RSA CONFERENCE ASIA PACIFIC 2013

THE TRUE COST OF SECURITY – THE IMPACT TO END USER QoS IN A MOBILE WORLD

Ankur Chadda
Product Manager – Application and Security
SPIRENT COMMUNICATIONS

Session ID: SPO-W04

Session Classification: Intermediate

"…Project management did not recognize the value of or need for independent tests…"

Nov 1990 – NASA The Hubble Space Telescope Optical Systems Failure Report

RFC 2889

RFC 5180

RFC 1242

RFC 4814

RFC 3511

RFC 2285

RFC 4689

RFC 2647

RFC 2432

RFC 3918

RFC 2544

High Scale Performance Testing

- Test for flood of new users joining
  - Multi-million conn/sec.
- High rate data transfer
  - Hundreds of Gbps of statefull line-rate bandwidth
- Concurrent users-sessions
  - 100s of million open connections
- Thousands of Apps
- Custom App Flows

Firewalls are getting bigger with Terabit ready platforms available in the market.

Consolidated services make it critical to support higher user loads

Advanced Security Testing

- Mix of Applications with DDoS attacks
  - ARPFlood, PingOfDeath, TearDrop, TCPPortScan, ResetFlood, Smurf, SynFlood, UDPPortScan, XMasTree,…
- Stateful & Stateless Attacks with evasion
  - Fragmentation, Re-ordering, Overlapping frags.
- One armed and two armed attacks
- Custom attacks with DDoS

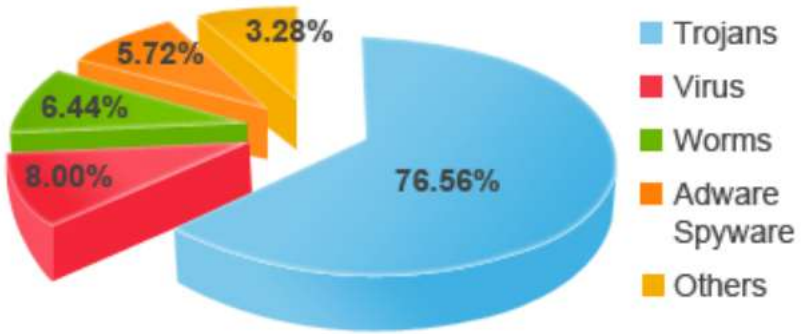
DDoS attacks even though well known are still commonly used to cause disruption

There have been documented 100G+ DDoS attacks

Malware Testing

- Infected host emulation
- Binary transfer emulation
- Malware testing under load
- Continuously updating database

MALWARE INFECTIONS BY TYPE IN 2012



There are 60,000 pieces of new malware discovered daily

Source: PandaLabs Annual Report for 2012 by Panda Security

Application Aware Testing

- Thousands of Apps
- Apps with different versions
- Multiple OSes – PC, iOS, Android, …
- Application behavior
- Custom application
- Application policy testing
- App server testing

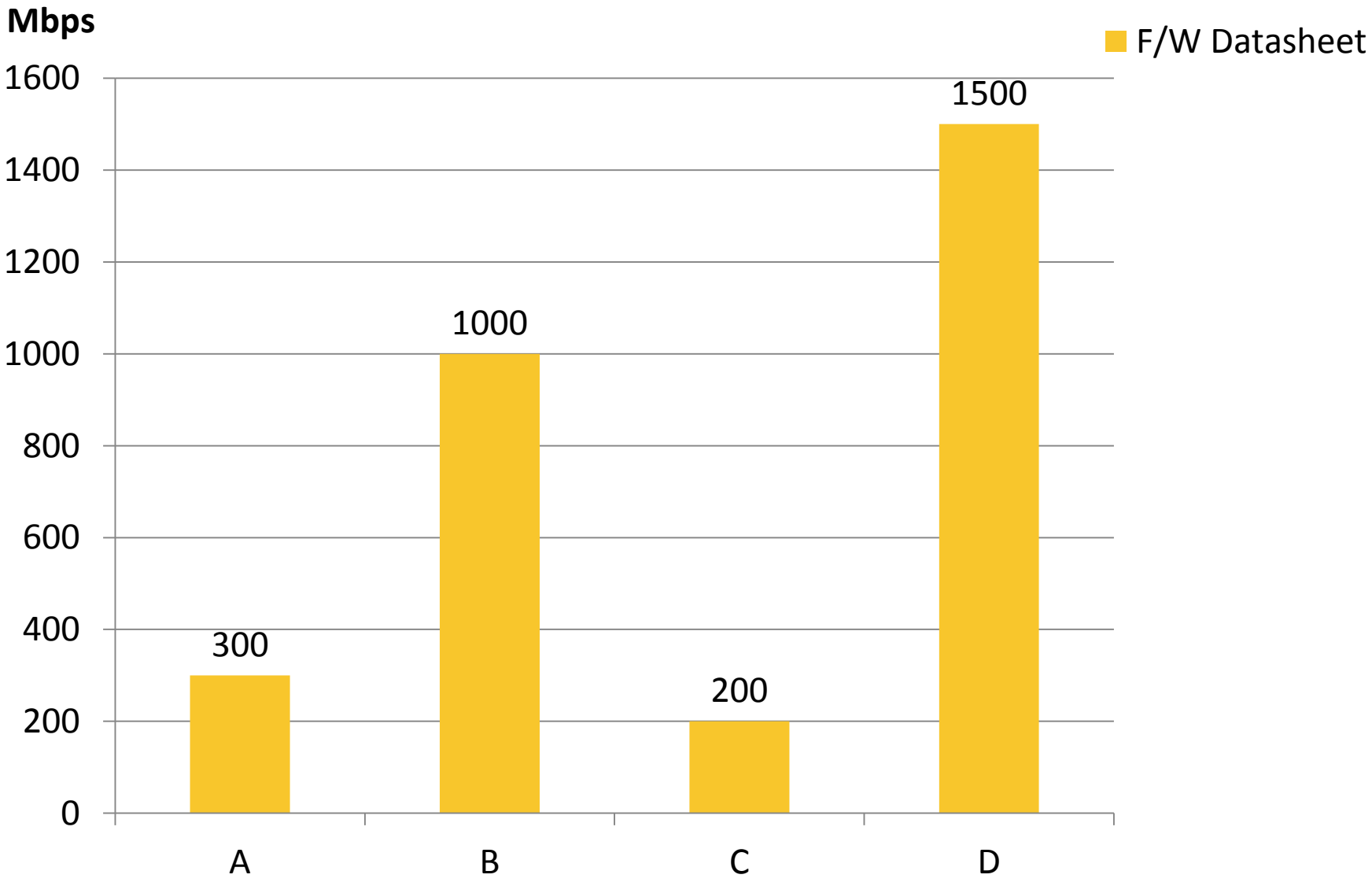
Measuring the True Cost…

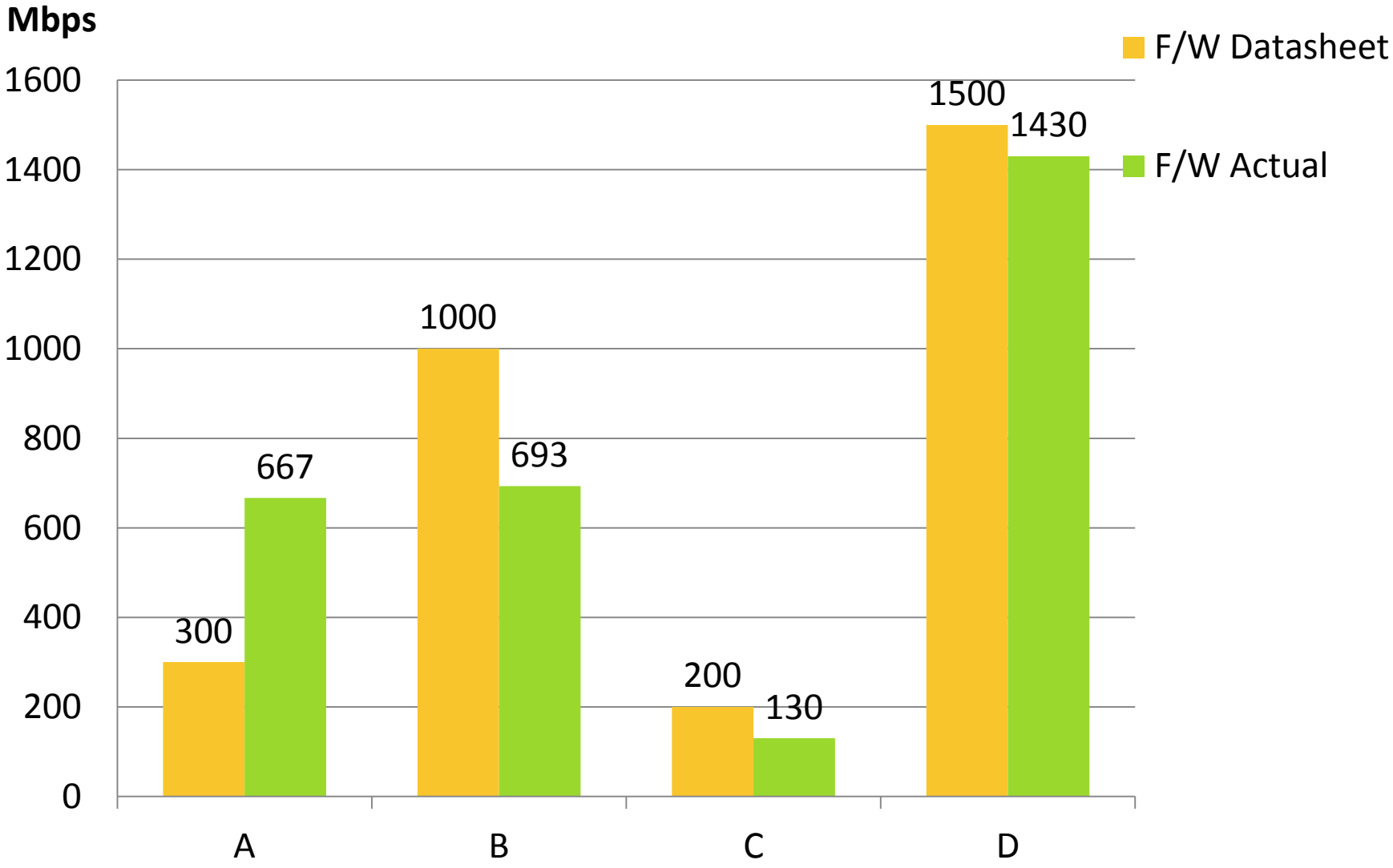
- Massive Performance
  - More connections per user
  - More internet connected devices
  - Higher data transfers
- Security Attacks
  - Malware, DDoS
  - Fuzzing
  - Authentication, SSL & IPSec
- Thousands of Applications
  - Many new apps released daily
  - For many endpoint devices
  - Unique impact on the network

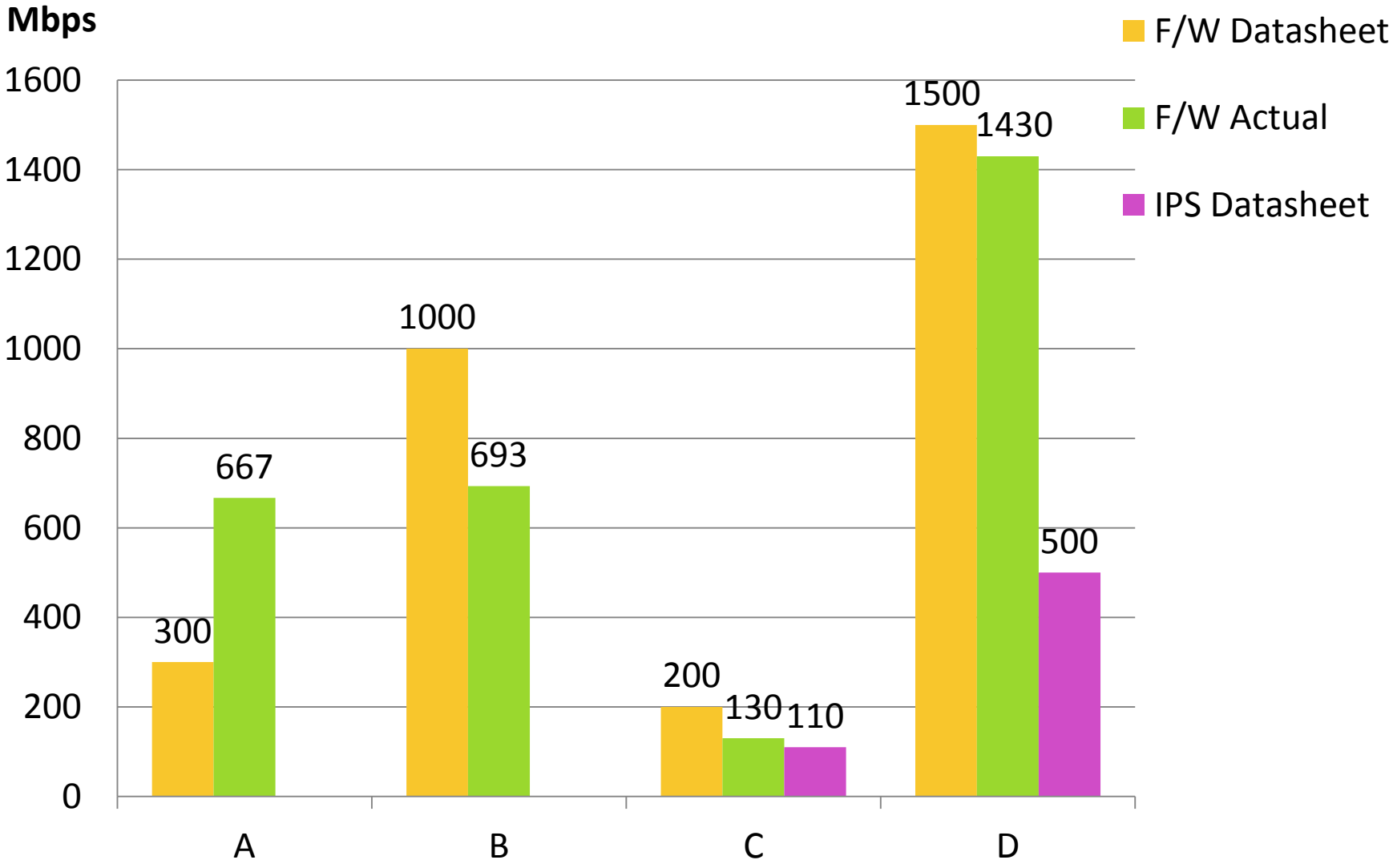
DATASHEET CLAIMS

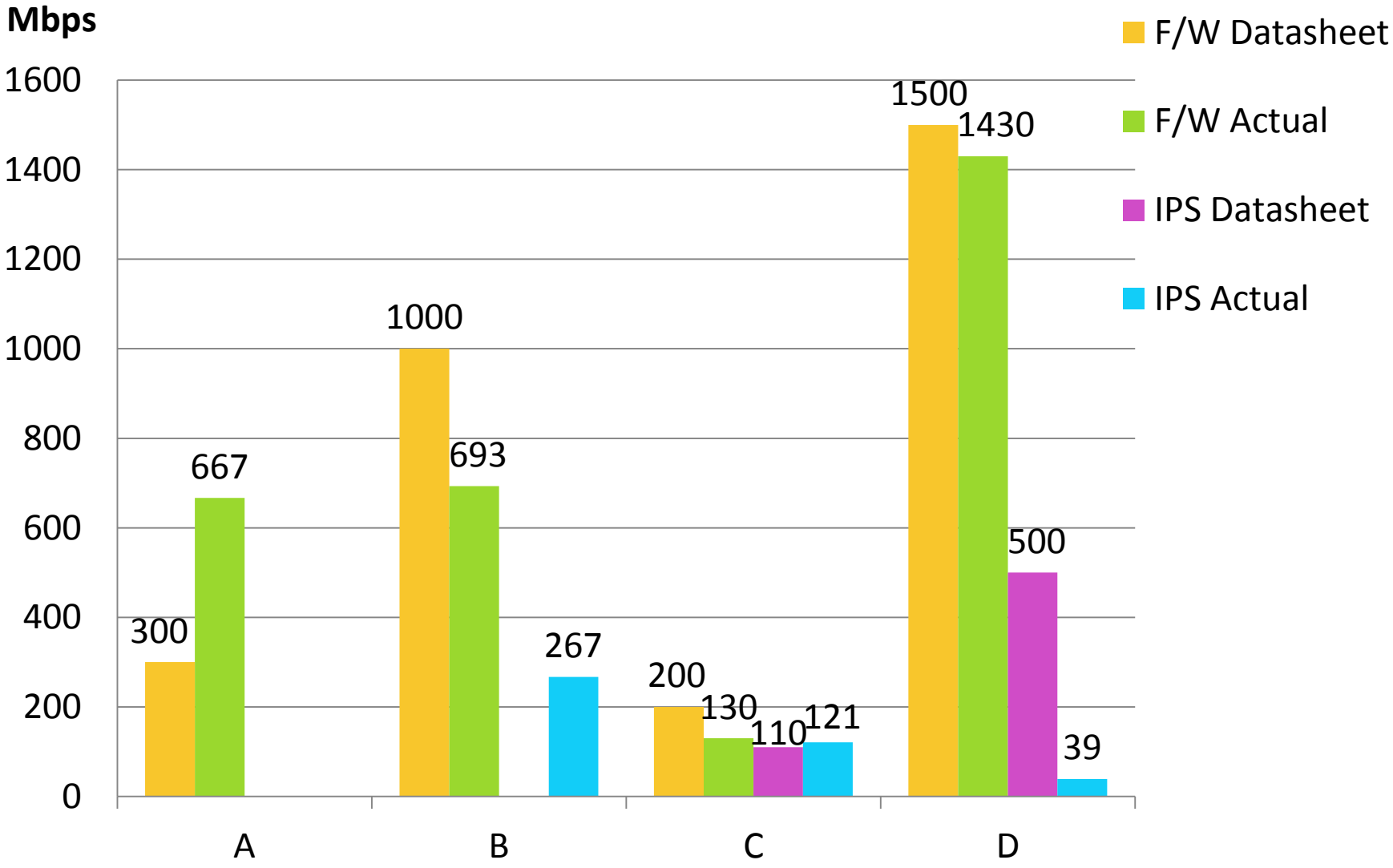
REAL WORLD TESTING

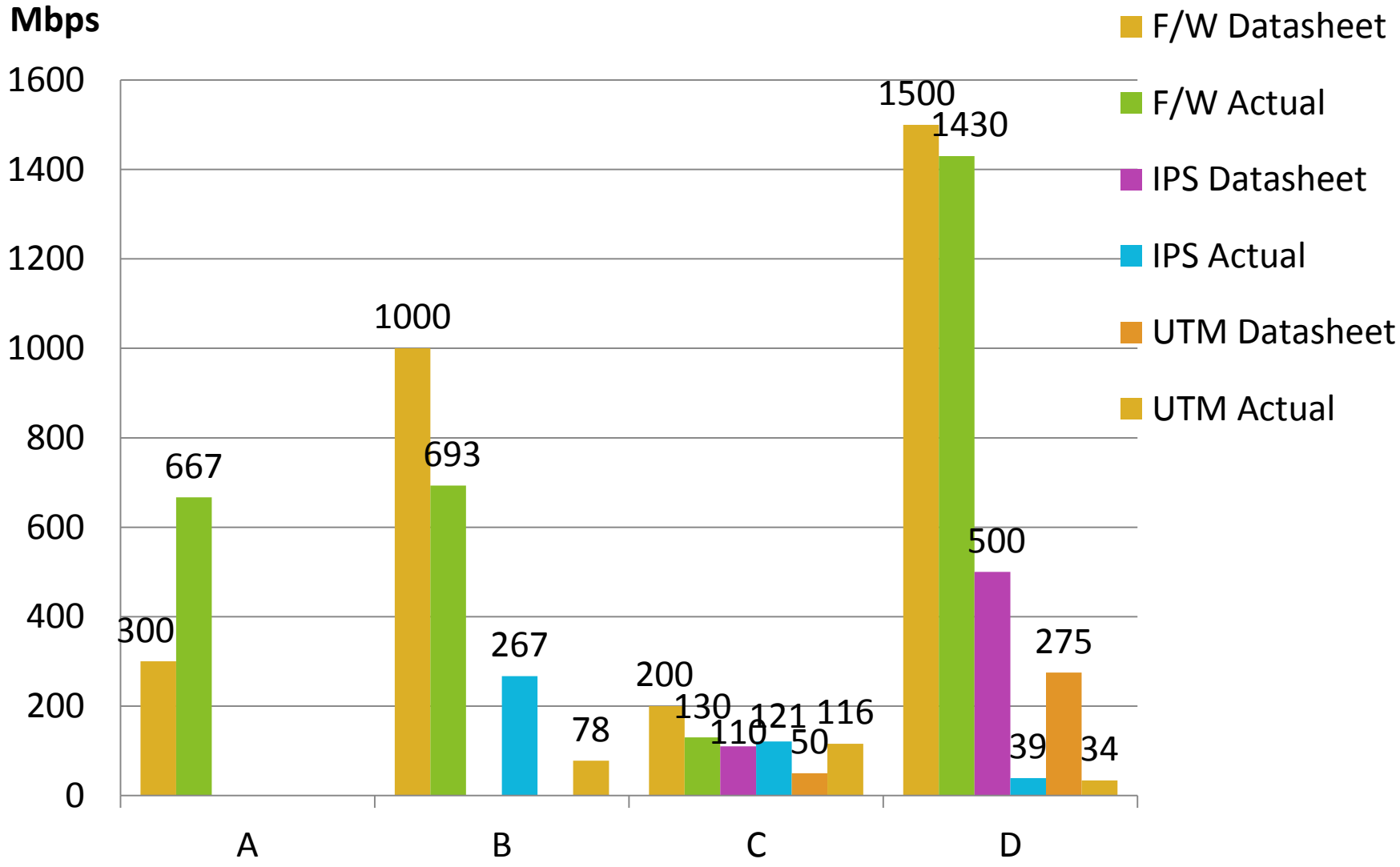
Vendor A	Vendor B	Vendor C	Vendor D
			
300 Mbps	1 Gbps	200 Mbps	1.5 Gbps


Mbps
F/W Datasheet
1600
1400
1200
1000
800
600
400
200
0
300
1000
200
1500
A
B
C
D


Mbps
F/W Datasheet
F/W Actual
1600
1400
1200
1000
800
600
400
200
0
300
667
1000
693
200
130
1500
1430
A
B
C
D


Mbps
1600
1400
1200
1000
800
600
400
200
0
F/W Datasheet
F/W Actual
IPS Datasheet
300
667
1000
693
200
130
110
1500
1430
500
A
B
C
D


Mbps
1600
1400
1200
1000
800
600
400
200
0
A
B
C
D
300
667
1000
693
267
200
130
110
121
1500
1430
500
39
F/W Datasheet
F/W Actual
IPS Datasheet
IPS Actual


Mbps
1600
1400
1200
1000
800
600
400
200
0
F/W Datasheet
F/W Actual
IPS Datasheet
IPS Actual
UTM Datasheet
UTM Actual
300
667
1000
693
267
78
200
130
110
121
50
116
1500
1430
500
39
275
34
A
B
C
D

Summary

- Security infrastructure testing is no longer legacy firewall testing, but more involved with multiple vectors
- BYOD adds complexity with number of devices, endpoints and versions of apps on your network
- Realistic emulation critical understand actual impact
- Datasheets do NOT give you the true picture and cost of security

RSA CONFERENCE ASIA PACIFIC 2013

THANK YOU

Ankur Chadda

ankur.chadda@spirent.com

TESTED WITH SPIRENT