Palo Alto Networks vs Fortinet

Fortinet Weaknesses

1. Fortinet Is Perceived As An SMB UTM Player

- UTM: Stateful Firewall + Add-on modules
- Integration between their firewall and add-on modules is weak

2. The FortiGate Firewall Performance Degrades As You Enable Features (AV, IPS, etc.)

- Fortinet Multi-pass UTM Architecture
- As you turn on more UTM features the performance degrades: Stateful Firewall vs App-Control vs Antivirus

3. Fortinet’s Multiple Log Files Complicate Troubleshooting

- Finding actionable information in the logs is difficult, making it harder for remediation
- Limited reporting on-box (some small branch boxes do not have on-box reporting - some boxes lack hard drives)
- Customizing off-box reporting is difficult (users require programming skills such as SQL)

4. The Firewall, Manager and Logging Interfaces Vary and Are Not as User Friendly As Palo Alto Networks

- Fortinet acknowledges that Palo Alto Networks has a better interface.
- They are trying to mimic our interface with each new release and succeeding poorly.
- FortiManager is different from the firewall and cumbersome to administer.

5. They Have Had Quality Control Problems in Their Major Software Releases

- FortiOS past releases were plagued by code stability issues
- Partner SEs reported Beta release code that stopped forwarding packets during testing
- There were many customer complaints that technical support was inefficient resolving code problems

Fortinet Strengths

1.They Offer Lower Cost Products

- It ties into the fact that smaller boxes that are as cheap as ~$500 (SOHO or Small branch devices)
- They attack us on the subscription – each subscription is 20% of our hardware cost while they give the customer bundled pricing
- They try to leverage the fact that the customer can turn on any feature at any time without having to get additional subscriptions (sold in bundles)

2.Their Products Have Fast Stateful Firewalling by Using Dedicated ASIC Chips

Typically they use two different chips in most platforms – dedicated resource chips (ASIC chips) to improve the performance for FW vs IPS:

- FortiASIC-NP (Network processor) to accelerate the firewall and VPN functions of the FortiGate range of multi-threat security platforms
- FortiASIC-CP (Content processor) provides IPsec VPN acceleration and implements the Content Processing Recognition Language (CPRL) that can be used to accelerate pattern matching and other computationally-intensive tasks

3.They Sell Bolt-On Products to Complement Their Core Firewall Offering

- Fortinet products scale from small to large business with nearly 30 different products within and outside of the security market
- Licensing is per-box basis for its hardware rather than per-user

4.They Have Many Hardware Models, Variations of Price, Performance, and Types of Interfaces

- Higher speed interfaces options; 40/100G
- Small branch boxes (low end ~$500)

Fortinet Marketing & Positioning

1.Fortinet Tries to Paint Next Generation Firewall Functionality As Just Another UTM Module

2.They will point to a wide range of third party validations and claim more effective security

3.They Will Say They Are Faster and Less Expensive

- Bundled pricing
- Less expensive hardware used

4. They Claim Fortinet Is Focused On Engineering and Palo Alto Networks Is Only Focused On Marketing

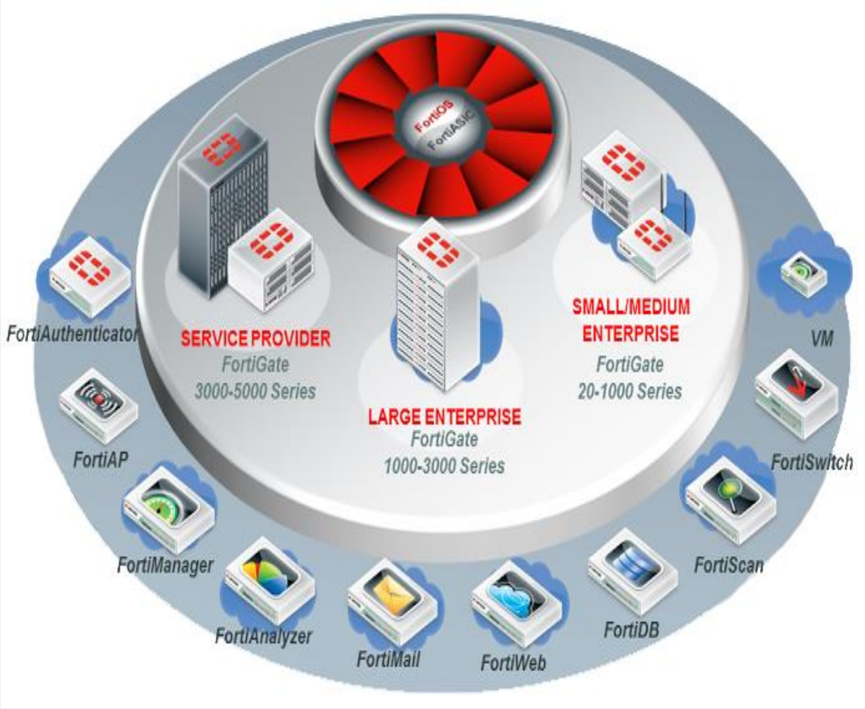
- They claim that have 250+ engineers in their research team

5.They Have Developed an ‘AVR like’ Report to Appear More Like Palo Alto Networks

- Fortinet avoids TAP mode because of poor performance

Core products competing against Palo Alto Networks

FortiGate	UTM – Firewall – AV – IPS – URL Filtering – APP
FortiManager	Centralized Management
FortiAnalyzer	Centralized logging for all their products



Palo Alto Networks vs Fortinet

Objection Handling

“Fortinet has more application signatures than Palo Alto Networks”

- Palo Alto Networks is focused primarily on enterprise business applications for policy enforcement
- Fortinet has padded their list with thousands of small irrelevant variations targeted for SOHO deployments
- Palo Alto Networks also has the ability to create custom application signatures

“Fortinet will claim that Palo Alto Networks enables Disable Server Response Inspection (DSRI) by default endangering customers by only inspecting half of the traffic for threats. They will also claim that our Data Sheet performance numbers are inflated as a result of enabling DSRI”

- This is absolutely FALSE. DSRI is disabled in our policy rules by default and it is NOT enabled for Data Sheet calculation.
- Palo Alto Networks would only recommend using DSRI in networks with trusted servers where performance is critical. This is not a system default.

“My Fortinet Firewall can do that”

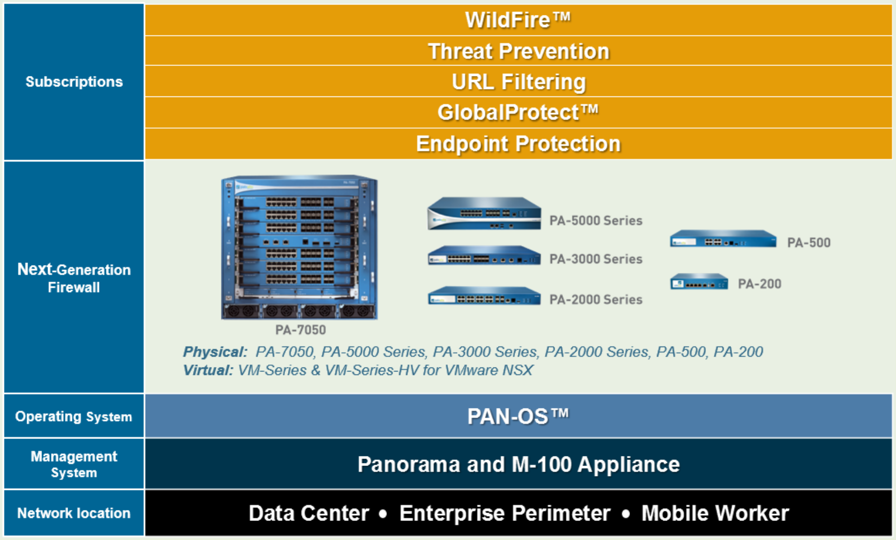
Port-based firewalls attempt to address application control with add-on, IPS-like components. This results in:

- Duplicate policies that cannot be easily reconciled
- Duplicate log databases which reduces visibility
- Inability to systematically manage unknown traffic
- Weakens the deny-all-else premise that firewalls are built on
- An IPS downstream from a firewall that has no context other than port number allowed, and has to decide whether to block purely on signature

“Fortinet provides more effective security – refer to third party validations”

- Any issues in the latest NSS report is addressed by Palo Alto Networks
- New evasions and vulnerabilities are discovered all the time, and all security vendors are constantly working to address new attacks, this is not unique to Palo Alto Networks
- Use this as an opportunity to talk about the broader issue of evasions, which includes packet, application, and encryption layer evasions

Palo Alto Networks Covering the Entire Enterprise

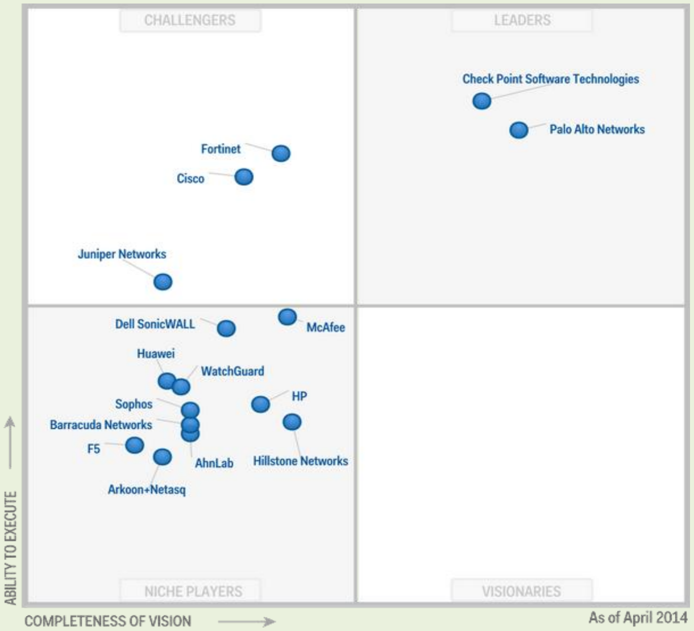


Subscriptions	WildFire™ Threat Prevention URL Filtering GlobalProtect™ Endpoint Protection
Next-Generation Firewall	PA-7050 PA-5000 Series PA-3000 Series PA-2000 Series PA-500 PA-200 *Physical:* *PA-7050, PA-5000 Series, PA-3000 Series, PA-2000 Series, PA-500, PA-200* *Virtual:* *VM-Series & VM-Series-HV for VMware NSX*
Operating System	PAN-OS™
Management System	Panorama and M-100 Appliance
Network location	Data Center • Enterprise Perimeter • Mobile Worker

Gartner MQ ENTERPRISE NETWORK FIREWALLS APRIL 2014

✓ Next-generation firewalls (NGFWs) are deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall.

✓ An NGFW should not be confused with a stand-alone network intrusion prevention system (IPS), which includes a commodity or non-enterprise firewall, or a firewall and IPS in the same appliance that are not closely integrated.


CHALLENGERS
LEADERS
Check Point Software Technologies
Palo Alto Networks
Fortinet
Cisco
Juniper Networks
Dell SonicWALL
McAfee
Huawei
WatchGuard
Sophos
HP
Barracuda Networks
F5
AhnLab
Hillstone Networks
Arkoon+Netasq
NICHE PLAYERS
VISIONARIES
ABILITY TO EXECUTE
COMPLETENESS OF VISION
As of April 2014