

Dell SonicWALL Next-Gen Firewalls:

What the competitors aren't saying

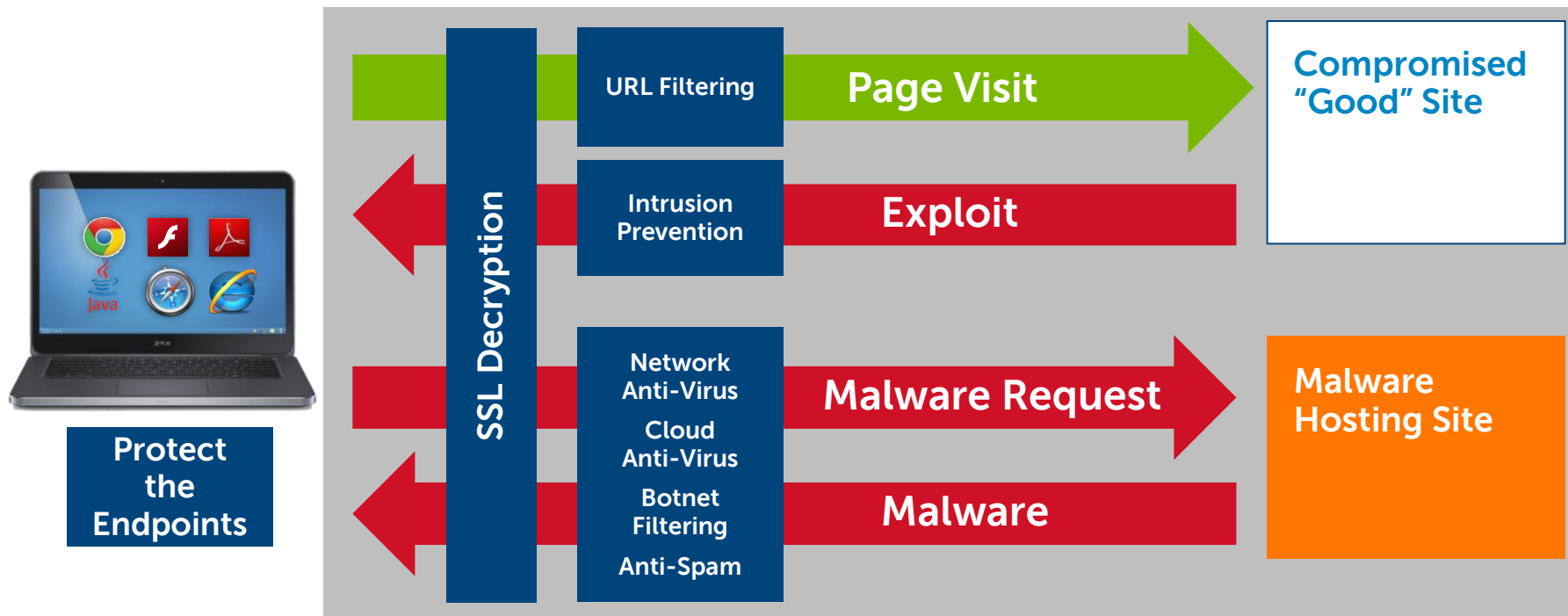
Mini Peak – Portugal

Hotel Palacio do Estoril

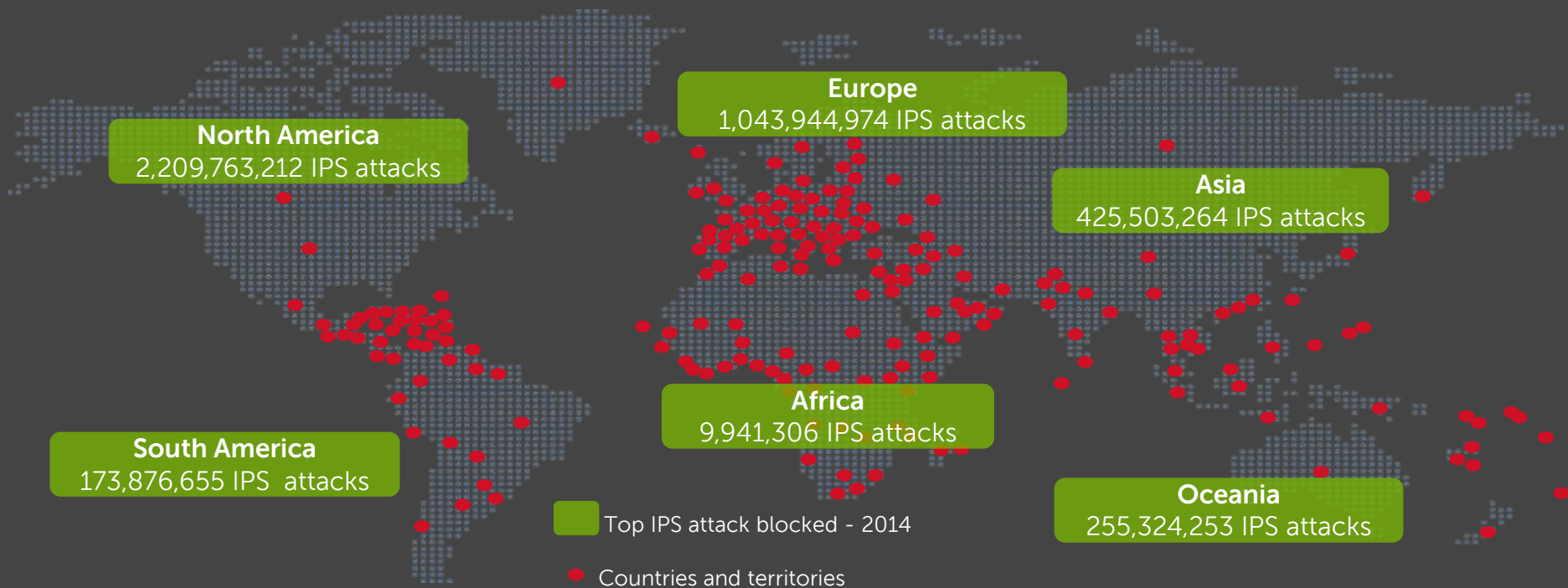
12 de Novembro 2015 – 16h30



Next Generation Firewall (NGFW)



Global Response Intelligent Defense (GRID) Network



1.0M+
Sensors

200+
Countries and
territories

**24x7
x365**

< 24 Hr.
response to 0-day
vulnerabilities

100K+
Malware samples
collected daily

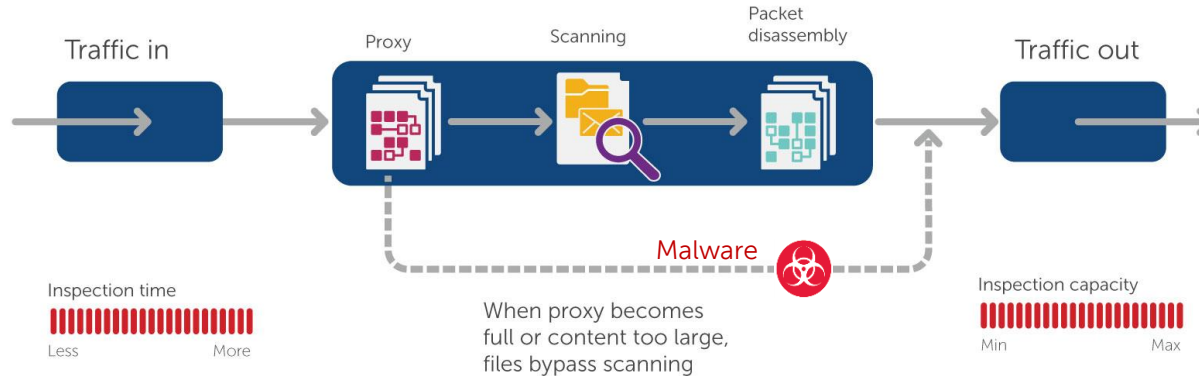
100K+
Malicious event
analyzed daily

Reassembly-Free Deep Packet Inspection® (RFDPI) versus Packet assembly-based architecture

Dell SonicWALL architecture

Packet assembly-based process

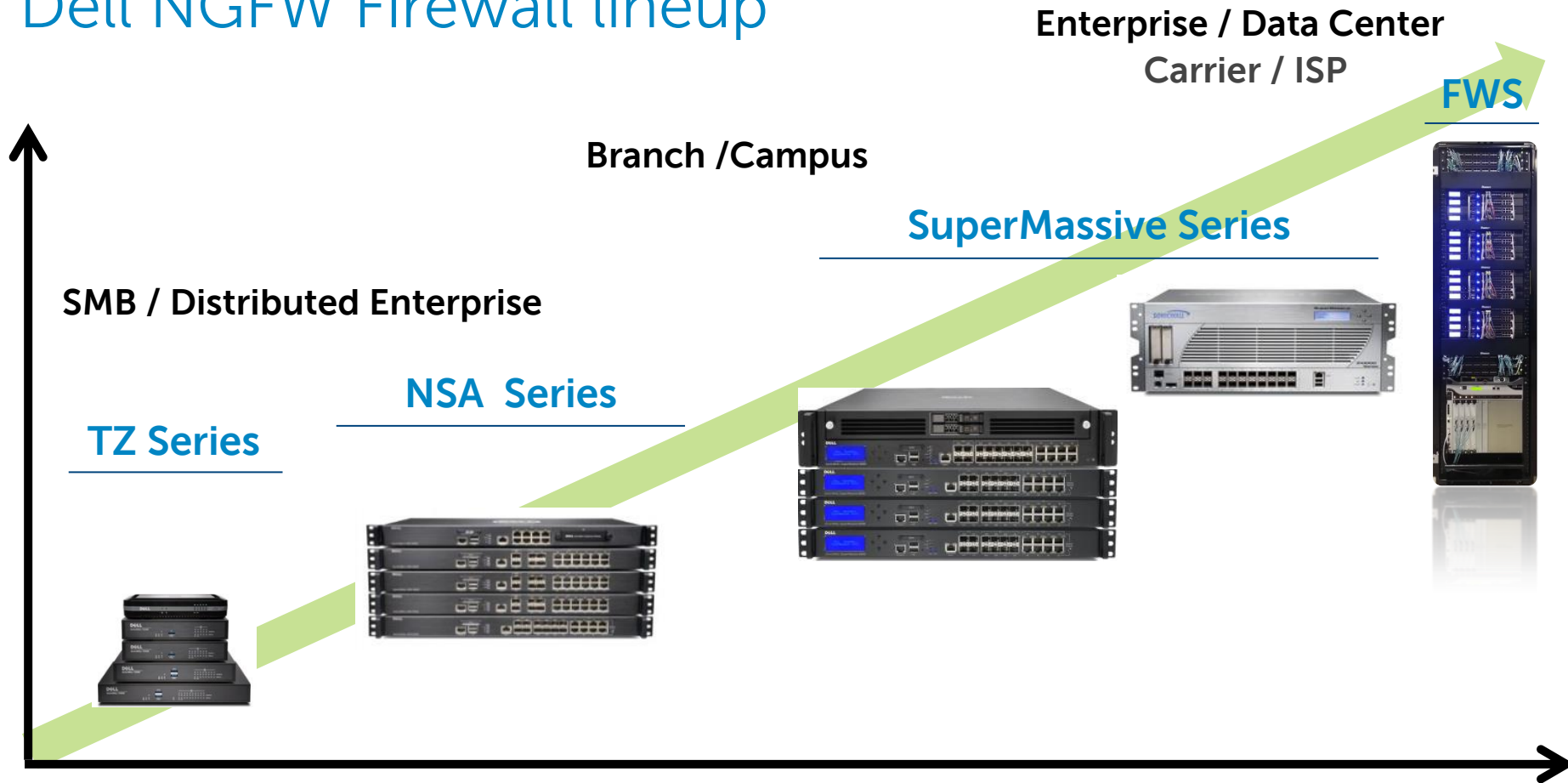
Competitive architecture



When proxy becomes full or content too large, files bypass scanning

Reassembly-free packet scanning without proxy or content size limitations

Dell NGFW Firewall lineup



Third party view of Dell SonicWALL

Gartner Magic Quadrant

- Unified Threat Management - Challenger
- Enterprise Network Firewall - Niche

Network World Firewall Challenge

- Dell SonicWALL made the Cover of Network World as the Winner
- Best Overall Performance for NGFW
- Best Overall Performance for UTM
- Best Overall Performance for SSL Decryption

NSS Labs Security Value Maps

- Next-Generation Firewall Recommended (3 years in a row)
- Intrusion Prevention System Recommended (3 years in a row)

ICSA Labs

- Enterprise Firewall Certification
- Next-Generation Firewall
- AV Certified



Understanding firewall performance



Firewall	Stateful (RFC 2544)	6 Gbps
Intrusion Prevention	Stateful + IPS	2 Gbps
Anti-Malware	Stateful + AV	1.1 Gbps
UTM or Full DPI	Stateful + AV + IPS	800 Mbps
SSL Decryption	Stateful + AV + IPS + SSL	500 Mbps
<hr/>		
IMIX (Internet Mix)	Stateful	1.6 Gbps



Palo Alto Networks

Inferior portfolio breadth (non-existent low end)

Usability over security

Limited scalability and resilience

Expensive



Dell NGFW Firewall lineup

Enterprise / Data Center
Carrier / ISP

FWS

Palo Alto Networks Portfolio

SMB / Distributed Enterprise

TZ Series



Nonexistent SOHO, SMB & distributed enterprise offering

- No integrated or AP wireless
- Slow & Expensive
- No 4G Failover
- No DDNS
- No Anti-Spam
- No WAN Acceleration



High-End

- Weak scalability (Conn/sec)
- 7050 Chassis less scalable and economical than the FWS Architecture
- Extremely expensive HA licensing
- Unstable central management



PAN DSRI - *Disable Server Response Inspection*

PERFORMANCE AND CAPACITIES¹

PA-7050 SYSTEM

Firewall throughput (App-ID enabled)

120 Gbps

Threat prevention throughput (DSRI Enabled²)

100 Gbps

Schedule None

QoS Marking None

☒ Disable Server Response Inspection

OK

Cancel

order to identify the

<https://www.dell.com/docs/DOC-5996>

PAN SSL Decryption "Shortcuts"

On SSL Decryption failure, do not decrypt for 12 hours

Decryption

SSL Failure

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted.

☐ Block sessions with expired certificate

☐ Block sessions with untrusted issuers

☐ Restrict certificate extensions [Details](#)

Unsupported Mode Checks

☐ Block sessions with unsupported version

☐ Block sessions with unsupported cipher suites

☐ Block sessions with client authentication

Failure Checks

☐ Block sessions if resources not available

Note: For unsupported modes and failures, the session information is cached for 12 hours, so future sessions between the same host and server pair are not decrypted. Checkboxes to block those sessions instead.

#	Name	Application
1	kdc.uas.aol.com	aim
2	bos.oscar.aol.com	aim
3	*.agnilindenlab.com	second-life
4	*.vedivi.com	wallcooler-vpn
5	update.microsoft.com	ms-update
6	www.update.microsoft.com	ms-update
7	activation.sls.microsoft.com	ms-product-activation
8	Yuuguu.com	yuuguu
9	yuuguu.com	yuuguu
10	*.PacketIX VPN	packetix-vpn
11	*.SoftEther VPN	packetix-vpn
12	*.softether.com	packetix-vpn
13	*.tpnccs.simplifymedia.net	simplify
14	tpnxmpp.simplifymedia.net	simplify
15	*.table14.fr	winamax
16	*.mozilla.org	firefox-update
17	lr.live.net	live-mesh
18	anywhere2.telus.com	call anywhere
19	accounts.mesh.com	live-mesh
20	storage.mesh.com	live-mesh
21	*.sharpcast.com	sugarsync
22	auth2.triongames.com	rft
23	*.zumodrive.com	zumodrive

Hidden DB of 58+ ignored applications



Palo Alto Networks High Availability TCO

Dell: 1 license
shared by HA cluster

PAN: 1 license per
firewall in HA cluster



Fortinet

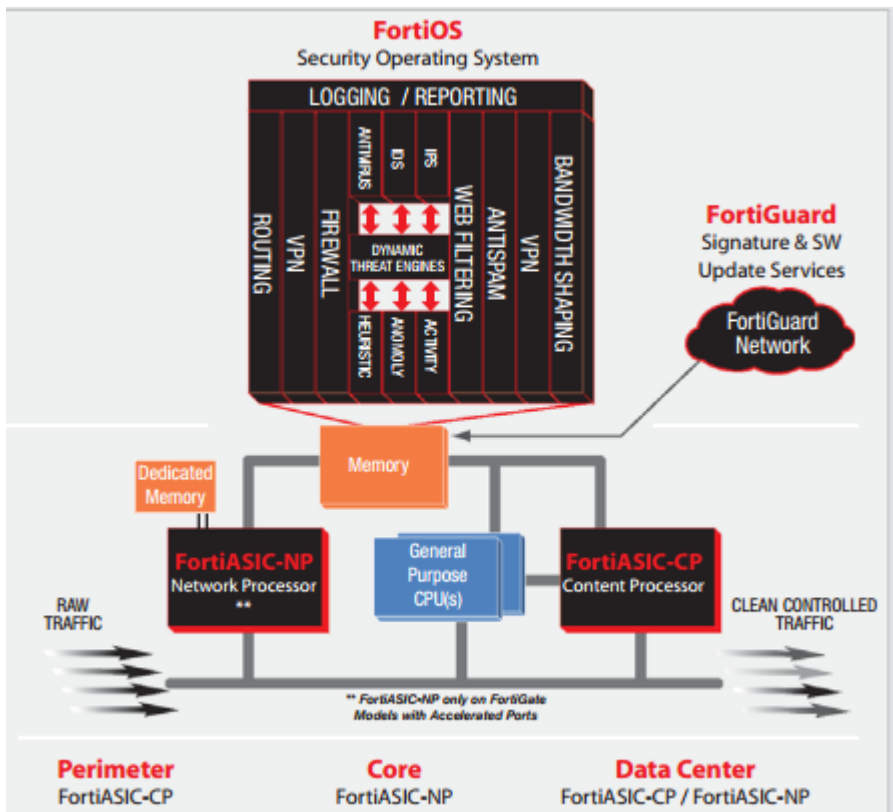
Optimized for Stateful Inspection

Fragile DPI engine

Terrible DPI performance



What Fortinet won't tell you



FortiASIC-NP (CORE)

Network Processor

Stateful, NAT, IPS, QOS, DoS



FortiASIC-CP (Perimeter)

Content Processor

AV, Content/File Inspection=DP

X86

X86 CPU

Mgmt/Routing, ALG, SPI/DPI Spill over



-95%



FortiGate 3700D
160 Gbps down to
7.5Gbps

~3.7Gbps in real world
(ask NSS Labs)



Different Inspection Methods

Proxy

The more
proced

proxy buffers the file as it arrives, then

Proxy

Flow

- More Secure
- **File Size limit**
- Prone to DoS
- Security vs. Access

- Faster
- Less secure
- Not true stream inspection

FORTINET.

FortiOS Handbook
Security Profiles for FortiOS 5.2



An abstract graphic in the top right corner consisting of several overlapping, translucent green and yellow-green triangles and polygons, creating a dynamic, geometric shape.

It's 2015, why are we
still talking about
file size limits?



Because file size limits continue to exist!

Proxy “Benefits”

FORTINET.

During the buffering and scanning procedure, the client must wait. With a default configuration, the file is released to the client only after it is scanned. You can enable client comforting in the Proxy Options profile to feed the client a trickle of data to prevent them from thinking the

IS Handbook
FortiOS 5.2

Since the FortiGate unit has a limited amount of memory, files larger than a certain size do not fit within the memory buffer. The default buffer size is 10 MB. You can use the `uncompresslimit` CLI command to set the buffer size. Files larger than the buffer are passed to the destination without scanning. You can use the

Therefore a threshold must be set to prevent the resources of the system from becoming overloaded. By default the threshold is 10 MB. Any files larger than the threshold will not be scanned for malware. With a maximum file size threshold in place, it must now be determined what is to be done with the files that are larger than threshold. There are only 2 choices; either

Coming up ... file size limit bonus: “Conserve mode”



Different AV Database size

DEFAULT



Normal	Incl Sec dat
Extended	Incl acti sinc
Extreme	Incl The tod long



Not
Supported on
all models

"The additional cost"

Takeaways

In PoC against Fortinet, check

- 1) Which database is used
- 2) Inspection method (Proxy of Flow)
- 3) Push to test "Extreme" and "Proxy"

Fortinet “Conserve Mode”

Critical infrastructure should
not be unpredictable!

"Conserve Mode" – Fortigate survival mode

Conserve mode

FortiGate units perform all Security Profiles processing in physical RAM. Since each model has a limited amount of memory, conserve mode is activated when the remaining free memory is nearly exhausted or the AV proxy has reached the maximum number of sessions it can service.

amount of memory. Conserve mode is designed to prevent all the component features of the FortiGate unit from trying to use more memory than it has. Because the AV proxy uses so much memory, conserve mode effectively disables it in most circumstances. As a result, the content inspection features that use the AV proxy are also disabled in conserve mode.

Summary

When running out of memory,
reject new connections (DoS!!)

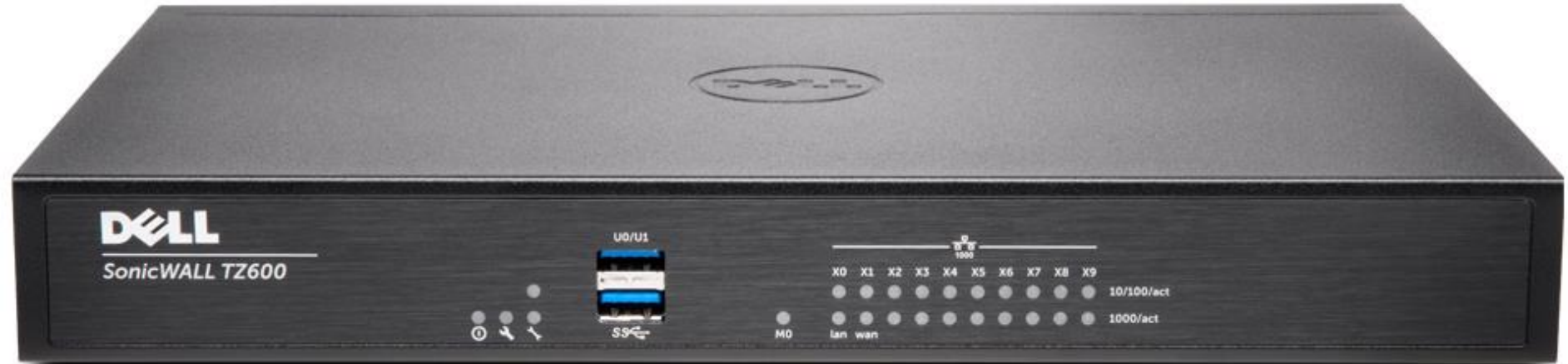
FortiGate 1500D



\$30,000 FW
\$50,000 UTM

80 Gbps Firewall
4.3 Gbps UTM/Full DPI (5%)
12,000,000 Connections

What are the chances that you'll run into the limit?



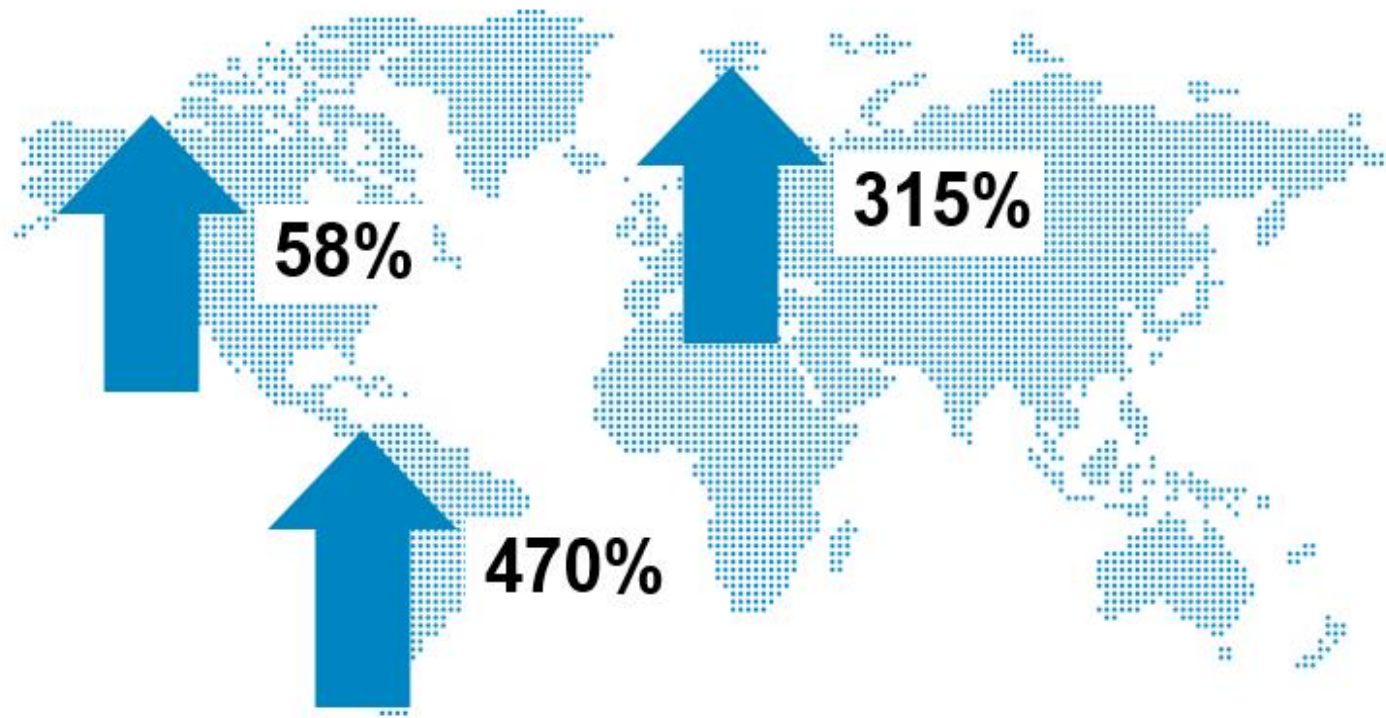
Hiding your blemishes – CLI Migration in FortiOS 5.2

Much advanced configuration has been moved to the CLI

- Choosing between Normal, Extended and Extreme Databases
 - All come with Normal by default, *only **some*** models offer Extended and Extreme
 - Comes at a cost, resource extensive when selecting anything other than normal
- Enabling the GrayWare database
- Enabling Heuristics scanning
- Oversized files much configured on per protocol basis
- Archive Scan depth
- Scan Buffer size
- Conserve mode (off, pass, one-shot, idledrop)
- Client Comfort



"Snowden" effect – SSL traffic use increase (2014 vs 2013)



-95%

Again



FG200D – 3Gbps Firewall SSL Inspection?

MAX TC			
Mu Dynamics PVA catch rate		96.77%	Not stated
		Units (Mbps)	Units (Mbps)
IPS Throughputs (Proxy)		337	Not stated
IPS Throughputs (Flow)		526	1700
AV Throughputs (Proxy)		333	600
AV Throughputs (Flow)		665	
DPI SSL with Max Sec		152	
IMIX (Mixed UDP Packet Sizes)		1769	
	Packet Size (Bytes)		
UDP Throughput	64	1555	3000
	512	1925	3000
	1518	1974	3000

152 Mbps!

Cisco

Inconsistent product line

Multiple management consoles

Slow and expensive (very slow, very expensive)

Inconsistent product line

Low-End

ASA-X 5506
ASA-X 5508
ASA-X 5512
ASA-X 5516



Mid-Range

ASA-X 5515
ASA-X 5525
ASA-X 5545
ASA-X 5555



High End

ASA-X 5585
(SSP-10, SSP-20,
SSP 40, SSP-60)



**NEW – Barely shipping
(2 month backlog)**

FirePOWER Saving Cisco Security?



Low-End

ASA-X 5506
ASA-X 5508
ASA-X 5512
ASA-X 5516



Mid-Range

ASA-X 5515
ASA-X 5525
ASA-X 5545
ASA-X 5555



SSD
Upgrade

High End

ASA-X 5585
(SSP-10, SSP-20,
SSP 40, SSP-60)



Modules

Centralized Management: Two Management Consoles
ASDM and FireSight

HA Cluster: Two FireSight licenses required

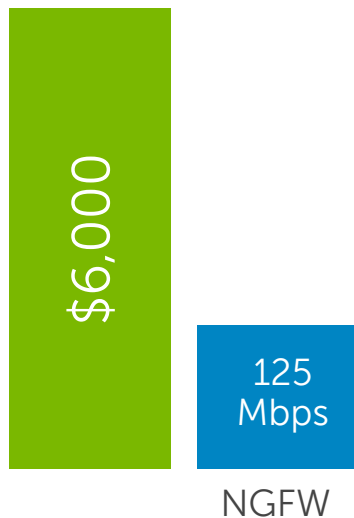
Single Firewall: Two management consoles

Cost & Performance – 3 Year fully loaded NGFW



ASA-X 5506

TZ400



7X

1/3rd

2.4X

300
Mbps

150
Mbps

NGFW

NGFW

DPI SSL



Dell's Security Strategy

Network

Deep protection and control without impacting network performance

- Next Gen Firewall
- Secure Mobile Access
- Email Security

Dell SonicWALL

User

Identity and access mgmt for the real world

- Identity Governance
- Privileged Management
- Access Management
- Compliance and IT Governance

Dell One Identity Solutions

Data and endpoints

Protect data wherever it goes

- Encryption
- Configuration and Patch Management
- Secure Cloud Client
- Protected Workspace

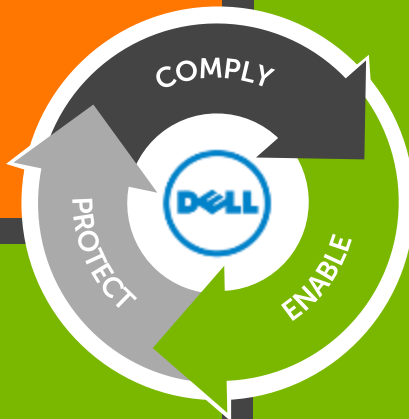
DDPE (Credant), Dell KACE

Services

Protect, predict and respond to threats

- Incident Response
- Managed Security Services
- Security and Risk consultation
- Threat Intelligence

Dell SecureWorks



Our approach allows customers to align security strategy to business needs.

Q&A

