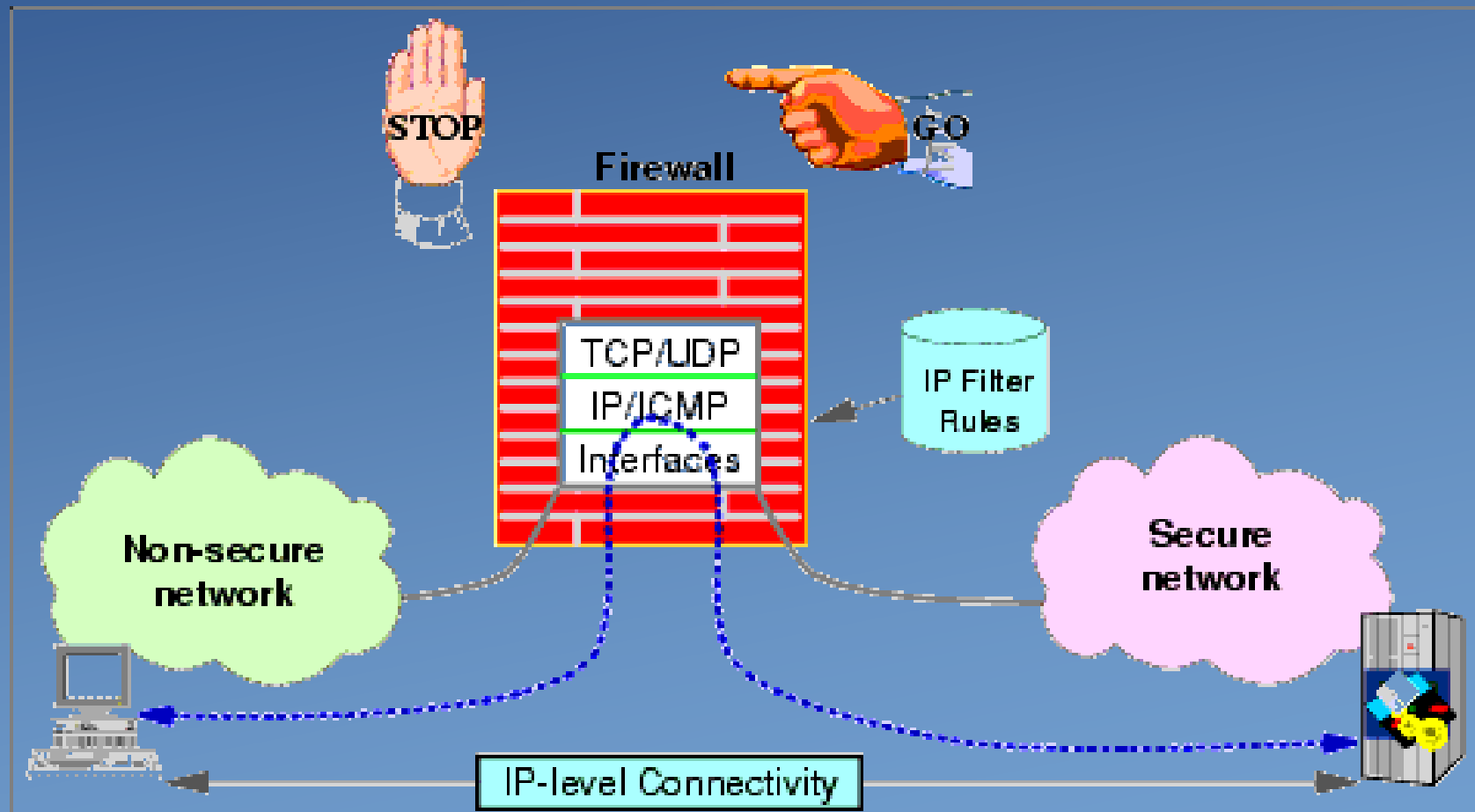


# Hacker Attack Log Analysis

Wigner Datacenter  
MTA Cloud

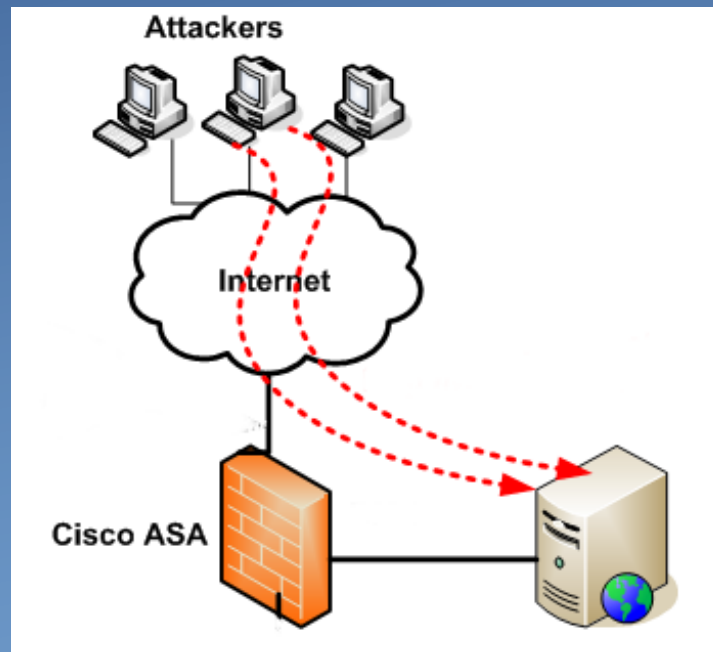
# Stateful Firewall

Keeps track of the state of network connections



# Blocked Traffic

Source Interface	Protocol	Source IP	Source Port	Dest. Interface	Dest. IP	Dest. Port	Action
Outside	TCP UDP ICMP	Public	Client Port	Inside	Private	Server Port	Deny
Inside	-	-	-	Outside	-	-	-





### Denied Outside Ip Count

a few seconds ago

# 291,390



### Attacked Port Count

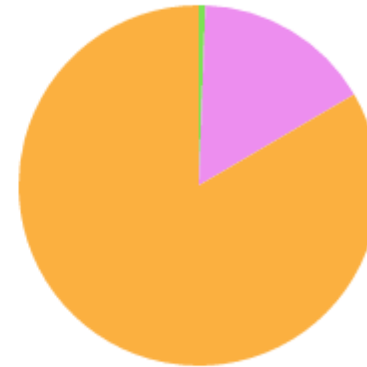
a few seconds ago

# 27,117



### Denied protocol count

a few seconds ago



Value	%	Count
Top values		
tcp	83.43%	22,599
udp	15.98%	4,328
icmp	0.60%	162



## Denied ports

a few seconds ago



Value	%	Count
Top values		
23	40.04%	116,647
5358	13.31%	38,774
7547	7.12%	20,729
5060	6.07%	17,677
22	3.40%	9,907
Others		
2323	3.13%	9,112
1900	2.54%	7,397
1433	1.49%	4,350
80	1.27%	3,714



## Denied Attacker IPs

a few seconds ago

Value	%	Count
Top values		
163.172.210.63	2.06%	5,988
91.223.133.8	1.29%	3,757
51.15.42.109	0.59%	1,728
176.63.67.179	0.58%	1,702
163.172.112.73	0.53%	1,536
Others		
195.3.145.218	0.46%	1,351
163.172.185.219	0.46%	1,343
183.60.48.25	0.42%	1,220
61.240.144.65	0.39%	1,140
89.163.242.107	0.33%	960
61.240.144.66	0.32%	929
80.82.70.26	0.26%	768
209.126.111.22	0.26%	768
37.61.218.45	0.26%	768
41.135.115.169	0.26%	768
221.229.204.202	0.26%	751
???	0.24%	702



## IP Address Geographical Location

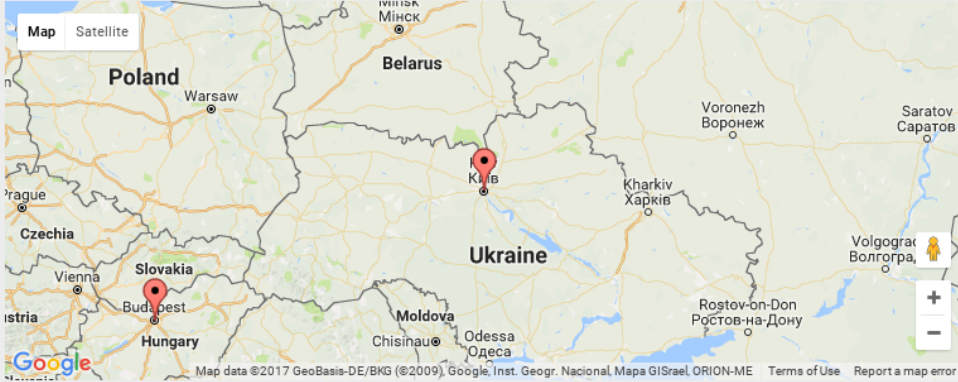
SHARE



91.223.133.8 (91.223.133.8)

Country : Ukraine (UA) Area Code : Unknown ISP : Uab  
City : Longitude : 30.523300  
State : Unknown Zip Code : Unknown Latitude : 50.450001  
Metro : Unknown

### On Map



91.223.133.8 Discover

## IP Address Geographical Location

SHARE



163.172.210.63 (163-172-210-63.rev.poneytelecom.eu)

Country : Netherlands (NL) Area Code : Unknown ISP : Online SAS N  
City : Amsterdam Longitude : 4.916700  
State : 07 Zip Code : 1091 Latitude : 52.349998  
Metro : Unknown

### On Map



163.172.210.63 Discover

## IP Address Geographical Location

SHARE



222.84.227.26 (222.84.227.26)

Country : China (CN) Area Code : Unknown ISP : China Telecom Guangxi  
City : Nanning Longitude : 108.316704  
State : 15 Zip Code : Unknown Latitude : 22.816700  
Metro : Unknown

### On Map



222.84.227.26 Discover

## IP Address Geographical Location

SHARE



195.3.145.218 (195.3.145.218)

Country : Latvia (LV) Area Code : Unknown ISP : RN Data SIA  
City : Longitude : 25.000000  
State : Unknown Zip Code : Unknown Latitude : 57.000000  
Metro : Unknown

### On Map



195.3.145.218 Discover

# Cloud Service Types



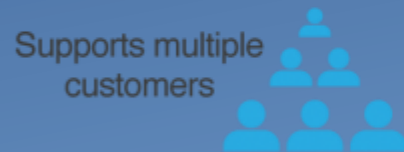
VS



Publically Shared  
Virtualised Resources



Privately Shared  
Virtualised Resources



Supports multiple  
customers

Cluster of dedicated  
customers



Supports connectivity  
over the internet



Connectivity over  
internet, fibre and private network



Suited for less  
confidential information



Suited for secured  
confidential information  
& core systems



## Incoming Traffic

Source Interface	Protocol	Source IP	Source Port	Dest. Interface	Dest. IP	Dest. Port	Action
Outside	TCP UDP ICMP	Public	Client Port	Inside	Private	Server Port	Permit / Deny
Inside	TCP UDP ICMP	Private	Server Port	Outside	Public	Client Port	Permit / Deny

## Outgoing Traffic

Source Interface	Protocol	Source IP	Source Port	Dest. Interface	Dest. IP	Dest. Port	Action
Outside	TCP UDP ICMP	Public	Client Port	Inside	Private	Server Port	Permit / Deny
Inside	TCP UDP ICMP	Private	Server Port	Outside	Public	Client Port	Permit / Deny