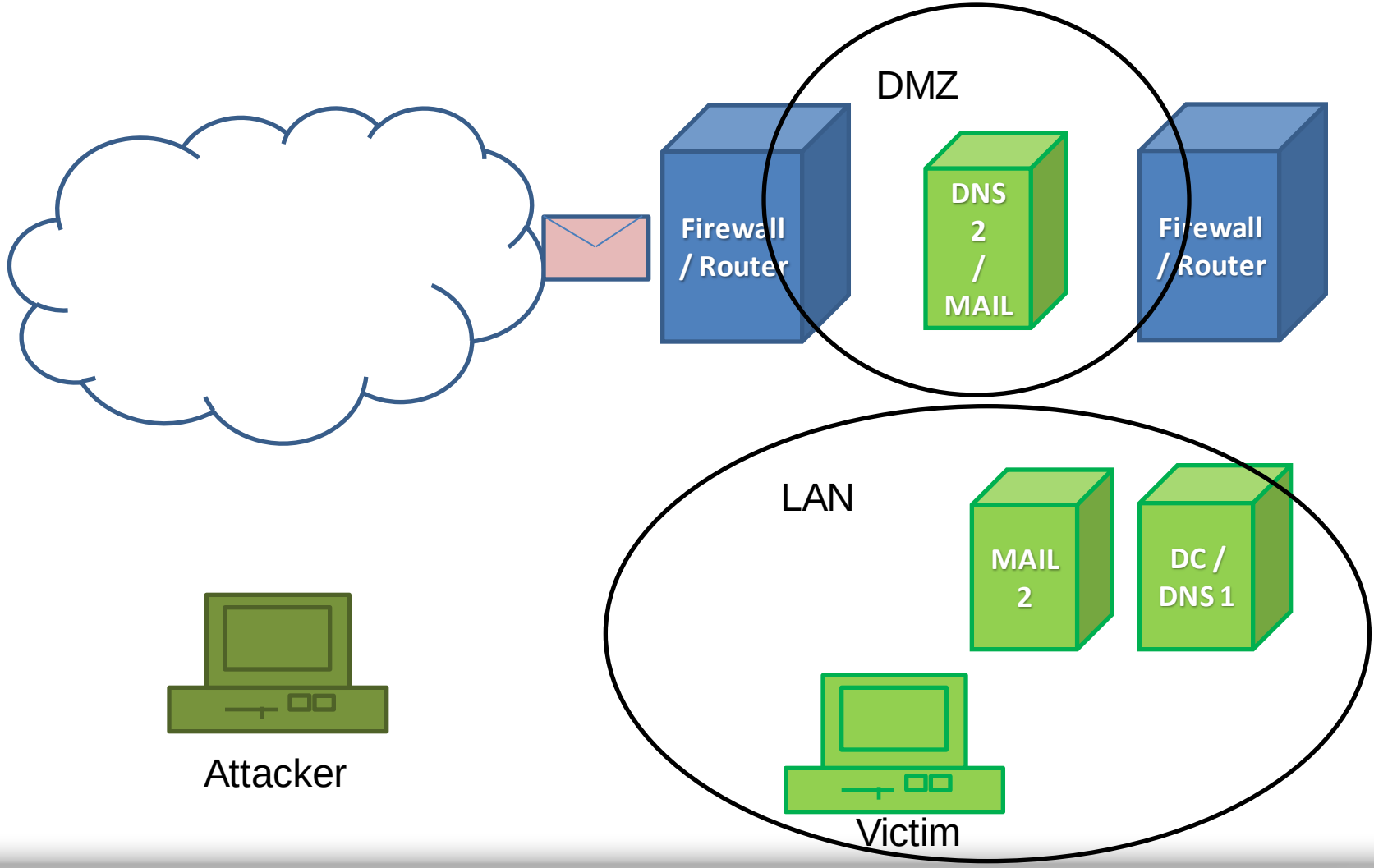
Step one – send mail.



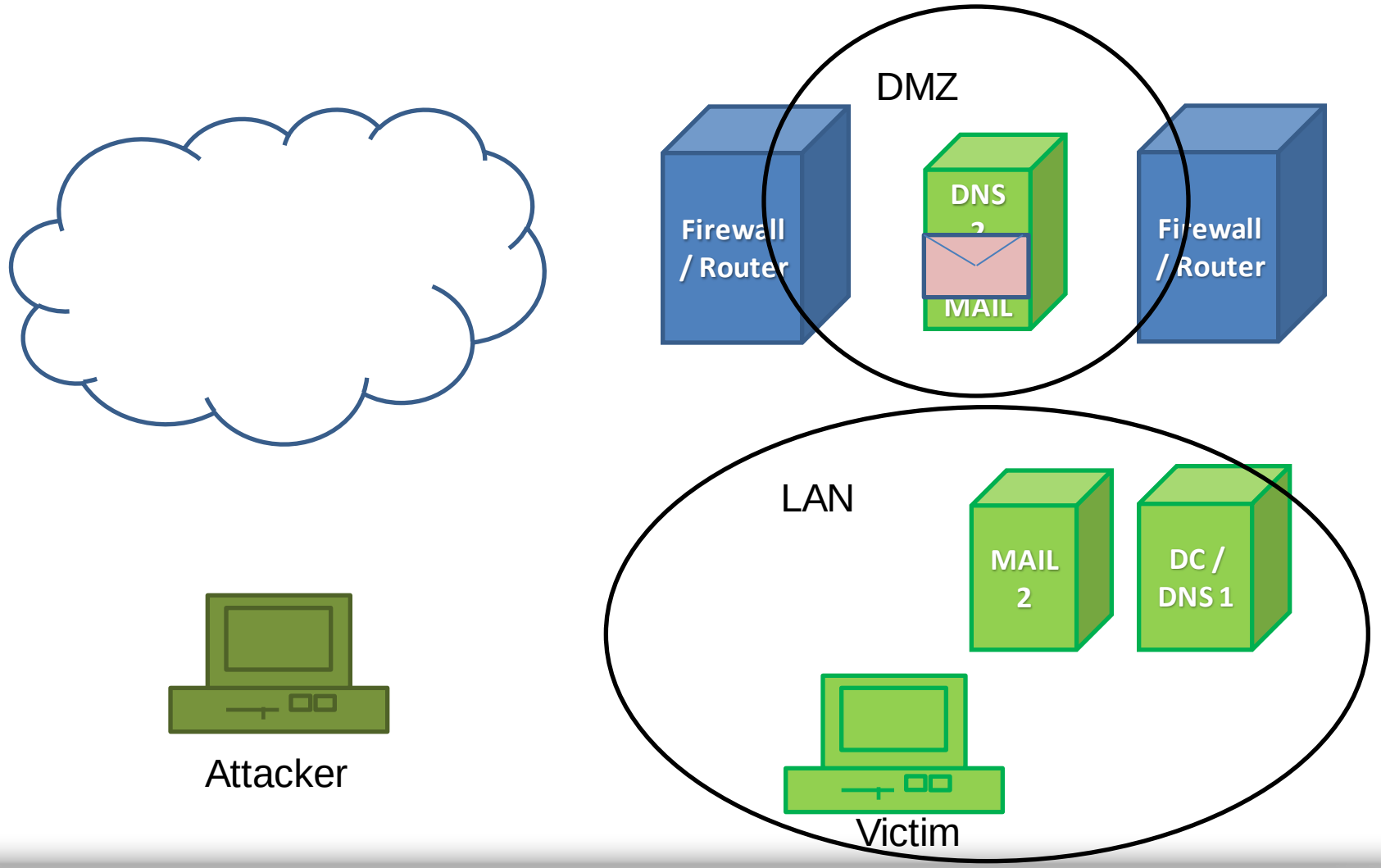
Step one – send mail



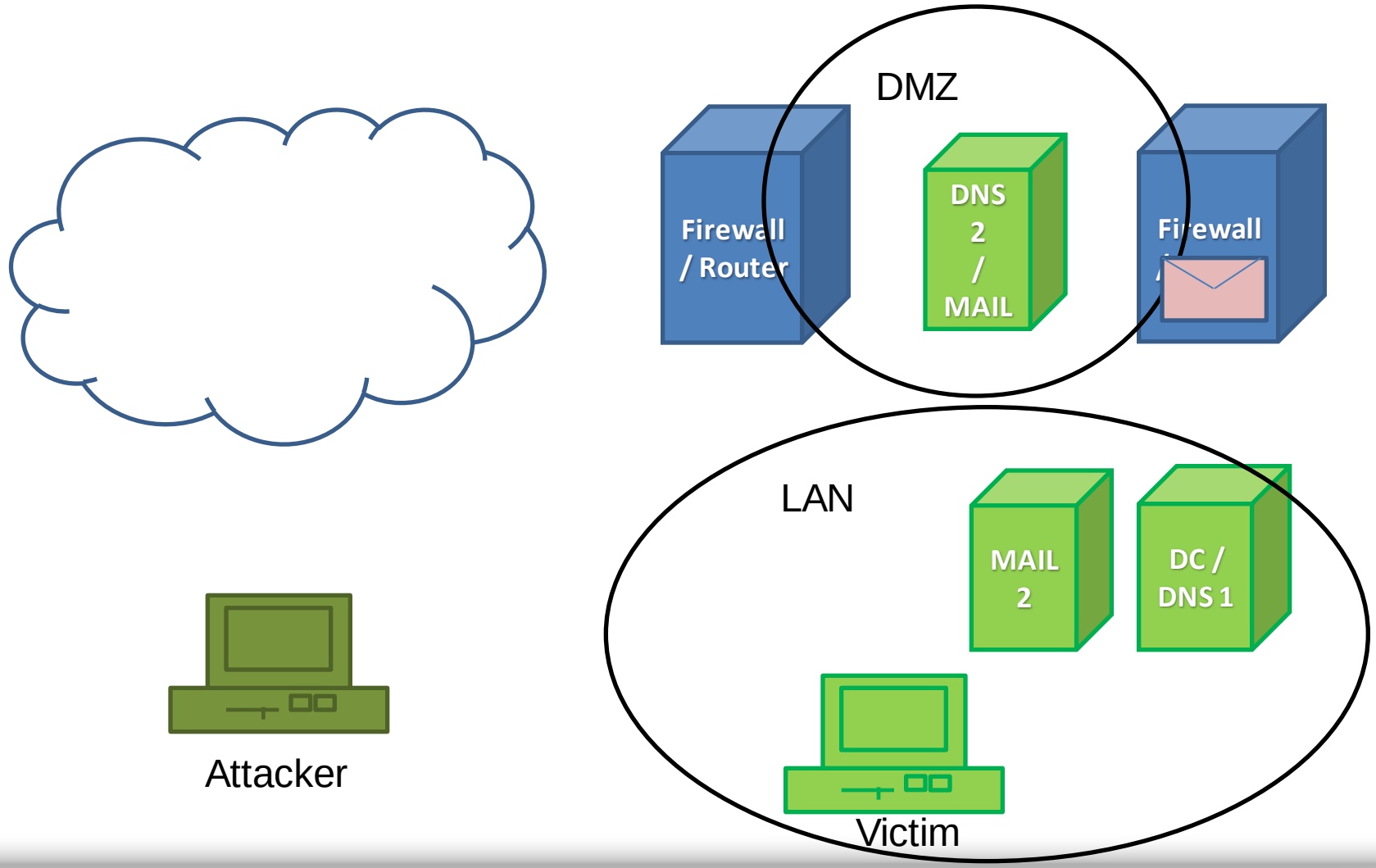
Step one – send mail



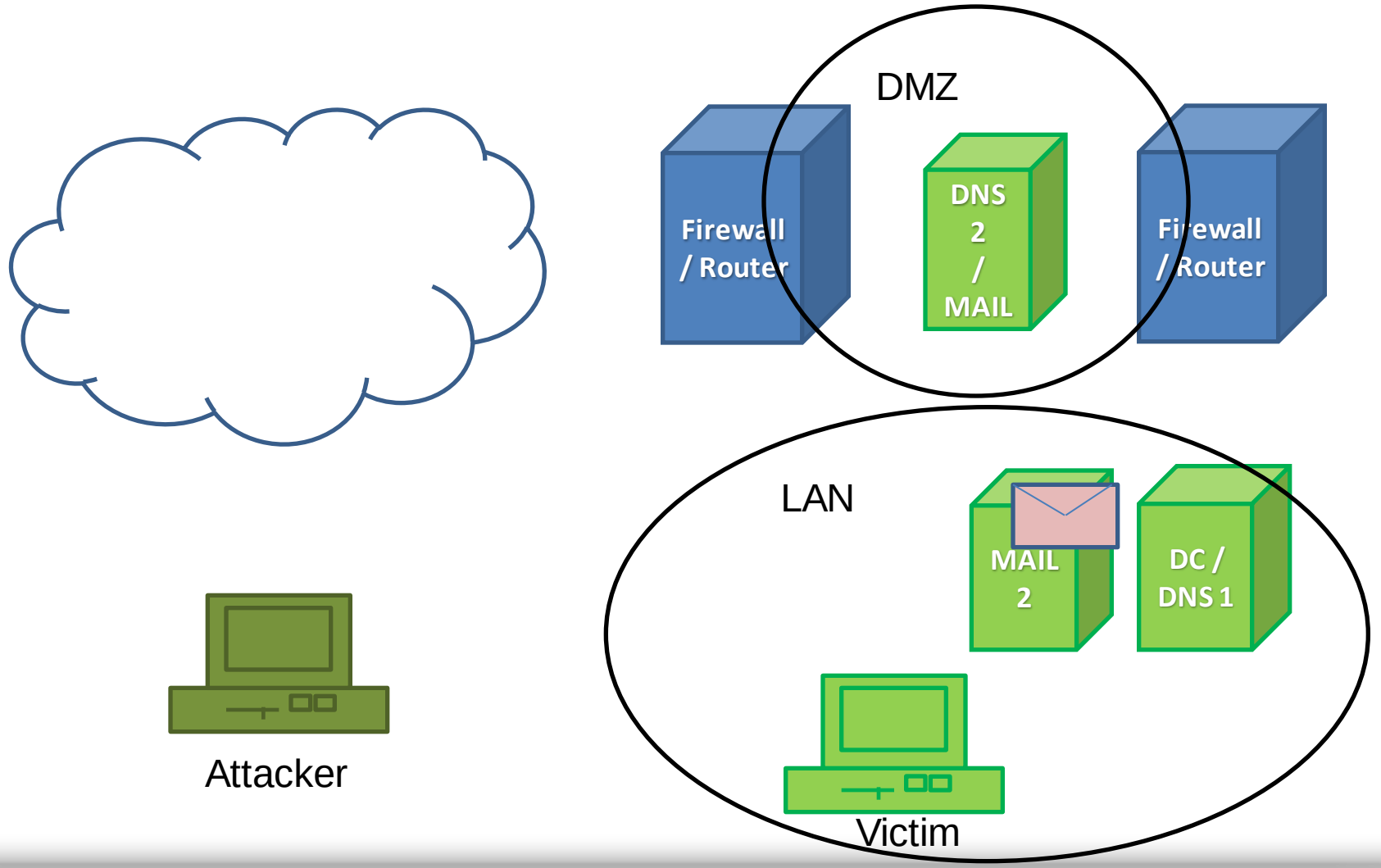
Step one – send mail



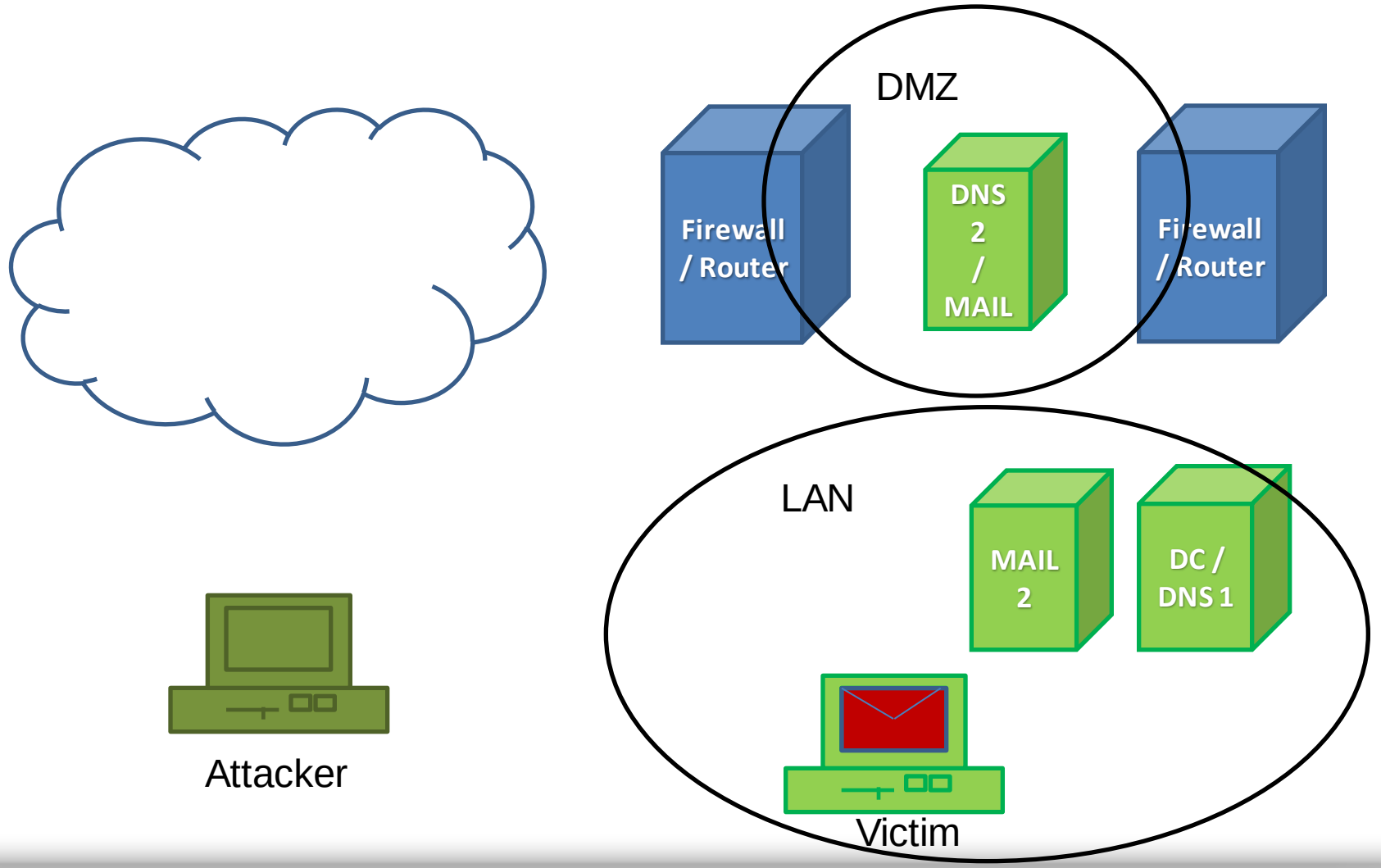
Step one – send mail



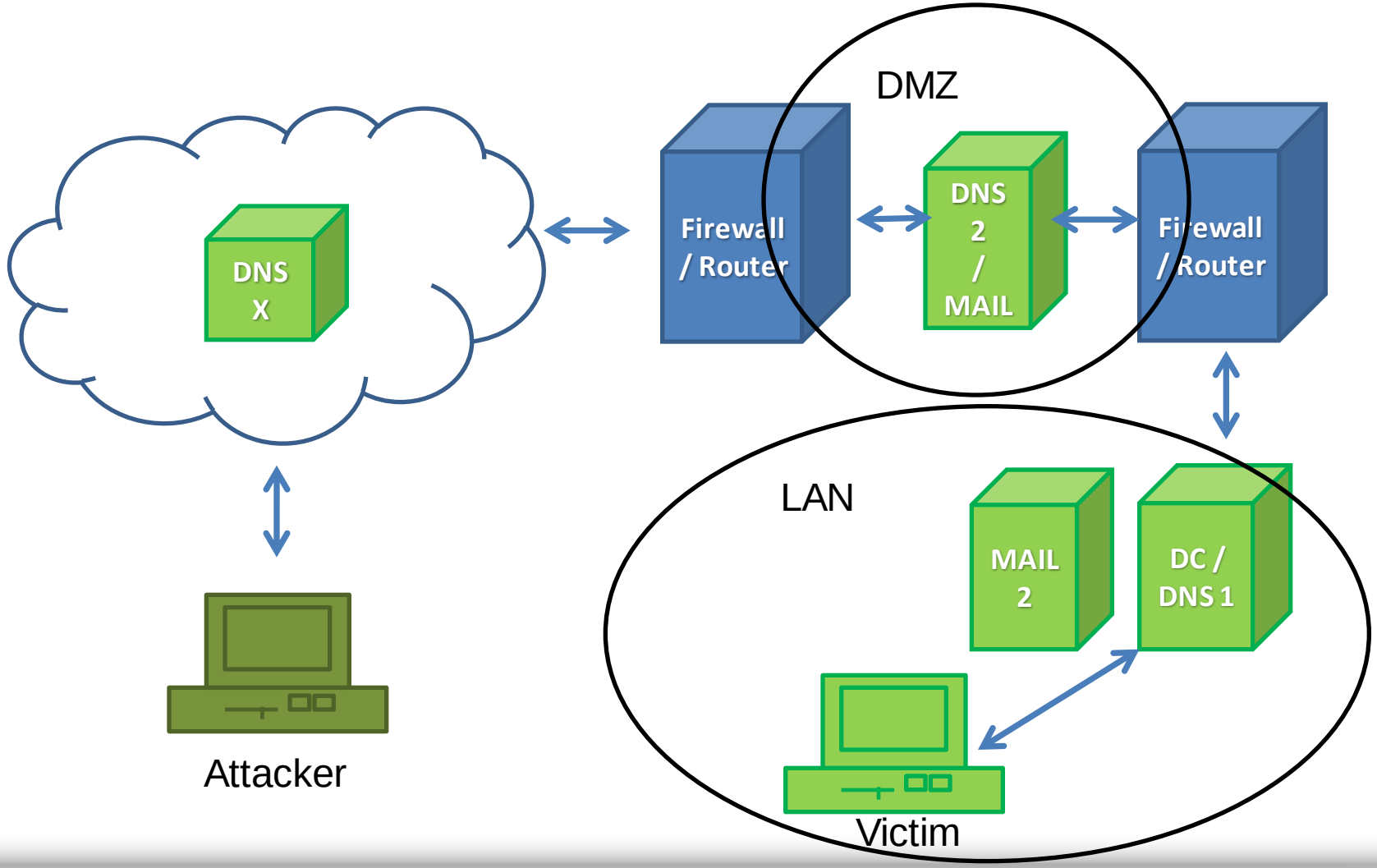
Step one – send mail



Step two – SE/infect



Step 3. DNS Tunnel



Fight!

Exploit: **CVE-2010-1240**

Fight!

Exploit: **CVE-2010-1240**

- ✓ Good for testing ‘awareness program’

Fight!

Exploit: **CVE-2010-1240**

- ✓ Good for testing ‘awareness program’
- ✓ Good for testing patch management procedures

Fight!

Exploit: **CVE-2010-1240**

- ✓ Good for testing ‘awareness program’
- ✓ Good for testing patch management procedures

SE scenario 1: **vacancy**

- ✓ Vacancy in west company …

Fight!

Exploit: **CVE-2010-1240**

- ✓ Good for testing ‘awareness program’
- ✓ Good for testing patch management procedures

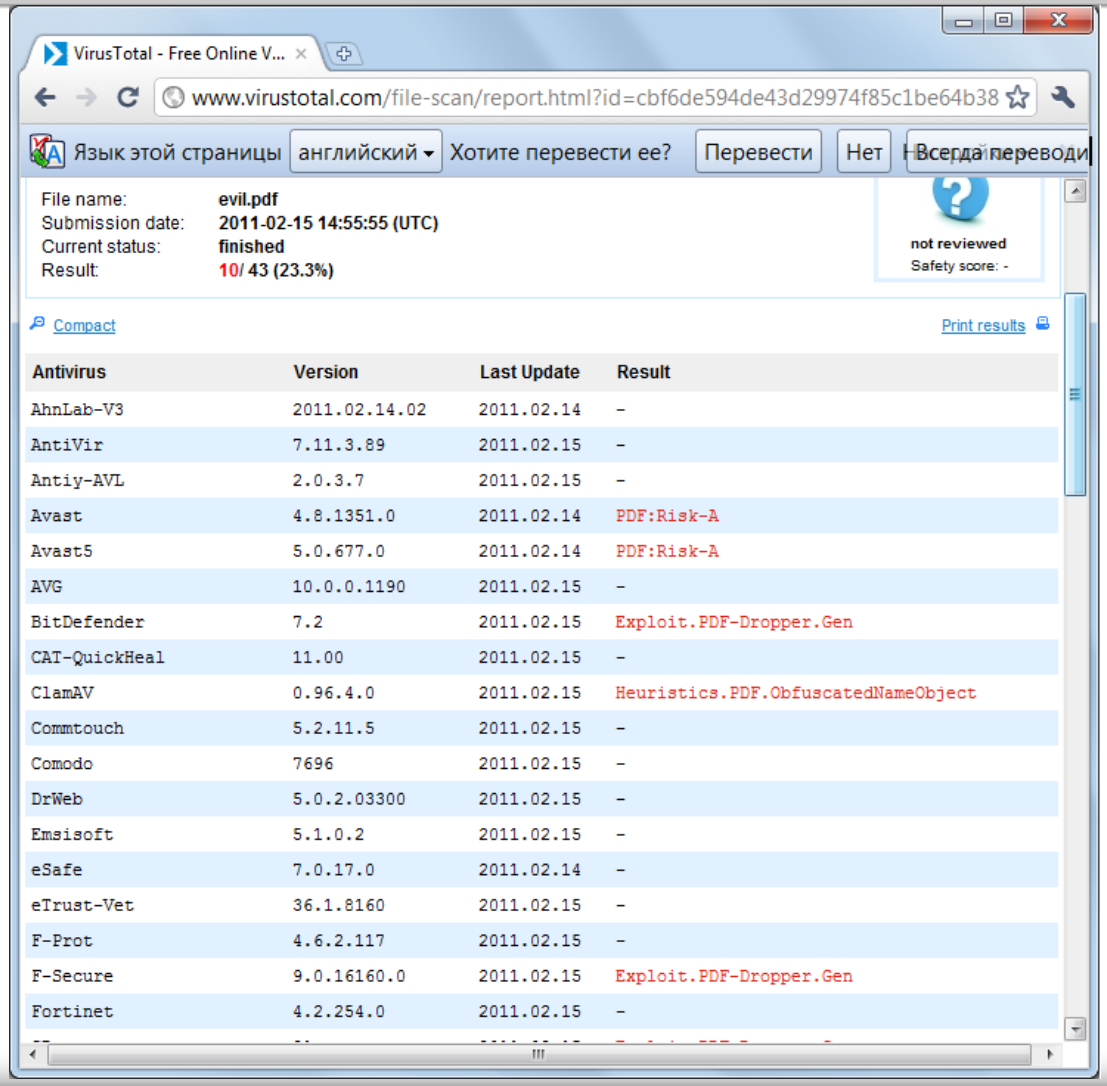
SE scenario 1: **vacancy**

- ✓ Vacancy in west company …

SE scenario 2: **mail from colleague**

- ✓ Spoof “From:” field
- ✓ Phone call give +1 to success (if it is pretty big company)

CVE-2010-1240



Antivirus	Version	Last Update	Result
AhnLab-V3	2011.02.14.02	2011.02.14	-
AntiVir	7.11.3.89	2011.02.15	-
Antiy-AVL	2.0.3.7	2011.02.15	-
Avast	4.8.1351.0	2011.02.14	PDF:Risk-A
Avast5	5.0.677.0	2011.02.14	PDF:Risk-A
AVG	10.0.0.1190	2011.02.15	-
BitDefender	7.2	2011.02.15	Exploit.PDF-Dropper.Gen
CAT-QuickHeal	11.00	2011.02.15	-
ClamAV	0.96.4.0	2011.02.15	Heuristics.PDF.ObfuscatedNameObject
Commtouch	5.2.11.5	2011.02.15	-
Comodo	7696	2011.02.15	-
DrWeb	5.0.2.03300	2011.02.15	-
Emsisoft	5.1.0.2	2011.02.15	-
eSafe	7.0.17.0	2011.02.14	-
eTrust-Vet	36.1.8160	2011.02.15	-
F-Prot	4.6.2.117	2011.02.15	-
F-Secure	9.0.16160.0	2011.02.15	Exploit.PDF-Dropper.Gen
Fortinet	4.2.254.0	2011.02.15	-

Obfuscation

```
pdf << "/F (cmd.exe) /P (/C echo Set
o=CreateObject^(\"Scripting.FileSystemObject\"^):Set
f=o.OpenTextFile^(\"#{file_name}\",1,True^):"
```

```
pdf << "/F (cMD.eXE) /P (/C e^cho
bb=\"Scri\"^&\"pti\"^&\"ng.FileSys\"^&\"temOb\"^&\"ject\":Set
o=Crea^teOb^ject^(bb^):Set f=o.OpenT^extFile^(\"#{file_name}\",1,Tr^ue^):"
```

DE-Obfuscation

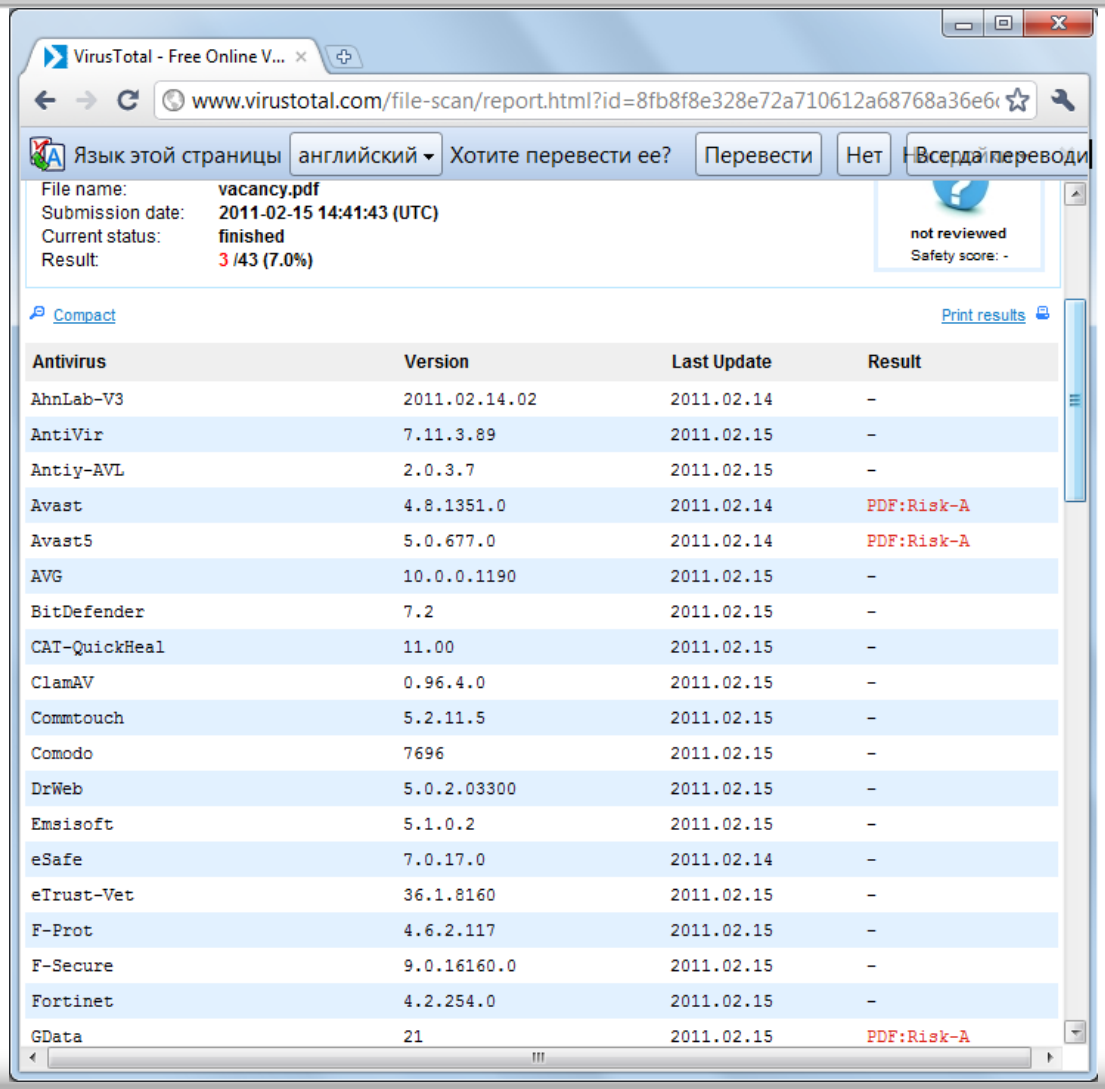
pdf << ioDef(2) << **nObfu**("<</Type/Outlines/Count 0>>") << endobj

pdf << ioDef(2) << "<</Type/Outlines/Count 0>>"<< endobj

pdf << ioDef(5) << **nObfu**("<</Type/Action/S/Launch/Win ") << "<< "

pdf << ioDef(5) << "<</Type/Action/S/L#**61**unch/Win " << "<< "

Result – 70%



Antivirus	Version	Last Update	Result
AhnLab-V3	2011.02.14.02	2011.02.14	-
AntiVir	7.11.3.89	2011.02.15	-
Antiy-AVL	2.0.3.7	2011.02.15	-
Avast	4.8.1351.0	2011.02.14	PDF:Risk-A
Avast5	5.0.677.0	2011.02.14	PDF:Risk-A
AVG	10.0.0.1190	2011.02.15	-
BitDefender	7.2	2011.02.15	-
CAT-QuickHeal	11.00	2011.02.15	-
ClamAV	0.96.4.0	2011.02.15	-
Commtouch	5.2.11.5	2011.02.15	-
Comodo	7696	2011.02.15	-
DrWeb	5.0.2.03300	2011.02.15	-
Emsisoft	5.1.0.2	2011.02.15	-
eSafe	7.0.17.0	2011.02.14	-
eTrust-Vet	36.1.8160	2011.02.15	-
F-Prot	4.6.2.117	2011.02.15	-
F-Secure	9.0.16160.0	2011.02.15	-
Fortinet	4.2.254.0	2011.02.15	-
GData	21	2011.02.15	PDF:Risk-A

Penetration

Penetration =
Antivirus bypass **+**
SE factor 1 (mail text) **+**
Vulnerability exist **+**
SE factor 2 (PDF warning text) **+**
DNS recursion is enabled**;**

- Antivirus software bypassed by (de)obfusication of exploit code
- SE always roxXx!
- Adobe Reader is not patched (it's hard if there no access to the Internet)
- DNS recursion is enabled by default (tunnel possible)

So we can control workstation that have not direct/web

access to the Internet

Tools

- DNScat - http://www.skullsecurity.org/wiki/index.php/Dnscat
- DNS reverse shellcode - http://www.projectshellcode.com/?q=node/5

Tools

- DNScat - http://www.skullsecurity.org/wiki/index.php/Dnscat
- DNS reverse shellcode - http://www.projectshellcode.com/?q=node/5

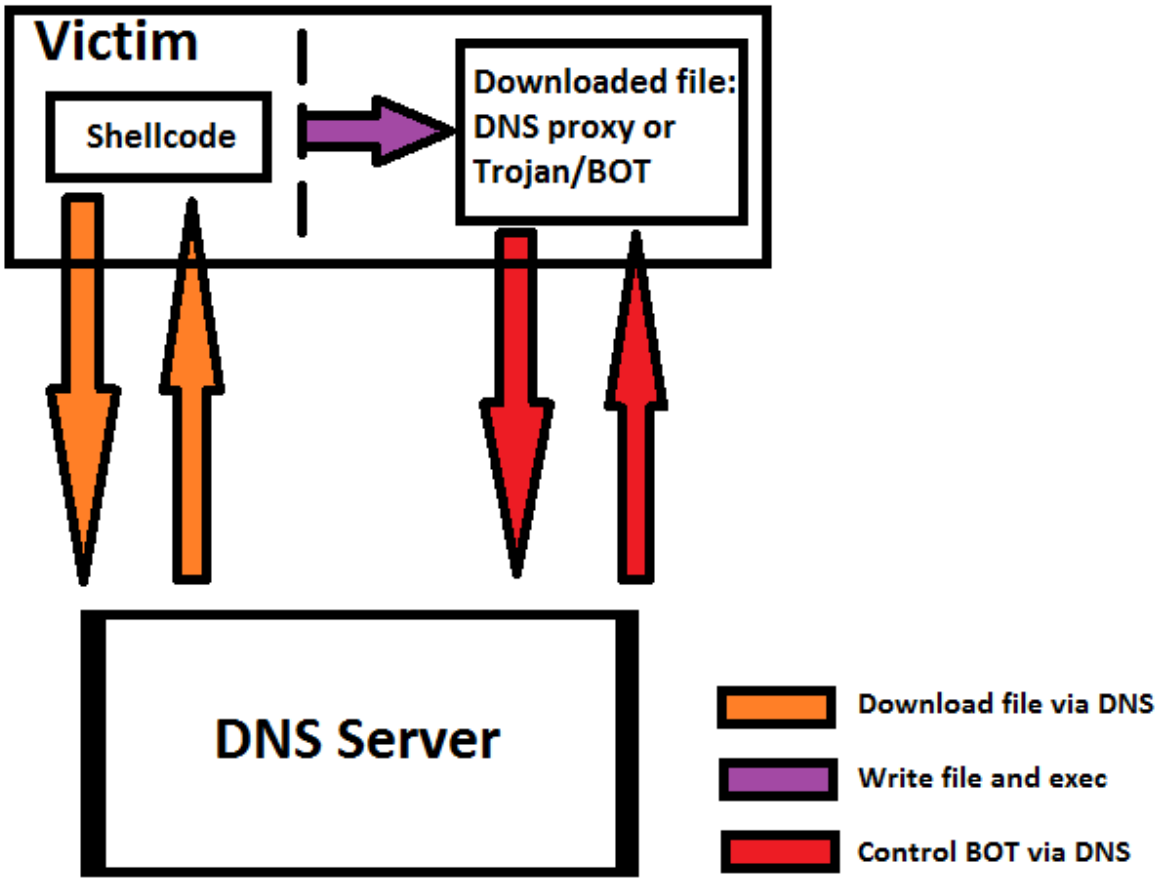
Not enough for my tasks:

- Not stable
- Doesn't support MULTI-shell
- Not comfortable to use
- DNScat use sockets in process…
- Too big size (more then 1000 bytes)

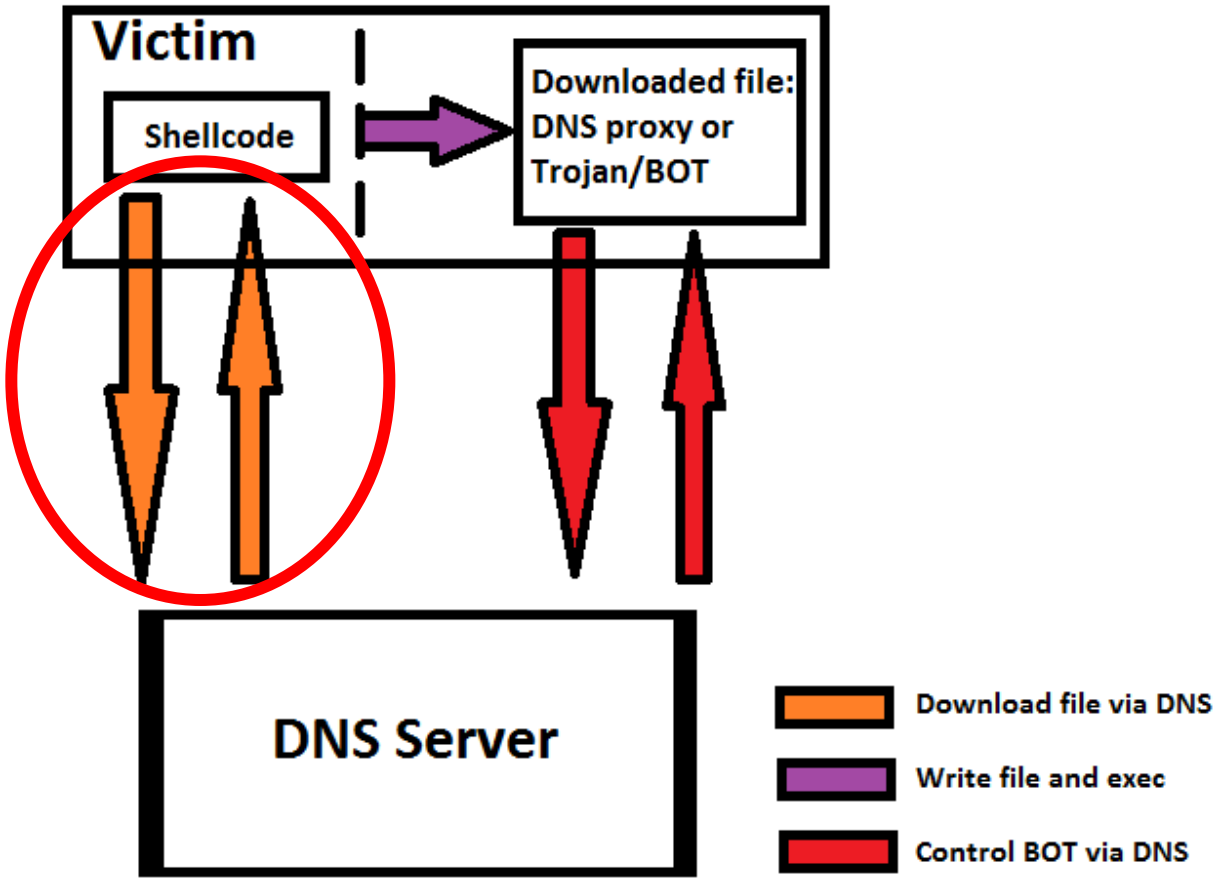
I need another one

- Size<900 bytes
- Multi-shell support
- Works with win7
- Auto-commands
- Easy to write NEW features
- Easy to manage
- Metasploit compatible
- Without TXT records 8)
- Without connections – Personal firewall bypass/ UAC bypass
- Fast =)

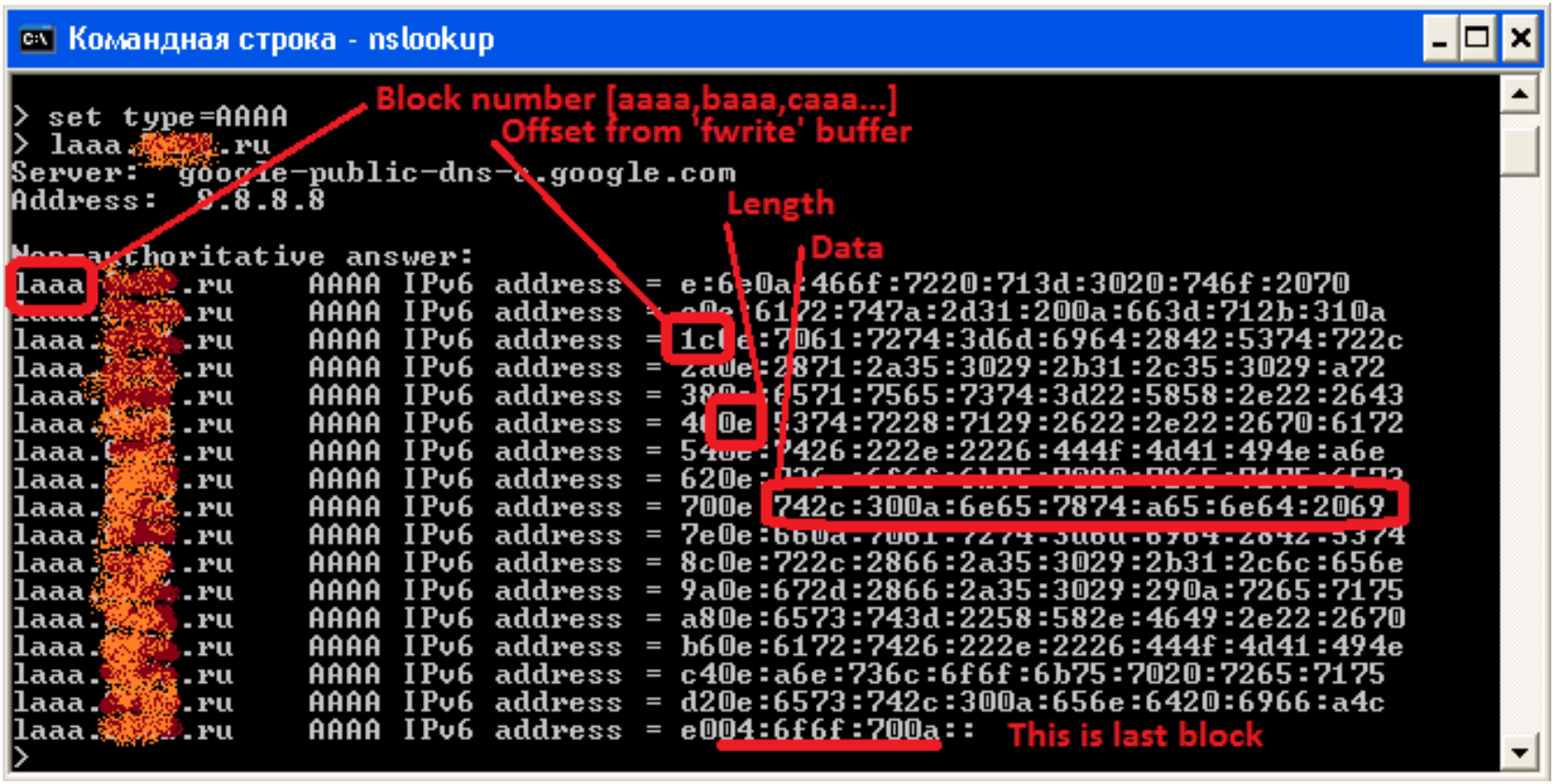
I need more then just shellcode



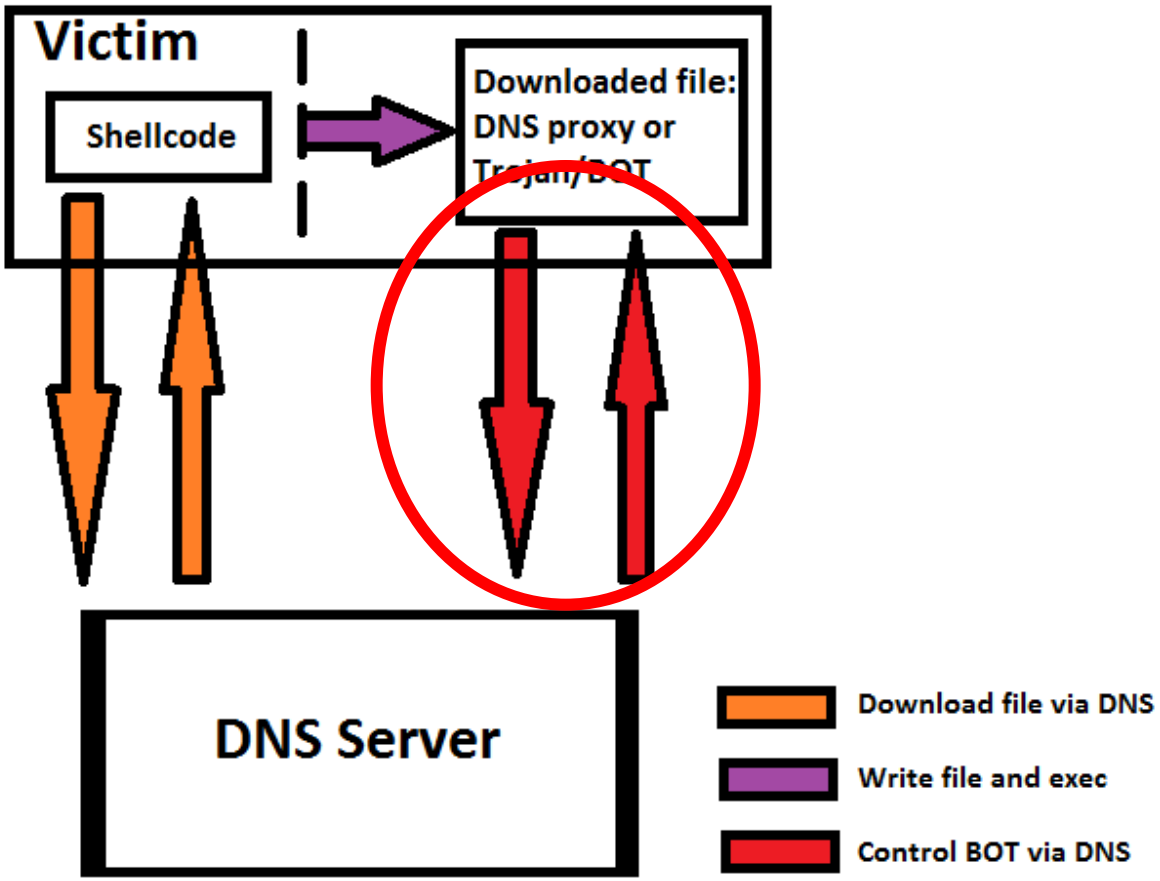
Download



Download...

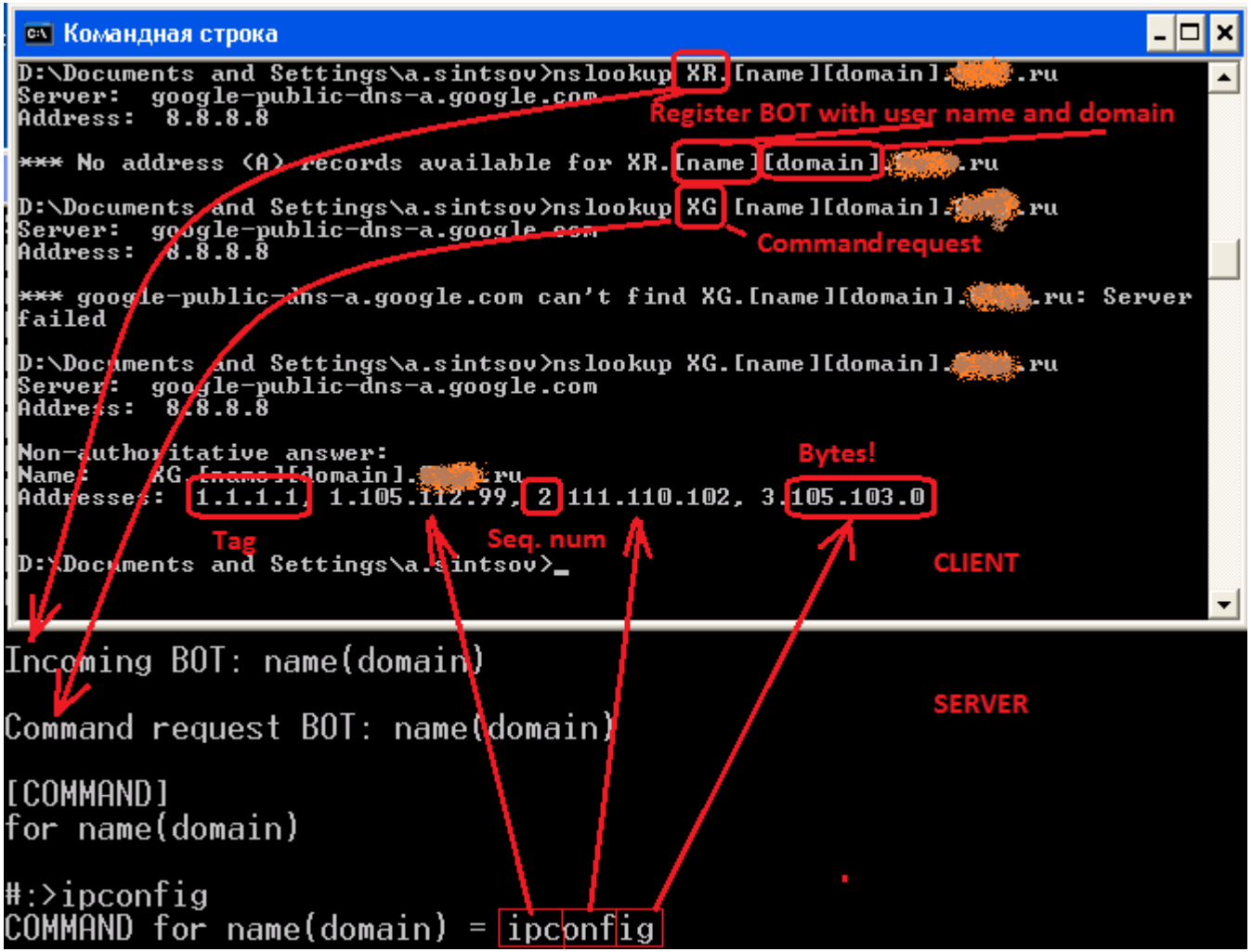


Protocol

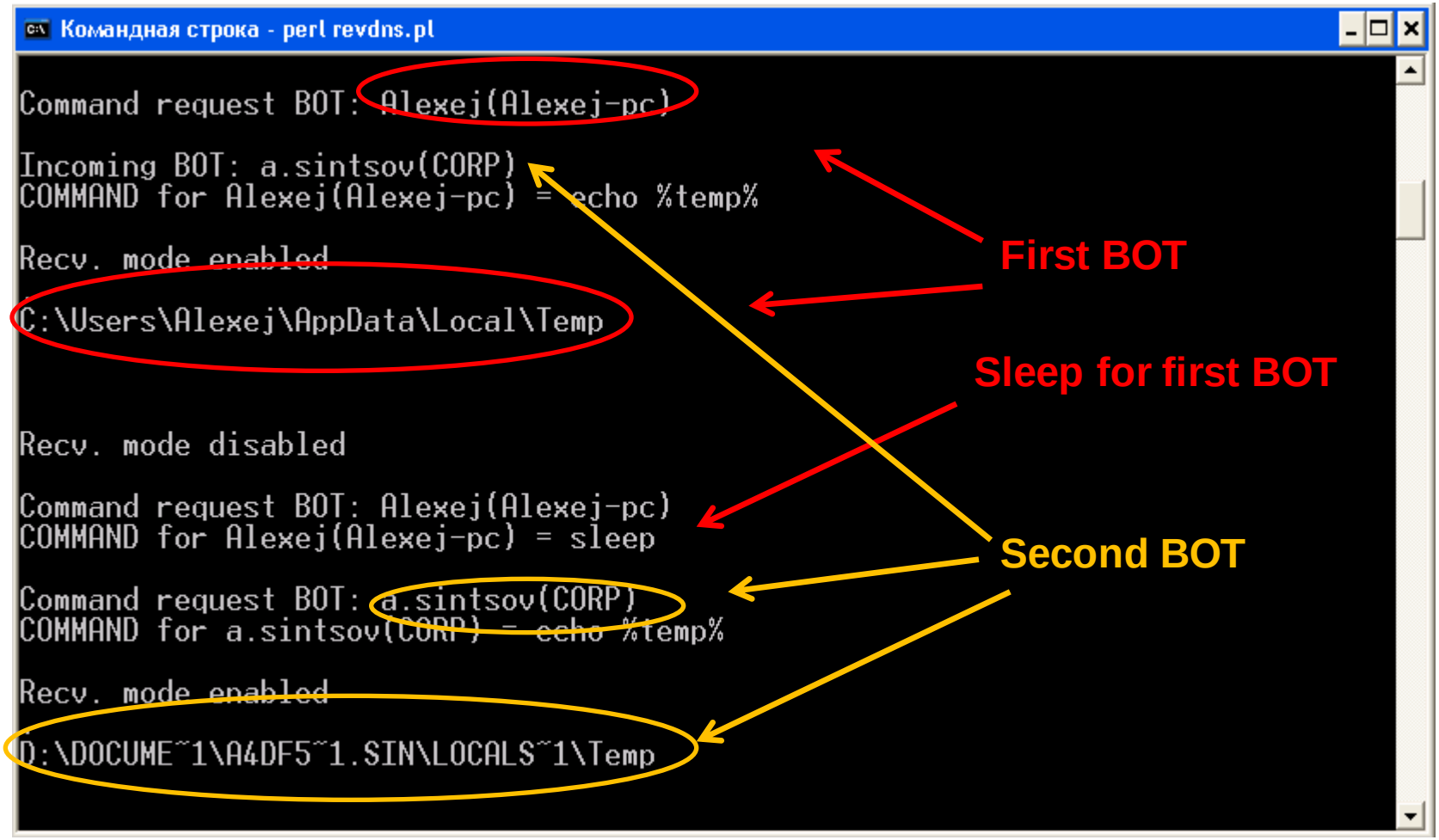


Digital Security
Research Group

Command for BOT…



Auto-manage(timeouts)/Multi-shells



BOT

- Written on VBS – small size, fast load ~ 2-3 sec!
- Can be upgraded (new functional that easy to add)
- You can write your own BOT (any language) by using my protocol without changing shellcode. Scalable.

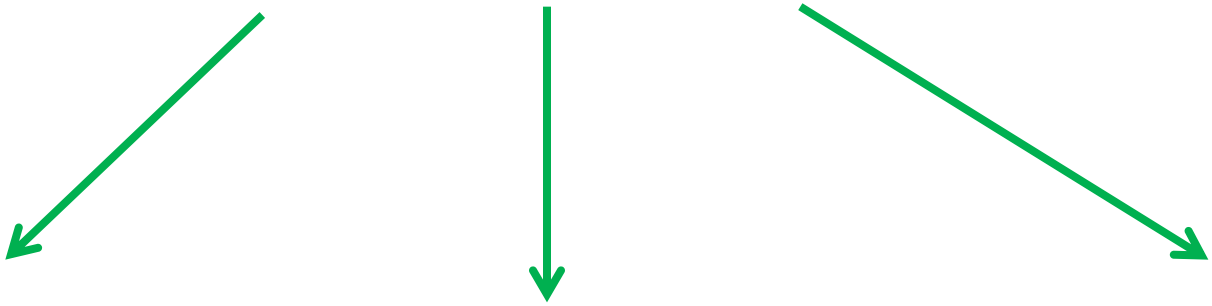
MINUSES:

- Long time for downloading binaries ~ up to 5 min
- Not more then 84 bytes for command at one time, sorry 8)

LIVE DEMO

Why it is dangerous

- DNS are everywhere (for example with Domain Controller)
- DNS recursion is enabled by default
- Local DNS is available for everyone

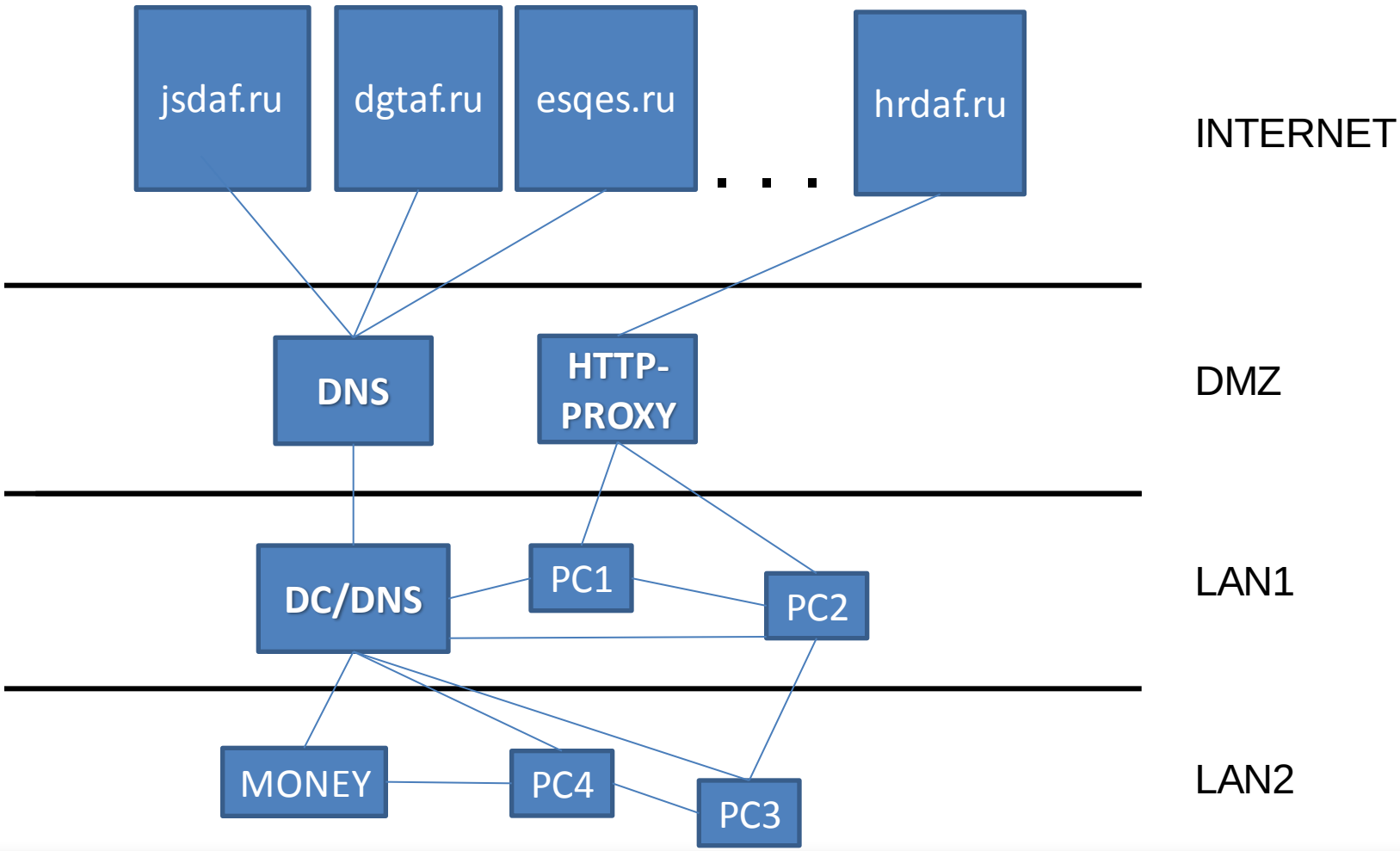


Is it good for PCI DSS, when it is possible to create tunnel to YOUR CDE?

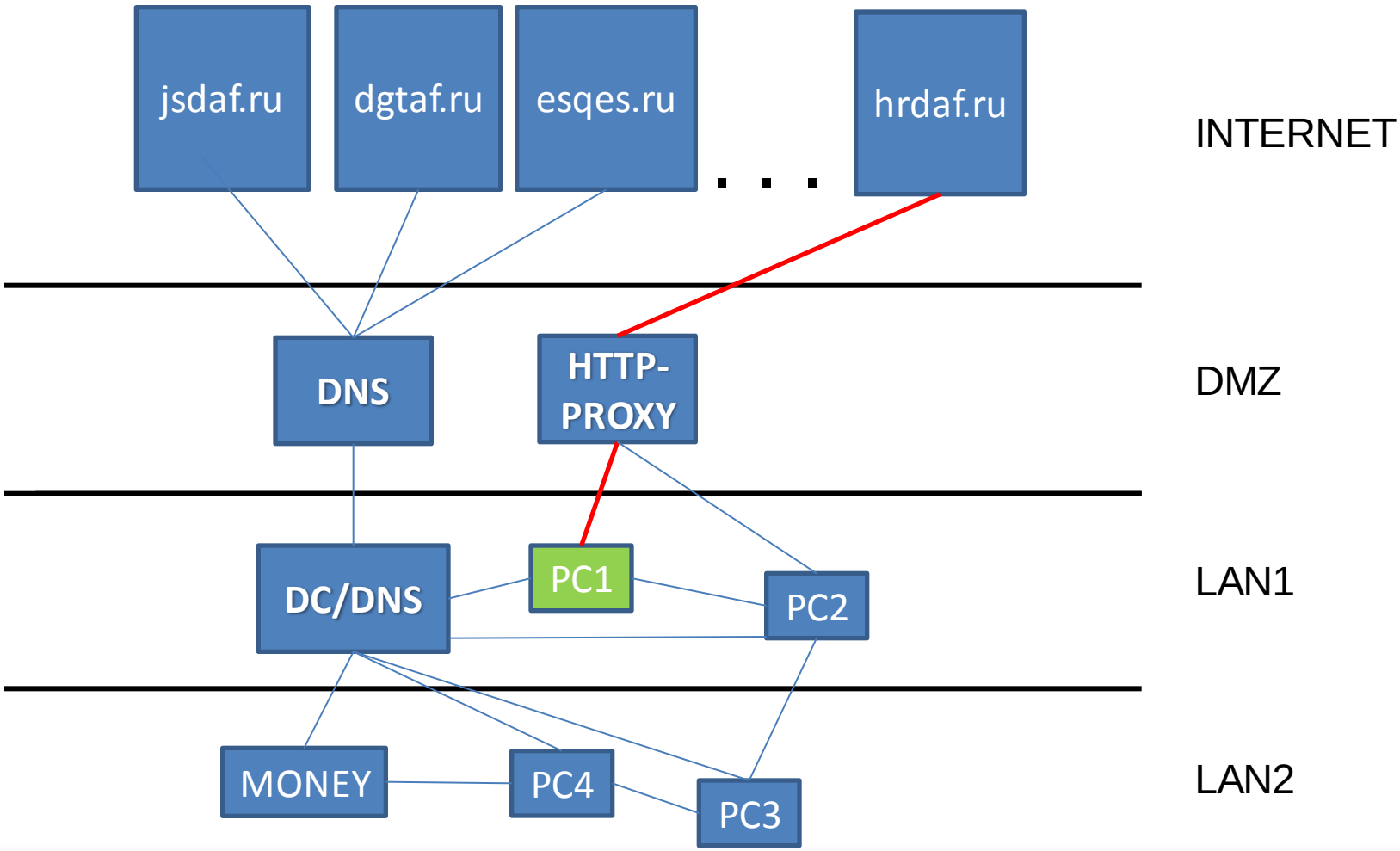
What about a SCADA? Is it possible to create tunnel to YOUR technologic networks?

It can be used by botnet owners and worms. Evil can get access to most securest zones.

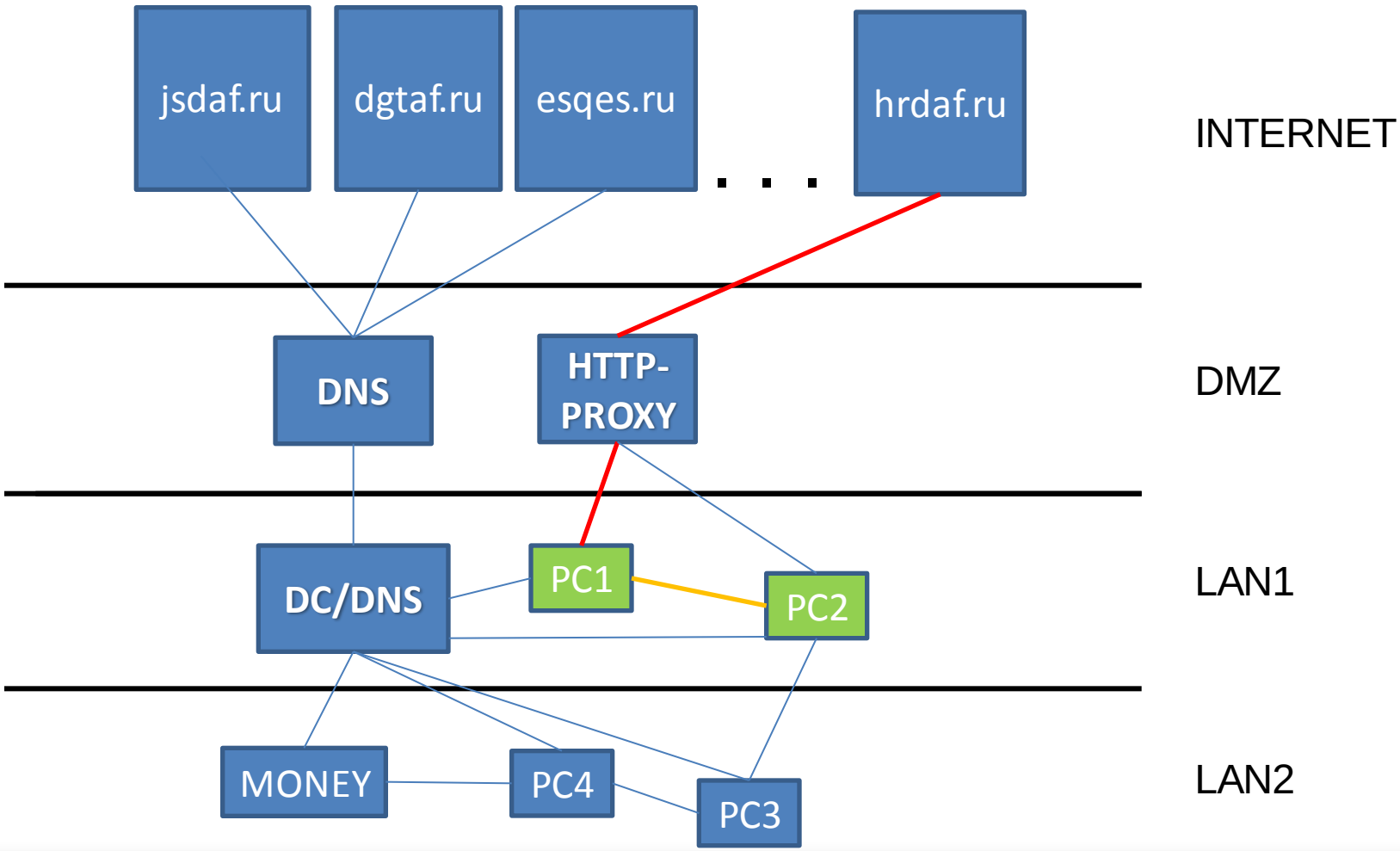
Tomorrow



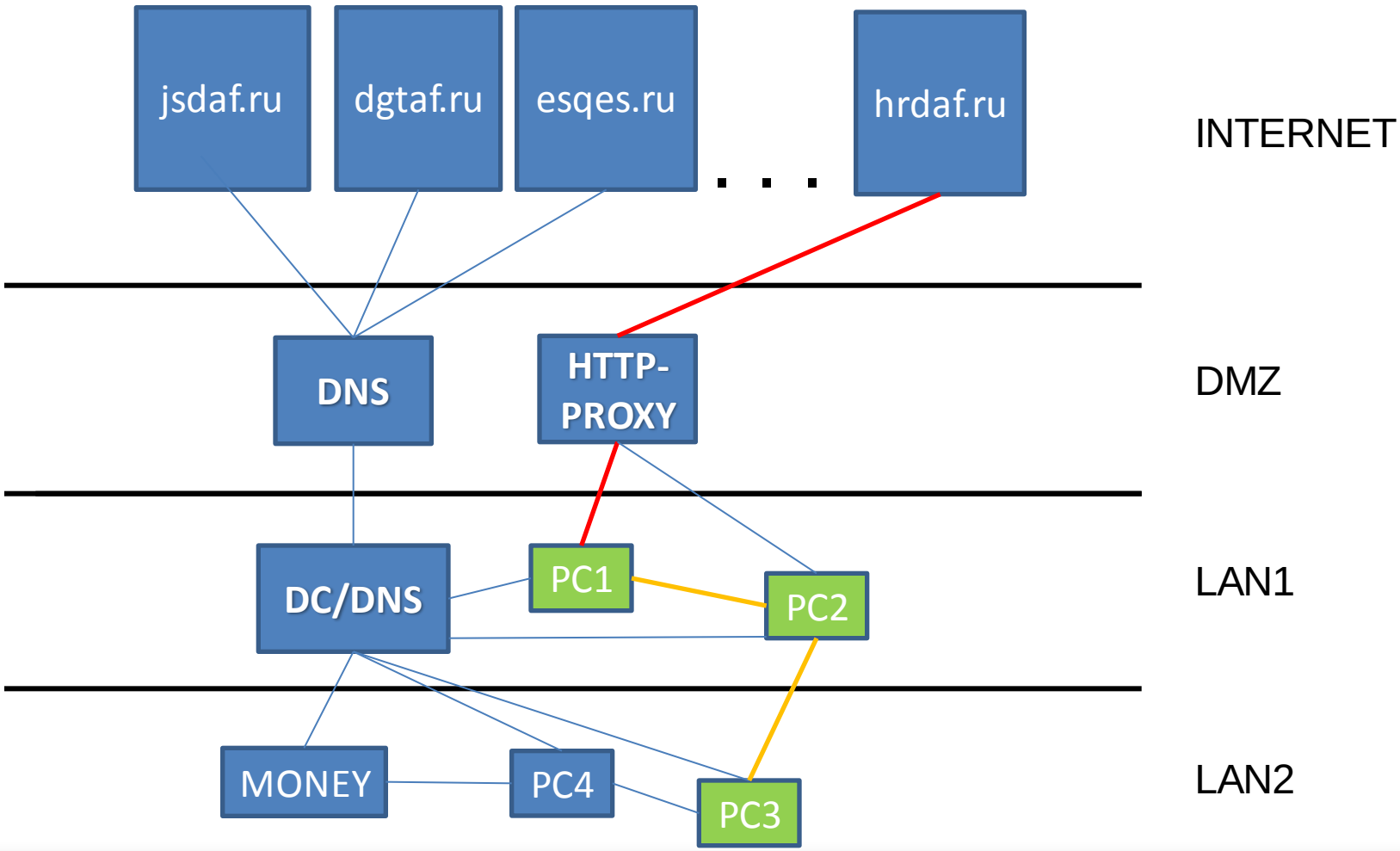
Exploiting...



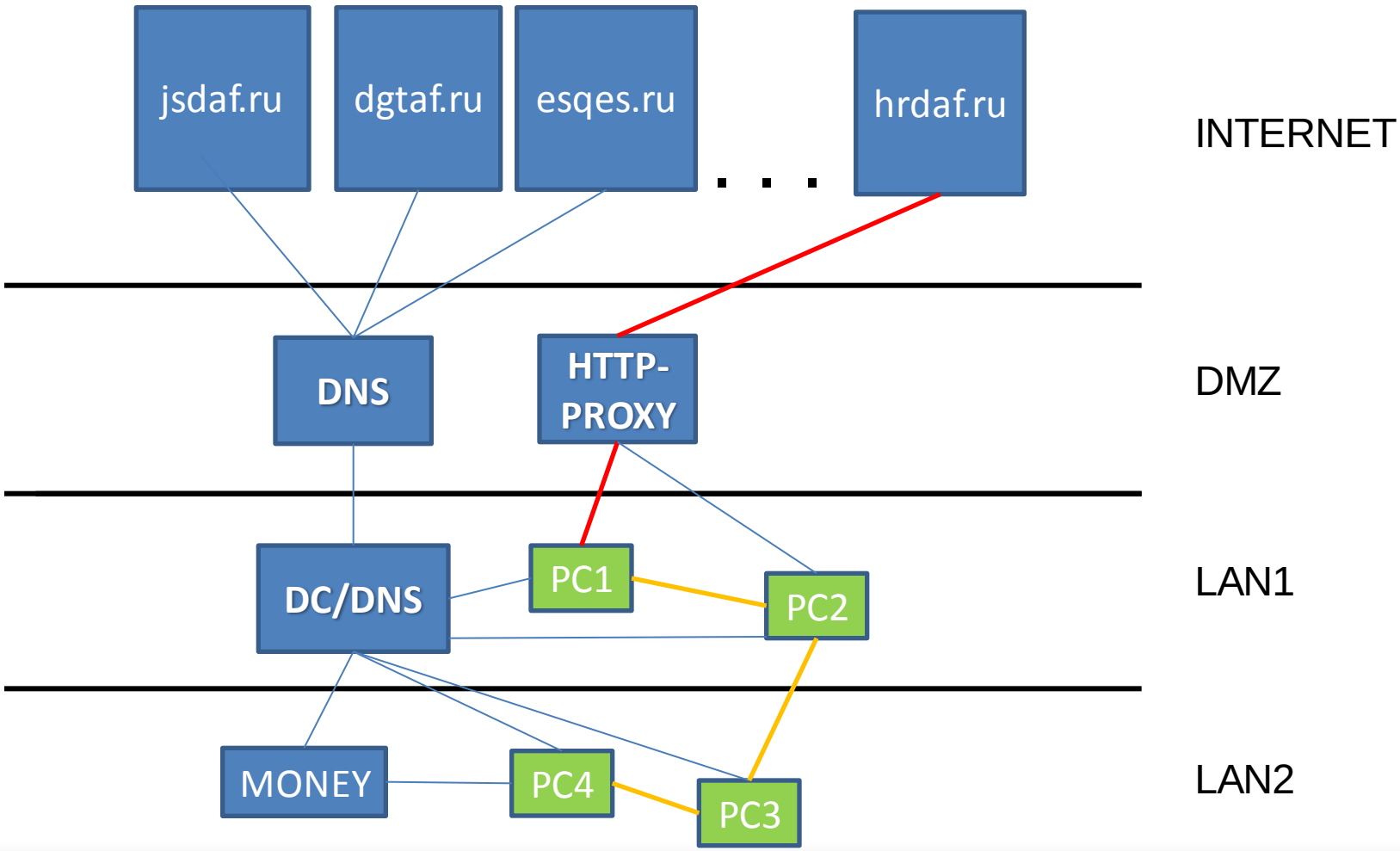
Worm...



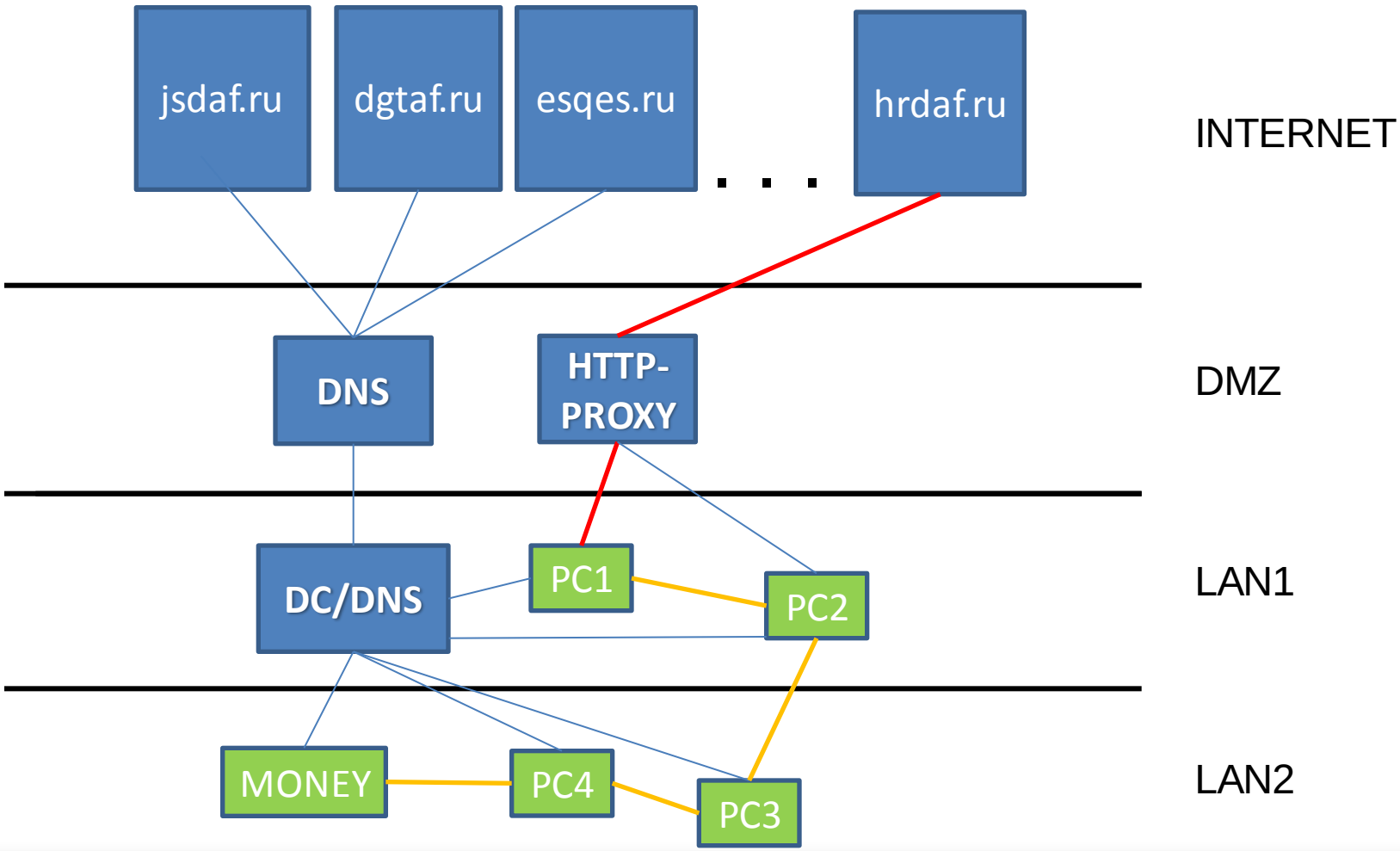
Worm…



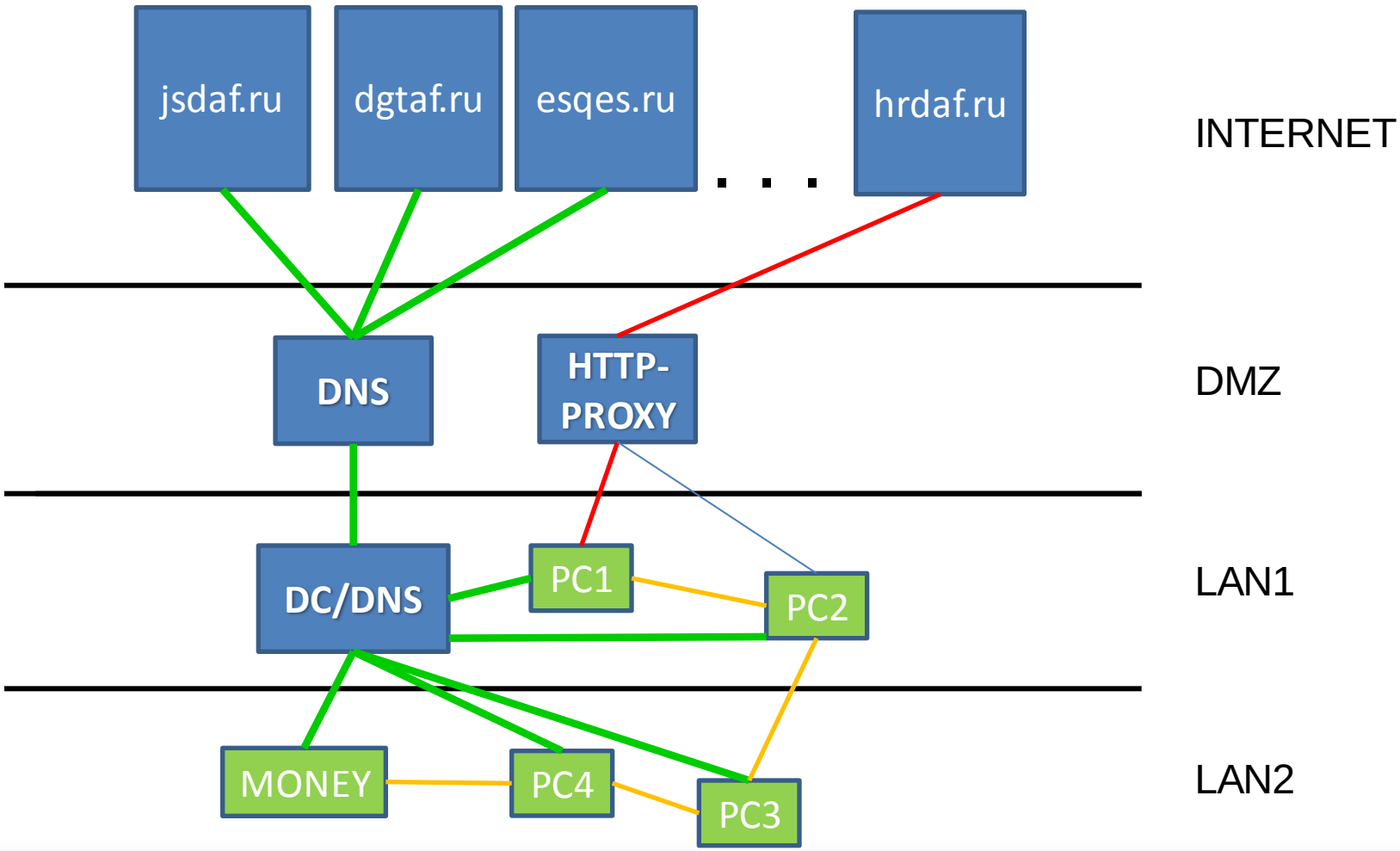
Worm...



Worm...



Control...



Countermeasures

- **Use any IDS that can see anomalies in DNS traffic**
- **Disable recursion on the DNS server**
- **Use /etc/hosts =)**
- **Pray**

Download

If you are interesting in this work, you can download it from:
www.dsecrg.com/files/pub/tools/revdns.zip

P.S. I am scary of Russian police, so I remove from VBS BOT some code that doing an execution of shell-command. If you need it for legal purposes (pen-tests) – just write me an e-mail and I'll send you full version. Fell free to add whatever you want to this code =)

Questions?

www.twitter.com/asintsov
a.sintsov@dsec.ru

ConfidEncE 2011