

Large-scale coordinated attacks: Impact on the cloud security

Damien Riquet Gilles Grimaud M. Hauspie

Team 2xS
Université Lille 1, France

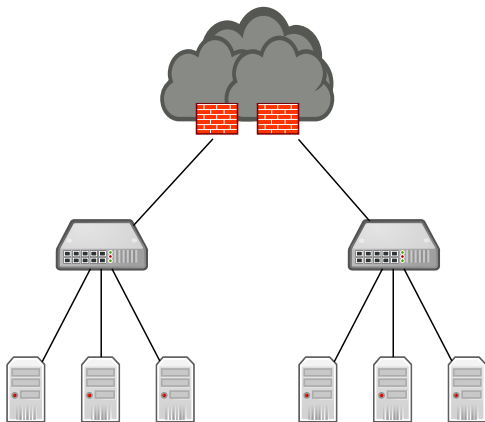
MCNCS, Palermo, 2012

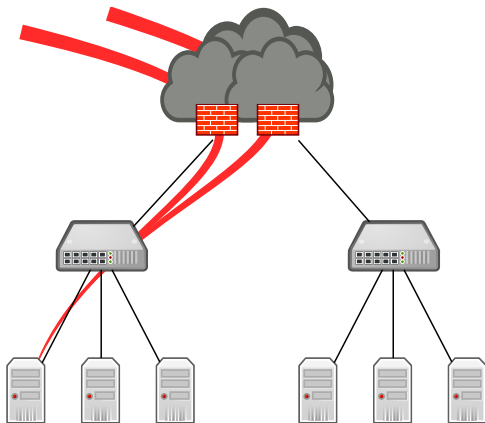
Study on the impact of distributed attacks on Cloud Computing

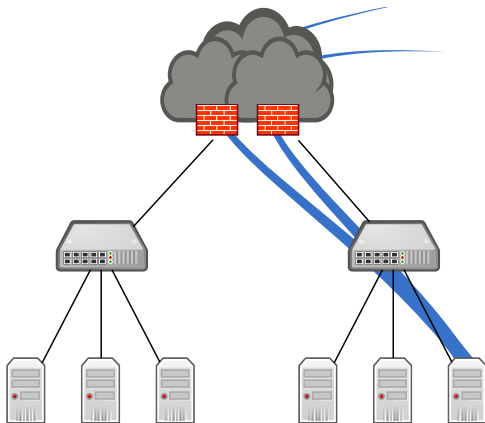
- Cloud Computing: a popular model to process large data set
- Several layers according to the needs of customers
- Store confidential data
- Growing concern about its security

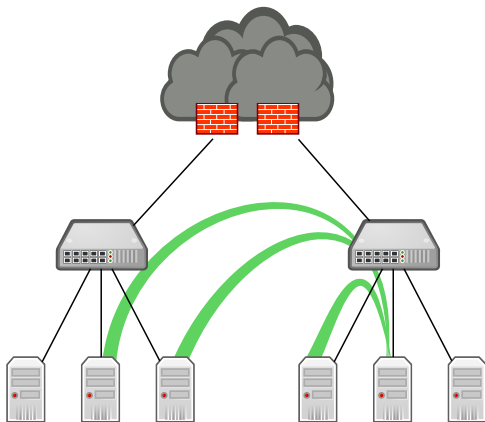
Attacks on the cloud

- Distributed attacks to evade security solutions
- Weaknesses of cloud structure









Goals of this paper

- Study security solutions used by Cloud Computing
- Show that distributed attacks could be very efficient
- 1-path architecture
- Use case: distributed portscan

Outline

- 1 How Cloud Computing can be secured
- 2 Distributed portscan
- 3 Experimental protocol
- 4 Results

Outline

- 1 How Cloud Computing can be secured
 - Security solutions commonly used
 - Detection methods
- 2 Distributed portscan
- 3 Experimental protocol
- 4 Results

Cloud security - Security solutions commonly used

Firewalls [BC94]

- At the border of the network
- Analyze traffic between two networks
- Security policies

Intrusion Detection System (IDS) [Ped05]

- Network or Host based
- Passive device: raise alarms
- Pattern-matching, analyze traffic

Detection methods

Misuse detection

- Look for known patterns of misuse
- Pattern-matching
- Need constant update of the database

Anomaly detection

- Knowledge of standard
- Raise an alarm when an anomaly is detected
- Detect unknown attacks
- May raise a lot of false positive

Outline

- 1 How Cloud Computing can be secured
- 2 **Distributed portscan**
 - Definition
 - Distribution methods
- 3 Experimental protocol
- 4 Results

Distributed portscan: a use case

[Shi00] A portscan is ...

«an attack that sends client requests to a range of server port addresses on a host, with the goal of finding an active port and exploiting a known vulnerability of that service.»

Usage and goals

- Reconnaissance phase
- Discover weaknesses of a network
- Used by worms, malicious hackers

How to distribute a portscan

Naive distribution [KCS07]

- Sequential utilization of scanners
- Use a scanner until it is detected then select another one

Parallel distribution

- Distribute ports among scanners
- Execute portscan on scanners
- Process results afterwards

Outline

- 1 How Cloud Computing can be secured
- 2 Distributed portscan
- 3 Experimental protocol**
 - Security solutions
 - Network architecture
 - Benchmark configurations
- 4 Results

Tested security solutions

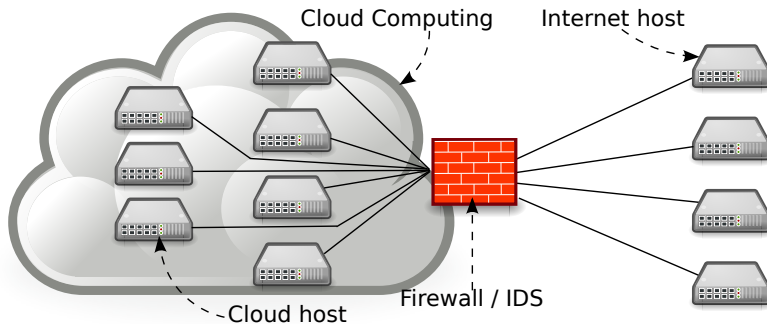
Snort

- Popular open source IDS
- Detection methods
 - Signature-based (written by the community)
 - Threshold-based (sfPortscan module)

Commercial firewall

- United Threat Management (network firewall and an IDS)
- Detection methods
 - Anomaly-based (TCP Automaton)
 - Threshold-based

Network architecture



Benchmark configurations

Network architecture

- Number of scanners: 2^n , with $1 \leq n \leq 6$
- Number of targets (Snort): 2^n , with $1 \leq n \leq 6$
- Number of targets (Commercial): 4
- Security solution configuration: default

Portscan

- Portscan timing:

| | | | |
|--------|------------|--------|--------|
| insane | aggressive | normal | polite |
| 5 ms | 10 ms | 0.4 s | 0.4 s |

- Number of ports: 100 per target (most used ports)
- Distribution methods: Naive and Parallel
- Portscan techniques: Connect, SYN, RPC, FIN, Xmas and Null

Outline

- 1 How Cloud Computing can be secured
- 2 Distributed portscan
- 3 Experimental protocol
- 4 Results**
 - Evaluation
 - Connect scanning
 - Null scanning
 - Results wrap up

Evaluation

Attacker Success Rate

n = Number of ports successfully scanned before detection

T = Total number of ports to scan

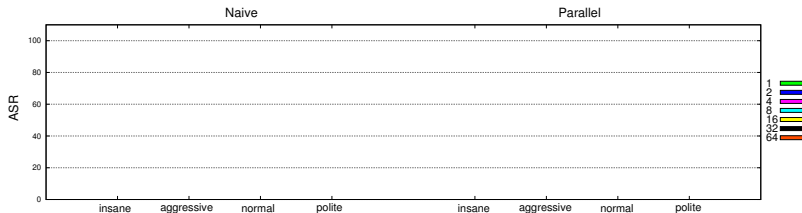
$$ASR = \frac{n}{T}$$

The lower is the ASR, the better is the security solution

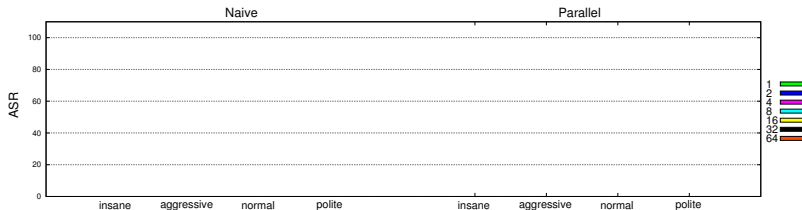
Successful portscan :

- undetected
- correct port state
- generated traffic reaches targets

Connect scanning - 4 targets

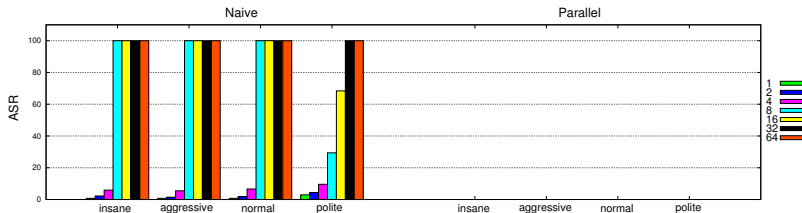


Snort

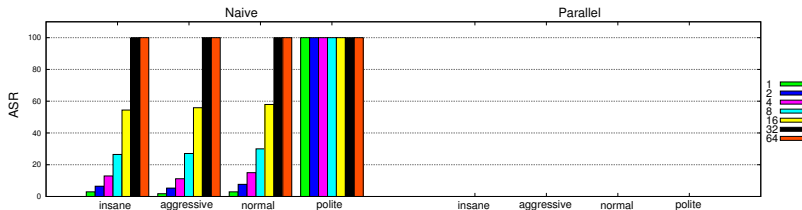


Commercial firewall

Connect scanning - 4 targets

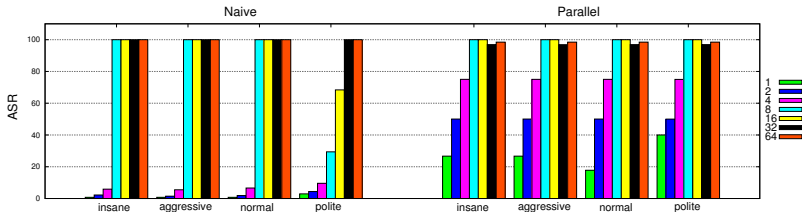


Snort

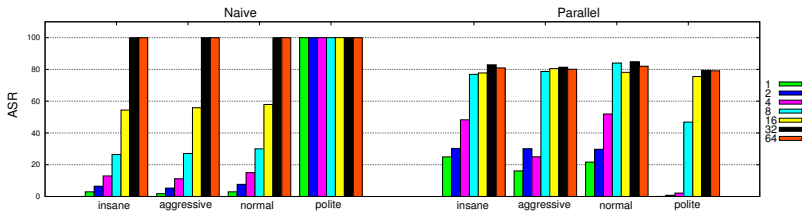


Commercial firewall

Connect scanning - 4 targets

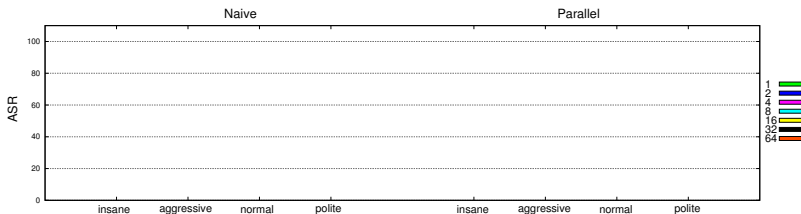


Snort

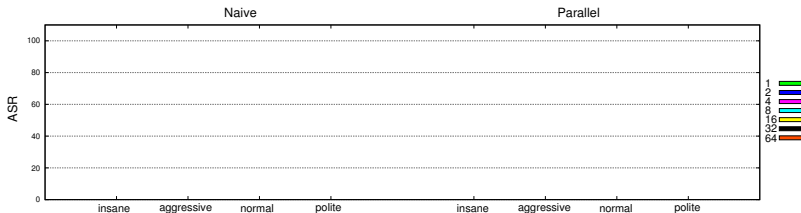


Commercial firewall

Connect scanning - Snort

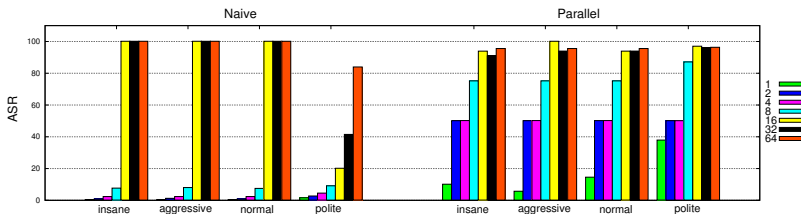


Snort - 8 targets

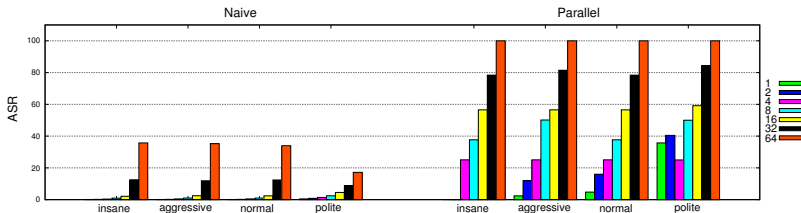


Snort - 32 targets

Connect scanning - Snort

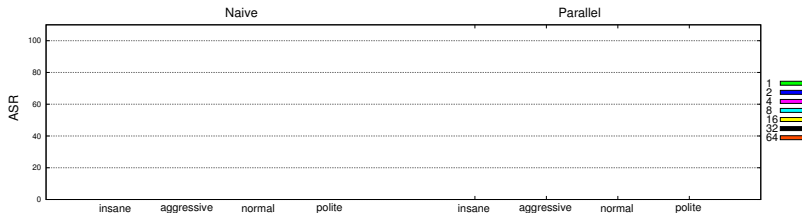


Snort - 8 targets

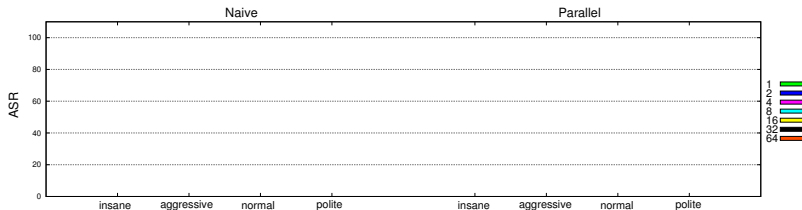


Snort - 32 targets

Null scanning - 4 targets

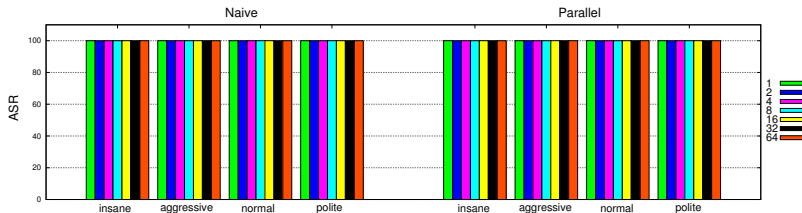


Snort

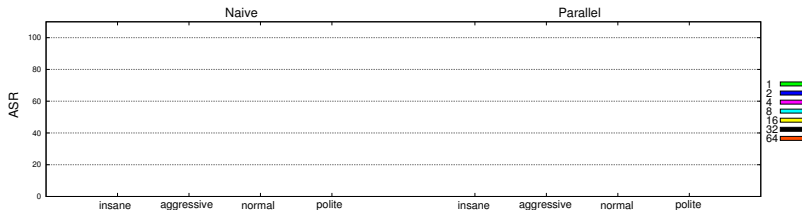


Commercial firewall

Null scanning - 4 targets



Snort



Commercial firewall

Results wrap up

Distributed attacks could be very efficient:

- 32/64 scanners are enough to remain undetected
- Weaknesses of security solution (timing, outdated database)
- Parallel distribution succeeds in obfuscating the attack
- Commercial firewall has better results

Conclusion

- Study of security solutions commonly used
- Impact of distributed attacks on Cloud Computing
- 32 scanners are enough to remain undetected
- No network noise

Future work

- Multipath attacks
- Collaborative IDS using virtual and physical probes

Questions

Large-scale coordinated attacks: Impact on the cloud security





Damien Riquet - damien.riquet@lifl.fr

Gilles Grimaud - gilles.grimaud@lifl.fr

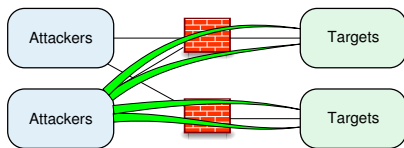
Michaël Hauspie - michael.hauspie@lifl.fr

<http://www.lifl.fr/~riquetd/>

References I

-  S. M Bellovin and W. R Cheswick, *Network firewalls*, IEEE Communications Magazine **32** (1994), no. 9, 50–57.
-  Min Gyung Kang, Juan Caballero, and Dawn Song, *Distributed evasive scan techniques and countermeasures*, Proceedings of the 4th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment (Berlin, Heidelberg), DIMVA '07, Springer-Verlag, 2007, p. 157–174.
-  Naga Raju Peddisetty, *State-of-the-art intrusion detection: Technology, challenges, and evaluation*, 2005.
-  R. Shirey, *RFC 2828 - Internet Security Glossary*, May 2000.

Multipath attacks



Collaborative security system

