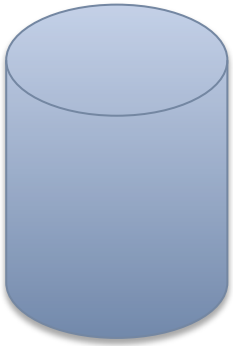
Carrier-Grade NAT and Source Port Logging

Dave O'Reilly, Chief Technologist, FTR Solutions

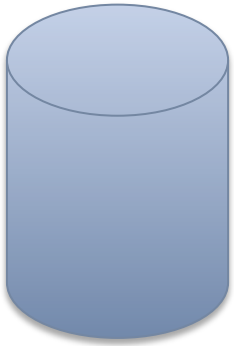
Europol workshop on Carrier-Grade NAT (CGN) and identification of cyber-attackers.

13th October 2017

The Problem



Victim/Service Provider Records



ISP/CGN Subscriber Database

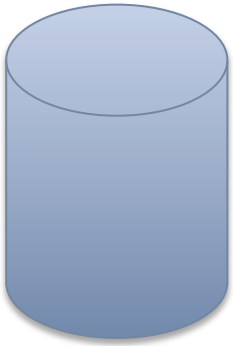
	Time	IP
Suspect →	1	W
	3	H
	3	I
	4	K
	5	M

Time	IP	Port	Subscriber
1	W	A	Bob
1	W	B	John
1	W	C	Liz
2	Y	D	Eric
2	Z	E	Joe

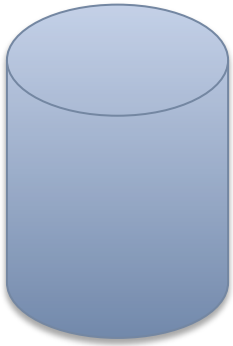
?

FTR solutions

The Solution (IPv6)



Victim/Service Provider Records



ISP/CGN Subscriber Database

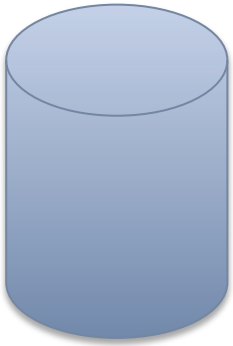
Suspect →

Time	IP
1	W::Z
3	H::L
3	I::M
4	K::R
5	M::S

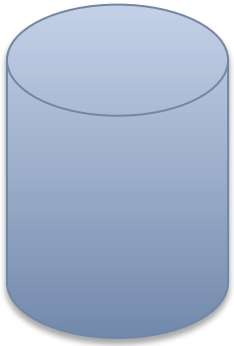
Time	IP	Subscriber
1	W::X	Bob
1	W::Z	John
1	W::H	Liz
2	Y::G	Eric
2	Z::T	Joe

FTR solutions

The Solution (Log Source Port)



Victim/Service Provider Records



ISP/CGN Subscriber Database

Suspect →

Time	IP	Port
1	W	B
3	H	9
3	I	8
4	K	7
5	M	6

Time	IP	Port	Subscriber
1	W	A	Bob
1	W	B	John
1	W	C	Liz
2	Y	D	Eric
2	Z	E	Joe

FTR solutions

Log Source Port: Challenges

Awareness

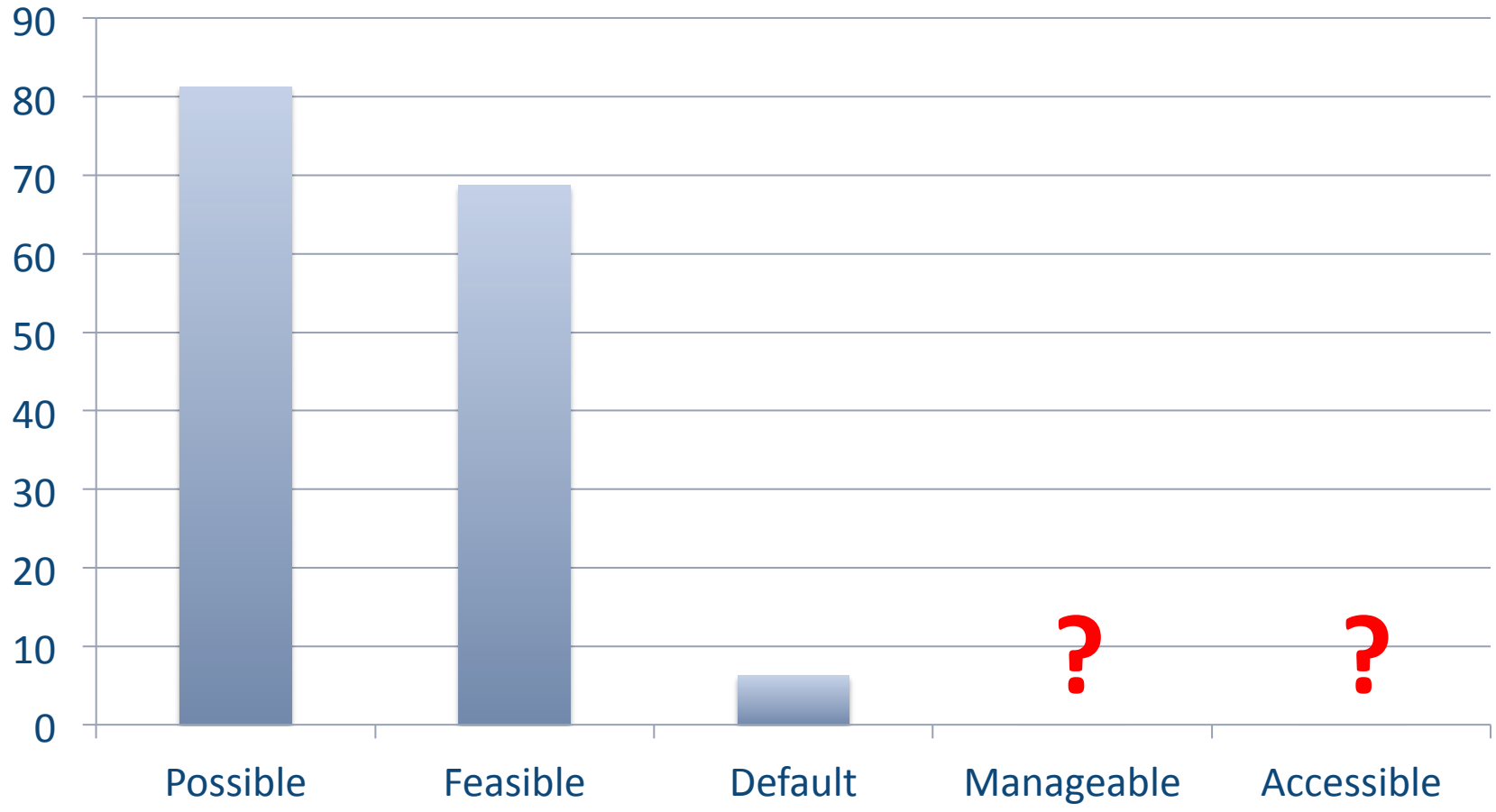
Software Support

Storage

Breaking Other Tooling

Time Accuracy

Software Support



Research Questions (Examples)

- Management:
  - What are the technical implications of logging source port for large enterprises?
  - What is involved in assessing and implementing downstream changes?
- Accessibility:
  - What would be involved in extracting timestamp, IP and source port information related to a particular connection?
  - What would be involved in querying for the activity related to a particular timestamp, IP and source port?

Further Reading

"Approaches to Address the Availability of Information in Criminal Investigations Involving Large-Scape IP Address Sharing Technologies."

https://tools.ietf.org/html/draft-daveor-cgn-logging-00

Thank You! Any Questions?

Dave O'Reilly
Chief Technologist
FTR Solutions

+353 (87) 231 3257
dave.oreilly@ftrsolutions.com